

**Міністерство освіти і науки, молоді та спорту України
Одеська національна академія зв'язку ім. О.С. Попова**

СИСТЕМИ ПЕРЕДАВАННЯ ДАНИХ

Том 1. Ефективність блокового кодування

Навчальний посібник

Одеса 2014

УДК 61.394; 621.397
З–38

Рецензенти:

д.т.н. проф. Климаш М.М. – Львівський національний політехнічний університет;
д.т.н. проф. Семенко А.І. – Державний університет інформаційно-комунікаційних технологій.

Рекомендовано Міністерством освіти і науки, молоді та спорту України як навчальний посібник для студентів, які навчаються за напрямом 6.050903 «Телекомунікації», 6.050904 «Мережі та системи поштового зв'язку» 6.050801 «Радіотехніка». (Лист № 1/11-16790 від 29.10.2012)

Захарченко М.В. Системи передавання даних. – Т.1: Ефективність блокового кодування / [Захарченко М.В., Кільдішев В.Й., Мартинова О.М., Ільїн Д.Ю., Трінтіна Н.А.]: навч. посіб. для студентів вищих технічних навчальних закладів, які навчаються за напрямом: 6.050903 «Телекомунікації»; 6.050904 «Мережі та системи поштового зв'язку»; 6.050801 «Радіотехніка». – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 440 с.

ISBN

У систематизованому вигляді розглянуті інформаційні характеристики джерел повідомлень, завад і каналів зв'язку, проблеми вибору сигналів та їх моделей, узгодження параметрів каналів і кодів, проблеми синтезу коригуючих помилок блокових позиційних кодів, особливості сигнальних конструкцій лінійних кодів.

Сформульовані принципи формування ефективних сигнальних конструкцій, забезпечуючих компенсацію надлишковості за рахунок зміни інформаційного параметра. Розглянуті питання збільшення пропускної здатності каналу за рахунок зміни обмежень на параметри сигналу, методи синтезу сигнальних конструкцій, виправляючих та виявляючих помилки окремих видів, алгоритми обміну приросту пропускної здатності на додаткові елементи кодових комбінацій. Проведена оцінка ефективності використання синтезованих конструкцій в однонаправлених та адаптивних системах із зворотнім зв'язком.

Розглянуті алгоритми побудови адаптивних систем із зворотнім зв'язком та симплексних систем на базі таймерних сигналів.

ISBN

© Захарченко М.В., Кільдішев В.Й.,
Мартинова О.М., Ільїн Д.Ю.,
Трінтіна Н.А., 2014
© ОНАЗ ім. О.С. Попова, 2014

ЗМІСТ

Вступ	3
ГЛАВА 1	
ІНФОРМАЦІЙНІ ХАРАКТЕРИСТИКИ ДЖЕРЕЛ ПОВІДОМЛЕНЬ. ФОРМУВАННЯ КОДОВИХ КОНСТРУКЦІЙ	13
1.1. Інформація та її виміри. Ентропія повідомлення	13
1.2. Інформаційні характеристики джерел повідомлень	26
1.3. Реєстрація елементів кодових конструкцій	47
1.4. Надійність передачі і фактори, що на неї впливають	72
1.5. Моделі потоку помилок	84
1.6. Моделі нестационарних каналів	93
1.7. Питання та задачі для самоперевірки	109
ГЛАВА 2	
СИГНАЛИ ПЕРЕДАВАННЯ ДИСКРЕТНИХ ПОВІДОМЛЕНЬ. ЗАВАДОСТІЙКІСТЬ ПРИЙМАННЯ ЕЛЕМЕНТІВ КОДОГРАМ	111
2.1. Сигнали та їх моделі	111
2.2. Спектри найбільш поширених сигналів	118
2.3. Сигнали дискретного часу та цифрова фільтрація	124
2.4. Математичні моделі вузлів апаратури зв'язку	130
2.5. Некогерентне та когерентне приймання при АМ	141
2.6. Некогерентне та когерентне приймання при ЧМ	149
2.7. Некогерентне та когерентне приймання при ФМ	161
2.8. Узгодження параметрів каналів та кодів	169
2.9. Питання та задачі для самоперевірки	193
ГЛАВА 3	
ТЕОРІЯ БЛОКОВИХ КОРИГУЮЧИХ КОДІВ	194
3.1. Основні характеристики блокових кодів, їхнє описання та властивості	194
3.2. Кодування і декодування в блокових кодах	206
3.3. Поля Галуа. Основи синтезу циклічних кодів	218
3.4. Синтез двійкових циклічних кодів	231
3.5. Лінійні блокові коди для каналів із групуванням помилок	238
3.6. Коди Ріда-Соломона	243
3.7. Декодування за максимумом правдоподібності	248
3.9. Синдромний метод декодування	266
3.10. Питання та задачі для самоперевірки	270

ГЛАВА 4	
ТАЙМЕРНІ СИГНАЛЬНІ КОНСТРУКЦІЇ ЯК ІНСТРУМЕНТАРІЙ УКРУПНЕННЯ СИГНАЛІВ ПРИ БЛОКОВОМУ КОДУВАННІ	273
4.1. Збільшення мірності сигнальних конструкцій при обмеженій довжині кодового слова	273
4.2. Виправляюча здатність групових кодів при довільному числі рівнів квантування	281
4.3. Подання сигналів через перетини нульового рівня	288
4.4. Статистичні параметри каналів моделі Гільберта	299
4.5. Передавання сигналів укрупненими сигнальними конструкціями позиційного клоодування	310
4.6. Таймерні сигнальні конструкції як інструментарій збільшення питомої ваги інформації на інтервалі найквістового елементу позиційного кодування	320
4.7. Пропускна здатність каналу при ТСК	331
4.8. Теорія синтезу простих ТСК	339
4.9. Питання та задачі для самоперевірки	344
ГЛАВА 5	
ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ ТСК В СИСТЕМАХ ПЕРЕДАВАННЯ З БЛОКОВИМ КОДУВАННЯМ	347
5.1. Синдромні методи оцінки якості передавання	347
5.2. Корегувальні коди ТСК в системі залишкових класів.	357
5.3. Основні теореми синтезу корегувальних ТСК в системі залишкових класів	370
5.4. Зв'язок коефіцієнтів рівняння якості $\sum A_i x_i = 0 \text{ mod } A_0$ з кодовою відстанню	385
5.5. Завадостійкість систем з реєстрацією нульового рівня	395
5.6. Ефективність використання наднайквістової швидкості модуляції при позиційному кодуванні	406
5.7. Ефективність корегуючи ТСК в адаптивних системах з вирішальним зворотним зв'язком (ВЗЗ)	412
5.8. Таймерні сигнальні конструкції як інструментарій укрупнення сигналів при блоковому кодуванні	425
5.9. Питання та задачі для самоперевірки	440
Література	442
Додатки	450

ВСТУП

На межі ХХ та ХХІІІ століть під впливом змін у структурі та масштабах виробництва, науково-технічного прогресу, підвищення ділової активності у суспільстві, зростання освітнього і культурного рівнів у державах, розширення зв'язків в усіх сферах життєдіяльності як у національному, так і в інтернаціональному масштабі суттєво зростає роль і значущість інформації.

Надаючи всім галузям і сферам суспільного виробництва та населенню послуги зі збирання, оброблення, передавання, зберігання та доставлення інформації, зв'язок має риси, які притаманні галузям матеріального виробництва, а саме – в галузі зв'язку також створюється споживча вартість і загальна вартість.

Економічною ж ознакою, що дозволяє віднести зв'язок до сфери матеріального виробництва є наявність трьох факторів матеріального виробництва: засобів праці, предметів праці та праці працівників зв'язку. У той самий час економічній природі зв'язку притаманні специфічні особливості.

Перша особливість визначається специфікою створюваного продукту, а саме – відсутністю при передаванні інформації матеріальних носіїв продукції.

Друга особливість зв'язку тісно пов'язана з першою і характеризується тим, що процес реалізації послуг зв'язку та їх споживання не є відокремленим за часом.

З урахуванням цієї особливості кінцевий результат виробничої діяльності галузі – послуга, не може перебувати у запасі, на складі. Вона повинна бути реалізована у нормовані терміни часу. Невідемність процесів виробництва та споживання послуг зв'язку *призводить до нерівномірності надходжень повідомлень у часі.*

Третья особливість полягає в тому, що на відміну від галузей промисловості, де предмет праці піддається речовинній зміні (механічній, хімічній тощо), надходить до сфери обліку, стає товаром і лише потім споживається. У виробничому процесі галузі зв'язку інформація, як предмет праці, повинна підлягати лише просторовому переміщенню, тобто зміні її місцезнаходження. Будь-яка інша зміна означає її спотворення, втрату споживчих властивостей та цінності, а отже завдає шкоду користувачеві.

Четверта особливість полягає в тому, що процес передавання інформації завжди є двостороннім, тобто відбувається між відправником та

отримувачем інформації. Оскільки потреба в передаванні інформації може виникнути між абонентами, що знаходяться будь-де у країні або за її межами, то це вимагає створення не тільки надійної, але й достатньо розгалуженої мережі зв'язку.

Слід зазначити, що в сучасному суспільстві обсяги інформації, що виникають та використовуються під час розв'язання виробничих, економічних, соціальних та інших задач, зростають більш швидкими темпами, ніж обсяги виробництва, сформованого матеріально-речовинними носіями. При цьому інформація стає найважливішим національним ресурсом, відмінною рисою якого є те, що він не лише не зменшується, а, навпаки, - збільшується (здебільшого при обміні даними), якісно удосконалюється і разом з тим сприяє найбільш раціональному використанню всіх інших видів інформаційних ресурсів.

Створення сучасного інформаційно-індустріального комплексу визначає необхідність прискореного розвитку засобів збирання, оброблення, збереження і передавання інформації. При цьому, чим вище рівень розвитку виробничих сил держави, тим більш високі вимоги рекомендуються до технічних засобів інформації, оскільки обсяг інформації, що виникає в процесі макроекономічного кругообігу, пропорційній валовому внутрішньому продукту (ВВП) створюваному країною. Ось чому у провідних країнах світу капітальні вклади у зв'язок завжди займали значну частку (до 4...6 %) від загальних інвестицій (кожний долар, вкладений в телекомунікації приносить три-чотири долари доходу).

Якісна перебудова виробництва на базі маніпуляторів, роботів, мікропроцесорної техніки неможлива без участі сучасних засобів електрозв'язку. Дослідження з оцінки ефективності застосування таких засобів у різних сферах свідчать про значний вигреш, який отримують споживачі послуг цієї важливої частини інфраструктури (використання зв'язку на промислових підприємствах, наприклад, скорочує на 20...25 % кількість відряджень; використання зв'язку на транспорті збільшує у 1,5...2 рази його пропускну здатність; оснащення засобами зв'язку машинного парку та польових бригад у сільському господарстві підвищує ефективність використання машин на 25 % та знижує втрати часу на 20...40 %; добре організований зв'язок у системі управління будівництвом дозволяє підвищити продуктивність праці та скоротити термін введення об'єктів в експлуатацію не менше ніж на 15 %.

За розрахунковими даними засоби електрозв'язку забезпечують економію в усіх сферах життєдіяльності суспільства у кількості не меншій

ніж 1 млрд. годин, що еквівалентно щорічній умовній економії працівників,ю зайнятих пртягом року, в кількості близько 500 тис. чол..

У той самий час через недостатній розвиток зв'язку держава та суспільство несуть значні втрати, що сягають 14 млрд. годин робочого і позаробочого часу, в тому числі близько 11 млрд. годин в галузях матеріального виробництва. Найчастіше це зумовлено незадовільним рівнем розвитку телекомунікацій, а також низькою платоспроможністю споживачів. У перерахунку на умовну економію штату це складає приблизно 5,5 млн. чол. додаткового штату або 8,4 % усіх зайнятих в суспільному виробництві.

Життя сучасного суспільства тісно пов'язане з обміном інформації. На сьогодні передавання інформації (зв'язок) є одним із найбільш дійових важелів управління економікою як усього світу, так і окремих країн.

Темпи зростання економічної, соціальної і політичної діяльності суспільства пропорційні темпам зростання сумарного трафіка в каналах обміну інформацією. Якщо з 1997 по 2003 рр. сумарний трафік зріс з 0,8 до 1,0 Тбіт/с, то за останні 5 років він досягнув 9,0 Тбіт/с.

Такими можливостями в темпах зростання обсягів надання телекомунікаційних послуг в обміні інформацією галузь зв'язку зобов'язана трьом фундаментальним відкриттям другої половини ХХ століття:

- закону Мура, який в 70-ті роки передбачив подвоєння продуктивності інтегральних схем кожні 18 місяців зменшенням їхньої вартості більш ніж у два рази за цей самий час;
- теоретичне обґрунтування можливості цифровізації будь-яких видів аналогових сигналів (теорема В.А. Котельникова);
- впровадження на телекомунікаційних мережах волоконно-оптичних технологій, які забезпечують більшу пропускну здатність (значна частина в загальному обміні інформацією належить трафіку даних, під яким насамперед розуміють трафік, що визначається обсягом обміну інформацією в цифровому вигляді).

Історія передавання даних починається з появи першого телеграфного апарата П.Л. Шилінга (1786 – 1837), в якому інформація передавалась одночасно по 8-ми проводах паралельним методом від клавіш до приймача, в якості якого використовувались 6 магнітних стрілок. Кожна зі стрілок у залежності від напрямку струму відхилялась вліво чи вправо. В 1832 р. П.Л. Шилінг продемонстрував свій телеграф російському царю Миколі II, який був приємно здивований побаченням. Наслідком цієї демонстрації було будівництво першої телеграфної мережі

з чотирьох апаратів Шилінга: в Зимовому палаці, кабінеті керівника жандармерії, міністра транспорту і однієї із фрейлін.

Міжміський телеграфний зв'язок починається в 1844 р. з організації зв'язку між Вашингтоном і Балтімором на базі апарата Морзе. Винахід літеродрукувальних пристроїв став суттєвим досягненням у популяризації телеграфного зв'язку. Кожний наступний із запропонованих літеродрукувальних апаратів був досконалішим від попереднього: 1850 р. – апарат Якобі, 1854 р. – апарат Юза, 1858 р. – апарат Уїтстона, 1874 р. – багатократний Бодо. Останній використовувався на телеграфних мережах до 50-х років ХХ століття.

Впровадження телеграфного зв'язку після Другої світової війни проходило семимильними кроками: від прокладання телеграфних ліній (Берлін – Франкфурт-на-Майні, 1853 р.; Лондон – Париж, 1852 р.). В кінці ХХ століття між Америкою та Європою знаходилось в експлуатації 20 підводних кабелів. У різних країнах (у тому числі і в СРСР) були побудовані спеціальні автоматизовані мережі телеграфного зв'язку з новітніми центрами комутації, діагностики та управління. Багато напрацьованих алгоритмів, методів кодування, сортування були адаптовані до сучасних методів передавання даних.

Історія розвитку Інтернету починається зі створення в 1958 р. (у відповідь на успішний запуск в СРСР першого супутника Землі) в США Агентства перспективних досліджень (ARPA). В цьому агентстві, яке також займалось питаннями обміну інформацією між комп'ютерами, була обґрунтована можливість побудови мережі комп'ютерного зв'язку, яка може працювати навіть при пошкодженні частини вузлів і ліній. В 1969 р. був створений інтерфейсний процесор для передачі інформаційних пакетів між комп'ютерами. В цьому ж році була створена перша мережа (ARPANET) із 4-х комп'ютерів, які були розміщені в університетах 4-х міст.

У період створення першої мережі Інтернет були напрацьовані перші технічні документи (положення, стандарти, рекомендації), регламентуючі послідовність дій при організації обміну інформацією. Щорічно перелік таких документів (Request for Comment – RFC) збільшується на десятки і на сьогодні становить понад 3500. Важливо зауважити, що ці RFC не є стандартами, а є рекомендаціями.

У 1971 р. на мережі ARPANET більшість комп'ютерів було багатофункційними, а введення єдиної програми передачі файлів дозволило створити праобраз сучасної електронної пошти.

У 1972 р. вперше був організований сеанс мережного чата, тобто комп'ютерного обміну інформацією в реальному часі (пацієнт у м. Стенфорт отримав медичну консультацію з офісу VBN). Слід зауважити, що таким режимом (чата) користувались телеграфісти при настроюванні телеграфних каналів.

Починаючи з 1983 р. кількість абонентів мережі ARPANET щорічно збільшувалась більше ніж у два рази. У 1986 р. в Інтернеті США настає новий період: науковий фонд країни вводить у дію нову мережу NSF, яка будується з конвергенцією до мережі ARPANET. NSF робить наголос на збільшення швидкості передавання, яка за два роки збільшилась з 56 кбіт/с до 1544 Мбіт/с. Це призвело до повного поглинання ARPANET.

У спільній мережі в 1989 р. функціонувало понад 100 тис. вузлів. У кінці 80-х років до NSFNET активно підключаються мережі інших країн. У 1987 р. був створений перший провайдер, який забезпечував доступ до Інтернету через модем. Зростання масштабів глобальної мережі Інтернет є прикладом прийняття технології масовим споживачем по відношенню до інших технологій: число користувачів радіо за 38 років досягло 50 млн.; глядачів телебачення – 50 млн. за 13 років; персональні комп'ютери стали доступними 50 млн. користувачів через 16 років.

Розглянемо темпи розвитку мобільного зв'язку, сучасна концепція якого була сформульована в 1971 р., а комерційна експлуатація розпочалася з 1981 року. На сьогодні стільниковим зв'язком користується понад 800 млн. абонентів.

Перші мережі пересувного зв'язку з'явилися в США у 1921 р. і використовувалися поліцією для організації зв'язку між центральним передавачем і приймачами, які знаходились на автомобілях.

Особливість перших мобільних систем, які існували до 1946 р., полягала в тому, що вони призначались для спеціального відомчого використання.

Перший переносний мобільний телефон загального користування з'явився в 1946 р. (м. Сент-Луїс). З 1946 по 1971 рр. мобільний зв'язок розвивався бурхливими темпами до появи ідеї реалізації стільникового зв'язку, що дозволило повторне використання частот у системі коміркової структури. У 1978 р. у Чикаго почалась експериментальна експлуатація системи стільникового мобільного зв'язку на 2000 абонентів. Через те, що аналогічні аналогові системи в цей період розроблялись в багатьох країнах, то стандарти їх роботи не були узгоджені. Тільки в кінці 80-х років було започатковано новий етап стільникового зв'язку, в якому використовуються цифрові методи обробки сигналів. У 1982 р.

Європейська конференція Адміністрацій Пошт і Електрозв'язку 26 країн створила спеціальну групу (Group Special Mobile) для розробки нового стандарту мережі стільникового зв'язку, в якій використовується часове ущільнення каналів, шифрування повідомлень, захист даних, використання блокового і згорткового кодування, новий вид модуляції GMSK.

Подальший розвиток мобільного зв'язку реалізується в рамках впровадження систем третього покоління: уніфіковані системи радіодоступу, об'єднуючі існуючі стільникові і "безпроводові" системи з інформаційними службами XXI століття.

Із наведених двох прикладів розвитку найбільш інтенсивно прогресуючих видів зв'язку зрозуміло, що невід'ємною частиною цифрових методів передавання інформації є її кодування.

Терміном передавання даних часто називають передавання будь-якого виду інформації, крім голосової.

Постійно зростаюча пропускна здатність оптоволоконних ліній зв'язку забезпечує більш вільне її використання. Зростання ринку оптоволоконних систем за останні 10 років призвело до зменшення вартості передавання майже на порядок, а пропускна здатність збільшилась на ту саму величину.

Незважаючи на зростання пропускної здатності і зменшення цін на послуги передавання інформації, витрати на послуги передавання даних в будь-якій організації залишаються одним із найдорожчих компонентів бюджету, передбаченого на зв'язок.

У зв'язку з цим доцільним є збільшення кількості інформації, яка передається за рахунок даного ресурсу. Існує два методи досягнення цієї мети – мультиплексування та компресія. Ці два методи можливо використовувати окремо або спільно.

Навчальна програма підготовки бакалаврів за напрямом 6.050903 – "Телекомунікації" передбачає вивчення навчальної дисципліни "Системи передавання даних", яка включає два модулі:

- 1) Завадостійке кодування.
- 2) Алгоритми і протоколи систем передавання.

Проблеми надійного й ефективного передавання інформації пов'язані з використанням ефективних кодів. Розвинена в роботах В.А. Котельникова і К.Є. Шеннона теорія передавання повідомлень оцінила граничні можливості і тим самим ініціювала виклик дослідникам, які прагнуть наблизитися до цих границь.

Подальшим розвитком сформульованих ідей ми зобов'язані вченим Т. Касамі, Кларку Дж., Галлагеру Р., Берлікемпу Е., Вітербі А.,

Нейфаку А., Фано Г., Зігангирову К., Блоху Є., Зяблову В., Золотарьову В., Овечкіну Г.

Навчальний посібник "Системи передавання даних" присвячений питанням ефективного блокового кодування. Робота включає питання синтезу оптимальних сигнальних конструкцій з метою підвищення ефективності систем передавання дискретної інформації. При описанні теорії надлишкових кодів використовувався апарат теорії матриць та n -мірної геометрії.

Перша глава посібника присвячена інформаційним характеристикам джерел повідомлень, завод і каналів зв'язку. Для бакалаврів, які навчаються за напрямами 6.050801 – "Радіотехніка", 6.050903 – "Телекомунікації", 6.050904 – "Мережі та системи поштового зв'язку", викладений матеріал є узагальненим змістом окремої навчальної дисципліни "Теорія електричного зв'язку", що вивчається до початку циклу професійної підготовки. Цінним цей матеріал є для студентів, які навчаються за бакалаврськими програмами напрямів 6.030504 – "Економіка підприємства", 6.030601 – "Менеджмент" при вивченні вибіркової навчальної дисципліни "Технологічні процеси галузі зв'язку", задача якої адаптувати зазначених фахівців до проблем конкретної галузі економічної діяльності суспільства.

У другій главі посібника розглядаються проблеми вибору сигналів та їх моделей, узгодження параметрів каналів та кодів.

Третя глава посібника присвячена проблемам синтезу корегуючих помилки блокових позиційних кодів, особливостям сигнальних конструкцій лінійних кодів.

У четвертій главі посібника розглянуті питання формування ефективних сигнальних конструкцій, забезпечуючих компенсацію надлишковості за рахунок зміни інформаційного параметра.

Розглянуті питання збільшення пропускної здатності каналу за рахунок зміни обмежень на параметри сигналу, методи синтезу сигнальних конструкцій, виправляючих та виявляючих помилки окремих видів, алгоритми обміну приросту пропускної здатності на додаткові елементи кодових комбінацій. В роботі проведена оцінка ефективності використання синтезованих конструкцій в однонаправлених та адаптивних системах із зворотнім зв'язком.

Пята глава посібника присвячена алгоритмам побудови адаптивних систем із зворотнім зв'язком та симплексних систем на базі таймерних сигналів.

Цей матеріал передбачений для використання при підготовці магістерських робіт з ефективних систем передавання.

Самоперевірка рівня якості розуміння та засвоєння матеріалу проводиться розв'язанням задач та питань, які розміщені в кінці кожної глави. Для розв'язання наведених задач без залучення допоміжної літератури в кінці посібника надані додатки.

Вважаю своїм обов'язком висловити подяку докторам технічних наук Є.М. Рудому, С.М. Горохову, А.І. Семенко, М.М. Климашу кандидатам технічних наук, доцентам О.О. Вараксіну, М.М. Балану, О.М. Мартиновій, С.В. Стайкуце порадами яких я користувався. Необхідно відзначити активну допомогу в розробці алгоритмів систем на базі таймерних сигналів, проведенні експериментів та оформленні роботи докторантів кафедри М.А. Мамедова, Гаджиєва М.М., Ільїна Д.Ю. та аспірантів Хомічу С.В., Белової Ю.В., Лемехе Т.М.

"Результати сумісних наукових робіт відображені в спільно підготовлених розділах: глава 1 – Захарченко М.В., Горохов С.М., Гаджієв М.М.; глава 2 – Захарченко М.В., Мартинова О.М., Трінтіна Н.А; глава 3 – Захарченко М.В., Горохов С.М., Ільїн Д.Ю.; глава 4 – Захарченко М.В., Кільдішев В.Й., Хомич С.В., Мартинова О.М., Михайлова Л.В.; глава 5 – Захарченко М.В., Гаджиєв М.М., Севастеев Є.О., Радзімовський Б.К., Лемеха Т.М., Белова Ю.В., Лисенко С.І."

На закінчення хочу відзначити, що теоретичною основою кодування є різні розділи вищої математики, що ставить навчальну дисципліну "Системи передавання даних" в ряд навчальних дисциплін підвищеної складності. Тому мені хотілося б особливо відзначити методичні напрацювання у викладанні теорії кодування «піонерів» практичного впровадження в реальних системах зв'язку 70-х років ХХ століття вчених ВІКА ім. А.Ф. Можайського – М.М. Буга, А.А. Вороніна, Є.В. Митряєва; ВІА ім. Ф.Е. Дзержинського – А.А. Кошевого, А.П. Мановцева; ВКАЗ ім. Будьонного – М.Я. Теплова, П.А. Котова; ОНАЗ ім. О.С. Попова – А.Г. Зюко, В.Л. Банкета.

ГЛАВА 1

ІНФОРМАЦІЙНІ ХАРАКТЕРИСТИКИ ДЖЕРЕЛ ПОВІДОМЛЕНЬ. ФОРМУВАННЯ КОДОВИХ КОНСТРУКЦІЙ

1.1. Інформація та її виміри. Ентропія повідомлення

Інформація – відомості, які є об'єктом передавання, розподілу, перетворення, зберігання чи безпосереднього використання. Це можуть бути відомості про результати вимірювання, спостереження, розрахунків тощо. Таким чином, під інформацією слід розуміти не самі предмети та процеси, а їх істотні характеристики, їхнє відбиття у вигляді чисел, формул, описів, креслень, символів чи інших абстрактних характеристик.

Легко переконатися в тому, що впровадження кількісної міри інформації є досить складною задачею. Дійсно, інформація може бути надзвичайно різноманітною: ми можемо одержати повідомлення про приїзд знайомих чи родичів, про одержання премії чи про хворобу друга; можемо почути по радіо або прочитати в газетах про ті чи інші події; дізнатись про нове відкриття чи винахід тощо. Різна інформація викликатиме у нас різні емоції і матиме різну цінність. Іноді коротке повідомлення, що містить лише кілька слів, може мати для нас невимірно більше значення, ніж текст, що складається з багатьох слів і сторінок. З двох книжок однакового обсягу ми можемо одержати зовсім різну інформацію. Два радіосигнали, що мають однакову потужність та тривалість, можуть переносити різну за змістом та обсягом інформацію. Очевидно, що кількісна міра інформації не повинна суперечити нашим інтуїтивним уявленням, має охоплювати те загальне, що є притаманним для всієї різноманітності інформації, і, головне, ця міра має бути корисною для теорії та практики побудови різних систем передавання й перетворення інформації.

У теорії інформації розглядаються:

– загальна кількісна міра інформації, яка не залежить від природи об'єктів;

– загальні закони передавання, оброблення та зберігання інформації.

Вони мають характер законів зберігання й установлюють низку найважливіших межових повідомлень, таких, як максимальна швидкість передавання інформації, найбільш важлива ефективність кодування сигналів тощо;

– загальні залежності, що визначають ті чи інші чинники, які впливають на перетворення, швидкість передавання, втрату і можливість зберігання інформації.

Незважаючи на те, що інформацію можна віднести до області абстрактних категорій, з'являється вона і в матеріально-енергетичній формі у вигляді сигналів (рис. 1.1). З передаванням та обробленням інформації пов'язані дії будь-якого автоматичного пристрою, поведінка живої істоти,

творча діяльність людини, економічні й соціальні перетворення у суспільстві й саме життя.

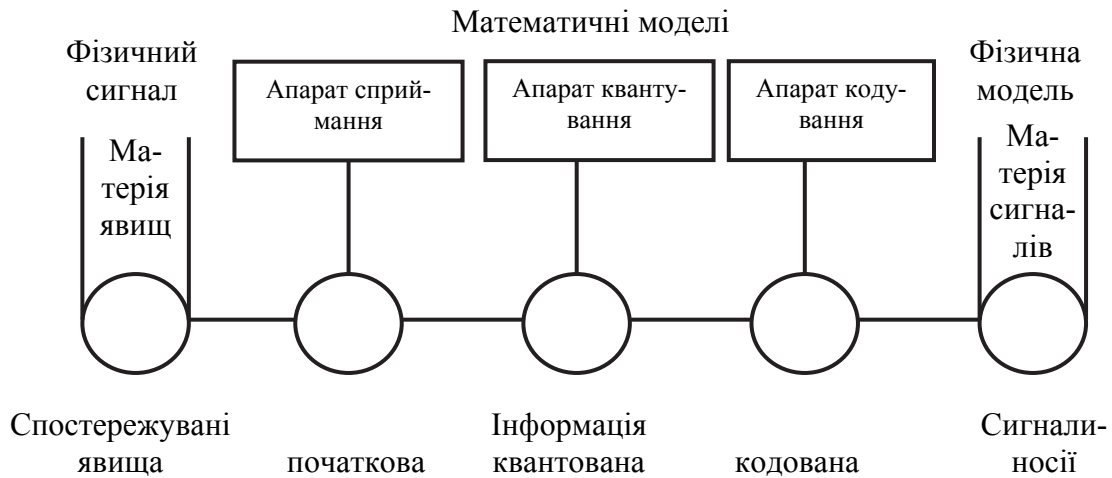


Рисунок 1.1 – Перетворення інформації при передаванні

Кількісна міра інформації. Передусім звернемо увагу на ту обставину, що будь-яка інформація здобувається внаслідок тієї чи іншої дії, якою може бути: одержання телеграми чи листа; читання книжки тощо; вимірювання тим чи іншим інструментом (приладом); просте візуальне спостереження події або за допомогою тих чи інших засобів; приймання та оброблення радіосигналів тощо.

Чим характеризується факт одержання інформації? З упевненістю можна сказати: для всіх наведених вище прикладів до дії має місце більша невизначеність щодо ситуації, яка нас цікавить.

Після одержання інформації ситуація стає більш визначеною й на поставлене питання ми можемо відповісти або однозначно, або принаймні, кількість можливих різних відповідей зменшиться, і, отже, зменшиться невизначеність, яка існувала раніше.

З рис. 1.1 випливає, що інформація передається на відстань в енергетичній формі, для чого кодується.

Одержана інформація збільшує знання й поглиблює інтелект. Інформація – це основний елемент, необхідний для прийняття рішення. Інформація, зображена в формалізованому виді, називається *даними*.

Через необхідність вірно доставати, враховувати й обробляти інформацію виникла нова дисципліна – інформатика. Ця дисципліна поставила і нові задачі перед різними галузями науки, техніки, знань, виробництва та ін.

Еволюцію оцінки інформації в різні періоди розвитку суспільства для окремих галузей діяльності показано на рис. 1.2.

Інформацію можна розрізнити за галузями знань (біологічна, технічна, економічна), за фізичною природою сприйняття (зорова, слухова, сма-

кова тощо), а також за метричними властивостями. Для технічних додатків найбільш придатною є параметрична інформація.



Рисунок 1.2 – Еволюція оцінки інформації в різні періоди розвитку суспільства

Існують три основних напрями в теорії інформації: структурний, статистичний, семантичний. Кожний з напрямів має свої галузі застосування.

Структурні міри інформації. При використанні структурних мір враховується лише дискретна будова даного інформаційного комплексу, кількість елементів, що містяться в ньому, зв'язків між ними чи комбінацій з них.

У структурній теорії розрізняються геометрична, комбінаторна та адитивна міри інформації.

За геометричного підходу визначення кількості інформації зводиться до оцінювання довжини лінії, площі чи об'єму геометричної моделі даного інформаційного комплексу в кількості одиниць – квантів. *Квант* – неподільна частина інформації, або елемент алфавіту.

Якщо дискретні відліки здійснюються по осях X , T , N відповідно через інтервали ΔX , ΔT , ΔN , то неперервні координати розпадаються на елементи в кількості

$$m_X = \frac{X}{\Delta X}; \quad m_T = \frac{T}{\Delta T}; \quad m_N = \frac{N}{\Delta N}. \quad (1.1)$$

Кількість інформації в повному комплексі визначена геометричним методом:

$$I = m_X m_T m_N. \quad (1.2)$$

Якщо використовується нерівномірна або нестационарна дискретизація, то кількість інформації визначається за більш складними формулами.

Комбінаторною мірою користуються тоді, коли необхідно оцінити можливість передавання інформації за допомогою різних комбінацій інформаційних елементів. Утворення різних комбінацій – одна з форм кодування інформації. В такому разі оцінюванню підлягає комбінаторна властивість потенційної структурної різноманітності інформаційних комплектів.

Однакові за своїми ознаками елементи можуть стати неоднаковими, якщо врахувати їхні стан, позицію. Як приклад прояву впливу елементів може слугувати перенесення знаків у позиційній системі подання двійкових чисел 00001 та 10000, коли одиниця перетворюється на 16. Переставлена точка (умовний знак) на карті докорінно може змінити воєнну ситуацію.

У комбінаториці розглядаються різні види з'єднання елементів.

З'єднання з h елементів по l розрізняються за складом елементів. Їх кількість

$$N_c = \frac{1}{h} = \frac{h!}{l!(h-l)!}. \quad (1.3)$$

Перестановки елементів розрізняються за їх порядком:

$$N_{\text{пер}} = 1 \cdot 2 \cdot 3, \dots, h = h!. \quad (1.4)$$

Перестановки з повтореннями елементів характеризуються і тим, що один із елементів повторюється α разів, другий – β разів, інший – γ разів:

$$N_{\text{пер повт}} = \frac{(\alpha + \beta + \dots + \gamma)!}{\alpha! \beta! \gamma!}. \quad (1.5)$$

Розміщення з h елементів по l відрізняються і за складом, і за порядком. Можливе число розміщень з h елементів по l

$$N_{\text{розм}} = \binom{l}{h} = \frac{h!}{(h-l)!}. \quad (1.6)$$

Можливе число розміщень з повтореннями по l з h елементів

$$N_{\text{розм повт}} = \binom{l}{h}_{\text{повт}} = h. \quad (1.7)$$

Таким чином, визначення кількості інформації $N_{\text{розм повт}}$ комбінаторною мірою полягає не в простому підрахунку квантів, як це робиться при

використанні геометричної міри, а у визначенні можливих комбінацій, тобто у структурній різноманітності. Тому кількість інформації за тієї самої кількості елементів багатократно збільшується. Наприклад, число з'єднань з 10 цифр (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) по 10 елементів:

$$N_c = \frac{10!}{0!(10-0)!} + \frac{10!}{1!(10-1)!} + \dots + \frac{10!}{10!(10-10)!} = 1024.$$

Число перестановок вказаних 10 елементів:

$$N_{\text{пер}} = h! = 1 \cdot 2 \cdot 3 \dots 8 \cdot 9 \cdot 10 = 3\,628\,800.$$

Розміщення 10 різних елементів з 10 різних позицій дають

$$N_{\text{розм}} = h^l = 10^{10} \text{ перетворень.}$$

Статистичні міри інформації. За ймовірнісним підходом інформація розглядається як повідомлення про результат випадкових величин та функцій, а кількість інформації ставиться в залежність від апріорних імовірностей цих подій.

Коли йдеться про подію, яка завжди відбувається (ймовірність якої наближається до одиниці), то повідомлення про неї є малоінформативним (інформація в словах «після ночі буде день» дорівнює 0). Так само малоінформативним є повідомлення про події (антиподії), ймовірність яких наближається до 0.

Подія та антиподія складають одну двійкову однопредметну подію. Більшість видів інформації можна звести до двійкових явищ «так – ні» або до пари «подія – антиподія». Ця пара і є найпростішим елементом (квантом) інформації. Подія може характеризуватися декількома станами, і тоді вони утворюють повну групу подій

$$p_1 + p_2 + p_3 + \dots + p_k = 1,$$

де $p_1, p_2, p_3, \dots, p_k$ – імовірності подій.

Якщо подія може набувати декількох станів, то перед її появою має місце невизначеність наслідку. Ця невизначеність називається *ентропією*.

У статистичній теорії інформації ентропія кількісно виражається як середня функція множини ймовірностей кожного зі станів:

$$\bar{I} = p = \frac{n_1(-\log_2 p_1) + n_2(-\log_2 p_2) + \dots + n_k(-\log_2 p_k)}{N},$$

де $N = \sum_{i=1}^k n_i$ – частота появи кожної з i подій,

$$I_i = \log_2 1/p_i = -\log_2 p_i$$

– кількість інформації в кожному i -му наслідку. Оскільки

$$\frac{n_i}{N} = p_i,$$

то

$$\bar{I} = -\sum_{i=1}^k p_i \log_2 p_i.$$

Середню величину інформації \bar{I} Шеннон назвав *ентропією* і позначив літерою H :

$$H = \bar{I} = -\sum_{i=1}^k p_i \log_2 p_i. \quad (1.8)$$

Основа логарифма визначає одиницю виміру ентропії та кількості інформації. Якщо основа дорівнює 2, інформація вимірюється в бітах; якщо основа $e = 2,718$, – в нітах (1 нйт = 1,4426 біт); якщо основа дорівнює 10, то за одиницю інформації прийнято 1 дїт = 3,32193 біт.

Зміна H в залежності від імовірності однопредметної події показана на рис. 1.3.

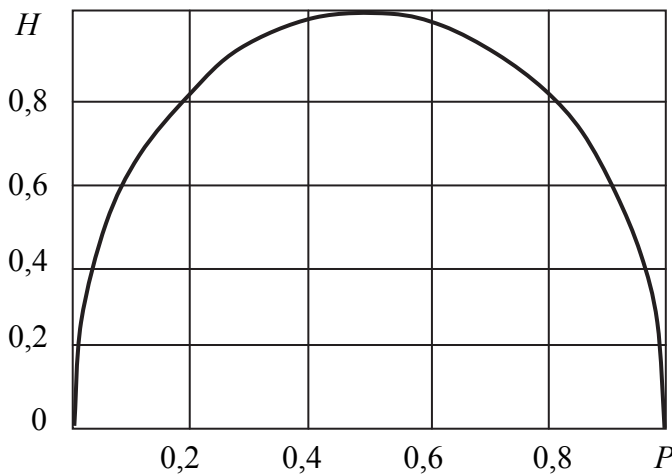


Рисунок 1.3 – Залежність ентропії від імовірності виникнення подій

Кількість інформації та надлишковість. Кількість інформації лише тоді дорівнює ентропії, коли невизначеність в результаті дослідження знімається повністю:

$$I = H.$$

У разі неповного розв'язання має місце часткова інформація, яка являє собою різницю початкової H_1 та кінцевої H_2 ентропії:

$$I = H_1 - H_2.$$

Абсолютна надлишковість

D_a інформації являє собою різницю між максимально можливою кількістю інформації та ентропією:

$$D_a = I' - H = H_{\text{макс}} - H.$$

Відносна надлишковість

$$D_b = \frac{H_{\text{макс}} - H}{H_{\text{макс}}} = 1 - \frac{H}{H_{\text{макс}}}. \quad (1.9)$$

Визначимо відносну надлишковість для двох джерел.

Приклад 1. Повна шкала вимірювання містить $H_{\text{макс}} = 1000$ елементарних одиниць (квантів), але припускається похибка $\pm 1\%$ повної шкали. Тоді $H = 50$, оскільки за похибки ± 10 квантів досить всю шкалу поділити на 50 квантів:

$$D_b = 1 - \frac{50}{1000} = 0,95.$$

Приклад 2. Випадкова величина $x(t)$ змінюється за законом, зображеним на рис. 1.4. На відрізку $t_2 - t_1$ $x(t)$ може змінюватися лише від x_2 до x_1 ; $x_1 = 4$, $x_2 = 11$; $D_B = 1 - \frac{4}{11} = 0,64$. Ця надлишковість пояснюється тим, що постійна складова $x_1 - x_0$ не несе інформації.

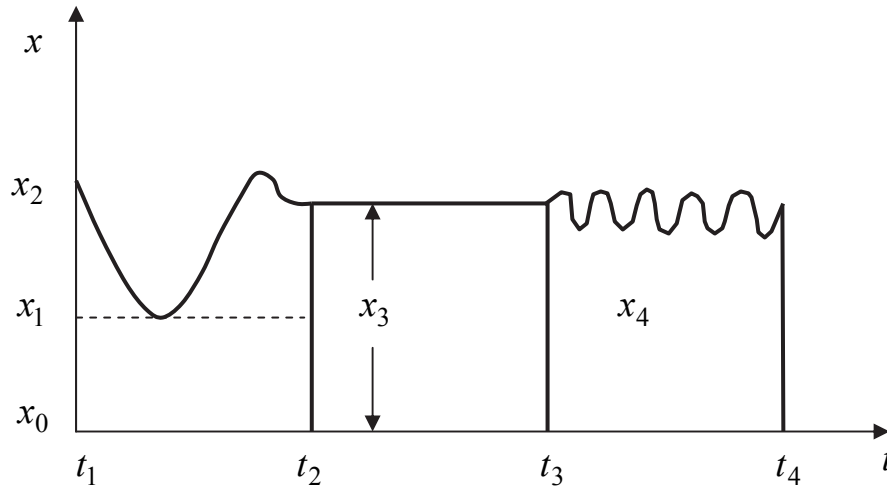


Рисунок 1.4 – Зміни неперервної величини у часі

Як випливає з наведених вище виразів, кількість інформації залежить від числа можливих станів системи. Для випадку систем зв'язку інформація залежить від числа можливих станів сигналу на виході передавача та приймача. Якщо події на вході каналу x_i ($i = 1, 2, \dots, m$), а на виході - y_j ($j = 1, 2, \dots, m$), то ймовірності виникнення подій x_i , y_j позначаються $p(x_i)$, $p(y_j)$. Ймовірність появи на виході y_j за наявності на вході x_i позначається $p(y_j/x_i)$.

Ймовірність $p(y_j/x_i)$ означає, що передавався символ x_i з появою сигналу на виході y_j :

$$\sum_{i=1}^m p(x_i) = \sum_{j=1}^m p(y_j) = 1;$$

$$p(x_i) = \sum_{j=1}^m p(x_i/y_j).$$

Кількість інформації, що міститься в події y_j відносно події x_i ,

$$I(x_i y_j) = \log_2 \frac{p(x_i/y_j)}{p(x_i)} = \log_2 \frac{p(x_i/y_j)}{p(x_i)p(y_j)}. \quad (1.10)$$

Умовна власна інформація події y_j за відомого x_i

$$I(x_i/y_j) = -\log p(x_i/y_j).$$

Власна інформація спільної події

$$I(x_i y_j) = -\log_2 p(x_i y_j).$$

Середня кількість взаємної інформації про систему X , що міститься в y_j ,

$$I(X, y_j) = -\sum_{i=1}^m p(x_i / y_j) \log_2 \frac{p(x_i / y_j)}{p(x_i)}.$$

Середня кількість взаємної інформації про систему X , що міститься у множині Y ,

$$I(X, Y) = -\sum_{i=1}^m \sum_{j=1}^n p(x_i / y_j) \log_2 \frac{p(x_i / y_j)}{p(x_i)}.$$

Середня власна інформація дорівнює ентропії:

$$\bar{I} = I(x) = -\sum_{i=1}^m p(x_i) \log p(x_i) = H(x).$$

Якщо система Y перебуває у стані y_j , то міра невизначеності системи X

$$H(X / y_j) = -\sum p(x_i / y_j) \log_2 p(x_i / y_j).$$

Міра невизначеності стану системи X після того, як стан системи Y повністю визначився, характеризується умовною ентропією

$$H(X / Y) = -\sum_{i=1}^m \sum_{j=1}^n p(x_i / y_j) \log_2 p(x_i / y_j). \quad (1.11)$$

Міра невизначеності стану складної системи характеризується ентропією поєднаної системи

$$H(X, Y) = -\sum_{i=1}^m \sum_{j=1}^n p(x_i / y_j) \log_2 p(x_i / y_j).$$

Якщо X та Y незалежні, то

$$H(X, Y) = H(X) + H(Y).$$

Для залежних X та Y

$$H(X, Y) = H(X) + H(Y / X) = H(Y) - H(X / Y).$$

Оскільки $H(X) = I(X)$, то середня взаємна ентропія

$$\begin{aligned} I(X, Y) &= H(X) - H(X / Y) = H(Y) - H(Y / X) = \\ &= H(X) + H(Y) - H(X, Y). \end{aligned} \quad (1.12)$$

Щоб інформацію можна було доставляти, зберігати, обробляти та використовувати, вона має бути подана у вигляді повідомлення, тобто повідомлення є формою подання інформації. Одну й ту саму інформацію можна подати в різній формі. Наприклад, повідомлення про час приїзду приятеля може бути передано телефоном чи у вигляді телеграми. У першому випадку маємо справу з неперервним повідомленням – змінюваним непе-

первно значенням напруги на виході мікрофона. У другому випадку повідомлення складається з окремих літер, тому називається дискретним.

Неперервне повідомлення характеризується нескінченним числом значень на скінченному інтервалі часу: число рівнів напруги на виході мікрофона зростає зі зменшенням порога розрізнення.

Дискретне повідомлення характеризується скінченним числом значень на нескінченному інтервалі часу: хоч скільки телеграм передаватимемо - число літер є скінченним.

Неперервні повідомлення легко перетворити на дискретні. Тому доцільно розглядати лише дискретні повідомлення.

Основні властивості ентропії. Сформулюємо деякі основні властивості ентропії як міри невизначеності результату ансамблю подій.

1. $H = 0$ лише в тому випадку, коли всі ймовірності $p(x_i)$, крім однієї, дорівнюють нулю, а ця єдина ймовірність дорівнює одиниці. Отже, $H = 0$ тільки у випадку повної визначеності результату досліду, а в інших випадках $H > 0$.

Останнє випливає з того, що ймовірність події p_i може лежати лише в інтервалі між нулем і одиницею, тобто $0 \leq p_i \leq 1$ і, отже, $-p_i \log p_i \geq 0$.

2. При заданому n H максимальна і дорівнює

$$H(X) = \log n$$

лише тоді, коли всі події рівноймовірні, тобто

$$p(x_1) = p(x_2) = \dots = p(x_n) = \frac{1}{n}.$$

Інтуїтивно зрозуміло, що такий стан відповідає найбільшій невизначеності. Ця властивість ентропії при $n = 2$ ілюструється рис. 1.3.

У загальному випадку вона може бути доведена таким чином.

Позначимо $p(x_i) = p_i$ і представимо вираз ентропії у вигляді

$$H = -\sum_{i=1}^n p_i \log p_i. \quad (1.13)$$

Крім того, повинна виконуватись очевидна умова

$$\sum_{i=1}^n p_i - 1 = 0.$$

Знайдемо значення p_i , за яких ентропія H має максимальне значення.

Згідно з правилом відшукування відносного максимуму функції декількох перемінних

$$\frac{\partial}{\partial p_i} \left[H + \lambda \left(\sum_{i=1}^n p_i - 1 \right) \right] = 0,$$

де λ – множник Лагранжа.

Підставивши в останню рівність H із (1.13) і виконавши диференціювання, одержимо

$$-\frac{1}{\ln 2} (\ln p_i + 1) + \lambda = 0 \text{ або } p_i = e^{-\lambda_1}, \quad (1.14)$$

де $\lambda_1 = 1 - \lambda \ln 2$.

З останніх виразів виходить, що $ne^{-\lambda_1} = 1$, звідки $\lambda_1 = \ln n$. Підставляючи це значення λ_1 в (1.14), одержимо

$$p_i = \frac{1}{n},$$

що відповідає рівній імовірності подій (повідомлень).

Неважко переконатися в тому, що знайдене екстремальне значення p_i відповідає максимуму.

Приклад 3. Візьмемо два ансамблі подій: X і Y , які описуються однаковими схемами

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_n) \end{pmatrix},$$

$$Y = \begin{pmatrix} y_1 & y_2 & \dots & y_m \\ p(y_1) & p(y_2) & \dots & p(y_m) \end{pmatrix}.$$

Будемо тепер розглядати спільні події x_i і y_j . Всі можливі пари (x, y) можуть розглядатися як елементи нового об'єданого ансамблю $X \otimes Y$.

Позначимо через $p(x_i, y_j)$ ймовірність спільної появи подій x_i і y_j .

Об'єднаний ансамбль описує (характеризує) більш складну фізичну систему, яка складається із двох підсистем X і Y , або таку систему, в якій стан або події можуть бути поділені на дві характерні групи X і Y . Зокрема, події x можуть породжувати події y (бути причиною), або навпаки.

Об'єднаний ансамбль $X \otimes Y$ може розглядатися як деякий новий ансамбль, в якому можливі nm різних подій (x, y) з заданим розподілом імовірностей $p(x, y)$.

Схема об'єданого ансамблю може бути записана у вигляді

$$X \otimes Y = \left(\begin{array}{c|cccc} & x_i & & & \\ \hline y_j & x_1 & x_2 & \dots & x_n \\ \hline y_1 & p(x_1, y_1) & p(x_2, y_1) & \dots & p(x_n, y_1) \\ y_2 & p(x_1, y_2) & p(x_2, y_2) & \dots & p(x_n, y_2) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots \\ y_m & p(x_1, y_m) & p(x_2, y_m) & \dots & p(x_n, y_m) \end{array} \right)$$

Ентропія такого ансамблю, тобто ентропія результату спільних подій (x, y) , дорівнює

$$H(X, Y) = - \sum_{i=1}^n \sum_{j=1}^m p(x_i, y_j) \log p(x_i, y_j). \quad (1.15)$$

$$H(Y) = - \sum_{j=1}^m p(y_j) \log p(y_j), \quad (1.16)$$

Приклад 4. Відомо, що ймовірність спільної події дорівнює

$$p(x_i, y_j) = p(x_i) p(y_j | x_i), \quad (1.17)$$

де $p(y_j | x_i)$ – ймовірність події y_j за умови, що відбулася подія x_i (умовна ймовірність y_j). Якщо врахувати також, що

$$\sum_{j=1}^m p(x_i) p(y_j | x_i) = p(x_i),$$

то рівність (1.15) можна подати у вигляді

$$H(X, Y) = - \sum_{i=1}^n p(x_i) \log p(x_i) - \sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j | x_i) \log p(y_j | x_i)$$

або

$$H(X, Y) = H(X) + H(Y | X),$$

де

$$H(Y | X) = - \sum_{i=1}^n p(x_i) \sum_{j=1}^m p(y_j | x_i) \log p(y_j | x_i).$$

$H(Y | X)$ ми будемо називати умовною ентропією ансамблю Y .

Із останнього виразу випливає, що $H(Y | X)$ дорівнює математичному сподіванню величин

$$H(Y | x_i) = - \sum_{j=1}^m p(y_j | x_i) \log p(y_j | x_i).$$

Визначення кількості інформації за неповної вірогідності результатів дослідів. Ми вже вказували, що інформація про ту чи іншу подію або факт досягається завжди в результаті того чи іншого дослідів, причому після дослідів ситуація виявляється не завжди повністю визначеною, і ми не можемо з повною вірогідністю стверджувати, яка саме подія мала місце. Визначимо кількість інформації, яка припадає в середньому на один досвід, коли повна вірогідність його результату відсутня.

Припустимо, що події або факти, які нас цікавлять, складають ансамбль X , а результати дослідів (наприклад, одержання повідомлень) на основі яких ми виносимо судження про результати подій x , складають ансамбль Y . Позначимо через $p(x_i | y_j)$ ймовірність того, що за відомого нам результату дослідів y_j мала місце подія x_i . Якщо, наприклад,

$$p(x_i | y_j) = \begin{cases} 1 & \text{за } j = l, \\ 0 & \text{за } j \neq l, \end{cases} \quad (1.18)$$

то в результаті досліду ситуація повністю визначена, і ми можемо з повною достовірністю стверджувати, яка подія x_i мала місце. Тому що невизначеність результату подій x до досліду дорівнювала $H(X)$, а після досліду невизначеність відсутня, то в цьому випадку

$$I(Y, X) = H(X) \frac{\text{Дв. од.}}{\text{дослід}}, \quad (1.19)$$

де $I(Y, X)$ – кількість інформації, яка міститься в середньому в дослідах y відносно подій x .

У більш загальному випадку, коли $0 < p(x_i | y_j) < 1$ для різних j , після досліду залишається невизначеність, яка в середньому може характеризуватись умовною ентропією $H(X | Y)$.

Кількість інформації, що одержуємо в середньому на один дослід, тепер може бути знайдена як зміна невизначеності в результаті досліду, і, отже,

$$I(Y, X) = H(X) - H(X | Y) \frac{\text{Дв. од.}}{\text{дослід}}, \quad (1.20)$$

де

$$H(X | Y) = - \sum_{j=1}^m p(y_j) \sum_{i=1}^n p(x_i | y_j) \log p(x_i | y_j) \frac{\text{Дв. од.}}{\text{дослід}}. \quad (1.21)$$

Легко побачити, що в окремому випадку, коли виконується (1.19), умовна ентропія $H(X | Y) = 0$ та (1.20) співпадає з (1.19).

Слід зауважити, що кількість інформації, що міститься в дослідах y відносно випадкових подій x , дорівнює кількості інформації, що міститься у випадкових подіях x відносно результату дослідів y .

Загальні зауваження про введення кількісної міри інформації. Наведені вище фундаментальні співвідношення визначають кількісну міру інформації, яка міститься в одній випадковій події (досліді) – Y відносно іншої випадкової події – X . При цьому ми мали на увазі такі події, в яких число можливих результатів (дослідів) скінченне. Події з нескінченно великим числом виходів розглядаються нижче.

Зі структури вказаних формул видно, що в основу вимірювання кількості інформації покладаються лише ймовірності (статистичні) характеристики подій. При цьому цілком ігнорується смисловий зміст інформації або, як говорять, її семантика, а також цінність інформації для її одержувача, можливі наслідки, що викликаються одержанням даної інформації та інші обставини.

Так, наприклад, батька, який одержав повідомлення про те, що його жінка народила трійню, можуть хвилювати не рідкість (мала ймовірність)

цієї події, а такі питання, як необхідність розширення помешкання, додаткової закупівлі речей і тому подібне. Теорія інформації все це ігнорує і кількість інформації, що міститься в даному повідомленні, визначає лише на основі статистики подій.

Наведемо ще один приклад.

Приклад 5. Припустимо, що організована лотерея, де ймовірність виграшу різних предметів однакова. Тоді повідомлення про виграш авто-ручки чи автомобіля з точки зору розглядуваної теорії містить однакову кількість інформації. Зрозуміло, що для одержувача цих повідомлень буде не байдуже, який з них він отримає.

Такий підхід до визначення кількісної міри інформації у сучасній теорії має як сильні, так і слабкі сторони.

Позитивними якостями введеної статистичної міри кількості інформації є:

1) спільність (універсальність) цієї міри, тому що вона пристосована до інформації будь-якого виду і змісту;

2) об'єктивність і незалежність від психологічних чинників, бо статистичні показники подій об'єктивні й установлюються на основі експерименту;

3) для аналізу роботи і вибору оптимальних характеристик більшості систем передачі і перетворення інформації ця міра є достатньою і найбільш раціональною.

У той самий час та обставина, що сучасна теорія інформації бере до уваги лише статистичні характеристики розглянутих подій, обмежує область її застосування.

Для випадків, коли повинні братися до уваги семантика або цінність інформації, ця теорія непридатна. Останнім часом робляться спроби розширення області застосування теорії інформації і введення, наприклад, об'єктивних показників цінності інформації.

Теорія інформації, існуюча на даний час, використовуючи статистичний підхід до визначення кількісної міри інформації, дозволяє аналізувати й установлювати загальні закони для величезного числа явищ у техніці і живій природі.

Розглянемо два типи найважливіших обмінів, що відбуваються в природі, техніці і суспільстві: енергетичний та інформаційний. Енергетичний обмін пов'язано з перетворенням одного виду енергії в іншій, з виконанням певної роботи робочими органами машин і т.п.

Для вивчення енергетичних обмінів необхідно було знайти спільну міру енергії для різних її видів, закони перетворення енергії, чинники, що визначають коефіцієнт корисної дії і т.п. Всі ці загальні закономірності були установлені ще в XVIII-XIX століттях.

Інформаційні обміни хоча і зв'язані з енергетичними, однак останні відіграють в них допоміжну роль. Важливими для інформаційних обмінів є

кількість одержуваних або перероблених відомостей (інформації), їхня ймовірність і втрати за різних перетворень.

Загальні закони для інформаційних обмінів встановлюються сучасною теорією інформації, що безпосередньо вказує на її значущість.

1.2. Інформаційні характеристики джерел повідомлень

Поняття про ергодичне джерело повідомлень. Джерелом повідомлень може бути об'єкт, стан якого визначається деяким фізичним процесом, проходить в часі або в просторі за випадковим (заздалегідь не відомим нам) законом.

Повідомлення про цей процес можуть безпосередньо сприйматися або фіксуватися (реєструватися) спостерігачем або автоматичною апаратурою, або передаватися на відстань по тому або іншому каналу.

Джерелами повідомлень, для яких характерна зміна їхнього стану в часі, можуть бути: людина, що виголошує промову або грає на музичному інструменті, прилад, що вимірює температуру, вологість, тиск або будь-які інші фізичні параметри і т.п.

Прикладами джерел повідомлень з просторовим розподілом носія інформації є книги, картини, записи на магнітну стрічку й інші. Надто часто має місце з'єднання розподілу в просторі і в часі: дії на сцені, в театрі, кінокартині і т.п.

При передаванні і перетворенні інформації, як правило, відбувається перетворення просторового розподілу в часове, внаслідок чого в подальшому ми будемо розглядати лише джерела повідомлень, які характеризуються випадковим процесом, що розвивається в часі. Однак всі одержані нижче висновки можуть бути безпосередньо застосовані і до джерел з просторовим розподілом носія інформації. В даній роботі розглядаються характеристики джерел дискретних повідомлень.

Такими дискретними повідомленнями можуть бути: літери або прості цифри, сукупність літер – слова або фрази, що мають певний смисловий зміст, типові команди або розпорядження, повідомлення про можливі дискретні стани об'єктів або подій, результати вимірювань виражених числами і т.п.

Будемо вважати, що число різних повідомлень скінченне, і позначатимемо їх символами x_1, x_2, \dots, x_n . Помітимо, що в даному випадку різними символами можуть позначатися як елементарні повідомлення типу «так», «ні» або «ввімкнути», «вимкнути», цифри 0, 1, ..., так і більш складні, наприклад, стандартні тексти, числа з заданим числом розрядів і т.п.

Важливо лише, щоб кожне повідомлення незалежно від складності його смислового змісту, було цілком визначено.

Джерело дискретних повідомлень виробляє деяку послідовність символів x_i , причому порядок проходження цих символів випадковий і характеризується деякою сукупністю ймовірностей.

Математична модель такої системи називається *стохастичним процесом*.

Нас буде цікавити питання про те, яка в середньому кількість інформації створюється таким джерелом на один символ або за одиницю часу. Для відповіді на це питання необхідно з'ясувати, які ймовірнісні (статистичні) показники можуть схарактеризувати розглядуване джерело. Незавжди переконалися в тому що одних імовірностей появи окремих символів в даному випадку для описання джерела, недостатньо. Розглянемо приклад.

Приклад 6. Припустимо, що передається послідовність із символів x_1, x_2, x_3 і x_4 з ймовірностями $p(x_1)=0,5$; $p(x_2)=0,25$; $p(x_3)=p(x_4)=0,125$. При цьому символ x_4 завжди передається після символу x_3 . Легко побачити, що хоча ймовірності передавання символів x_3 і x_4 однакові, але символ x_4 не несе ніякої інформації, бо, одержавши символ x_3 , ми уже достовірно знаємо, що наступним буде символ x_4 . Отже, необхідні більш глибокі і детальні ймовірні характеристики джерела і, зокрема, треба врахувати залежність імовірності передавання даного символу x_i від того, які символи були передані раніше. Ймовірнісні або, як їх ще називають, корелятивні зв'язки між символами можуть розповсюджуватись на більші або менші групи символів. Припустимо, наприклад, що передавана послідовність символів є $x_g, x_h, x_i, x_j, \dots$; якщо символи незалежні, то умовна ймовірність передавання символу x_j дорівнює

$$p(x_j | x_i, x_h, x_g, \dots) = p(x_j)$$

для всіх g, h, i, j ; якщо є корелятивний зв'язок тільки між двома сусідніми символами, то

$$p(x_j | x_i, x_h, x_g, \dots) = p(x_j | x_i),$$

тобто ймовірність передавання символу x_j залежить лише від того, який був попередній символ x_i , і не залежить від символів, які передавались раніше; у випадку, коли такий зв'язок є між трьома сусідніми символами

$$p(x_j | x_i, x_h, x_g, \dots) = p(x_j | x_i, x_h).$$

Аналогічні співвідношення можуть бути написані при розповсюдженні корелятивних зв'язків та групи з великого числа символів.

У більшості джерел, що зустрічаються на практиці, корелятивні зв'язки розповсюджуються на кінцеве число попередніх символів; такі джерела називаються *ергодичними*. В ергодичному джерелі для символів x_g, \dots, x_s , віддалених надто далеко один від одного, корелятивний зв'язок відсутній, тобто поява x_s не залежить від того, яким було x_g , і, отже, $p(x_s | x_g) = p(x_s)$ для всіх g .

Ергодичні послідовності володіють властивостями ергодичних функцій. Будь-яка досить довга (з великим числом символів) ергодична послідовність з імовірністю, як завгодно близькою до одиниці, буде *типовою*. Останнє означає, що частота передавання будь-якого символу (наприклад, x_i)¹ в цій послідовності відрізняються від імовірності передавання цього символу – $p(x_i)$ на скільки завгодно малу величину, частота передавання x_j після x_i мало відрізняється від умовної ймовірності $p(x_j | x_i)$ і т.п. Таким чином, досить довга ергодична послідовність, яка є частиною всієї послідовності символів, що виробляється джерелом повідомлення, з імовірністю, близькою до одиниці, характеризує ймовірності окремих символів і корелятивні зв'язки між ними, властиві джерелу. Ця властивість ергодичних джерел є надто важливою. Як приклад ергодичних повідомлень можна навести мову. Майже у будь-якій книзі даною мовою (якщо це тільки не дуже спеціалізована література, як, наприклад, тлумачний або енциклопедичний словник або праця, насичена спеціальними термінами) частота окремих літер і з'єднання різних літер однакова, хоча смисловий зміст книг різний. Ця обставина дозволяє застосувати математичний апарат при вивченні структури мови і має велике значення для побудови систем зв'язку, машин для друку, перекладу та ін.

Ентропія ергодичного джерела. Одержане раніше співвідношення (1.8) не може бути використане для обчислення ентропії ергодичного джерела, оскільки воно справедливе лише для незалежних повідомлень і, отже, не враховує корелятивних зв'язків. Урахування корелятивних зв'язків значно спрощується для ергодичного джерела повідомлень. Для такого джерела може бути знайдене кінцеве число характерних станів – S_1, S_2, \dots таких, коли умовна ймовірність появи чергового символу залежить лише від того, в якому із цих станів знаходиться джерело. Виробляючи черговий символ, джерело переходить із одного стану в іншій або повертається в вихідне положення².

Розглянемо окремі випадки. Якщо корелятивні зв'язки в послідовностях, що виробляються деяким джерелом, відсутні, то у джерела є лише один характерний стан S_1 . Ймовірність появи символу x_i в момент, коли система знаходиться в цьому стані, дорівнює $p(x_i)$; виробивши символ x_i , джерело повертається в той самий стан S_1 . На рис. 1.5 наведена діаграма переходу для джерела, що має один характерний стан S_1 і виробляє три різних символи – x_1, x_2 і x_3 . Стан джерела показано на графіку точкою, лінії зі стрілками характеризують процес генерації символів, надписи біля ліній показують імовірність цього процесу, якщо стан джерела нам відомий.

¹ Частота x_i в даному випадку визначається як відношення числа символів x_i до загального числа символів у розглядуваній послідовності.

² Стохастичний процес такого типу в математиці називається ланцюгом Маркова.

Коли корелятивні зв'язки мають місце лише між двома сусідніми символами, ймовірність появи символу x_i залежить лише від того, який символ був вироблений до цього. Джерело, що генерує n різних символів – x_1, x_2, \dots, x_n , в цьому випадку може мати n характерних станів; S_1 – після появи символу x_1 ; S_2 – після появи символу x_2 і т.п. Приклад такого джерела для випадку $n = 3$ наведений на діаграмі рис.1.6. Для опису такого джерела необхідно задати розподіл ймовірностей $p(x_i)$ і ймовірностей переходів $p(x_i | x_j)$ для всіх i, j . Замість цього можуть бути задані ймовірності всіх можливих пар символів – $p(x_i, x_j)$.

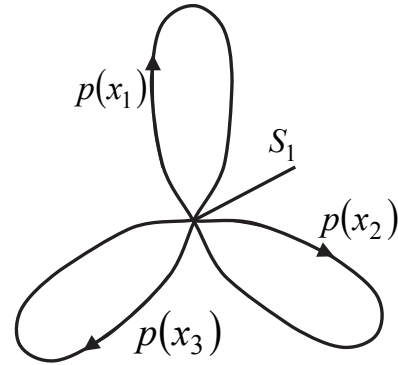


Рисунок 1.5 – Діаграма переходу для джерела, що має один характерний стан S_1 і виробляє три різних символи – x_1, x_2 і x_3

Якщо відомі $p(x_i, x_j)$, то $p(x_i)$ і $p(x_i | x_j)$ можуть бути знайдені за відомими формулами

$$p(x_i) = \sum_j p(x_i, x_j), \quad p(x_i | x_j) = \frac{p(x_i, x_j)}{p(x_j)}.$$

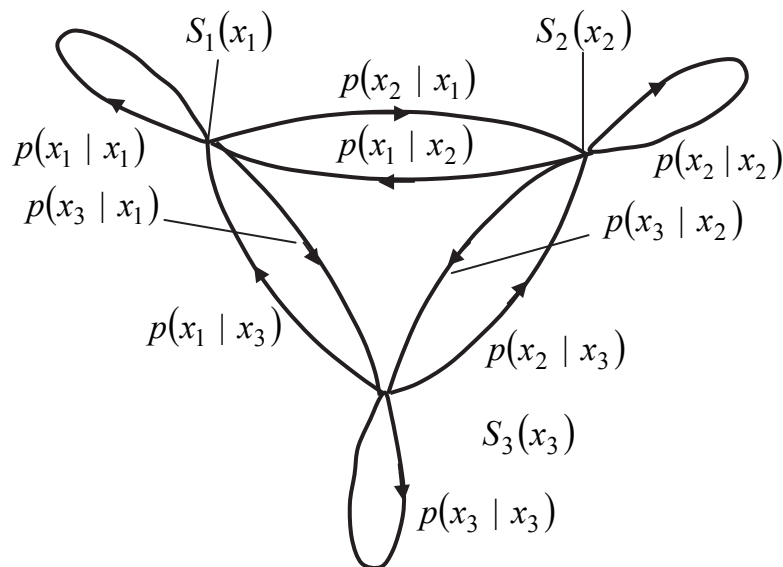


Рисунок 1.6 – Приклад джерела для випадку $n = 3$

Якщо корелятивні зв'язки є тільки між трьома символами, то ймовірність появи символу x_i залежить від того, які два символи були вироблені перед цим, отже, число характерних станів джерела визначається числом різних пар x_i, x_j . Для опису такого джерела повинні бути задані ймовірності

сті появи окремих символів $p(x_i)$ і ймовірності переходів $p(x_i | x_j, x_h)$, або ймовірності всіх можливих груп, що складаються із трьох символів – $p(x_i, x_j, x_h)$.

Ентропію джерела повідомлень ми будемо обчислювати у припущенні, що воно працює довгий час, і кожного разу, коли ми чекаємо появи чергового символу, нам відомо, які символи були вироблені раніше, і, отже, нам відомо, в якому характерному стані знаходиться джерело. Очевидно, що при цьому досить пам'ятати лише ті символи, які корелятивно зв'язані з очікуванням. За такої умови ентропія джерела повідомлень може обчислюватись вже як умовна ентропія.

Припустимо, що розглядуване джерело повідомлень x_1, \dots, x_n має характерні стани S_1, S_2, \dots, S_n , при цьому $p(S_l | S_k)$ є ймовірністю того, що джерело, знаходячись в стані S_k , перейде в стан S_l при появі чергового символу; тоді

$$H(X) = - \sum_k p(S_k) \sum_{l|k} p(S_l | S_k) \log p(S_l | S_k) \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}, \quad (1.22)$$

де $p(S_k)$ – ймовірність стану S_k . Знаки біля сум означають: k – підсумовування за всіма можливими станами; $l|k$ – за всіма можливими переходами зі стану S_k в S_l .

Співвідношення (1.22) може бути також записане у вигляді

$$H(X) = - \sum_k p(S_k) H(S_k) \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}},$$

де

$$H(S_k) = - \sum_l p(S_l | S_k) \log p(S_l | S_k) \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}},$$

$H(S_k)$ є ентропія джерела в стані S_k і, отже, ентропія $H(X)$ є середнє значення (математичне сподівання) ентропій всіх характерних станів джерела.

У випадку, коли символи джерела незалежні, є лише один стан S_1 , ймовірність якого $p(S_1) = 1$. З появою символу x_i джерело знову повертається в стан S_1 , і при цьому $p(S_1 | S_1) = p(x_i)$ і, отже,

$$H(X) = H(S_1) = - \sum_{i=1}^n p(x_i) \log p(x_i),$$

що повністю співпадає з (1.8).

Якщо корелятивні зв'язки є лише між двома сусідніми символами, то $p(S_k) = p(x_k)$ і $p(S_l | S_k) = p(x_l | x_k)$. Тоді із (1.22) одержимо

$$H(X) = - \sum_{k=1}^n p(x_k) \sum_{l=1}^n p(x_l | x_k) \log p(x_l | x_k) \quad (1.23)$$

або, тому що порядок підсумовування значення не має, то

$$H(X) = - \sum_{k=1}^n \sum_{l=1}^n p(x_k, x_l) \log p(x_l | x_k) \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}$$

У випадку, коли корелятивні зв'язки є між трьома символами, характерні стани визначаються передаванням двох символів, і їх зручно нумерувати двома індексами; так, якщо генеруються $x_h x_j$, то джерело переходить в стан S_{hj} . Тоді

$$p(S_{hj}) = p(x_h, x_j) \text{ і } p(S_{jl} | S_{hj}) = p(x_l | x_h, x_j).$$

Із (1.22) одержуємо

$$H(X) = - \sum_{h=1}^n \sum_{j=1}^n p(x_h, x_j) \sum_{i=1}^n p(x_i | x_h, x_j) \log p(x_i | x_h, x_j)$$

або

$$H(X) = - \sum_{h=1}^n \sum_{j=1}^n \sum_{i=1}^n p(x_h, x_j, x_i) \log p(x_i | x_h, x_j) \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}$$

Аналогічні співвідношення утворюються й у випадках, коли корелятивні зв'язки розповсюджуються на більше число символів.

Розглянемо декілька прикладів на визначення ентропії джерела.

Приклад 7. Джерело виробляє чотири символи: x_1, x_2, x_3, x_4 з ймовірностями $p(x_1) = p(x_2) = p(x_3) = p(x_4) = \frac{1}{4}$.

Корелятивні зв'язки між різними символами відсутні. Безпосередньо використовуючи $H(X) = \log n$, одержимо

$$H(X) = 2 \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}$$

Приклад 8. Ймовірність появи символів джерела дорівнює $p(x_1) = \frac{1}{2}, p(x_2) = \frac{1}{4}, p(x_3) = p(x_4) = \frac{1}{8}$.

Корелятивні зв'язки між символами відсутні.

Для цього випадку, використовуючи (1.8), знаходимо

$$H(X) = \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + 2 \frac{1}{8} \log_2 8$$

або

$$H(X) = \frac{7}{4} = 1,75 \quad \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}$$

Приклад 9. Ймовірності появи символів джерела такі ж самі, як і в прикладі 4, але між двома сусідніми символами мають місце корелятивні зв'язки, які описуються табл. 1.1. У 2-му стовбці цієї таблиці наведені ймовірності різних з'єднань із двох символів, що дає повний опис статистичних властивостей даного джерела. Із нього можуть бути одержані ймовірності появи окремих символів $p(x_i)$ і ймовірності переходів $p(x_j | x_i)$, наведені у 3-му стовбці.

Таблиця 1.1 – Корелятивні зв'язки між подіями

x_i, x_j	$p(x_i, x_j)$	$p(x_j x_i)$	x_i, x_j	$p(x_i, x_j)$	$p(x_j x_i)$
x_1, x_1	13/32	13/16	x_3, x_1	0	0
x_1, x_2	3/32	3/16	x_3, x_2	0	0
x_1, x_3	0	0	x_3, x_3	0	0
x_1, x_4	0	0	x_3, x_4	1/8	1
x_2, x_1	1/32	1/8	x_4, x_1	1/16	1/2
x_2, x_2	1/8	1/2	x_4, x_2	1/32	1/4
x_2, x_3	3/32	3/8	x_4, x_3	1/32	1/4
x_2, x_4	0	0	x_4, x_4	0	0

Із табл. 1.1 видно, що за символом x_3 в даному джерелі завжди проходить символ x_4 , а після символу x_1 генерується або той самий символ x_1 , або символ x_2 . Через те, що ймовірність деяких пар символів дорівнює нулю, то всього в розглянутому джерелі є дев'ять характерних станів.

Використовуючи (1.23), безпосередньо одержимо

$$H(X) = 0,886 \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}.$$

Надлишковість джерела повідомлення. Згадаємо тепер, що ентропія характеризує кількість інформації, яка припадає в середньому на одне повідомлення. Розглянуті приклади 3, 4 і 5 показують, що за однакової кількості різних символів (повідомлень) кількість інформації, що припадає на одне повідомлення, може бути різною в залежності від статистичних характеристик джерела. Ентропія джерела максимальна і дорівнює $H_{\text{макс}} = \log n$, якщо символи виробляються з різними ймовірностями; якщо ж це не так і деякі символи повторюються часто, а інші рідко, то ентропія джерела зменшується, а за появи додаткових корелятивних зв'язків між символами ентропія стає ще меншою. Це положення добре узгоджується з інтуїтивною уявою про кількість інформації, яка виробляється тим чи іншим джерелом. Так, наприклад, якщо із попереднього дослідження властивості лектора чи доповідача відомі настільки добре, що слухачі з високим ступенем достовірності знають про що він буде говорити, то кількість інформації, що повідомляється таким лектором, буде дуже малою, незважаючи на велике число сказаних слів.

Для того щоб з'ясувати, наскільки добре в джерелі повідомлень використовуються різні символи (а джерело буде тим краще, чим більше інформації воно буде виробляти) вводиться параметр, який називається *надлишковістю* і дорівнює

$$R = \frac{H_{\text{макс}} - H(X)}{H_{\text{макс}}}. \quad (1.24)$$

При цьому $H_{\text{макс}} = \log n$ є максимальна ентропія або найбільша кількість інформації, яка може припадати на один символ джерела при даному числі n використовуваних символів.

Із (1.24) видно, що при $R = 0$ ентропія джерела $H(X) = H_{\text{макс}}$, тобто джерело генерує максимальну кількість інформації на символ. Якщо $R = 1$, то $H(X) = 0$, і, отже, інформація, що виробляється джерелом, дорівнює нулю. У загальному випадку $0 \leq R \leq 1$. Чим менша надлишковість R , тим раціональніше працює джерело, тим більшу кількість інформації воно виробляє.

Проте слід мати на увазі, що не завжди треба прагнути до того, що $R = 0$. Деяка надлишковість буває корисною для забезпечення надійності передавання, реєстрації та інших перетворень інформації. Відомо, наприклад, що лектора, який не повторює або не пояснює більш докладно на прикладах окремі положення, слухати і конспектувати значно складніше, ніж лектора, який розумною мірою користується цими прийомами.

Якщо не розрізняти літери «е» і «ё», а також м'який і твердий знаки, то в російському алфавіті всього 31 літера, до них треба додати ще пропуск між словами, так що всього виходить 32 символи. Якщо б всі символи були рівноймовірні, то ентропія такої мови дорівнювала б

$$H_0 = \log_2 32 = 5 \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}.$$

Проте насправді ймовірності різних символів різні, так, наприклад, ймовірність літери «о» дорівнює приблизно 0,09, а літери «ф» – 0,002. Крім того, між словами мають місце значні корелятивні зв'язки.

Проведенні дослідження³, додають наступні значення ентропії: при врахуванні різної ймовірності окремих символів

$$H_1 = 4,39 \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}},$$

при врахуванні корелятивних зв'язків між двома символами

$$H_2 = 3,41 \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}},$$

при врахуванні корелятивних зв'язків між трьома символами

$$H_3 = 3 \frac{\text{ДВ. ОД.}}{\text{СИМВОЛ}}.$$

Таким чином, можна стверджувати, що надлишковість російської мови

$$R > \frac{5-3}{5} = 0,4.$$

Аналіз англійської мови з врахуванням корелятивних зв'язків, що розповсюджуються на вісім сусідніх літер, показав, що надлишковість його $R > 0,5$. Якщо урахувати корелятивні зв'язки, що розповсюджуються на досить велике число літер, то можна, очевидно, переконатися, що надлишковість російської та інших європейських мов понад 50%. Наявність

³ Лебедев Д.С., Гармаш В.А.. О возможности увеличения скорости передачи телеграфных сообщений // Электросвязь. – 1958. – № 1. – С. 68–69.

цієї надлишковості дозволяє легко виправити окремі помилки або поновити пропуски літер і навіть складів без спотворення тексту.

Для прикладів, розглянутих вище, одержуємо:

$$\text{в прикладі 7 } R = 0,$$

$$\text{в прикладі 8 } R = \frac{2-1,75}{2} = 0,125,$$

$$\text{в прикладі 9 } R > \frac{2-0,886}{2} \approx 0,56.$$

Зв'язок між ентропією і числом різних послідовностей повідомлення. Розглянемо послідовності повідомлень ергодичного джерела, що містять M символів. Коротко будемо вважати: послідовності C довжини M .

Для таких послідовностей можна довести наступну теорему, яка має фундаментальне значення в теорії інформації.

Теорема 1. Скільки б не були малі числа $\varepsilon > 0$, за досить великому $\eta > 0$, всі послідовності можуть бути розбиті на дві групи, що володіють наступними властивостями:

1) Ймовірність $p(C)$ будь-якої послідовності першої групи (типові послідовності) задовольняє нерівності

$$\left| \frac{\log \frac{1}{p(C)}}{M} - H \right| < \eta,$$

де H – ентропія джерела, що визначається за (1.22).

2) Сума ймовірностей послідовностей другої групи (нетипові послідовності) менше ε .

Можна показати, що для всіх типових послідовностей

$$2^{-M(H+\eta)} < p(C) < 2^{-M(H-\eta)}.$$

Для досить довгих послідовностей з дуже малою похибкою можна прийняти

$$p(C) \approx 2^{-MH}.$$

Останнє означає, що ймовірності всіх типових, досить довгих послідовностей однакові і, якщо врахувати властивість 2), то число таких послідовностей дорівнює

$$N_1 \approx \frac{1}{p(C)} \text{ або } N_1 \approx 2^{HM}.$$

Точніше це співвідношення може бути записане у вигляді

$$2^{(H-\eta)M} < N_1 < 2^{(H+\eta)M},$$

де η може бути як завгодно малою, причому якщо $M \rightarrow \infty$, то $\eta \rightarrow 0$.

Нетипові послідовності будуть з'являтися (вироблятися джерелом) дуже рідко, тому з цими послідовностями у низці випадків можна не рахуватися.

У випадку, коли всі n символів джерела незалежні і рівноймовірні, то ентропія його визначається виразом $H(X) = \log n$. Тоді маємо

$$N_1 = 2^{M \log_2 n} \text{ або } N_1 = n^M.$$

Потік інформації джерела повідомлень. Співвідношення (1.22) дозволяє визначити кількість інформації, що переноситься (в середньому) одним символом джерела. При роботі джерела повідомлень на його виході окремі символи з'являються через деякі інтервали часу; в цьому розумінні ми можемо говорити про *тривалість* окремих *символів*, і, отже, може бути поставлено питання про кількість інформації, що виробляється джерелом за одиницю часу.

Для відповіді на це питання обчислимо середню тривалість символу.

Позначимо через

$\tau_{x_i}(S_l | S_k)$ – тривалість символу x_i , що переводить джерело із стану S_k в стан S_l .

$p_{x_i}(S_l | S_k)$ – ймовірність того, що джерело, знаходячись в стані S_k , буде переведене в стан S_l символом x_i ; тоді середня тривалість символу

$$\bar{\tau}_i = \sum_k p(S_k) \sum_{l|k} \sum_i p_{x_i}(S_l | S_k) \tau_{x_i}(S_l | S_k).$$

Величина, яка нас цікавить дорівнює

$$\bar{H}(X) = \frac{H(X)}{\bar{\tau}_i} \frac{\text{дв. од.}}{\text{с}}.$$

Ентропія джерела, яка припадає на одиницю часу, може бути названа швидкістю створення повідомлень⁴ або ж *поток*ом інформації. Двійкова одиниця інформації часто позначається через *біт* (англійська bit, скорочення від «binary digit» – двійкова одиниця), потік інформації в цьому випадку виражається в $\frac{\text{біт}}{\text{с}}$.

Очевидно, що потік інформації залежить від кількості різних символів, які виробляються джерелом, їх терміну і статистичних характеристик джерела.

Оптимальне кодування. Будь-яке повідомлення вже в момент свого зародження являє собою низку найпростіших елементів, вибраних з певного набору. Цей набір, чи сукупність умовних знаків, зазвичай називається *первинним алфавітом*, або *кодом* (приміром, український алфавіт). Інколи те саме повідомлення необхідно зобразити у вигляді низки інших елементів, вибраних з іншого набору, який називається *вторинним алфавітом*

⁴ Термін, використовуваний К. Шенноном.

(кодом). Процес переходу від первинного до його вторинного зображення називається *кодуванням*.

Поняття «кодування» містить дуже широке коло явищ. Приміром, будь-яке вимірювання є кодуванням, оскільки його можна розглядати як перетворення багатьох значень, яких може набувати вимірювана величина (її алфавіт), у вихідний алфавіт вимірювального приладу – множину відлічуваних значень стрілки приладу. Кодування відбувається в мікрофоні, в якому кожному певному значенню повітряного тиску (первинний алфавіт) відповідає певне значення струму в колі мікрофона (вторинний алфавіт) тощо.

Дуже важливим параметром кодування є обсяг первинного та вторинного алфавіту – кількість різних символів, з яких будується повідомлення і які відрізняються один від одного тими чи іншими фізичними ознаками. Наприклад, китайський алфавіт містить декілька десятків тисяч елементів (ієрогліфів), а український – лише 33 знаки.

В окремому випадку кількість елементів у первинному і вторинному алфавітах може бути однаковою.

При побудові кодів не має значення, якими фізичними параметрами відрізняються один від одного елементи алфавіту. Однак для побудови кодуючих пристроїв це є істотним.

Якщо повідомлення має бути передано електричним каналом зв'язку, а алфавіт складено з неелектричних елементів, то необхідно шляхом кодування перетворити алфавіт, складений з елементів, що відрізняються між собою неелектричними параметрами (наприклад, літери алфавіту – формою), в алфавіт такого самого обсягу, елементи якого відрізняються між собою за яким-небудь електричним параметром – струмом, напруженістю електричного чи електромагнітного поля тощо. Інакше кажучи, для створення вторинного алфавіту в такому разі слід перетворити неелектричні параметри в електричні, здійснивши модуляцію одного з параметрів електричного стану кола, тобто утворити електричні сигнали.

Таким чином, перетворення повідомлення, поданого у вигляді набору елементів, що мають неелектричні параметри, на повідомлення, подане елементами алфавіту, складеного з різних (за параметрами) електричних сигналів, включає три операції: 1) кодування; 2) перетворення неелектричної величини в електричну; 3) модуляцію.

Кодування інформації. Кодування визначає математичну, а модуляція – фізичну сторони процесу перетворення повідомлення на електричні сигнали.

Розглянемо методику перетворення дискретного повідомлення, записаного знаками українського алфавіту, на відповідні електричні сигнали.

Для побудови коду дуже зручно кожній літері алфавіту надати цифру й оперувати не літерами, цифрами та розділовими знаками даного алфавіту, загальна сума яких дорівнює обсягові вихідного коду, а лише числами:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	...
1	2	3	4	5	6	7	8	9	10	11	12	...

При цьому ми перетворили елементи одного алфавіту на елементи чи комбінації елементів іншого алфавіту, в загальному випадку, з іншим обсягом. Комбінація, чи сукупність елементів алфавіту, що відбиває одне повідомлення, називається *кодовою комбінацією*.

Тепер при передаванні будь-якого тексту будемо передавати послідовний ряд чисел, але при цьому більше значення має те, за якою системою побудовано числення. Так, у звичній для нас десятковій системі числення є десять відмінних один від одного знаків, з яких може бути побудовано будь-яке число (обсяг алфавіту дорівнює десяти): 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Але можуть бути й інші системи числення. П'ятіркова система числення передбачає наявність п'яти різних знаків для написання будь-якого числа – 0, 1, 2, 3, 4; трійкова система має три різних знаки – 0, 1, 2; двійкова система числення має два різних знаки – 0, 1.

Кількість різних знаків даної системи числення (обсяг коду) називається її основою. Так, у десятковій системі числення основа дорівнює десяти, у двійковій – двом тощо.

У будь-якій системі числення кожне число N , відмінне від нуля, можна записати як

$$N = \dots k_i m_c^{i-1} + \dots + k_3 m_c^2 + k_2 m_c^1 + k_1 m_c^0, \quad (1.25)$$

де $k_i m_c^{i-1}$ - знаки (цифри) даної системи числення, що показують число в i -му розряді; m_c - основа системи числення.

Наприклад, число 105 у десятковій системі числення можна записати так: $105 = 1 \cdot 10^2 + 0 \cdot 10^1 + 5 \cdot 10^0$.

У двійковій системі числення те саме число запишемо в такому вигляді:

$$(105)_{10} = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (1101001)_2.$$

Ряд чисел, записаних у десятковій та двійковій системах числення, відповідно має вигляд

0	1	2	3	4	5	6	7	8	9	10	11	...
0	01	10	11	100	101	110	111	1000	1001	1010	1011	...

Легко визначити максимальне число, котре може бути записано заданою кількістю знаків (розрядів) в якій-небудь системі числення:

$$N_{\text{макс}} = m_c^n - 1,$$

де $N_{\text{макс}}$ – максимальне записане число.

Загальна ж кількість різних чисел (з урахуванням нуля)

$$N = m_c^n.$$

Наприклад, двома знаками в різних системах числення можна записати такі максимальні числа:

у десятковій системі $102 - 1 = 99$;

у двійковій системі $22 - 1 = 3$.

Із розглянутого видно, що чим більше основа системи числення m , тим менша кількість знаків потрібна для запису одного й того самого числа, але, разом з тим, зростає кількість різних знаків системи.

Будь-яке число у двійковій системі числення записується у вигляді комбінації з двох відмінних один від одного знаків 0 та 1 і являє собою комбінацію елементів двійкового коду. Якщо потрібно передати це число каналом зв'язку, то його слід перетворити на таку саму комбінацію двох значень якого-небудь параметра переносія електричної енергії.

Наприклад, число десять у двійковій системі числення має вигляд 1010. Джерелом енергії є генератор постійного струму. Нехай одиниці однополюсного телеграфування відповідає струмова, а нулю - безструмова послілка. Тоді вказане число у вигляді електричних посилок може бути подане так, як показано на рис. 1.7, а. За двополусної роботи запис того самого числа наведено на рис. 1.7, б.

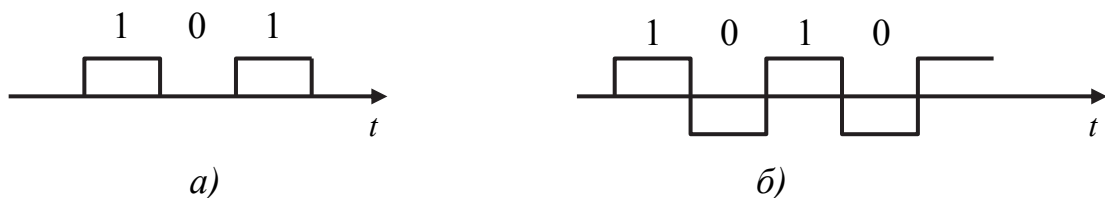


Рисунок 1.7 - Передавання двійкових чисел

Отже, будь-яке число можна передати на сусідню станцію у вигляді кодової комбінації елементарних (найбільш коротких) посилок. Кожна елементарна послілка є елементом коду, тобто знаком даного алфавіту. В двійковому кодi елементарна послілка може набувати двох станів, відмінних один від одного за якоюсь фізичною ознакою, наприклад, струмовий і безструмовий, позитивний і негативний.

Відмінність між станами елементарних посилок дає змогу приймальному пристрою розрізняти їх між собою, тобто прочитати записані у двійковій системі числення числа.

Розглянемо двійковий код (код, побудований за двійковою системою числення), число елементів в комбінації якого не перевищує п'яти. Максимальне число, яке можна записати, використовуючи не більше п'яти знаків, $N_{\text{макс}} = 2^5 - 1 = 31$.

Пронумеруємо знаки первинного алфавіту в двійковій системі числення

А	Б	В	Г	Д	Е	Є	Ж	...
1	10	11	100	101	110	111	1000	...

і подамо числа у вигляді комбінацій елементарних посилок (рис. 1.8). Це буде нерівномірний код, оскільки в ньому не всі числа подано однаковою кількістю елементарних посилок.

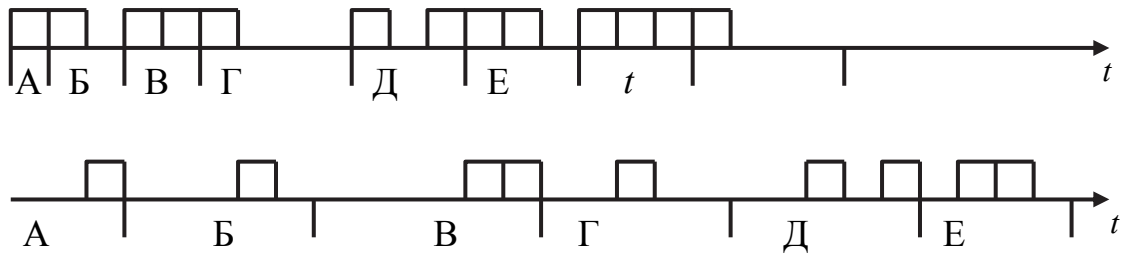


Рисунок 1.8 – Кодові сигнальні конструкції

Оскільки комбінації посилок проходять одна за одною безперервно, то на станції приймання важко визначити початок і кінець кожної комбінації, що є вкрай необхідним, аби прочитати записані числа. Задача значно спрощується, якщо комбінації, що належать до кожного з ряду переданих чисел, будуть розпочинатися через проміжки часу. Для цього доповнимо кожен комбінацію до максимально можливої кількості елементарних посилок – п'яти і дістанемо двійковий п'ятизначний рівномірний код. Виникає питання: з якого боку слід розміщувати елементарні послілки, яких бракує, – ліворуч чи праворуч від записаної комбінації – і який стан («0» чи «1») повинен мати ці відсутні елементарні послілки?

Дивлячись на написаний ряд чисел, бачимо, що кожне число розпочинається з одиниці й відрізняється від іншого числа кількістю знаків, доданих праворуч від першого знака. Отже, аби не порушувати закономірності накреслення окремих чисел і зрівняти число розрядів у кожному числі, знаки, яких бракує, мають бути нулями, і додавати їх слід ліворуч.

Для визначення меж комбінацій, що належать до різних чисел, достатньо відрахувати на станціях передавання та приймання однакові відліки часу. Ці функції виконують розподільувачі передавання та приймання.

Таким чином, для одержання рівномірного коду доводиться не передавати каналом зв'язку низку посилок, зовсім не потрібних для запису чисел. Незважаючи на цей недолік, рівномірний код, що спрощує приймальний пристрій прикінцевого апарата, набув широкого розповсюдження в системах передавання дискретної інформації.

З нерівномірних кодів набули широкого застосування код Морзе та кабельний код.

Код Морзе будується за двійковою системою числення (рис. 1.9), причому знакам, що найчастіше зустрічаються в даному алфавіті, надаються числа, записувані мінімальною кількістю елементарних посилок (враховується статистика даної мови, для коду Морзе – англійської). Для передавання кодом Морзе, з урахуванням прогалін, потрібно в середньому близько $9,5 t_0$ на кожний знак, де t_0 – тривалість елементарної послілки. Переваги коду Морзе – легка запам'ятовуваність, можливість запису найпростішими засобами та приймання на слух у разі сильних завад.

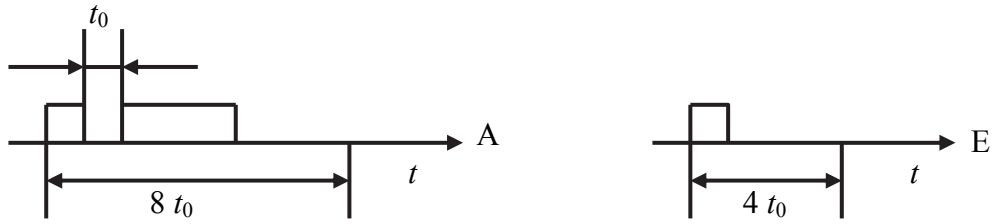


Рисунок 1.9 - Сигнальні кодові конструкції при двопозиційних сигналах

У кабельному кодi (рис. 1.10) точка записується позитивною посилюю, тире – від'ємною і прогалина – безструмовою. Таким чином, кабельний код є трійковим кодом, побудованим на трійковій системі числення (має три різних знаки для записування чисел). На кожний знак первинного коду припадає в середньому близько чотирьох елементарних посилок. Таке різке зменшення кількості елементарних посилок у кодовій комбінації пояснюється застосуванням трійкової системи числення. Застосовується кабельний код за малого рівня завад у каналі зв'язку, оскільки його завадостійкість значно нижче ніж у двійкового коду.

Оптимальним називається такий код, у якого середнє число елементів є мінімальним. Зрозуміло, що в такому разі знаки первинного алфавіту, які найчастіше зустрічаються, мають записуватись меншою кількістю елементарних посилок, тобто оптимальний код не може бути рівномірним. Наприклад, код Морзе є оптимальним у такому розумінні для англійської мови (для української мови відміна від оптимальності становить 8%). Однак у ньому після кожного знаку йде прогалина з трьох елементарних посилок, що знижує ефективність коду. Було б доцільно побудувати нерівномірний оптимальний код без прогалин поміж комбінаціями.

Для оцінки ступеня оптимальності коду слід знати ту межу, до якої треба наблизитись, зменшуючи кількість елементів вторинного коду на кожний знак переданого повідомлення (первинного коду).

Відомо, що для передавання повідомлення, записаного алфавітом, який містить m різних літер, потрібно не менш ніж H двійкових одиниць (елементів) на літеру. При цьому H визначається за формулою:

$$H = \sum_{i=1}^m p_i \log_2 p_i \frac{\text{дв. од. (біт)}}{\text{літеру}},$$

де p_i – ймовірність появи i -ї літери в повідомленні. Всі p_i пов'язані між собою співвідношенням

$$H = \sum_{i=1}^m p_i = 1.$$

При цьому $0 \leq p_i \leq 1$.

Якщо в повідомленні міститься одна літера, ймовірність появи якої дорівнює одиниці, а ймовірність появи решти $m - 1$ літер дорівнює нулю, то

$$H = -(1 \cdot \log_2 1 + 0 \cdot \log_2 0 + \dots + 0 \cdot \log_2 0) = 0,$$

тобто ентропія повідомлення дорівнює нулю. Передавати таке повідомлення немає необхідності, оскільки воно заздалегідь відоме одержувачеві.

Припустимо, що в повідомленні поява всіх m літер є рівноймовірною. Звідси $p_i = 1/m$,

$$H = -\left(\frac{1}{m} \log_2 \frac{1}{m} + \frac{1}{m} \log_2 \frac{1}{m} + \dots\right) = -\frac{m}{n} \log_2 \frac{1}{m} = \log_2 m.$$

Ентропія при цьому буде максимальною.

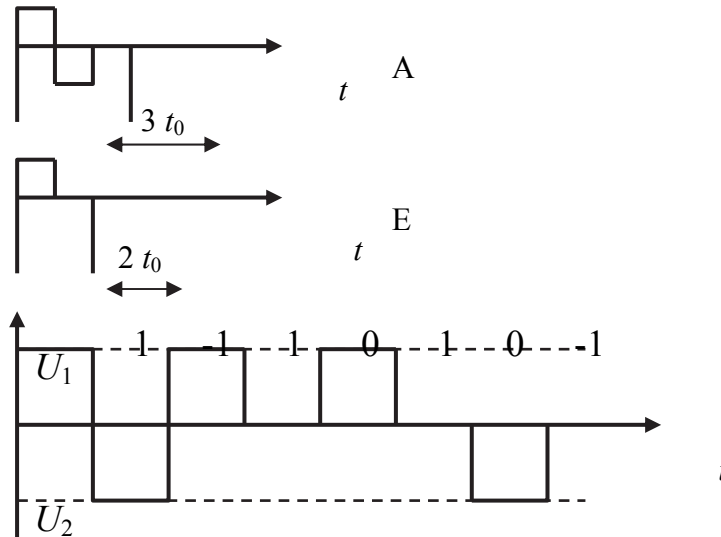


Рисунок 1.10 - Сигнальні кодові конструкції за різної позиційності

К. Шеннон показав, що передане повідомлення може бути закодоване таким чином, щоб середнє число двійкових одиниць на літеру повідомлення скільки завгодно наближалось до ентропії даного повідомлення. Але це число не може бути меншим за ентропію. Отже, знання значення ентропії дає змогу оцінити ступінь наближення використовуваного коду до оптимального.

Ентропія H джерела повідомлень телеграфного тексту для української мови визначається статистичними дослідженнями декількох тисяч телеграм. Ймовірності використання різних літер є різними. Наприклад, $p(\text{пропуск}) = 0,17$; $p(0) = 0,078$; $p(a) = 0,0626$ тощо, причому $\sum p(i) = 1$ (без урахування ймовірностей проходження літерних з'єднань).

На підставі одержаних вище даних $H = 4,363$ біт/літеру.

Із розглянутого видно, що кількість інформації, що міститься в кожному знакові алфавіту, залежить від обсягу даного алфавіту та ймовірностей появи різних літер.

Наприклад, у двійковому алфавіті з рівноймовірними знаками $H = \log_2 2 = 1 \frac{\text{біт}}{\text{знак}}$, тобто кожний елемент двійкового коду містить один біт інформації. Якщо ж основа коду $m > 2$, то кожний елемент такого коду міс-

тять більшу кількість біт інформації, що дає можливість підвищити ефективність системи зв'язку. Якщо $m = 32$, то $H = \log_2 m = \log_2 2^5 = 5 \frac{\text{біт}}{\text{знак}}$.

Однак зі зростанням m кількість інформації, що припадає на кожний знак алфавіту, зростає за логарифмічним законом, а складність апаратури – за лінійним. Тому, з точки зору простоти апаратури, найбільш вигідним є використання двійкових кодів. При двійковій системі дуже просто реалізуються схеми запам'ятовування, комутації, кодування тощо. Крім того, елементарні послідовності двійкового коду мають найбільшу завадостійкість. Через це в сучасних апаратах системи передавання дискретної інформації переважно застосовуються двійкові коди. Розглянемо один зі способів побудови оптимального двійкового коду. Було відзначено, що оптимальним може бути лише нерівномірний код. При цьому літерам, що найбільш часто зустрічаються, надаються найбільш короткі кодові комбінації.

Для визначення меж поміж кодовими комбінаціями можна скористатися двома способами:

1) після кожної комбінації передбачається знак поділу (саме так побудовано код Морзе), але це збільшує довжину кодової комбінації;

2) для кожної літери алфавіту вибирають таку послідовність двійкових знаків, яка не є початком якої-небудь іншої, більш довгої, комбінації.

Розглянемо наступний приклад.

Приклад 10. Нехай є чотирилітерний алфавіт A_1, A_2, A_3, A_4 з ймовірностями появи окремих літер

$$p_1 = 0,5; p_2 = 0,25; p_3 = 0,125; p_4 = 0,125; \sum p_i = 1.$$

Ентропія джерела повідомлення з таким алфавітом

$$\begin{aligned} H &= -\sum_{i=1}^4 p_i \log_2 p_i = -(0,5 \log_2 0,5 + 0,25 \log_2 0,25 + 2 \cdot 0,125 \log_2 0,125) = \\ &= 0,5 \cdot 1 + 0,25 \cdot 2 + 0,25 \cdot 3 = 1,75 \frac{\text{біт}}{\text{літеру}}. \end{aligned}$$

Максимальне значення ентропії, коли всі значення p_i , є однаковими між собою, становить $H_{\max} = \log_2 m = \log_2 4 = 2 \frac{\text{біт}}{\text{літеру}}$.

Отже, надлишковість $D = H_{\max} - H = 2 - 1,75 = 0,25$.

Для розглядуваного алфавіту найбільш простим оптимальним двійковим кодом був такий:

$$A_1 \rightarrow 0, A_2 \rightarrow 1, A_3 \rightarrow 01, A_4 \rightarrow 10.$$

Проте кодові позначення для A_1 та A_2 є початковими частинами для A_3 та A_4 , тому розділити прийняті комбінації на станції приймання неможливо. Комбінація 0100110 може бути розшифрована в декількох варіантах, наприклад:

0 1 0 0 1 1 0 0 1 0 0 1 1 0
 A_1 A_2 A_1 A_1 A_2 A_2 A_1 A_3 A_1 A_3 A_4

Для вибору кодових комбінацій користуються таким правилом (рис. 1.11).

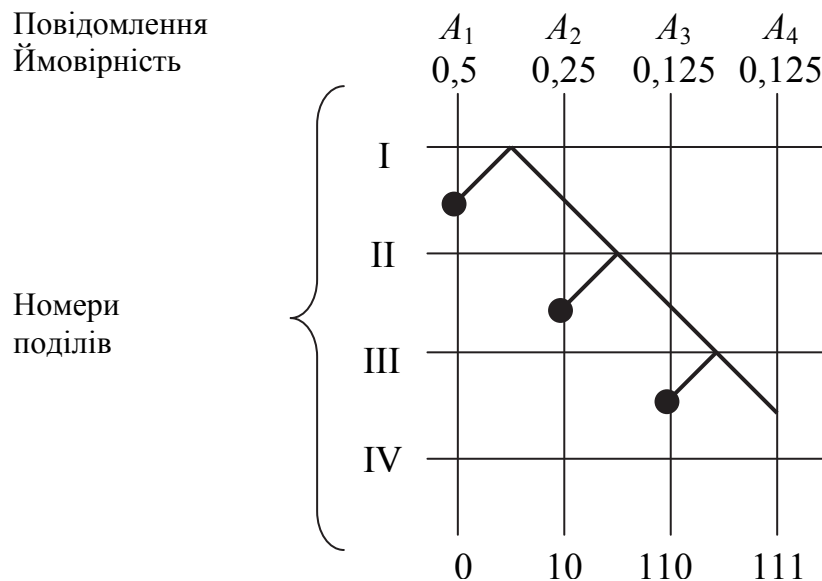


Рисунок 1.11 – Формування слів оптимального коду

Усі літери записуються в порядку спадання ймовірностей. Добута послідовність розбивається на дві групи так, аби сумарні ймовірності розподілились між групами за можливістю рівномірно. Потім кожна підгрупа, в свою чергу, розбивається на дві підгрупи з дотриманням тієї самої умови рівності ймовірностей. Такий поділ триває до тих пір, доки в підгрупах не залишиться по одному повідомленню. Кодове позначення кожної підгрупи визначається таким чином: крок ліворуч дає цифру 0, крок праворуч – цифру 1.

Наведена вище комбінація розшифровується однозначно:

0 1 0 0 1 1 0
 A_1 A_2 A_1 A_3

Визначимо середню довжину кодової комбінації

$$l_{\text{сеп}} = \sum_{i=1}^m l_i p_i = 1 \cdot 0,5 + 2 \cdot 0,25 + 3 \cdot 0,125 + 3 \cdot 0,125 =$$

$$= 0,5 + 0,5 + 0,75 = 1,75 \frac{\text{дв. од.}}{\text{знак}},$$

тобто середня кількість двійкових одиниць на знак дорівнює ентропії джерела повідомлень.

Незважаючи на те, що оптимальні коди зменшують середню тривалість кодового слова, на практиці користуються рівномірними кодами, що істотно спрощує апаратуру зв'язку.

Отже, при передаванні кожному символу вихідного алфавіту повідомлень обсягу N_B ставиться у відповідність m -елементарна двійкова послідовність – кодова комбінація. Очевидно, що можлива кількість послідовностей

$$N_0 = 2^m.$$

Якщо при передаванні використовуються всі можливі кодові комбінації, то код називається *простим* ($N_B = N_0$).

Ступінь різниці комбінацій називається кодовою відстанню. Між двома кодовими комбінаціями (векторами) вона визначається числом відмінних елементів (розрядів). Наприклад, комбінації 010 та 100 відрізняються двома розрядами.

Векторні простори. Розглянемо деякі види векторних просторів, що використовуються у теорії зв'язку, та їхні метрики:

1. Числова пряма є простором, що утворений множиною дійсних чисел з метрикою

$$d = |x - z|. \quad (1.26)$$

2. Евклідовий простір являє собою арифметичну множину дійсних чисел з метрикою

$$d = \sqrt{\sum_{k=1}^n (x_k - z_k)^2}. \quad (1.26a)$$

3. Дискретний L -простір утворено дійсними числами і володіє метрикою

$$d = \sum_{k=1}^n (x_k - z_k)^2. \quad (1.26b)$$

Цей простір виявляється дуже зручним в теорії двійкових кодів. Із виразу (1.26б) виходить, що геометричною моделлю n -значного двійкового коду з рівноймовірними комбінаціями слугує n -вимірний *гіперкуб* з одиничними ребрами, вершини якого відповідають кодовим комбінаціям. Відстань між кодовими векторами чисельно дорівнює числу розрядів, в яких різняться між собою кодові комбінації. Враховуючи властивості додавання за $\text{mod } 2$, вираз (1.26б) можна представити у вигляді

$$d = \sum_{k=1}^n (x_k \oplus z_k). \quad (1.27)$$

Величина d в теорії кодування називається *хемінговою* або *кодовою відстанню*. Так, множина комбінацій (наприклад) тризначного двійкового коду характеризується матрицею d_x , симетричною відносно діагоналі. Геометрично це означає, що відстань між двома n -значними кодовими комбінаціями дорівнює числу ребер n -вимірного гіперкуба, які лежать на найкоротшому шляху між відповідними його вершинами.

4. Простір L_p -функцій, інтегрованих з p -м степенем на проміжку $[a, b]$, має метрику

$$d = \sqrt[p]{\int_a^b |x(t) - z(t)|^p dt} \quad (p \geq 1) \quad (1.28)$$

і являє собою узагальнення дискретного евклідового простору на безперервні функції. Якщо $p = 2$, то простір L_2 називається *функціональним гільбертовим простором*.

5. Простір L_p послідовностей дійсних чисел має метрику

$$d = \sqrt[p]{\sum_{k=1}^{\infty} (x_k - z_k)^p} \quad (p \geq 1) \quad (1.28a)$$

і являє собою узагальнення евклідового простору на нескінченну множину чисел. При $p = 2$ одержуємо *координатний гільбертовий простір*.

6. Простір C безперервних функцій на проміжку $[T_1, T_2]$, який задано метрикою

$$d = \max |x(t) - z(t)|, \quad (1.286)$$

часто використовується в різних схемах селекції сигналів за максимумом різницевої напруги.

Кодова відстань дорівнює числу одиниць в кодовому слові, яке дістають при сумуванні розрядів порівнюваних кодових слів за модулем два. Наприклад:

$$\oplus \begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \\ \hline 1 & 1 & 0 \end{array}$$

Якщо число використовуваних кодових слів $N_b < N_0$ (не всі можливі комбінації використовуються), то коди називаються *надлишковими*, або *коригуючими*.

Принцип побудови коригуючих кодів розглянемо на геометричній моделі триелементного коду (рис. 1.12), усі вісім комбінацій якого можна подати у вигляді точок у тривимірному просторі, що збігаються з координатами вершин одиничного куба.

Якщо для передавання використовуються усі вісім комбінацій, то виходить звичайний триелементний код. Найменша кодова відстань d_{\min} — найменша відстань між двома використовуваними комбінаціями — дорівнює довжині ребра куба, тобто одиниці. За помилкового приймання будь-якого елемента кожна комбінація переходить в іншу використовувану комбінацію, і помилка не може бути виявлена. При використанні для передавання лише деяких комбінацій, наприклад, з парним числом одиниць (011, 101), дістанемо код виявленням однократної та трикратної помилок.

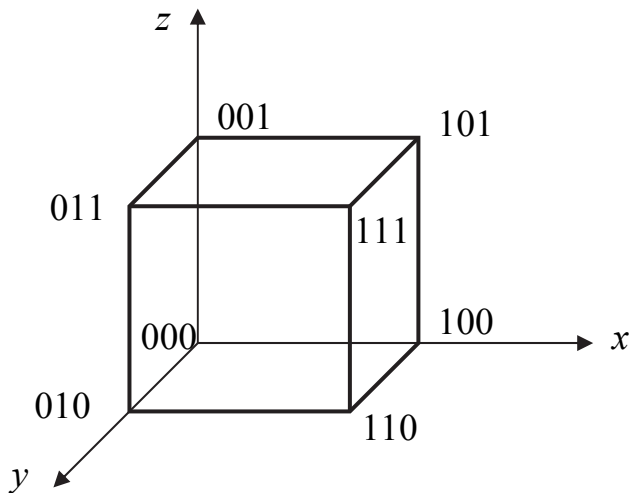


Рисунок 1.12 – Геометрична модель триелементного коду

Кратність помилки дорівнює кількості вірно зареєстрованих елементів комбінації. Найменша відстань між двома використовуваними комбінаціями становить дві одиниці (два ребра куба). Тому за будь-якої непарної помилки дозволена комбінація перетворюється на недозволену і приймальний апарат покаже на наявність помилки (наприклад, у цьому місці тексту віддрукується знак питання).

За помилкового приймання двох елементів кодової комбінації (двократна помилка) одна дозво-

лена комбінація перетворюється на іншу, також дозволена комбінацію. Отже, двократна помилка не виявляється.

Число помилок, які виявляються, t_b та найменша потрібна відстань $d_{\text{мін}}$ взаємозалежні: $d_{\text{мін}} = t_b + 1$.

Для того щоб однократна помилка могла бути не лише виявлена, але й виправлена, необхідно, щоб найменша відстань становила не менше трьох одиниць (три ребра куба). Цій вимозі задовольняє будь-яка пара точок, розміщених на діагоналі куба, наприклад, 000 та 111.

За однократної помилки, наприклад, при заміні комбінації 000 на комбінацію 010, одержана недозволена комбінація буде ближче до дійсної, а ніж до хибної (111). Це і дає можливість виправити помилку. Крім того, такий код виявляє без виправлення двократну помилку, оскільки за останньої здобувається недозволена комбінація.

Число помилок, які виправляються, $t_{\text{вп}}$ та кодова відстань $d_{\text{мін}}$ пов'язані формулою $d_{\text{мін}} = 2t_{\text{вп}} + 1$.

Таким чином, ідея двійкових коригуючих кодів полягає в тому, що із загальної кількості кодових комбінацій $N = 2^n$ для передавання інформації вибирається S комбінацій ($S < N$) так, аби за помилкового приймання S елементів одна використовувана комбінація не перетворилась на іншу використовувану комбінацію. Отже, коригуючі коди мають надлишковість.

Для оцінки економічності та ефективності кодів з виявленням помилок вводиться поняття коефіцієнта надлишковості $K_{\text{нд}}$ та коефіцієнта виявлення $K_{\text{в}}$:

$$K_{\text{нд}} = \frac{\log_2 N}{\log_2 S}, \quad (1.29)$$

Де $N = 2^n$ – загальна кількість комбінацій, які можна одержати в n -елементному коді; S – кількість використовуваних комбінацій;

$$K_b = \frac{L}{L + M}, \quad (1.30)$$

де L – загальна кількість помилкових комбінацій, помилка в яких може бути виявлена; M – те саме, але помилка не піддається виявленню.

1.3. Реєстрація елементів кодових конструкцій

При послідовному способі передавання сигналів одиничні елементи передаються послідовно у часі. При цьому елементи інформації можуть передаватися один за іншим без перерви або з перервою, але вони ніколи не передаються одночасно. Такий спосіб застосовується при передаванні інформації каналами зв'язку й дозволяє більш економічно використовувати канали, хоча й ускладнює схему прикінцевих пристроїв.

При паралельному способі передавання сигналів одночасно передається певне число одиничних елементів по декільком незалежним каналам, число яких визначається кількістю елементів у кодовій комбінації. Для цього способу необхідно більша кількість каналів, проте забезпечується більша, ніж при послідовному способі швидкість передачі інформації. Такий спосіб використовується в основному для передачі інформації між окремими вузлами одного й того самого пристрою передачі інформації, наприклад, між вузлами ЕОМ.

Розглянемо способи передавання інформації залежно від можливої структури сигналів. Загальним типом сигналу є сигнал, що складається із двійкових елементів довільної довжини. Сигнали такого типу використовуються в телеметрії, а також у пристроях документального електров'язку при взаємодії між вузлами комутації в процесі встановлення з'єднання.

Сигнали, елементи яких можуть мати будь-яку тривалість, але не менш $\tau_{\text{мін}}$, і відстають один від одного на довільні відстані, одержали назву *анізохронних*. Іншим типом сигналу є *ізохронний* сигнал, елементи якого мають однакову тривалість і надходять через однакові інтервали часу. Проміжними між анізохронними й ізохронними є сигнали відомої структури.

Передавання дискретної інформації каналами зв'язку може здійснюватися, залежно від структури сигналів, синхронним, асинхронним або стартозастопним способом.

Синхронна передача – це спосіб передавання ізохронними сигналами, при якому, між двома значущими позиціями, завжди є ціле число одиничних елементів.

Передача дискретних сигналів наведеними способами пояснюється на рис. 1.13.

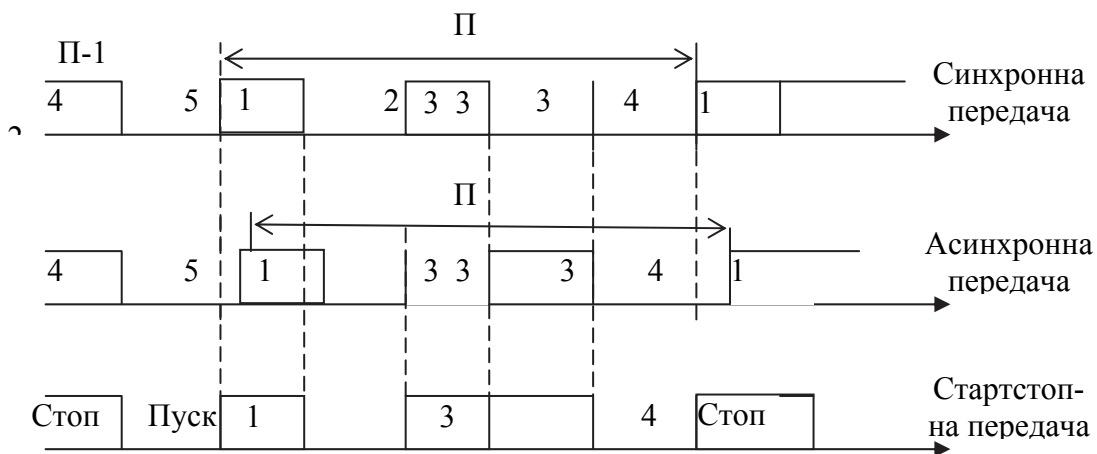


Рисунок 1.13 – Способи передавання сигналів

При передаванні дискретної інформації використовуються рівномірні первинні коди, що мають однакову кількість одиничних елементів у будь-якій кодовій комбінації й, отже, реалізується синхронний спосіб передачі.

Асинхронна передача характеризується тим, що:

- між будь-якими двома значущими моментами в одній і тій самій кодовій комбінації завжди є ціле число одиничних інтервалів;
- число одиничних інтервалів між двома значущими моментами, розташованими в різних кодових комбінаціях, не завжди є цілим числом.

Прикладом використання асинхронного методу й анізохронних сигналів є апарат Морзе.

Стартстопна передача є різновидом асинхронної передачі, коли кожній кодовій комбінації передуює стартовий (пуск) сигнал, а після кожної кодової комбінації надходить стоповий сигнал. Стартстопна комбінація служить для підготовки приймача до приймання й запису сигналу, а стоповий сигнал для приведення приймача в стан спокою.

Асинхронність передачі в цьому випадку полягає в тому, що тривалість стопового сигналу дорівнює 1,5 одиничного елемента для телеграфного коду МТК-2. Стартстопний спосіб передавання сигналів застосовується у всіх прикінцевих пристроях увводу-виводу при ручному введенні інформації.

Залежно від способу передавання сигналів джерел розділяють канали на асинхронні й синхронні. У *синхронних* каналах приймач точно синхронізований з передавачем, і введення кожного одиничного інтервалу проводиться в певні моменти часу. Тривалість одиничного елемента при цьому повинна дорівнювати або бути кратною $1/B$, де B – швидкість модуляції. Канали, якими можуть передаватися лише сигнали певної структури, одержали назву непрозорих.

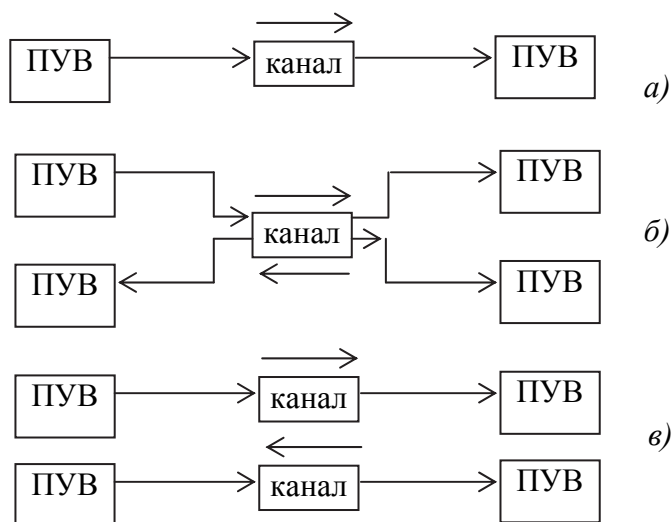


Рисунок 1.14 – Способи передавання каналом зв'язку

На відміну від синхронних каналів, асинхронні канали є прозорими, тому що забезпечують передачу анізохронних сигналів, тобто сигналів довільної структури з елементами сигналу довільної тривалості, але не менш $\tau_{хв}$, обумовленої фізичними властивостями каналу. Звісно, що по асинхронному каналу можуть передаватися також ізохронні сигнали й сигнали відомої структури, звідки й назва «прозорий».

Передача дискретних повідомлень, зокрема телеграфних, факсимільних, може бути побудована по одній з наступних схем (рис. 1.14): *симплексна, напівдуплексна й дуплексна*.

Симплексна схема (рис. 1.14, а) передбачає наявність на станції А передавача, а на станції Б – приймача. Ці пристрої з'єднані між собою однобічним (симплексним) каналом. При симплексній схемі передавання інформації можна вести лише в одну сторону, від станції А – до станції Б. У цей час симплексна передача використовується вкрай рідко, тому що завжди існує зворотний потік інформації.

Напівдуплексна схема (рис. 1.14, б) дозволяє здійснювати передавання по черзі в обох напрямках. При цьому на кожній станції встановлюється передавач і приймач. Контроль переданої інформації здійснюється приймачем тієї ж станції, з якої в цей момент ведеться передавання.

У цей час напівдуплексна схема зв'язку є основною на телеграфних мережах загального користування й абонентського телеграфу.

Дуплексна схема зв'язку (рис. 1.14, в) дозволяє здійснювати передавання інформації одночасно в обох напрямках. По суті це два симплексні однобічні зв'язки, кожний з яких використовується для передавання у своєму напрямку (А – Б и Б – А). Контроль переданої інформації ведеться так само, як і при напівдуплексній схемі. Двостороннє одночасне передавання застосовується в основному на магістральних зв'язках з великим обміном.

Пристрої уводу-виводу дискретних повідомлень підключаються до систем передачі, ЕОМ і каналам зв'язку за допомогою системи уніфікованих зв'язків – інтерфейсів уводу-виводу.

Інтерфейсом називають пристрої сполучення, а в більш точному тлумаченні – сукупність електричних, механічних і програмних засобів, що дозволяють з'єднувати між собою різні пристрої.

На рис. 1.15 наведена схема сполучення ПУВ із каналом зв'язку.



Рисунок 1.15 – Сполучення ПУВ з каналом зв'язку

Складовими частинами інтерфейсу є: апаратні й програмні засоби із протоколом, що описують процедуру взаємодії модулів (вузлів) при обміні даними.

Протокол – сукупність правил обміну інформацією, який може визначати структуру з'єднання і встановлює формат повідомлення, одиницю обміну, набір сигналів обміну й взаємодії, алгоритм обміну даними, спосіб кодування сигналів.

Апаратна частина утворюється з вузлів інтерфейсу, з'єднувачів, елементів узгодження й ліній зв'язку.

Програмне забезпечення інтерфейсу складається із програм, що здійснюють функціонування інтерфейсу, що й реалізують алгоритм обміну інформацією із заданого протоколу.

Інтерфейси класифікують у відповідності зі способом взаємодії їх зі своїми пристроями вводу-виводу.

За способом обміну інформацією розрізняють інтерфейси: паралельного вводу-виводу, які взаємодіють із пристроями в паралельному форматі, і послідовної передачі, які передають і приймають інформацію послідовно.

За способом підключення пристрою вводу-виводу розрізняють інтерфейси індивідуальні (для радіального підключення – ІРПР – «інтерфейс радіальний для паралельної передачі») та ІРПС – «інтерфейс радіальний для послідовної передачі») і групові (для магістрального підключення – «інтерфейс загальна шина»).

Структура системи передачі дискретної інформації. Система зв'язку при передаванні дискретної інформації являє собою сукупність каналу передачі дискретної інформації, джерела й одержувача дискретної інформації. Канал електрозв'язку в загальному значенні являє собою сукупність технічних засобів і середовища поширення (фізичного середовища) абонентських пристроїв, що забезпечують при підключенні, передавання повідомлень від джерела до одержувача.

Залежно від виду переносника й структури переданих сигналів канали зв'язку можна розділити на чотири групи:

- 1) *безперервно-безперервні*, у яких безперервний переносник і безперервні сигнали на вході й виході каналу;
- 2) *безперервно-дискретні*, у яких дискретний переносник і безперервні сигнали на вході й виході каналу;
- 3) *дискретно-безперервні*, у яких переносник безперервний, а сигнали на вході й виході каналу дискретні;

4) *дискретно-дискретні*, у яких переносник дискретний, а сигнали на вході й виході каналу безперервні.

Предметом нашого розгляду є лише два останні типи каналів, пов'язаних з передачею дискретної інформації.

Типовим представником дискретно-безперервного каналу є канал передачі даних, утворений у системі із частотним поділом, а дискретно-дискретного каналу – канал передачі даних з тимчасовим поділом.

Система передачі дискретної інформації (повідомлень), що забезпечує двостороннє передавання інформації, може містити велику кількість джерел і одержувачів повідомлень, передавачів, приймачів і ліній зв'язку.

Структурна схема односторонньої системи передачі дискретних повідомлень (ПДП) представлена на рис. 1.16.

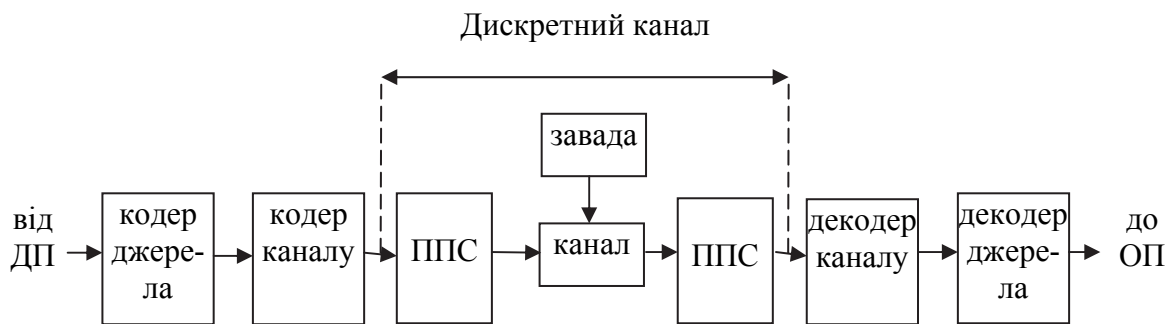


Рисунок 1.16 – Структурна схема системи ПДП

Джерело й одержувач повідомлень разом з перетворювачем повідомлення до складу системи ПДС не входять.

Символи переданого алфавіту повідомлень від джерела повідомлень (ДП) у вигляді кодових комбінацій надходять на кодер джерела, де визначається довжина кодового слова й спосіб передавання. Повідомлення, що надходить від ДП, у ряді випадків містить надлишковість.

Однак надлишковість призводить до того, що за заданий проміжок часу буде передано менше повідомлень і, отже, менш ефективно буде використовуватися канал ПДП. Завдання усунення надлишковості на передачі в системі ПДП виконує кодер джерела, а відновлення прийнятого повідомлення – декодер джерела. Часто кодер і декодер джерела включають до складу ДП і ОП.

З метою підвищення вірності передачі використовується надлишкове кодування, що дозволяє на прийманні виявити або навіть виправити помилки. У процесі кодування, здійснюваного кодером каналу, вихідна кодова комбінація простого k -елементного коду перетвориться, і до неї вноситься надлишковість. На приймальному кінці декодер каналу виконує зворотне перетворення (декодування), у результаті якого одержуємо комбінацію вихідного коду. Часто кодер і декодер каналу називають пристроєм захисту від помилок (ПЗП).

Сигнал на виході ПЗП являє собою деяку послідовність одиничних елементів постійного струму. Такий первинний сигнал у більшості випадків не може бути безпосередньо переданий по каналу зв'язку. Так, наприклад, у дискретно-безперервних каналах виникає необхідність спектрального узгодження характеристик дискретного джерела інформації й безперервного переносника в каналі, оскільки основна частина енергії послідовності двійкових імпульсів припадає на ділянку низьких частот, що не пропускаються каналом. Спектральне узгодження, а також узгодження по амплітуді сигналів джерела й каналу здійснюється в пристрої перетворення сигналів (ППС), що є одним з основних елементів передавача й приймача системи ПДП, пристроєм, що перетворює сигнали джерела в лінійні сигнали й лінійні сигнали в сигнали одержувача повідомлень. В окремому випадку – це модулятор і демодулятор. Разом з каналом зв'язку ППС утворюють дискретний канал (ДК), тобто канал, призначений для передачі лише дискретних сигналів. Розрізняють синхронні й асинхронні дискретні канали.

Дискретний канал з кодером і декодером каналу ПЗП називається розширеним дискретним каналом або каналом передавання даних. Дискретний канал характеризується швидкістю передачі інформації, яка вимірюється в бітах у секунду (біт/с), або швидкістю модуляції, яка вимірюється в бодах. Іншою характеристикою дискретного каналу є вірність передачі одиничних елементів. Для характеристики каналу передачі даних використовуються наступні параметри – коефіцієнт помилок по кодових комбінаціях і ефективна швидкість передачі інформації.

У системі ПДП іноді виділяють дискретний канал безперервного часу (рис. 1.17).

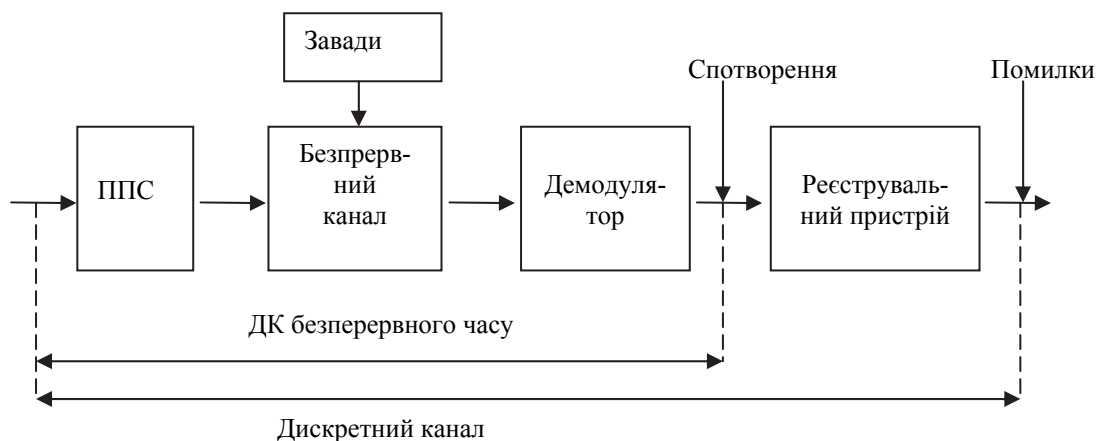


Рисунок 1.17 – Структура дискретного каналу

Якщо на виході дискретного каналу є сигнал, що є дискретною функцією дискретного часу, то на виході дискретного каналу безперервного часу сигнал є дискретною функцією безперервного часу. Часто дискретний канал безперервного часу називають каналом постійного струму (КПС),

тому що на його виході сигнали мають форми імпульсів постійного струму (ШТ).

Канал постійного струму – поняття, що дозволяє розглянути передавання сигналів як процес проходження імпульсів через деякий фільтр, у якому діють спотворюючі завади. Назва каналу обумовлена тим, що він здатний забезпечити передавання будь-якого імпульсного сигналу з постійною складовою.

Сучасні системи збору й обробки інформації орієнтовані на передачу даних із заданими імовірнісними й часовими характеристиками, тому доцільно розглянути структуру тракту передачі даних при організації зв'язку по існуючих каналах і мережах – телефонних, телеграфних, локальних та інших.

Тракт передачі даних, у свою чергу, як і система передавання містить всі перераховані вище елементи структури системи ПДП (рис. 1.16), але з урахуванням протоколів і правил взаємодії на різних рівнях мережі ПД.

У цей час розроблена й впроваджена концепція побудови структури каналу передавання даних при апаратно-програмному способі її реалізації.

Функції програмно-апаратних засобів ПД систематизовані в еталонній моделі архітектури відкритих систем (OSI – Open System Interconnection), прийнятою й рекомендованою Міжнародною організацією стандартів МККТТ (ITU-T), заснованій на багаторівневій ієрархічній концепції мережі. Основною перевагою цієї концепції є те, що вона, визначивши автономні функціональні рівні, що підлягають стандартизації, відкрила можливість незалежного створення і вдосконалення обладнання й програмного забезпечення різних функціональних ланок. Дана модель поширюється на всі програмно-апаратні засоби, де використовується передавання дискретної інформації й відповідно закріплена протоколами й стандартами. Для різних мереж, наприклад: телефонної мережі загального користування, локальної мережі, глобальній мережі і т.д. – еталонна модель відрізняється деякими додатковими (окремими) функціями, але основні функції присутні у всіх мережах.

Еталонна модель OSI відкритих систем складається з наступних семи рівнів:

- *фізичний* забезпечує інтерфейс із фізичним середовищем і передавання цифрового потоку каналом передачі даних;
- *канальний (ланковий)* виконує функції захисту каналу від помилок при передаванні інформації;
- *мережний* реалізує фізичне або віртуальне з'єднання через мережу між прикінцевими користувачами;
- *транспортний* забезпечує встановлення логічного з'єднання між користувачами згідно з адресою джерела (ініціатора) і одержувача;

- *сеансовий* виконує завдання організації й проведення сеансу зв'язку (відкриття й закриття сеансу зв'язку, синхронізація сеансового з'єднання і т.д.);
- *представницький* реалізує завдання представлення й перетворення даних у мову й формат, що відповідають користувачеві;
- *прикладний* виконує різні функції взаємодії прикладних процесів і безпосередньо пов'язаний з користувацькими програмами (ідентифікація користувачів, взаємодія з іншими рівнями, відображення інформації і т.д.);

Згідно з еталонною моделлю, канал ПД являє собою сукупність засобів двох рівнів: першого, який називається фізичним, і другого – канального (ланкового).

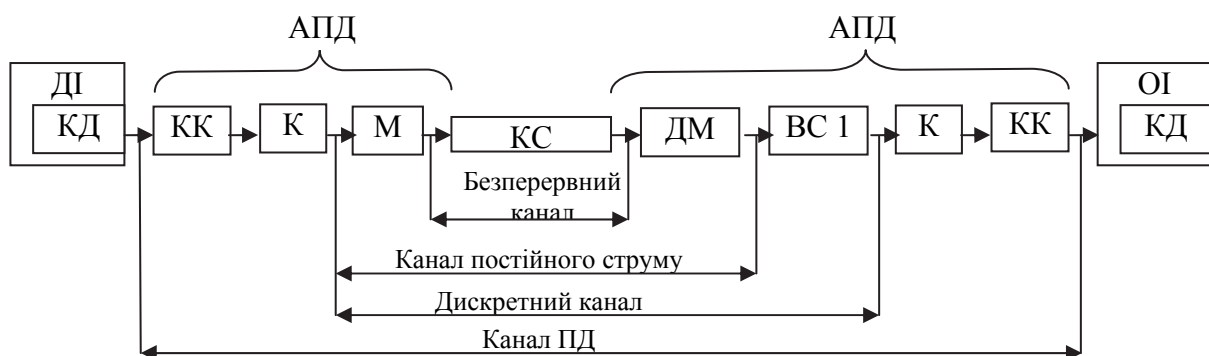


Рисунок 1.18 – Структура каналу передавання даних

Згідно зі структурою каналу ПД (рис. 1.18), визначимо призначення його окремих елементів:

- ДІ, ОІ – джерело й одержувач інформації;
- КД – кодек (кодер – декодер) джерела інформації;
- АПД – апаратура передавання даних;
- КК – засоби керування каналом передавання даних;
- К – кодек каналу (пристрій, що здійснює операції кодування переданої й декодування прийнятої інформації);
- М – модулятор пристрою перетворення сигналів;
- КС – канал зв'язку;
- ДМ – демодулятор пристрою перетворення сигналів;
- ВС 1 – вирішальна схема (реєструвальний пристрій).

Склад засобів наведений для випадку, коли канал зв'язку є безперервним. При використанні цифрового каналу замість модемів застосовуються контролери, що здійснюють сполучення засобів керування з каналом зв'язку.

Складність структури каналів ПД обумовлена, у першу чергу, тим, що для передачі по мережі дані необхідно спеціальним образом відформувати і темп одержання їх від джерела узгодити зі швидкістю передачі каналу. На приймальній стороні необхідно розв'язати зворотні завдання:

- відновити вихідну послідовність даних (з урахуванням можливих втрат і дублювань);
- погодити швидкість приймання інформації з каналу з темпом її видачі одержувачеві.

Крім того, у цей час для ПД широко використовуються канали (найчастіше телефонні), які не забезпечують необхідної вірності переданої інформації й вимагають попереднього перетворення сигналів.

Таким чином, окрім каналу електрозв'язку для передачі даних необхідно додаткове обладнання, що забезпечує високий рівень автоматизації й підвищення завадозахищеності інформаційної взаємодії кореспондуючих сторін.

Фізичному каналу (рис.1.18) відповідає ланцюжок блоків: модулятор М – канал зв'язку – демодулятор ДМ – перша вирішальна схема ВС1. До функцій керування фізичним каналом відносяться наступні:

- встановлення й роз'єднання з'єднань;
- перетворення сигналів (зміна діапазону значень параметрів переносника інформації або перехід до нового переносника з метою узгодження частотних, часових і енергетичних параметрів сигналу з характеристиками каналу зв'язку);
- реалізація інтерфейсу (правила взаємодії) із другим (канальним) рівнем.

Канальний рівень наведений на рис. 1.18 засобами керування каналом передачі, на які покладають наступні основні функції:

- форматування даних (розбивка послідовності бітів на блоки, додавання службової інформації, ознак початку й кінця кадру – самостійно адресованої одиниці інформації другого рівня);
- завадостійке кодування даних кадру на передавальній стороні й декодування на приймальній з метою виявлення помилок, що виникають у процесі передавання по каналу зв'язку;
- організація запитів на повторне передавання кадрів, прийнятих з помилками;
- відновлення вихідної послідовності переданих біт на приймальній стороні;
- узгодження швидкості передачі по каналу зв'язку з темпом їх приймання й видачі користувачеві

Сукупність правил взаємодії однойменних рівнів мережі, що містять характеристики взаємодіючих елементів, називаються протоколом.

Правила взаємодії суміжних рівнів (в одній системі), що містять регламент параметрів сигналу, коду й ланцюгів обміну, називають міжрівневим інтерфейсом. Протоколи й інтерфейси підлягають обов'язковій стандартизації.

Наведені вище функції фізичного й каналного рівнів регламентуються відповідними протоколами.

Характеристики протоколів семирівневої моделі взаємодії відкритих систем розглядаються при вивченні інформаційно-обчислювальних мереж.

Завади в каналах зв'язку. При проходженні переносника інформації по каналу зв'язку він зазнає впливу численних факторів, що змінюють значення його параметрів і, отже, що спотворюють передаваний сигнал. Впливи випадкового характеру називаються завадами, або шумами. Вони спричиняють зміну масштабу (загасання або посилення), часу затримки й форми (викривлення) сигналу. Класифікація завад є можливою за різними ознаками, зокрема, за місцем й *причинам* виникнення й за характером впливу на передаваний сигнал наведена на рис. 1.19.

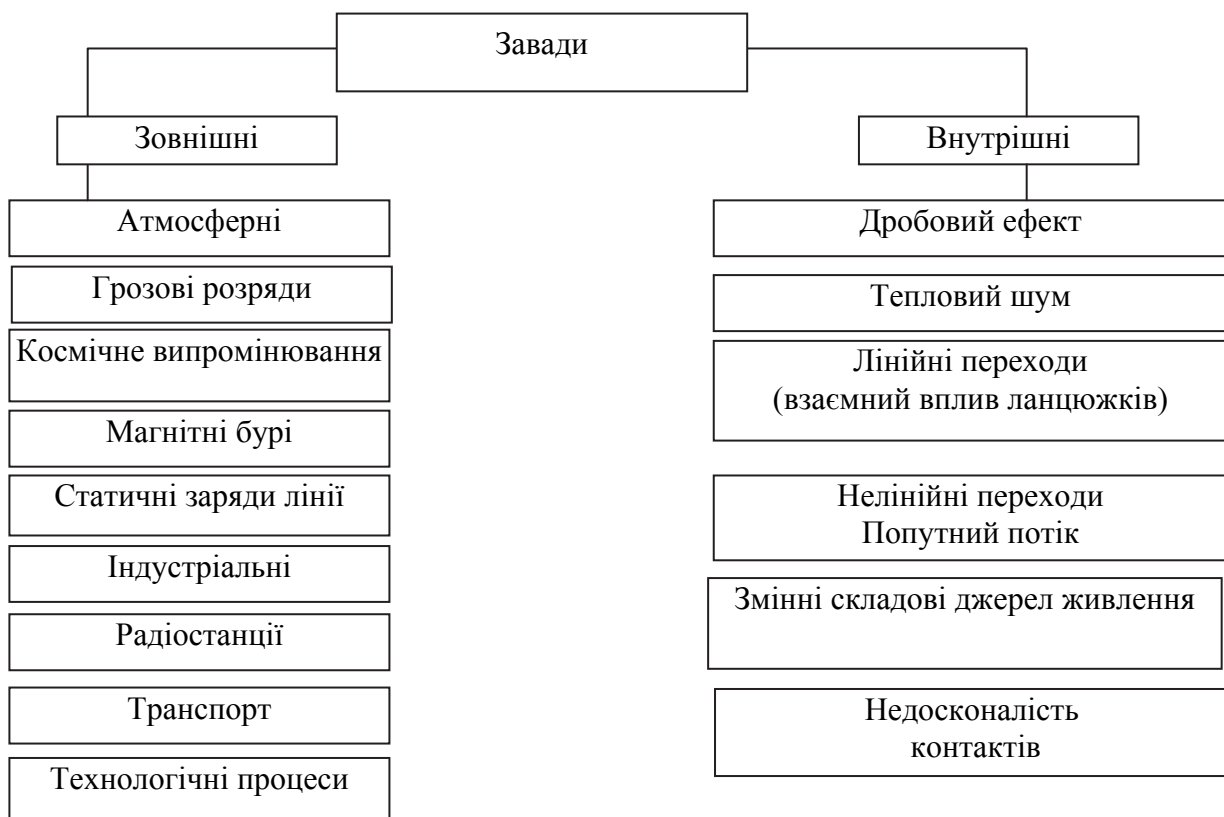


Рисунок 1.19 – Класифікація завад за різними ознаками

Модель безперервного каналу описує нелінійні перетворення сигналу в каналі – мультиплікативні завади й адитивні завади, класифікацію яких відображає структура (рис. 1.20).

Розподіл ймовірностей, окремі параметри й системні функції, що відображають випадкові фактори, які впливають на якість передавання інформації, становлять безліч статистичних характеристик каналу.

Характеристики безперервного каналу називаються *первинними*. Вони відображають, головним чином, причини, які викликають спотворення

сигналу, – нестабільність генераторів несучих і піднесучих частот, стрибки й тремтіння фази, завмирання (у радіоканалах) і зміни залишкового загасання (у кабельних і повітряних лініях), флуктуаційні шуми, імпульсні й гармонійні завади, перерви й нелінійність перетворень, амплітудно- і фазочастотні характеристики. Неідеальність частотних і амплітудних характеристик виникає через регулярні спотворення лише регулярних сигналів. При передаванні випадкових (інформаційних) послідовностей спотворення мають характер, тому що їхня величина залежить від вигляду (форми) сигналу.

Флуктуаційна завада характеризується широким спектром і максимальною ентропією, і тому з нею найскладніше боротися. Однак у провідних каналах зв'язку рівень флуктуаційних завад досить малий і вони при малій питомій швидкості передачі інформації практично не впливають на коефіцієнт помилок.

Зосереджені за спектром, або гармонійні, завади являють собою вузькосмуговий модульований сигнал. Причинами виникнення таких завад є зниження перехідного загасання між ланцюгами кабелю, вплив радіостанцій та ін.

Зосереджені за часом, або імпульсні, завади являють собою випадкову послідовність імпульсів, що мають випадкові амплітуди й проходять один за одним через випадкові інтервали часу, причому, викликані ними перехідні процеси не перекриваються за часом. Причини появи цих завад: комутаційні шуми, наведення з високовольтних ліній, грозові розряди й інші.

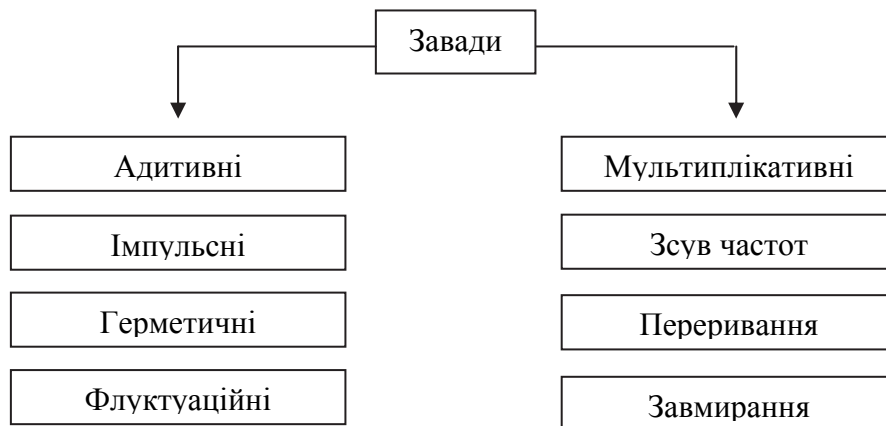


Рисунок 1.20 – Класифікація адитивних і мультиплікативних завад

Мультиплікативні завади обумовлені випадковими змінами параметрів каналу зв'язку. Зокрема, ці завади проявляються в зміні рівня сигналу на виході демодулятора. Розрізняють плавні й стрибкоподібні зміни рівня. Плавні зміни відбуваються за час, який набагато більше, ніж тривалість одиничного інтервалу τ_0 , а стрибкоподібні – за час, менше τ_0 . Причиною

плавних змін рівня можуть бути коливання загасання ліній зв'язку, викликані, наприклад, зміною стану погоди, а в радіоканалах – завмирання. Причиною стрибкоподібних змін рівня можуть бути погані контакти в апаратурі, недосконалість експлуатації апаратури зв'язку, технології вимірів та ін. Зниження рівня більш, ніж 17,4 дБ нижче номінального, називається *перервою*. При перерві рівень падає нижче порога чутливості приймача й приймання сигналів фактично припиняється. Перерви, тривалістю менше 0,3 с, прийнято називати *короткочасними*, більше 0,3 с – *тривалими*, що призводять до руйнування (роз'єднання) тракту передавання.

Основними завадами для каналу передачі даних, наприклад по телефонній мережі, будуть, по-перше, дробовий ефект, обумовлений, в основному, імпульсними завадами, а по-друге, зовнішні технологічні процеси, індустріальні, що є основною причиною появи помилок при передаванні дискретної інформації із провідних каналів зв'язку.

Імпульсні завади виникають, в основному, через зниження перехідного загасання між парами кабелю в одному кабелі або проникають із ланцюгів живлення. Підтримка на необхідному рівні перехідного загасання, фільтрація в ланцюгах живлення, застосування розв'язувальних агрегатів живильного обладнання суттєво знижує рівень імпульсної завади.

До спотворень форми сигналу на виході безперервного каналу призводить також зсув його спектральних складових по частоті, фазові стрибки й фазове тремтіння несучого коливання, в результаті яких з'являється паразитна кутова модуляція сигналу.

Крім випадкових змін під дією завад, сигнал одержує також спотворення регулярного характеру, які можуть бути як лінійними, так і нелінійними. Лінійні спотворення обумовлені відхиленнями амплітудно-частотних (АЧХ) і фазочастотних (ФЧХ) характеристик від ідеальних форм. Нелінійні спотворення обумовлені нелінійністю характеристик підсилювальних елементів і перетворювачів, включенням обмежників амплітуд для захисту від перевантажень, залежністю залишкового загасання від рівня вхідного сигналу. При розгляді питань передачі дискретної інформації регулярними нелінійними спотвореннями, як правило, зневажають, оскільки діючі норми на власні нелінійності каналу й сумарну потужність групового сигналу практично виключають їх із числа істотних факторів підвищення невизначеності сигналу.

Характеристики сигналу на виході каналу постійного струму називають *вторинними*. Вони відображають ступінь спотворення одиничних елементів і включають крайові спотворення, дроблення, масу спотворень. Найбільш повною характеристикою якості дискретного каналу є статистика помилок, що виникають при передачі інформації.

Завдання дослідження – вивчити вторинні характеристики (крайові, дроблення, помилки) на основі зібраних статистичних даних, описати модель потоку помилок у каналі передачі даних, попередньо визначивши за-

кон розподілу помилок. За допомогою моделі потоку помилок можна визначити необхідні заходи для збільшення вірності передаваної інформації.

Причинами спотворення кодових посилок є первинні характеристики каналу зв'язку, але залежність між цими характеристиками й вірогідністю приймання інформації до теперішнього часу в повному обсязі ще не встановлена.

Наявність же даних про вторинні характеристики каналу зв'язку, хоча й не дозволяє виявити причини спотворення кодових посилок, але забезпечує можливість оцінки вірогідності прийнятої інформації. Розглянемо вторинні статистичні характеристики каналів зв'язку.

Якість кодових посилок, передаваних джерелом інформації з каналу зв'язку, визначається точністю їх відтворення вхідним прийомним пристроєм. Якщо тривалість відтворених посилок відрізняється від тривалості переданих (вони вкорочені або подовжені), то це означає, що кодові посилки прийняті зі спотворенням. Таким чином, сутність спотворення полягає в зсуві границь (країв) між кодовими посилками різної полярності щодо ідеального їхнього положення.

Якщо зсув границі в ту або іншу сторону не перевищує виправляючої здатності μ приймача ($0 \leq \mu \leq 0,5$), то спотворення, яке виникло через цей зсув, називається *крайовим*. Таке спотворення може бути виправлене реєструючим (регенеративним) пристроєм приймача.

Вивчення спотворень кодових елементів можливо як шляхом установлення закономірних залежностей між первинними й вторинними характеристиками каналу зв'язку, так і шляхом безпосереднього виміру вторинних характеристик (крайових спотворень, дроблень, помилок).

Нехай на вхід каналу постійного струму (КПС) надходить послідовність прямокутних імпульсів тривалістю τ_0 . Якщо на вході каналу всі значущі моменти (ЗМ) зміщені щодо вихідних на однаковий час Δt , що визначається часом перехідного процесу, то ЗМ збігаються з ідеальними, а значущі інтервали часу – з ідеальними значущими інтервалами. При цьому значущі інтервали часу сигналів на виході каналу дорівнюють відповідним значущим інтервалам часу сигналів, що надходять на вхід каналу. Однак причиною зсуву ЗМ щодо ідеальних моментів може бути не тільки запізнення, обумовлене кінцевим часом поширення сигналів, але й інші фактори. При цьому КПС у каналі спотворюються. На рис. 1.21 зображено дві послідовності імпульсів: прийнята ідеальна й прийнята реальна.

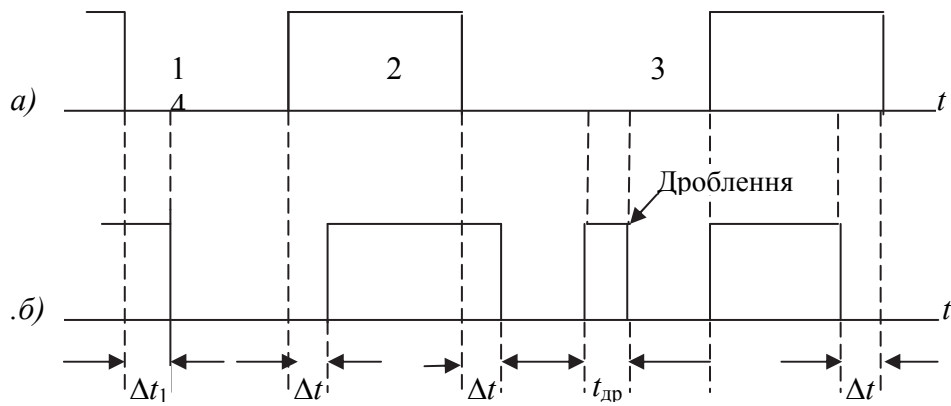


Рисунок 1.21 – Послідовність сигналів

Якщо в ідеальній послідовності тривалість усіх прийнятих імпульсів дорівнює τ_0 , то в реальній послідовності зсуву ЗМ щодо ідеальної тривалості елементів сигналу відрізняються від τ_0 .

Для характеристики зсуву кожного зі ЗМ сигналу щодо ідеального ЗМ вводять поняття індивідуального крайового спотворення.

Для i -го ЗМ цей зсув дорівнює $\Delta t_{сп\ i}$. Величина (ступінь) індивідуального спотворення визначається як $\delta_{інд} = \Delta t_{сп\ i} / \tau_0$. Зсув ЗМ щодо ідеального ЗМ вправо прийнято вважати позитивним, а вліво – негативним. Максимальний розкид зсувів ЗМ на інтервалі $2\tau_0$ називається ступенем ізохронного спотворення:

$$\delta_{ізохр} = \frac{\Delta t_{макс} - \Delta t_{мін}}{2\tau_0} \times 100\%,$$

де $\Delta t_{мін\ i}$ – максимальне й мінімальне значення ЗМ.

Спотворення, які виникли через зсув границь між кодовими послілками, можуть бути розділені на три види: випадкові, від переважання й характеристичні.

Випадкові спотворення обумовлені завадами, дія яких не є регулярною (індуктивні впливи між ланцюгами, короткочасні торкання проводів, атмосферні явища й ін.). При цьому величина $t_{іск\ i}$ має випадковий характер.

Спотворення від переважання пов'язані з наявністю часткового переважання вихідного й вхідного релейних (порогових) пристроїв, нестабільністю напруг джерел живлення й ін. Ці спотворення, якщо вони не усунуті регулюванням, зберігають постійну величину.

Характеристичні спотворення визначаються характеристиками каналу зв'язку, параметрами вхідного релейного пристрою, швидкістю передачі послілок та ін. Ці викривлення міняються за величиною й полярністю залежно від комбінації послілок у кодових послідовностях. Характеристичні спотворення, як і спотворення від переважання, виникають під впливом регулярно діючих факторів і мають назву *систематичних спотворень*.

Характеристичні спотворення проявляються за умови, якщо час наростання перехідного процесу $\tau_{\text{пн}} > \tau_0$. При передаванні послідовності змін полярностей сигналу (типу точок) характеристичні спотворення відсутні.

Крім крайових спотворень, елементи імпульсної послідовності можуть зазнати дроблень (рис. 1.21, б) – короткочасні зміни полярностей імпульсів у межах прийнятого одиничного елемента τ_0 . Цей вид спотворень переважає при передаванні інформації по каналах радіозв'язку й по комутуваних каналах зв'язку.

Оскільки зсуви границь кодових посилок обумовлені великою кількістю взаємно незалежних випадкових факторів (завад), дія кожного з яких у порівнянні із сумарною їхньою дією невелика, то згідно з відомою теоремою А.М. Ляпунова, закон розподілу зсувів границь лише незначно буде відрізнятися від нормального закону. Численні виміри підтверджують цей висновок.

Якщо не враховувати систематичні спотворення (постійні переважання й характеристичні спотворення), то густина розподілу зсувів границь

$$f(\delta) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\delta^2}{2\sigma^2}},$$

де δ – величина зсуву границі; σ – середнє квадратичне відхилення δ , характеризує розкид зсувів границь кодових посилок від їхніх ідеальних положень; σ^2 – дисперсія величини δ .

При визначенні частоти появи й закону розподілу дроблень користуються поняттям «імпульс дроблення». Під імпульсом дроблення розуміється зміна полярності поданої в канал зв'язку постійної напруги (переривання ланцюга).

Імпульси дроблень характеризуються середньою кількістю переривань каналу в одиницю часу (інтенсивністю дроблень) і тривалістю переривань. На підставі експериментальних даних встановлено, що густина розподілу тривалостей імпульсів дроблень визначається логарифмічно-нормальним законом:

$$f(x) = \frac{1}{\tau\sigma_\tau\sqrt{2\pi}} e^{-\frac{(\ln \tau - \alpha)^2}{2\sigma_\tau^2}},$$

де τ – тривалість дроблення; α – середнє значення випадкової величини $\ln \tau$; σ_τ – середнє квадратичне відхилення $\ln \tau$.

Слід зазначити, що імпульси дроблень часто виникають у вигляді «пачок дроблень», які є однією з основних причин помилок.

Очевидно, що помилка може виникнути в результаті одночасного впливу крайових викривлень і дроблень.

Якщо помилки, що виникають у передаваній інформації, відбуваються незалежно одна від іншої, то прийнято вважати, що розподіл їх підкоряється біноміальному закону. Нехай імовірність помилкового приймання

однієї кодової послідовності дорівнює p_0 , тоді ймовірність правильного її приймання буде $1 - p_0$. Правильне приймання символу повідомлення можливо лише в тому випадку, якщо усі n кодових послідовностей комбінації зв'язку, що надійшли з каналу, зберегли свою полярність. Згідно з теоремою про сумісні й незалежні події ймовірність правильного приймання всіх n послідовностей кодової комбінації рівна $(1 - p_0)^n$, а $p_{\text{пом}} = 1 - (1 - p_0)^n$.

Слід зазначити, що в практичних умовах помилки, що з'являються в передаваній інформації, у більшості випадків є залежними (корельованими), причому вони виникають у поруч розташованих елементах кодової послідовності у вигляді окремих груп або пачок. Результати експериментальних досліджень показали, що час групування помилок у пачки становить незначну частку всього часу передавання, але протягом цього часу зосереджена найбільша кількість помилок. В інтервалах же між пачками виникають рідкі незалежні помилки. Наприклад, при середній ймовірності помилок $1 \cdot 10^{-4} \dots 1 \cdot 10^{-6}$ ймовірність помилки в межах часу групування зростає до $2 \cdot 10^{-1} \dots 5 \cdot 10^{-1}$. Тому оцінка якості зв'язку на основі біноміального закону розподілу помилок є приблизною.

Закони розподілу помилок у каналах зв'язку вивчаються переважно експериментальним шляхом.

При розробці систем передавання інформації використовуються також аналітичні методи, що базуються на побудові математичних моделей появи помилок. У цих моделях прагнуть відобразити з достатньою для інженерних розрахунків точністю отримані експериментальним шляхом характеристики різномісних каналів зв'язку.

Методи приймання дискретних сигналів. При відновленні переданого повідомлення за сигналом, прийнятому з каналу з завадами й спотвореннями, можна судити лише про ймовірність того, що був переданий той чи інший сигнал з множини використовуваних. Приймач на основі аналізу прийнятого сигналу й з обліком усіх відомих відомостей про характер джерела й властивості каналу зв'язку повинен прийняти рішення щодо того, яке повідомлення було передано.

Відомо два методи приймання сигналів – *поелементний* спосіб приймання й приймання *в цілому*. При *поелементному* прийманні перша вирішальна схема дає остаточне рішення про окремі елементи сигналу, причому це рішення може супроводжуватися втратою деякої інформації. Тому друга вирішальна схема, що ототожнює прийняту послідовність елементів сигналу (кодову комбінацію) з відповідним символом, має в загальному випадку неповну інформацію про прийнятий сигнал.

При прийманні *в цілому* вся інформація, що міститься в прийнятому сигналі (кодовій комбінації), щодо передаваного повідомлення може бути використана об'єднаною вирішальною схемою, у результаті чого забезпечується більша вірність приймання по елементах. Лише при безнадлишковому кодуванні приймання в цілому не має переваг у порівнянні із поеле-

ментним прийманням. Проте приймання в цілому не знаходить широкого застосування через технічну складність його реалізації.

У процесі передавання сигналу $S_i(t)$ на вході приймального пристрою надходить суміш спотвореного сигналу й завад $\tau_i(t) = \mu \cdot S_i^0(t) + n(t)$, $0 \leq t \leq \tau_0$, де τ_0 – тривалість елемента сигналу: $i=1, 2$; μ – коефіцієнт передавання каналу; $n(t)$ – адитивна завада. Завдання приймача полягає в тому, щоб на основі аналізу прийнятої конкретної реалізації $\tau_k(t)$ протягом інтервалу часу τ_0 встановити, який з можливих сигналів: S_1 або S_2 – є присутнім на його вході й, відповідно до цього, який елемент послідовності був переданий.

Процес одержання корисної інформації, що міститься в прийнятому сигналі, називається обробкою сигналу. При передаванні дискретної інформації, на відміну від безперервної, у функції приймача не входить відновлення форми переданого сигналу (оскільки вона відома), а лише прийняття правильного рішення.

Для розрізнення сигналів у приймачі необхідно забезпечити можливість установлювати границі інтервалу аналізу ($0 \leq t \leq \tau_0$) кожної реалізації сигналу $\tau_k(t)$, що забезпечується пристроєм синхронізації по елементах.

Процес ототожнення прийнятого елемента сигналу з певним кодовим символом реалізується в процесі демодуляції. У результаті дії завад і спотворень у каналі зв'язку приймач може прийняти неправильне рішення, тобто ототожнювати прийнятий сигнал не з фактично переданим символом, а з якимось іншим, у результаті чого виникає помилка. З теорії зв'язку відомо, що ймовірність помилки визначається відношенням енергії корисного сигналу й енергії завади. Тому одним з найважливіших завдань приймача є підвищення цього відношення, яке реалізується у вхідному блоці (рис. 1.22).

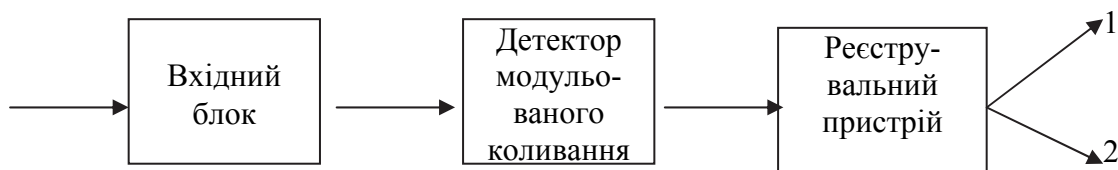


Рисунок 1.22 – Приймач дискретних сигналів

Іншим найважливішим завданням приймача є виділення із прийнятого сигналу моделюючої функції, тобто демодуляції. І, нарешті, третє завдання – прийняття рішення, яке здійснюється у вирішальному (реєструвальному) пристрої.

Способи приймання залежно від методу виділення моделюючої функції можна розділити на дві групи: *когерентні* й *некогерентні*.

При когерентному детектуванні використовуються опорні сигнали, що являють собою точні копії передаваних (з точністю до початкової фа-

зи). При некогерентному детектуванні апіорні відомості про початкову фазу несучої частоти не враховуються.

Приймач приймає рішення на основі аналізу прийнятого елемента сигналу. Час аналізу не перевершує τ_0 , тому що після закінчення цього періоду відбувається приймання наступного елемента. По видах приймання рішення (реєстрації) методи приймання можна розділити на три групи: кореляційні, стробування, інтегральні.

Процес визначення й запам'ятовування значущої позиції дискретного сигналу називається *реєстрацією*. Пристрій реєстрації сигналів, що забезпечує мінімальну ймовірність неправильного приймання $p_{\text{пом}}$, називають *оптимальним*. Реалізація оптимального пристрою реєстрації має певні труднощі, тому на практиці застосовують спрощені методи реєстрації, які хоча й програють у завадостійкості оптимальному, однак більш прості в реалізації. До числа найпоширеніших методів реєстрації відноситься: метод *стробування* й *інтегральний*.

При реєстрації методом *стробування* вид прийнятого елемента (0) або (1) визначається на підставі аналізу знака ІПС (сигнали на виході КПС) у середині одиничного інтервалу. Будь-який зсув моменту реєстрації щодо середини одиничного інтервалу призводить до збільшення ймовірності неправильної реєстрації сигналу, тому що при дії крайових викривлень середина є найбільш стійкою частиною прийнятого елемента сигналу.

Розглянемо більш докладно метод стробування. Структурна схема пристрою, що здійснює реєстрацію елементів дискретних сигналів методом стробування, наведена на рис. 1.23, а часові діаграми, що пояснюють принцип його роботи, – на рис. 1.24.

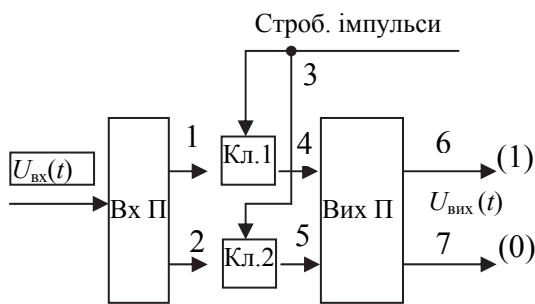


Рисунок 1.23 – Схема приймача стробування

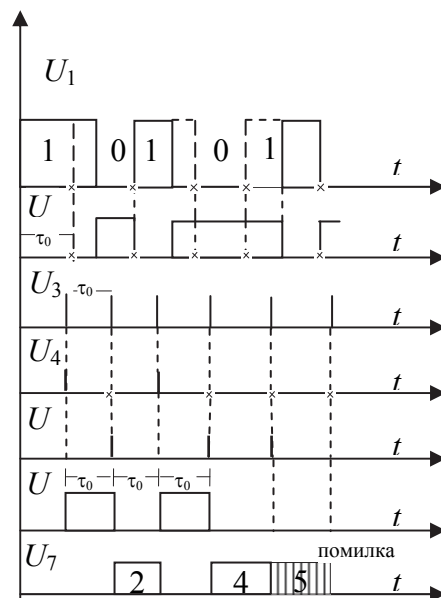


Рисунок 1.24 – Часова діаграма роботи приймача зі стробуванням

Нехай передавалася послідовність (10101). На виході вхідного пристрою (Вх.П, точки 1 і 2) сигнали відновлені за формою, але спотворені за тривалістю. Пунктиром на рис. 1.24 показані неспотворені сигнали. Ключі Кл.1 і Кл.2 відкриваються лише на час надходження стробімпульсів (точка 3). При цьому імпульси реєстрації з'являються на виході або Кл.1 (точка 4), або Кл.2 (точка 5). Залежно від цього вихідний пристрій (Вих. П) приймає стан вхідного й видає (1) або (0). Якщо зсув ЗМ щодо ідеального положення не перевищує $0,5\tau_0$, то елементи сигналу реєструються правильно. Максимальний зсув ЗМ, що не викликає неправильне приймання, визначає виправляючу здатність приймача. У нашому випадку виправляюча здатність (теоретична) дорівнює $0,5\tau_0$, або 50 %. На рис. 1.24 показано (U_7), що п'ятий елемент приймається невірно через зсув ЗМ щодо ідеального положення на величину, що перевищує $0,5\tau_0$.

Спочатку метод стробування застосовувався у приймачах з електро-механічними реєструвальними пристроями.

Правильність прийнятих методом стробування рішень визначається одномірними статистичними характеристиками випадкового процесу $r(t)$. І хоча це рішення проводиться в середній частині елементарного сигналу, що найменше піддається спотворенням, є певна ймовірність прийняття помилкового рішення.

Прагнення зменшити ймовірність цієї помилки призводить до ідеї прийняття рішення на основі не одноразового, а багаторазового аналізу сигналу або його безперервного аналізу на інтервалі τ_0 . Такий метод реєстрації називається *інтегральним*.

При інтегральному методі реєстрації одиничних елементів рішення про знак елемента вноситься на основі аналізу сигналу, що знімається з виходу КПС, на інтервалі всієї його тривалості

$$U_{\text{вих}} = \int_0^{\tau_0} U_{\text{вх}}(t) dt,$$

де $U_{\text{вих}}$ – сигнал на виході реєструвального пристрою; $U_{\text{вх}}(t)$ – сигнал на вході реєструвального пристрою, приймає значення (0) або (1).

Інтегральний метод часто реалізується на основі багаторазового аналізу (стробування) елемента сигналу $U_{\text{вх}}(t)$ в N точках. Рішення вноситься за правилом більшості: якщо число стробувальних імпульсів, що надійшли в лічильник аналізу за час τ_0 , перевищило $N/2$, то сигнал, що $U_{\text{вх}}(t)$ надійшов, зчитується одиницею.

Схема, що пояснює принцип дії такого пристрою реєстрації, наведено на рисунку 1.25, а часова діаграма роботи – на рисунку 1.26.

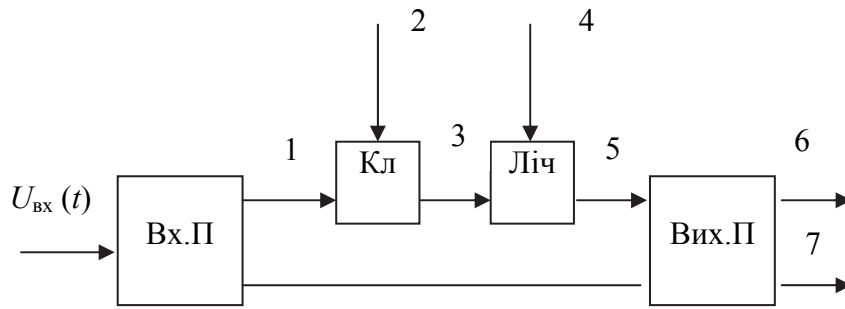


Рисунок 1.25 – Схема дискретного інтегрального приймача

Сигнал $U_1(t)$ (точка 1, рис. 1.25) керує відмиканням і запиранням ключа. При відімкнутому ключі тактові (стробувальні) імпульси проходять на вхід лічильника (Ліч). За час дії неспотвореної струмової посилки $U_1(t)$ (на інтервалі τ_0) на виході ключа (точка 3) з'являється N тактових імпульсів. Якщо на виході ключа на одиничному інтервалі з'явиться $\frac{N}{2} + 1$ й більш стробімпульсів, то можна зробити висновок про те, що прийнятий сигнал – (1). Ємність лічильника достатньо обрати рівною $\frac{N}{2} + 1$. Наприкінці одиничного інтервалу, який визначається за допомогою пристрою поелементної синхронізації, показання лічильника зчитуються, і він обнулюється.

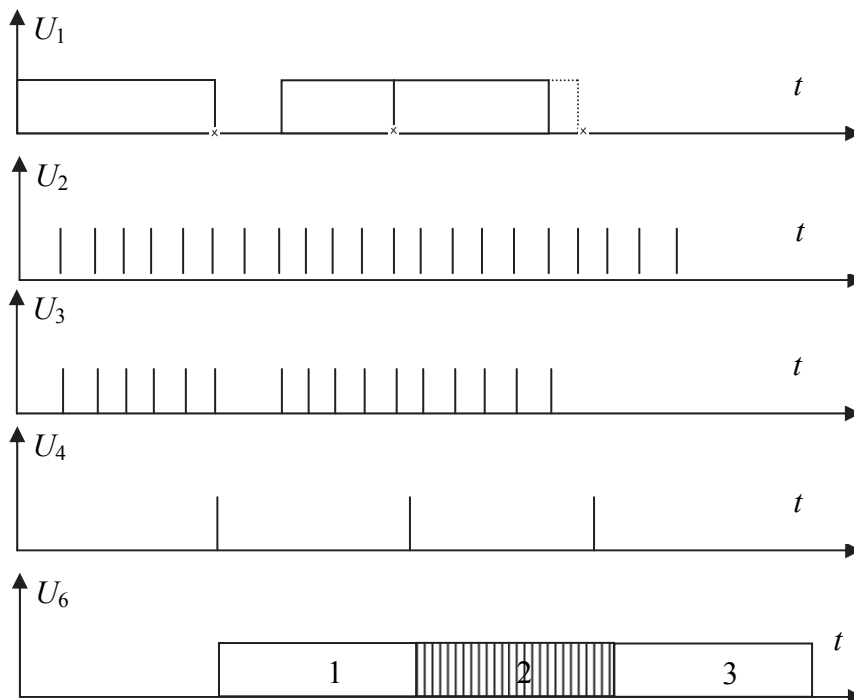


Рисунок 1.26 – Часова діаграма роботи дискретного інтегрального приймача

На часовій діаграмі (рис. 1.26) ілюструється процес реєстрації серії ПС. Передавана послідовність – (101), прийнята – (111). Очевидно, що другий елемент реєструється невірно.

Сутність *кореляційного* методу приймання полягає в тому, що рішення про конкретну реалізацію сигналу вноситься на основі порівняння з порогом випадкової функції

$$r'(t) = \int_0^{\tau_0} \eta(t)r(t)dt$$

у фіксований момент часу $0 \leq t_p < \tau_0$. При цьому розрізняють *взаємно кореляційний* метод приймання, при якому опорна напруга $\eta(t)$ відрізняється від передаваного сигналу лише початковою фазою несучої, і *автокореляційний* метод приймання, при якому опорна напруга являє собою прийнятий сигнал, зміщений на $k\tau_0$, де $k=1, 2, \dots$ [$k=1$, тобто $\eta(t) = r(t - \tau_0)$].

Вважаючи $\eta(t) = 1$, приходимо до алгоритму інтегрального приймання, тобто інтегральне приймання є окремий випадок кореляційного.

В останні роки ведеться пошук простих у реалізації, але близьких до оптимальних по завадостійкості методів реєстрації. Запропоновано ряд методів, серед яких розглянуті нижче багатоінтервальний метод і метод інтегрування з ваговою функцією.

Особливість багатоінтервального методу полягає у відмові від обов'язкової обробки сигналів на одиничному інтервалі, який дорівнює τ_0 . Інтервал обробки, на якому здійснюється реєстрація інтервальним методом, вибирається залежно від характеру викривлення ПС. Алгоритм вибору інтервалу обробки полягає в наступному. Якщо надходить одиничний елемент, що містить дві границі (два ЗМ), причому кожна із границь зміщена щодо ідеального ЗМ не більше, чим на задану граничну величину, то сигнал інтегрується в інтервалі часу, обмеженому цими двома границями. Якщо ж зсув границі (обох границь) перевищує граничну величину, то границя (границі) замінюється тактовим імпульсом (імпульсами), що виробляються системою поелементної синхронізації. У випадку, коли у елементі сигналу, що надходить, немає границі (границь), тобто надходять підряд кілька однакових елементів сигналу, то як і раніше відсутня границя замінюється тактовим імпульсом. Коли в інтервал часу, обмежений граничними зсувами границь (інтервал фіксації t_ϕ), попадає кілька границь (з'являються неправильні границі), то інтегрування сигналу починається (закінчується) з появою першої границі, що надійшла.

На рис. 1.27 для прикладу наведено спотворений елемент сигналу. Реєстрація цього елемента звичайним інтервальним методом проводиться в інтервалі а...г (інтервалі, що відповідає випадку неспотвореного приймання одиничного елемента). При цьому забирається попередній і наступний елементи. При використанні багатоінтервального способу інтегрування

здійснюється в інтервалі б...в, що дозволяє краще використовувати енергію сигналу.

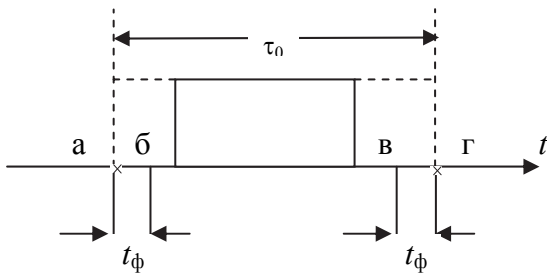


Рисунок 1.27 – Приймання зі спотворенням

Зменшити ймовірність помилки можна також, застосовуючи реєстрацію з ваговою функцією. Якщо відомо характер спотворень різних ділянок на тривалості одиничного елемента τ_0 , то відлік необхідно робити з різною вагою: там, де викривлення з'являються рідше, вагу необхідно збільшити, і навпаки. Описані раніше методи реєстрації інтегральний і стробування мож-

на розглядати як окремий метод реєстрації з ваговою функцією. При інтегральному методі кожній точці аналізу надається вага, однакова на усьому інтервалі τ_0 , а при стробування середня частина береться з вагою 1, а всі інші частини – з вагою 0 (не враховуються).

Широко застосовуване на практиці поелементне приймання, хоча й простіше в реалізації, ніж приймання в цілому, але програє останньому по завадозахищеності. Причина цього полягає в тому, що в процесі демодуляції при поелементному прийманні відбувається незворотня втрата інформації, тому що параметри прийнятого сигналу й обчислені значення апостеріорних ймовірностей можливих символів ніяк не використовуються в другій вирішальній схемі (декодері) при прийнятті остаточного рішення про передану кодову комбінацію. У зв'язку із цим розроблено ряд методів, що забезпечують підвищення завадостійкості за рахунок часткового використання тієї інформації, яка губиться при поелементному прийманні. До числа найпростіших з них і в той же час досить ефективних слід віднести приймання зі стиранням.

Сутність приймання зі стиранням полягає в тому, що у вирішальному пристрої встановлюють не одно-, а двопороговий детектор (ДТ). Демодульований у ДМ сигнал $Y(t)$ ототожнюється з одиницею, якщо він перевищує деякий поріг C_1 , якщо ж він не досягає іншого порога C_0 , то вирішальним пристроєм виробляється нуль. Якщо ж $C_1 \geq Y(t) \geq C_0$, тобто виникає сумнів у визначенні символу, то вирішальний пристрій виробляє спеціальний сигнал стирання (S), який подається на декодувальний пристрій (ДКП) (рис. 1.28).

Як контрольований параметр може бути обраний будь-який параметр сигналу. Контроль параметрів сигналу може відбуватися як в аналоговому каналі – додетекторний контроль, так і в дискретному каналі – післядетекторний контроль. Доцільним є спостереження за

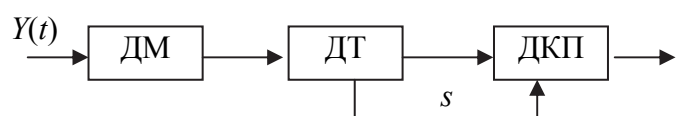


Рисунок 1.28 – Схема приймача зі стиранням

тими параметрами сигналу, зміна яких з великою ймовірністю сприяє виникненню помилок. Відповідно до Рекомендацій МККТТ в аналоговому каналі контролюється величина амплітуди обвідної (рівень) сигналу. У дискретному каналі контролюють амплітуду сигналу й величини крайових спотворень. Використовується також різновид дискретного інтегрального методу приймання, що полягає в тому, що на одиничному елементі робиться кілька проб, і рішення про приймання того або іншого символу вноситься лише при обов'язковому збіганні результатів усіх проб. Якщо ж результат хоча б однієї із проб відрізняється від інших, виробляється сигнал стирання.

Проведемо оцінку завадостійкості окремих методів реєстрації дискретних сигналів при наявності спотворень у каналі зв'язку.

Через те, що спотворення тривалості елементів є результатом дії завад (рис. 1.29 *a, б, в*), то можна оцінювати завадостійкість приймачів по їхній здатності правильно реєструвати знак спотвореного елемента. Кількісно ця властивість приймачів оцінюється величиною *виправляючої здатності*. За величину виправляючої здатності приймача слід вважати максимальну величину спотворень одиничних елементів, при якій приймальний пристрій ще здатний правильно зареєструвати двійковий елемент.

Виправляюча здатність є одним з найбільш важливих параметрів, що характеризують якість роботи приймального пристрою. Її величина в значній мірі впливає на вірогідність приймання повідомлень.

Слід розрізнити виправляючу здатність приймача за крайовими спотвореннями μ і за дробленнями ν .

Виправляюча здатність за крайовими спотвореннями чисельно дорівнює відносному зсуву однієї із границь (ЗМ) одиничних елементів від ідеального (неспотвореного) положення, при якому ще можлива правильна реєстрація знака імпульсу (рис. 1.29):

$$\mu = \frac{\Delta t_{\text{макс}}}{\tau_0} \times 100\%,$$

де $\Delta t_{\text{макс}}$ – максимальна величина зсуву ЗМ, при якому ще забезпечується правильне приймання.

Виправляюча здатність за дробленнями дорівнює відносній максимальній тривалості дроблення, що не викликає невірної реєстрації знака імпульсу:

$$\nu = \frac{\Delta t_{\text{др}}}{\tau_0} \times 100\%.$$

Розрізняють три види виправляючої здатності: теоретичну, номінальну й робочу.

Теоретична виправляюча здатність μ_T , ν_T , обчислюється на основі конструктивних або схемних даних приймального пристрою в припущенні, що воно працює в ідеальних умовах. При цьому виходять із наявності ідеа-

льної синхронізації між передавачем і приймачем, тобто передбачається, що номінальне положення границь одиничних елементів визначене пристроєм поелементної синхронізації з ідеальною точністю: аналізуючі імпульси подаються точно в середину елементів при реєстрації в середній точці й відповідають точно краям елемента при реєстрації інтегральним методом.

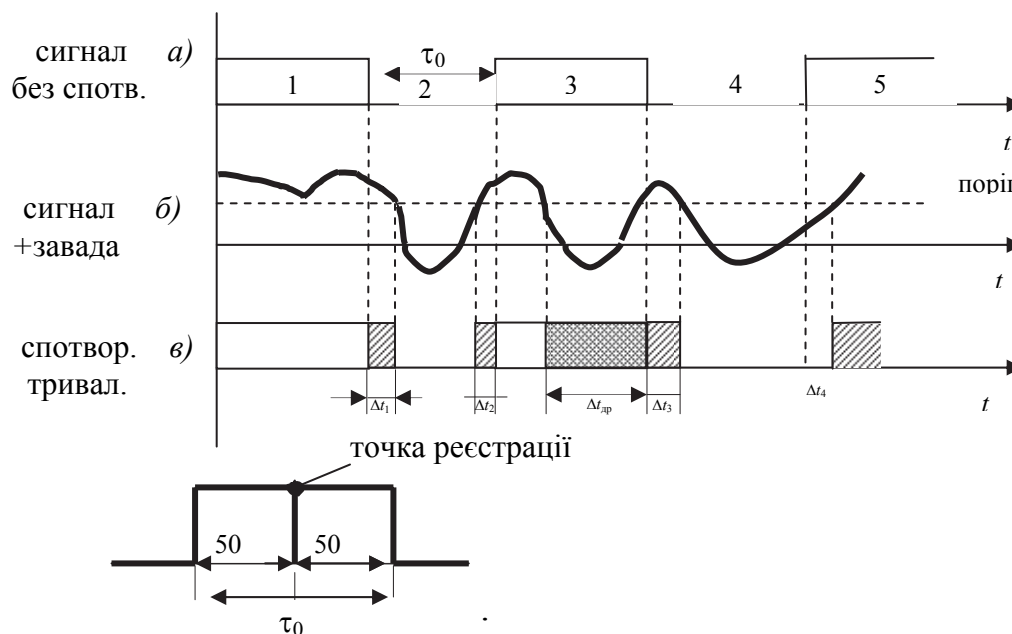


Рисунок 1.29 – Приклади спотворень дискретних сигналів

Тоді для методу реєстрації в середині одиничного елемента згідно рис. 1.29, з, маємо

$$\mu_{\tau} = \frac{0,5\tau_0}{\tau_0} \times 100\% = 50\%, \quad \nu_{\tau} = 0.$$

Для інтегрального методу реєстрації умова правильної реєстрації записується як $\Delta t_{\Sigma} < \tau_0 / 2$, де Δt_{Σ} – час, протягом якого елемент відрізняється від переданого. Якщо елемент спотворюється із двох сторін, то $\mu_{\tau} = 25\%$. Очевидно, що $\nu_{\tau} = 50\%$.

У реальних системах неточність місця розташування аналізуючих імпульсів визначається похибкою синхронізації, яка викликана неточністю роботи схеми синхронізації й спотворенням сигналів. Виправляюча здатність реальних приймачів завжди менше її теоретичної межі. Це зменшення враховується величиною номінальної ($\mu_{н}$, $\nu_{н}$) і робочої ($\mu_{р}$, $\nu_{р}$) виправляючої здатності.

Порівняємо методи стробування й інтегральний при дії крайових спотворень. Оскільки при реєстрації методом стробування елемент реєструється в середині, то допускається зсув кожного зі ЗМ на величину, що не перевищує $0,5\tau_0$. При реєстрації інтегральним методом сумарний зсув гра-

ниця Δt_{Σ} не повинен перевищувати $0,5 \tau_0$. Очевидно, що остання умова виконується з меншою ймовірністю, тобто

$$P_{\text{пом кр с}}^{\text{інт}} > P_{\text{пом кр с}}^{\text{стр}}$$

де $P_{\text{пом кр с}}^{\text{інт}}$ і $P_{\text{пом кр с}}^{\text{стр}}$ – відповідно ймовірність неправильного приймання при крайових спотворень і реєстрації інтегральним методом і методом стробування.

Якщо крайові спотворення δ описуються гаусовим законом

$$\varphi(\delta) = \frac{1}{\sqrt{2\pi}\delta} e^{-\frac{(\delta-a)^2}{2\sigma^2}},$$

де a – математичне очікування спотворення; σ^2 – дисперсія δ , то ймовірність помилки при стробуванні

$$P_{\text{пом кр}}^{(\text{стр})} = 0,75 - 0,5\Phi(t) - 0,25[\Phi(t)]^2, \quad (1.31)$$

де

$$\Phi(t) = \frac{2}{\sqrt{2\pi}} \int_0^t e^{-x^2/2} dx, \quad t = \frac{\mu - a}{\sigma}. \quad (1.32)$$

В (1.32) μ – виправляюча здатність приймача; a – математичне очікування зсуву границь елемента; σ – середньоквадратичне відхилення.

При реєстрації інтегральним методом

$$P_{\text{пом кр}}^{(\text{інт})} = 0,75 - 0,5\Phi(t) - 0,25\left[\Phi\left(\frac{t}{\sqrt{2}}\right)\right]^2. \quad (1.33)$$

Розглянемо дію дроблень. Будемо вважати, що на одиничний елемент доводиться лише одне дроблення. Позначимо тривалість дроблення $t_{\text{др}}$. Очевидно, що всі дроблення можуть бути розділені на дві групи:

$$t_{\text{др}} \geq \frac{\tau_0}{2}, t_{\text{др}} < \frac{\tau_0}{2}.$$

Якщо $t_{\text{др}} < \frac{\tau_0}{2}$, то при інтегральному методі приймання буде прави-

льним, тому що спотворюється менш половини ІПС. Якщо $t_{\text{др}} > \frac{\tau_0}{2}$ й при

цьому спотворено більше половини ІПС, то інтегральний метод реєстрації дає неправильне приймання. Однак, оскільки спотворено більше половини одиничного елемента, то буде спотворена і його середина. Отже, приймання буде неправильним і при реєстрації методом стробування. Таким чином, при реєстрації методом стробування неправильне приймання можливе як

при $t_{\text{др}} < \frac{\tau_0}{2}$, так і при $t_{\text{др}} \geq \frac{\tau_0}{2}$ й тому

$$P_{\text{пом др}}^{\text{стр}} > P_{\text{пом др}}^{\text{інт}},$$

де $P_{\text{пом др}}^{\text{стр}} > P_{\text{пом др}}^{\text{інт}}$ – відповідно ймовірність помилки при дії дроблень для випадків реєстрації стробуванням і інтегральним методом.

Ймовірність помилки буде тим більше, чим частіше з'являються дроблення, а також чим більше середня тривалість дроблення й дисперсія тривалості дроблення.

При спільній дії крайових спотворень і дроблень ймовірність помилки приблизно може бути визначена по формулі:

$$P_{\text{пом}} = P_{\text{пом ін}} + P_{\text{пом кр і}} - P_{\text{пом ін}} \cdot P_{\text{пом кр і}}.$$

На інтервалі аналізу визначається число помилок, а ймовірність помилки (оцінка ймовірності помилки) визначається за формулою

$$\hat{P}_{\text{пом}} = n_{\text{пом}} / n_{\text{пер}}, \quad (1.34)$$

де $n_{\text{пом}}$ – число помилкове прийнятих елементів на інтервалі аналізу T ;

$n_{\text{пер}}$ – число елементів, переданих за час T . При цьому

$$P_{\text{пом}} = \lim_{n_{\text{пер}} \rightarrow \infty} \frac{n_{\text{пом}}}{n_{\text{пер}}} = \lim_{n_{\text{пер}} \rightarrow \infty} \frac{n_{\text{ош}}}{T \cdot B},$$

де B – швидкість модуляції сигналів.

Оцінка ймовірності помилки, одержувана з використанням (1.34) є незміщеною. Якщо виміри робити на декількох інтервалах тривалості T , то на кожному з них значення $\hat{P}_{\text{пом}}$ будуть відрізнятися одне від одного, тобто $\hat{P}_{\text{пом}}$ є випадковою величиною. Зі збільшенням часу аналізу T ці відмінності будуть зменшуватися, отже, буде зменшуватися й дисперсія.

1.4. Надійність передачі і фактори, що на неї впливають

Ймовірність правильної передачі символу залежить від того, як формується імпульс, призначений для передачі символу, як і якою апаратурою він приймається, які реальні завади і т.п.; однак можна встановити загальні закономірності, справедливі по відношенню до імпульсів будь-якого типу.

Для імпульсів заданої тривалості і середньої потужності при заданих властивостях і потужності завади можна встановити межу надійності передачі, яка не може бути перевищена при використанні імпульсів будь-якої форми. З аналізу конкретних використовуваних на практиці сигналів видно, що майже в усіх випадках реалізовувана надійність передачі близька до теоретичної межі. Розглядаючи загальні закономірності, встановлені теорією потенціальної завадостійкості, яку розробив В.О. Котельников, можна одержати ряд практично важливих висновків, не вдаючись у деталі конкретних систем зв'язку.

В теорії потенціальної завадостійкості доводяться такі положення. Якщо по каналу зв'язку протягом часу T був переданий один із двох сигнала-

лів $U_1(t)$ або $U_2(t)$, імовірності посилки яких однакові, і якщо був прийнятий сигнал $f(t)$, то максимальна імовірність правильного прийому буде в тому випадку, якщо вважати прийнятим сигналом $U_1(t)$ при умові

$$\int_0^T [U_1(t) - f(t)]^2 dt < \int_0^T [U_2(t) - f(t)]^2 dt. \quad (1.35)$$

Якщо нерівність має обернений знак, переданим вважається сигнал $U_2(t)$. Приймач, який так розрізняє переданий сигнал, називається ідеальним приймачем за В.О. Котельниковим.

Якщо посилки сигналів $U_1(t)$ або $U_2(t)$ рівноймовірні, то імовірність помилки в прийомі переданого сигналу

$$p = 0,5 - \Phi(z), \quad (1.36)$$

де

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_0^z e^{-\frac{x^2}{2}} dx; \quad (1.37)$$

$$z = \frac{1}{\sqrt{2}} \sigma_n \sqrt{[U_1(t) - U_2(t)]^2 dt}; \quad (1.38)$$

$\Phi(z)$ – функція Лапласа; σ_n – питомий шум в ефективних вольтах, віднесений до смуги в 1 Гц.

Якщо сигнали $U_1(t)$ і $U_2(t)$ відрізняються лише знаком:

$$U_1(t) = -U_2(t)$$

(це буває при різнополярних імпульсах або при фазовій маніпуляції зі змінною фази на кут π), то

$$z = \sqrt{\frac{2W_c \tau}{\sigma_n^2}} = \sqrt{\frac{2E}{\sigma_n^2}}, \quad (1.39)$$

де W_c – середня потужність сигналу; τ – тривалість сигналу; E – енергія сигналу.

Якщо другий сигнал передається паузою, так що $U_2(t) = 0$, то

$$z' = \sqrt{\frac{W_c \tau}{2\sigma_n^2}} = \sqrt{\frac{E}{2\sigma_n^2}} = \frac{1}{2} z.$$

Якщо, нарешті,

$$\int_0^T U_1(t)U_2(t)dt = 0,$$

що буває при передачі сигналів посилками різних частот, то

$$z'' = \sqrt{\frac{W_c \tau}{\sigma_n^2}} = \sqrt{\frac{E}{\sigma_n^2}} = \frac{1}{\sqrt{2}} z.$$

У загальному випадку, при інших формах сигналів $U_1(t)$ і $U_2(t)$, вираз для z_s запишуватимемо так:

$$z_s = \omega \sqrt{\frac{2E}{\sigma_n^2}},$$

де коефіцієнт ω враховує форму сигналу. Величина $z = \sqrt{\frac{2E}{\sigma_n^2}}$ характеризує відношення енергії сигналу до потужності шуму.

Позначаючи смугу пропускання приймального пристрою через f , знайдемо потужність завади у смузі пропускання

$$W_n = f \sigma_n^2.$$

Тому z також може бути виражене через відношення потужності сигналу до потужності завади:

$$z = \sqrt{\frac{2W_c \tau f}{\sigma_n^2 f}} = \sqrt{\frac{W_c}{W_n}} 2\tau f.$$

При великих значеннях z функція Лапласа може бути виражена наближено

$$\Phi(z) \approx 0,5 - \frac{1}{z\sqrt{2\pi}} e^{-\frac{z^2}{2}}. \quad (1.40)$$

Тому при малих значеннях імовірності помилки імовірність правильного прийому символу тривалістю τ

$$q = 1 - p = 1 - \frac{1}{\sqrt{2\pi}} \sqrt{\frac{2\sigma_n^2}{W_c \tau}} e^{-\frac{W_c \tau}{4\sigma_n^2}} \text{ при } U_2(t) = 0. \quad (1.41)$$

Так визначають надійність передачі символу при двобуквенному алфавіті. Якщо алфавіт каналу зв'язку містить m різних символів (m букв в алфавіті) однакової потужності, то імовірність неправильного прийому символу виражається складнішою залежністю:

$$p_m = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-\frac{(y-\sqrt{2}z)^2}{2}} [0,5 + \Phi(y)]^{m-1} dy. \quad (1.42)$$

При малих імовірностях помилки (великі значення z)

$$p_m \approx (m-1)[0,5 - \Phi(z)]. \quad (1.43)$$

Цими виразами будемо користуватись і надалі.

Так зв'язується надійність правильного прийому сигналу з його середньою потужністю, тривалістю передачі і інтенсивністю шуму.

Імовірність неправильного прийому символу різко падає при зростанні z . Справді, порівнявши (1.36) і (1.40), знаходимо

$$p = \frac{1}{\sqrt{2\pi}} \cdot \frac{1}{z} e^{-\frac{z^2}{2}}. \quad (1.44)$$

Зв'язок між p і z видно з табл. 1.2

Таблиця 1.2 – Значення функції $\psi(x) = \frac{1}{\sqrt{2\pi x}} e^{-\frac{x^2}{2}}$

x	$\psi(x)$	x	$\psi(x)$	x	$\psi(x)$
1,0	-0,242	2,1	-0,0209	3,1	-0,00105
1,1	-0,198	2,2	-0,0161	3,2	-0,00075
1,2	-0,162	2,3	-0,0123	3,3	-0,00052
1,3	-0,132	2,4	-0,00934	3,4	-0,00035
1,4	-0,107	2,5	-0,00700	3,5	-0,00025
1,5	-0,0865	2,6	-0,00523	3,6	-0,00017
1,6	-0,0693	2,7	-0,00385	3,7	-0,00011
1,7	-0,0554	2,8	-0,00282	3,8	-0,00008
1,8	-0,0439	2,9	-0,00206	3,9	-0,00005
1,9	-0,0345	3,0	-0,0015	4,0	-0,00002
2,0	-0,0270				

Тому відповідним вибором параметрів, які визначають z , можна впливати на імовірність неправильної передачі. Зокрема, завжди можна підвищити надійність передачі символу, підвищуючи його тривалість τ . Однак це не повинно бути простим «затягуванням» сигналу. Відповідно до змісту виразу (1.35) приймальний пристрій повинен мати ланку, яка інтегрує суму сигналу і завади. Тільки при цій умові із збільшенням тривалості сигналу збільшується відношення сигналу до завади, оскільки інтеграл від знакозмінної завади буде флюктувати біля нуля, а інтеграл від корисного сигналу безперервно наростатиме. Найпростішою інтегруючою ланкою може бути фільтр (контур) RC . На рис. 1.30 показаний прийом символу – імпульсу постійного струму електромагнітним реле без інтегруючої ланки (а) і з нею (б). У першому випадку реле може помилково спрацювати від завади, або сигнал може бути заглушений завадою. У другому випадку тривалість сигналу повинна бути більшою, але і завада буде значно послаблена. Якщо перед реле ввімкнутий фільтр RC і тривалість сигналу відповідно збільшена, то вплив пере шкоди буде значно послаблений. (Природно, що подовження сигналу в першому випадку не дало б позитивного ефекту).

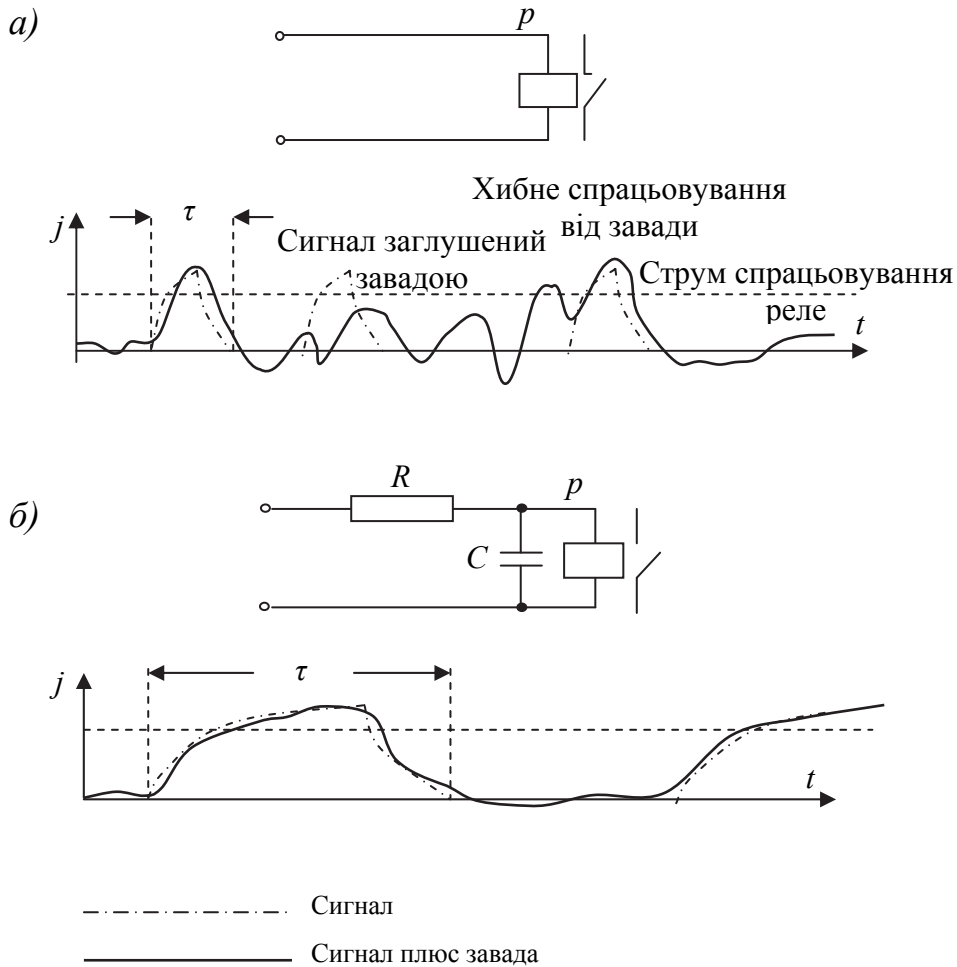


Рисунок 1.30 – Вплив подовження сигналу на імовірність помилки при прийманні

Імовірність правильної передачі повідомлення, що складається з n символів, дорівнює імовірності складної події, яка полягає в тому, що всі n символів повідомлення будуть передані правильно. При рівності імовірностей правильної передачі кожного з m символів використовуваного алфавіту надійність передачі повідомлення Q не залежить від конкретного складу символів, з яких воно складається, і є функцією тільки довжини повідомлення (n) і імовірності помилки в передачі одного символу (p). Згідно з теоремою про множення імовірностей можна записати

$$Q = (1 - p)^n = q^n \quad (1.45)$$

для всіх $N = m^n$ можливих повідомлень довжини n . З цього виразу виходить, що надійність передачі повідомлення різко падає із збільшенням кількості символів у повідомленні. Так, якщо надійність передачі одного символу $q = 0,999$, то вже при $n = 10$ надійність передачі повідомлення дорівнює всього лише $q \approx 0,99$.

У загальному випадку імовірності помилок при передаванні символів алфавіту нерівні між собою. При цьому й імовірності правильної передачі

різних повідомлень однієї і тієї ж довжини неоднакові. Природно, вони залежать від складу символів, з яких складається повідомлення.

Позначимо імовірності помилок при передачі символів алфавіту $A_1, A_2, \dots, A_i, \dots, A_m$ через $p_1, p_2, \dots, p_i, \dots, p_m$ відповідно. Нехай у дане повідомлення n_1 раз входить символ A_1 ; n_2 раз – символ A_2 ; ... n_m раз – символ A_m . Числа n_1, n_2, \dots, n_m зв'язані між собою очевидним співвідношенням

$$\sum_{i=1}^m n_i = n.$$

В цьому випадку надійність передачі повідомлення

$$Q = (1 - p_1)^{n_1} (1 - p_2)^{n_2} \dots (1 - p_i)^{n_i} \dots (1 - p_m)^{n_m},$$

або

$$Q = \prod_{i=1}^m (1 - p_i)^{n_i}.$$

Повідомлення, що складаються з одних і тих же символів і відрізняються лише порядком їх розміщення, мають однакову надійність.

При великій довжині повідомлень ($n \rightarrow \infty$) статистичні структури повідомлень вирівнюються, кількість символів кожного типу (n_i) в таких повідомленнях близька до найбільш імовірної кількості, яка визначається імовірністю появи даного символу p_i . Надійність передачі повідомлення прямує до виразу

$$Q_{n \rightarrow \infty} = \prod_{i=1}^m (1 - p_i)^{np_i}.$$

За певних умов імовірність правильного прийому сигналу можна підвищити повторним (багаторазовим) передаванням його. При цьому швидкість передачі інформації знижується. При методі повторення використовують ту ж саму приймально-передавальну апаратуру, що й при одноразовій передачі інформації. Цим з якісного боку характеризується метод підвищення надійності передачі повторенням. Перейдемо до визначення кількісних характеристик.

Нехай передаються дві букви a і b (двійковий код). Посилки букв рівноімовірні і безперервно ідуть одна за одною, тобто завжди передається і приймається або буква a , або b ⁵. Позначимо імовірність правильного прийому букви a через q_a , а імовірність неправильного прийому букви a через p_a (тобто імовірність того, що замість a буде прийнято b), а букви b відповідно через q_b і p_b . Далі прийнемо

$$q_a = q_b = q; p_a = p_b = p.$$

⁵ Буквою b може бути пауза, тобто відсутність сигналу

Передамо букву a три рази. Умовимось, що буква a буде вважатися переданою в тому випадку, коли із трьох посилок вона була прийнята три або два рази. В противному разі вважатимемо, що передавалась буква b . При цій умові імовірність правильного прийому букви a

$$q^3 + 3q^2 p,$$

а неправильного –

$$p^3 + 3p^2 q.$$

Нехай $p = 0,1$ і $q = 0,9$, тоді

$$q^3 + 3q^2 p = 0,9^3 + 3 \cdot 0,9^2 \cdot 0,1 = 0,972; \quad p^3 + 3p^2 q = 0,028.$$

З цього прикладу видно, що в даному разі при триразовому передаванні надійність передачі підвищилась з $0,9$, до $0,972$.

У загальному випадку триразової повторної передачі надійність підвищується тільки при умові

$$q^3 + 3q^2 p > q,$$

тобто $q > p$, тобто $q > 0,5$.

При кратності повторення $2k + 1$ імовірність правильного прийому знаходять із таких міркувань. Знову вважатимемо правильно прийнятим той символ (із двох можливих a і b), який при $(2k + 1)$ -кратній передачі одного із символів прийнятий більшу кількість раз, ніж другий, тобто не менше $(k + 1)$ раз. Одночасне приймання двох символів вважаємо виключеним. Тоді правильний прийом буде в тих випадках, коли посланий символ буде прийнятий $2k + 1$ раз, $2k$ раз, $2k - 1$ раз і так далі до $k + 1$. Імовірність цих випадків дорівнює, відповідно,

$$q^{2k+1}; C_{2k+1}^1 q^{2k} p^1; C_{2k+1}^2 q^{2k-1} p^2; \dots, C_{2k+1}^{k+1} q^{k+1} p^k$$

і тому імовірність правильного прийому

$$q_{2k+1} = \sum_{j=0}^k C_{2k+1}^j q^{2k+1-j} p^j, \quad (1.46)$$

а імовірність неправильного прийому

$$p_{2k+1} = 1 - q_{2k+1} = \sum_{j=k+1}^{2k+1} C_{2k+1}^j q^{2k+1-j} p^j. \quad (1.47)$$

При великій кількості k імовірність правильного прийому може бути знайдена за граничною інтегральною теоремою Муавра–Лапласа, яка формулюється так: якщо імовірність появи події a дорівнює p , а імовірність появи протилежної події b дорівнює $1 - p$, то імовірність того, що в n дослідах ($n \rightarrow \infty$) кількість μ появи події a лежатиме в межах $\mu_1 \dots \mu_2$

$$p\{\mu_1 < \mu < \mu_2\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{x_1}^{x_2} e^{-\frac{z^2}{2}} dz = \Phi(x_2) - \Phi(x_1), \quad (1.48)$$

$$\text{де } \begin{cases} x_1 = \frac{\mu_1 - np}{\sqrt{np(1-p)}}; \\ x_2 = \frac{\mu_2 - np}{\sqrt{np(1-p)}}. \end{cases}$$

Імовірність правильного прийому є імовірність того, що кількість випадків прийому букви b (при $2k+1$ раз переданій букві a) лежатиме в межах від 0 до k . Таким чином,

$$x_1 = \frac{0 - (2k+1)p}{\sqrt{(2k+1)p(1-p)}} = -\sqrt{\frac{p}{1-p}} \sqrt{2k+1};$$

$$x_2 = \frac{k - (2k+1)p}{\sqrt{(2k+1)p(1-p)}} \approx \frac{0,5 - p}{\sqrt{p(1-p)}} \sqrt{2k+1} = \frac{0,5\sqrt{2k+1}}{\sqrt{p(1-p)}} + x_1.$$

Оскільки $p < 0,5$, то $x_2 > 0$ і $x_1 < 0$.

Приклад 11. Визначимо імовірність правильного прийому при $2k+1=51$ і $p=0,4$; $q=0,6$. Знаходимо

$$x_1 = -\sqrt{\frac{0,4}{0,6}} \sqrt{51} = -5,83; \quad x_2 = \frac{0,5 - 0,4}{\sqrt{0,4 \cdot 0,6}} \sqrt{51} = +1,46.$$

Імовірність правильного прийому $\Phi(x_2) = \Phi(1,46) - \Phi(-5,83) = \Phi(1,46) + \Phi(5,83) = 0,428 + 0,5 = 0,928$.

Із прикладу видно, що методом повторень можна істотно підвищити надійність навіть при дуже низькій надійності прийому символу.

Для простоти обчислень іноді доцільно вираховувати не імовірність правильного прийому, а імовірність неправильного прийому, тобто імовірність того, що кількість випадків приймання букви b лежатиме в межах від $k+1$ до $2k+1$. При цьому

$$x_1 = \frac{0,5 - p}{\sqrt{p(1-p)}} \sqrt{2k+1};$$

$$x_2 = \frac{1 - p}{\sqrt{p(1-p)}} \sqrt{2k+1} = \sqrt{\frac{1-p}{p}} \sqrt{2k+1}.$$

Звичайно x_2 велике, і можна вважати, що $\Phi(x_2) = 0,5$. Тоді

$$p = \frac{1}{\sqrt{2\pi}} \int_{x_1}^{x_2} e^{-\frac{z^2}{2}} dz = \frac{1}{\sqrt{2\pi}} \int_{x_1}^0 e^{-\frac{z^2}{2}} dz + \frac{1}{\sqrt{2\pi}} \int_0^{x_2} e^{-\frac{z^2}{2}} dz =$$

$$= 0,5 - \frac{1}{\sqrt{2\pi}} \int_0^{x_1} e^{-\frac{z^2}{2}} dz = 0,5 - \Phi(x_1);$$

$$q = 0,5 + \Phi(x_1).$$

Розглянемо тепер випадок повторної передачі однієї з букв при m буквах в алфавіті. Розширимо постановку задачі, припускаючи можливість

одночасного приймання (внаслідок завад) кількох букв. Така можливість була і при двобуквенному алфавіті, але при двобуквенному алфавіті її легко виключити апаратними методами, а іноді вона і не виникає. Наприклад, якщо спрацювання реле означає прийом однієї букви (1), неспрацювання – другої (0). В цьому випадку одночасне приймання 0 і 1 виключене.

При багатобуквенному алфавіті одночасне приймання кількох символів важко усунути. Цим розглядуваний випадок якісно відрізняється від попереднього – виникає можливість невизначеного приймання (захисна відмова).

Позначимо імовірність прийому i -го символу i -м селектором через q , а імовірність прийому i -го символу j -м селектором ($j \neq i$) – через p (імовірності неправильного прийому цих символів, як і імовірності їх правильного прийому, вважаємо рівними). Передамо i -й символ k раз. Нехай при цьому приймальні селектори спрацювали таку кількість раз:

Номер селектора	1	2	3	...	i	...	m
Кратність приймання	M_1	M_2	M_3	...	M_i	...	M_m

Умовимось, що символ A_i вважається прийнятим, якщо $M_i > M_j$ для всіх $j \neq i$.

Імовірність правильного прийому переданого символу в такій системі q_{Σ} не дорівнюватиме імовірності правильного прийому символу його селектором q .

Припустимо, що спрацювання будь-якого селектора в будь-який такт передачі (із k тактів повторення) не залежить від спрацювання інших селекторів. Відшукаємо імовірність правильного прийому за цих умов.

При k -кратному передаванні символу A_i i -й селектор може спрацювати або один раз, або два, або три рази і так далі до k раз включно. При цьому правильний прийом буде в тому випадку, коли жоден із $m - 1$ решти селекторів не спрацював відповідно жодного разу, не більш ніж один раз, не більш ніж два рази і так далі і не більше ніж $k - 1$ разів.

Імовірність того, що i -й селектор спрацює точно n раз, дорівнює

$$C_k^n (1 - q)^{k-n} q^n.$$

Імовірність того, що j -й селектор спрацює не більше $n - 1$ разів, дорівнює

$$\sum_{j=0}^{n-1} C_k^j (1 - p)^{k-j} p^j.$$

Для правильного прийому символу A_i , прийнятого n разів із k передач, необхідно, щоб жоден із $m - 1$ решти приймачів не спрацював більше $n - 1$ разів. Тому імовірність правильного прийому символу A_i , якщо селектор i -й правильно прийняв його n разів із k передач, буде

$$C_k^n (1-q)^{k-n} q^n \left[\sum_{j=0}^{n-1} C_k^j (1-p)^{k-j} p^j \right]^{m-1}.$$

А повна імовірність правильного прийому i -го символу при серії в k передач

$$q_\Sigma = \sum_{n=1}^{n=k} C_k^n (1-2)^{k-n} q^n \left[\sum_{j=0}^{n-1} C_k^j (1-p)^{k-j} p^j \right]^{m-1}.$$

При великих значеннях k суми можуть бути замінені інтегралами. Тоді

$$q_\Sigma = \int_0^k V_+(n) \left[\int_0^{n-1} V_-(y) dy \right]^{m-1} dn, \quad (1.49)$$

де $V_+(n)$ – густина розподілу ймовірностей кількості приймання i -го символу i -м селектором; $V_-(y)$ – густина розподілу ймовірностей кількості приймання i -го символу j -м селектором ($j \neq i$).

У відповідності з інтегральною теоремою Муавра-Лапласа інтеграл у квадратних дужках можна записати так:

$$\int_0^{n-1} V_-(y) dy = 0,5 + \Phi \left(\frac{n-1-kp}{\sqrt{kp(1-p)}} \right). \quad (1.50)$$

Функція $V_+(n)$ записується за Муавром-Лапласом так:

$$V_+(n) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}, \quad (1.51)$$

де

$$x = \frac{n-kq}{\sqrt{kq(1-q)}}.$$

Підставивши вирази (1.50) і (1.51) в (1.49), одержимо

$$q_\Sigma = \frac{1}{\sqrt{2\pi}} \int_{x_1}^{x_2} e^{-\frac{x^2}{2}} \left[0,5 + \Phi \left(\frac{n-1-kp}{\sqrt{kp(1-p)}} \right) \right]^{m-1} dx; \quad (1.52)$$

$$p_\Sigma = 1 - \frac{1}{\sqrt{2\pi}} \int_{x_1}^{x_2} e^{-\frac{x^2}{2}} \left[0,5 + \Phi \left(\frac{n-1-kp}{\sqrt{kp(1-p)}} \right) \right]^{m-1} dx.$$

Цей вираз має таку ж саму структуру, як вираз (1.42) для надійності прийому символу m -буквеного алфавіту ідеальним приймачем (за Котельниковим).

Для визначення теоретичних можливостей підвищення надійності передачі методом повторення дослідимо вираз (1.52), взявши $k \rightarrow \infty$. Тоді, виразивши n через x :

$$n = x\sqrt{kp(1-p)} + kp$$

і підставивши його у вираз (1.52), маємо

$$q_{\Sigma} = \frac{1}{\sqrt{2\pi}} \int_{x_1=-\infty}^{x_2=+\infty} e^{-\frac{x^2}{2}} \left[0,5 + \Phi_{k \rightarrow \infty} \left(\frac{x\sqrt{kp(p-1)} + k(q-p)}{\sqrt{kp(p-1)}} \right) \right]^{m-1} dx.$$

При умові $q > p$ вираз у круглих дужках завжди додатній і тому

$$\Phi_{k \rightarrow \infty} \left(\frac{x\sqrt{kp(p-1)} + k(q-p)}{\sqrt{kp(p-1)}} \right) \rightarrow 0,5,$$

а сума в квадратних дужках прямує до 1. При цьому

$$q_{\Sigma} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-\frac{x^2}{2}} \cdot 1 dx = 1.$$

Таким чином, методом повторень в принципі можна одержати яку завгодно високу надійність передачі символів, але при цьому знижуватиметься швидкість передачі.

Для з'ясування співвідношень, справедливих при повторному передаванні символів m -буквеного алфавіту, розглянемо приклад.

Приклад 12. Нехай в алфавіті п'ять символів ($m = 5$) при

$$q = 0,6 \text{ і } p = 0,1; \quad q + p \neq 1(!)$$

Тоді імовірність правильного прийому першого символу при одноразовій передачі ($k = 1$)

$$q_{\Sigma 1} = 0,6(1 - 0,1)^4 = 0,6 \cdot 0,9^4 = 0,394,$$

оскільки при одноразовій посилці і правильному прийомі першого символу решта чотири символи не повинні бути прийняті.

Таким чином, імовірність правильного спрацювання селектора ($q = 0,6$) і імовірність правильного прийому символу ($q = 0,394$) не збігаються.

Імовірність неправильного прийому одного з чотирьох символів

$$p_{\Sigma 1} = 0,1 \cdot 0,4 \cdot 0,9^3 = 0,0282.$$

Взагалі імовірність неправильного прийому будь-якого з чотирьох символів (ці події несумісні)

$$(m-1)p_i = 4 \cdot 0,0282 = 0,112.$$

Сума ймовірностей правильного і неправильного прийомів тепер не дорівнює одиниці:

$$0,394 + 0,112 = 0,506 \neq 1.$$

Це пояснюється тим, що є ще одна категорія – захисні відмови, коли однакою кількістю раз прийняті кілька символів. В цьому випадку жодному з них не можна віддати перевагу. Це, безумовно, неправильний прийом, але помилка виявлена і тому помилкова команда не буде виконана. Імовірність захисної відмови

$$S = 1 - 0,506 = 0,494.$$

У розглянутому випадку повторення передачі інформації доцільне і при імовірності правильного спрацювання одного селектора, меншій від 0,5, але не меншій – $\frac{1}{m}$. Для цього ж прикладу імовірність правильного прийому при дворазовому передаванні становитиме $q_{\Sigma 2} = 0,6$.

Тепер розглянемо докладно розрахунок імовірності при триразовому передаванні для цього ж прикладу.

Імовірність того, що переданий символ буде прийнятий його селектором:

$$\text{три рази з трьох} \quad 0,6^3 = 0,218;$$

$$\text{два рази з трьох} \quad 3 \cdot 0,6^2 \cdot 0,4 = 0,432;$$

$$\text{один раз із трьох} \quad 3 \cdot 0,6 \cdot 0,4^2 = 0,288.$$

Імовірність того, що при цьому якийсь «чужий» селектор не спрацював:

$$\text{зовсім} \quad (1 - 0,1)^3 = 0,9^3 = 0,728;$$

$$\text{один раз} \quad 3 \cdot 0,9^2 \cdot 0,1 = 0,243;$$

$$\text{два рази} \quad 3 \cdot 0,9 \cdot 0,1 = 0,027.$$

Імовірність правильного прийому при триразовому передаванні

$$q_{\Sigma 3} = 0,218(0,728 + 0,243 + 0,027)^4 + 0,432(0,728 + 0,243)^4 + 0,288 \cdot 0,728 = \\ = 0,218 \cdot 0,999^4 + 0,432 \cdot 0,971^4 + 0,288 \cdot 0,728^4 = 0,217 + 0,385 + 0,081 = 0,683.$$

Підрахуємо імовірність неправильного (помилкового) прийому при $k = 3$. Імовірність того, що j -й селектор спрацював помилково у всі три рази,

$$0,1^3 = 0,001.$$

Імовірність того, що j -й селектор спрацював помилково два рази,

$$3 \cdot 1^2 \cdot 0,9 = 0,027.$$

Імовірність того, що j -й селектор спрацював помилково один раз,

$$3 \cdot 0,1 \cdot 0,9^2 = 0,243.$$

Імовірність неправильного прийому за рахунок помилкової роботи j -го селектора

$$0,001(0,728 + 0,243 + 0,027)^3 (0,4^3 + 0,288 + 0,432) + \\ + 0,027(0,728 + 0,243)^3 (0,4^3 + 0,288) + 0,243 \cdot 0,728^3 \cdot 0,4^3 = \\ = 0,001 \cdot 0,999^3 \cdot 0,782 + 0,027 \cdot 0,971^3 \cdot 0,352 + 0,243 \cdot 0,728^3 \cdot 0,064 = 0,0155.$$

А оскільки неправильно можуть бути прийняті чотири символи, і ці події несумісні, то імовірність неправильного приймання взагалі

$$p_{\Sigma 3} = 0,0155 \cdot 4 = 0,062.$$

Імовірність захисної відмови (виявлення помилки)

$$S_{\Sigma 3} = 1 - 0,683 - 0,062 = 0,255.$$

В даному випадку інформація передається не по одному i -му каналу, а по всіх m каналах, і вся інформація про стан усіх селекторів бере участь у визначенні передаваного сигналу.

1.5. Моделі потоку помилок

Випадковий процес виникнення помилок в дискретному каналі буде повністю описаний, якщо задані: вхідний (A) і вихідний (\hat{A}) алфавіти символів, а також сукупність перехідних ймовірностей виду $p(\hat{a}/a)$, де $a = (a_1, a_2, a_3, \dots, a_i, \dots)$ – довільна послідовність символів вхідного алфавіту і $a_i \in A$ – символ на вході каналу в i -й момент часу $\hat{a} = (\hat{a}_1, \hat{a}_2, \hat{a}_3, \dots, a_i, \dots)$ – відповідна a послідовність символів із вихідного алфавіту, а $\hat{a}_i \in \hat{A}$ – символ на виході каналу в i -й момент; $p(\hat{a}/a)$ – умовна ймовірність прийому послідовності \hat{a} за умови, що передана послідовність a .

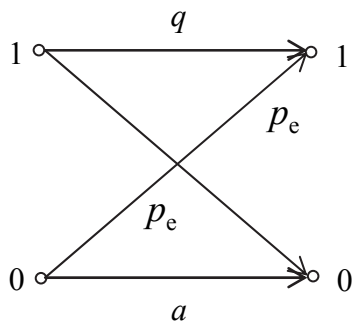


Рисунок 1.31. Діаграма переходів у бінарному каналі

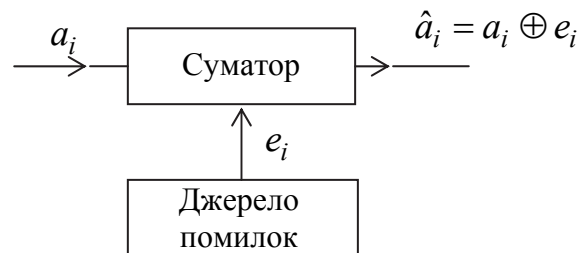


Рисунок 1.32. Еквівалентна схема дискретного симетричного каналу

Число заданих перехідних ймовірностей зі збільшенням довжини вхідних та вихідних послідовностей зростає. Так, якщо використовується двійковий код і вихідний алфавіт дорівнює вхідному, то при послідовності довжини n загальне число заданих перехідних ймовірностей буде дорівнювати 2^{2n} . Очевидно, що вже при $n = 20$ подання перехідних ймовірностей у виді таблиці хоча і можливо, але навряд чи доцільно.

Спотворення кодограми можуть мати характер r -кратних незалежних помилок і пакетів помилок. Під r -кратною помилкою розуміється спотворення в кодограмі r символів. Так, якщо передавалась кодограма 101100, а прийняті послідовності імпульсів 111100 та 100110, то відбулись відповідно одинична ($r = 1$) і двократна ($r = 2$) помилки.

Особливим видом двократних помилок є помилки зміщення, коли в кодограмі одночасно трансформуються символ 0 в 1 і символ 1 в 0. В результаті число символів 0 і 1 в кодограмі не змінюється, і коди, що використовують зміни цього числа для виявлення помилок, не фіксують спотворення такого типу.

Під пакетом помилок розуміється послідовність кодових слів, що містять кілька помилок, і розміщена між першим та останнім спотвореними символами цієї послідовності, при цьому відстань між двома сусідніми пакетами помилок повинна бути не менше визначеного числа неспотворених символів (розділювального інтервалу l_p). Очевидно, що в середині пакета помилок можуть міститися неспотворені символи. Загальна кількість символів в пакеті характеризує його довжину l_n , а число спотворених символів – його вагу w_n . Якщо передавалася, наприклад, кодограма 1110001110, то $l_n = 3$ і $w_n = 2$; при прийомі послідовностей 11110011000 або 1110011000 відповідно маємо $l_n = 8$, $w_n = 2$ та $l_n = 8$, $w_n = 5$.

Наведене вище поняття пакета помилок потребує кількісного уточнення, тому що незрозуміло, які спотворені символи слід віднести до одного й того ж пакета, а які символи до різних пакетів. Розглянемо послідовність символів довжиною n , що містить r помилок і розміщену між першим та останнім спотвореними символами. Якщо помилки всередині пакета незалежні і з'являються з ймовірністю p_{e_n} , то їхнє число підкоряється біноміальному закону розподілу. Частість появи помилок $\xi_0 = \frac{r}{n}$ може бути визначена експериментально. Задамося довірчою ймовірністю β_0 і будемо шукати верхню межу ймовірності $p_{e_n} = p_{e_b}$, за якої мало ймовірно одержати частість помилок $\xi < \xi_0$. Ця межа шукається із рівняння

$$\sum_{i=0}^r C_n^i p_{e_b}^i (1 - p_{e_b})^{n-i} = 1 - \beta_0. \quad (1.53)$$

Нижня межа ймовірності $p_{e_n} = p_{e_n}$, при якій мало ймовірно, що $\xi > \xi_0$, знаходиться із рівняння

$$\sum_{i=r}^n C_n^i p_{e_n}^i (1 - p_{e_n})^{n-i} = 1 - \beta_0. \quad (1.54)$$

Якщо $r = 0$, то рівняння (1.53) набуде вигляду

$$(1 - p_{e_b})^n = 1 - \beta_0.$$

Найбільше значення $n = n_m$, яке задовольняє цьому рівнянню, характеризує максимальну відстань між спотвореними символами, які належать одному пакету помилок, тобто визначає довжину пакета l_n :

$$n_m = l_{\Pi} = \frac{\lg(1 - \beta_0)}{\lg(1 - p_{eB})}.$$

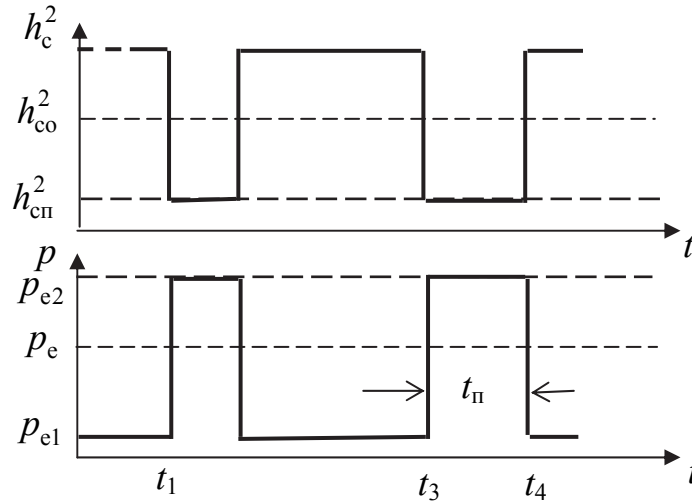


Рисунок 1.33 – Модель каналу з двома станами

Якщо ж інтервал між спотвореними символами $l_p \geq l_{\Pi} + 1$, то вони відносяться до суміжних пакетів помилок. Наприклад, при $p_{eB} = 0,4$ і $\beta_0 = 0,9$, $l_{\Pi} = 5$ символів, а інтервал $l_p = 6$ символів; при $p_{eB} = 0,4$ і $\beta_0 = 0,999$ $l_{\Pi} = 14$ і $l_p = 15$ символів.

При кореляції помилок з коефіцієнтом ρ_0 ймовірність спотворення символу всередині пакета

$$p'_{e\Pi} = 2p_{e\Pi}(1 - \rho_0),$$

а довжина пакета

$$l_{\Pi} = \frac{\lg(1 - \beta_0)}{\lg \rho_0}. \quad (1.55)$$

Природа виникнення пакетів помилок полягає в наступному. Замирання сигналів в каналі призводить до залежності $h_c^2 = f(t)$, де h_c^2 – перевищення сигналу. Через те що ймовірність спотворення символу $p_e = \varphi(h_c^2)$, де нелінійний функціональний оператор φ визначається способами маніпуляції, передавання й приймання сигналів, то одержується нелінійна залежність $p_e = \varphi(t)$.

В таблиці 1.3 і 1.4 наведені статистичні параметри завод в каналі МТМ (переривів сигналу) і ймовірності помилкового приймання кодового слова при зміні числа елементів n .

Нехай функція $h_c^2(t)$ має прямокутну форму (рис.1.33).

Таблиця 1.3 – Статистичні параметри завад в каналі МТМ

$\Delta F, \text{Гц}$	$\gamma, 1/\text{год}$	$L_0, \text{мс}$	\bar{l}	$D_0, (\text{мс})^2$	$\sigma_0, \text{мс}$
80	143	25000	14,67	56,18	7,43
140	160	22727	8,41	6,15	2,48
320	212	17020	4,1	2,01	1,42
700	795	4100	1,775	1,562	1,235
1700	1224	2527	0,676	0,12	0,346

Такий випадок на практиці може мати місце при інтенсивних імпульсних завадах, стрибках напруги в провідних каналах, короточасних перервах зв'язку та ін. В інтервалах часу (t_1, t_2) і (t_3, t_4) , які відповідають хорошему стану каналу, перевищення сигналу велике і ймовірність помилки буде мінімальною ($p_e = p_{e1}$). В інтервалах (t_2, t_3) і (t_4, t_5) перевищення сигналу мале, стан каналу поганий і ймовірність помилки зростає ($p_e = p_{e2}$). Тому всередині цих інтервалів символи будуть спотворюватися частіше, тобто відбудеться начебто групування помилок і з'являться пакети помилок. Очевидно, що середня ймовірність спотворення символів ($p_{e1} < p_e < p_{e2}$). Якщо стрибкоподібні зміни коефіцієнта передачі каналу настають незалежно один від одного, то пакети помилок будуть некорельованими між собою, в протилежному разі пакети помилок групуються в ланцюжки пакетів помилок.

Таблиця 1.4 – Вплив довжини конструкції на якість передавання

РЦК				ТСК			
				$s = 7$			
				$i = 3$			
n	$N_{\text{пер}}$	$N_{\text{пом}}$	P_n	n	$N_{\text{пер}}$	$N_{\text{пом}}$	P_n
20	100000	700	$7 \cdot 10^{-3}$	17	100000	11,50	$11,5 \cdot 10^{-3}$
40	100000	1500	$15 \cdot 10^{-3}$	$n=33$	100000	1620	$16,2 \cdot 10^{-3}$
10	100000	720	$7,2 \cdot 10^{-3}$	$n=9$	100000	104	$7,1 \cdot 10^{-4}$

За тривалих розривів каналу зв'язку пакет (ланцюжок) помилок може охопити кілька сусідніх кодограм. У цьому випадку іноді говорять, що відбувся викид помилок. Число спотворених кодограм характеризує довжину викиду помилок l_v .

Для повної ймовірності оцінки потоку помилок необхідно знати середню ймовірність спотворення кодового символу p_e , ймовірність спотворення кодограми P_{e_k} , а також функції розподілу помилок в спотворених

кодограмах $F(n_c)$, інтервалів між помилками $F(\tau_c)$ та інтервалів між помилками відносно попередніх інтервалів $F_t(\tau_c)$.

Характер функції розподілу $F(n_c)$ залежить від типу лінії зв'язку. Так кабельні канали характеризуються в основному кодограмами з малим значенням n_c (крива 1 на рис. 1.34, а); для провідних ліній функція $F(n_c)$ більш рівномірна, причому відсоток кодограм з помилками більш високої кратності зростає.

Функція $F(n_c)$ характеризує кореляцію помилок (на рис.1.34, б інтервал між помилками виражений в двійкових символах).

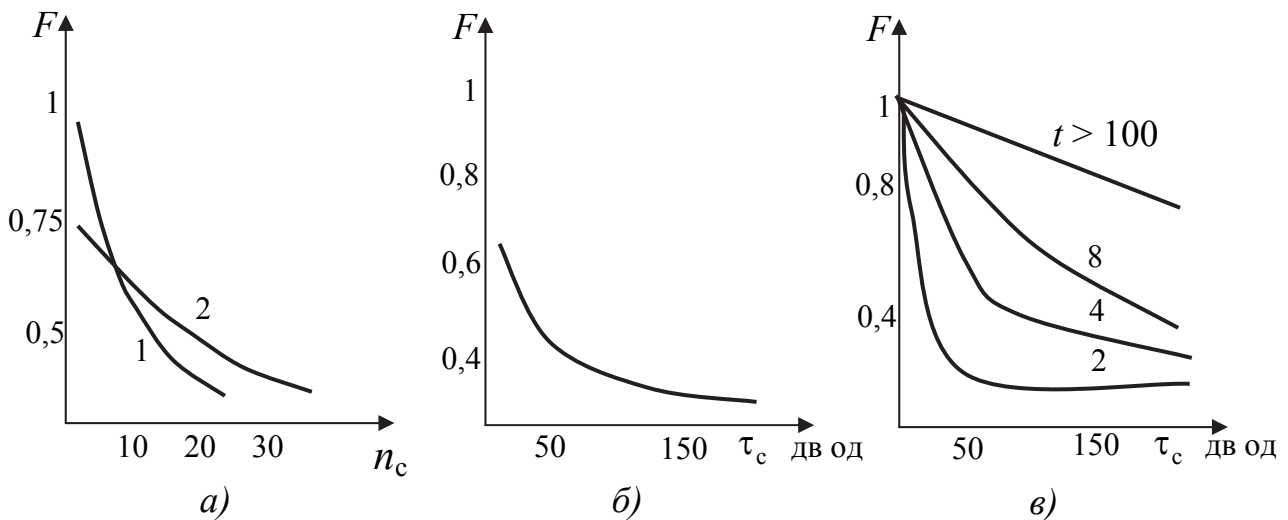


Рисунок 1.34 – Статистичні характеристики кабельних каналів

Функція $F(n_c)$ більш тонко відображає статистичну структуру потоку помилок, оскільки враховує вплив попередніх моментів часу (на рис. 1.34, в за віссю абсцис відкладені поточні часові інтервали між помилками в двійкових символах, а біля кривих – попередні часові інтервали).

В основі моделі потоку помилок у двійковому симетричному каналі (ДСК) лежать наступні припущення: канал симетричний; спотворення символів відбувається незалежно один від одного; число помилок r в кодовому слові значності n описується біноміальним законом розподілу

$$p_n(r) = C_n^r p_e^r (1 - p_e)^{n-r}.$$

Найбільш імовірним є одиничні помилки ($r = 1$); ймовірність появи помилок великої кратності нижче ймовірності появи помилок малої кратності.

У реальних каналах зв'язку значущість кодограми n велика, а середня ймовірність спотворення символу p_e мала. При цьому число помилок добре апроксимується розподілом помилок Пуассона

$$p_n(r) = \frac{(np_e)^r}{r!} e^{-np_e}.$$

Із цієї формули виходить, що при використанні моделі ДСК досить знайти тільки ймовірність p_e , що суттєво спрощує розрахунок. Але гіпотеза про незалежність помилок у більшості випадків не підтверджується на практиці, і результати розрахунків, основані на моделі ДСК, можуть слугувати лише наближеною оцінкою вірності зв'язку.

Модель потоку помилок в каналі з двома станами, запропонована Гільбертом, описує потік помилок у каналі простим однорідним ланцюгом Маркова з двома станами. В одному стані – хорошому – перевищення сигналу h_c^2 більше порогового значення $h_{cп}^2$ (рис.1.33) і ймовірність спотворення символів p_{e1} значно менше середнього значення p_e . В іншому стані каналу – поганому – в межах інтервалів (t_1, t_2) і (t_3, t_4) величина $h_c^2 < h_{cп}^2$, і ймовірність спотворення символів $p_{e2} \gg p_e$. Моменти часу t_1 та t_3 відповідають появі пакетів помилок довжиною $l_{п}$ символів, при цьому помилки всередині пакетів і самі пакети передбачаються некорельованими.

Для кабельних каналів можна прийняти $p_{e2} \approx 0,3...0,4$ і $p_{п} \approx 3 \cdot 10^{-5} ... 3 \cdot 10^{-6}$.

Розглянута модель задовільно відображає властивості реальних каналів, порівняно просто і в той самий час дозволяє застосовувати математичний апарат теорії імпульсних потоків для аналізу групування помилок при рознесеному прийомі.

В табл. 1.5 наведені основні параметри реальних каналів зв'язку при передаванні дискретних повідомлень.

Статистична ймовірність появи спотворених комбінацій визначається як відношення кількості спотворених комбінацій $N_{пом}(n)$ до загальної кількості комбінацій $N_3(n)$:

$$P(\geq 1, n) = \frac{N_{пом}(n)}{N_3(n)}$$

Ймовірність $P(\geq 1, n)$ є неспадною функцією, при $n \rightarrow \infty$ $P(\geq 1, n) \rightarrow 1$ за будь-якого значення $p > 0$. Міра зростання $P(\geq 1, n)$ зі збільшенням n залежить від характеру розподілу помилок. Для каналу з незалежним розподілом помилок $P(\geq 1, n) = 1 - (1 - p)^n$, а при $np \ll 1$ $P(\geq 1, n) \approx np$. У цьому випадку ймовірність появи спотворених комбінацій лінійно залежить від кількості елементів у комбінаціях при фіксованому значенні p .

На рис. 1.35 наведена залежність $P(\geq 1, n)$ від n для трьох виділених кабельних телефонних каналів, одного комутованого телефонного каналу і одного каналу тонального телеграфування. Масштаб на всіх рисунках по обох осях є логарифмічним. Точками нанесено експериментальні дані, які

достатньо добре апроксимуються прямими лініями при кількості елементів у комбінаціях від 1 до 500

Таблиця 1.5 – Характеристики реальних каналів

№ каналу	Тип каналу	Вид модуляції	Швидкість модуляції, Бод	Кількість переприймачів по НЧ або потужність перелавача	Середня частота помилок p	Показник групування α	Ступінь середньої асиметрії, ρ/p
1	Кабельний телефонний виділений	ВФМ	1200	1	$2,82 \cdot 10^{-4}$	0,770	-0,296
2	Так само	ВФМ	1200	5	$1,29 \cdot 10^{-4}$	0,510	-1
3	Так само	ВФМ	1200	5	$5,20 \cdot 10^{-4}$	0,710	+0,114
4	Кабельний телефонний комутований (МАТС)	ЧМ	1200	Дві МАТС	$2,00 \cdot 10^{-3}$	0,340	+0,170
5	Радіорелейний телефонний	ВФМ	1200	3	$2,66 \cdot 10^{-4}$	0,606	-0,520
6	Так само	ЧМ	1200	3	$7,03 \cdot 10^{-4}$	0,545	-0,240
7	Тропосферний телефонний	ВФМ	1200	-	$7,3 \cdot 10^{-4}$	0,439	+0,033
8	Так само	ЧМ	1200	-	$7,05 \cdot 10^{-4}$	0,449	-0,020
9	Радіотелеграфний КХ	ЧМ	150	20 кВт	$2,85 \cdot 10^{-4}$	0,373	-0,544
10	Так само	ЧМ	50	5 кВт	$5,85 \cdot 10^{-3}$	0,320	+0,232
11	Так само	ЧМ	150	1 кВт	$1,64 \cdot 10^{-2}$	0,550	-0,141

Установлено, що звичайно для однакових каналів нахил прямих приблизно є однаковим, а зі зміною частоти помилок апроксимуюча пряма зміщується не змінюючи кута нахилу [70]. Для каналів різного виду нахил прямих є різним. На підставі рівняння прямої лінії можна одержати

$$P(\geq 1, n) = n^{1-\alpha} p, \quad 0 < \alpha < 1. \quad (1.56)$$

Величина параметра α певною мірою відображає фізичні причини появи помилок. Тому параметр α є надто важливим параметром послідовності помилок E .

При встановленні взаємозв'язку коефіцієнтів кореляції та групування одержані залежності статистичних параметрів потоку помилок від середнього значення спотворених помилок у кодовому слові:

$$- \text{коефіцієнт групування } \alpha = \frac{\ln \bar{t}}{\ln n};$$

– ймовірність появи спотвореного кодового слова із n елементів

$$P(\geq 1, n) = \frac{n}{\bar{t}} P_e;$$

– ймовірність появи спотвореного кодового слова з m і більше помилками

$$P(\geq m, n) = \frac{n}{m} \frac{m^\alpha}{\bar{t}} P_e.$$

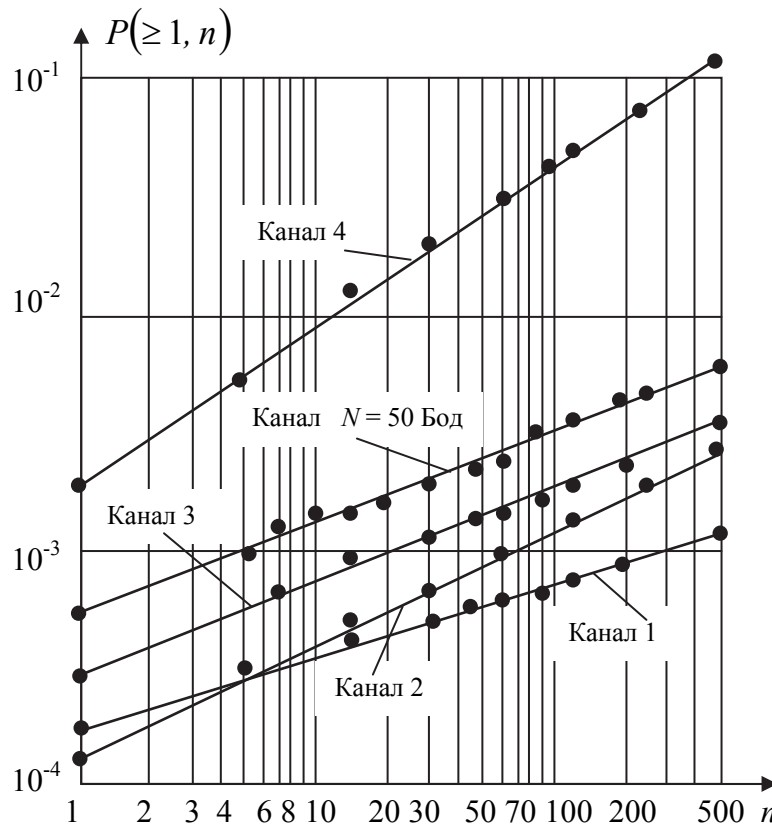


Рисунок 1.35 – Залежність $P(\geq 1, n)$ від n для телефонних кабельних каналів

Одним із відомих способів зменшення впливу групування помилок на ефективність систем підвищення достовірності є декореляція помилок рознесенням елементів, що передаються, у часі. На рис. 1.36 наведено залежності $P(\geq 1, n) = f(n)$ для каналів 2, 4 і 11 в табл. 1.5 при інтервалах декореляції $j = 10$ і 1000 елементів (випадок $j = 1$ відповідає відсутності декореляції). Пунктиром на рис. 1.36 нанесено залежності $P(\geq 1, n) = f(n)$ для незалежного розподілу помилок.

При оцінці ефективності блокових коригуючих кодів викликає зацікавленість не тільки ймовірність появи n -елементних спотворених комбінацій $P(\geq 1, n)$, але й ймовірності появи спотворених комбінацій з однією $P(1, n)$, двома $P(2, n)$ і m помилками $P(m, n)$. Якщо ці ймовірності визначаються по відношенню до всіх переданих комбінацій, то очевидно

$$P(\geq 1, n) = P(1, n) + P(2, n) + \dots + P(m, n) + \dots + P(n, n) = \sum_{i=1}^n P(i, n). \quad (1.57)$$

Для оцінки ефективності деяких коригуючих кодів необхідно також знати сумарну (накопичену) ймовірність появи спотворених комбінацій з m і більше помилками:

$$P(\geq m, n) = P(m, n) + P(m+1, n) + \dots + P(n, n) = \sum_{i=m}^n P(i, n).$$

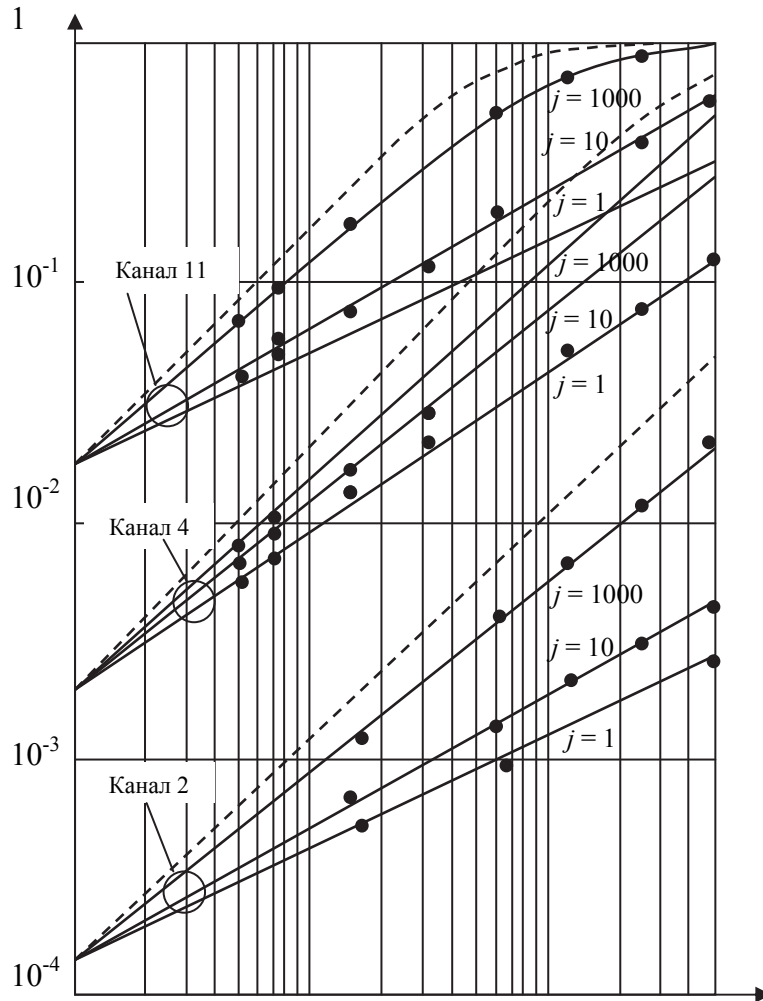


Рисунок 1.36 – Залежність $P(\geq 1, n)$ від n за різних інтервалів декореляції

Статистична ймовірність появи n -елементних комбінацій з m і більше помилками визначається як відношення кількості комбінацій з m і більше помилками до загальної кількості комбінацій:

$$P(\geq m, n) = \frac{\sum_{i=m}^n N(i, n)}{N_3(n)}, \quad (1.58)$$

де $N(i, n)$ – кількість n -елементних комбінацій, що містять i помилок;
 $N_3 = \sum_{i=0}^n N(i, n)$ – загальна кількість переданих n -елементних комбінацій.

При статистичному обробленні кількість комбінацій з i помилками $N(i, n)$ визначається діленням послідовності помилок $E = (e_1, e_2, e_3, \dots, e_L)$ на підпослідовності $E_n = (e_1, e_2, e_3, \dots, e_n)$ і наступним підрахунком кількості підпослідовностей E_n з вагою i . При цьому $N_3 = L/n$.

На рис. 1.37 у подвійному логарифмічному масштабі наведено графіки $P(\geq m, n)$ в залежності від кількості помилок m у комбінаціях різної довжини n для трьох різних типів каналів: кабельного і радіорелейного телефонних і радіотелеграфного (канали 1, 6, 9 в табл. 1.5). Точками на цих рисунках нанесено експериментальні дані, які на ділянці $1 \leq m \leq n/3$ достатньо добре апроксимуються прямими лініями. Установлено, що для всіх реальних каналів значення $P(\geq m, n)$ зі зростанням m на ділянці $m < n/3$ спадають повільно, що пояснюється наявністю спотворених комбінацій з великою кількістю помилок і груповим характером розподілу останніх.

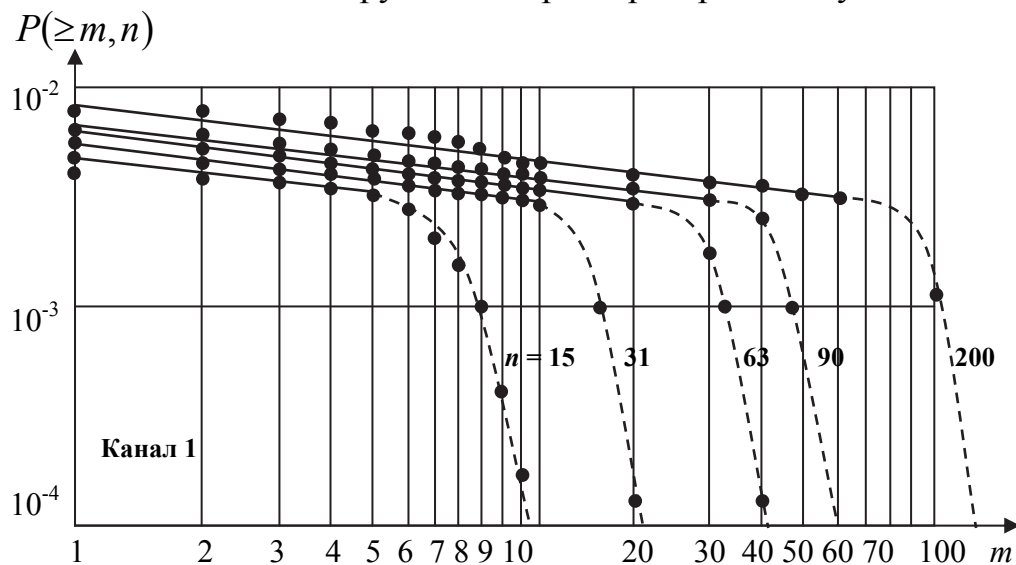


Рисунок 1.37 – Залежність $P(\geq m, n)$ від m для каналу 1

Порівнюючи рис. 1.36 – 1.37 бачимо, що швидкість спадання ймовірності $P(\geq m, n)$ є різною і залежить від виду каналу. Через те, що найбільше групування помилок спостерігається у кабельних каналах, швидкість спадання ймовірності $P(\geq m, n)$ зі зростанням m у цих каналах (рис. 1.37) є найменшою.

1.6. Моделі нестационарних каналів

Аналitичні методи дослідження методів підвищення вірності (МПВ) обов'язково базуються на певній математичній моделі потоку помилок дискретного каналу зв'язку. Число різноманітних математичних моделей,

запропонованих для опису потоків помилок, надто велике. Так, у монографіях Блоха, Попова, Туріна їх наведено більше двадцяти, у монографії Мізіна, Урінсона, Храмина – більше п'ятнадцяти. Оскільки в означених роботах досить докладно описано моделі і дано їхній аналіз, ми обмежимося лише коротким обговоренням цього питання.

Моделі, побудовані за аналогією з найпростішими імовірнісними структурами, не відбивають усіх закономірностей, притаманних реальним потокам. Характерна для більшості каналів тенденція помилок до групування не знаходить відбиття в тому разі, коли потік помилок подається як найпростіший.

Подання потоку у вигляді процесу відтворення не виключає можливості групування помилок, що зазначено Мергцем. Процес відтворення цілковито характеризується одновимірною функцією розподілу інтервалів між послідовними помилками, яка збігається з нульовою функцією Пальма. В якості такої функції використовуються різноманітні розподіли: в моделі Бергера–Мальденброта – розподіл Парето, в моделі Брусилівського – розподіл Вейбулла. Зауважимо, що існує й загальний метод переходу від функції Пальма до ймовірностей розподілу, дістаний в роботах Амосова й Колпакова.

Однак докладне дослідження властивостей потоку помилок засвідчує, що у більшості випадків інтервали між помилками стають залежними, випадковими величинами, що суперечить гіпотезі про подання потоку процесом відтворення.

Зокрема, при дослідженні обґрунтованості моделі Бергера–Мандельброта для телефонного каналу Льюїс та Кокс виявили потужну додатну кореляцію в області інтервалів великої довжини. Аналіз кореляційних властивостей потоку помилок в радіоканалах зі завмираннями дав можливість Ветишеву, Місорину, Петрову дійти висновку щодо того, що гіпотеза про незалежність між помилковими інтервалами може бути слушна лише в одному окремому випадку, коли є великі відношення сигнал/шум та інтервал кореляції процесу завмирань.

Ця обставина спричинила виникнення більш складних гіпотез. Так, наприклад, Елліот подає потік помилок у вигляді суперпозиції трьох процесів відтворення.

Існує й більш загальна модель, запропонована Монтером та Вольфом, в якій складові потоку помилок є потоками з миттєвим відтворенням, а зміна складових відбувається зі сталою ймовірністю.

Як правило, моделі, які ґрунтуються на процесах відтворення, призводять до громіздких виразів.

Не вдалося відобразити закономірності, притаманні реальним послідовностям помилок, і користуючись порівняно простим аналітичним апаратом стохастично визначених процесів, наприклад, простими марковськими ланцюгами. Тому в праці Петровича потік помилок розглянуто як v -

зв'язний марковський ланцюг. Однак способи визначення параметрів моделі на підставі статистичних даних запропоновано лише для $\nu=2$.

Головні труднощі при використанні моделей цього класу пов'язані з необхідністю оцінювання значної кількості параметрів. Наприклад, для радіоканалів із завмираннями, досліджених Коржиком, оптимальна апроксимація імовірнісних характеристик потоку помилок досягається за $\nu>19$. Ця цікава й важлива модель не набула широкого розповсюдження, найперше, через відсутність оцінок для параметрів за $\nu>2$ та громіздких обчислень.

В моделі Дувакіна статистичні закономірності потоку помилок описуються на підставі подання послідовності довжини між помилковими інтервалами процесом з різноманітною пам'яттю. У першому наближенні пам'ять вважається за нульову, тобто дістаємо процес відтворення. Моделі Дувакіна перетворюється на окремий випадок моделі Елліота. У другому наближенні цей процес є простим ланцюгом Маркова, а у третьому – двозв'язним й т.д. Для побудови такої моделі потрібне задання матриці перехідних ймовірностей марковського ланцюга зі значною (в загальному випадку необмеженою) кількістю станів.

Отже, моделі, побудовані за аналогією з найпростішими імовірнісними структурами, є неадекватними до реальних процесів. Більш складні моделі типу моделі Елліота, Мюнтера–Вульфа, Петровича, Дувакіна з великою кількістю штучно уведених параметрів не матимуть практичної цінності доти, поки не вдасться віднайти спосіб визначення їхніх параметрів за експериментальною статистикою.

Процес зміни стану може бути в загальному випадку будь-яким: процесом відтворення, простим чи складним, марковським ланцюгом тощо.

Найпростіші моделі, в яких процес зміни станів описується як простий марковський ланцюг, мають два-три різних стани й відрізняються лише обмеженнями на параметри матриці перехідних ймовірностей марковського ланцюга. До них належать моделі Гілберта, Елліота, Маккалоха, Сміта–Боуена–Джойса, Елспаса, Кохена та Берковіца, Охордини.

Найбільш загальна з цих моделей, запропонована Кохеном та Берковіцем, визначається дев'ятьма параметрами – трьома умовними ймовірностями помилок в кожному з можливих станів та шістьма ймовірностями переходу зі стану в стан. На жаль, моделі такого типу застосовані лише для вузького класу каналів чи для надто наближених розрахунків.

Узагальнення розглянутих моделей, яке дає можливість забезпечити більш високу точність апроксимації експериментальних характеристик, пов'язане зі збільшенням або кількістю можливих станів, або зв'язністю марковського ланцюга.

Відповідно до моделі Петровича, послідовність “добрих” та “поганих” станів є двозв'язний ланцюг Маркова, що є еквівалентним до однозв'язного ланцюга з чотирма станами.

Існує також низка окремих моделей, які оперують поняттям “пакет” помилок. В пакет поєднуються всі помилки, інтервал між якими не перевищує певної величини N , називаної інтервалом єднання. Для цієї групи є типовою модель Беннета–Фройліха, яка доволі повно відбиває процес виникнення помилок на відносно коротких трактах міських телефонних ліній.

Зручною модифікацією моделі Беннета–Фройліха є модель Мізіна–Муравйова, в якій розподіл проміжків між пакетами є геометричний.

За загальний недолік, притаманний всій групі “пакетних” моделей, слід вважати невизначеність таких понять, як “пакет” чи “ланцюжок пакетів”. Винятком є модель Морева–Юнакова, для якої розроблено емпіричний спосіб розбивання потоку помилок на незалежні пакети, який дозволяє чітко визначати параметри моделей. В решті робіт вибір інтервалу об’єднання не є обґрунтований і величина N коливається для різних моделей від 5 до 25 символів.

Водночас розподіл пакетів за довжиною, а також властивості розподілу помилок усередині пакета істотно залежать від інтервалу об’єднання. В роботі Климушина зазначено, що згруповані помилки всередині пакета стають незалежними лише за малого інтервалу єднання ($N = 6 \dots 8$ розрядів), що можна пояснити специфікою механізму пакетоутворення в розглянутих ним телефонних каналах з короткочасними перериваннями.

Окрім загальних моделей, існує ще низка способів часткового описування потоків помилок, які дозволяють обчислювати найбільш важливі характеристики каналів (Мертц, Елліот, Зелігер, Амосов та Колпаков, Ланко, Пуртов, Замрій, Захаров, Брусиловський, Мартинов).

Різноманіття пропонованих способів описування потоку помилок можна пояснити тим, що автори моделей досліджували різноманітні канали за різноманітних умов роботи.

Спроби надати конкретний фізичний зміст параметрам моделі здійснено в роботах Брусиловського, Вольфбейна, Ланка, Коржика, однак моделі виявились або неповними, або надто громіздкими.

Логічно й зручно розглядати потік помилок дискретного каналу зв’язку як ступінчастий випадковий процес. Такий підхід дозволяє при дослідженні каналів зв’язку використовувати численні важливі результати, дістані для випадкових процесів.

Дотримуючись Хінчина, виокремимо серед різноманітних способів завдання потоків два.

За першого способу завдання потоків помилок необхідно для будь-якого натурального числа $r \geq 1$ й довільного набору чисел $0 < \tau_1 < \tau_2 < \tau_3 < \dots < \tau_r$ зазначити r -вимірну функцію розподілу випадкового вектора $\{x(\tau_i), i = \overline{1, r}\}$, де $x(\tau)$ – кількість помилок, які з’явились за проміжок часу $[0, \tau]$, або віднайти

$$\begin{aligned}
P\{[x(\tau + \tau_i) - x(\tau + \tau_{i-1})] = k_i, \quad i = \overline{1, r}\} = \\
= \mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r), \quad k_i \geq 0, \quad r \geq 1, \quad t_i = \tau_i - \tau_{i-1},
\end{aligned}
\tag{1.59}$$

де τ – початок відліку часу. Отже, $\mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r)$ є ймовірність того, що на послідовно розміщених проміжках часу t_i (відкладуваного від моменту часу τ), t_2, \dots, t_r з'являються відповідно k_1, \dots, k_r помилок. Цей розподіл цілком визначає потік помилок. На практиці (1.59) найчастіше використовується для $r_1 = 1$, що відповідає одновимірному розподілу кількості помилок за проміжок часу $[\tau, \tau + 1)$:

$$\mathfrak{G}_k(\tau; t) = P\{x(\tau + t) - x(\tau) = k\}, \quad k \geq 0.
\tag{1.60}$$

Для стаціонарного потоку залежність від τ є відсутня. В цьому разі позначатимемо розподіл через $\mathfrak{G}_k(t)$.

Іноді вважають, що для завдання потоку доволі віднайти одновимірний розподіл (1.60). Як бачимо, що у загальному випадку це не є вірно. Для потоків помилок каналів зв'язку згадана обставина має особливе значення.

Останнім часом широкого застосування набув метод моделювання, який ґрунтується на уведенні поняття породжувального процесу. Згідно з термінологією Амосова й Колпакова, таким є певний випадковий процес, який кожний момент часу характеризує стан каналу зв'язку. Кожному стану відповідає (детерміновано чи статистично) певна ймовірність помилкового приймання символу. Ймовірність помилкового приймання символу в границях тривалості стану вважається за сталу.

В роботі Амосова та Колпакова розглядається більш загальний випадок, коли породжувальний процес є або процесом відтворення, або марковським ланцюгом з кінцевою кількістю стійких станів. Вимога щодо стійкості станів означає, що перехід з кожного внутрішнього стану є можливий лише у двох сусідніх з ймовірностями, наближеними до нуля.

При цьому розподіл помилок в блоці фіксованої довжини являє собою рандомізований за параметром біноміальний розподіл

$$\mathfrak{G}_k(t) = C_n^k \int_0^1 x^{k^1} (1-x)^{n-k} dF(x).
\tag{1.61}$$

Більш досконаліми з точки зору точності апроксимації реальних розподілів порівняно з моделлю Беннета–Фройліха є способи описування потоків помилок, запропоновані в роботах Морева, Юнакова, Нахимовича й Попова, Туріна, що враховують групування самих пакетів у ланцюжках складної структури.

Для моделі Попова, Туріна перевірено відповідність експериментальних та теоретичних розподілів методами математичної статистики. Але цінність моделі багато в чому залежить від того, набором яких параметрів вона характеризується та чи існують статистичні оцінки цих параметрів.

На жаль, кількість штучно уведених параметрів у моделі Попова–Туріна є значна, і спосіб їхнього визначення не зазначено.

Хінчин установив фундаментальну якість стаціонарних потоків, довів, що для кожного стаціонарного потоку існує межа

$$\lim_{t \rightarrow 0} \frac{1 - \mathfrak{G}_0(t)}{t} = \lambda, \quad (1.62)$$

яку він назвав параметром потоку. Цей параметр для кожного стаціонарного ординарного потоку дорівнює математичному сподіванню кількості подій потоку за одиницю часу. Іноді зручніше користуватися й іншим виразом для обчислення λ :

$$\lambda = -\mathfrak{G}_0'(0).$$

Зауважимо, що відома характеристика каналу зв'язку – ймовірність спотворення символу елемента P_e пов'язана простим співвідношенням з параметром λ : $P_e = \lambda T$, де T – швидкість передавання інформації каналом (у двійкових символах за одиницю часу).

Моделі нестаціонарних каналів. Для нестаціонарного потоку також існує відповідна границя, називана миттєвим параметром, який залежить від поточного часу:

$$\lambda(\tau) = - \left. \frac{\partial \mathfrak{G}_0(\tau, t)}{\partial t} \right|_{t=0}.$$

Для ординарного нестаціонарного потоку математичне сподівання кількості помилок за проміжок часу $[\tau; \tau + t)$ визначається співвідношенням

$$\Lambda(\tau; t) = \sum_{k=1}^{\infty} k \mathfrak{G}_k(\tau, t) = \int_{\tau}^{\tau+t} \lambda(x) dx, \quad (1.63)$$

що дозволяє для нестаціонарного пуассонівського потоку одержати співвідношення

$$\begin{aligned} \mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r) = \\ = \prod_{s=1}^r \frac{\Lambda^{k_s}(\tau + \sum_{i=1}^{s-1} t_i; t_s)}{k_s} \exp[-\Lambda(\tau + \sum_{i=1}^{s-1} t_i; t_s)], \end{aligned} \quad (1.64)$$

Тобто твірна функція дорівнює

$$\begin{aligned} \Phi(\tau; t_1, \dots, t_r; z_1, \dots, z_r) = \sum_{k_1, \dots, k_r} z_1^{k_1} \dots z_r^{k_r} \mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r) = \\ = \prod_{i=1}^r \exp[-\Lambda(\tau + \sum_{i=1}^{s-1} t_i; t_s)(1 - z_i)], \end{aligned} \quad (1.65)$$

де

$$\Lambda(a; t_s) = \int_a^{a+t_s} \lambda(x) dx; \quad a = \tau + \sum_{i=1}^{s-1} t_i. \quad (1.66)$$

При цьому слід зауважити, що потік помилок дискретного каналу зв'язку є ординарним.

Важливу роль при вивченні й використанні властивостей потоків відіграють так звані функції Пальма–Хінчина $\varphi_k(t)$. Цю функцію можна розглядати як імовірність появи, що дорівнює k подіям потоку (помилкам) за проміжок часу t за умови, що в початковий момент часу з'явилася подія потоку (помилка). Зауважимо, що при визначенні $\varphi_k(t)$ проміжок t відраховується від моменту настання події потоку, при визначенні ж $\vartheta_k(t)$ цей проміжок відлічується від довільно обраного моменту часу. Зв'язок між функціями $\varphi_k(t)$ та $\vartheta_k(t)$:

$$\left. \begin{aligned} \vartheta'_0(t) &= -\lambda\varphi_0(t); \\ \vartheta'_k(t) &= \lambda[\varphi_{k-1}(t) - \varphi_k(t)], \quad k > 0 \end{aligned} \right\}$$

або в іншій формі

$$\left. \begin{aligned} \vartheta_0(t) &= 1 - \lambda \int_0^t \varphi_0(x) dx = \lambda \int_t^\infty \varphi_0(x) dx; \\ \vartheta_k(t) &= \lambda \int_0^t [\varphi_{k-1}(x) - \varphi_k(x)] dx. \end{aligned} \right\} \quad (1.67)$$

Зауважимо, що оскільки $\vartheta_0(0) = 1$, то з (1.67) випливає $\lambda = \left\{ \int_0^\infty \varphi_0(x) dx \right\}^{-1}$, тобто для визначення λ можна скористатися кожним із співвідношень:

$$\lambda = \sum_{k=1}^{\infty} k \vartheta_k(t) = -\vartheta'_0(0) = \left\{ \int_0^\infty \varphi_0(x) dx \right\}^{-1}. \quad (1.68)$$

Є всі підстави вважати, що для нестационарних каналів проблема може бути розв'язана, якщо за основу брати математичний апарат пуассонівських потоків з параметром – випадковою величиною чи випадковим процесом. Обґрунтуванням такого висновку, окрім гнучкості математичного апарату, може бути й можливість тлумачення твірного функціоналу довільного потоку подій як твірного функціоналу пуассонівського потоку з випадковою інтенсивністю.

Припустимо, що є певний ступінчастий випадковий у часі процес $x(\tau; \lambda)$, відмінний від процесу $x(\tau)$, введеного раніше, лише тим, що в ньому виокремлено певну сукупність параметрів $\lambda = \{\lambda_i; i = \overline{1, s}\}$. Численний клас процесів може бути одержано з вихідного процесу $x(\tau; \lambda)$, якщо розглядати λ як випадкову величину чи випадковий процес, тобто шляхом рандомізації λ . Задаючи різноманітні розподіли для λ й усереднюючи за

ними характеристики процесу $x(\tau; \lambda)$, одержимо відповідні характеристики нових процесів $x(\tau)$. Можна записати, що в цьому разі

$$x(\tau) = Mx(\tau; \lambda), \quad (1.69)$$

де M – оператор математичного сподівання.

Такий підхід часто використовується в теорії ймовірностей, математичній статистиці, теорії надійності, теорії масового обслуговування для здобуття нових процесів та розподілів.

Називатимемо $x(\tau; \lambda)$ умовним процесом, процес λ (λ -процес) – породжувальним процесом, а $x(\tau)$ – рандомізованим, або безумовним процесом.

Позначимо через $\mathfrak{G}_{k_1, \dots, k_r}^*(\tau; t_1, \dots, t_r; \lambda)$ ймовірність, визначувану з (1.59) для умовного процесу $x(\tau; \lambda)$; це ймовірність того, що з'явиться саме k_1, \dots, k_r подій потоку $x(\tau; \lambda)$ на послідовно розміщених відрізках часу $\tau = t_2$ (відкладуваному від моменту часу $\tau + t_1$), \dots , τ_r . Тоді для рандомізованого процесу $x(\tau)$ на підставі (1.63) матимемо

$$\mathfrak{G}_{k_1, \dots, k_r}^*(\tau; t_1, \dots, t_r) = M\mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r; \lambda), \quad (1.70)$$

або в формі твірних функцій

$$\begin{aligned} \Phi(\tau; t_1, \dots, t_r; z_1, \dots, z_r) &= \\ &= \sum_{k_1, \dots, k_r} z_1^{k_1} \dots z_r^{k_r} \mathfrak{G}_{k_1, \dots, k_r}(\tau; t_1, \dots, t_r) = \\ &= M\Phi^*(\tau; t_1, \dots, t_r; z_1, \dots, z_r; \lambda), \end{aligned}$$

де

$$\begin{aligned} \Phi^*(\tau; t_1, \dots, t_r; z_1, \dots, z_r) &= \\ &= \sum_{k_1, \dots, k_r} z_1^{k_1} \dots z_r^{k_r} \mathfrak{G}_{k_1, \dots, k_r}^*(\tau; t_1, \dots, t_r). \end{aligned}$$

У подальшому в якості умовного розглянемо як приклад пуассонівський процес (потік). Здобуваний з нього рандомізований процес називатимемо узагальненим пуассонівським потоком (УПП). Для пуассонівського потоку твірна функція Φ^* визначається за допомогою (1.67). Розглядаючи $\lambda(x)$ як певний випадковий процес та застосовуючи до (1.67) оператор математичного сподівання, дістанемо твірну функцію для рандомізованого процесу, тобто для УПП:

$$\begin{aligned} \Phi(\tau; t_1, \dots, t_r; z_1, \dots, z_r) &= \\ &= M \prod_{s=1}^r \exp[-\Lambda(\tau + \sum_{i=1}^{s-1} t_i; t_s)(1 - z_s)], \end{aligned} \quad (1.71)$$

де $\Lambda(a, b) = \int_a^{a+t} \lambda(x) dx$, $\alpha = \tau$.

Якщо для умовного потоку подати $\mathfrak{G}_0^*(\tau; t) = \exp[-\Lambda(\tau; t)] \equiv \mathfrak{G}_0^*[\Lambda(\tau; t)]$, то вираз (1.70) можна записати в такому вигляді:

$$\begin{aligned} \Phi^*(\tau; t_1, \dots, t_r; z_1, \dots, z_r) &= \\ &= M \mathfrak{G}_0^*[\sum_{s=1}^r \Lambda(\tau + \sum_{i=1}^{s-1} t_i; t_s)(1 - z_s)]. \end{aligned}$$

Для $\tau = 1$ з (1.70) одержується одновимірна твірна функція

$$\begin{aligned} \Phi(\tau; t_1; z) &= M \exp[-\Lambda(\tau; t)(1 - z)] = \\ &= M \mathfrak{G}_0^*[\Lambda(\tau; t)(1 - z)]. \end{aligned} \quad (1.72)$$

Зважаючи на те, що реальні канали зв'язку є нестационарні, подальший аналіз КПС побудуємо виходячи з того, що його параметри істотно змінюються в часі.

Спочатку розглянемо різновиди спотворень та математичний опис КПС у стаціонарному випадку, що необхідно для подальшого описування реального каналу постійного струму квазістаціонарною моделлю.

Під впливом дії в каналі зазначених завад прийняте кодове надсилання спотворюється, що може спричинитися до помилкової реєстрації символу кодового слова. Наслідки впливу завади на кодове слово може бути розглянуто на підставі вторинних характеристик каналу: дроблень, крайових спотворень та помилок. Дроблення та крайові спотворення характеризують дискретний за рівнем та неперервний за часом канал зв'язку, тобто КПС, а помилки – дискретний за рівнем та часом канал, тобто ДКЗ.

За синхронного передавання інформації закон розподілення характеристичних моментів відтворення доволі точно апроксимується нормальним законом]

$$f_1(x) = (\sigma_1 \sqrt{2\pi})^{-1} \exp[-(x - \bar{x})^2 / (2\sigma_1^2)], \quad (1.73)$$

тут x – випадкова величина, яка характеризує час відновлення сигналу до рівня реєстрації кодового надсилання або час відхилення фронту надсилання відносно межі розподілу надсилань; \bar{x} – математичне сподівання випадкової величини x ; σ_1 – середньоквадратичне відхилення x від \bar{x} .

Інколи крайові спотворення доволі точно апроксимуються сумою зважених нормальних законів з різноманітними дисперсіями.

Розподілення тривалості дроблень для провідних каналів та для телеграфних радіоканалів підпорядковуються логарифмічно-нормальному закону

$$f_2(\tau_{\text{др}}) = (\tau_{\text{др}} \sigma_2 \sqrt{2\pi})^{-1} \exp[-(\ln \tau_{\text{др}} - \overline{\ln \tau_{\text{др}}})^2 / (2\sigma_2^2)], \quad (1.74)$$

тут $\tau_{\text{др}}$ – випадкова величина, яка характеризує тривалість дроблень; $\overline{\ln \tau_{\text{др}}}$ – середнє значення логарифму випадкової величини $\tau_{\text{др}}$; σ_2 – середньоквадратичне відхилення $\ln \tau_{\text{др}}$ від $\overline{\ln \tau_{\text{др}}}$.

Зазначені закони розподілу параметрів завади та вторинних характеристик каналу зв'язку з постійними параметрами є ідеалізацією при описуванні реального каналу. Розглянуті закони та оцінки їхніх параметрів за описаного підходу здобуваються за істотного усереднення даних експериментального дослідження каналів як за часом, так і за іншими параметрами, характерними для каналу певного виду. Тому при розв'язанні задач проектування системи передавання інформації в суттєво нестаціонарних каналах, де параметри розподілу змінюються в широкому діапазоні, потрібне урахування нестаціонарності каналу при обчисленні основних показників якості функціонування системи.

З урахуванням сказаного розв'язання завдання побудови універсальних адекватних динамічних моделей каналу зв'язку поки що являє собою значні труднощі як через недостатній обсяг статистики параметрів каналів, так і через трудомісткість обчислень навіть за використання ЕОМ. Проте, побудова квазістаціонарних моделей зі значно меншим усередненням характеристик є цілком можлива. Такий підхід при описуванні каналів зв'язку має велике значення при обчисленні показників якості адаптивних систем, розробленню й дослідженню яких сьогодні приділяється все більше уваги.

Найбільш придатною формою квазістаціонарної моделі є кусочно-стаціонарна марковська модель КПС. Марковська модель описується матрицею $P = \|p_{ij}\|$ перехідних ймовірностей стаціонарних станів та матрицею $\Theta = \|\theta_{ik}\|$ параметрів спотворень, до числа яких належать статистичні характеристики крайових спотворень та дроблень кодових надсилань.

Кусочно-стаціонарна модель дискретного каналу зв'язку передбачає, що зміни параметрів ДКЗ наступають миттєві, і можна припустити, що можливі набори значень їхніх параметрів утворюють дискретну множину і можуть бути пронумеровані цифрами: $u = 1, 2, \dots, l$. Тоді модель нестаціонарного ДКЗ можна подати у вигляді l моделей Еліота, які розрізняються чисельними значеннями параметрів й підключаються до каналу певним випадковим комутувальним процесом $U = \{u\}$. Якщо $u = j$, то канал перебуває в j -му стаціонарному стані (рис. 1.38 а).

У більш загальному випадку складові моделі стаціонарних станів можуть розрізняватися не лише параметрами, але й самими моделями. Для завдання такої кусочно-стаціонарної моделі ДКЗ за зазначеного підходу слід описати статистику переходів з одного стаціонарного стану в інший

$\{u\}$ для $u=1, 2, \dots, l$; статистику розподілень інтервалів стаціонарних станів $f_u(t \geq \tau)$, а також форму та параметри моделі u -го стаціонарного стану ДКЗ. Наприклад, як модель u -го стаціонарного стану ДКЗ може бути використано модель Елліота-Гільберта, яка є ланцюгом Маркова з двома станами. Імовірнісний граф моделі Елліота-Гільберта подано на рис. 1.38, б).

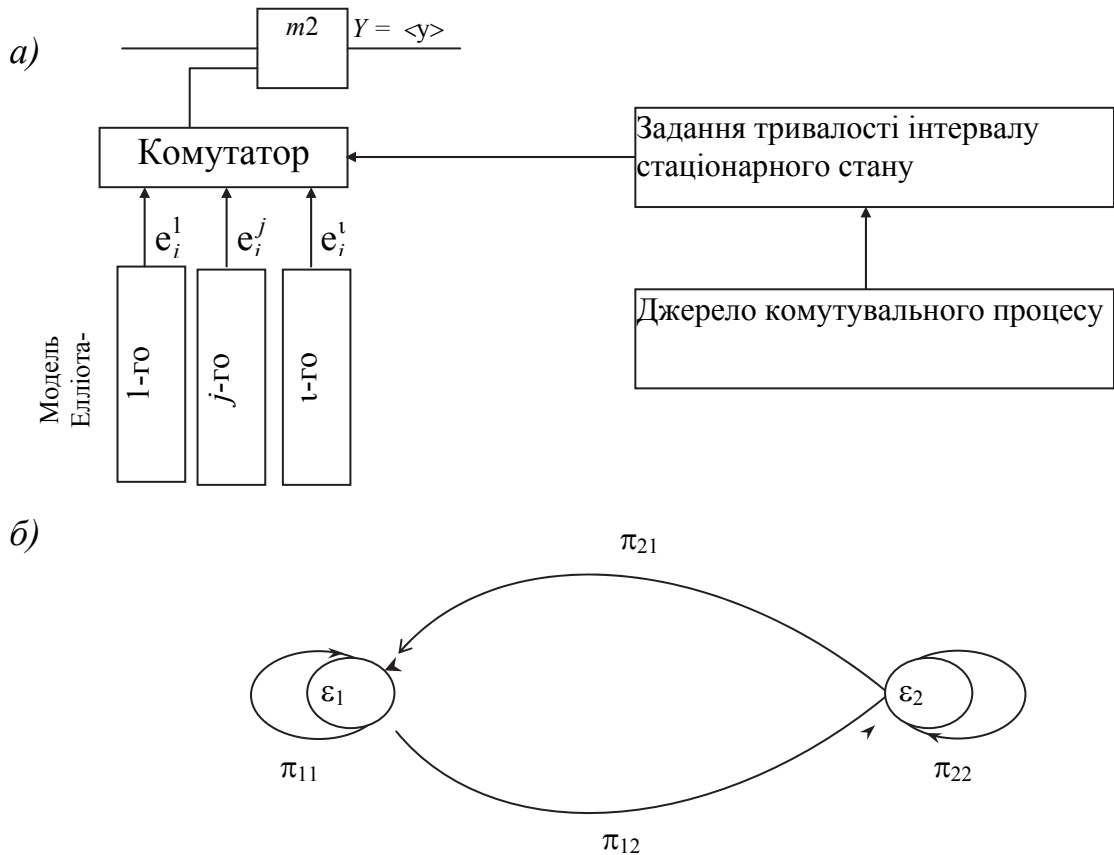


Рисунок 1.38 – Кусочно-стаціонарна модель

Матриця перехідних ймовірностей має форму

$$\Pi = \begin{vmatrix} \pi_{11} & \pi_{12} \\ \pi_{21} & \pi_{22} \end{vmatrix}, \quad (1.75)$$

де $\pi_{11} + \pi_{12} = \pi_{21} + \pi_{22} = 1$, а матриця ймовірностей появи помилки в станах $-\Theta_\varepsilon = \|\varepsilon_1 \varepsilon_2\|$, де ε_1 означає ймовірність появи помилки у стані 1, а ε_2 – ймовірність появи помилки у стані 2.

Джерело процесу комутації і переходу від одного стаціонарного стану до іншого є також ланцюгом Маркова з l -станами, матриця перехідних ймовірностей якого має вигляд

$$P = \begin{vmatrix} p_{11} & p_{12} & \dots & p_{1l} \\ p_{21} & p_{22} & \dots & p_{2l} \\ \dots & \dots & \dots & \dots \\ p_{l1} & p_{l2} & \dots & p_{ll} \end{vmatrix}. \quad (1.76)$$

Після того, як комутатор визначить номер стаціонарного стану, слід визначити тривалість перебування моделі в цьому стаціонарному стані. Розподіл ймовірностей часу перебування у стаціонарних станах задається матрицею

$$P(t) = \begin{pmatrix} p_1(t) \\ p_2(t) \\ \dots \\ p_2(t) \end{pmatrix}, \quad (1.77)$$

а для описування $p_u(t)$ може бути обрано експоненційний закон $p_u(t) = \exp(-t/T_{\text{сер}}^u)$, звідки $t = -T_{\text{сер}}^u \ln R$ ($T_{\text{сер}}^u$ – середній час перебування в u -ому стаціонарному стані; R – датчик випадкових чисел, рівномірно розподілених на інтервалі $[0,1]$).

Параметри потоків дроблень та зміщень ЗМВ. Важливою характеристикою, що визначає доцільність застосування конкретних методів кодування і декодування при використанні критерію ξ_j , є розподіл кратностей помилок $p_u(m, n)$ для кожного стану ДКЗ. На рис. 1.39 як приклад наведені в напівлогарифмічному масштабі експериментальні $p_u(m, n)$ для $n = 16$ (компонування кривих на рисунку довільне). Для $p_0(m, n)$ усі спостережувані кратності практично мають ймовірність одного порядку, причому значення, що спостерігаються, лежать здебільшого в межах $n/2$, що ще раз підтверджує локальну асиметрію помилок у даному стані. Зі збільшенням u спостерігається монотонне зростання ймовірностей усіх кратностей помилок.

У результаті якісного розгляду $p_u(m, n)$ можна зробити два основних висновки щодо можливості використання отриманих результатів на етапі завадостійкого оброблення прийнятої інформації в ДКЗ:

1. При класифікації станів ДКЗ за критерієм ξ_j доцільно використовувати кодову надмірність у «поганих» станах для виявлення помилок, а в «хороших» – для часткового виправлення помилок і стирань, що повинно збільшити інформаційну швидкість через зменшення кількості перезапитів у системі з керуючим зворотним зв'язком порівняно з випадком виявлення помилок.

2. Оскільки ймовірність появи помилок високої кратності для «поганих» станів ДКЗ досить велика і лежить у діапазоні $10^{-2} - 10^{-1}$, то для забезпечення заданої завадостійкості при збереженні досить високої інформаційної швидкості доцільно використовувати виявлення помилок високої кратності непрямыми методами, не збільшуючи для цього надмірно кодову надлишковість.

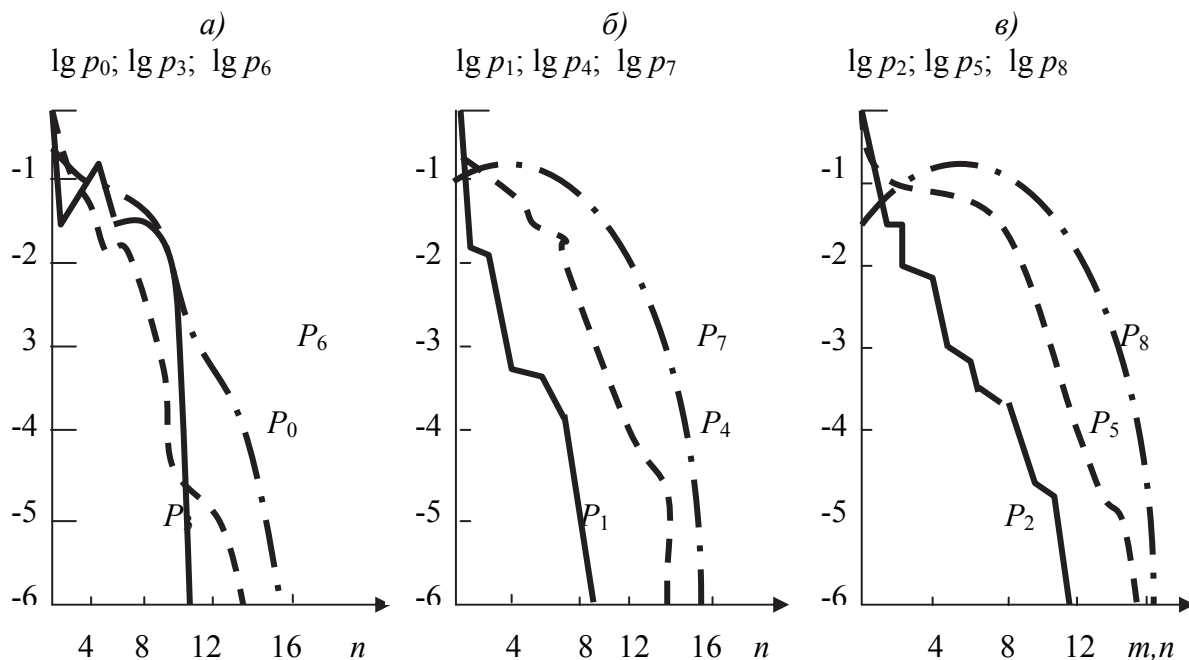


Рисунок 1.39 – Розподіл кратності помилок ДКЗ

Розглянемо експериментальні розподіли довжини пачок помилок $p_u(l)$ для станів ДКЗ, що класифікуються. Залежності $p_u(l)$ для $n = 16$ наведені на рис. 1.40. Одержані залежності задовільно апроксимувалися логарифмічно-нормальним законом з параметрами середнього значення $\ln l_u$ тривалості пачок l і середньоквадратичного відхилення. Розподіли $p_u(l)$ використовуються для апроксимації розподілу тривалості дроблень $p_u(\tau_d)$.

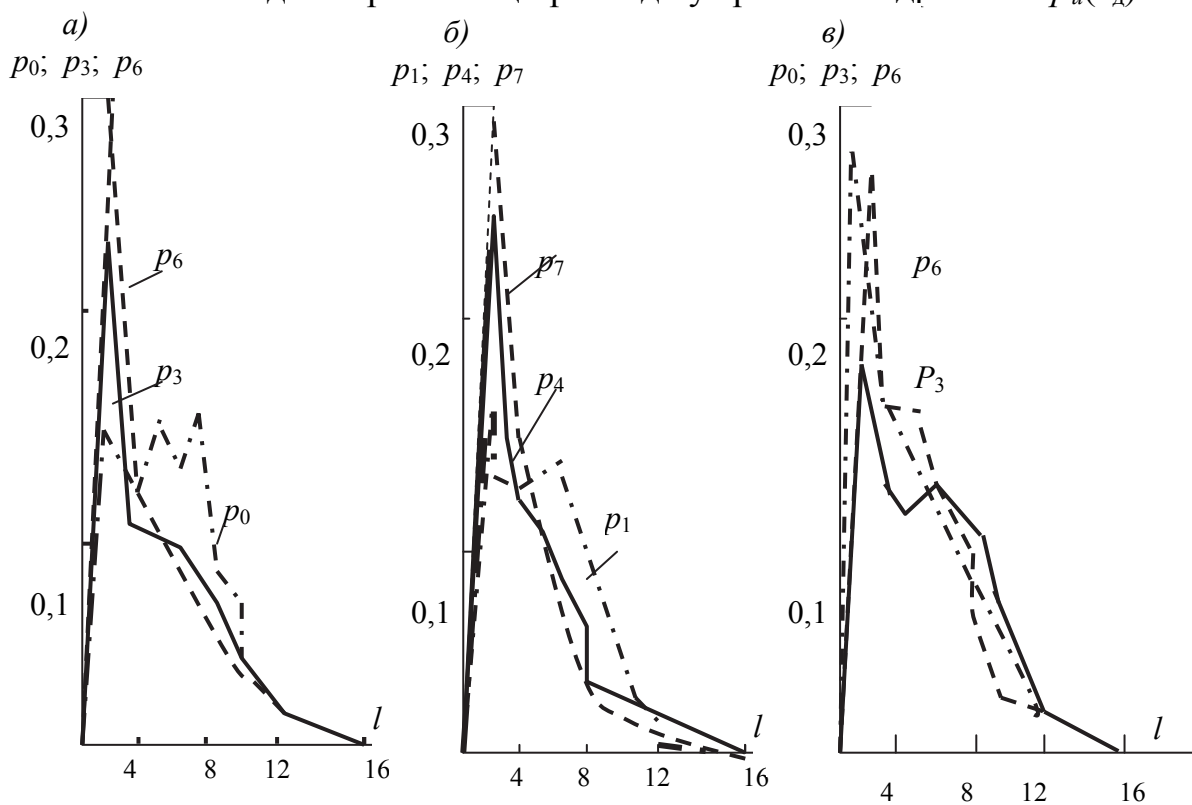


Рисунок 1.40 – Криві залежностей $p_u(l)$

Оцінені параметри розподілів $\overline{\ln l_u}$ і σ_u^d можуть бути використані як вихідні дані при аналітичному розрахунку першої розв'язувальної схеми з адаптивною зоною стирання при експрес-оцінюванні стану ДКЗ за критерієм ξ_j .

Отримані результати класифікації станів ДКЗ за критерієм ξ_j дозволяють зробити висновок про ефективність застосування даного критерію при експрес-оцінюванні стану ДКЗ з метою адаптивного приймання у першій розв'язувальній схемі й адаптивного декодування.

Для аналітичного опису імовірнісних характеристик адаптивної вирішальної схеми необхідне експериментальне дослідження вторинних характеристик каналу й апроксимація експериментального розподілу теоретичними.

Результати дослідження спотворень кодових посилок для всіх класифікованих критерієм станів при $n=8$ подані у вигляді експериментального розподілу спотворень кодових посилок на r дискрет квантування $p_{u \text{ експ}}(r)$.

Розподіл $p_{u \text{ експ}}(r)$ описують спотворення кодових посилок, викликані крайовими спотвореннями разом з дробленнями.

Для виділення з $p_{u \text{ експ}}(r)$ складової, обумовленої дробленнями $p_{\text{експ}}^d(r)$, може бути прийнята наступна модель спотворення кодових посилок у КПС. Спотворення довільної кодової послідовності за кожною границею тактових інтервалів можливо або тільки через крайові спотворення, або тільки внаслідок дроблень. При цьому ймовірність спотворень послідовності на r дискрет квантування визначається як

$$p(r) = p_d p_d(r) + (1 - p_d) p_k(r), \quad (1.78)$$

де p_d – ймовірність появи дроблення; $p_d(r)$ – ймовірність спотворення послідовності імпульсом дроблення на r дискрет; $p_k(r)$ – ймовірність спотворення послідовності на r дискрет через крайове спотворення.

Прийнята в моделі спотворення кодових посилок несумісність спотворення двох типів відповідає дійсному прояву завади (у вигляді спотворень) у КПС для розглянутого класу каналів. Насправді за високої вірогідності тактової синхронізації немає сенсу розглядати крайові спотворення в КПС у випадку появи в ДКЗ щільного пакета помилок у наслідок дроблення, тому що за результатами статистичного дослідження потоку F_i помилки в межах пакета в більшості випадків носять асиметричний характер.

При аналізі двійкових каналів адекватною для аналізу є модель Гільберта. Відомо, що до 80% обсягу інформації передається по каналах мереж LAN, MAN. У каналах такого виду перевищення сигналу над завадою (h_c^2) є функцією часу, отже, ймовірність, що змінюється, помилкового прийому елемента коду теж є функцією часу.

$$p_s = [\varphi(h_c^2), F(t)] h_c^2 = \tau(t). \quad (1.79)$$

Тут $F(t)$ – нелінійний функціональний оператор, який визначається способом модуляції, передаванням й обробленням сигналу тощо.

Імовірність появи пакета на інтервалі T_c визначається середнім числом пропаданя чи появи сигналу імпульсних завад

$$p_n = \gamma_0 T_c e^{-\gamma_0 T_c}. \quad (1.80)$$

Імовірність же появи пачки помилок довжиною l_n визначається середньою тривалістю в символах пакета помилок \bar{l}_c [58]

$$p(l_n) = \exp\left[-\frac{\pi(l_n - 0,5)^2}{4l_c^2}\right] - \exp\left[-\frac{\pi(l_n + 0,5)^2}{4l_c^2}\right]. \quad (1.81)$$

Середня довжина пакета визначається середньою тривалістю переривання \bar{l}_c і швидкістю модуляції B

$$\bar{l}_c = \bar{l}_n B. \quad (1.82)$$

При смузі $\Delta F = 700$ Гц середнє число переривань відповідає $\gamma_0 = 0,26$ дроблень за секунду при середній тривалості $\bar{l}_d = 1,775$ вс.

Отже, величина $\bar{l}_c = 1,065$. Тоді, згідно з (1.82), частка i -кратних помилок $p(i)$ складе

$$p(1) = \exp\left[-\frac{\pi(0,5)^2}{4,48}\right] - \exp\left[-\frac{\pi(1,5)^2}{4,48}\right] = 0,64.$$

Аналогічно одержимо для інших значень i

$$p(2)=0,21; \quad p(3)=0,084; \quad p(4)=0,025.$$

Оскільки на інтервалі «хорошого» стану $h_c^2 > 100$, то загальна ймовірність помилки буде визначатися тільки помилками «поганого» стану згідно з (1.81). Для тривалості $T_c = 6t_0$

$$p_n = 0,26 \cdot 10^{-2} e^{-0,26 \cdot 10^{-2}} = 2,5 \cdot 10^{-3}.$$

Слід зазначити, що в реальних умовах імовірності появи помилок i -ї кратності, як і ймовірність спотворення блока, визначається довжиною блока n . У табл. 1.5 наведені значення $p_d(i)$, $p_{бл}$, p_α для деяких значень n , розраховані на основі результатів вимірювання якості передавання каналами ГТС з двома АТС при швидкості $B = 600$ Бод і смузі $\Delta F = 700$ Гц.

Таблиця 1.5 – Імовірність появи i -кратних помилок

Довжина блока	$N_{\text{пом}}$	$P_d(i)$, кратність помилки у відсотках										$P_{\text{пб}}$	$P_e \cdot 10^{-4}$	α
		1	2	3	4	5	6	7	8	9	10			
4	6286	78	21	1	–	–	–	–	–	–	–	0,0016	4,9	0,27
9	4787	56	32	9	3	–	–	–	–	–	–	0,00274	4,72	0,27
16	3951	42	37	12	6	2	1	–	–	–	–	0,004	4,82	0,24
30	3338	40	29	13	8	5	2	1,5	1	0,5		0,0063	4,96	0,25

Значення p_e розраховувалося за формулою

$$p_e = \frac{1}{n} p_{\text{пб}} \sum_{i=s}^n p_{\text{д}(i);i}, \quad (1.83)$$

де $p_{\text{пб}}$ – імовірність помилкового приймання блок довжиною n .

Значення коефіцієнта групування α визначалося залежно з імовірністю появи помилкового блока $p(\geq 1, n)$ від довжини блоку n і значення p_e :

$$p(\geq 1, n) = p_{\text{бл}} = n^{1-\alpha} p_e,$$

$$\log \frac{p_{\text{пб}}}{p_e} = (1 - \alpha) \log n,$$

$$\alpha = 1 - \frac{\log \frac{p_{\text{пб}}}{p_e}}{\log n}.$$

Деякі коливання розрахованих значень α (табл. 1.5) можна пояснити недостатністю обсягу вибірки.

Для підтвердження гіпотези існування моделі дискретного каналу з двома станами (типу Гільберта) на каналах низового рівня LAN і MAN були проведені статистичні дослідження. При цьому тракт передавання був організований через послідовно з'єднані вузли комутації (міська телефонна мережа).

Було проведено дослідження якості передачі сигнальних конструкцій БЧК з трьома переходами при фіксованій послідовності сигнальної конструкції на комутованих каналах, що проходять через МАТС. На прийомі одиничні елементи на проміжку тривалістю t_0 реєструвались в 100 точках. Під час такої реєстрації забезпечувалась точність визначення місць ЗМВ. При цьому під помилковими розуміються такі комбінації, в котрих ЗМВ зміщені на величину $\Theta \geq 7,07t_0$ або змінено кількість переходів.

У таблиці 1.6 приведені значення ймовірності зміщення кожного із трьох ЗММ окремо (або разом) на величину $\Theta \geq \Delta/2$ для кодів слів при швидкостях передачі $B = 100; 200; 600$ Бод для полоси $\Delta F = 700$ Гц, та розраховані на підставі вимірювань параметри середньоквадратичного відхилення σ середнього інтервалу між помилковими сигнальними конструкціями.

Середньоквадратичне відхилення не перевищує 3% при вибраному базовому елементі (Δ) БЧК, який дорівнює 14% від t_0 . Середньоквадратичне відхилення визначалось за формулою:

$$\sigma = 2\Delta * \Psi^{-1}(0,5 - p_{\text{зм}}),$$

де Ψ^{-1} – обернена функція Крампа.

З аналізу таблиці 1.7 виходить, що помилковий прийом за рахунок дроблень, які збільшують число переходів. Це говорить про те, що середня тривалість сигналу поміж моментами модуляції $\bar{\tau}_c > \bar{\ell}_{\text{др}}$.

Таблиця 1.6 – Зміщення ЗМВ

Параметри	B, Бод		
	100	200	600
Зміщення переходів для наступних комбінацій ЗМВ:			
1	5,40E-03	6,27E-03	8,20E-03
2	5,43E-03	6,70E-03	8,07E-03
3	5,46E-03	6,67E-03	8,16E-03
1,2	1,26E-04	1,34E-04	1,55E-04
2,3	1,20E-04	1,33E-04	1,55E-04
1,3	1,29E-04	1,33E-04	1,55E-04
1,2,3	7,20E-07	7,59E-07	8,56E-07
σ , % (600 бод)	2,8	2,87	3
L_c , мс	17000	11000	3780

Таблиця 1.7 – Вплив дроблень на сигнал

Завади	B, Бод		
	100	200	600
Дроблення	2,44E-02	2,25E-02	1,90E-02
Збільшене число переходів	2,40E-02	2,20E-02	1,85E-02
Зменшене число переходів	4,50E-04	5,78E-04	5,12E-04
Зміщення $\Theta > \Delta/2$	6,96E-03	8,38E-03	9,97E-03
Σp_i	3,14E-02	3,09E-02	2,90E-02

Через те, що значення Θ при різних швидкостях визначалось як відсоток відносно до тривалості елемента при швидкості $B = 600$ Бод, то відносно до табл. 1.6 можна зазначити, що зі зміною швидкості σ , практично, не змінюється. Збільшення значення σ на швидкості 600 Бод можна пояснити наявністю МСЗ при $\Delta F = 700$ Гц.

Так як $\Theta \geq 0,07t_0$, то можна показати що $\sigma = 0,03$.

$p_{\text{пом.зм}} = P(\Theta > \Delta/2) = 0,5 - \Phi(2,33) = 1,2 \cdot 10^{-2}$,
що, практично, відповідає значенню $9,97 \cdot 10^{-3}$.

1.7. Питання та задачі для самоперевірки

1. Яка міра інформації відповідає ентропійному підходу визначення кількості переданої інформації?
2. В яких випадках інформація вимірюється в бітах, нітах, дітах?
3. Що характеризує середня взаємна ентропія складної системи?
4. Що характеризує відносна та абсолютна надлишковість? Яка похибка буде для прикладу 1, якщо всю шкалу поділити на 25 квантів?
5. Розрахуйте значення D_b для прикладу 2, коли точки t_2 і t_3 об'єднуються в одну.

6. Яким параметром характеризується об'єднаний ансамбль складної фізичної системи?
7. Які недоліки сучасної теорії інформації, що базується на статистичних характеристиках подій?
8. Які джерела називаються ергодичними? В якому випадку ергодична послідовність є типовою?
9. Розрахуйте значення ентропії для прикладу 6, коли залежність між x_4 і x_3 буде відсутня.
10. Для прикладу 7 введіть вісім рівно ймовірних символів та розрахуйте ентропію $H(x)$.
11. Розрахуйте ентропію для прикладу 8 для випадку, коли після символу x_3 завжди передається символ x_4 .
12. Якому розподілу ймовірностей окремих повідомлень відповідає значення H_{\max} у виразі (1.24)?
13. Який параметр характеризується швидкістю створення інформації джерелом?
14. Запишіть числа 0; 1; 2; 3; 4; 5; 6; 7; 8; 9 у системах числення $m_c = 2; 3; 5; 10$.
15. Для прикладу 10 визначте надлишковість рівномірного коду мінімальної елементності.
16. Опишіть процес появи характеристичних спотворень.
17. Чим визначається виправляюча здатність приймального пристрою зі стробуванням у середині посилки за наявності зсувів ЗМВ?
18. Чим відрізняється дискретне інтегрування сигналу посилки від аналогового?
19. Що характеризує коефіцієнт групування помилок α ?
20. Наведіть приклади повідомлень при передаванні яких коефіцієнт групування є позитивним фактором, а для яких негативним?
21. Як змінюється пропускна здатність при використанні числа стнів інформаційного параметра $a > 2$?

ГЛАВА 2

СИГНАЛИ ПЕРЕДАВАННЯ ДИСКРЕТНИХ ПОВІДОМЛЕНЬ. ЗАВАДОСТІЙКІСТЬ ПРИЙМАННЯ ЕЛЕМЕНТІВ КОДОГРАМ

2.1. Сигнали та їх моделі

Широко використовуване у різноманітних сферах людської діяльності поняття «сигнал» відбиває інформаційний зміст подій, явищ, процесів. У системах електрозв'язку під сигналом розуміють процес зміни за часом величин струму, напруги, напруженості електричного та магнітного полів, що слугує для відбиття, реєстрації й передачі інформації.

Сигнали, які функціонують у реальній апаратурі, являють собою дійсні функції часу і можуть бути описані відповідними функціональними залежностями. Наприклад, сигнал, який змінюється за часом за гармонічним законом (рис. 2.1), описується аналітичною формулою:

$$s(t) = A_m \cos(2\pi f_0 t + \varphi_0), \quad -\infty < t < \infty, \quad (2.1)$$

де A_m, f_0, φ_0 відповідно – амплітуда, частота і початкова фаза сигналу.

Сигнал, який являє собою нескінченну послідовність прямокутних імпульсів тривалістю τ (мс) і постійної амплітуди A , які проходять з постійним інтервалом T (рис. 2.2), описуються функціональною залежністю

$$s(t) = \sum_{k=-\infty}^{\infty} s_{\Pi}(t - kT),$$
$$s_{\Pi}(t) = \begin{cases} A, & -\tau/2 \leq t < \tau/2, \\ 0, & -\tau/2 > t > \tau/2. \end{cases} \quad (2.2)$$

Опис сигналів за допомогою математичних формул дозволяє відобразити лише головні й істотні характеристики реальних процесів. Наприклад, описуючи гармонічний сигнал виразом (2.1), ми не враховуємо такі характеристики реального сигналу, як паразитні коливання рівня і зміна частот сигналу. Не враховуємо також форму і тривалість фронтів прямокутних імпульсів (2.2) тощо.

Таким чином, щоби уможливити аналіз, реальні процеси заміняють їхніми математичними моделями. Метод математичного моделювання є основоположним в теорії аналізу й синтезу електронних та радіотехнічних пристроїв різного призначення.

Поряд з періодичними, детермінованими за часом сигналами, у системах зв'язку функціонують і сигнали, характеристики яких точно не відомі до моменту їх реалізації й можуть бути лише завбачені з певною імовірністю. Такі сигнали називаються випадковими і їхні характеристики задаються відповідними законами розподілу. В теорії зв'язку при

моделюванні систем зв'язку широкого застосування набуває модель випадкових сигналів з гаусовим розподілом (рис. 2.3)

$$F(x) = \frac{1}{\sqrt{2\pi\sigma}} \int_{-\infty}^x \exp\left[-\frac{(\xi - m)^2}{2\sigma^2}\right] d\xi, \quad (2.3)$$

де σ – середньоквадратичне відхилення випадкової величини x ; m – математичне чекання.

Цьому закону підлягає, наприклад, амплітуда напруги теплового шуму, спричиненого нагрітими елементами пристроїв зв'язку.

У теоретичних дослідженнях, при моделюванні складних пристроїв, в яких функціонує не один сигнал, для зручності опису впроваджуються складніші моделі сигналів.

Найпоширенішим є комплексний сигнал виду

$$s(t) = A \cos 2\pi ft - jB \sin \pi ft, \quad (2.4)$$

який «природно» отримується перенесенням на комплексну площину сигналу (2.1) при $A = A_m \cos \varphi_0$ і $B = A_m \sin \varphi_0$. Скориставшись формулою Ейлера, можна перейти до експоненційної форми зображення сигналу (2.1):

$$s(t) = A_m e^{-j\varphi_0};$$

$$A_m = \sqrt{A^2 + B^2}; \varphi_0 = -\arctg \frac{B}{A}. \quad (2.5)$$

Комплексний сигнал, у якого дійсна і уявна складові пов'язані перетворенням Гільберта (аналітичний сигнал), широко використовується при описі та моделюванні алгоритмів модуляції і демодуляції сигналів систем зв'язку:

$$\begin{aligned} \dot{s}(t) &= z(t) + jz_{\Gamma}(t); \\ z_{\Gamma}(t) &= \Gamma[s(t)], \end{aligned} \quad (2.6)$$

де $\Gamma(\cdot)$ – перетворення Гільберта.

Крім двовимірних комплексних моделей використовуються також більш складні моделі сигналів – багатовимірні.

Розглянуті вище сигнали та їх моделі є неперервними функціями часу і визначені у будь-який момент часу. Такі сигнали й відповідні їхні моделі називаються аналоговими. Аналогові сигнали функціонують у пристроях і системах, алгоритми роботи яких також є неперервними функціями часу, в наслідок чого такі системи називають аналоговими. Поряд з аналоговими існують також дискретні сигнали, які функціонують в імпульсних та цифрових пристроях.

Дискретні сигнали являють собою періодичну чи випадкову послідовність імпульсів напруги (струму), певної найчастіше прямокутної форми. Однак для опису дискретних сигналів використовується модель, яка враховує лише амплітуду й час приходу (реєстрації) сигналу. Поза моментами реєстрації дискретні сигнали вважаються дорівнюваними

нулю. Таким чином, при описі дискретних сигналів абстрагуються від форми сигналів. Математичною моделлю дискретного сигналу є скінченна або нескінченна послідовність

$$\{s(t_0), s(t_1), s(t_2), \dots, s(t_m), \dots\}, m = 0, 1, \dots \quad (2.7)$$

де $s(t_m)$ – значення сигналу в момент часу t_m .

Процес перетворення аналогового сигналу в дискретний називається дискретизацією.

Дискретні сигнали, отримані рівномірною дискретизацією (інтервал часу $\Delta t = t_m - t_{m-1}$ є постійним) аналогових сигналів, аналітичне описуються відповідними функціями дискретного аргумента. Наприклад, дискретизований з частотою $F_d = 1/\Delta t = 1/4f_0$ гармонічний сигнал (2.1) описується формулою

$$s(k\Delta t) = A_m \cos(2\pi f_0 k / 4f_0 + \varphi_0), k = 0, \pm 1, \pm 2, \dots, \quad (2.8)$$

або

$$s(k) = A_m \cos(k\pi/2 + \varphi_0).$$

Графік функції (2.8) зображено на рис. 2.4.

Амплітуди відліків дискретизованого сигналу неперервні у деякому діапазоні значень напруг $-U_m < s(k) < U_m$. Для можливості цифрової обробки сигналів амплітуди відліків квантують за рівнем – подають цілим числом m із деякого вибраного діапазону чисел $-M + 1 < m \leq M - 1$. Найбільшого поширення дістало подання амплітуд числами у двійковій системі числення. Тоді

$$M = 2^n,$$

де n – кількість розрядів (позицій) коду.

Дискретизовані за часом і квантовані за амплітудою аналогові сигнали називають цифровими. Умови адекватного подання аналогових сигналів цифровими розглядатимуться далі у гл. 2.3. У цифровій формі сигнал $s(t)$ (див. рис. 2.1 та 2.4) являє собою послідовність додатних та від'ємних чисел, які кодують у двійковій формі амплітуди відліків.

Важливою теоретичною моделлю є дельта-сигнал $\delta(t)$ [8], який являє собою нескінченно короткий імпульс нескінченно великої амплітуди, одиничної площі в момент часу $t = 0$ (рис. 2.5). Аналітичне він описується δ -функцією, визначеною як границя, до якої прямує послідовність прямокутних імпульсів амплітуди k/T й тривалості T/k при $k = 1, 2, \dots$ (рис. 2.6). У корисності цієї моделі сигналу можна переконатися після розгляду гл. 2.4.

Спектральне подання сигналів. Спектральне подання сигналів є важливою формою опису сигналів. Під спектром сигналу $s(t)$ розуміють послідовність (кінцеву або нескінчену) коефіцієнтів C_i розкладення сигналу $\delta(t)$ за вибраною системою базисних функцій $\eta_i(t)$, $i = 0, 1, 2, \dots$:

$$s(t) = \sum_{i=0}^{\infty} C_i \eta_i(t), 0 \leq t \leq T. \quad (2.9)$$

Якщо система базисних функцій ортонормована

$$\int_0^T \eta_i(t) \eta_j(t) dt = \begin{cases} 1, & \text{якщо } i = j; \\ 0, & \text{якщо } i \neq j, \end{cases} \quad (2.10)$$

то спектральні складові C_i (можуть бути розраховані за формулою

$$C_i = \int_0^T s(t) \eta_i(t) dt. \quad (2.11)$$

У такому разі подання сигналу (2.9) називають узагальненим рядом Фур'є.

За базисні функції може бути вибрана будь-яка повна система функцій, наприклад функції Уолша, Хаара, поліноми Чебишева тощо. Але найбільшого поширення в техніці зв'язку набула тригонометрична система функцій, що має важливу перевагу, яка полягає в тому, що ці функції є власними функціями лінійних систем. З огляду на це гармонічні сигнали проходять через лінійні системи, зазнаючи лише тимчасову затримку й зміну амплітуди. Це зумовило зручність спектрального розкладення сигналів по гармонічним функціям. У техніці зв'язку під спектром, якщо не обумовлена спеціально система функцій, розуміється коефіцієнт розкладення сигналу за гармонічними функціями. У такому разі ряд (2.9) набуває вигляду:

$$s(t) = a_0 / 2 + \sum_{n=1}^{\infty} (a_n \cos n\omega_0 t + b_n \sin n\omega_0 t); \quad (2.12)$$

$$\omega_0 = 2\pi/T,$$

де

$$a_0 = 2/T \int_{-T/2}^{T/2} s(t) dt,$$

$$a_n = 2/T \int_{-T/2}^{T/2} s(t) \cos n\omega_0 t dt,$$

$$b_n = 2/T \int_{-T/2}^{T/2} s(t) \sin n\omega_0 t dt.$$

Спектральне подання періодичної послідовності (2.2), графік якої наведений на рис. 2.2, описується виразом

$$s(t) = A/2 + A \sum_{n=1}^{\infty} \frac{\sin \pi n / 2}{\pi n / 2} \cos n\omega_0 t. \quad (2.13)$$

Графік спектру сигналу з(1) при $m = T/2$ показано на рис. 2.7.

Значення спектральних складових періодичного сигналу (2.2) можна практично виміряти, скориставшись вузькосмуговим частотновибірним показчиком рівня (вольтметром).

У теоретичних дослідженнях, в моделюванні широко застосовується комплексне спектральне подання періодичних сигналів

$$s(t) = \sum_{n=-\infty}^{\infty} C_n e^{jn\omega_0 t}, \quad \omega_0 = 2\pi / T, \quad (2.14)$$

де

$$C_n = 1/T \int_{-T/2}^{T/2} s(t) e^{-jn\omega_0 t} dt.$$

При спрямуванні T до нескінченності ω_0 прямує до нуля. В результаті ряд (2.14) переходить в інтеграл Фур'є. Пара перетворень Фур'є (пряме й обернене) записується таким чином:

$$S(\omega) = \int_{-\infty}^{\infty} s(t) e^{-j\omega t} dt; \quad (2.15)$$

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} S(\omega) e^{j\omega t} d\omega.$$

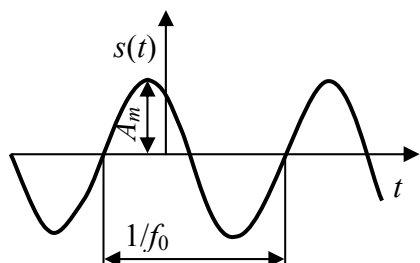


Рисунок 2.1 – Гармонічний сигнал

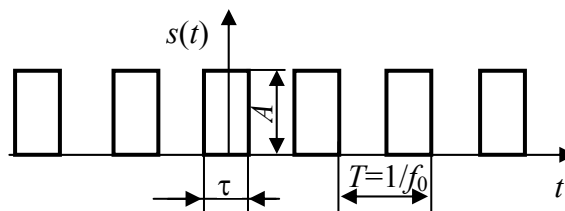


Рисунок 2.2 – Періодичний прямокутний сигнал

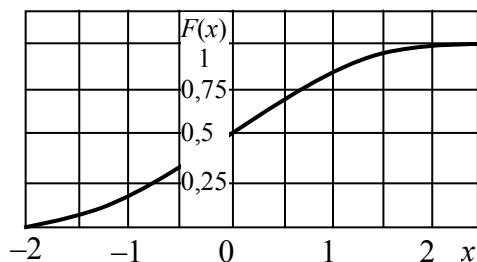


Рисунок 2.3. – Функція розподілу гаусової випадкової величини

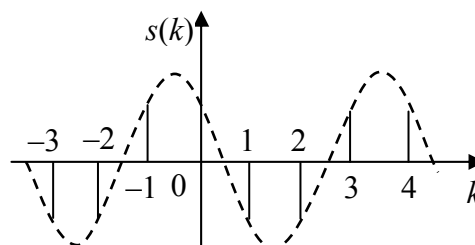


Рисунок 2.4 – Дискретизований гармонічний сигнал

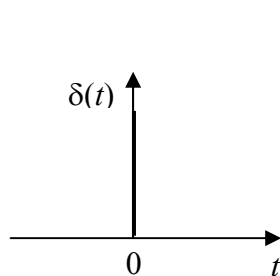


Рисунок 2.5 – δ -сигнал

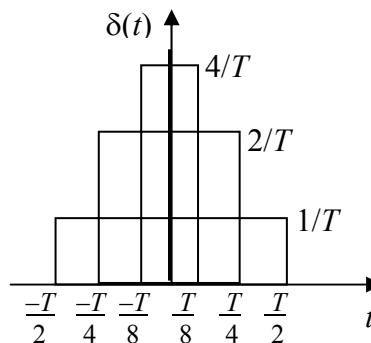


Рисунок 2.6 – Модель δ -сигналу

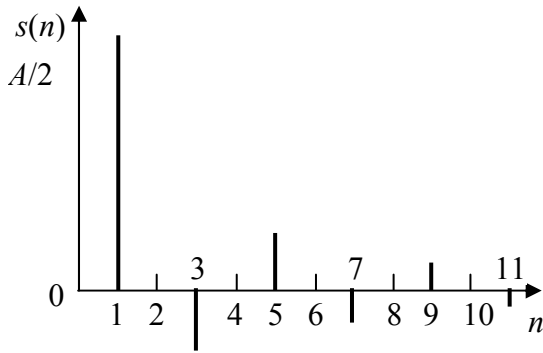


Рисунок 2.7 – Спектр періодичного прямокутного сигналу

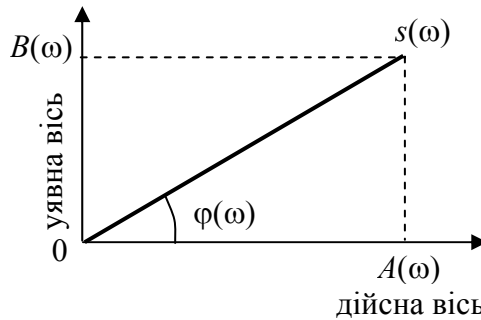


Рисунок 2.8 – Геометричний зміст комплексного сигналу

Із визначення функції $S(\omega)$ випливає її комплексний характер:

$$S(\omega) = A(\omega) + jB(\omega), \quad (2.16)$$

де

$$A(\omega) = \int_{-\infty}^{\infty} s(t) \cos \omega t dt,$$

$$B(\omega) = \int_{-\infty}^{\infty} s(t) \sin \omega t dt.$$

Тут ми почали експоненту за формулою Ейлера.

Із виразу (2.16) впливає, що через парність функції $\cos \omega t$ $A(\omega) = \text{Re } S(\omega)$ є парною функцією частоти. Аналогічно, $B(\omega) = \text{Im } S(\omega)$ є непарною функцією частоти через непарність функції $\sin \omega t$.

Комплексна функція $S(\omega)$ може бути подана у виді

$$S(\omega) = |S(\omega)| e^{j\varphi(\omega)}, \quad (2.17)$$

де у відповідності з теорією комплексних функцій

$$|S(\omega)| = \sqrt{A^2(\omega) + B^2(\omega)} \quad (2.18)$$

– модуль спектра, а

$$\varphi(\omega) = -\arctg B(\omega)/A(\omega) \quad (2.19)$$

– аргумент спектра із оберненим знаком. Геометричний зміст співвідношень (2.16) ... (2.19) ілюструє рис. 2.8.

Модуль і аргумент спектра мають цілком визначений фізичний зміст: $|S(\omega)|$ – називають амплітудно-частотною характеристикою сигналу (АЧХ), а $\varphi(\omega)$ – його фазочастотною характеристикою (ФЧХ). Дійсно, якщо розглянути довільно вибрані її частотний компонент (при $\omega = \omega_0$) сигналу (2.15) і подати його у вигляді виразу

$$S(\omega_0) e^{j\omega_0 t} = |S(\omega_0)| e^{j\varphi(\omega_0)} e^{j\omega_0 t} = |S(\omega_0)| e^{j(\omega_0 t + \varphi(\omega_0))},$$

тоді стане зрозумілим, що $|S(\omega_0)|$ визначає її амплітуду, а початкову фазу (із оберненим знаком).

Властивості спектрів. Наведемо без доведення низку відомих і важливих для подальшого вивчення властивостей спектрів.

1. Амплітудно-частотна характеристика та реальна частина спектра $S(\omega)$ довільного дійсного сигналу $s(t)$ є парними функціями частоти, а його уявна частина і фазочастотна характеристика — непарними, тобто

$$A(\omega) = A(-\omega); |S(\omega)| = |S(-\omega)|; \quad (2.20)$$

$$B(\omega) = -B(-\omega); j(\omega) = -j(-\omega). \quad (2.21)$$

2. **Теорема 1 (масштабів).** Нехай сигнал $s(t)$ має спектр $S(\omega)$. Тоді сигнал $s(\alpha t)$, де α – довільне дійсне число, має спектр $(1/\alpha)S(\omega/\alpha)$.

Цю теорему ілюструє рис. 2.9, де показані прямокутні сигнали $s(t)$ і $s(\alpha t)$, $\alpha = 2$ (рис. 2.9,а) і відповідні їм спектри $S(\omega)$ і $(1/\alpha)S(\omega/\alpha)$ (рис. 2.9,б)

Висновок 1. Перехід від дійсного сигналу $s(t)$ до інвертованого за часом сигналу $s(-t)$ призводить до перетворення спектра вихідного сигналу $S(\omega)$ в комплексно-спряжений спектр $\bar{S}(\omega)$.

Дане ствердження впливає безпосередньо із теореми масштабів і наведеної вище властивості 1 спектрів, з огляду на яку $\text{Re } S(\omega)$ – парна функція, а $\text{Im } S(\omega)$ – непарна. Дійсно, спектр сигналу $x(-t)$ має вигляд

$$\frac{1}{|-1|} S\left(\frac{\omega}{-1}\right) = \text{Re } S(-\omega) + j \text{Im } S(-\omega) = \text{Re } S(\omega) - j \text{Im } S(\omega) = \bar{S}(\omega).$$

3. **Теорема 2. (Релея-Парсєваля).** Енергія сигналу дорівнює поділеній на 1 енергії його спектра:

$$\int_0^{\infty} s^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |S(\omega)|^2 d\omega. \quad (2.22)$$

Зауваження 1. Із рівності (2.22) випливає, що енергія сигналу не залежить від його фазочастотної характеристики, оскільки остання "не бере участі" в правій частині (2.22).

4. **Теорема 3 (запізнення).** Нехай сигнал $s(t)$ має спектр $S(\omega)$. Тоді сигнал $s(t - \tau)$ (сигнал $s(t)$, спізнаний на час τ) має спектр $S(\omega)e^{-j\omega\tau}$.

Дану теорему ілюструє рис. 2.10, на якому показано проходження сигналу через лінію затримки на час τ .

5. **Теорема 4 (В. О. Котельникова).** Довільний сигнал $s(t)$, спектр $S(\omega)$ якого поза смугою частот $-\Omega < \omega < \Omega$ дорівнює 0 (такі сигнали називають смугообмеженими), може бути відновлений за своїми дискретними значеннями (відліками), взятими через інтервал часу

$$T = \pi/\Omega \quad (2.23)$$

(інтервал Котельникова), чи з подвійною верхньою частотою, оскільки періоду (2.23) відповідає частота дискретизації

$$f_d = \frac{1}{T} = \frac{\Omega}{\pi} = \frac{2\pi f_b}{\pi} = 2f_b, \quad (2.24)$$

де f_b – верхня частота в спектрі сигналу $s(t)$, Гц. Формула відновлення сигналу має вид

$$s(t) = \sum_{k=-\infty}^{\infty} s(kT) \frac{\sin \Omega(t - kT)}{\Omega(t - kT)}. \quad (2.25)$$

На рис. 2.11,а подано модуль спектра смугообмеженого сигналу, а на рис. 2.11,б – його дискретні значення, взяті у відповідності з теоремою В. О. Котельникова.

Зауваження 2. Можна показати, що сума квадратів усіх "котельниківських" відліків сигналу $s(kt)$, $k = 0, 1, 2, \dots$, пов'язана з його енергією співвідношенням

$$T \sum_{k=-\infty}^{\infty} x^2(kT) = \int_{-\infty}^{\infty} x^2(t) dt. \quad (2.26)$$

6. Теорема 5 (про згортку). Нехай маємо два сигнали $u(t)$ і $v(t)$. Введемо третій сигнал $w(t)$ за допомогою так званої формули згортки:

$$w(t) = \int_{-\infty}^{\infty} u(\tau)v(t - \tau) d\tau. \quad (2.27)$$

Тоді спектри сигналів $u(t)$, $v(t)$ і $w(t)$ пов'язані співвідношенням

$$W(\omega) = U(\omega)V(\omega).$$

7. Теорема 6 (диференціювання). Якщо сигнал $s(t)$ має спектр $S(\omega)$, то похідна сигналу

$$s'(t) = \frac{d}{dt}s(t)$$

має спектр $i\omega S(\omega)$.

8. Теорема 7 (зміщення спектра). Перемноження сигналу $s(t)$ зі спектром $S(\omega)$ на функцію $2\cos \omega_0 t$ чи $2\sin \omega_0 t$ призводить до таких наслідків:

$$\begin{aligned} \int_{-\infty}^{\infty} s(t) 2 \cos(\omega_0 t) e^{-j\omega t} dt &= S(\omega + \omega_0) + S(\omega - \omega_0); \\ \int_{-\infty}^{\infty} s(t) 2 \sin(\omega_0 t) e^{-j\omega t} dt &= jS(\omega + \omega_0) - jS(\omega - \omega_0). \end{aligned} \quad (2.28)$$

2.2. Спектри найбільш поширених сигналів

Розглянемо спектральні характеристики деяких найбільш поширених сигналів, які нам будуть потрібні в подальшому.

Дослідимо спектр прямокутного імпульсу (див. рис. 2.2) тривалістю T . Спектр імпульсу у відповідності із виразу (2.15) дорівнює

$$S(\omega) = \int_{-\infty}^{\infty} s(t) e^{-j\omega t} dt = \int_{-T/2}^{T/2} 1 e^{-j\omega t} dt = \frac{e^{-j\omega T/2} - e^{j\omega T/2}}{-j\omega} = 2 \frac{\sin \omega T / 2}{\omega}. \quad (2.29)$$

Побудуємо графік отриманого спектра (рис. 2.12). Звернемо увагу на те, що даний спектр є дійсною функцією частоти (цю властивість мають спектри усіх парних сигналів). Можна зауважити, що максимального значення функція (2.29) набуває в точці $\omega = 0$ (воно дорівнює, як легко перевірити, якщо розкрити невизначеність за правилом Лопіталя, T); інакше кажучи, найбільший «внесок» при «побудов» прямокутного імпульсу дає функція $e^{j\omega t}$ нульової частоти, так звана постійна складова. Щонайменший (нульовий) «внесок» дають комплексні експоненти з частотами $\omega = k(2\pi/T)$, $k = \pm 1, \pm 2 \dots$ коефіцієнти при них $S(k2\pi/T)$ дорівнюють нулю. Вплив на форму прямокутного сигналу експоненціальних функцій $e^{j\omega t}$ при $\omega \rightarrow \pm\infty$ стає все меншим. Дійсно, спектр цього сигналу прямує до 0 зі зростанням частоти:

$$\lim_{\omega \rightarrow \pm\infty} 2 \frac{\sin \omega T / 2}{\omega} = 0.$$

Корисно порівняти останній графік спектра зі спектром періодичної послідовності прямокутних імпульсів (див. рис. 2.7). Легко побачити, що спектри на частотах $\omega = \pi(2n - 1)/T$, $n = 1, 2, \dots$ співпадають з точністю до постійного множника, який дорівнює T .

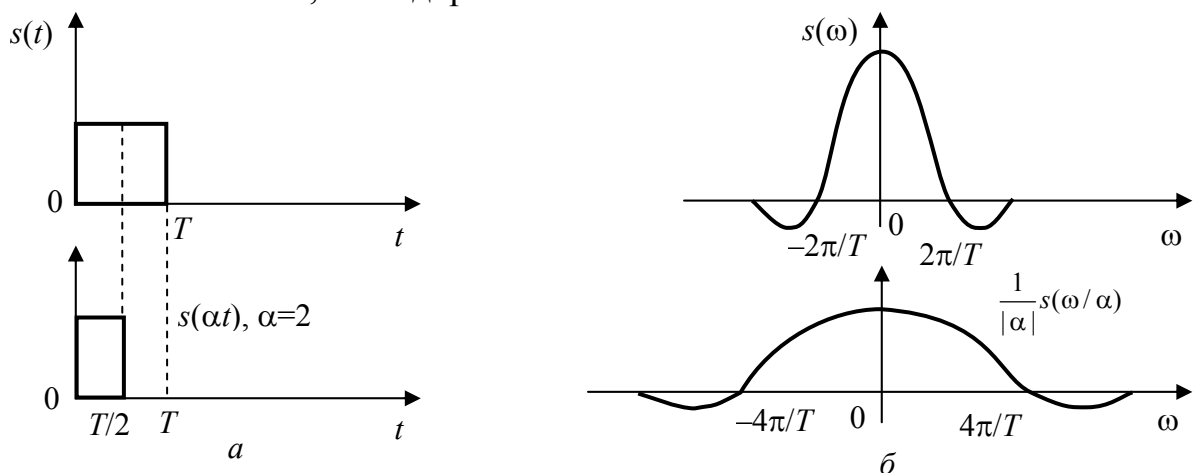


Рисунок 2.9 – Ілюстрація до теореми масштабів

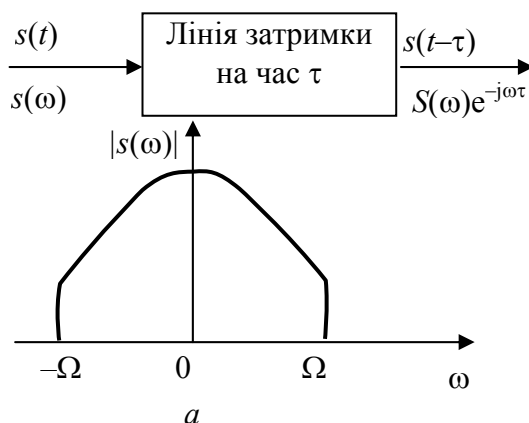


Рисунок 2.10 – Проходження сигналу через лінію затримки на час

Рисунок 2.11 – Модуль спектра смугообмеженого сигналу (а). Дискретизація смугообмеженого сигналу (б)

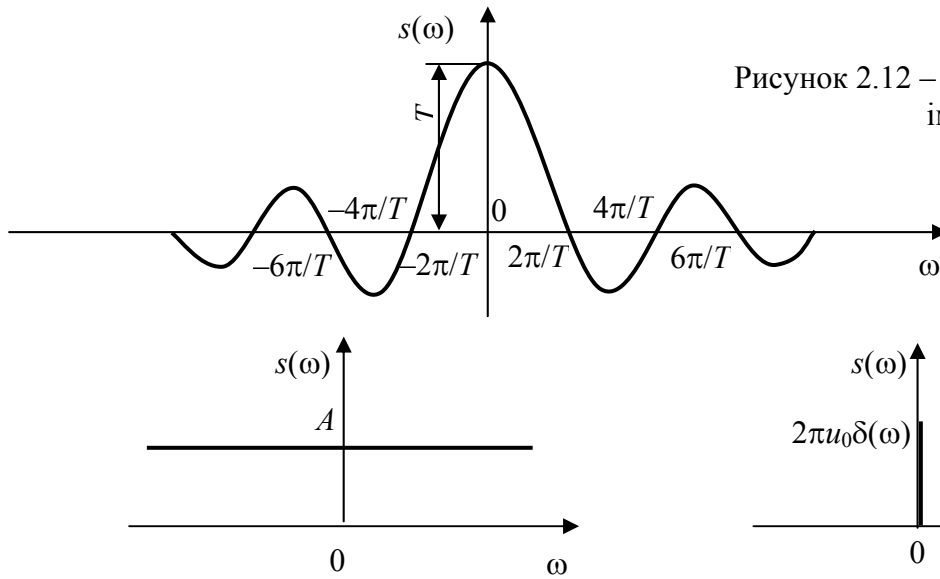


Рисунок 2.12 – Спектр прямокутного імпульсу

Рисунок 2.13 – Спектр δ -сигналу

Рисунок 2.14 – Спектр постійного за часом сигналу

Перш ніж зайнятися визначенням спектра δ -сигналу, нагадаємо одну важливу його властивість, яка дістала назву фільтруючої властивості дельта-функції. Можна довести справедливість такого співвідношення [8]:

$$s(t) = \int_{-\infty}^{\infty} s(\tau)\delta(t - \tau)d\tau. \quad (2.30)$$

Інтуїтивно відчувається справедливість цього співвідношення, якщо згадати, що δ -функція визначена лише при $t = 0$. Тому інтегрування за τ дорівнює значенню $s(\tau)$ при $\tau = t$. Спираючись на цю властивість δ -функції, визначимо спектр δ -сигналу:

$$s(t) = A\delta(t);$$

$$S(\omega) = \int_{-\infty}^{\infty} A\delta(t)e^{-j\omega t} dt = A \int_{-\infty}^{\infty} e^{-j\omega t} \delta(0 - t) dt = Ae^{-j\omega 0} = A = \text{const}. \quad (2.31)$$

Спектр δ -сигналу є рівномірним на усіх частотах (рис. 2.13).

Легко перевірити, що спектр постійного у часі сигналу $u(t) = u_0 = \text{const}$, описується виразом

$$S(\omega) = 2\pi u_0 \delta(\omega). \quad (2.32)$$

Для цього достатньо вираз для спектра (2.32) підставити у формулу оберненого перетворення Фур'є (2.15) і знову скористатись властивістю δ -функції.

Із виразу (2.32) випливає, що спектр постійного у часі сигналу зосереджений на нульовій частоті ($\omega = 0$). Графік спектра є дельта-функцією (рис. 2.14).

Спектр комплексного експоненціального сигналу $s(t) = e^{j\omega_0 t}$ описується виразом $S(\omega) = 2\pi\delta(\omega - \omega_0)$, що перевіряється виконанням співвідношення

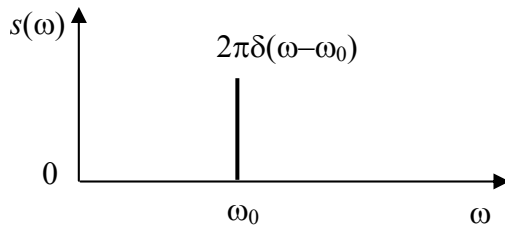


Рисунок 2.15 – Спектр експоненціального сигналу

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} 2\pi\delta(\omega - \omega_0) e^{j\omega t} d\omega.$$

Графік спектра є дельта-функцією на частоті ω_0 (рис. 2.15). Враховуючи останній результат і відомий вираз тригонометричних функцій через експоненціальний за формулою Ейлера запишемо вирази для спектрів косинусоїдального сигналу

$$S_c(\omega) = \pi[\delta(\omega - \omega_0) + \delta(\omega + \omega_0)] \quad (2.33)$$

і синусоїдального сигналу:

$$S_s(\omega) = -j\pi[\delta(\omega - \omega_0) + \delta(\omega + \omega_0)]. \quad (2.34)$$

Графіки спектрів наведені на рис. 2.16, а і б.

Розглянемо перетворення Фур'є періодичного сигналу $s(t)$ довільної форми. Раніше ми вже наводили розклад періодичного сигналу в комплексний ряд Фур'є

$$s(t) = \sum_{n=-\infty}^{\infty} C_n e^{jn\omega_1 t},$$

де $\omega_1 = 2\pi/T$; T – період.

Пряме перетворення Фур'є $s(t)$ має вигляд

$$S(\omega) = \int_{-\infty}^{\infty} \left(\sum_{n=-\infty}^{\infty} C_n e^{jn\omega_1 t} \right) e^{-j\omega t} dt.$$

Перетворимо останній вираз:

$$S(\omega) = \sum_{n=-\infty}^{\infty} C_n \int_{-\infty}^{\infty} e^{jn\omega_1 t} e^{-j\omega t} dt = 2\pi \sum_{n=-\infty}^{\infty} C_n \delta(\omega - n\omega_1). \quad (2.35)$$

Ми скористались виразом для спектра експоненціального сигналу.

Періодична послідовність δ -сигналів аналітично описується виразом

$$\eta(t) = \sum_{k=-\infty}^{\infty} \delta(t - kT), \quad (2.36)$$

T – період.

Визначимо його спектр, для чого скористаємося знову поданням $\eta(t)$ через комплексний ряд Фур'є

$$\eta(t) = \sum_{k=-\infty}^{\infty} C_n e^{j2\pi nt/T};$$

$$C_n = \frac{1}{T} \int_{-\infty}^{\infty} \eta(t) e^{-j2\pi nt/T} dt = \frac{1}{T} \int_{-\infty}^{\infty} \left[\sum_{n=-\infty}^{\infty} \delta(t - kT) \right] e^{-j2\pi nt/T} dt =$$

$$= \frac{1}{T} \sum_{n=-\infty}^{\infty} \int_{-T/2}^{T/2} \delta(t - kT) e^{-j2\pi nt/T} dt = \frac{1}{T}.$$

Скористаємось тепер виразом (2.35), підставивши в нього значення $C_n = 1/T$:

$$S_{\eta}(\omega) = 2\pi / T \sum_{n=-\infty}^{\infty} \delta\left(\omega - n \frac{2\pi}{T}\right). \quad (2.37)$$

Таким чином, спектр періодичної послідовності δ -сигналів є періодичною послідовністю δ -функцій в частотній області (рис. 2.17).

Передаточні функції та імпульсні реакції лінійних систем.

Визначення 1. Лінійною системою (колом) називають «чорну скриньку» (пристрій із входом і виходом, внутрішня структура якого може бути невідомою) (рис. 2.18), що задовольняє таким умовам:

1) якщо сигнал $s(t)$ на вході «чорної скриньки» породжує сигнал $y(t)$ на його виході, то при поданні на вхід сигналу $\alpha s(t)$, $\alpha = \text{const}$, на виході дістанемо $\alpha y(t)$;

2) якщо сигнали $s_1(t)$ і $s_2(t)$ на вході "чорної скриньки" породжують на виході сигнали $y_1(t)$ і $y_2(t)$ відповідно, то при поданні на вхід сигналу $s_1(t) + s_2(t)$ на виході дістанемо $y_1(t) + y_2(t)$.

Якщо лінійна система задовольняє умові стаціонарності, тобто її властивості й параметри незмінні у часі, то сигнали на її вході $s(t)$ і на виході $y(t)$ пов'язані згадуваним вище співвідношенням згортки (2.27):

$$y(t) = \int_{-\infty}^{\infty} s(\tau) h(t - \tau) d\tau = \int_{-\infty}^{\infty} h(\tau) s(t - \tau) d\tau,$$

де $h(t)$ – імпульсна реакція цієї системи. Нагадаємо у чому сутність поняття «імпульсна реакція».

Визначення 2. Імпульсною реакцією називають відгук системи на вхідний сигнал у вигляді δ -функції (рис. 2.19). Якщо імпульсна реакція характеризує поведінку лінійної системи в часовій області, то для її опису в частотній області використовують передаточну функцію.

Визначення 3. Перетворення Фур'є від імпульсної реакції називають передаточною функцією:

$$H(\omega) = \int_{-\infty}^{\infty} h(t) e^{-j\omega t} dt. \quad (2.38)$$

З огляду на згадану вище теорему про згортку між вхідним і вихідним спектрами лінійної стаціонарної системи (таку систему часто називають

системою із інваріантними у часі параметрами) існує вельми простий зв'язок (див. рис. 2.18):

$$Y(\omega) = S(\omega)H(\omega). \quad (2.39)$$

Зауваження 3. Іноді передаточну функцію впроваджують за допомогою рівності (2.39), визначаючи цю функцію як відношення спектра на виході лінійної стаціонарної системи до спектра на вході цієї системи:

$$H(\omega) = Y(\omega)/S(\omega). \quad (2.40)$$

Впроваджена таким чином передаточна функція задовольняє, як неважко перевірити, рівності (2.38).

Зауваження 4. Безпосередньою перевіркою можна встановити, що парній імпульсній реакції $h(t)$ відповідає парна дійсна передаточна функція $H(\omega)$, а непарній імпульсній реакції – уявна передаточна функція. За аналогією з амплітудно- і фазочастотними характеристиками (формули (2.18), (2.19)), які має спектр довільного сигналу, для передаточної функції лінійної системи

$$H(\omega) = |H(\omega)|e^{-j\varphi(\omega)} \quad (2.41)$$

впроваджують амплітудно-частотну характеристику $|H(\omega)|$ і фазочастотну характеристику $\varphi(\omega)$. Великого поширення набула тісно пов'язана з ФЧХ характеристика групового часу проходження (ГЧП):

$$\tau(\omega) = d\varphi(\omega)/d\omega. \quad (2.42)$$

Оскільки неспотворююча (ідеальна) передаточна функція повинна тотожно дорівнювати одиниці (при цьому з огляду на (2.39) спектри, отже і сигнали, на вході та виході лінійної системи збігаються):

$$H(\omega) = 1, \quad -\infty < \omega < \infty, \quad (2.43)$$

то для неспотворюючих АЧХ, ФЧХ та ГЧП дістаємо співвідношення

$$\left. \begin{aligned} |H_{ig}(\omega)| &= 1, \\ \varphi_{ig}(\omega) &= 0, \\ \tau_{ig}(\omega) &= 0, \end{aligned} \right\}, \quad -\infty < \omega < \infty \quad (2.44)$$

На практиці, однак, підсиленням (ослабленням), а також запізненням сигналу (при збереженні його форми незмінною) в багатьох випадках можна знехтувати, і систему з передаточною функцією $Ae^{-j\omega\tau_0}$, $A = \text{const}$, $\tau_0 = \text{const}$ вважати неспотворюючим колом. Тому за ідеальні часто розглядають характеристики, подані на рис. 2.20:

$$\left. \begin{aligned} |H_{ig}(\omega)| &= A, \\ \varphi_{ig}(\omega) &= \omega\tau_0, \\ \tau_{ig}(\omega) &= \frac{d(\omega\tau_0)}{d\omega} = \tau_0, \\ \tau_0 &= \text{const}. \end{aligned} \right\}, \quad -\infty < \omega < \infty \quad (2.45)$$

Якщо порушується хоча б одна з цих умов, вихідний сигнал відрізнятиметься за формою від вхідного. Так, спотворення АЧХ типу «завал» високих частот призводить до подовження часу наростання фронтів імпульсів (фронти стають пологими). До збільшення тривалості фронтів приводять також спотворення ФЧХ чи ГЧП. Характерною ознакою спотворень ФЧХ чи ГЧП є поява асиметрії вихідного сигналу за умови, що вхідний сигнал був парно симетричний.

2.3. Сигнали дискретного часу та цифрова фільтрація

Враховуючи важливість дискретного подання сигналів та спектрів, розглянемо докладніше ефекти, пов'язані з дискретизацією сигналів. Теорема Котельникова визначає умови однозначного подання аналогового сигналу $s(t)$ дискретним $s(kT)$ (2.25). Однак при цьому залишаються нерозкритими перетворення його спектра.

Процес дискретизації неперервного сигналу $s(t)$, $-\infty < t < \infty$, який має смугообмежений спектр $S(\omega)$, $-\Omega < \omega < \Omega$, може бути описаний як добуток $s(t)$ і періодичної послідовності δ -сигналів (2.36):

$$s(kT) = s(t) \sum_{k=-\infty}^{\infty} \delta(t - kT), \quad T = \pi/\Omega. \quad (2.46)$$

Спектр дискретного сигналу з може бути знайдений шляхом згортки відповідно до спектрів помножуваних сигналів

$$S_A(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} S(v) S_{\eta}(\omega - v) dv. \quad (2.47)$$

Підставимо вираз (2.37) в рівняння (2.47) і після нескладних перетворень отримаємо

$$\begin{aligned} S_A(\omega) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \left[S(v) \frac{2\pi}{T} \sum_{n=-\infty}^{\infty} \delta\left(\omega - \frac{2\pi n}{T} - v\right) \right] dv = \\ &= \frac{1}{T} \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} S(v) \delta\left(\omega - \frac{2\pi n}{T} - v\right) dv = \frac{1}{T} \sum_{n=-\infty}^{\infty} S\left(\omega - \frac{2\pi n}{T}\right) = \frac{1}{T} \sum_{n=-\infty}^{\infty} S(\omega - n\Omega_A), \end{aligned} \quad (2.45)$$

$$\Omega_A = 2\pi/T,$$

де Ω_A – частота дискретизації.

Отже, спектр дискретного сигналу $s(kT)$, $k = 0, \pm 1, \pm 2, \dots$ дорівнює сумі зсуень спектра $s(t)$ неперервного сигналу (рис. 2.21,а). Рис. 2.21,б ілюструє випадок $\Omega_A = 2\Omega$, рис. 2.21,в – випадок $\Omega_A < 2\Omega$ і рис. 2.21,г – випадок $\Omega_A > 2\Omega$. Видно, що при $\Omega_A < 2\Omega$ виникає перекриття спектрів сигналу, яке не дозволяє встановити початковий неперервний сигнал. Таким чином стає більш наочним зміст теореми Котельникова.

Дискретизація неперервних сигналів і квантування амплітуд отриманих дискретних відліків $s(kT)$ на певну кількість рівнів дозволяє перейти від аналогового спектра до цифрового й обробляти його за допомогою універсальних ЕОМ або спеціалізованих цифрових процесорів. Одним із найпоширеніших пристроїв в апаратурі зв'язку є фільтр. Із загальних позицій будь-яке лінійне коло з постійними параметрами можна подати у вигляді чотиріполосника (фільтра), описаного імпульсною реакцією або передаточною функцією. Враховуючи важливість фільтра як універсальної моделі лінійної системи, розглянемо фільтрацію за допомогою цифрового фільтра.

Практично цифрова фільтрація аналогових сигналів здійснюється у відповідності зі структурною схемою, зображеною на рис. 2.22. Аналоговий сигнал $s(t)$ надходить на вхід аналого-цифрового перетворювача (АЦП), на виході якого з'являються взяті у відповідності із теоремою Котельникова відліки $s(kT)$, $k = 0, +1, \dots$, (рис. 2.23); при цьому інтервал дискретизації T вибирається меншим чи дорівнюючим $0,5/f_v$, де f_v – верхня частота в спектрі сигналу $s(t)$. Реально АЦП видає відліки $s(kT)$, $k = 0, +1, \dots$ в цифровій формі, тобто у вигляді комбінацій двійкового коду, тому кожна комбінація цього коду є поданням відповідного відліку в двійковій системі числення. Точність такого опису дискретних відліків сигналу $s(t)$, як вже говорилося, залежить від кількості розрядів у кодових комбінаціях і в принципі може бути як завгодно високою. В подальшому будемо нехтувати ефектами, викликаними збереженням лише кінцевої кількості розрядів в двійковому запису відліків $s(kT)$. Це скорочене подання відлічених значень аналогового сигналу здійснюється в АЦП за допомогою операцій квантування і округлення.

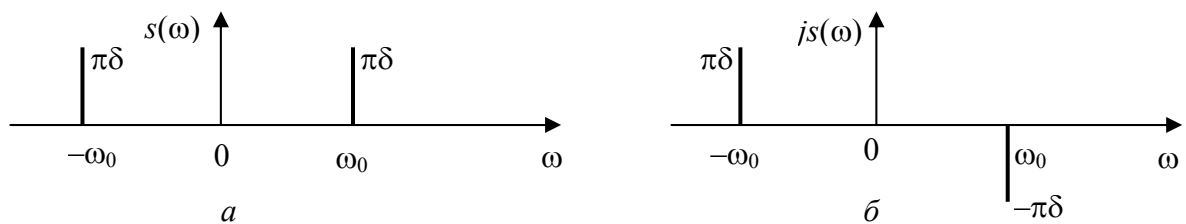


Рисунок 2.16 – Комплексні спектри гармонічних сигналів

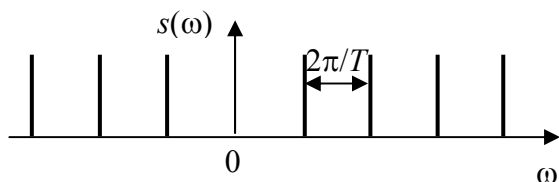


Рисунок 2.17 – Спектр періодичної послідовності δ -сигналів

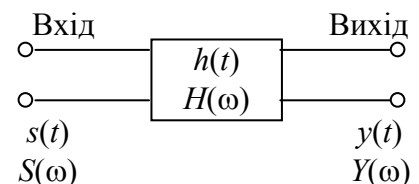


Рисунок 2.18 – Лінійна система

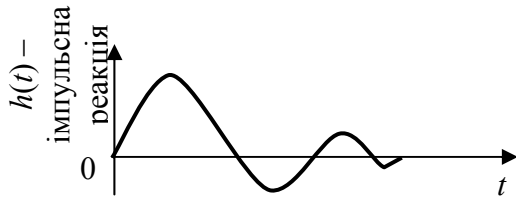


Рисунок 2.19 – Імпульсна реакція лінійної системи

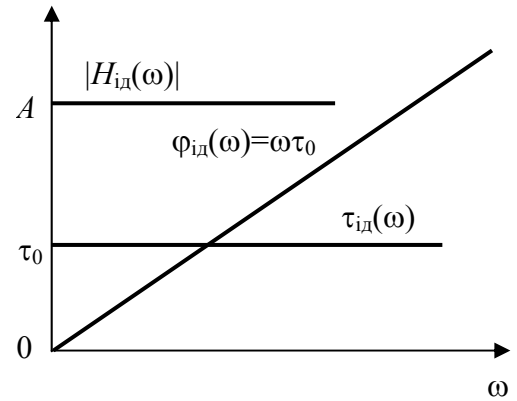


Рисунок 2.20 – Ідеальні характеристики лінійної системи

Послідовність відліків $s(kT)$, $k = 0, +1, \dots$, з виходу АЦП надходить на вхід цифрового фільтра (ЦФ), який за заданим алгоритмом "перераховує" її в послідовність вихідних відліків $y(kT)$, $k = 0, +1, \dots$, подавляючи чи підсилюючи при цьому ті чи інші частотні компоненти сигналу $s(t)$. Зрозуміло, вихідна послідовність відліків ЦФ $y(kT)$, $k = 0, +1, \dots$, також являє собою послідовність кодових комбінацій двійкового коду. За цими комбінаціями цифро-аналоговий перетворювач (ЦАП) відновлює імпульси прямокутної форми, амплітуда яких з точністю дорівнює записаним в двійковій системі числення значенням $y(kT)$, $k = 0, +1, \dots$. Аналоговий сигнал $y(t)$ знаходять за його відліками за допомогою фільтра-інтерполятора, який наближено реалізує співвідношення із теореми Котельникова – формулу (2.25), відновлюючи смугообмежений сигнал за його відліками. Інтерполятор і ЦАП можна об'єднати в один вузол (штрихова лінія на рис. 2.23), здійснюючий перетворення кодових комбінацій у відфільтрований аналоговий сигнал.

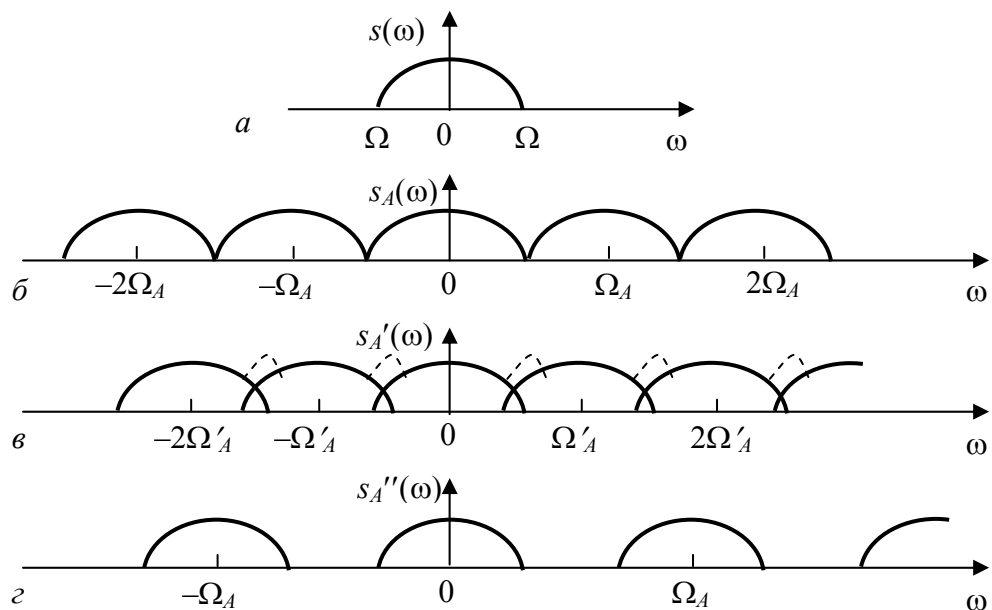


Рисунок 2.21 – Перетворення спектру сигналу при дискретизації

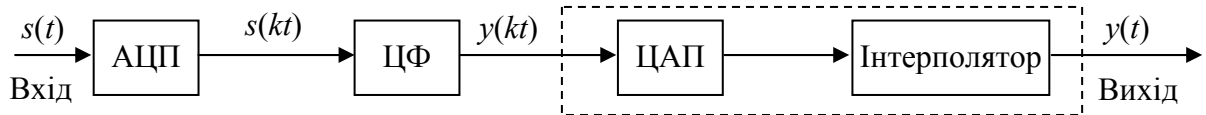


Рисунок 2.22 – Структурна схема цифрового фільтра

Операції, виконувані АЦП, ЦАП і фільтром-інтерполятором, в багатьох випадках стандартні і незалежні від призначення й властивостей цифрового фільтра, тоді як його характеристики й параметри значною мірою визначаються конкретною задачею фільтрації, яку розв'язує даний ЦФ.

Як відомо, теорія лінійних систем з дискретним часом є подібною до теорії лінійних аналогових систем.

Для дискретних лінійних стаціонарних (тобто, таких, які не змінюють з протягом часу своїх характеристик) систем введено поняття імпульсної реакції (часто говорять імпульсної характеристики), що являє собою відгук $g(kT)$, $k = 0, +1, \dots$ (рис. 2.24) на вхідний вплив виду

$$u(kT) = \begin{cases} 1, & k = 0, \\ 0, & k = \pm 1, \pm 2, \dots, \end{cases} \quad (2.49)$$

зображений на рис. 2.25, який відіграє роль δ -функції в теорії лінійних аналогових систем.

Розглянемо для спрощення вхідний сигнал цифрового фільтра у вигляді кінцевої послідовності відліків

$$s(0), s(T), \dots, s[(N-1)T]. \quad (2.50)$$

Зазначимо, що m -й член послідовності відліків (2.50) – $s(mT)$ точно в $s(mT)$ разів більше (чи менше) за сигнал (2.49); поза тим, він запізнюється на mT секунд у порівнянні із сигналом на рис. 2.25. Отже, при поданні на вхід лінійного цифрового фільтра такого сигналу на його виході дістанемо відгук

$$s(mT)g(kT - mT), \quad m = 0, \pm 1, \pm 2, \dots, N-1, \quad (2.51)$$

де $g(kT)$, $k = 0, +1, \dots$, – імпульсна реакція розглянутого фільтра.

При поданні ж на вхід цього ЦФ всієї послідовності (2.50) дістанемо, спираючись, як і раніше, на визначення у вигляді суми відгуків типу (2.51):

$$y(kT) = \sum_{m=0}^{N-1} s(mT)g(kT - mT), \quad k = 0, 1, \dots \quad (2.52)$$

Співвідношення (2.52), яке є дискретним аналогом рівності (2.27), називають його дискретною згорткою. Важливість його полягає у тому, що, як випливає із виразу (2.52), довільна лінійна стаціонарна обробка сигналів може бути виконаною в цифровій формі за допомогою наступних відносно простих операцій зсувів, множень та додавань.

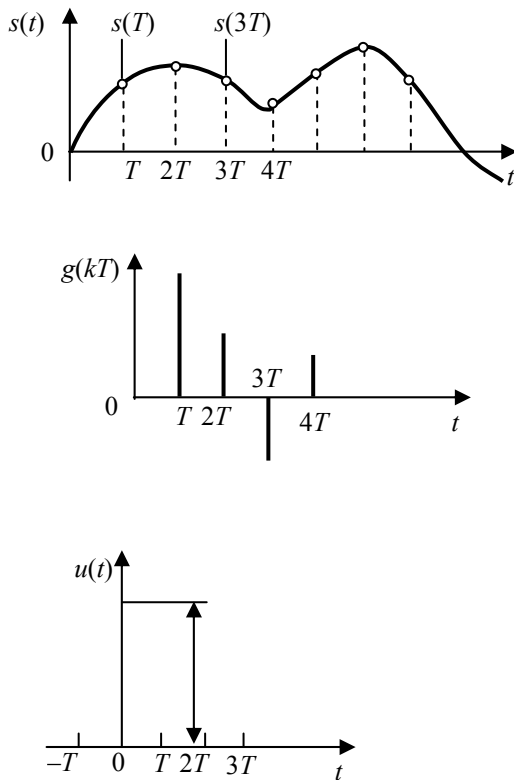


Рисунок 2.25 – Дискретний аналог δ -функції

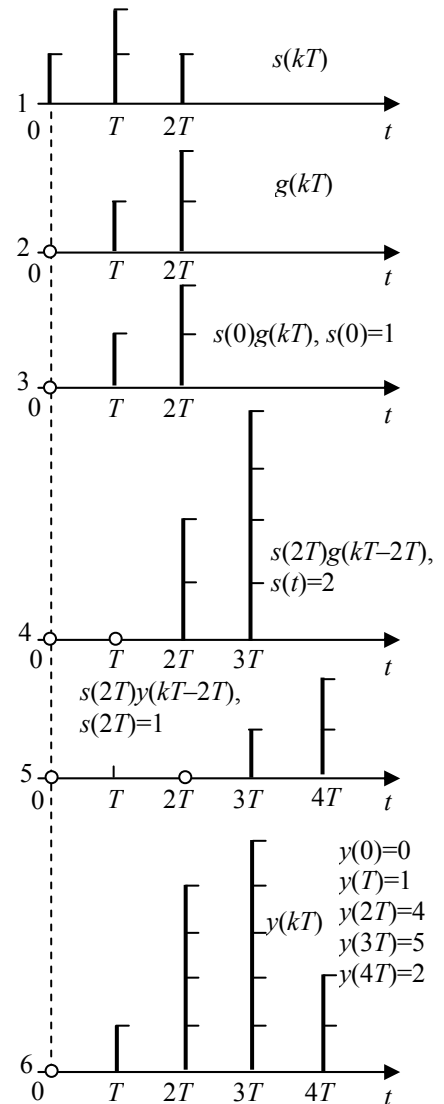


Рисунок 2.26 – Згортка сигналу $s(kT)$ з імпульсною реакцією $g(kT)$

Порядок, в якому повинні виконуватись ці операції, пояснює рис. 2.26, на якому подано "проходження" сигналу $s(kT)$, $k = 0, +1, \dots$, що має три відмінні від 0 відліки (рядок 1), через ЦФ з імпульсною реакцією $g(kT)$, $k = 0, +1, \dots$, з двома ненульовими відліками (рядок 2). Рядки 3 ... 5 даного рисунка стримані у відповідності з виразом (2.51), а на рядку 6 показано вихідний сигнал ЦФ $y(kT)$, $k = 0, +1, \dots$, який визначається як сума дискретних сигналів рядків 3 ... 5.

Зрозуміло, значення нескінченної кількості відліків $g(kT)$, $k = 0, +1, \dots$, не можуть бути впроваджені в цифрову пам'ять безпосередньо. В такому разі в пам'ять записують кінцеву кількість параметрів, що реалізують непрямим шляхом нескінченну імпульсну характеристику. Легко перевірити, що структурна схема (рис 2.27) відповідає алгоритму дискретної згортки (2.52) при кінцевій довжині імпульсної характеристики (кількість її відмінних від 0 відліків дорівнює M). Квадрати з розміщеною в

них буквою T є комірками пам'яті, в яких здійснюється затримка сигналу на час T , а рівнобедрений трикутник з записаним поруч літерним виразом $g(kT)$ символізує операцію множення на число $g(kT)$ відліку вхідного сигналу, який знаходиться в відповідній комірці пам'яті.

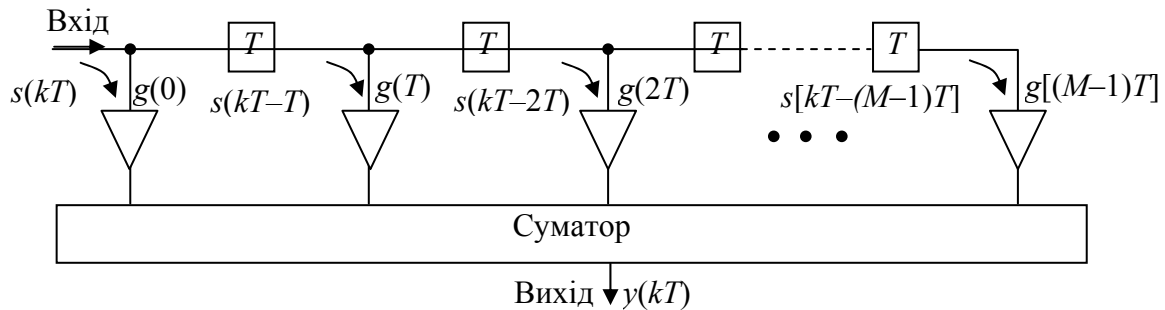


Рисунок 2.27 – Структурна схема СІХ-фільтра

Таким чином, можна сказати, що на рис. 2.27 подана структурна схема алгоритму СІХ-фільтрації. Для її реалізації необхідні регістр зсуву, утворений каскадним сполученням комірок пам'яті (квадратів з літерою T , див. рис. 2.27), помножувач і суматор. Названі функціональні вузли припускають просту реалізацію алгоритму на мікропроцесорах різного типу.

За допомогою теореми 2.3 (запізнення) неважко показати, що передаточна функція фільтра за схемою рис. 2.27 має вигляд

$$G(e^{j\omega T}) = \sum_{k=0}^{M-1} g(kT)e^{-j\omega kT}. \quad (2.53)$$

Формула (2.53) записана стосовно випадку обробки дискретного сигналу за допомогою ЦФ. Щоби підкреслити цю обставину, за аргумент передаточної функції беруть експоненту $e^{j\omega T}$, а не просто частоту, як це прийнято робити в передаточних функціях аналогових кіл.

На закінчення відзначимо деякі загальні положення. Для сигналу дискретного часу $s(kT)$, $k = 0, +1, \dots$, перетворення Фур'є (спектр) впроваджують за допомогою рівності

$$S(e^{j\omega T}) = \sum_{k=-\infty}^{\infty} s(kT)e^{-j\omega kT}. \quad (2.54)$$

Функція $S(e^{j\omega T})$ є, очевидно, сумою ряду Фур'є і тому періодичною з періодом $2\pi/T$.

Сигнал $s(kT)$ може бути відновлений за своїм спектром згідно з формулою

$$s(kT) = \frac{1}{2\pi} \int_{-T/2}^{T/2} S(e^{j\omega T}) e^{j\omega kT} d\omega; \quad k = 0, \pm 1, \dots, \quad (2.55)$$

яка є аналогом рівності (2.15) – оберненого перетворення Фур'є. Для систем з дискретним часом зв'язок між спектрами вхідного сигналу $s(kT)$

вихідного сигналу $y(kT)$ і передаточною функцією $G(e^{j\omega T})$ фільтра описується подібним до виразу (2.39) співвідношенням

$$Y(e^{j\omega T}) = S(e^{j\omega T})G(e^{j\omega T}). \quad (2.56)$$

2.4. Математичні моделі вузлів апаратури зв'язку

Напевне, найбільш поширеним вузлом після фільтра в апаратурі зв'язку є модулятор. Модулятор здійснює зміну параметрів (амплітуди, частоти, фази і тощо) модульованого (несучого) сигналу за законом модулюючого сигналу. Найпростіший амплітудний модулятор (рис. 2.29) здійснює множення несучого гармонічного сигналу $s(t) = A \cos \omega_0 t$ на модулюючий сигнал $s_M(t)$, $-\infty < t < \infty$:

$$s = A \cos \omega_0 t \cdot s_M(t) = A_M \cos \omega_0 t; \quad (2.57)$$

$$A_M = A s_M(t).$$

Для обчислення спектра модульованого сигналу (2.57) необхідно здійснити згортку спектра (2.33) зі спектром $S_M(\omega)$

$$S_M(\omega) = \frac{1}{2\pi} \int_{-T/2}^{T/2} s(t) e^{-j\omega t} dt; \quad -\Omega < \omega < \Omega; \quad (2.58)$$

$$S(\omega) = S_M(\omega) \otimes A\pi[\delta(\omega - \omega_0) + \delta(\omega + \omega_0)].$$

\otimes – символ згортки.

$$S(\omega) = A\pi[S_M(\omega - \omega_0) + S_M(\omega + \omega_0)]. \quad (2.59)$$

Графіки спектрів несучого, модулюючого та результуючого сигналів подані на рис. 2.30. Із спектрального опису процесу амплітудної модуляції випливає, що спектр модульованого сигналу зміщується в область додатних та від'ємних частот на ω_0 .

Отже, математичною моделлю амплітудного модулятора може слугувати вираз (2.57) в часовій області або (2.59) – в частотній.

У системах передачі дискретної інформації (моделях) широко використовується квадратурна амплітудна модуляція (КАМ). У такому разі модулятор передавача на кожному тактовому інтервалі формує сигнал з вибраного двовимірного ансамблю сигналів. Приклад шістнадцяти-точкового сузір'я КАМ-16 подано на рис. 2.31. Функціональна схема такого модулятора показана на рис. 2.32.

Математична модель квадратурного модулятора описується виразом

$$s(t) = A_i \cos \omega_0 t + B_i \sin \omega_0 t, \quad -\frac{T}{2} < t < \frac{T}{2}, \quad (2.60)$$

де A_i , B_i – інформаційні параметри, які набувають значення ± 1 , ± 3 ; T – тривалість тактового інтервалу.

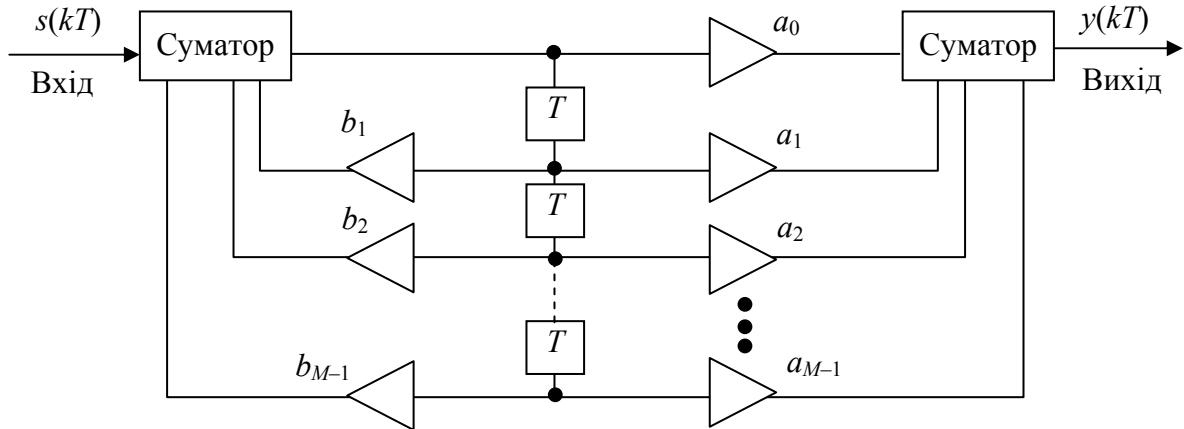


Рисунок 2.28 – Структурна схема НІХ-фільтра

Опис сигналу (2.60) в частотній області можна знайти, скориставшись виразами (2.33) і (2.34) за аналогією з висновком виразу (2.59):

$$S(\omega) = \pi A_i [S_M(\omega - \omega_0) + S_M(\omega + \omega_0)] - j\pi B_i [S_M(\omega - \omega_0) + S_M(\omega + \omega_0)] = \pi [S_M(\omega - \omega_0)(A_i - jB_i) + S_M(\omega + \omega_0)(A_i + jB_i)]. \quad (2.61)$$

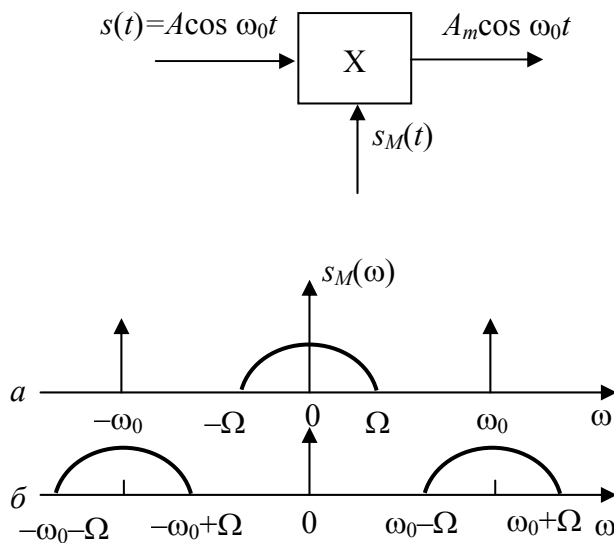


Рисунок 2.30 – Спектри: *a* – несучого та модулюючого сигналів; *b* – модульованого сигналу

Рисунок 2.29 – Амплітудний модулятор

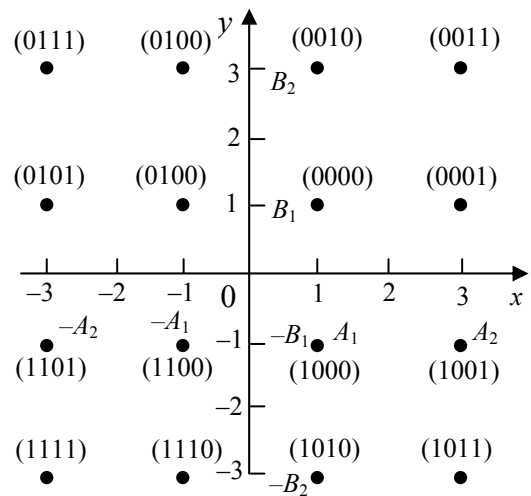
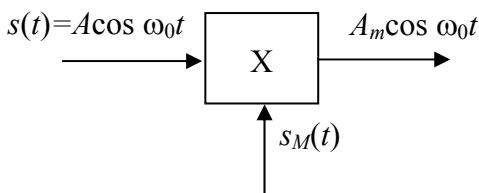


Рисунок 2.31 – Сигнальне сузір'я КАМ-16

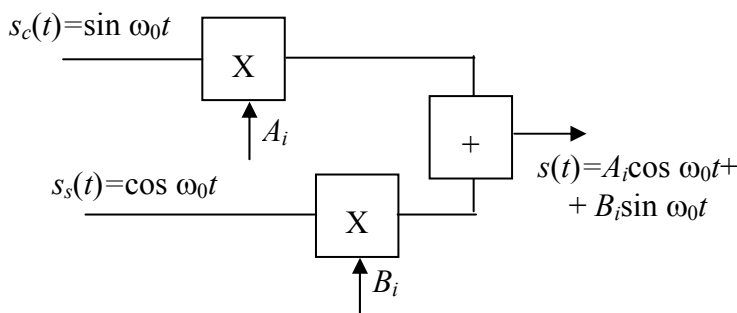


Рисунок 2.32 – Квадратурний модулятор

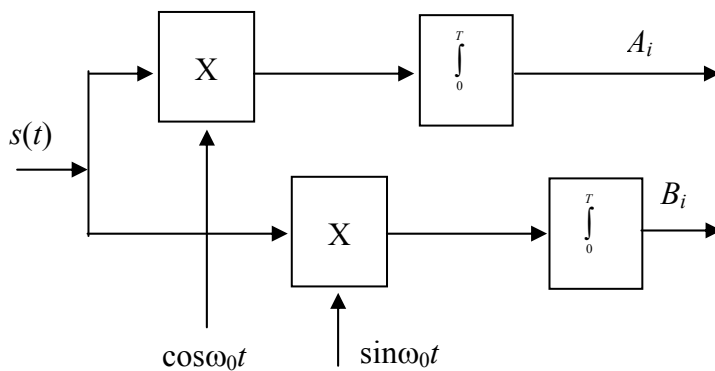


Рисунок 2.33 – Демодулятор сигналів КАМ

На приймальній стороні для вилучення передаваних інформаційних параметрів A_i , B_i треба сигнал $s(t)$ окремо помножити з опорними несучими сигналами, а результати проінтегрувати (рис. 2.33):

$$X = \frac{2}{T} \int_0^T s(t) \cos \omega_0 t dt = A_i;$$

$$Y = \frac{2}{T} \int_0^T s(t) \sin \omega_0 t dt = B_i \quad (2.62)$$

Розглянемо модель складнішої системи передачі дискретної інформації – багатоканального (паралельного) модема (БМ). Передавач БМ складається з N квадратурних модуляторів (див.рис.2.32), а приймач – відповідно із N ко-реляторів (див. рис. 2.33), причому N може досягати величин порядку тисячі. Несучі сигнали БМ являють собою відрізки гармонійних сигналів кратних частот

$$\begin{cases} \cos n\omega_0 t \\ \sin n\omega_0 t \end{cases}, \quad 0 < t \leq T, n = 1, 2, \dots, N; \omega_0 = 2\pi/T.$$

У такому разі забезпечується їх ортогональність на інтервалі часу T , що дозволяє поділити сигнали на прийомі за допомогою кореляційної обробки (2.62).

Модель сигналу передавача описується виразом

$$s(t) = \sum_{n=1}^N A_{n_i} \cos n\omega_0 t + B_{n_i} \sin n\omega_0 t, \quad 0 < t \leq T. \quad (2.64)$$

Демодуляція сигналу (2.64) виконується за алгоритмом

$$X = \frac{2}{T} \int_0^T s(t) \cos I\omega_0 t dt = \begin{cases} A_{n_i}, & n = 1; I = 1, 2, \dots, N; \\ 0, & n \neq 1; \end{cases};$$

$$Y = \frac{2}{T} \int_0^T s(t) \sin I\omega_0 t dt = \begin{cases} B_{n_i}, & n = 1; i = 1, 2, \dots, N; \\ 0, & n \neq 1. \end{cases} \quad (2.65)$$

Виконання операцій модуляції (2.64) і демодуляції (2.65) при великому N вимагає досить складного обладнання. Однак при цифровій

реалізації БМ було знайдено (16) вельми ефективні алгоритми модуляції–демодуляції на основі швидких методів обчислення дискретного перетворення Фур'є (ДПФ).

Не розглядаючи докладно і зберігаючи попередні позначення, подамо алгоритм модуляції й демодуляції сигналів БМ із застосуванням ДПФ:

$$s(k) = \operatorname{Re} \left[\sum_{j=0}^{N_0-1} C_j e^{j \frac{2\pi}{N_0} l k} \right], \quad i_0 = t/\Delta t;$$

$$C_j = \sum_{k=0}^{N_0-1} s(k) e^{-j \frac{2\pi}{N_0} l k};$$

$$C_j = A_{n_i} - jB_{n_i}, \quad I = I_0 + n, \quad n = 1, 2, \dots, N_0; \quad (2.66)$$

$$C_I = 0, \quad I = 0, 1, 2, \dots, I_0, I_0 + N_0, I_0 + N_0 + 1, \dots, N_0 - 1,$$

де $\Delta t = 1/F_d$ – інтервал дискредитації сигналів, I_0 – константа.

Спрощена модель N -канального БМ подана на рис. 2.34. Дискретна (двійкова) інформація, що підлягає передачі, розбивається послідовно на N m -бітових символів (m визначається кількістю біт інформації, передаваної в кожному каналі БМ на одному такті тривалістю T). Кодовий пристрій кожному m -бітовому символу ставить у відповідність комплексний вектор $(A_{n_i} - jB_{n_i})$. Якщо для певності вважати, що в БМ використовується сигнальне сузір'я КАМ-16 (див. рис. 2.31), то $m = 4$, а A_{n_i}, jB_{n_i} набувають значень $\pm 1, \pm 3$ в залежності від значення чотирибітового символу. На рис. 2.31 у круглих дужках вказаний двійковий номер відповідного вектора. Далі формується N -вимірна послідовність C_I (2.66) і здійснюється обернене ДПФ за стандартним, добре відомим алгоритмом [].

Для демодуляції сигналу $s(t)$ треба визначити границю одиничного елемента сигналу тривалістю T і здійснити пряме ДПФ цього елемента. Отримані комплексні сигнали $(A_{n_i} - jB_{n_i})$ необхідно декодувати і в послідовному коді видати одержувачеві прийняту інформацію.

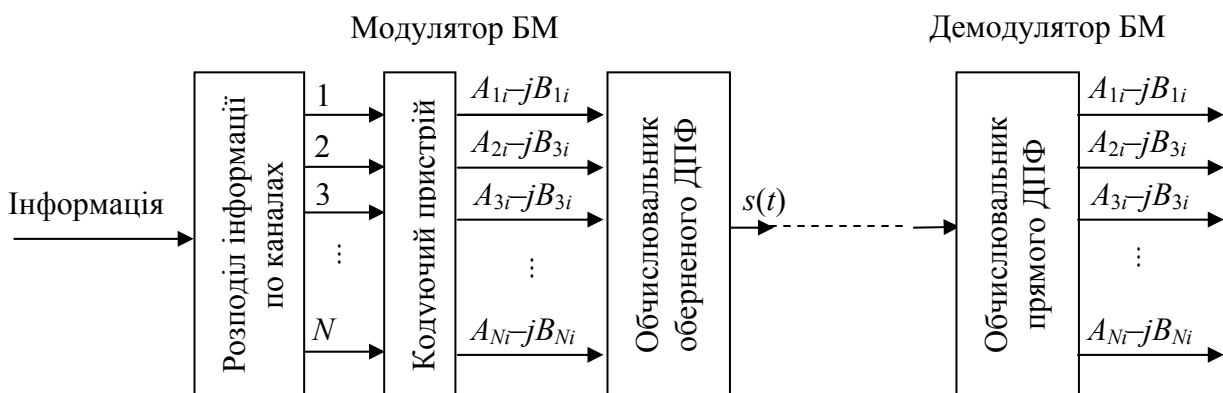


Рисунок 2.34 – Багатоканальний модем

Сигнали техніки зв'язку. В зв'язку з тим, що задачею галузі зв'язку є передача не енергії на відстань, а інформації, сигнали техніки зв'язку характеризуються тривалістю T_c шириною спектра ΔF_c й динамічним діапазоном D_c . У якості узагальненої характеристики використовується об'єм сигналу $V_c = T_c \cdot \Delta F_c \cdot D_c$. Тривалість сигналу визначає час його існування, ширина спектра – діапазон частот, у якому зосереджена основна енергія сигналу. Динамічний діапазон характеризує відношення найбільшої миттєвої потужності сигналу P_{\max} до найменшої P_{\min} , припустиме значення якої визначається потужністю завад.

Важливою характеристикою сигналів є також база $v = T_c \cdot \Delta F_c$ (часто база позначається індексом B – $B = T_c \cdot \Delta F_c$). Сигнали називаються *вужькосмуговими* (простими), якщо $v \leq 1$, і *широкосмуговими* (складними), якщо $v \gg 1$.

Елементарні сигнали, одержувані на виході УПС при використанні m -позиційного коду, можна розділити на наступні групи:

– сигнали $s_1(t), \dots, s_m(t)$, що забезпечують одержання максимальної завадостійкості стосовно флуктуаційних завад у детермінованих каналах. Енергія цих сигналів найчастіше однакова:

$$\int_0^{T_c} s_j^2(t) dt = Q^2 \text{ за } 1 \leq j \leq m, \text{ а скалярний добуток } \int_0^{T_c} s_i(t) s_j(t) dt = -Q^2 / (m-1)$$

за $i \neq j$; *ортогональні сигнали*, для яких $\int_0^{T_c} s_i(t) s_j(t) dt = 0$ за $i \neq j$;

– *біортогональні сигнали*, для яких величина m завжди парна, будь-якому з m сигналів завжди відповідає один протилежний сигнал, а інші $m - 2$ сигналів ортогональні;

– *неортогональні сигнали*, для яких виконується умова

$$\int_0^{T_c} s_i(t) s_j(t) dt > 0 \text{ за } i \neq j.$$

Прикладом сигналів, що забезпечують максимальну завадостійкість при детермінованому неспотворюючому каналі і адитивному білому шумі, є сигнали, модульовані за фазою, і двополюсні сигнали постійного струму. До ортогональних належать сигнали двійкової частотної модуляції (ЧМ), якщо частоти відрізків гармонійних сигналів $s_1(t)$ і $s_2(t)$ кратні частоті модуляції. Біортогональні сигнали використовуються при двократній фазовій модуляції, коли $m = 4$. Неортогональні сигнали застосовуються при фазовій модуляції, коли зрушення між окремими сигналами становлять, наприклад 0° , 120° і 240° .

Багато задач аналізу й синтезу реальних сигналів спрощуються завдяки тому, що ці сигнали, як правило, складні за формою, можна

представити у вигляді простих сигналів. Це зручно для наступного аналізу їх проходження через ті або інші ланцюги. Наприклад, деякий сигнал $s(t)$ може бути представлений у вигляді сукупності ортогональних складових (елементарних сигналів):

$$s(t) = \sum_{k=0}^{\infty} a_k \Psi_k(t), \quad t \in [t_1, t_2], \quad (2.67)$$

причому незліченною кількістю способів. Запис (2.67) називають *узагальненим рядом Фур'є*. Інтервал $[t_1, t_2]$ показує час дії сигналу. Оскільки система ортогональних функцій $\{\Psi_k(t)\}$, застосовувана при розкладанні, заздалегідь відома, то сигнал визначається набором вагових коефіцієнтів a_k $k = 0, 1, 2, \dots$, для цих функцій. Такі набори чисел називаються *спектрами сигналів*. Спектр сигналу, представлений у вигляді суми спектральних складових (2.67), називається *дискретним*.

Якщо для перетворення сигналу $s(t)$ недостатньо дискретного набору базисних функцій $\Psi_k(t)$, а потрібна безліч базисних функцій $\psi(\beta, t)$, що відрізняються значенням безупинно мінливого параметра β , то сигнал представляється у вигляді інтеграла

$$s(t) = \int_{-\infty}^{\infty} s(\beta) \psi(\beta, t) d\beta, \quad (2.68)$$

який називається *узагальненим інтегралом Фур'є*. Спектр такого сигналу характеризується функцією $s(\beta)$ безперервною змінною β й називається *безперервним*.

Розглядаючи проходження кожної складової спектра через лінійний ланцюг із заданими характеристиками, сигнал на виході ланцюга одержуємо також у вигляді (2.67) або (2.68) з ваговими коефіцієнтами a'_k або $s'(\beta)$ в загальному випадку відмінними від a_k або $s(\beta)$ й залежними від характеристик розглянутого ланцюга.

Крім аналізу в теорії ПДС доводиться вирішувати задачі синтезу сигналів. Вони можуть бути двох типів: структурний синтез – визначення форми сигналів, що задовольняють заданим вимогам; параметричний синтез – визначення параметрів сигналів відомої форми. Якщо в процесі синтезу необхідно забезпечити екстремум того або іншого функціонала (або функції), який характеризує якість синтезу, то синтез називається *оптимальним*.

На практиці широко використовуються системи сигналів прямокутної й синусоїдальної форм. Прямокутні сигнали відрізняються один від одного амплітудою, тривалістю, числом і місцем розташування імпульсів прямокутної форми на одиничному інтервалі τ_0 . Елементарні сигнали синусоїдальної форми являють собою відрізки синусоїдальних коливань, відмінних один від одного по амплітуді, частоті й фазі.

Імпульси постійного струму. Типовим прикладом імпульсів прямокутної форми служать первинні телеграфні сигнали й сигнали передачі даних, що мають назву *імпульси постійного струму*. Вони мають вигляд послідовностей дво- або однополярних прямокутних імпульсів (рис. 2.35,а).

Визначимо спектр періодичної послідовності однополярних імпульсів з періодом $T = \alpha\tau_0$ і амплітудою U_0 . Така послідовність може бути представлена у вигляді ряду Фур'є:

$$s(t) = a_0 + \sum_{k=1}^{\infty} a_k \sin(k\Omega_1 t + \varphi_k), \quad (2.69)$$

де Ω_1 – кругова частота повторення або перша гармоніка (спектральна складова) сигналу $s(t)$, $\Omega_1 = 2\pi/T$. Коефіцієнти a_k визначають так званий спектр амплітуд, а φ_k – спектр фаз. При цьому

$$a_k = \frac{2U_0}{\alpha} \frac{\sin(k\Omega_1 T / 2\alpha)}{k\Omega_1 T / 2\alpha}, \quad (2.70)$$

де $\alpha = T/\tau_0$ – шпаруватість імпульсної послідовності. Постійна складова або середнє значення сигналу $s(t)$ за період $a_0 = U_0/\alpha$. Спектр амплітуд для випадку $\alpha = 2$ наведено на рис. 2.35, б.

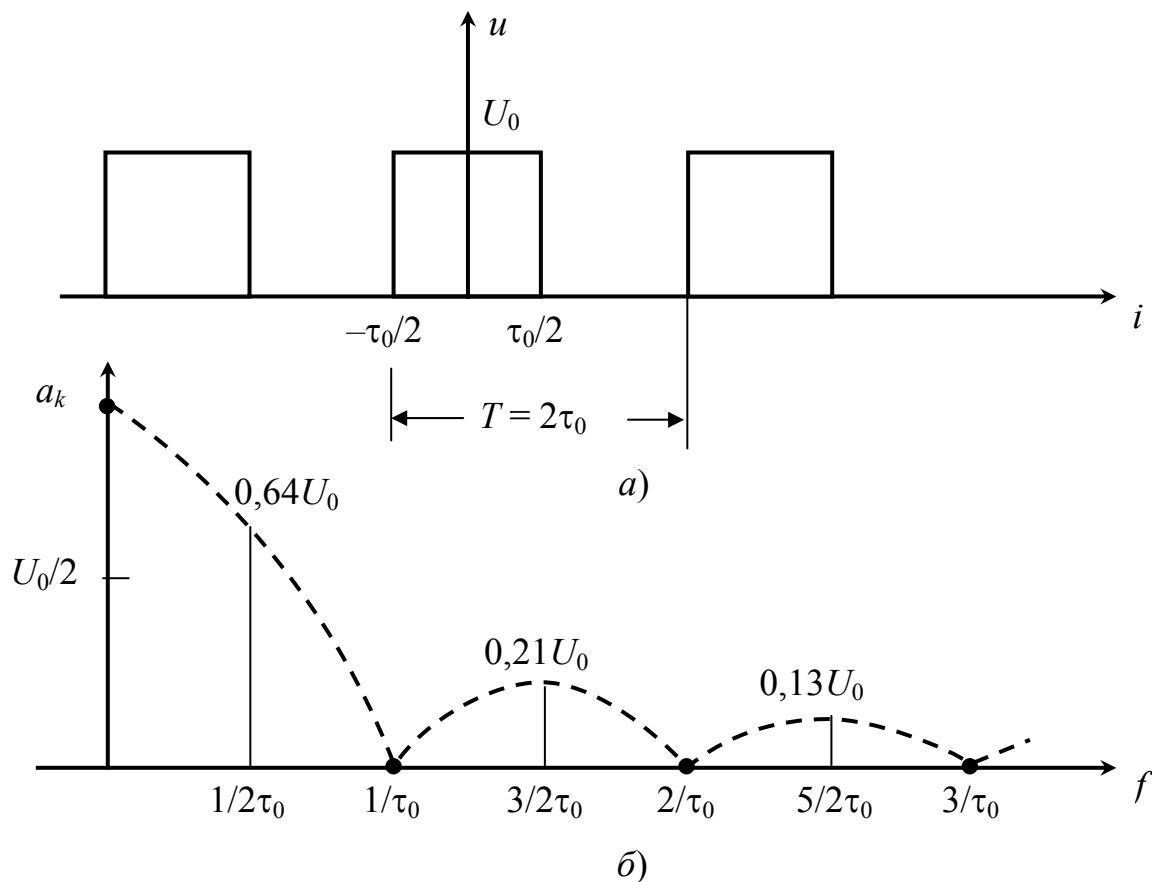


Рисунок 2.35 – Послідовність імпульсів (а) та її спектр (б)

Спектр періодичної послідовності однополярних імпульсів при $\alpha = 2$ містить крім постійної складової складові із частотами $f_1 = 1/T$, $f_3 = 3f_1$, $f_5 = 5f_1$, $f_7 = 7f_1$ і т.д. Різниця між цими спектральними складовими $\Delta f = f_{i+2} - f_i = 2f_1 = 2/T$ зі зростанням T зменшується, при цьому самі складові також зменшуються по амплітуді. При $\alpha \rightarrow \infty$ ($T \rightarrow \infty$) сигнал стає неперіодичним, а спектр – безперервним. Замість поняття спектра амплітуд при цьому вводиться поняття спектральної густини. Спектральна густина визначається як відношення «амплітуди спектральної складової» до нескінченно малої смуги частот $d\Omega$ і обчислюється через інтеграл Фур'є :

$$s(\Omega) = \int_{-\infty}^{\infty} s(t)e^{-j\Omega t} dt = s(\Omega)e^{j\varphi(\Omega)}, \quad (2.71)$$

де $s(\Omega)$ – спектральна густина амплітуд; $\varphi(\Omega)$ – спектр фаз.

Знаючи $s(\Omega)$, можна знайти $s(t)$, використовуючи зворотне перетворення Фур'є:

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} s(\Omega)e^{j\Omega t} d\Omega, \quad (2.72)$$

Спектральна густина амплітуд одиночного прямокутного імпульсу з точністю до множника зображена штриховою лінією на рис. 2.35, б.

Спектр періодичної послідовності імпульсів і одиночного імпульсу містить складові із частотою від 0 нескінченності, тобто є нескінченним. Якщо послідовність прямокутних імпульсів передається по каналу зв'язку, який завжди пропускає тільки обмежений спектр, то форма сигналу на виході каналу змінюється. Форму сигналу можна визначити, використовуючи зворотне перетворення Фур'є (2.72).

На практиці під *шириною спектра сигналу* звичайно розуміють ту область частот, у якій зосереджена основна енергія сигналу. При цьому вводиться поняття *ефективної ширини спектра сигналу*. На рис. 2.35, б – це діапазон частот від 0 до $1/\tau_0$, в якому зосереджено близько 90% енергії сигналу. Виходить, чим менше тривалість імпульсу (вище швидкість модуляції $B = 1/\tau_0$), тем ширше спектр. Зокрема, нескінченно короткий імпульс має нескінченно протяжний спектр із рівномірною густиною. Таким чином, передача з більш високою швидкістю вимагає каналів з більш широкою смугою пропускання.

При заданій тривалості одиничного елемента τ_0 на спектр переданого сигналу впливають два фактори. Один з них – форма імпульсу, яку слід ретельно вибирати для одержання хорошого (компактного) спектра сигналу. Інший фактор – характер передаваної цифрової послідовності, тобто спектр залежить від статистичних характеристик передаваної послідовності, та її перекодуванням спектр можна змінити.

Для оцінки спотворень імпульсів постійного струму, викликаних обмеженням спектра, розглянемо проходження імпульсу через ідеальний фільтр нижніх частот (ФНЧ). У якості вхідного впливу скористаємося східчастою функцією

$$u_{\text{вх}}(t) = \begin{cases} U_0 & \text{за } t \geq \tau; \\ 0 & \text{за } t < \tau, \end{cases} \quad (2.73)$$

представленою графічно на рис. 2.36. Вибір такого вхідного впливу обумовлений тим, що, по-перше, його використання спрощує математичні викладення, по-друге, одиночний прямокутний імпульс кінцевої тривалості можна представити як послідовність двох одиничних стрибків напруги протилежного знака, зрушених у часі на величину, рівну тривалості імпульсу (рис. 2.36). І, нарешті, знаючи характеристику процесу, що встановлюється, при впливі одиничного стрибка, за допомогою теореми згортання можна знайти, що встановлюється процес для довільної форми впливу.

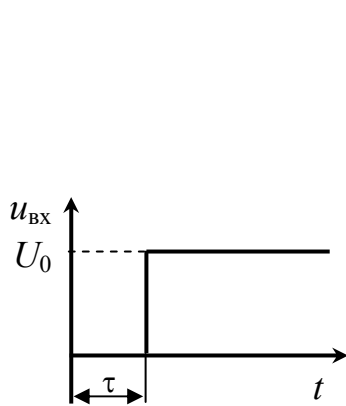


Рисунок 2.36 – Східчаста функція

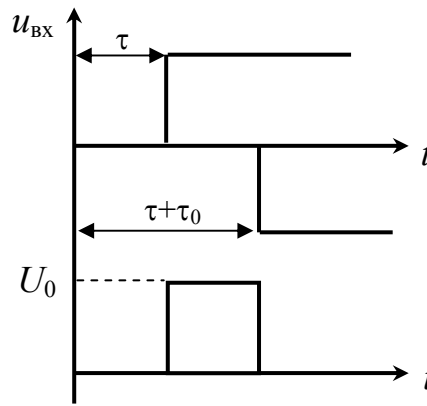


Рисунок 2.37 – Подання одиночного імпульсу

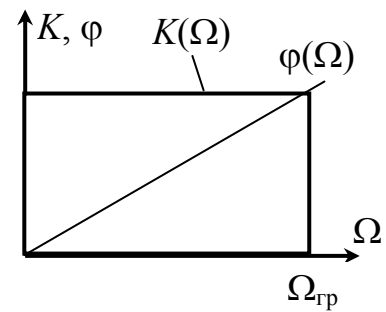


Рисунок 2.38 – Характеристика ідеального ФНЧ

Нехай на вхід ідеального ФНЧ із частотою зрізу $\Omega_{\text{гр}} = 2\pi F_{\text{гр}}$, амплітудно- і фазочастотна характеристики якого мають вигляд (рис. 2.38):

$$K(\Omega) = \begin{cases} K(0) = K_0 & \text{за } \Omega \leq \Omega_{\text{гр}}, \\ 0 & \text{за } \Omega > \Omega_{\text{гр}}, \end{cases} \quad (2.74)$$

$$\varphi(\Omega) = \Omega t_0 \quad \text{за } 0 \leq \Omega \leq \infty,$$

де t_0 – груповий час проходження фільтра, у момент $t = 0$ подається сигнал (2.74), який може бути поданий у вигляді

$$u_{\text{вх}}(t) = U_0 \left(\frac{1}{2} + \frac{1}{\pi} \int_0^{\infty} \frac{\sin \Omega t}{\Omega} d\Omega \right).$$

Для одержання сигналу на виході ФНЧ помножимо всі компоненти вхідного сигналу на модуль коефіцієнта передачі фільтра й віднімемо з аргументу синуса зсув фаз на кожній із частот:

$$u_{\text{вих}}(t) = U_0 \left(\frac{1}{2} K_0 + \frac{1}{\pi} \int_0^{\infty} \frac{K(\Omega) \sin \Omega(t - t_0)}{\Omega} d\Omega \right). \quad (2.75)$$

Підставивши в (2.75) значення коефіцієнта передачі з (2.74), одержимо

$$u_{\text{вих}}(t) = U_0 K_0 \left(\frac{1}{2} + \frac{1}{\pi} \int_0^{\Omega_{\text{гр}}} \frac{\sin \Omega(t - t_0)}{\Omega} d\Omega \right). \quad (2.76)$$

На рис. 2.39 подано вид сигналу на виході ФНЧ, розрахований за формулою (2.76). Час зростання перехідного процесу можна визначити із трикутника ABC , у якому AC є дотичною у точці $t = t_0$:

$$t_n = \frac{BC}{\text{tg}\psi} = \frac{U_0 K_0}{\left[\frac{\partial u_{\text{вих}}(t)}{\partial t} \right]_{t=t_0}}, \quad (2.77)$$

де

$$\left[\frac{\partial u_{\text{вих}}(t)}{\partial t} \right]_{t=t_0} = \frac{U_0 K_0}{\pi} \int_0^{\Omega_{\text{гр}}} [\cos(\Omega t - \Omega t_0)]_{t=t_0} d\Omega = \frac{U_0 K_0}{\pi} \Omega_{\text{гр}}. \quad (2.78)$$

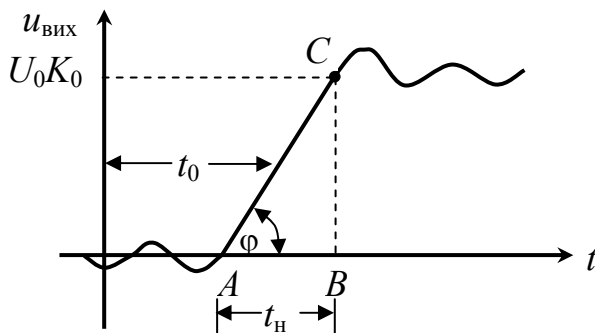
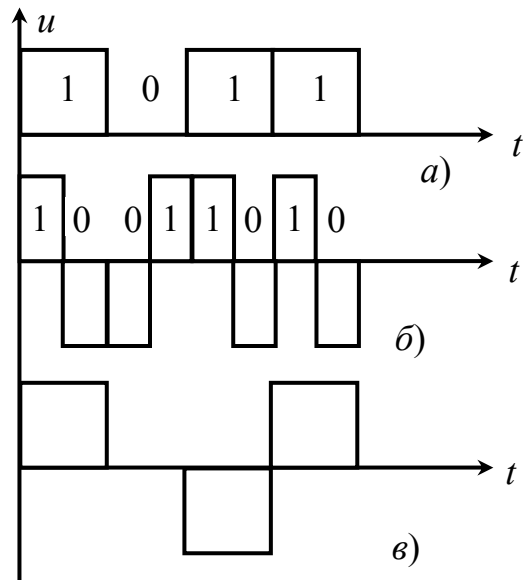


Рисунок 2.39 – Сигнал на виході ФНЧ

Рисунок 2.40 – Перекодування сигналів з уведенням надлишковості:
 а – початкова послідовність; б – бі-імпульсний сигнал; в – біполярний сигнал



Враховуючи (2.78), одержимо $t_n = 1/2F_{\text{гр}}$. Таким чином, час зростання зворотно пропорційно граничній частоті ідеального ФНЧ.

Цікаво відзначити зв'язок отриманої формули з так званою умовою Найквіста, що обмежує швидкість передавання двійкових сигналів зверху:

$B_{\text{макс}} = 2\Delta F_k = 2F_{\text{гр}}$, Бод. Враховуючи, що $B_{\text{макс}} = 1/\tau_{0\text{мін}}$, маємо $\tau_{0\text{мін}} = 1/2F_{\text{гр}}$. Отже, тривалість одиничного елемента відповідно до умови Найквіста повинна бути не менше, ніж час зростання перехідного процесу, тобто $\tau_0 \geq t_n$.

Вигляд сигналу на виході ФНЧ залежить від його АЧХ і ФЧХ. Так, чим плавніше перехід АЧХ фільтра від смуги пропускання до смуги затримки, тим менше коливальні викиди перехідного процесу. Відхилення ФЧХ від ідеальної призводить до подовження перехідного процесу й, як наслідок, до взаємного впливу імпульсів або своєрідній заваді, яка має назву міжсимвольна або інтерференційна

Перекодування первинних сигналів з уведенням надлишковості. Розрізняють два способи введення надлишковості, використовувані в перетворювачах кодів:

1. Шляхом перетворення кожного одиничного елемента в послідовність із k сигналів, при цьому основа коду на виході перетворювача не змінюється. Коефіцієнт надлишковості в цьому випадку

$$\chi_1 = (k \log_2 m - \log_2 m) / (k \log_2 m) = 1 - 1/k. \quad (2.79)$$

2. За рахунок збільшення в процесі перетворення сигналів основи коду, при цьому число m різних елементарних вхідних сигналів, що діють на вході перетворювача, менше числа вихідних елементарних сигналів m^1 . Коефіцієнт надлишковості в цьому випадку

$$\chi_1 = (\log_2 m^* - \log_2 m) / \log_2 m^* = 1 - (\log_2 m) / \log_2 m^*. \quad (2.80)$$

Наведемо приклади перекодування. Типовим прикладом перекодування за першим способом введення надлишковості є біімпульсне. Особливістю біімпульсних сигналів є наявність на будь-якому одиничному інтервалі двох різнополярних імпульсів. Одиниця вихідної послідовності (рис. 2.40, а) передається у вигляді 10, а 0 – у вигляді 01 (рис. 2.40, б). Спектр біімпульсної послідовності характеризується відсутністю постійної складової й значним зменшенням енергії низькочастотних складових. Це дозволяє передавати біімпульсні сигнали фізичними лініями, а також каналами ТЧ. Надлишковість біімпульсного сигналу відповідно до (2.79) дорівнює 0,5.

Постійна складова може бути також усунута шляхом перетворення первинного сигналу в біполярний псевдотрійковий код. При цьому символ «0» передається в канал безструмовою послілкою, а символи «1» – прямокутними імпульсами, що поперемінно чергуються за полярністю (рис. 2.40, в). Надлишковість сигналу відповідно до (2.80) дорівнює 0,37.

¹ Розглядувані первинні (елементарні) сигнали вважаємо рівно ймовірними.

2.6. Некогерентне та когерентне приймання при АМ

Смуга частот при АМ. В техніці зв'язку за ширину займаної смуги вважається ширина такої смуги частот, за нижнім і верхнім межами якої середні випромінювані потужності дорівнюють 0,5 % всієї середньої потужності даного випромінювання. Вибір числового значення коефіцієнта позасмугового випромінювання 0,5 % довільний і не має теоретичного обґрунтування. Однак смуга частот, що містить 99 % випромінюваної потужності, забезпечує малий рівень перехідних завад при якісній відтворенні сигналу. Зменшити ширину смуги сигналу заданої тривалості можна лише за рахунок зміни його форми, наприклад шляхом округлення. Досвід показує, що округлення може проводитися до певних меж, після чого вірність зв'язку може погіршуватися.

Таким чином, існує поняття *необхідної ширини смуги*, під якою розуміється «мінімальне значення ширини смуги, займаної випромінюванням, достатнє при цьому класі випромінювання, щоб забезпечити передачу повідомлення з такою швидкістю й такою якістю, які потрібні для системи, використовуваної за певних умов». В реальних умовах смуги частот для різних класів випромінювання має наступні значення:

– за АМ незатухаючими коливаннями:

$$\Delta f = \begin{cases} 5B & \text{– для каналів із завмираннями;} \\ 3B & \text{– для каналів з постійними параметрами;} \end{cases} \quad (2.81)$$

– за АМ тональними коливаннями:

$$\Delta f = \begin{cases} 5B + 2F_T & \text{– для каналів із завмираннями;} \\ 3B + 2F_T & \text{– для каналів з постійними параметрами;} \end{cases} \quad (2.82)$$

Вибір форми імпульсу. Бажано використовувати сигнали, що не тільки займають найменшу смугу частот, але, що володіють найменшим часом встановлення t_b . Час t_b являє собою час, протягом якого струм проходить від 0,1 до 0,9 (або навпаки) значення, що досягається у встановленому стані. Рівні 0,1 і 0,9 обрані довільно, як і граничні значення ширини смуги.

Вираз для енергетичного спектра імпульсних сигналів різної форми містять параметр

$$\zeta_c = \frac{\pi \Delta f T_c}{2}, \quad (2.83)$$

де Δf – ширина смуги в герцах, обумовлена формулами (2.81) і (2.82).

Чим менше ζ_c , тим краще використовуються частотно-часові параметри сигналу з точки зору концентрації потужності.

Якщо припустити, що імпульси мають симетричну форму, то тривалість посилки

$$T_c = T_b + 2t_b, \quad (2.84)$$

де T_b – тривалість сигналу у встановленому стані. Тоді параметр

$$\zeta_c = \zeta_0 + 2\zeta_b = \frac{\pi\Delta f T_b}{2} + 2 \frac{\pi\Delta f t_b}{2} \quad (2.85)$$

характеризує сигнал з точки зору ширини смуги частот і тривалості часу встановлення. Ідеальний прямокутний імпульс має $t_b = 0$, але коефіцієнт ζ_0 у нього більше, ніж, наприклад, у дзвоноподібного імпульсу. Тому вибір форми імпульсу повинен проводитися у кожному конкретному випадку з урахуванням важливості концентрації спектра сигналу або мінімізації часу його встановлення. Так, для економії смуги частот може виявитися доцільним посилати в лінію зв'язку округлені посилки. Однак на приймальній стороні системи вони перетворюються в імпульси прямокутної форми.

Некогерентне приймання сигналів при АМ. Вплив адитивних флуктуаційних завад при некогерентному прийманні сигналів АМ проявляється в змінюванні рівня струмових посилок і в утворенні неправильних сигналів у паузах.

Стійкий зв'язок буде лише тоді, коли мінімальний рівень сигналу буде перевищувати максимальний рівень завад у паузах. Для чіткого розділення наявності і відсутності сигналу приймач повинен мати, граничний пристрій, завдяки чому відтинається більшість завад у паузах. Наявність такого порога обмеження по мінімуму є характерною ознакою каналів АМ.

Дія флуктуаційних завад призводить до того, що густина ймовірності $w(U_p)$ амплітуди сумарного коливання $U_p = U_c + U_{ш}$ при передаванні наявного сигналу описується узагальненим законом Релея, а густина ймовірності обгинаючої завади $U_{ш}$ за відсутності сигналу характеризується простим законом Релея.

Вважаючи наявність й відсутність сигналу рівноймовірними, для ймовірності помилок маємо

$$p_0 = \frac{1}{2} [p(0/1) + p(1/0)], \quad (2.86)$$

де $p(0/1)$ – ймовірність перевищення наявності сигналу; $p(1/0)$ – ймовірність створення неправильного сигналу.

Принцип реєстрації сигналів АМ ілюструється рис. 2.41, де $U_{ш1}$, $U_{ш2}$ – синфазна й квадратурна складові завади. Коли амплітуда сумарного коливання U_p перевищує граничний рівень $U_{ог}$, фіксується наявність сигналу; а якщо ні, то реєструється відсутність сигналу.

Відповідно до цього принципу ймовірність помилки

$$p_0 = \frac{1}{2} \int_0^{U_{\text{ор}}} w(U_p) dU_p + \int_{U_{\text{ор}}}^{\infty} w(U_{\text{ш}}) dU_{\text{ш}}.$$

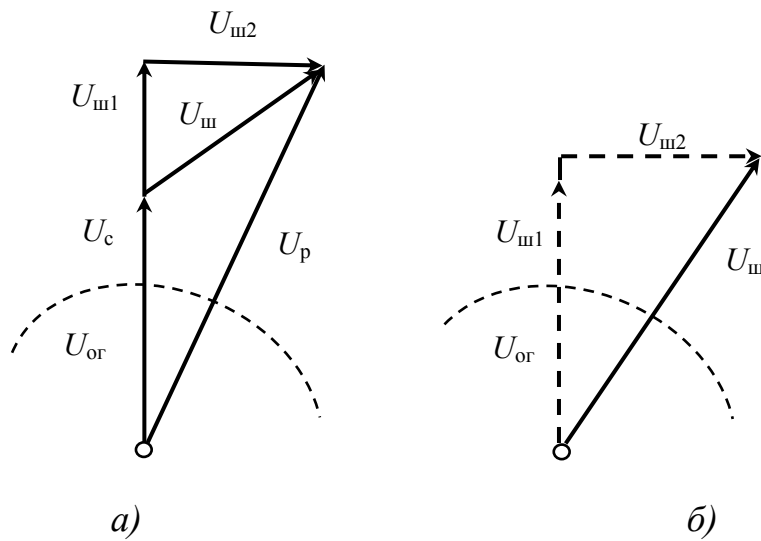


Рисунок 2.41 – Векторна діаграма некогерентного приймання сигналів АМ за флуктуаційних завад:
а) наявність сигналу; б) відсутність сигналу

Підставляючи вирази для простого і узагальненого законів Релея і інтегруючи, одержимо

$$p_0 = \frac{1}{2} \left[R(q_{\text{ор}}; h_c^2) e^{-h_c^2} + e^{-\frac{q_{\text{ор}}^2}{2}} \right], \quad (2.87)$$

де функція

$$R(q_{\text{ор}}; h_c^2) = \int_0^{q_{\text{ор}}} q_p e^{-\frac{q_p^2}{2}} I_0(q_p; \sqrt{2h_c^2}) dq_p. \quad (2.88)$$

З формули (2.87) випливає, що завадостійкість каналів АМ при цьому h_c^2 залежить від рівня $U_{\text{ор}}$ й зі збільшенням h_c^2 зростає. Розв'язання рівняння

$$\frac{dR(q_{\text{ор}}; h_c^2)}{dq_{\text{ор}}} = 0$$

призводить до виразу

$$I_0(\sqrt{2h_c^2}; q_{\text{ор опт}}) = e^{h_c^2}, \quad (2.89)$$

що дозволяє визначити оптимальний поріг обмеження $U_{\text{ор опт}}$. Розв'язання

цього рівняння у вигляді залежності $\frac{U_{\text{ор}}}{U_{c \text{ макс}}} = f(h_c^2)$ наведено на рис. 2.42,

що дозволяє зробити кілька важливих практичних висновків.

Оптимальні канали АМ повинні мати можливість автоматичного регулювання порога обмеження залежно від величини h_c^2 , при цьому значення $U_{ог\ опт}$ визначається з виразу (2.89).

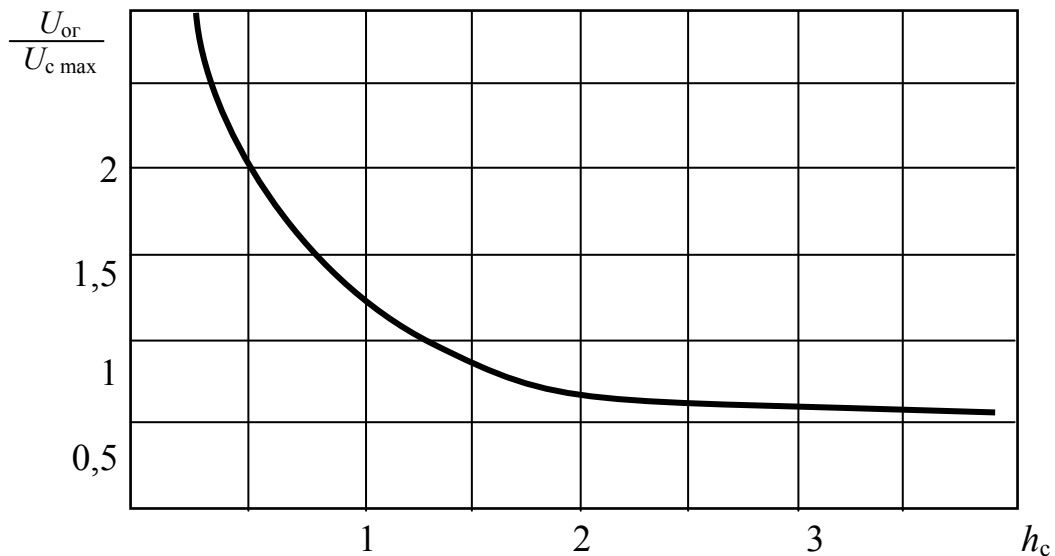


Рисунок 2.42 – Про оптимальний поріг обмеження сигналів АМ

Технічна реалізація цієї задачі складна. З рис. 2.42 також виходить, що автоматичне розв'язання рівняння (2.89) необхідно лише при $h_c^2 < 3...4$; при значеннях $h_c^2 > 4...6$ оптимальний поріг обмеження може бути встановлений постійним і дорівнювати $0,5U_{c\ макс}$, що відповідає значенню $q_{ог\ опт} = 0,5h_c^2$.

При цьому ймовірність помилки буде мінімальною

$$p_{0\ мин} = \frac{1}{2} \left[R(q_{ог\ опт}; h_c^2) + e^{-\frac{h_c^2}{4}} \right] \quad (2.90)$$

і залежить тільки від перевищення h_c^2 .

Встановимо зв'язок формули (2.90), що описує реальну завадостійкість каналів АМ при оптимальному порозі обмеження, з формулою, що визначає потенційну завадостійкість каналів АМ. У виразі (2.90) перший доданок характеризує помилку, обумовлену перевищенням наявності сигналу завадою, а другий доданок – помилку створення неправильного сигналу. При значеннях $h_c^2 \gg 1$ синфазна й квадратурна складові завади $U_{ш1} \ll U_c$ і $U_{ш2} \ll U_c$. При цьому приблизно можна вважати, що ймовірність помилки буде визначатися ймовірністю виконання нерівності $|U_{ш}| \approx |U_{ш}| < 0,5U_{c\ макс}$, оскільки $U_{ог\ опт} = 0,5U_c$. Враховуючи, що амплітуда синфазної складової завади (так само, як і

квадратурної) відповідає нормальному закону розподілу, для ймовірності перевищення наявності сигналу одержимо

$$p(0/1) = \int_{\frac{U_{c \text{ макс}}}{2}}^{\infty} w(U_{\text{ш}}) dU_{\text{ш}} = V \left(\sqrt{\frac{h_c^2}{2}} \right). \quad (2.91)$$

Тоді вираз (2.90) набуде вигляду

$$p_0 = \left[V \left(\sqrt{\frac{h_c^2}{2}} \right) + e^{-\frac{h_c^2}{4}} \right]. \quad (2.92)$$

Когерентне приймання двійкових сигналів при АМ. При когерентному прийманні сигналів АМ помилки викликаються лише синфазною складовою флуктуаційної завади $U_{\text{ш}1}$; квадратурна складова завади $U_{\text{ш}2}$ виключається в процесі синхронного детектування. Тому індекс «1» можна вилучити й писати просто $U_{\text{ш}}$.

Оскільки синфазна складова розподілена за нормальним законом, то ймовірності перевищення й неправильної реєстрації посилок відповідно описуються виразами

$$p(0/1) = \int_{U_{c \text{ макс}} - U_{\text{ог}}}^{\infty} w(U_{\text{ш}}) dU_{\text{ш}}; \quad p(1/0) = \int_{U_{\text{ог}}}^{\infty} w(U_{\text{ш}}) dU_{\text{ш}}. \quad (2.93)$$

Вважаючи, що наявність й відсутність сигналу є рівноймовірними, для повної ймовірності помилкового приймання сигналів АМ одержимо:

$$p_0 = \frac{1}{2} [p(0/1) + p(1/0)] = \frac{1}{4} [2 - F(q_c - q_{\text{ог}}) - F(q_{\text{ог}})]. \quad (2.94)$$

Звідси випливає, що величина порога обмеження $U_{\text{ог}}$ суттєво впливає на завадостійкість каналів АМ при когерентному прийманні. З рівняння

$$\frac{dp_0}{dU_{\text{ог}}} = 0 \quad (2.95)$$

визначимо оптимальну величину порога обмеження

$$U_{\text{ог опт}} = \frac{U_{c \text{ макс}}}{2},$$

що забезпечує мінімальну ймовірність помилки

$$p_0 = V \left(\sqrt{\frac{h_c^2}{2}} \right). \quad (2.96)$$

Необхідно зазначити, що величина $U_{\text{ог опт}}$ при когерентному прийманні на відміну від некогерентного приймання сигналів АМ при

флуктуаційних завадах не залежить від їхнього рівня й при рівноймовірних посылках дорівнює $0,5U_{c \text{ макс}}$.

Некогерентне приймання при імпульсних завадах. Принцип реєстрації сигналів АМ при дії в каналі імпульсних завад залишається таким же, що й при флуктуаційних завадах, однак при обчисленні ймовірності помилки необхідно враховувати ймовірність появи імпульсної завади p_{zi} .

Вважаючи, що наявність й відсутність сигналу є рівноймовірними, вираз для ймовірності помилки можна записати у вигляді

$$p_0 = \frac{P_{zi}}{2} [p(0/1) + p(1/0)]. \quad (2.97)$$

Поява помилок залежить від амплітудних і фазових співвідношень між сигналом і імпульсною завадою. При відсутності сигналу помилка виникає завжди, якщо $U_{з \text{ макс}} > U_{ог}$, незалежно від фазового кута завади $\varphi_з$ відносно сигналу (рис. 2.43). За наявності сигналу помилка з'явиться, якщо амплітуда завади

$$U_{c \text{ макс}} - U_{ог} < U_{з \text{ макс}} < U_{c \text{ макс}} + U_{ог}, \quad (2.98)$$

фазовий кут $|\varphi_з| > 90^\circ$, а амплітуда сумарного коливання $U_{з \text{ макс}} < U_{ог}$, тобто за

$$U_{з \text{ макс}} = \sqrt{(U_{c \text{ макс}} - U_{з \text{ макс}} \cos \varphi_з)^2 + U_{з \text{ макс}}^2 \sin^2 \varphi_з} < U_{ог},$$

звідки

$$U_{ог}^2 > U_{c \text{ макс}}^2 - 2U_{c \text{ макс}} U_{з \text{ макс}} \cos \varphi_з + U_{з \text{ макс}}^2.$$

Поділивши обидві частини цієї нерівності на $U_{з \text{ макс}}$ й увівши позначення для нормованого відносно сигналу граничного рівня й перевищення сигналу

$$q_{oc} = \frac{U_{ог}}{U_{c \text{ макс}}}, \quad (2.99)$$

$$h_c^2 = \frac{U_{c \text{ макс}}^2}{U_{з \text{ макс}}^2}, \quad (2.100)$$

одержимо нерівність

$$\varphi_з > \arccos \frac{h_c^2(1 - q_{oc}^2) + 1}{2h_c^2}. \quad (2.101)$$

Ймовірність перевищення наявності сигналу $p(0/1)$ може бути отримана шляхом

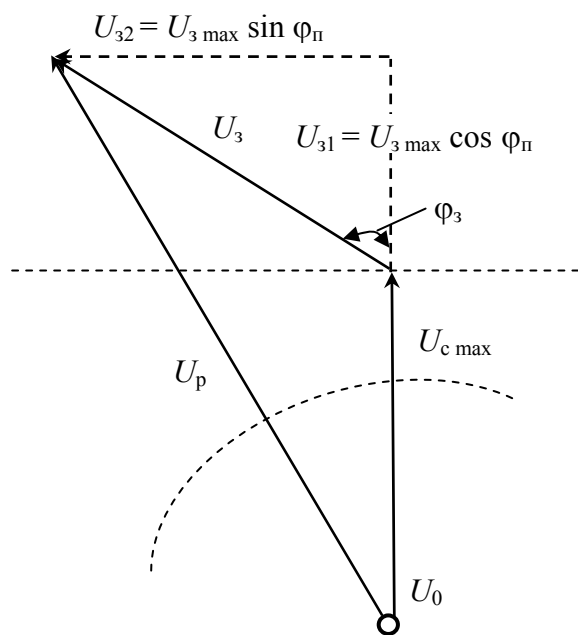


Рисунок 2.43 – Векторна діаграма прийому сигналів АМ за імпульсних завадах

інтегрування виразу (2.101) у границях змінювання величини h_c^2 , відповідної до нерівності (2.97):

$$\alpha_2^2 > h_c^2 > \alpha_1^2,$$

де

$$\alpha_1 = \frac{1}{1+q_{oc}}; \alpha_2 = \frac{1}{1-q_{oc}}.$$

Оскільки значення фазового кута завади розподілені за рівномірним законом в інтервалі $(0, 2\pi)$, то при відомій густині розподілу ймовірностей перевищення $w(h_c^2)$ ймовірність $p(0/1)$ становить

$$p(0/1) = \frac{1}{\pi} \int_{\alpha_1^2}^{\alpha_2^2} \arccos \left[\frac{h_c^2(1-q_{oc})+1}{2h_c^2} \right] w(h_c^2) dh_c^2. \quad (2.102)$$

Для фіксованого значення h_c^2 ймовірність помилок

$$p_0 = \frac{p_{zi}}{2} \left[\frac{1}{\pi} \arccos \frac{h_c^2(1-q_{oc})+1}{2h_c^2} + p(1/0) \right], \quad (2.103)$$

де ймовірність неправильної реєстрації сигналу

$$p(1/0) = \begin{cases} 1 & \text{за } U_{з\text{ макс}} > U_{ог}; \\ 0 & \text{за } U_{з\text{ макс}} < U_{ог}. \end{cases} \quad (2.104)$$

З формули випливає, що ймовірність спотворень сигналів АМ при імпульсних завадах залежить від параметрів h_c^2 , $q_{ог}$ і ймовірності p_{zi} . Тому тут оптимальний поріг обмеження вимагає регулювання за складнішим законом, оскільки при фіксованому h_c^2 величина $q_{ог}$ буде змінюватися залежно від p_{zi} . Це ускладнює конструювання оптимальних пристроїв обробки сигналів і знижує в загальному випадку реальну завадостійкість каналів АМ при імпульсних завадах.

Когерентне приймання при імпульсних завадах. При когерентному прийманні сигналів АМ помилки викликаються синфазною складовою імпульсної завади $U_{з1} = U_{з\text{ макс}} \cos \varphi_з$.

Ймовірність перевищення наявності сигналу $p(0/1)$ дорівнює ймовірності виконання нерівності $U_{з1} > U_{с\text{ макс}} > U_{ог}$, а ймовірність неправильної реєстрації посилки $p(1/0)$ визначається ймовірністю виконання нерівності $U_{з1} > U_{ог}$. Тоді для зазначених ймовірностей одержимо:

$$p(0/1) = \frac{1}{\pi} \left[\arccos(1-q_{oc}) \sqrt{h_c^2} \right], \quad 0 < h_c^2 < \frac{1}{(1-q_{oc})^2}; \quad (2.105)$$

$$p(1/0) = \frac{1}{\pi} \arccos(q_{oc} \sqrt{h_c^2}), \quad 0 < h_c^2 < \frac{1}{q_{oc}^2}. \quad (2.106)$$

При рівномірних наявності і відсутності сигналу з урахуванням імовірності появи імпульсної завади p_{zi} ймовірність помилкового приймання сигналів при заданому перевищенні h_c^2 буде

$$p_0 = \frac{p_{zi}}{\pi} \arccos(1 - q_{oc}) \sqrt{h_c^2} + \arccos q_{oc} \sqrt{h_c^2}. \quad (2.107)$$

Якщо відносний поріг спрацьовування $q_{oc} = 0,5$, то ймовірність помилки

$$p_0 = \frac{p_{zi}}{2\pi} \arccos \frac{h_c^2}{4}. \quad (2.108)$$

У тих випадках, коли величина h_c^2 не задана, але відомий закон її розподілу, ймовірність помилкового приймання описується формулою

$$p_0 = \frac{p_{zi}}{2\pi} \left[\int_0^{\alpha_2^2} \arccos(1 - q_{oc}) \sqrt{h_c^2} w(h_c^2) dh_c^2 + \int_0^{\frac{1}{q_{oc}^2}} \arccos(q_{oc} \sqrt{h_c^2}) w(h_c^2) dh_c^2 \right]. \quad (2.109)$$

При $q_{oc} = 0,5$ ймовірність

$$p_0 = \frac{p_{zi}}{\pi} \int_0^4 \arccos\left(\frac{h_c^2}{4}\right) w(h_c^2) dh_c^2. \quad (2.110)$$

Наведені вирази дозволяють робити кількісну оцінку впливу імпульсних завад при прийманні сигналів АМ.

Некогерентне приймання при зосереджених завадах. Нехай у каналі зв'язку діють сигнали АМ $u_c(t) = U_{c \text{ макс}} \sin \omega_c t$ і зосереджена завада $u_3(t) = U_{3 \text{ макс}} \sin \omega_3 t$. Останню можна подати у вигляді суми синфазної і квадратурної складових:

$$u_3(t) = U_{31} \sin \omega_c t + U_{32} \cos \omega_c t = U_{3 \text{ макс}} \sin \varphi_3 t \sin \omega_c t + U_{3 \text{ макс}} \sin \varphi_3 \cos \omega_c t,$$

де значення фазового кута завади $\varphi_3 = (\omega_c - \omega_3)t$ рівно ймовірні в інтервалі $(0, 2\pi)$. Тоді за аналогією з імпульсною завадою для ймовірності помилки можна написати

$$p_0 = \frac{p_{пз}}{2} \left[\frac{1}{\pi} \arccos \frac{h_c^2 (1 - q_{oc}^2) + 1}{2h_c^2} + p(1/0) \right], \quad (2.111)$$

де $p_{пз}$ – ймовірність появи зосередженої завади.

Когерентне приймання при зосереджених завадах. Вплив зосереджених завад при когерентному прийманні сигналів АМ аналогічно впливу імпульсних завад: тут також необхідно враховувати лише синфазну

складову, а фазовий кут завади може приймати будь-які значення з рівною ймовірністю в інтервалі $(0, 2\pi)$. Тому на підставі формальної аналогії для ймовірності помилок маємо

$$p_0 = \frac{P_{\text{пз}}}{\pi} \left[\arccos(1 - q_{\text{ос}}) \sqrt{h_c^2} + \arccos q_{\text{ос}} \sqrt{h_c^2} \right]. \quad (2.112)$$

При відносній границі обмеження $q_{\text{ос}} = 0,5$ одержимо

$$p_0 = \frac{P_{\text{пз}}}{\pi} \arccos \frac{h_c^2}{4}. \quad (2.113)$$

Якщо закон розподілу величини h_c^2 є відомим, то ймовірність помилкового приймання описується виразом (2.109) і (2.110)

2.6. Некогерентне та когерентне приймання при ЧМ

Спектр сигналів ЧМ. Якщо модулюючі імпульси мають прямокутну форму й змінюються в границях $0 < u_m(t) < 1$, то сигнали ЧМ можуть бути описані виразом

$$u_c(t) = U_{c \text{ макс}} \sin \left[\omega_0 t + F_d \int_{-\frac{T}{2}}^{\frac{T}{2}} [2u_m(t) - 1] dt + \varphi_0 \right], \quad (2.114)$$

де $U_{c \text{ макс}}$ – амплітуда модульованого високочастотного сигналу; ω_0 , φ_0 – кругова частота й початкова фаза несучих коливань. Цей вираз можна подати у вигляді

$$u_c(t) = U_{c \text{ макс}} \sin(\omega_0 t + \varphi_0) \cos \theta(t) + \cos(\omega_0 t + \varphi_0) \sin \theta(t), \quad (2.115)$$

де поточна фаза

$$\theta(t) = F_d \int_{-\frac{T}{2}}^{\frac{T}{2}} [2u_m(t) - 1] dt. \quad (2.116)$$

Для визначення спектра сигналу ЧМ необхідно знайти розкладання за Фур'є функцій $\cos \theta(t)$ і $\sin \theta(t)$ на інтервалі $-\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$. Нехай частота коливань ω_0 періодично змінюється від ω_{02} до ω_{01} й назад відповідно до модулюючих прямокутних імпульсів (рис. 2.44). Оскільки миттєва частота

$$\omega(t) = \frac{d\theta(t)}{dt} = \begin{cases} +F_d & \text{за } 0 < t < T_c; \\ -F_d & \text{за } -T_c < t < 0, \end{cases}$$

то, вибравши постійні інтегрування з умови безперервності фази, одержимо

$$\theta(t) = \int_{-\frac{T}{2}}^{\frac{T}{2}} \omega(t) dt = \begin{cases} +F_d \left(t - \frac{T_c}{2} \right) & \text{за } 0 < t < T_c; \\ -F_d \left(t + \frac{T_c}{2} \right) & \text{за } -T_c < t < 0. \end{cases}$$

Поточна фаза є періодичною функцією часу й, отже, $\cos\theta(t)$ і $\sin\theta(t)$ на інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$ можуть бути розкладені в ряди Фур'є:

$$\cos\theta(t) = a_0 + 2 \sum_{k=2, 4, 6, \dots}^{\infty} a_k \cos k\Omega t, \quad \sin\theta(t) = a_0 + 2 \sum_{k=1, 3, 5, \dots}^{\infty} b_k \cos k\Omega t,$$

де $\Omega = \frac{2\pi}{T}$.

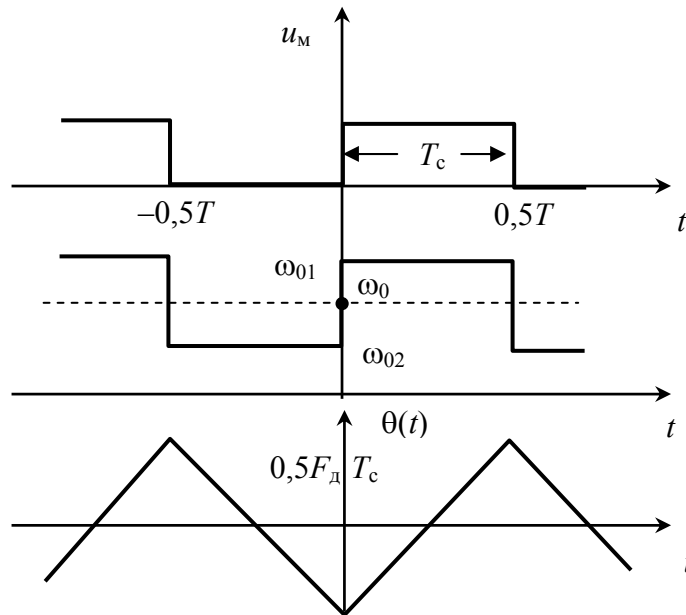


Рисунок 2.44 – ЧМ без розриву фази коливань:
а) сигнал; б) зміна частоти; в) зміна фази

Згідно з формулами коефіцієнти розкладання

$$a_0 = \frac{\sin \frac{\pi m_q}{2}}{\frac{\pi m_q}{2}}, \quad a_k = \frac{2m_q}{\pi} \cdot \frac{\sin \frac{\pi m_q}{2}}{m_q^2 - k^2}, \quad b_k = \frac{2m_q}{\pi} \cdot \frac{\cos \frac{\pi m_q}{2}}{m_q^2 - k^2}. \quad (2.117)$$

Тоді вираз (2.114) буде

$$u_c(t) = U_{c \text{ макс}} a_0 \sin(\omega_0 t + \varphi_0) + \\ + U_{c \text{ макс}} \sum_{k=2, 4, 6, \dots}^{\infty} a_k \left\{ \sin[(\omega_0 + k\Omega)t + \varphi_0] + \sin[(\omega_0 - k\Omega)t + \varphi_0] \right\} +$$

$$+U_{c \text{ макс}} \sum_{k=1, 3, 5, \dots}^{\infty} b_k \left\{ \cos[(\omega_0 + k\Omega)t + \varphi_0] + \cos[(\omega_0 - k\Omega)t + \varphi_0] \right\}, \quad (2.118)$$

де коефіцієнти a_0 , a_k і b_k визначаються формулами (2.117).

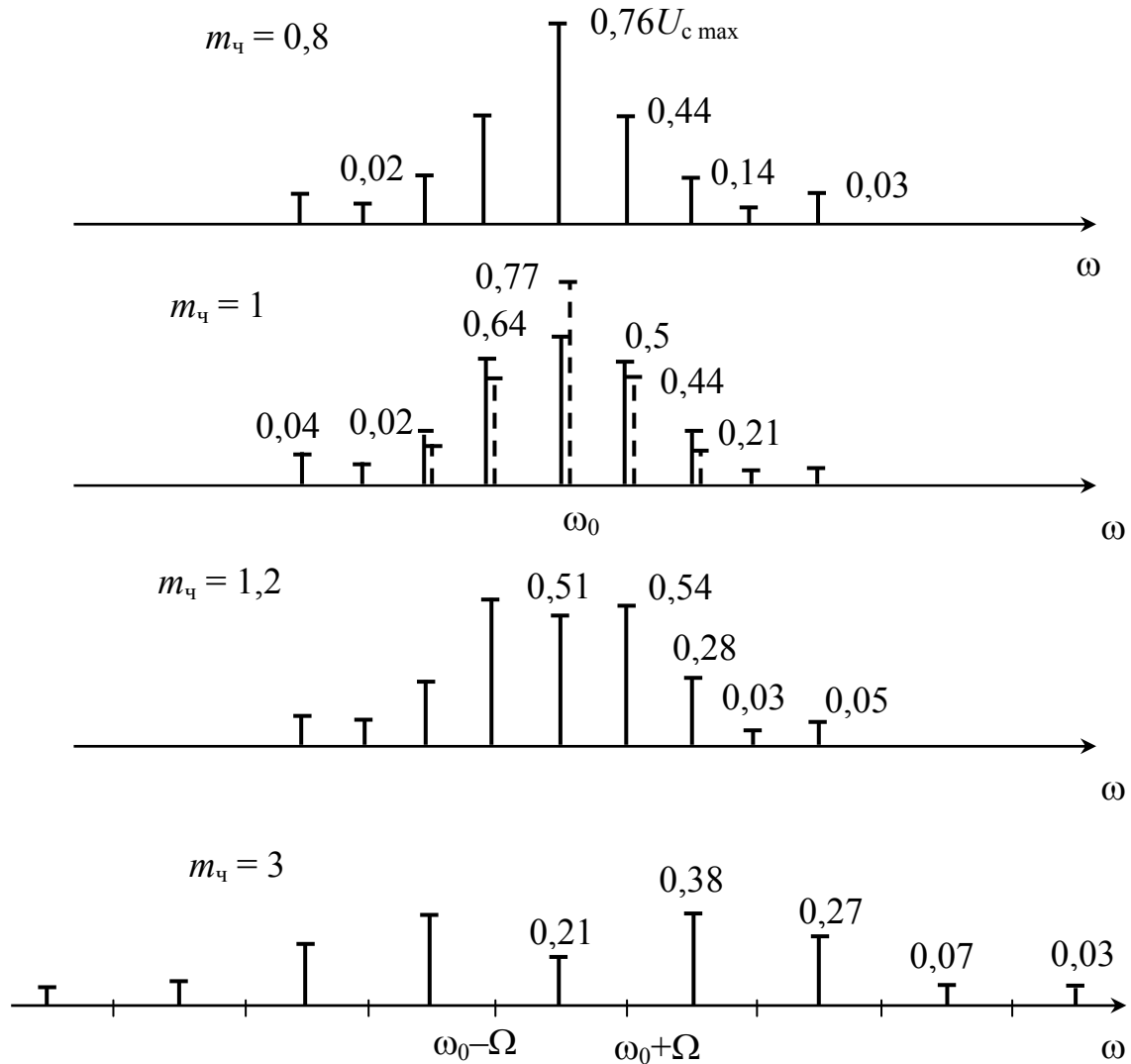


Рисунок 2.45 – Спектр сигналів ЧМ

Аналіз виразу (2.118) показує, що спектр сигналу ЧМ містить несуче коливання й дві бічні смуги частот. Складові цих смуг, що мають парні й непарні номери, підкоряються різним законам і мають фази, що відрізняються на 90° . Приклади спектрів при різних значеннях індексу m_q наведені на рис. 2.45, звідки видно, що форма спектра сигналу ЧМ складна й залежить від величини m_q . При $m_q = 1$ основна частка енергії сигналів знаходиться в несучому коливанні й перших двох бічних складових й, отже, ширина спектра вузькосмугового сигналу ЧМ приблизно дорівнює ширині спектра АМ сигналу. Зі збільшенням m_q спектр, сигналу ЧМ розширюється.

Якщо модуляція здійснюється «закругленими» послідовностями, близькими до синусоїдального коливання, то

$$u_c(t) = U_{c \text{ макс}} \sin\left(\omega_0 t + F_d \int \cos \Omega t dt + \varphi_0\right)$$

і вираз для спектра ЧМ сигналу має вигляд

$$u_c(t) = U_{c \text{ макс}} I_0(m_u) \sin(\omega_0 t + \varphi_0) + U_{c \text{ макс}} \sum_{k=1, 3, 5, \dots}^{\infty} I_k(m_u) \left\{ \sin[(\omega_0 + k\Omega)t + \varphi_0] + (-1)^k \sin[(\omega_0 - k\Omega)t - \varphi_0] \right\}, \quad (2.119)$$

де $I_k(m_u)$ – бesselеві функції першого роду.

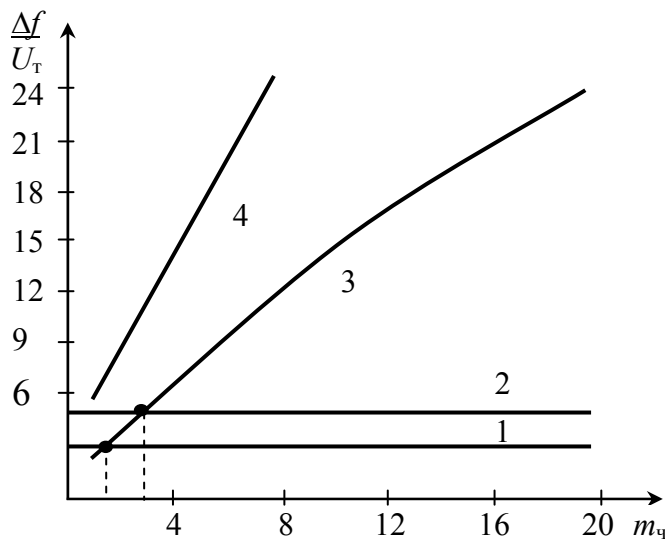


Рисунок 2.46 – Витрата смуги частот у дискретних каналах:

- 1 – канал АМ з постійними параметрами;
- 2 – канал АМ із завмираннями;
- 3 – канал ЧМ; 4 – канал ДЧМ

Спектр сигналу ЧМ при синусоїдальній функції $u_m(t)$ для значення $m_u = 1$ подано пунктиром на рис. 2.46. Порівняння його з випадком прямокутної функції $u_m(t)$ свідчить, що у першому випадку амплітуди бічних складових зі збільшенням їхнього номеру спадають швидше.

З виразів (2.118) і (2.119) випливає, що залежність між модулюючим $u_m(t)$ і модульованим $u_c(t)$ сигналами виражається нелінійною функціональною залежністю. Внаслідок цього частотну

модуляцію називають *нелінійною*.

Смуга частот при ЧМ. Смуга частот при ЧМ із точністю до 20% визначається виразами

$$\Delta f = \begin{cases} (1,3m_u + 1,4)B & \text{за } 1,5 \leq m_u \leq 8; \\ (1,1m_u + 3,1)B & \text{за } 8 < m_u \leq 20. \end{cases} \quad (2.120)$$

Для оцінювання смуги частот при заданих значеннях B і m_u зручно користуватися формулою

$$\Delta f = B(1 + m_u + \sqrt{m_u}), \quad (2.121)$$

що дає похибку оцінювання, у порівнянні з формулою (2.120) близько 3 – 5%.

На рис. 2.46 наведені криві, побудовані за формулами (2.118) і (2.120), що характеризують смугу частот на 1 Бод у режимах АМ (крива 1

– канал з постійними параметрами, крива 2 – канал із завмираннями) і ЧМ (крива 3). Із графіків видно, що в каналах із завмираннями ЧМ вимагає меншої смуги частот, ніж АМ, при значеннях $m_q < 2,8$, а в каналах з постійними параметрами – при $m_q < 1,5$. При великих індексах m_q смуга частот при ЧМ виходить ширше.

Некогерентне приймання сигналів. Дія флуктуаційних завад при некогерентному прийманні сигналів ЧМ має ряд особливостей у порівнянні із прийманням сигналів АМ. Ці особливості обумовлені наявністю у приймальному пристрої, частотних трактів, що не перекриваються, утворених роздільними фільтрами з однаковими ефективними смугами пропускання і коефіцієнтами передавання. Якість сигналу (його наявність або відсутність) визначається полярністю напруги на виході частотного детектора. Якщо передавалася, наприклад, наявність сигналу, то енергія коливань у тракті Φ_1 буде більше, ніж у тракті Φ_2 й вихідна напруга буде мати позитивну полярність; при наявності сигналу все навпаки. Це означає, що змінювання знака може відбутися в тому випадку, якщо пікове значення завади $|U_{ш}|$ в тракті без сигналу («холостий» тракт) перевищить амплітуду сумарного коливання сигналу й завади $|U_p|$ в тракті з посилкою («робочий» тракт). Ймовірність спільного настання зазначених подій – наявність коливання з амплітудою $|U_p|$ в робочому тракті й коливання з амплітудою $|U_{ш}|$ в холостому тракті – згідно з теоремою множення ймовірностей дорівнює

$$w(U_p) dU_p \int_{U_p}^{\infty} w(U_{ш}) dU_{ш}.$$

Тоді ймовірність спотворення посилки

$$p(0/1) = p(1/0) = \int_0^{\infty} w(U_p) \left[\int_{U_p}^{\infty} w(U_{ш}) dU_{ш} \right] dU_p.$$

При некогерентному прийманні сигналів необхідно враховувати синфазну й квадратурну складові флуктуаційної завади. Підставляючи значення $w(U_p)$ і $w(U_{ш})$, одержимо

$$p(0/1) = p(1/0) = e^{-h_c^2} \int_0^{\infty} q_p e^{-q_p^2} I_0(\sqrt{2h_c^2} q_p) dq_p,$$

де $q_p = \frac{U_p}{\sigma_{ш}}$.

Зазначений інтеграл – табличний і має значення

$$p(0/1) = p(1/0) = \frac{1}{2} e^{-\frac{h_c^2}{2}}. \quad (2.122)$$

Вважаючи наявність й відсутність сигналу рівноймовірними, для повної ймовірності помилок одержимо

$$p_0 = \frac{1}{2} e^{-\frac{h_c^2}{2}}.$$

Когерентне приймання сигналів. У цьому випадку необхідно враховувати, що в кожному частотному тракті приймального пристрою діють лише синфазні складові завади, що підлягають нормальному закону розподілу і мають однакові дисперсії $\sigma_{ш}^2$. Спотворення посилок трапляються тоді, коли амплітуда завади в холостому тракті $|U_{шx}|$ перевищує амплітуду сумарного коливання сигналу $|U_c|$ і завади $|U_{шp}|$ в робочому тракті. Ймовірність цієї події

$$p(U_{шx} > U_c + U_{шp}) = \int_{U_c + U_{шp}}^{\infty} w(U_{шx}) dU_{шx}.$$

Інтегруючи за всіма значеннями амплітуди завади $|U_{шp}|$, одержимо ймовірність спотворення послілки

$$p(0/1) = p(1/0) = \int_{-\infty}^{\infty} w(U_{шp}) \left[\int_{U_c + U_{шp}}^{\infty} w(U_{шx}) dU_{шx} \right] dU_{шp}.$$

Вважаючи наявність й відсутність сигналу рівноймовірними, для повної ймовірності помилок маємо

$$p_0 = V(\sqrt{h_c^2}). \quad (2.123)$$

Некогерентне приймання сигналів при імпульсних завадах. Оскільки обидва частотних тракту в приймальному пристрої однакові, то вплив завад за наявності й відсутності сигналу буде однаковим. Умова спотворення посилок залишається таким, як і при флуктуаційних завадах, і може бути записана у вигляді

$$U_p^2 = (U_{c \text{ макс}} - U_{з \text{ макс}} \cos \varphi_3)^2 + U_{з \text{ макс}}^2 \sin^2 \varphi_3 < U_{з \text{ макс}}.$$

Звідси ймовірність спотворення послілки дорівнює ймовірності виконання нерівності $h_c^2 - 2h_c \cos \varphi_3 < 0$ або $\varphi_3 > \arccos \frac{h_c^2}{4}$ за $0 < h_c^2 < 4$.

Враховуючи ймовірність появи завади p_{zi} й рівномірний закон розподілу її фазового кута в інтервалі $(0, 2\pi)$, для повної ймовірності помилки одержимо

$$p_0 = \frac{p_{zi}}{\pi} \arccos \frac{h_c^2}{4}, \quad 0 < h_c^2 < 4. \quad (2.124)$$

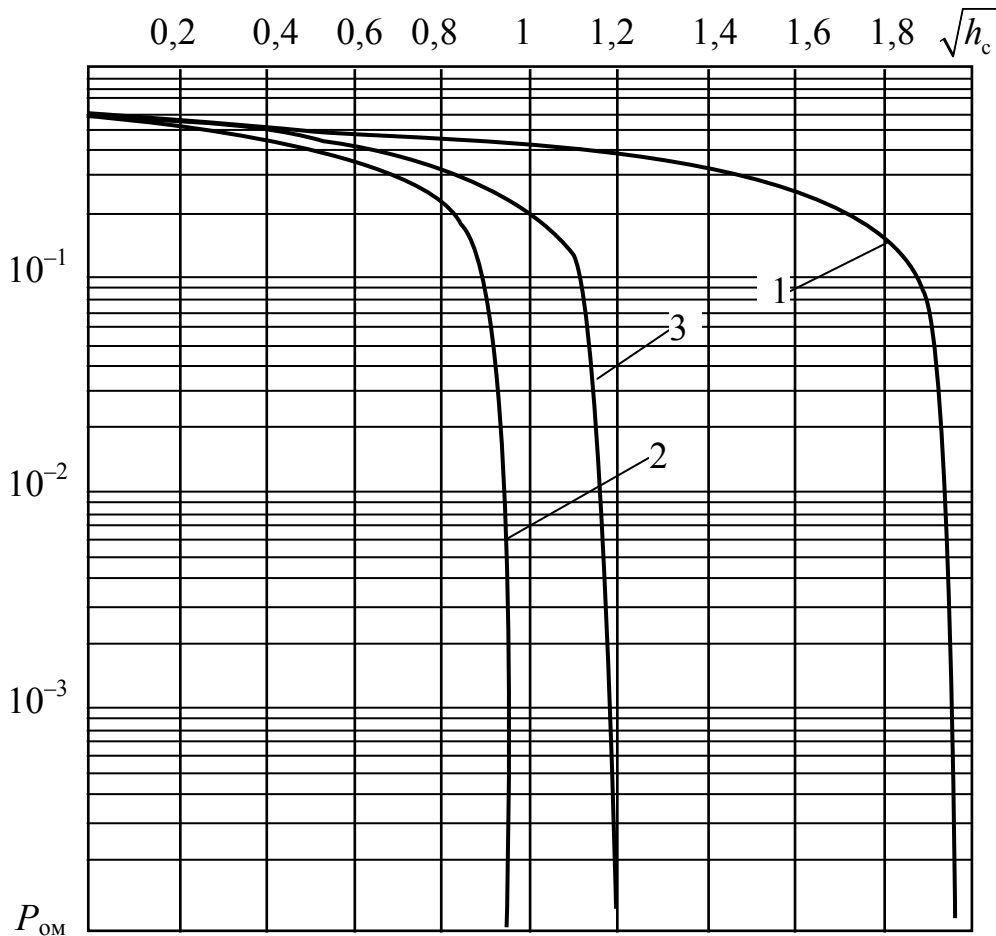


Рисунок 2.47 – Характеристики завадостійкості дискретних каналів при імпульсних (ІЗ) та зосереджених (ЗЗ) завадах:
 1 – когерентне АМ при ІЗ та ЗЗ, когерентне та некогерентне ЧМ при ІЗ;
 2 – ФМ при ІЗ та ЗЗ; 3 – ДФМ при ІЗ та ЗЗ

Якщо відомий закон розподілу спектральної густини завади в границях смуги пропускання розділового фільтра, тобто якщо відома функція $w(h_c^2)$, то ймовірність помилки

$$p_0 = \frac{P_{zi}}{\pi} \int_0^4 \arccos \frac{h_c^2}{4} w(h_c^2) dh_c^2. \quad (2.125)$$

Вираз (2.124) подано на рис. 2.47 (крива 1), де по осі ординат відкладена нормована ймовірність помилки $p_{он} = \frac{p_0}{P_{zi}}$. На цьому ж рисунку наведена характеристика завадостійкості когерентного приймання сигналів АМ при імпульсних завадах. Збіг обох кривих свідчить про рівність завадостійкості каналів ЧМ при некогерентному прийманні й каналів АМ при когерентному прийманні.

Як зазначалося раніше, технічна реалізація когерентного приймання сигналів пов'язана зі значними труднощами, особливо при флуктуаціях

параметрів каналів. Тому постає питання порівняти завадостійкість каналів ЧМ і АМ при некогерентному прийманні. Припустимо, що величина h_c^2 в інтервалі значень $0 < h_c^2 < 4$ постійна й дорівнює h_{co}^2 . Тоді на підставі (2.125) ймовірність помилки

$$p_{0(\text{чм})} = \frac{2}{\pi} \sqrt{h_c^2} p_{zi}.$$

При некогерентному прийманні сигналів АМ ймовірність помилки при тих же допущеннях описується виразом

$$p_{0(\text{ам})} = p_{zi} h_{co}^2 \left[\frac{1}{2\pi} \int_{\frac{4}{9}}^4 \arccos\left(\frac{3h_c^2 + 4}{8h_c^2}\right) dh_c^2 + \frac{1}{2} \right].$$

Якщо величина інтеграла не перевищує двох. Тоді ймовірність помилки

$$p_{0(\text{ам})} \leq \frac{2 + \pi}{2\pi} p_{zi} \sqrt{h_c^2}.$$

і, отже, $p_{0(\text{ам})} \approx 1,3 p_{0(\text{чм})}$.

Одержана оцінка, звичайно, є приблизною, але корисною для практики; вона дозволяє стверджувати, що завадостійкість некогерентного приймання сигналів ЧМ при дії імпульсних завад приблизно на 30 – 40% краще, ніж при некогерентному прийманні сигналів АМ.

Когерентне приймання сигналів при імпульсних завадах. У цьому випадку, як і раніше, необхідно враховувати вплив лише синфазної складової завади в обох частотних трактах приймального пристрою. Оскільки ці тракти однакові, то амплітуди складових завади будуть однаковими та дорівнювати $U_{z \text{ макс}} \cos \varphi_3$. Умова спотворення посилки має вигляд

$$U_{z \text{ макс}} \cos \varphi_3 > U_{c \text{ макс}} - U_{z \text{ макс}} \cos \varphi_3$$

і означає перевищення рівня завади в холостому тракті над рівнем сумарного колювання в робочому тракті. Звідси випливає нерівність

$$\cos \varphi_3 > \frac{h_c^2}{4}.$$

З урахуванням рівномірного розподілу фазового кута завади в інтервалі $(0, 2\pi)$ ймовірність спотворення посилки

$$p(0/1) = p(1/0) = \frac{1}{\pi} \arccos \frac{h_c^2}{4}.$$

Вважаючи, як і раніше, що наявність й відсутність сигналу рівноймовірні, для повної ймовірності спотворень сигналів ЧМ при величині перевищення сигналу h_c^2 і ймовірності появи імпульсної завади p_{zi} одержимо

$$p_0 = \frac{P_{zi}}{\pi} \arccos \frac{h_c^2}{4}, \quad (0 < h_c^2 < 4). \quad (2.126)$$

Якщо відомий закон розподілу спектральної густини завади в границях смуги пропускання розділового фільтра, тобто величина $w(h_c^2)$, то ймовірність помилки

$$p_0 = \frac{P_{zi}}{\pi} \int_0^4 \arccos \frac{h_c^2}{4} w(h_c^2) dh_c^2. \quad (2.127)$$

Отже, канали ЧМ мають однакову завадостійкість до імпульсних завад при когерентному і некогерентному прийманні сигналів. Тому для розглянутого випадку можна користуватися кривій 1 рис. 2.47.

Розглянемо завадостійкість при зосереджених завадах.

Некогерентне приймання сигналів при зосереджених завадах. Дія зосереджених завад при некогерентному прийманні сигналів ЧМ характеризується деякими особливостями. Завади так же, як і посилки, являють собою гармонійні коливання й можуть потрапити в смугу пропускання кожного з розділових фільтрів. Тому в цей момент часу завадами можуть бути уражені кожний із частотних трактів приймача або обидва тракти одночасно. При цьому слід враховувати, що поява завади з амплітудою $U_{з\text{ макс}}$ в холостому тракті по своїй дії аналогічно введенню граничного рівня $U_{ог} = U_{з\text{ макс}}$ в каналах АМ, оскільки посилка в робочому тракті буде зареєстрована лише в тому випадку, якщо вона буде перевищувати цей рівень. Повна ймовірність помилки

$$p_0 = p_0^{(12)} + p_0^{(1)} + p_0^{(2)}, \quad (2.128)$$

де $p_0^{(1)}$, $p_0^{(2)}$ – ймовірності спотворення посилок при потраплянні завади в один із частотних трактів; $p_0^{(12)}$ – ймовірність спотворення посилок при одночасній дії завади в обох частотних трактах. Якщо завада потрапила в робочий тракт, то вона не призведе до спотворення посилки, а призведе лише до зростання рівня сумарного коливання. При потраплянні завади в холостий тракт спотворення посилок будуть виникати з ймовірністю

$$p_0^{(1)} = p_0^{(2)} = \begin{cases} 1 & \text{за } U_{з\text{ макс}} > U_{с\text{ макс}}; \\ 0 & \text{за } U_{з\text{ макс}} < U_{с\text{ макс}}. \end{cases} \quad (2.129)$$

Вираз для ймовірності спотворень посилок при одночасному потраплянні завади в обидва частотних тракти може бути наведено за аналогією з формулою (2.103). При цьому необхідно врахувати наступне. У виразі (2.103) параметр q_{oc} являє собою нормований відносно амплітуди сигналу поріг обмеження. При ЧМ наявність двох частотних трактів призводить до двох нормованих порогів обмеження:

– для тракту наявності сигналу на частоті f_{01}

$$q_{\text{ос}}^{(1)} = \frac{U_{3 \text{ макс}}^{(2)}}{U_{c \text{ макс}}} = \frac{1}{\sqrt{h_{c1}^2}};$$

– для тракту відсутності сигналу на частоті f_{02}

$$q_{\text{ос}}^{(2)} = \frac{U_{3 \text{ макс}}^{(1)}}{U_{c \text{ макс}}} = \frac{1}{\sqrt{h_{c2}^2}}.$$

Тоді, якщо p_{312} – імовірність одночасного потрапляння зосередженої завади в обидва розділових фільтри, то повна ймовірність помилки

$$p_0 = \frac{p_3^{(12)}}{2\pi} \left[\arccos \frac{h_{c1}^2 \left(1 - \frac{1}{h_{c2}^2}\right) + 1}{2\sqrt{h_{c1}^2}} + \arccos \frac{h_{c2}^2 \left(1 - \frac{1}{h_{c1}^2}\right) + 1}{2\sqrt{h_{c2}^2}} \right]. \quad (2.130)$$

де значення перевищень сигналу для трактів наявності і відсутності сигналу лежать у границях

$$\frac{h_{c2}^2}{h_{c2}^2 - 1} > h_{c1}^2 > \frac{h_{c2}^2}{h_{c2}^2 + 1}; \quad \frac{h_{c1}^2}{h_{c1}^2 - 1} > h_{c2}^2 > \frac{h_{c1}^2}{h_{c1}^2 + 1}. \quad (2.131)$$

Когерентне приймання сигналів при зосереджених завадах. Повна ймовірність помилки приймання сигналів ЧМ при дії в каналі зосереджених завад описується виразом (2.94). Однак при оцінці завадостійкості когерентного приймання необхідно також враховувати можливий зсув синфазних складових завади за частотою і фазою відносно наявності і відсутності сигналу у границях смуги пропускання розділових фільтрів.

Тоді вираз для повної ймовірності помилок, вважаючи наявність й відсутність сигналу рівноймовірними, можна подати у вигляді

$$p_0 = \frac{1}{2} \left[\left(p_3^{(12)} p_{11} + p_0^{(2)} p_{12} \right) + \left(p_3^{(12)} p_{21} + p_{21} p_{22} \right) \right], \quad (2.132)$$

де p_{11} , p_{12} , p_{21} , p_{22} – імовірності спотворення наявного і відсутнього сигналу відповідно в першому й другому трактах.

При когерентному прийманні сигналів спотворення посилок можуть викликатися двома причинами. При наявності завад в обох частотних трактах (імовірність $p_3^{(12)}$) спотворення посилок з ймовірностями p_{11} й p_{21} може відбуватися через вплив синфазних складових завади, розладнаних за частотою і фазою відносно робочого сигналу. Величина цих складових дорівнює:

– у тракті наявного сигналу

$$U_{3 \text{ макс}}^{(1)} \cos \nu_1;$$

– у тракці відсутнього сигналу

$$U_{3 \text{ макс}}^{(2)} \cos \nu_2.$$

Тут $\nu_1 = \Delta\omega_{31}t + \varphi_{31}$, $\nu_2 = \Delta\omega_{32}t + \varphi_{32}$ – поточні значення фази завади, рівномірно розподілені в інтервалі $(0, 2\pi)$, де $\Delta\omega_{31} = \omega_3 - \omega_{01}$, $\Delta\omega_{32} = \omega_3 - \omega_{02}$ – розладнання несучої частоти завади відносно частот наявних і відсутніх сигналів ω_{01} і ω_{02} ; φ_{31} , φ_{32} – початкові фазові кути завади відносно робочих сигналів.

Умова спотворення наявного сигналу при цьому має вигляд

$$U_{3 \text{ макс}}^{(2)} \cos \nu_2 > U_{c \text{ макс}} - U_{3 \text{ макс}}^{(1)} \cos \nu_1$$

або після перетворень

$$\cos \nu_1 > \sqrt{h_{c1}^2} - \xi_{21} \cos \nu_2, \quad (2.133)$$

де $\xi_{21} = \frac{U_{3 \text{ макс}}^{(2)}}{U_{3 \text{ макс}}^{(1)}}$ – відношення амплітуд завади в трактах відсутнього сигналу.

Аналогічна умова спотворення відсутнього сигналу буде

$$\cos \nu_2 > \sqrt{h_{c2}^2} - \xi_{12} \cos \nu_1, \quad (2.134)$$

де $\xi_{12} = \frac{U_{3 \text{ макс}}^{(1)}}{U_{3 \text{ макс}}^{(2)}}$.

Спотворення посилок може викликатися також влученням завади лише в тракт наявного сигналу (ймовірність $p_3^{(1)}$) або лише в тракт відсутнього сигналу (ймовірність $p_3^{(2)}$), але за умови, що в цей момент часу цей тракт є холостим. У цьому випадку умови спотворення посилок будуть:

$$U_{3 \text{ макс}}^{(2)} \cos \nu_2 > U_{c \text{ макс}}; U_{3 \text{ макс}}^{(1)} \cos \nu_1 > U_{c \text{ макс}}. \quad (2.135)$$

На підставі нерівності (2.99) ймовірність спотворення наявного сигналу в першому частотному тракці

$$p_{11} = \frac{1}{\pi} \arccos\left(\sqrt{h_{c1}^2} - \xi_{21} \cos \nu_2\right). \quad (2.136)$$

Для обчислення ймовірності p_{01} необхідно встановити границі змінювання випадкової величини ν_2 й проінтегрувати вираз (2.136) у зазначених границях з врахуванням того, що густина ймовірності

$$w(\nu_2) = \frac{1}{2\pi}.$$

З виразу (2.136) виходить, що $\sqrt{h_{c1}^2} > \xi_{21} \cos \nu_2 > \sqrt{h_{c1}^2} - 1$, звідки

$$\alpha_2 > \cos \nu_2 > \alpha_1 \left(\alpha_1 = \frac{\sqrt{h_{c1}^2} - 1}{\xi_{21}}; \alpha_2 = \frac{\sqrt{h_{c1}^2}}{\xi_{21}} \right).$$

Тому ймовірність спотворення наявного сигналу

$$p_{11} = \frac{1}{\pi^2} \int_{\alpha_1}^{\alpha_2} \arccos(\sqrt{h_{c1}^2} - \xi_{21} \cos \nu_2) d\nu_2. \quad (2.137)$$

Аналогічно для ймовірності спотворення відсутнього сигналу з врахуванням (2.134) одержимо

$$p_{11} = \frac{1}{\pi^2} \int_{\alpha_3}^{\alpha_4} \arccos(\sqrt{h_{c2}^2} - \xi_{12} \cos \nu_1) d\nu_1, \quad (2.138)$$

де

$$\alpha_3 = \frac{\sqrt{h_{c1}^2} - 1}{\xi_{12}}; \quad \alpha_4 = \frac{\sqrt{h_{c2}^2}}{\xi_{12}}.$$

Вирази для ймовірностей спотворення p_{12} і p_{22} виходять із умови (2.135) і становлять

$$p_{12} = \frac{1}{\pi} \arccos \sqrt{h_{c2}^2}; \quad p_{22} = \frac{1}{\pi} \arccos \sqrt{h_{c1}^2}. \quad (2.139)$$

Тоді остаточно повна ймовірність помилки приймання сигналів ЧМ при значеннях перевищення сигналів h_{c1}^2 і h_{c2}^2 описується виразом

$$p_0 = \frac{1}{2\pi^2} \left[p_3^{(12)} \int_{\alpha_1}^{\alpha_2} \arccos(\sqrt{h_{c1}^2} - \xi_{21} \cos \nu_2) d\nu_2 + p_0^{(2)} \arccos \sqrt{h_{c2}^2} + \int_{\alpha_3}^{\alpha_4} \arccos(\sqrt{h_{c2}^2} - \xi_{12} \cos \nu_1) d\nu_1 + p_0^{(1)} \arccos \sqrt{h_{c1}^2} \right]. \quad (2.140)$$

Якщо відомі закони розподілу завад в обох частотних трактах, тобто якщо відомі величини $w(h_{c1}^2)$, $w(h_{c2}^2)$, $w(\xi_{12})$ і $w(\xi_{21})$, то ймовірність повної помилки

$$p_0 = \frac{1}{2\pi^2} \left[p_3^{(12)} \int_0^\infty w(\xi_{21}) \left[\int_0^{\xi_{21}} w(h_{c1}^2) \left(\int_{\alpha_1}^{\alpha_2} \arccos(\sqrt{h_{c1}^2} - \xi_{21} \cos \nu_2) d\nu_2 \right) dh_{c1}^2 \right] d\xi_{21} + p_3^{(2)} \int_0^1 \arccos \sqrt{h_{c2}^2} w(h_{c2}^2) dh_{c2}^2 + p_3^{(12)} \int_0^\infty w(\xi_{12}) \left[\int_0^{\xi_{12}} w(h_{c2}^2) \times \left(\int_{\alpha_3}^{\alpha_4} \arccos(\sqrt{h_{c2}^2} - \xi_{12} \cos \nu_1) d\nu_1 \right) dh_{c2}^2 \right] d\xi_{12} + p_3^{(1)} \int_0^1 \arccos \sqrt{h_{c1}^2} w(h_{c1}^2) dh_{c1}^2 \right]. \quad (2.14)$$

1)

Наведені вирази дозволяють оцінювати завадостійкість когерентного приймання сигналів ЧМ при зосереджених завадах. Однак велике число складових параметрів ускладнює побудову розрахункових графіків. Тому

становлять практичний інтерес граничні оцінки завадостійкості. Потрапляння зосередженої завади в холостий тракт приймача за своїм ефектом еквівалентно дії імпульсних завад у паузах при АМ з тією лише різницею, що амплітуда сигналу ЧМ відіграє роль границі обмеження. Потрапляння зосередженої завади в робочий тракт приймача спотворень сигналів ЧМ не викликає. Якщо ж завада потрапляє одночасно в обидва частотних тракти, то залежно від параметрів зосередженої завади її дія може бути наближена або до флуктуаційних завад, або до імпульсних. Тому в загальному випадку завадостійкість каналів ЧМ при зосереджених завадах може коливатися в границях, характерних для флуктуаційних й імпульсних завад.

2.7. Некогерентне та когерентне приймання при ФМ

Спектр сигналів ФМ. Змінювання частоти в границях $\pm F_d$ модулюючим коливанням із частотою F_m еквівалентно змінюванню фази в межах кута

$$|\varphi_{\text{макс}}| = \frac{\Omega_d}{\Omega_m}.$$

Тому при ФМ так само, як і при ЧМ, можна користуватися поняттям *індексу фазової модуляції*, що характеризує величину стрибка фази, величина якого

$$m_\phi = \frac{\Omega_d}{\Omega_m}. \quad (2.142)$$

Якщо модулюючі імпульси змінюються в границях $0 < u_m(t) < 1$, то високочастотні модульовані сигнали будуть

$$u_c(t) = U_{c \text{ макс}} \sin[\omega_0 t + m_\phi u_m(t) + \varphi_0]. \quad (2.143)$$

Цей вираз можна подати у вигляді

$$u_c(t) = U_{c \text{ макс}} \left\{ \sin(\omega_0 t + \varphi_0) \cos[m_\phi u_m(t)] + \cos(\omega_0 t + \varphi_0) \sin[m_\phi u_m(t)] \right\}. \quad (2.144)$$

Для визначення спектра сигналу ФМ досить знайти спектри функцій $\cos[m_\phi u_m(t)]$ і $\sin[m_\phi u_m(t)]$, використовуючи загальний метод розкладання їх у ряди Фур'є. Однак для прямокутних модулюючих імпульсів $u_m(t)$ можна скористатися іншим, більш простим і наочним способом.

Фазову маніпуляцію з довільним кутом m_ϕ можна розглядати як результат додавання немодульованого несучого коливання $u_c(t) = U_{c \text{ макс}} \sin[\omega_0 t + \varphi_0]$ й двох сигналів АМ тривалістю T_c такої ж

амплітуди і з фазами $\varphi_0 + \pi$ й $\varphi_0 + m_\phi$ (рис. 2.48, а, б, в). Ці сигнали можна подати як один імпульс із новими значеннями амплітуди й фази:

$$\begin{aligned} u_p(t) &= U_{c \text{ макс}} \sin(\omega_0 t + \varphi_0 + \pi) + U_{c \text{ макс}} \sin(\omega_0 t + \varphi_0 + m_\phi) = \\ &= U_{c \text{ макс}} \left[(\cos m_\phi - 1) \sin(\omega_0 t + \varphi_0) + \sin m_\phi \cos(\omega_0 t + \varphi_0) \right]. \end{aligned}$$

Останній вираз можна подати у вигляді

$$u_p(t) = U_{p \text{ макс}} \sin(\omega_0 t + \varphi_0 + \theta_\phi),$$

де

$$U_{p \text{ макс}} = U_{c \text{ макс}} \sqrt{(\cos m_\phi - 1)^2 + \sin^2 m_\phi} = 2U_{c \text{ макс}} \sin \frac{m_\phi}{2};$$

$$\theta_\phi = \operatorname{arctg} \frac{\sin m_\phi}{\cos m_\phi - 1} = \frac{\pi}{2} + \frac{m_\phi}{2}.$$

Тоді остаточно

$$u_p(t) = 2U_{c \text{ макс}} \sin \frac{m_\phi}{2} \sin \left(\omega_0 t + \varphi_0 + \frac{\pi}{2} + \frac{m_\phi}{2} \right), \quad (2.146)$$

і при передаванні височастотних посилок тривалістю T_c утворюється послідовність сигналів, модульованих за фазою на кут m_ϕ (рис. 2.48, г).

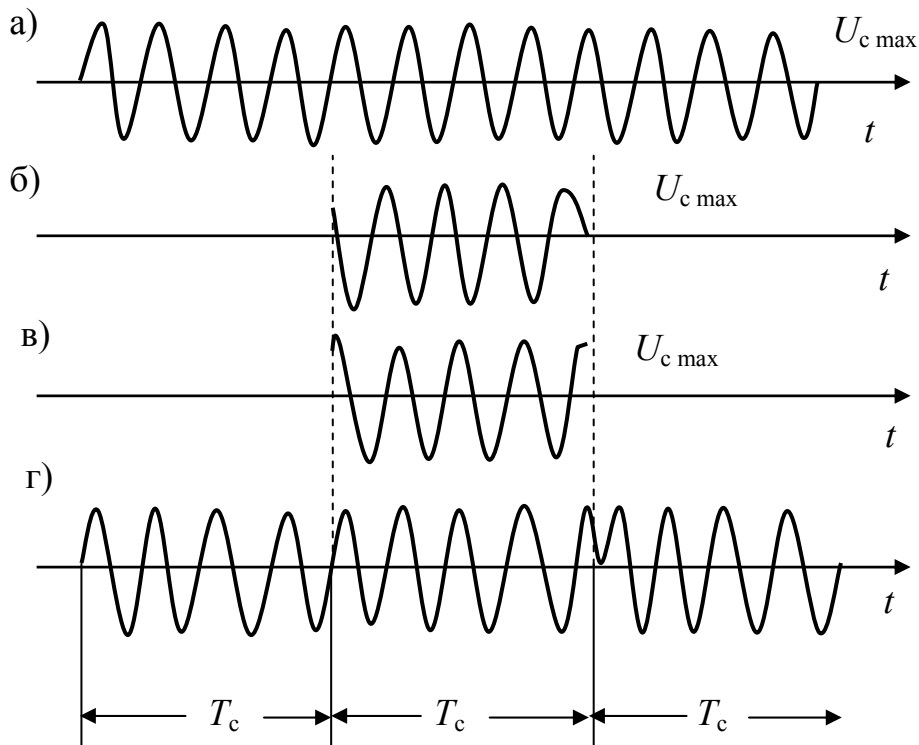


Рисунок 2.48 – Формування сигналів ФМ

Отже, фазову модуляцію при стрибку фази на будь-який кут m_ϕ можна розглядати як суму сигналу АМ і немодульованого несучого колювання. Це означає, що спектри сигналів ФМ і АМ збігаються за формою обвідної.

Вираз для спектра сигналу (2.145) можна одержати, помноживши амплітуди бічних складових сигналу АМ на $2 \sin \frac{m_\phi}{2}$ й зрушивши їх фази на кут $\frac{\pi}{2} + \frac{m_\phi}{2}$. Тоді після перетворень будемо мати:

$$u_c(t) = \frac{U_{c \text{ макс}}}{q_0} \sqrt{(q_0 - 1 + \cos m_\phi)^2 + \sin^2 m_\phi} \sin \left(\omega_0 t + \varphi_0 + \arctg \frac{\sin m_\phi}{q_0 - 1 + \cos m_\phi} \right) +$$

$$+ \frac{2U_{c \text{ макс}}}{q_0} \sin \frac{m_\phi}{2} \sum_{k=1}^{\infty} \frac{\sin \frac{k\pi}{q_0}}{\frac{k\pi}{q_0}} \left\{ \sin \left[(\omega_0 + k\Omega_m) t + \varphi_0 + \frac{\pi}{2} + \frac{m_\phi}{2} \right] + \right.$$

$$\left. + \sin \left[(\omega_0 - k\Omega_m) t + \varphi_0 + \frac{\pi}{2} + \frac{m_\phi}{2} \right] \right\}. \quad (2.147)$$

При шпаруватості $q_0 = 2$ і $m_\phi = \pi$ вираз (2.147) спрощується й приймає вигляд:

$$u_c(t) = U_{c \text{ макс}} \sum_{k=1}^{\infty} \frac{\sin \frac{k\pi}{2}}{\frac{k\pi}{2}} \left\{ \sin [(\omega_0 + k\Omega_m) t + \varphi_0] + \sin [(\omega_0 - k\Omega_m) t + \varphi_0] \right\}. \quad (2.148)$$

Приклади спектрів сигналів ФМ наведені на рис. 2.49. Оскільки амплітуди бічних складових сигналу ФМ відрізняються від сигналу АМ на $2 \sin \frac{m_\phi}{2}$, то при $m_\phi = \frac{\pi}{3}$ вони збігаються; при $m_\phi = \frac{\pi}{2}$ рівень складових у спектрі сигналу ФМ приблизно в 1,5 рази, а при $m_\phi = \pi$ у два рази більше, ніж при АМ. Амплітуда несучого колювання при ФМ значно відрізняється від амплітуди несучого колювання при АМ; при зростанні m_ϕ від 0 до π вона зменшується від $U_{c \text{ макс}}$ до $U_{c \text{ макс}} \left(1 - \frac{2}{q_0} \right)$ і при періодичному передаванні «точок» ($q_0 = 2$) перетворюється на нуль.

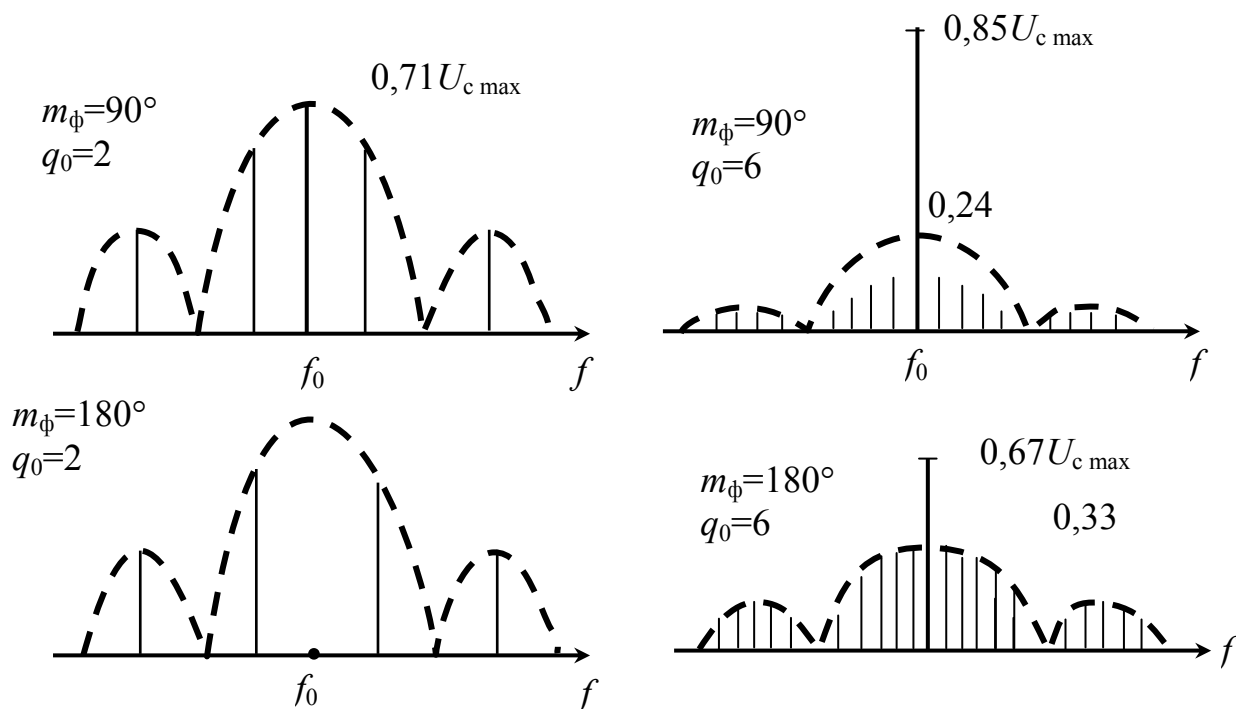


Рисунок 2.49 – Спектри сигналів ФМ

Таким чином, при модуляції прямокутними імпульсами, обвідна спектра сигналу ФМ має таку ж форму, що й спектр модулюючих імпульсів.

При фазовій модуляції синусоїдальними коливаннями високочастотний сигнал

$$u_c(t) = U_{c \text{ макс}} \sin\left(\omega_0 + \varphi_0 + \frac{m_\phi}{2} \cos \Omega_m t\right)$$

має спектр, описуваний виразом

$$u_c(t) = U_{c \text{ макс}} I_0\left(\frac{m_\phi}{2}\right) \sin(\omega_0 t + \varphi_0) + \sum_{k=1, 3, 5, \dots}^{\infty} (-1)^{\frac{k+3}{2}} I_k\left(\frac{m_\phi}{2}\right) \left\{ \cos[(\omega_0 + k\Omega_m)t + \varphi_0] + \right. \\ \left. + \cos[(\omega_0 - k\Omega_m)t + \varphi_0] \right\} + U_{c \text{ макс}} \sum_{k=2, 4, 6, \dots}^{\infty} (-1)^{\frac{k}{2}} I_k\left(\frac{m_\phi}{2}\right) \left\{ \sin[(\omega_0 + k\Omega_m)t + \varphi_0] + \right. \\ \left. + \sin[(\omega_0 - k\Omega_m)t + \varphi_0] \right\}, \quad (2.149)$$

де $I_k\left(\frac{m_\phi}{2}\right)$ – бesselеві функції першого роду.

Із цього виразу випливає, що спектр фазомодульованого сигналу містить нескінченно велику кількість складових. Лише при малих значеннях індексу m_ϕ (менше $\frac{\pi}{3}$) усіма бічними складовими, крім перших, у формулі (2.149) можна знехтувати. Тоді одержимо

$$u_c(t) = U_{c \text{ макс}} \sin(\omega_0 t + \varphi_0) + \frac{U_{c \text{ макс}} m_\phi}{4} \left\{ \cos[(\omega_0 + k\Omega_m)t + \varphi_0] + \cos[(\omega_0 - k\Omega_m)t + \varphi_0] \right\}$$

де m_ϕ виміряється в радіанах.

Спектр сигналу при МФМ. Напряга на виході n -фазного модулятора за час $\frac{n}{F_m}$, яка відповідає повороту вектора сигналу на кут 2π , складатиме

$$u_c(t) = \sum_{k=1}^n u_k(t),$$

де

$$u_k(t) = \begin{cases} U_{c \text{ макс}} \cos \left[\omega_0 t - (k-1) \frac{2\pi}{k} \right] & \text{за } \frac{k-1}{2F_m} < t < \frac{k}{2F_m} \\ 0 & \text{за } \frac{1}{2F_m} < t < \frac{n}{2F_m} \text{ і } \frac{2}{2F_m} < t < \frac{n}{2F_m} (k=2) \text{ і т.д.} \end{cases}$$

Таким чином, сигнал МФМ також може бути поданий у вигляді суми періодичних коливань, модульованих по амплітуді. Розкладаючи кожне з коливань $u_k(t)$ у ряд Фур'є, одержимо вираз для спектра сигналу МФМ:

$$u_c(t) = U_{c \text{ макс}} \sum_{k=1}^{\infty} \left[\frac{1}{B_1} \sin B_1 \cos(\omega_0 + \gamma_1)t + \frac{1}{B_1} (1 - \cos B_1) \sin(\omega_0 + \gamma_1)t \right] + \\ + \sum_{k=0}^{\infty} \left[\frac{1}{B_2} \sin B_2 \cos(\omega_0 + \gamma_2)t - \frac{1}{B_2} (1 - \cos B_2) \sin(\omega_0 + \gamma_2)t \right], \quad (2.150)$$

де

$$B_1 = \frac{2\pi}{n}(kn-1); \quad B_2 = \frac{2\pi}{n}(kn+1); \quad \gamma_1 = \frac{2\Omega_m}{n}(kn-1); \quad \gamma_2 = \frac{2\Omega_m}{n}(kn+1).$$

Несуче коливання в спектрі сигналу МФМ відсутнє, а потужності бічних смуг значно відрізняються одна від одної. Для ілюстрації оцінимо розподіл потужності в спектрі сигналу при числі фаз $n=4$. З формули (2.150) випливає, що потужність нижньої бічної смуги

$$P_n = \frac{4U_{c \text{ макс}}^2}{\pi^2} \left(1 + \frac{1}{5^2} + \frac{1}{9^2} + \frac{1}{13^2} + \dots \right).$$

Оскільки потужність обох смуг $P_c = \frac{U_{c \text{ макс}}^2}{2}$, то

$$P_n = \frac{8}{\pi^2} \left(1 + \frac{1}{5^2} + \frac{1}{9^2} + \frac{1}{13^2} + \dots \right) P_c \approx 0,87 P_c.$$

Отже, одна бічна смуга містить 87% усієї потужності сигналу, а інша – лише 13%. Це дозволяє, застосовуючи односмугове передавання, звузити

смугу частот приблизно у два рази. Оскільки перехід від однократної ФМ до чотирьохфазної ФМ з індексом $m_\phi = \frac{\pi}{2}$ при сталості смуги пропускання приймача еквівалентний зменшенню потужності передавача у два рази, а звуження смуги приймача при односмужовій роботі еквівалентно збільшенню потужності передавача у два рази, то приблизно можна вважати, що завадостійкість чотирьохфазного односмужового каналу ФМ буде такою, як і при однократній ФМ.

Спектр сигналу при ДФМ. Нехай передавання в обох каналах ведеться зі швидкостями, відповідними до кругових частот модуляції Ω_{m1} й Ω_{m2} . У загальному випадку амплітуди каналних сигналів через неідентичність параметрів каналів можуть мати різну величину:

$$u_{c1}(t) = \frac{U_{c1}}{2} [\sin(\omega_0 + k\Omega_{m1})t + \sin(\omega_0 - k\Omega_{m1})t];$$

$$u_{c2}(t) = \frac{U_{c2}}{2} \{ \cos[(\omega_0 + k\Omega_{m1})t + \varphi_c] + \cos[(\omega_0 - k\Omega_{m2})t + \varphi_c] \},$$

де φ_c – фазовий зсув між сигналами, що характеризує асинхронізм їхньої послідовності.

Ширина смуги системи визначається більшою з частот модуляції й не залежить від того, ведеться передавання по іншому каналу чи ні. При однаковій швидкості роботи $\Omega_{m1} = \Omega_{m2}$ й характер результуючого спектра залежить від кута φ_c . При синхронній роботі $\varphi_c = 0$ і бічні коливання обох спектрів складаються у квадратурі. Якщо ж послідовності в каналах зміщені на кут 90° , то результуючий сигнал

$$u_c(t) = u_{c1}(t) + u_{c2}(t) = \frac{U_{c1} - U_{c2}}{2} \sin(\omega_0 + \Omega_{m1})t + \frac{U_{c1} + U_{c2}}{2} \sin(\omega_0 - \Omega_{m1})t$$

стає несиметричним і при рівності амплітуд $U_{c1} = U_{c2}$ одна з бічних смуг може зникнути. Таким чином, спектр сигналу в загальному випадку стає симетричним. Крім того, перехід від АМ до ДФМ еквівалентний збільшенню потужності передавача у два рази, що підвищує завадостійкість зв'язку.

Спосіб амплітудно-базового детектування сигналів. Для усунення зворотної роботи Д.В. Агеевим була запропонована схема амплітудно-фазового детектора сигналів (АФД). Цей пристрій являє собою двотактний синхронний детектор, в якому вхідний сигнал одночасно подається в протифазі на аноди обох ламп і у фазі на їхні сітки. Опорна напруга створюється в сітковому контурі $L_k C_k$, постійна часу якого значно більше періоду модуляції фази сигналів. Завдяки цьому одна з ламп виявляється відкритою, а інша закритою. При зміні фази вхідного сигналу на π режим ламп змінюється на зворотний, що приводить до зміни полярності вихідної напруги.

Дослідження Ю.С. Лезіна показали, що в цій схемі також можлива зворотна робота, ймовірність якої

$$p_{op} = V \left(\sqrt{2h_c^2 \xi_d} \right), \quad (2.151)$$

де $\xi_d = \frac{\Delta f_1}{\Delta f_2}$ – коефіцієнт стійкості детектора; Δf_1 – смуга пропускання приймача до детектора; Δf_2 – смуга пропускання сіткового контуру детектора.

Завадостійкість каналів ФМ при флуктуаційних завадах. Приймання сигналів ФМ – когерентне, тому амплітуда $U_{ш}$ синфазної складової флуктуаційної завади розподілена за нормальним законом і ймовірності спотворення посилок

$$p(0/1) = \int_{-U_{c \text{ макс}}}^{\infty} w(U_{ш}) dU_{ш}; \quad p(1/0) = \int_{U_{c \text{ макс}}}^{\infty} w(U_{ш}) dU_{ш}$$

де $U_{c \text{ макс}}$ – амплітуда сигналу. Враховуючи парність підінтегральної функції, визначимо

$$p(0/1) = p(1/0) = V \left(\sqrt{2h_c^2} \right). \quad (2.152)$$

Вважаючи наявність й відсутність сигналу рівноймовірними, остаточно для повної ймовірності помилки одержимо

$$p_0 = V \left(\sqrt{2h_c^2} \right). \quad (2.153)$$

Отже, найбільшою завадостійкістю при флуктуаційних завадах має ФМ, що забезпечує вигреш за потужністю сигналу на 6 дБ у порівнянні з АМ і на 3 дБ у порівнянні зі ЧМ. Однак це досягається ціною технічного ускладнення приймального пристрою, що містить синхронний детектор.

Завадостійкість дискретних сигналів при зосереджених завадах. Векторна діаграма дії імпульсних завад в каналі ФМ наведена на рис. 2.50, а. З рисунка видно, що збій послілки трапиться лише у тому випадку, якщо синфазна складова завади $U_{з \text{ макс}} \cos \varphi_з > U_{c \text{ макс}}$, звідки абсолютне значення

фазового кута завади $|\varphi_з| > \frac{\pi}{2}$. Тоді ймовірність збою посилок

$$p(0/1) = p(1/0) = \frac{1}{\pi} \arccos \sqrt{h_c^2}, \quad (2.154)$$

а повна ймовірність помилки з врахуванням ймовірності появи завади p_{zi} при цьому значенні перевищення сигналу h_c^2 буде

$$p_0 = \frac{p_{zi}}{\pi} \arccos \sqrt{h_c^2}. \quad (2.155)$$

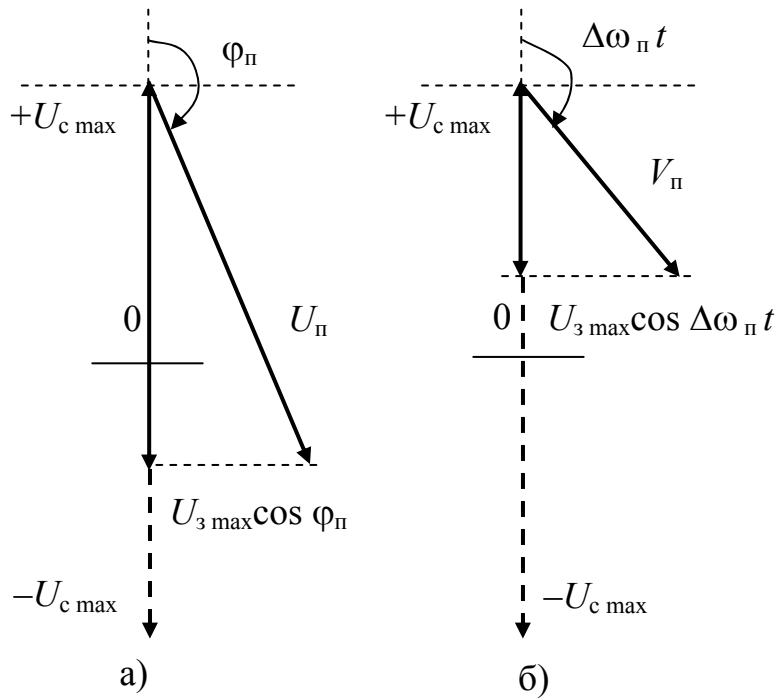


Рисунок 2.50 – Векторна діаграма прийому сигналів ФМ:
а) імпульсні завади; б) зосереджені завади

Якщо відомий закон розподілу амплітуди завади, тобто функція $w(h_c^2)$, то ймовірність помилки

$$p_0 = \frac{P_{zi}}{\pi} \int_0^1 \arccos \sqrt{h_c^2} w(h_c^2) dh_c^2. \quad (2.156)$$

Вираз (2.156) наведено на рис. 2.46 (крива 2), звідки виходить, що завадостійкість ФМ до імпульсних завад значно перевищує завадостійкість АМ і ФМ.

З векторної діаграми рис. 2.50, б випливає, що збій послілки відбудеться тоді, коли синфазна складова завади $U_{3 \text{ макс}} \cos \Delta\omega_3 t > U_{c \text{ макс}}$, звідки абсолютне значення фазового кута завади обумовлений її розладнанням $\Delta\omega_3$ відносно сигналу. Тоді ймовірність збою послілок

$$p(0/1) = p(1/0) = \frac{1}{\pi} \arccos \sqrt{h_c^2}. \quad (2.157)$$

З урахуванням ймовірності появи завади p_{33} при цьому значенні перевищення сигналу h_c^2 повна ймовірність помилки

$$p_0 = \frac{P_{33}}{\pi} \arccos \sqrt{h_c^2}. \quad (2.158)$$

Якщо відомий розподіл амплітуди завади, то ймовірність помилки

$$p_0 = \frac{P_{33}}{\pi} \int_0^1 \arccos \sqrt{h_c^2} w(h_c^2) dh_c^2. \quad (2.159)$$

Вираз (2.158) збігається з формулою (2.155), що свідчить про однакову завадостійкість каналів ФМ при імпульсних і зосереджених завадах. Тому крива 2 на рис. 2.47 також справедлива й для розглянутого випадку.

2.8. Узгодження параметрів каналів та кодів

Достатньо велика кількість відомих математичних моделей і, зокрема, більшість моделей першої групи ґрунтуються на теорії процесів відновлення, що характеризуються сукупністю моментами появи помилок $\{u_1, u_2, \dots, u_n\}$, інтервали Ψ між якими є взаємно незалежними однаково розподіленими випадковими величинами. Математичний апарат теорії відновлення дозволяє достатньо точно описати процес появи «згустків» (груп) і «розріджень» помилок, характерних для реальних потоків спотворень, а також врахувати достатньо велику ймовірність появи малих інтервалів, характерних для «згустків» помилок, і великих інтервалів, характерних для «незбурених» станів реального каналу, що так само оцінюються, як достатньо високоймовірнісні події. Це суперечить геометричному закону розподілу інтервалів між помилками, який часто використовується для опису реального потоку помилок і характеризується швидким убуттям ймовірностей інтервалів із зростанням їхньої довжини.

У разі використання біноміальної моделі розподіл інтервалів між помилками повинен підкорятися геометричному закону

$$P\{\Psi = u\} = (1 - p)^u p, \quad (2.160)$$

де p – ймовірність появи помилки, яка є параметром моделі. Проте експериментальні дослідження каналів свідчать про значно більшу ймовірність появи великих інтервалів, ніж це виходить з (2.160).

Явище групування помилок в реальних дискретних каналах може бути враховано при розгляданні потоку помилок як процесу відновлення. При цьому події процесу відновлення мають тим більшу схильність до групування, ніж більше скривленість густини розподілу довжин інтервалів Ψ між сусідніми помилками, тобто малим і великим значенням аргументу повинні відповідати порівняно великі значення ймовірностей, а проміжним значенням аргументу – порівняно малі. Відомі методи кількісної оцінки скривленості розподілів, ґрунтуючись на яких можна знайти розподіл, що дозволяє добре відобразити тенденцію помилок до групування. Зокрема, можна скористатися наступним достатньо простим методом.

Хай в розподілі $F(u) = P\{\Psi < u\}$ виділяється область проміжних значень інтервалів Ψ між сусідніми помилками, наприклад область $[0,5 - \delta; 0,5 + \delta]$. Тоді існують такі u_1 і u_2 , за яких

$$\left. \begin{aligned} F(u_1) &= 0,5 - \delta, \\ F(u_2) &= 0,5 + \delta \quad (u_2 > u_1). \end{aligned} \right\} \quad (2.161)$$

Відношення $u_2/u_1 = \theta$ можна визначити як параметр пакетоутворення. Якщо θ приймає великі значення, то проміжним значенням аргументу u відповідають малі ймовірності. Тому чим більше θ , тим сильніше виражена тенденція до групування.

Хай розглядається рівномірний на відтинку $[0, C]$ розподіл $F(u) = u/C$. Припустимо $\delta = 0,1$, тоді система матиме вигляд

$$u_1/C = 0,5 - 0,1, \quad u_2/C = 0,5 + 0,1,$$

звідки $\theta = 1,5$.

Для експоненціального розподілу $F(u) = 1 - e^{-\lambda u}$ і $\delta = 0,1$ система (2.161) має вигляд

$$\left. \begin{aligned} 1 - \exp(-\lambda u_1) &= 0,5 - 0,1, \\ 1 - \exp(-\lambda u_2) &= 0,5 + 0,1, \end{aligned} \right\}$$

розв'язуючи яку одержимо $\theta = u_2/u_1 = \ln 0,4 / \ln 0,6 \approx 1,8$.

Розподіл Парето з параметром α для $\delta = 0,1$ призводить до системи

$$\left. \begin{aligned} F(u) &= \begin{cases} 0 & u < 1, \\ 1 - u^{-\alpha} & u \geq 1, \end{cases} \\ 1 - u_1^{-\alpha} &= 0,5 - 0,1, \\ 1 - u_2^{-\alpha} &= 0,5 + 0,1, \end{aligned} \right\}$$

звідки $\theta = u_2/u_1 = (1,5)^{-\alpha}$. Очевидно, що з убутанням α величина θ швидко зростає. Так, при $\alpha = 0,25$ $\theta \approx 5$, а при $\alpha = 0,1$ $\theta \approx 60$.

Розподіл Вейбулла $F(u) = 1 - e^{-\lambda u^v}$, $u \geq 0$, для $\delta = 0,1$ призводить до системи

$$\left. \begin{aligned} 1 - \exp(-\lambda u_1^v) &= 0,5 - 0,1, \\ 1 - \exp(-\lambda u_2^v) &= 0,5 + 0,1, \end{aligned} \right\}$$

звідки $\theta = u_2/u_1 = (1,8)^{-v}$, тобто параметр v в розподілі Вейбулла впливає на параметр пакетоутворення так само, як α в розподілі Парето. Наприклад, при $v = 0,25$ $\theta \approx 60$, а при $v = 0,1$ $\theta \approx 330$.

Таким чином, можна зробити висновок, що розподіли Парето і Вейбулла дозволяють імітувати процес з групуванням помилок. Можна знайти і інші розподіли, які характеризуються великою скривленістю густини розподілу і тому можуть бути використані для опису реального потоку помилок.

Розробка універсальної моделі, що дозволяє достатньо просто і з хорошим наближенням до експерименту описати розподіл помилок в

дискретних каналах зв'язку будь-якого типу, є в практичному відношенні майже нездійсненим завданням, оскільки при досить великій кількості використовуваних типів каналів спроба відобразити специфіку (характер розподілу помилок) кожного каналу в межах однієї моделі призводить до різкого і невиправданого ускладнення останньої. В той же час зведення до мінімуму загального числа моделей, достатніх для опису всіх використовуваних типів каналів, є вже цілком реальним завданням, що представляє великий інтерес для інженерної практики. Для вирішення цього завдання необхідно зіставити результати статистичного дослідження всіх типів каналів з метою виявлення загальних закономірностей в характері розподілів помилок. При цьому як базову статистику, на основі якої можна здійснювати зіставлення результатів експериментального дослідження різних каналів, доцільно використовувати розподіл інтервалів між помилками, що містить найповнішу інформацію про характер помилок у цілому і дозволяє з достатньою для практичних цілей точністю обчислити найбільш важливі похідні характеристики передачі інформації в цих каналах.

Кумулятивні функції розподілу інтервалів між одиночними помилками в телефонних каналах кабельних, радіорелейних, тропосферних і телеграфних каналах короткохвильових (канал 5) і проводових ліній (канал 6) показані відповідно на рис. 2.51, *а, б, в, г*. Щоб полегшити зіставлення різних розподілів, всі рисунки наведені у подвійному логарифмічному масштабі, тобто по осі абсцис відкладений аргумент – десятковий логарифм інтервалу між сусідніми помилками $\lg u$, а по осі ординат – десятковий логарифм кумулятивної функції розподілу $\lg R(u) = \lg \{\Psi \geq u\}$. Криві побудовані за результатом дослідження некомутованих (виділених) каналів зв'язку різного типу. Основні характеристики каналів і загальні статистичні показники їхнього дослідження наведені в табл. 2.1.

У телефонних каналах кабельних ліній основна маса помилок (90–95%) з'являється частіше ніж через 10 символів, що пояснюється короткочасними перервами зв'язку, під час яких спостерігається різке зростання інтенсивності помилок, що настають через інтервали $\Psi \leq 10$. Тому початкова ділянка кривої, яка в першому наближенні може бути апроксимована прямою, має більшу крутизну, ніж наступна ділянка, яка в першому наближенні також може бути апроксимована прямою до значень $u_{\max} \leq W$.

Характер розподілу інтервалів між помилками в радіорелейних каналах (див. рис. 2.51 *б*) аналогічний характеру розподілу, показаному на рис. 2.51 *а*. Це свідчить про те, що природа спотворень в радіорелейних телефонних каналах має багато спільного з природою спотворень в кабельних телефонних каналах.

Таблиця 2.1 – Основні характеристики і загальні статистичні показники дослідження каналів

№ каналу	Тип каналу	Довжина каналу	Число перетримань за низькою частотою	Вид модуляції	Швидкість передавання даних, біт/с	Час досліджування каналу, хв	Число переданих символів $\times 10^5$	Число спотворених символів	Частість появи помилок p
1	Телефонний кабельний канал	5000	5	ФРМ	1200	3558	256176	78525	$3,07 \cdot 10^{-4}$
2	Телефонний радіорелейний канал	1000	1	ФРМ	1200	1747	125784	108592	$8,65 \cdot 10^{-4}$
3	Телефонний радіорелейний канал	1000	3	ЧМ	1200	838	60336	42416	$7,01 \cdot 10^{-4}$
4	Телефонний тропосферний канал	580	–	ЧМ	1200	1457	104064	66551	$6,34 \cdot 10^{-4}$
5	Телеграфний КХ радіоканал	1000	–	ЧМ	33	710	1405,635	1444	$1,03 \cdot 10^{-3}$
6	Телеграфний проводний канал	2500	5	ІПС	33	550	1088,635	2123	$1,9 \cdot 10^{-3}$

Кумулятивну функцію розподілу інтервалів між помилками в телефонних каналах кабельних і радіорелейних ліній можна апроксимувати в координатах $\{\lg R(u), \lg u\}$ двома відтинками прямих, що мають різний нахил: α_1 – на ділянці $[1, \psi_0]$ і α_2 – на ділянці $[\psi_0, W]$. Іншими словами, $R(u)$ для цих каналів можна представити у вигляді

$$R(u) = P\{\psi \geq u\} = \begin{cases} 1, & u < 1, \\ u^{-\alpha_1}, & 1 \leq u \leq \psi_0, \\ Au^{-\alpha_2}, & \psi_0 < u \leq W, \\ 0, & u > W, \end{cases} \quad (2.162)$$

де коефіцієнт A визначається з очевидного співвідношення $\psi_0^{-\alpha_1} = A\psi_0^{-\alpha_2}$, звідки

$$A = \psi_0^{-\alpha_1 + \alpha_2}. \quad (2.163)$$

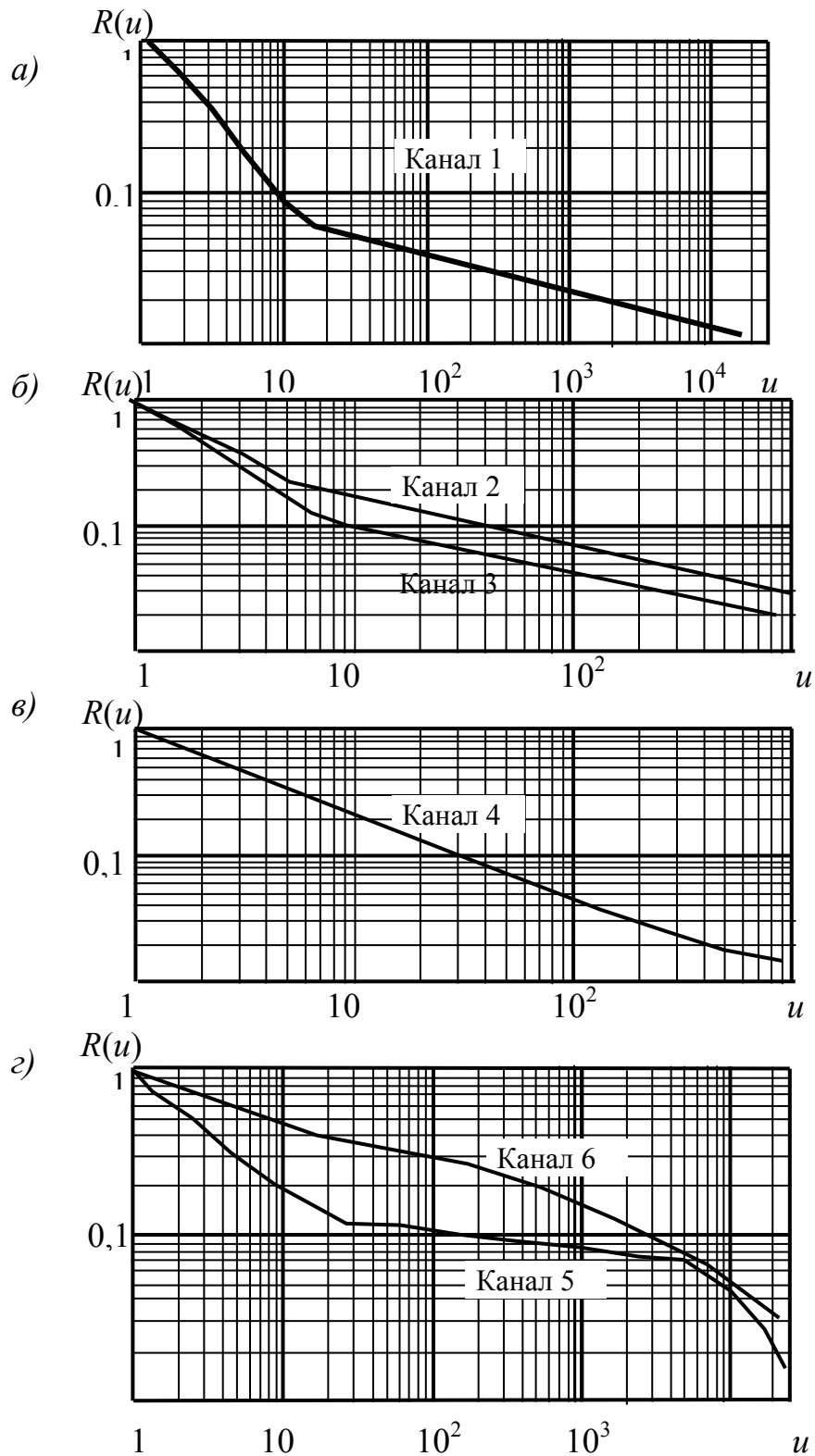


Рисунок 2.51 – Кумулятивна функція розподілу інтервалів між помилками в телефонних каналах:

- а) кабельної; б) радіорелейної;
- в) тропосферної лінії зв'язку і телеграфних каналах;
- г) короткохвильовому (канал 5) і провідному (канал 6)

Параметр W , що визначає верхню межу усікання вихідного розподілу, надалі виражається через середню ймовірність помилки p й інші параметри відповідної моделі і самостійного значення не має. Проте, оскільки параметр W формально є одним з первинних параметрів відповідної моделі, його можна враховувати разом з іншими, відображаючи факт можливої заміни W параметром p символом $W \rightarrow p$.

Розподіл інтервалів між помилками в тропосферних каналах (рис. 2.51 в) з достатньою для практики точністю апроксимується прямою, що має постійну крутизну α , і може бути представлений як усічений розподіл Парето

$$R(u) = \begin{cases} 1, & u < 1, \\ u^{-\alpha_1}, & 1 \leq u \leq W, \\ 0, & u > W. \end{cases} \quad (2.164)$$

Розподіли інтервалів між помилками в телеграфних каналах КХ і проводових ліній (рис. 2.51 з) мають приблизно однаковий характер і на ділянці зміни аргументу $\psi \leq 10$ можуть бути апроксимовані прямою, а далі – кривою, точки якої з достатньою точністю підкоряються розподілу Вейбулла. У цьому можна перекопатися, побудувавши ці ділянки кривих в координатах $\{\lg[\lg R(u)], \lg u\}$ по методу імовірнісних шкал. У цих координатах криві повинні перетворюватися в прямі лінії, що і відбувається практично на достатньо великому інтервалі зміни параметра u (рис. 2.52).

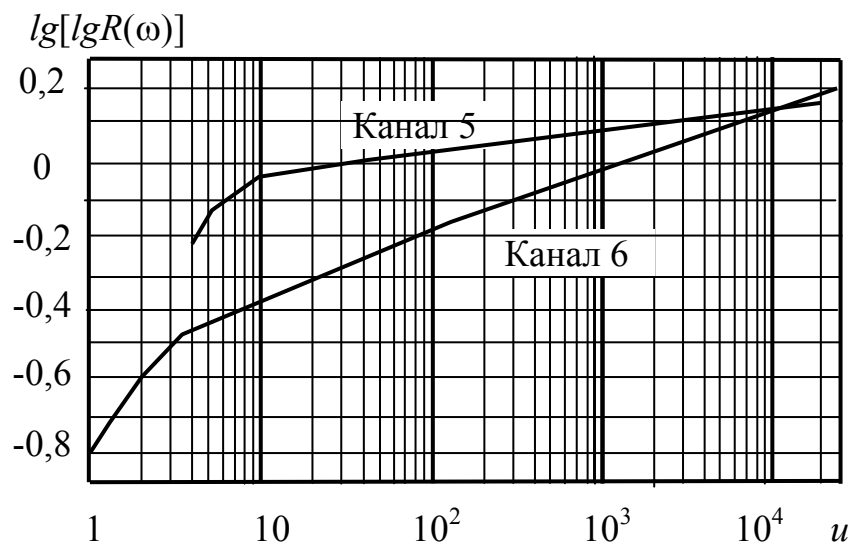


Рисунок 2.52 – Кумулятивні функції розподілу інтервалів між помилками в короткохвильовому (канал 5) і проводовому (канал 6) телефонних каналах, побудовані в координатах

Таким чином, для телеграфних КХ і проводових ліній можна записати

$$R(u) = \begin{cases} 1, & u < 1, \\ u^{-\alpha}, & 1 \leq u \leq \Psi_0, \\ A \exp \left[- \left(\frac{u}{a} \right)^b \right], & \Psi_0 < u \leq W, \\ 0, & u > W, \end{cases} \quad (2.165)$$

де A можна знайти із співвідношення

$$\Psi_0^{-\alpha} = A \exp \left[- \left(\frac{\Psi_0}{a} \right)^b \right]. \quad (2.166)$$

Модель потоку помилок з двома станами, запропонована Гільбертом, описує потік помилок в каналі простим однорідним ланцюжком Маркова з двома станами. В одному стані – «хорошому» – перевищення сигналу h_c^2 більше граничного значення $h_{\text{сп}}^2$ й ймовірність спотворення символів p_{01} значно менше середнього значення p_0 . В іншому стані каналу – «поганому» – у межах інтервалів (t_1, t_2) і (t_3, t_4) величина $h_c^2 < h_{\text{сп}}^2$, і ймовірність спотворень символів $p_{02} \gg p_0$. Моменти часу t_1 t_3 відповідають появі пакетів помилок довжиною $l_{\text{п}}$ символів, при цьому помилки усередині пакетів і самі пакети є некорельованими.

При завмираннях, за законом Релея, густина ймовірності

$$w(h_c^2) = \frac{2\sqrt{h_c^2}}{h_{c0}^2} e^{-\frac{h_c^2}{h_{c0}^2}}, \quad (2.167)$$

де h_{c0}^2 – середнє значення h_c^2 . У цьому випадку при некогерентному прийманні ортогональних сигналів ймовірності

$$p_{e1} = \frac{1}{2} e^{-\frac{h_c^2}{h_{c0}^2}}; \quad p_{e2} = \frac{1}{2 + h_{c0}^2}, \quad (2.168)$$

Тоді при $\alpha_0 = 0,99$ одержимо

$$h_c^2 \approx 3; \quad \varphi_1 = 1 - e^{-\frac{9}{h_{c0}^2}} \approx \frac{9}{h_{c0}^2}.$$

При $h_{c0}^2 > 100$, що часто виконується на практиці, ймовірності

$$p_{e1} \approx 10^{-2} p_e; \quad p_{e1} \approx 0,11 p_e h_{c0}^2. \quad (2.169)$$

Ймовірність

$$p(l_{\text{п}}) = \exp \left[- \frac{\pi(l_{\text{п}} + 0,5)^2}{4l_{\text{п}0}^2} \right] - \exp \left[- \frac{\pi(l_{\text{п}} - 0,5)^2}{4l_{\text{п}0}^2} \right], \quad (2.170)$$

де $l_{\text{п}0}$ – середня довжина пакета помилок у символах

$$p_{\text{п}} = 0,99 \frac{P_0}{p_{\text{е}2} I_{\text{п}0}} = \frac{9}{h_{\text{с}0}^2 I_{\text{п}0}}. \quad (2.171)$$

Для кабельних каналів можна прийняти $p_{\text{е}2} \approx 3 \cdot 10^{-5} \div 3 \cdot 10^{-6}$.

Розглянемо особливості окремих видів каналів, які характеризуються відповідними законами розподілу та їх параметрами.

Модель каналу з розподілом відстаней між помилками за законом Парето. Модель такого типу можна використовувати для опису каналів, розподілу інтервалів між помилками, заснованому на зрізаному розподілі Парето. До таких каналів, зокрема, можна віднести тропосферні телефонні канали.

Для розподілу інтервалів між помилками при відсутності обмежень на залежність між спотвореннями справедливо співвідношення

$$P(\geq 1, n) = p \sum_{u=1}^n R(u), \quad (2.172)$$

звідки отримаємо

$$P(\geq 1, n) = p \sum_{u=1}^n u^{-\alpha}. \quad (2.173)$$

При невеликих значеннях n для оцінки $P(\geq 1, n)$ необхідно користуватися лише формулою (2.172), тобто обов'язково враховувати дискретний характер суми. Для обчислень при великих значеннях n вираз (2.172) можна представити в більш зручному вигляді

$$P(\geq 1, n) \approx p \left[\sum_{u=1}^{u_0} u^{-\alpha} + \int_{u_0}^n u^{-\alpha} du \right] = p \left[\sum_{u=1}^{u_0} u^{-\alpha} + \frac{n^{1-\alpha} - u_0^{1-\alpha}}{1-\alpha} \right], \quad (2.174)$$

де $u_0 = 7 \dots 10$. Підсумовування в інтервалі $u = 1$ і до $u_0 = 7 \dots 10$ дозволяє отримати більш точну оцінку $P(\geq 1, n)$, в той час як заміна суми інтегралом в інтервалі від u_0 до n практично не впливає на кінцевий результат. Для наближеної оцінки $P(\geq 1, n)$ замість (2.174) можна користуватися формулою

$$P(\geq 1, n) \approx p \left[\int_0^1 du + \int_n^1 u^{-\alpha} du \right] = \frac{n^{1-\alpha} - \alpha}{1-\alpha} p. \quad (2.175)$$

Аналогічні вирази одержано в моделі Бергера-Мандельброта. Однак тут ймовірність $P(\geq m, n)$ визначена тільки для $m \leq 2$.

Співвідношення для $P(\geq m, n)$ отримані для довільних n і m . Тут ми скористаємось наближеними виразами для $P(\geq m+1, n)^2$, які були отримані для $m \leq 0,5 n$, що цілком прийнятно для більшості практичних додатків:

² Використання ймовірності $P(m+1, n)$ замість $P(\geq m, n)$ дозволяє спростити проміжні викладення і результуючі вирази, нічого не змінюючи по суті.

$$P(\geq m+1, n) \approx p(1-b_m) \left[\frac{(n-m)^{1-\alpha} - \alpha(2-\alpha)}{(1-\alpha)(2-\alpha)} \right], \quad (2.176)$$

де

$$b_m \approx \left(1 + \frac{n-m}{m^{1/\alpha}} \right)^{-\alpha} \quad \text{для } n \geq 15, m \leq 0,5n \quad (2.177)$$

Якщо $(n-m)$ достатньо завелике (наприклад, $n-m \geq 20$), то можна знехтувати в (2.176) членом $\alpha(2-\alpha)$. Тоді $P(\geq m+1, n)$ набуде вигляду

$$P(\geq m+1, n) \approx p(1-b_m) \frac{(n-m)^{1-\alpha}}{(1-\alpha)(2-\alpha)}. \quad (2.178)$$

Розглянемо у (2.176) і (2.178) $1-b_m \approx 1 - \left(1 + \frac{n-m}{m^{1/\alpha}} \right)^{-\alpha}$. Якщо величина $\frac{n-m}{m^{1/\alpha}}$ достатньо велика, а саме $\frac{n-m}{m^{1/\alpha}} > 0,1$, то $1-b_m$ треба обчислювати точно. Якщо ж $\frac{n-m}{m^{1/\alpha}} < 0,1$, то можна скористатися наближенням $\left[1 - \left(1 + \frac{n-m}{m^{1/\alpha}} \right)^{-\alpha} \right] \approx \alpha \frac{n-m}{m^{1/\alpha}}$. Тоді при $n \geq 15, m \leq 0,5n, \frac{n-m}{m^{1/\alpha}} < 0,1$ і відповідно до (2.176) можна визначати $P(\geq m+1, n)$ у вигляді

$$P(\geq m+1, n) \approx p \alpha \frac{n-m}{m^{1/\alpha}} \frac{(n-m)^{1/\alpha} - \alpha(2-\alpha)}{(1-\alpha)(2-\alpha)}, \quad (2.179)$$

а при $\frac{n-m}{m^{1/\alpha}} > 0,1$

$$P(\geq m+1, n) \approx p \left[1 - \left(1 + \frac{n-m}{m^{1/\alpha}} \right)^{-\alpha} \right] \frac{(n-m)^{1-\alpha} - \alpha(2-\alpha)}{(1-\alpha)(2-\alpha)}. \quad (2.180)$$

У тих випадках, коли обмеження $m \geq 0,5 n$ може виявитися неприйнятним, можна скористатися точними виразами для $P(\geq m+1, n)$.

Модель телефонних, кабельних та радіорелейних ліній зв'язку. Модель цього типу ґрунтується на розподілі, яке характеризує розподіл помилок у телефонних каналах, кабельних або радіорелейних лініях зв'язку

$$R(u) = \begin{cases} u^{-\alpha}, & 1 \leq u \leq \Psi_0, \\ \Psi_0^{-\alpha_1 + \alpha_2} u^{-\alpha_2}, & \Psi_0 < u \leq W, \alpha_1 > \alpha_2 \end{cases}, \quad (2.181)$$

звідки у відповідності з (2.172) для $n > \Psi_0$

$$P(\geq 1, n) = p \sum_{u=1}^n R(u) \approx \left[\sum_{u=1}^{\psi_0} u^{-\alpha_1} + \int_{\psi_0}^n \psi_0^{-\alpha_1 + \alpha_2} u^{-\alpha_2} du \right] =$$

$$= p \left[\sum_{u=1}^{\psi_0} u^{-\alpha_1} + \psi_0^{-\alpha_1 + \alpha_2} \frac{n^{1-\alpha_2} - \psi_0^{1-\alpha_2}}{1-\alpha_2} \right] = D p + E n^{1-\alpha_2} p, \quad (2.182)$$

де $D = \sum_{u=1}^{\psi_0} u^{-\alpha_1} - \frac{\psi_0^{1-\alpha_1}}{1-\alpha_1}$ та $E = \frac{\psi_0^{\alpha_2}}{\psi_0^{\alpha_1} (1-\alpha_2)}$.

За аналогією з (2.175) замість (2.182) для оцінки $P(\geq 1, n)$ можна користуватися наближеною формулою

$$P(\geq 1, n) = p \int_0^{n > \psi_0} R(u) du = p \left[\int_0^1 du + \int_1^{\psi_0} u^{-\alpha_1} du + \psi_0^{-\alpha_1 + \alpha_2} \int_{\psi_0}^n u^{-\alpha_2} du \right] =$$

$$= p \left[1 + \frac{\psi_0^{1-\alpha_1} - 1}{1-\alpha_1} + \psi_0^{-\alpha_1 + \alpha_2} \frac{n^{1-\alpha_2} - \psi_0^{1-\alpha_2}}{1-\alpha_2} \right] = \left[\frac{\psi_0^{1-\alpha_1} - 1}{1-\alpha_1} - \frac{\psi_0^{1-\alpha_2}}{1-\alpha_2} \right] p +$$

$$+ \frac{\psi_0^{\alpha_1}}{\psi_0^{\alpha_1} (1-\alpha_2)} n^{1-\alpha_2} p = D_1 p + E_1 n^{1-\alpha_2} p. \quad (2.183)$$

Порівнюючи (2.183) і (2.182) зауважимо, що вони відрізняються лише значеннями коефіцієнтів D і D_1 .

При малих $n (n \leq \psi_0)$ можна скористатися наступним наближеним виразом для оцінки $P(\geq 1, n)$:

$$P(\geq 1, n) = p \int_0^{n \leq \psi_0} R(u) du = \frac{n^{1-\alpha_1} - \alpha_1}{1-\alpha_1} p, \quad (2.184)$$

що збігається з (2.175).

Первинними параметрами моделі розподілу помилок у телефонних, кабельних та радіорелейних ліній зв'язку є ψ_0 , α_1 , α_2 і $W \rightarrow p$. При необхідності параметр W може бути знайдений через математичне сподівання $M[u]$. Як видно з (2.182)...(2.184), параметр W зазвичай не використовується для отримання вторинних параметрів моделі, і тому потреба в ньому може виникнути лише при порівнянні середніх характеристик моделі (математичного сподівання інтервалу між помилками, дисперсії) з відповідними експериментальними характеристиками. Для оцінки ступеня наближення формул (2.183) і (2.182) до експериментальних значень $P(\geq 1, n)$ скористаємося реальною статистикою для телефонного каналу кабельної лінії. Із розглядання рис. 2.51, а маємо $\alpha_1 = 1,16$; $\alpha_2 = 0,236$; $\psi_0 = 10$, а з табл. 2.1 (канал 1) – $p = 3,07 \cdot 10^{-4}$. Із (2.182) і (2.183) отримаємо: $D = 1,69$; $D_1 = 2,04$; $E = E_1 = 0,157$. За формулами (2.182) і (2.183) визначимо значення $P(\geq 1, n)$ при $n = 15$; 31; 63; 127; 255 і зіставимо їх з відповідними експериментальними значеннями

$P(\geq 1, n)$. Результати розрахунків зведемо в табл. 2.2. З цієї таблиці можна зробити наступні висновки. Розрахунки за формулою (2.182) в цілому дають більше наближення до експериментальних значень, ніж розрахунки за формулою (2.183), хоча ступінь збігу розрахункових і експериментальних значень $P(\geq 1, n)$ достатня для інженерної практики в обох випадках. Найкращій збіг при розрахунках за цими формулами має місце при малих і середніх значеннях n . Розрахункові значення дають більш песимістичну оцінку каналу, ніж це впливає з експерименту, який дозволяє створити певний «запас» в прогнозованих характеристиках неспотвореного передавання блоків інформації.

Таблиця 2.2 – Результати розрахунків $P(\geq 1, n)$

Довжина блоку	Експериментальні значення	Розрахункові значення	
		формула (2.182)	формула (2.183)
15	$1 \cdot 10^{-3}$	$0,9 \cdot 10^{-3}$	$1 \cdot 10^{-3}$
31	$1,18 \cdot 10^{-3}$	$1,18 \cdot 10^{-3}$	$1,28 \cdot 10^{-3}$
63	$1,43 \cdot 10^{-3}$	$1,66 \cdot 10^{-3}$	$1,77 \cdot 10^{-3}$
127	$1,86 \cdot 10^{-3}$	$2,44 \cdot 10^{-3}$	$2,54 \cdot 10^{-3}$
255	$1,26 \cdot 10^{-3}$	$3,84 \cdot 10^{-3}$	$3,94 \cdot 10^{-3}$

Розбіжність експериментальних і розрахункових оцінок $P(\geq 1, n)$, що збільшується із зростанням n , обумовлюється тим, що в експериментальному розподілі $R(u)$, отриманих на реальних каналах (табл. 2.1), враховувалися всі тривалості перерв зв'язку. Якщо з розгляду вилучити перерви зв'язку з тривалістю, більшої деякої встановленої межі, перевищення якої можна розглядати як відмова каналу зв'язку, то розбіжність між експериментальними і розрахунковими оцінками $P(\geq 1, n)$ можна звести до мінімуму. Як приклад було проведено експериментальне дослідження реальних каналів зв'язку, при якому з розглядання вилучалися інтервали більше 1 для телефонних каналів при швидкості передачі 1200 біт/с і інтервали більше 15 с для телеграфних каналів при швидкості роботи 75 Бод. Були отримані експериментальні оцінки $P(\geq 1, n)$ і побудовані графіки кумулятивних функцій розподілу $R(u)$, що наведені на рис. 2.53 та 2.54.

За графіками $R(u)$ отримані параметри моделі телефонних, кабельних та радіорелейних ліній зв'язку (при цьому для телеграфних провідних і радіоканалів, описуваних моделлю телеграфних каналів та КХ-каналів, використовувалася апроксимація на ділянці $[\psi_0, W]$ розподілом Парето. Це дозволяло звести цю модель до моделі телефонних, кабельних та радіорелейних ліній зв'язку. На їх основі за формулою (2.183) визначені розрахункові значення $P(\geq 1, n)$ для $n = 80; 120; 200; 300; 500$. Зіставлення експериментальних і розрахункових оцінок $P(\geq 1, n)$, свідчить про хороший збіг, що є достатнім для інженерних додатків.

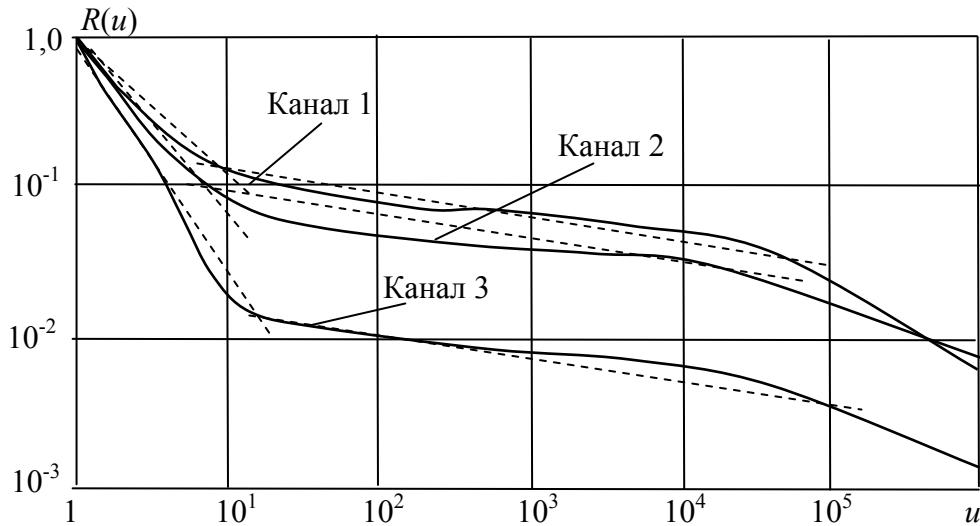


Рисунок 2.53 – Кумулятивна функція розподілу інтервалів між помилками для телефонних кабельних каналів зв'язку

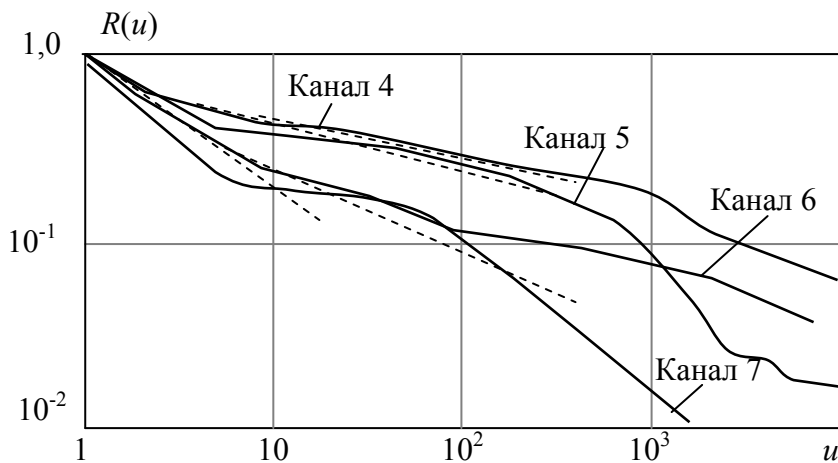


Рисунок 2.54 – Кумулятивна функція розподілу інтервалів між помилками для радіо- і провідних телеграфних каналів зв'язку

При обчисленні $P(\geq t, n)$ досить знати вигляд функції розподілу безпомилкових інтервалів $R(u)$ тільки на певній ділянці, обмеженій зверху деяким значенням u_0 , що обумовленим практичним використанням для передачі інформації довжинами блоків $n \geq 500$. У випадку моделі телеграфних, кабельних та радіорелейних ліній зв'язку функція $R(u)$ описується досить складним розподілом зі зломом (2.181), яке для зручності подальшого розгляду доцільно апроксимувати гамма-розподілом (Γ -розподілом). Параметри останнього необхідно підбирати так, щоб узгодженість з вихідною функцією $R(u)$ була особливо хорошою на ділянці $[1 - u_0]$, яка нас цікавить.

$$\rho = \frac{\hat{M}_a[u]}{\hat{D}_a[u]} = \frac{\hat{M}_b[u]}{\hat{D}_b[u]} \quad (2.185)$$

i

$$\beta = \rho \hat{M}_a[u] = \frac{\hat{M}_a^2[u]}{\hat{D}_a[u]} = \frac{\hat{M}_b^2[u]}{\hat{D}_b[u]}. \quad (2.186)$$

Г-розподіл з параметрами ρ і β , отриманими з (2.185) і (2.186), використовуються для апроксимації вихідної функції $R(u)$ на інтервалі $[1, u_b]$.

З урахуванням прийнятої апроксимації вихідного розподілу на ділянці $[1, u_b]$ для довільних значень m і n отримано співвідношення

$$P(\geq m, n) = p \frac{[\rho(n-m)]^{(m-1)\beta}}{\Gamma[(m-1)\beta+1]} \left\{ (2k-1) + k \frac{(n-m)}{(m-1)\beta+1} - \right. \\ \left. - k^2 \frac{(n-m)[(n-m)\rho]^\beta \Gamma[(m-1)\beta+1]}{\Gamma(m\beta+2)} \right\}, \quad (2.187)$$

де

$$k = \frac{3 + \exp[-\rho(n-m)]}{4}. \quad (2.188)$$

При $m = 1$ з (2.187) маємо

$$P(\geq 1, n) = p \left[(2k-1) + k(n-1) - k^2 \frac{(n-1)[\rho(n-1)]^\beta}{\Gamma(2+\beta)} \right], \quad (2.189)$$

при $m = 1$ і $n = 1$ відповідно з виразом (2.188) $k = 1$ і $P(\geq 1, 1) = p$, чого і слід було очікувати.

Порівнюючи (2.189) з (2.182), (2.183) і (2.184), зазначимо, що вираз (2.189) є більш універсальним, оскільки його можна використовувати при малих і при великих значеннях n . Крім того, для оцінки $P(\geq 1, n)$ з (2.189) потрібно знання лише трьох параметрів моделі – p , ρ і β – замість чотирьох параметрів – p , α_1 , α_2 , ψ_0 , необхідних при оцінці $P(\geq 1, n)$ з (2.182) і (2.183), проте, з іншого боку, визначення параметрів α_1 , α_2 та ψ_0 не пов'язане з будь якими обчислювальними процедурами та може бути здійснено безпосередньо за графіком експериментальної функції $R(u)$. Тому для обчислення $P(\geq 1, n)$ в залежності від ситуації можна користуватися як виразами (2.182), (2.183), (2.184), так і виразом (2.189). Однак при оцінці $P(\geq m, n)$ можна користуватися тільки співвідношенням (2.187), який потребує попереднього визначення параметрів ρ і β .

Модель телеграфних каналів та КХ-каналів. Модель такого типу характеризує розподіл помилок у телеграфних каналах провідних і КХ мереж зв'язку (див. рис. 2.51, з). Ймовірності $P(\geq 1, n)$ і $P(\geq m, n)$ при використанні цієї моделі можна оцінити за допомогою виразів, отриманих

для моделі телеграфних, кабельних та радіорелейних ліній зв'язку, оскільки і в цьому випадку початкова ділянка розподілу інтервалів між помилками також з достатньою для практики точністю може бути апроксимована за допомогою Γ -розподілу.

Як приклад розглянемо апроксимацію початкової ділянки експериментального розподілу інтервалів між помилками $R(u)$, наведеного на рис. 2.51 (канал 5). Інтервал апроксимації оберемо $[1, 100]$. Для отримання значень $\hat{M}_B[u]$ і $\hat{D}_B[u]$ попередньо апроксимуємо криву $R(u)$ двома відрізками прямих: прямої з нахилом $\alpha_1 = 0,845$ на інтервалі $[1, 10]$ і прямої з нахилом $\alpha_2 = 0,187$ на інтервалі $[10, 100]$. Відповідно до (2.185)

$$\begin{aligned}\hat{M}_B[u] &= -\int_0^{u_B} x \frac{dR(x)}{dx} dx = \alpha_1 \int_1^{\psi_0} x x^{-(\alpha_1+1)} dx + \alpha_2 \psi_0^{-\alpha_1+\alpha_2} \int_{\psi_0}^{u_B} x x^{-(\alpha_2+1)} dx = \\ &= \frac{\alpha_1}{1-\alpha_1} (\psi_0^{1-\alpha_1} - 1) + \frac{\alpha_2 \psi_0^{-\alpha_1+\alpha_2}}{1-\alpha_2} (u_B^{1-\alpha_2} - \psi_0^{1-\alpha_2}),\end{aligned}\quad (2.190)$$

і для заданих значень $\psi_0 = 10$, $\alpha_1 = 0,845$, $\alpha_2 = 0,187$ отримаємо $\hat{M}_B[u^2] \approx 42$.

Визначивши аналогічно (2.190) з урахуванням $\hat{D}_B[u] = \hat{D}_a[u] = \hat{M}_B[u^2] - \hat{M}_B^2[u] = \hat{M}_a[u^2] - \hat{M}_B^2[u]$ маємо

$$\begin{aligned}\hat{M}_B[u] &= -\int_0^{u_B} x^2 \frac{dR(x)}{dx} dx = \alpha_1 \int_1^{\psi_0} x^2 x^{-(\alpha_1+1)} dx + \alpha_2 \psi_0^{-\alpha_1+\alpha_2} \int_{\psi_0}^{u_B} x^2 x^{-(\alpha_2+1)} dx = \\ &= \frac{\alpha_1}{2-\alpha_1} (\psi_0^{2-\alpha_1} - 1) + \frac{\alpha_2 \psi_0^{-\alpha_1+\alpha_2}}{2-\alpha_2} (u_B^{2-\alpha_2} - \psi_0^{2-\alpha_2}),\end{aligned}\quad (2.191)$$

для цих самих значень α_1 , α_2 , ψ_0 отримаємо $\hat{M}_B[u^2] \approx 101$, звідки

$$\hat{D}_B[u] = \hat{M}_B[u^2] - \hat{M}_B^2[u] \approx 83. \quad \text{Нарешті, з } \rho = \frac{\hat{M}_a[u]}{\hat{D}_a[u]} = \frac{\hat{M}_B[u]}{\hat{D}_B[u]} \quad \text{і}$$

$$\beta = \rho \hat{M}_a[u] = \frac{\hat{M}_a[u]}{\hat{D}_a[u]} = \frac{\hat{M}_B[u]}{\hat{D}_B[u]} \quad \text{знайдемо } \rho = \frac{\hat{M}_B[u]}{\hat{D}_B[u]} \approx 0,05 \quad \text{і } \beta = \rho \hat{M}_B[u] \approx 0,2$$

Для оцінки відповідності моделі телеграфних каналів та КХ-каналів експериментальним результатам при використанні прийнятої в моделі телеграфних, кабельних та радіорелейних ліній зв'язку апроксимації початкової ділянки розподілу інтервалів між помилками в телеграфних каналах (рис. 2.51, з) за допомогою Γ -розподілу обчислимо значення $P(\geq t, n)$ і $P(\geq 1, n)$ та порівняємо їх з експериментальними. З цією метою як приклад для каналу 5 із параметрами $p = 1,03 \cdot 10^{-3}$, $\rho = 0,05$ і $-\beta = 0,2$ за

формулами (2.187) і (2.189) обчислимо для двох значень $n_1 = 5$ і $n_2 = 20$ – ймовірності $P(\geq m, n)$ і $P(\geq 1, n)$ і зіставимо їх з експериментальними. Результати розрахунку наведені в табл. 2.3.

З таблиці можна зробити висновок, що отримані при розгляді моделі телеграфних, кабельних та радіорелейних ліній зв'язку формули для $P(\geq m, n)$ і $P(\geq 1, n)$ дають досить добрий збіг з експериментом і можуть бути використані для розрахунку ймовірнісних характеристик передачі інформації в каналах, розподіл помилок в яких описується моделлю для телеграфних каналів та КХ-каналів.

Таблиця 2.3 – Результати розрахунку ймовірностей

Умови оцінки	$P(\geq 1)$ при		$\frac{P(\geq m, n)}{P(\geq 1, n)}$ при $n = 15$ і			$\frac{P(\geq m, n)}{P(\geq 1, n)}$ при $n = 20$ і	
	$n = 5$	$n = 20$	$m = 2$	$m = 3$	$m = 4$	$m = 3$	$m = 11$
Розрахунок	$2,3 \cdot 10^{-3}$	$4,6 \cdot 10^{-3}$	0,63	0,36	0,11	0,78	0,045
Експеримент	$2,3 \cdot 10^{-3}$	$4,6 \cdot 10^{-3}$	0,64	0,37	0,14	0,60	0,064

Прикладне використання моделей. Для оцінки параметрів реальних систем передачі та захисту інформації від помилок при обраних алгоритмах їх функціонування і використовуваних завадостійких кодах зазвичай буває достатньо визначити ймовірності спотворення кодових комбінацій $P(\geq 1, n)$ і на їх основі оцінити ефективну швидкість передачі повідомлень ρ_e конкретної системи при роботі на каналах різного типу і якості, а для оцінки виявляючої (виправляючої) здатності використовуваного коригуючого коду – знайти ймовірності $P(\geq m, n)$ і оцінити ймовірності не виявлення помилок в кодових комбінаціях $P_{н.п}$. При зіставленні ефективності різних систем можна користуватися різними комбінованими параметрами оцінки і, зокрема, відносною вірністю ξ_0 , які також залежать від зазначених вище ймовірностей $P(\geq 1, n)$, $P(\geq m, n)$, $P_{н.п}$. При цьому, як правило, шукані ймовірності виражаються через сукупність інших ймовірностей з урахуванням того, що сума ймовірностей виявлення помилки P_0 , правильної (неспотвореної) передачі $P_{п.п}$ і появи невиявленої помилки $P_{н.п}$ дорівнює 1, а сума $P_{п.п} + P_{н.п} = P_{п.к}$ визначає ймовірність удаваного правильного прийому кодової комбінації.

Для відповідного типу використовуваного каналу, заданого кумулятивної функцією розподілу інтервалів між помилками $R(u)$, ймовірності $P(\geq 1, n)$, $P(\geq m, n)$ можуть бути обчислені з співвідношень, отриманих для усіх моделей. При порівнянні систем в широкому діапазоні якості каналів оцінка $P(\geq 1, n)$ на основі співвідношень (2.176)...(2.180) для моделі каналу з розподілом відстаней між помилками за законом Парето та (2.187) для моделей телефонних, кабельних та радіорелейних ліній зв'язку і телеграфних каналів та КХ-каналів пов'язана з досить великим

обсягом обчислень, хоч і забезпечує досить високу точність результатів. При цьому можна скористатися наближеними емпіричними співвідношеннями:

$$P(\geq 1, n) = n^{1-\sigma} p, \quad (2.192)$$

$$P(\geq m, n) = \left(\frac{n}{m}\right)^{1-\sigma} p, \quad m \leq 0,3n, \quad (2.193)$$

$$P_{\text{н.п}} \approx 2^{-r} P(\geq m = d, n) = 2^{-r} \left(\frac{n}{m}\right)^{1-\sigma} p, \quad (2.194)$$

де σ – деякий параметр групування помилок; d – кодова відстань у використовуваному груповому коді; r – число перевірочних символів у кодовій комбінації.

Для встановлення взаємозв'язку параметра σ з параметрами моделей каналу з розподілом відстаней між помилками за законом Парето, моделі телефонних, кабельних та радіорелейних ліній зв'язку (модель телеграфних каналів та КХ-каналів зводиться до моделі телефонних, кабельних та радіорелейних ліній зв'язку і реальних розподілів $R(u)$ можна скористатися зіставленням (2.192) з (2.175) і (2.183), звідки для моделі каналу з розподілом відстаней між помилками за законом Парето отримаємо

$$\sigma = 1 - \frac{\lg(n^{1-\alpha} - \alpha) - \lg(1 - \alpha)}{\lg n}, \quad (2.195)$$

а для моделі телефонних, кабельних та радіорелейних ліній зв'язку

$$\sigma = 1 - \frac{1}{\lg n} \left\{ \lg \left[\frac{\Psi_0^{1-\alpha_1} - \alpha_1}{1 - \alpha_1} + \Psi_0^{1-\alpha_1} \frac{\left(\frac{n}{\Psi_0}\right)^{1-\alpha_2} - 1}{1 - \alpha_2} \right] \right\}. \quad (2.196)$$

Для визначення точності обчислень параметра σ за формулами (2.195) і (2.196) через параметри моделей каналу з розподілом відстаней між помилками за законом Парето і телефонних, кабельних та радіорелейних ліній зв'язку порівняємо розрахункові значення σ_p зі значеннями σ_e , отриманим на основі даних статистичного дослідження каналів зв'язку різного типу з урахуванням співвідношення

$$\sigma_e = \frac{\lg n_i - \lg M(\geq 1, n)}{\lg n}, \quad (2.197)$$

де n_i – загальне число спотворених символів в каналі, яке залежить від типу і якості каналу і обсягу вибірки; $M(\geq 1, n)$ – загальна кількість уражених блоків довжини n .

Дані статистичного дослідження отримані як на реальних каналах зв'язку, так і з використанням потоку помилок, що генеруються програмною моделлю розподілів для:

- каналу з розподілом відстаней між помилками за законом Парето (табл. 2.4);
- моделі телефонних, кабельних та радіорелейних ліній зв'язку (табл. 2.5);
- моделі телеграфних каналів та КХ-каналів (табл. 2.6).

Таблиця 2.4 – Результати статистичного дослідження каналу з розподілом відстаней між помилками за законом Парето

№ каналу	p	α	W
1	$1,3 \cdot 10^{-3}$	0,2	$3 \cdot 10^4$
2	$5 \cdot 10^4$	0,2	10^4
3	$1,4 \cdot 10^{-3}$	0,333	10^4
4	$2,3 \cdot 10^{-3}$	0,333	$5 \cdot 10^3$
5	$3,1 \cdot 10^{-4}$	0,333	10^5
6	$6 \cdot 10^{-6}$	0,333	10^7
7	$1,1 \cdot 10^{-2}$	0,5	$2 \cdot 10^3$
8	$5,1 \cdot 10^{-3}$	0,5	10^4
9	$1,6 \cdot 10^{-3}$	0,5	10^5
10	$6,5 \cdot 10^{-4}$	0,5	$6 \cdot 10^5$
11	$4,8 \cdot 10^{-5}$	0,5	10^6
12	$6,1 \cdot 10^{-5}$	0,5	10^7
13	$1 \cdot 10^{-2}$	0,6	10^4
14	$3,6 \cdot 10^{-2}$	0,8	10^4

Таблиця 2.5 – Результати статистичного дослідження моделі телефонних, кабельних та радіорелейних ліній зв'язку

№ каналу	p	α_1	α_2	ψ_0	W
15	$1,1 \cdot 10^{-3}$	0,5	0,2	5	$4 \cdot 10^3$
16	$7,7 \cdot 10^{-4}$	0,75	0,2	6	$2 \cdot 10^4$
17	$1,3 \cdot 10^{-3}$	0,75	0,2	6	10^4
18	$2,2 \cdot 10^{-3}$	0,6	0,3	10	10^4
19	$2 \cdot 10^{-3}$	0,6	0,3	8	10^4
20	$5,8 \cdot 10^{-3}$	0,5	0,333	8	$2 \cdot 10^3$
21	$1,86 \cdot 10^{-2}$	0,8	0,333	10	10^3
22	$1 \cdot 10^{-3}$	0,7	0,4	6	10^5
23	$4 \cdot 10^{-3}$	0,7	0,4	6	10^4
24	$1 \cdot 10^{-3}$	0,6	0,4	10	10^5
25	$1,5 \cdot 10^{-2}$	0,6	0,4	10	10^3
26	$3 \cdot 10^{-4}$	0,75	0,4	6	10^6
27	$2,7 \cdot 10^{-4}$	0,9	0,333	20	10^6
28	$2,6 \cdot 10^{-4}$	0,875	0,167	100	10^6
29	$2,8 \cdot 10^{-4}$	0,933	0,2	80	10^6
30	$1,38 \cdot 10^{-4}$	0,8	0,333	5	10^3

31	$2,6 \cdot 10^{-4}$	1,167	0,25	10	$8,4 \cdot 10^5$
32	$2,9 \cdot 10^{-4}$	1,167	0,25	20	$1,5 \cdot 10^6$
33	$5,5 \cdot 10^{-3}$	1,167	0,25	50	10^5
34	$1,8 \cdot 10^{-4}$	0,933	0,25	30	$1,5 \cdot 10^6$
35	$0,85 \cdot 10^{-3}$	0,75	0,25	10	$4 \cdot 10^4$
36	$1,4 \cdot 10^{-4}$	0,6	0,125	6	$5 \cdot 10^4$
37	$1,23 \cdot 10^{-2}$	1,167	0,25	20	10^4
38	$2,2 \cdot 10^{-3}$	1,167	0,25	20	10^4

Таблиця 2.6 – Результати статистичного дослідження моделі телеграфних каналів та КХ-каналів

№ каналу	p	α	ψ_0	a	b
39	$1,38 \cdot 10^{-3}$	0,5	4	235	0,25
40	$1,05 \cdot 10^{-2}$	0,6	6	42	0,37
41	$7,95 \cdot 10^{-3}$	0,5	8	42	0,37

Результати порівняння свідчать про досить добрий збіг експериментальних і розрахункових оцінок параметра σ . Це є підставою використовувати співвідношення (2.192)...(2.194) для наближених оцінок ймовірностей $P(\geq 1, n)$, $P(\geq t, n)$ за заданими кумулятивними функціями розподілів $R(u)$ з обчисленням σ з (2.195) і (2.196). Для спрощення оцінок σ при інженерних розрахунках можна скористатися графіками залежностей σ від α і n для моделі каналу з розподілом відстаней між помилками за законом Парето і від ψ_0 , α_1 , α_2 і n для моделі телеграфних, кабельних та радіорелейних ліній зв'язку, що відповідно наведено на рис. 2.55 і 2.56.

При більш тонкому дослідженні характеристик систем передачі даних виникає необхідність в оцінці розподілів довжин серій підряд спотворених кодових комбінацій довжини n . Отримання таких розподілів аналітичним шляхом при знятті припущення про незалежність спотворень суміжних кодових комбінацій пов'язане з великими труднощами і практично може бути здійснено тільки на програмній моделі каналів, в якій характер спотворень задається усіма моделями, які були розглянуті. Для отримання параметрів вказаних розподілів в широкому діапазоні вимірювання якості каналів, які характеризуються параметрами p і α для моделі каналу з розподілом відстаней між помилками за законом Парето, параметрами p , α_1 , α_2 , ψ_0 для моделей телефонних, кабельних та радіорелейних ліній зв'язку і параметрами p , α , ψ_0 , a , b для моделі телеграфних каналів та КХ-каналів, в умовах обмеженого обсягу експериментальних статистичних даних може бути використаний метод генерації статистики на програмній моделі каналу. У табл. 2.4, 2.5 і 2.6 наведені параметри каналів, для яких на програмній моделі отримано

розподіл довжин серій υ посліпль спотворених $R(V = \upsilon)$ кодових комбінацій довжини $n = 50; 80; 100; 120; 200; 300; 500; 1000$ (канали 1...14 для моделі каналу з розподілом відстаней між помилками за законом Парето, канали 15...38 для моделі телефонних, кабельних та радіорелейних ліній зв'язку і канали 39...41 для моделі телеграфних каналів та КХ-каналів).

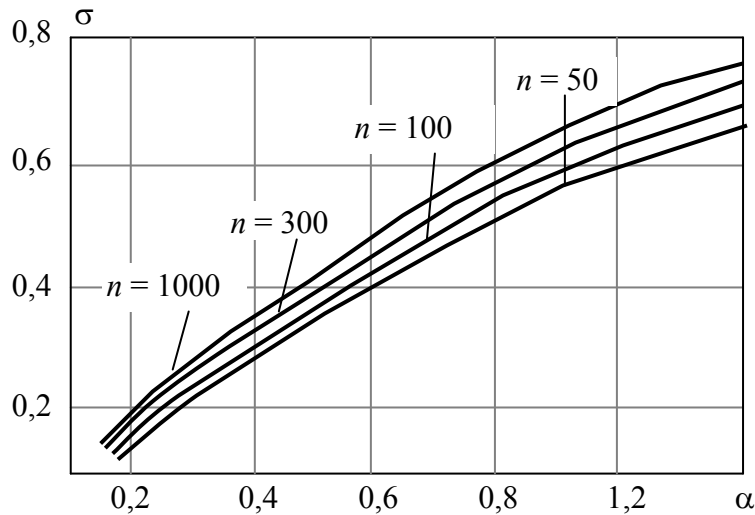


Рисунок 2.55 – Графік залежності σ від α для моделі каналу з розподілом відстаней між помилками за законом Парето

Дослідження характеру розподілів $R(V = \upsilon)$, отриманих на основі статистичного моделювання каналів, показано, що для каналів, розподіл спотворень в яких описується моделлю каналу з розподілом відстаней між помилками по закону Парето, $R(V = \upsilon)$ практично не залежить від параметра зрізання W , оскільки $W \geq n$, а залежність $R(V = \upsilon)$ від довжини кодової комбінації n настільки незначна, що при інженерних розрахунках нею можна знехтувати. При цьому характер розподілу $R(V = \upsilon)$ для моделі каналу з розподілом відстаней між помилками по закону Парето (канали 1...14) може бути описаний емпіричним виразом

$$R(V = \upsilon) = b^{-\upsilon} (b - 1), \quad (2.198)$$

звідки

$$R(V \leq \upsilon) = \sum_{\upsilon=1}^{\upsilon} R(V = \upsilon) = 1 - b^{-\upsilon}, \quad (2.199)$$

де

$$b = \frac{0,6}{\alpha - 0,035} + 0,5, \quad \alpha > 0,05 \quad (2.200)$$

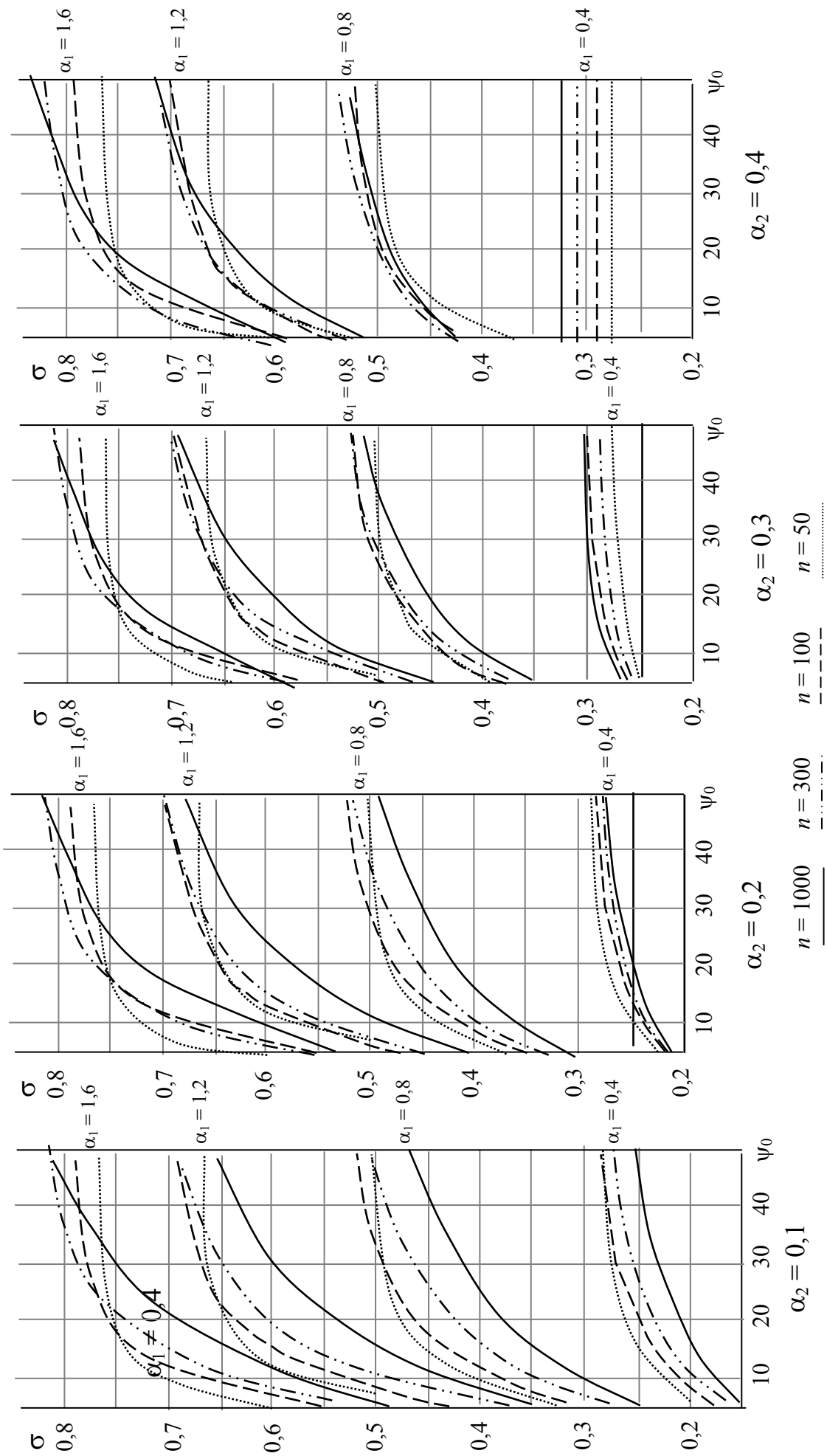


Рисунок 2.56 – Графік залежності σ від ψ_0 і α_1, α_2 для моделі телеграфних, кабельних та радіорелейних ліній зв'язку

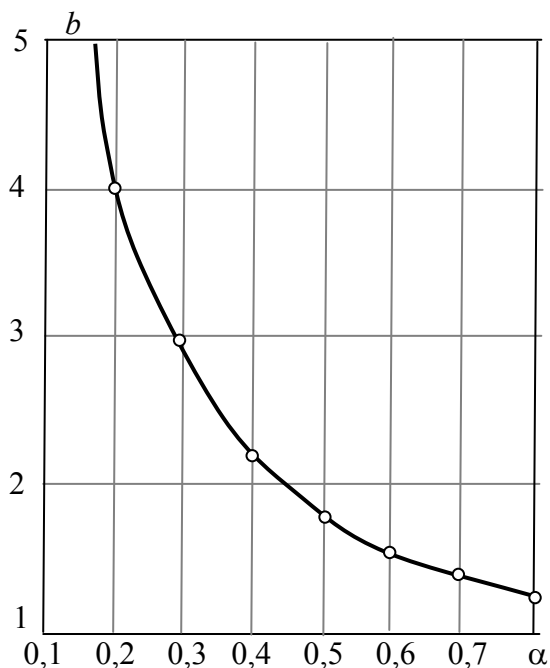


Рисунок 2.57 – Графік залежності b від α

Залежність b від α наведено на рис. 2.57.

Для каналів, розподіл спотворень в яких описується моделлю телефонних, кабельних та радіорелейних ліній зв'язку, розподіл R ($V = v$) залежить від параметрів α_1 , α_2 , ψ_0 , n і може бути також апроксимований співвідношеннями (2.198)...(2.200), в яких наведений параметр α може бути отриманий з виразу

$$\alpha = \alpha_1 k (\alpha_1 - \alpha_2), \quad (2.201)$$

де

$$k = \frac{\psi_0 \cdot 10^{C_1}}{(\psi_0 + C_2)^{C_3}}, \quad 5 \leq \psi_0 \leq 100, \quad (2.202)$$

$$C_1 = \frac{233}{n + 85} + 0,035; \quad 50 \leq n \leq 1000, \quad (2.203)$$

$$C_2 = \frac{1440}{n + 163}; \quad 50 \leq n \leq 1000, \quad (2.204)$$

$$C_3 = \frac{171}{n + 80} + 1,03; \quad 50 \leq n \leq 1000, \quad (2.205)$$

Визначити b для моделі телеграфних, кабельних та радіорелейних ліній зв'язку можна за допомогою номограми, що показана на рис. 2.58. Для цього за відомими n і ψ_0 в нижній частині номограми знаходять значення коефіцієнта k . На верхній частині номограми через відомі значення α_1 і α_2 проводиться пряма лінія, перетин якої з знайденим значенням k визначить значення α . Нарешті, за визначеним значенням α визначається значення b . На рис. 2.58 наведений приклад визначення b для значень $n = 150$, $\psi_0 = 12$, $\alpha_1 = 1,15$ і $\alpha_2 = 0,25$, при яких $\alpha = 0,365$ і $b = 2,32$.

Математичне сподівання і дисперсія довжини серій підряд спотворених комбінацій можуть бути знайдені з виразів:

$$M[v] = \sum_{v=1}^{\infty} v P(V = v) = \frac{b}{b-1}, \quad (2.206)$$

$$\sigma^2[v] = \sum_{v=1}^{\infty} (v - M[v])^2 P(V = v) = \frac{b}{(b-1)^2}, \quad (2.207)$$

де b визначається з (2.200).

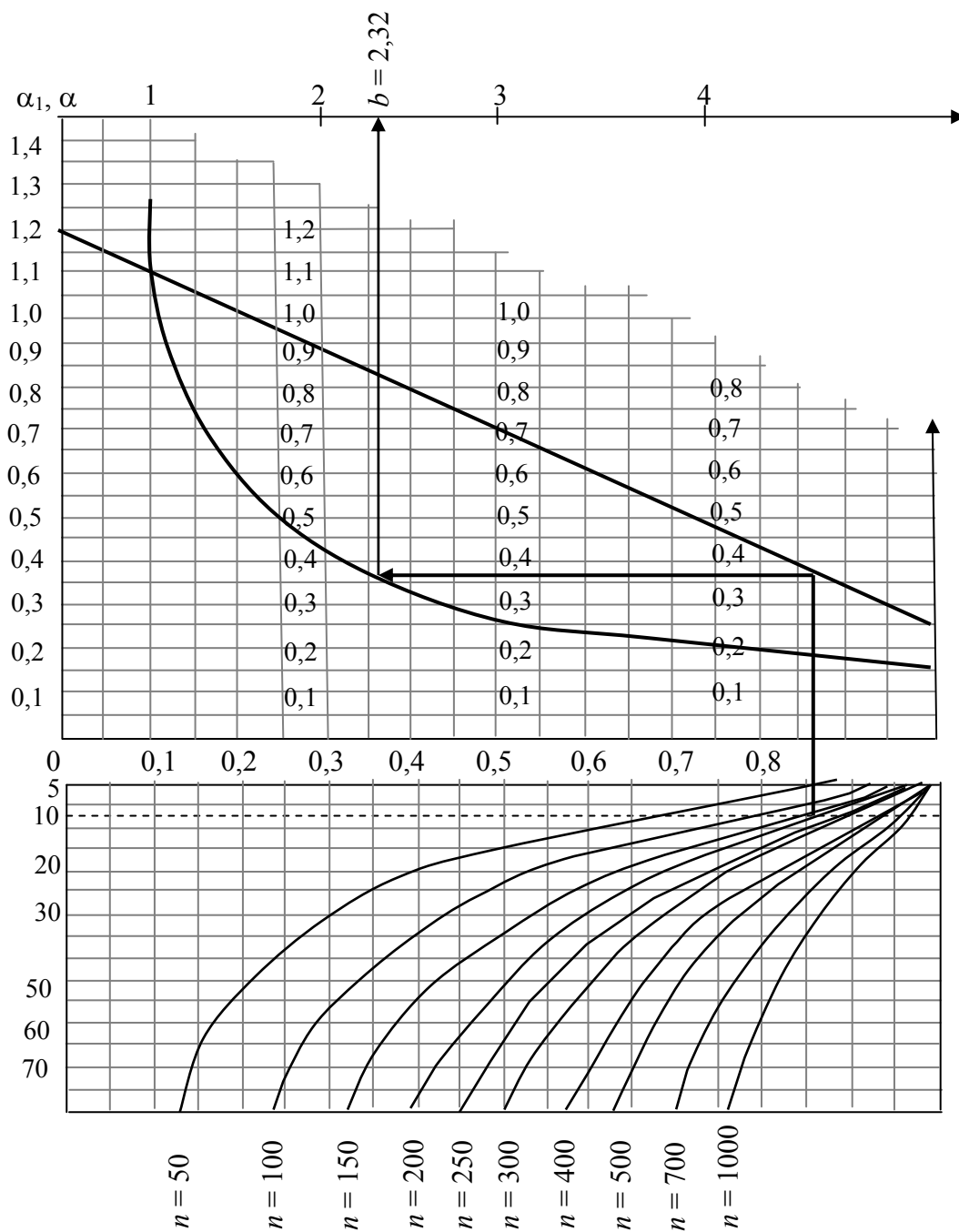


Рисунок 2.58 – Номограми для визначення $b = f(\alpha_1, \alpha_2, \psi_0, n)$

При тонких оцінках характеристик ефективності систем передачі даних і при дослідженні кількісних показників ефективності функціонування складних алгоритмів обміну повідомленнями в трактах необхідно знати не тільки параметри виду $R(V = v)$, $R(V \leq v)$, $M[v]$, $\sigma^2[v]$, але і аналогічні параметри, що визначають розподіл ймовірностей довжин серій z суміжних неспотворених кодових комбінацій. При цьому безпосереднє застосування аналітичних моделей може не дати бажаних результатів через використання в них параметра W , що обмежує максимальну довжину серії z величиною $[W/n]$. З цієї ж причини

недоцільно користуватися методом генерації статистики з використанням параметрів усіх розглянутих моделей на програмній моделі реального каналу зв'язку і отримувати на її основі емпіричні залежності для розподілу ймовірностей $R(Z \leq z)$. Для отримання розподілів виду $R(Z \leq z)$ необхідно безпосередньо використовувати результати експериментального дослідження реальних каналів зв'язку за розподілом інтервалів між помилками $R(u)$. Дослідження реальних каналів зв'язку показало, що для аналітичного опису функції $R(Z \leq z)$ може бути використана апроксимація виду

$$R(Z \leq z) = 1 - \exp(-\tau z^\gamma), \quad (2.208)$$

де параметр γ для телефонних та провідних телеграфних каналів змінюється в межах $0,4 \leq \gamma \leq 0,5$, для телеграфних КХ радіоканалів в межах $0,5 \leq \gamma \leq 0,6$, а параметр τ залежить від математичного сподівання довжини серії суміжних неспотворених блоків $M[z]$. Переходячи в (2.208) до безперервних величин, для густини ймовірності $p(z)$ отримуємо

$$p(z) = \frac{dR(Z \leq z)}{dz} = \gamma \tau z^{\gamma-1} \exp(-\tau z^\gamma). \quad (2.209)$$

Математичне очікування з урахуванням (2.209) визначиться як

$$M[z] = \int_0^\infty zp(z) dz = \int_0^\infty \gamma \tau z^\gamma \exp(-\tau z^\gamma) dz = \tau^{-\frac{1}{\gamma}} \Gamma\left(\frac{\gamma+1}{\gamma}\right). \quad (2.210)$$

Число неспотворених блоків $M(0, n)$ при загальному числі переданих в каналі блоків M дорівнює

$$M(0, n) = M[1 - P(\geq 1, n)], \quad (2.211)$$

число серій різної довжини z

$$\sum_{\{z\}} M_z(0, n) = \frac{M[1 - P(\geq 1, n)]}{M[z]}, \quad (2.212)$$

і з точністю до одиниці при досить великому M справедлива рівність

$$\frac{MP(\geq 1, n)}{M[v]} \approx \frac{M[1 - P(\geq 1, n)]}{M[z]}, \quad (2.213)$$

звідки

$$M[z] = \frac{1 - P(\geq 1, n)}{P(\geq 1, n)} M[v], \quad (2.214)$$

де $M[v]$ визначається з (2.206). З використанням (2.210) і (2.214) знаходимо

$$\tau = \left\{ \frac{\Gamma\left(\frac{1+\gamma}{\gamma}\right) P(\geq 1, n)}{1 - P(\geq 1, n) M[v]} \right\}^\gamma, \quad (2.215)$$

і для $R(Z \leq z)$ з (2.208) з урахуванням того, що в інженерних розрахунках можна прийняти $\gamma = 0,5$, не здійснюючи при цьому будь-якої суттєвої помилки, запишемо

$$R(Z \leq z) = 1 - \exp \left\{ - \left[\frac{2P(\geq 1, n)z}{1 - P(\geq 1, n)} \frac{1}{M[v]} \right]^{0,5} \right\}, \quad (2.216)$$

звідки з урахуванням (10.50)

$$R(Z \leq z) = 1 - \exp \left[- \left(\frac{2z}{M[z]} \right)^{0,5} \right], \quad (2.217)$$

де

$$M[z] = \frac{b[1 - P(\geq 1, n)]}{(b - 1)P(\geq 1, n)}, \quad (2.218)$$

що впливає з (2.214) і (2.206).

Значення ймовірностей $R(Z \leq z)$, визначені з (2.217), відрізняються від експериментальних даних незначно. При цьому особливо гарний збіг має місце при малих і великих значеннях z . На рис. 2.59 наведені експериментальні дані, що отримані методом генерації статистики на програмній моделі і апроксимуюча крива побудована за формулою (2.217) для каналу № 1.

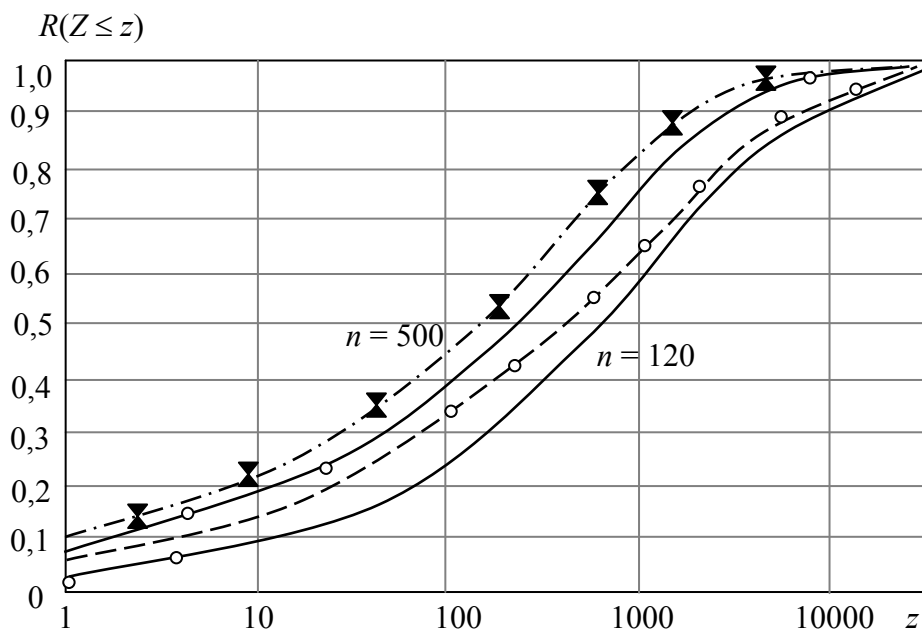


Рисунок 2.59 – Експериментальні дані та апроксимація розподілу $R(Z \leq X)$ для каналу №5

———— $\gamma = 0,5$; - - - - - $\gamma = 0,4$

2.9. Питання та задачі для самоперевірки

1. Які сигнали є періодичними й неперіодичними, одномірними й багатомірними, детермінованими й випадковими?
2. Що являє собою дельта-функція й у чому полягає зміст її фільтруючої властивості?
3. Що розуміють під узагальненим рядом Фур'є, як визначаються його коефіцієнти і який зміст вони мають?
4. Записати ряд Фур'є в комплексній формі. Пояснити зміст вхідних у нього величин.
5. Написати ряд Котельникова й пояснити, що в ньому є базисними функціями.
6. Пояснити, як здійснити відновлення аналогового сигналу по дискретних вибірках і вказати через які проміжки часу вони беруться.
7. Який вид має спектр періодичного сигналу?
8. Яка практична цінність спектральної вистави при розв'язанні завдання про проходження сигналу через лінійну систему передачі інформації?
9. Дайте визначення поняттю середньої потужності періодичного сигналу.
10. Яким образом вводиться поняття спектра для неперіодичних сигналів?
11. Запишіть вираження для прямого й зворотного перетворень Фур'є, дайте визначення поняття спектральної щільності і її розмірності.
12. Дайте визначення понять реалізації й ансамблю реалізацій випадкового процесу.
13. Який випадковий процес називається стаціонарним?
14. Дайте визначення основних характеристик випадкового процесу.
15. Які завдання розглядаються при прийманні сигналів?
16. Як формується критерій оптимального приймання сигналів?
17. Сформулюйте й поясніть критерій Котельникова при прийманні дискретних сигналів.
18. Як визначається ймовірність помилки при когерентному прийманні дискретних сигналів?
19. Дайте порівняльну оцінку завадостійкості когерентного приймання двійкових дискретних сигналів з типовими видами модуляції й покажіть її зв'язок з представленням сигналів у вигляді векторів у функціональному просторі.
20. Як оцінюється завадостійкість некогерентного приймання в каналах із завмираннями?

ГЛАВА 3

ТЕОРІЯ БЛОКОВИХ КОРИГУЮЧИХ КОДІВ

3.1. Основні характеристики блокових кодів, їхнє описання та властивості

Класифікація основних коригуючих кодів. На сьогодні відома значна кількість кодів, коригуючих помилки, які використовуються в системах цифрового зв'язку, і тому їхня систематизація і класифікація дуже ускладнена. У зв'язку з цим, при побудові класифікаційної діаграми (рис. 3.1) розглядаються тільки ті коди, які знаходять застосування у системах передачі дискретних повідомлень (СПДП).

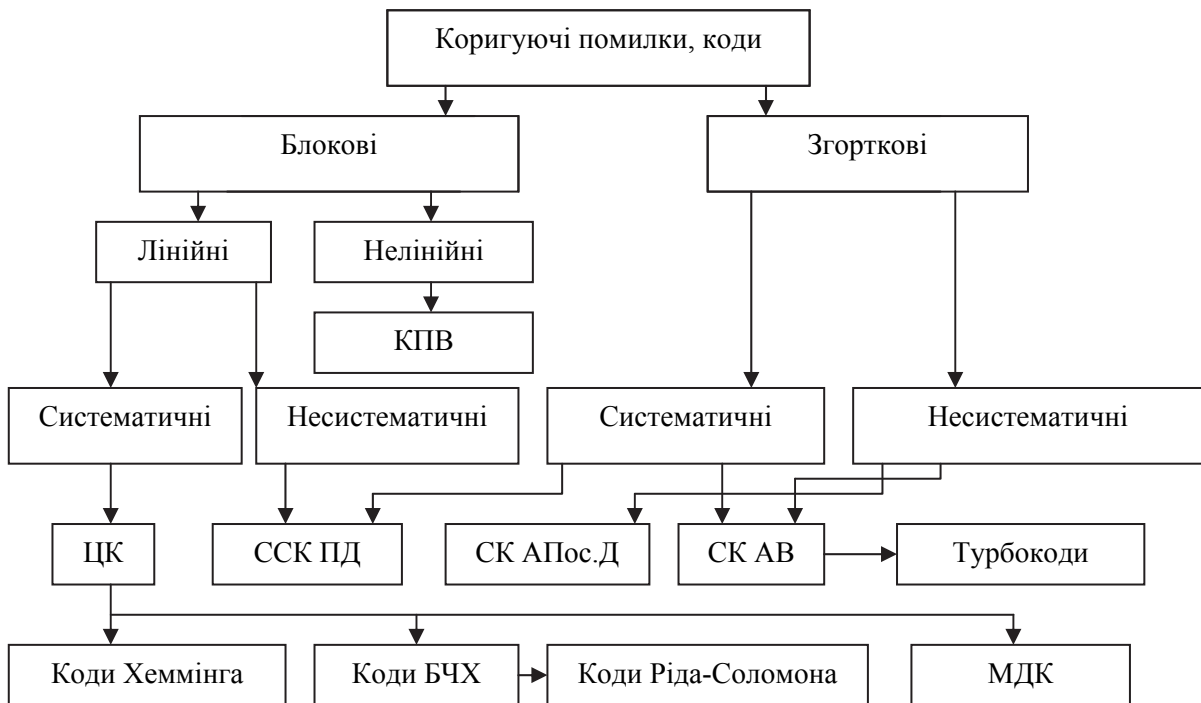


Рисунок 3.1 – Класифікація основних завадостійких кодів

Двійкові коригуючі коди можна поділити на два великих класи – *блокові* та *згорткові*.

До блокових відносяться такі коди, в яких кодування і декодування здійснюються в межах блока, що складається з певного числа кодових символів. У літературі з завадостійкого кодування блоки кодових символів називають по-різному: кодовими словами, кодовими комбінаціями й кодовими векторами. До згорткових кодів, що називалися раніше неперервними, рекурентними або ланцюговими, відносяться такі коди, в яких процес кодування має неперервний характер без виділення меж при формуванні послідовності кодових символів. При аналізі блокових кодів передбачаєть-

ся синхронний метод передачі, який характеризується постійними величинами довжини кодового слова та довжини елементарної послідовності, яка дорівнює $t_0 = 1/2\Delta F$ ($t_0 = 1/\Delta F$). При синхронному методі передачі реалізується послідовна передача коефіцієнтів α_i полінома

$$G(a) = \alpha_{n-1}a^{n-1} + \alpha_{n-2}a^{n-2} + \dots + \alpha_1a + \alpha_0, \quad (3.1)$$

де a – позиційність системи (число станів інформаційного параметру);

α_i – коефіцієнти, число яких дорівнює a :

$$\alpha = a - 1; a - 2; \dots 0 \quad (\alpha_i \leq a - 1).$$

При передачі по каналу з базою $B = t_0 \cdot \Delta F = 1$ ($t_0 = 1/\Delta F$) кожний із коефіцієнтів α_i передається відповідним сигналом тривалістю t_0 . Такий метод кодування називається позиційним (або розрядно-цифровим кодуванням РЦК).

Важливою відмінністю згорткового кодування є те, що кодові символи на виході кодера залежать не тільки від інформаційних символів, що надійшли на даний момент часу, але й від попередніх символів на його вході.

Блокові коди, в свою чергу, поділяються на *лінійні* та *нелінійні*. До лінійних відносяться такі коди, в яких формування блоків, тобто кодування здійснюється з використанням лінійних операцій (підсумовування і множення над інформаційними символами з урахуванням арифметики за модулем 2). У протилежному разі коригуючі коди відносяться до нелінійних, тому що сума двох кодових комбінацій (КК) з заданими властивостями не утворює комбінацію, що належить до даного коду. Найпростішим прикладом нелінійного коду є міжнародний семиелементний код МТА-3, який ще називають кодом з постійною вагою (КПВ), в кожній кодовій комбінації якого міститься три одиниці і чотири нуля.

Лінійні коди, в свою чергу, поділяються на *систематичні* та *несистематичні*. В систематичних кодах інформаційні символи на виході кодера формуються в кінці кодового слова. Належність до систематичних або несистематичних кодів визначається вибором коду й алгоритму кодування. Значну частину лінійних кодів займають циклічні коди (ЦК), які знаходять застосування у системах цифрової передачі різного роду повідомлень. До них відноситься досить велике число коригуючих кодів, серед яких найбільш відомими є:

- коди Хеммінга, що виправляють однократні і виявляють двократні помилки;

- коди БЧХ, що володіють високою коригуючою здатністю, запропоновані Хоквінгом, Боузом і Чоудхурі;

- коди Ріда-Соломона, що являють собою важливий підклас кодів БЧХ з коефіцієнтами кінцевих полів Галуа, які знайшли застосування у системах космічного зв'язку (NASA);

– мажоритарно декодовані коди (МДК), що виправляють багаторазові помилки, яким властиві прості алгоритми декодування.

Згорткові коди (ЗК), вперше запропоновані Елайесом, як і блокові, також поділяються на *систематичні* і *несистематичні*. Перші, до яких відносяться самоортогональні згорткові коди (ОЗК), декодуються надто простим пороговим методом, а другі – з використанням алгоритму послідовного декодування (ЗК АПос. Д), запропоновані Дж. Возенкрафтом.

Заслуговує на згадку внесок, зроблений російськими вченими з питань завадостійкості кодування Зяблова В.В. і Золотарьова В.В., а саме в області каскадного кодування і багатопорогового декодування самоортогональних ЗК.

Широко використовуваний на даний час алгоритм Вітербі може застосовуватись як до несистематичних, так і до систематичних кодів. На основі алгоритму Вітербі розроблені і впроваджені турбокоди К. Берроу.

Загальні поняття і визначення. Геометрична інтерпретація коригуючих кодів. Ефективним методом підвищення надійності СПДП є використання коригуючих кодів. Кодер систематичного коду – це пристрій, що формує на основі інформаційної послідовності символів a_1, a_2, \dots, a_m послідовність перевірочних символів b_1, b_2, \dots, b_r . За допомогою введеної надлишковості декодер має можливість, в залежності від вибору коригуючого коду й алгоритму декодування, виявляти або виправляти помилково прийняті інформаційні символи (елементи), що утворилися в результаті дії різного роду завад у каналі зв'язку.

Блокові коди характеризуються довжиною блока або значністю кодового слова (КС) n і кількістю інформаційних символів m . Для них прийнято позначення (n, m) . До лінійних (n, m) кодів належать такі, в яких $r = n - m$ надлишкових символів формуються із m інформаційних за допомогою лінійних операцій, тобто операцій підсумовування і множення (Для двійкових кодів додавання виконується за $\text{mod } 2$, тобто $0 + 1 = 1$, $1 + 0 = 1$, $0 + 0 = 0$ і $1 + 1 \equiv 0$, а операція множення – в звичайному розумінні, тобто $0 \times 1 = 0$, $1 \times 0 = 0$, $0 \times 0 = 0$ і $1 \times 1 = 1$; знак \equiv тут можна розглядати як результат підсумовування в двійковій системі числення без урахування старшого розряду. Наприклад, $1 + 1 = 2_{10} = 10_2 \equiv 0$).

Перевірочні символи для деякого групового коду можуть бути визначені наступними j виразами:

$$b_j \equiv \left(\sum_{i=0}^m a_i \times \alpha_{ji} \right) \text{mod } 2, \quad (3.2)$$

де a_i – інформаційні символи; $\alpha_{ji} = 0$; 1 – коефіцієнти, що визначають алфавіт коду; $j = 1, 2, \dots, n - m$ – індекси перевірочних елементів. При цьому

коефіцієнти α_{ji} утворюють прямокутну матрицю для визначення переві- рочних символів

$$B_{(n-m),m} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1(n-m)} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2(n-m)} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{m(n-m)} \end{pmatrix}.$$

Базисні вектори-рядки даної матриці лінійно незалежні. Нагадає- мо, що вектори-рядки називаються лінійно незалежними, якщо жоден із них не може бути поданий у вигляді лінійної комбінації інших рядків. Іншими словами, їх сума не повинна утворювати рядок, в якому всі еле- менти нульові.

В n -значних кодах з усіх можливих з'єднань кодових комбінацій

$$N_{об} = C_n^0 + C_n^1 + C_n^2 + \dots + C_n^n = 2^n$$

для передавання повідомлень використовується тільки $N_p = 2^m$ КК, які на- зиваються *дозволеними*. Останні невикористовувані комбінації $(N_{об} - N_p)$ називаються *недозволеними*.

Лінійні блокові коди мають властивості замкненості, які означають, що сума за mod 2 двох і більше дозволених кодових комбінацій утворюють іншу дозволена кодову комбінацію, що належить цьому ж коду. Із зазначе- ного можна зробити висновок, що будь-який лінійний код завжди має ну- льове кодове слово (000...000), утворене в результаті підсумовування декі- лькох дозволених.

Коригуючі коди призначені для виправлення або виявлення помилок певної кратності. *Кратність* помилки визначається кількістю спотворених символів у прийнятій кодовій комбінації значності n .

При незалежних помилках у каналі зв'язку ймовірність випадкового утворення t -кратної помилки в інтервалі n елементів визначається відомою з курсу математики з теорії ймовірності формулою Бернуллі

$$P_t = C_n^t p_0^t (1 - p_e)^{n-t},$$

де C_n^t – біномінальні коефіцієнти; $p_0 = P(1/0) + P(0/1)$ – повна ймовірність помилки у каналі зв'язку.

Коригуюча здатність двійкових кодів залежить від мінімальної кодо- вої відстані за Хеммінгом

$$d_0 = \min \sum_{i=1}^n (A_{ji} + A_{li}) \text{ mod } 2,$$

де A_{ji}, A_{li} – порівняльні КС; $j, l = 1, 2, 3, \dots, 2^k$, $j \neq l$. Таким чином, *мінімаль- на кодова відстань* або *кодова відстань* дорівнює найменшій із усіх мож- ливих відстаней в метриці Хеммінга між усіма можливими парами КС. Для

лінійних кодів, з урахуванням того, що в кодї завжди є нульове КС, кодова відстань визначається мінімальною вагою $W(t)$ кодових слів, тобто

$$d_0 = \min W(t).$$

Вага КС дорівнює арифметичній сумі числа одиниць серед інформаційних та перевірючих кодових символів n -значного кодового слова (КС), тобто:

$$Wt(A_j) = \sum_{i=1}^m a_i + \sum_{i=1}^r b_i.$$

Максимальна кратність виявлення помилок t_B або виправлення помилок $t_{ВП}$ пов'язані з кодовою відстанню наступними виразами:

– в режимі виявлення помилок

$$t_B = d_0 - 1; \quad (3.3)$$

– в режимі виправлення помилок

$$t_{ВП} = \lceil (d_0 - 1) / 2 \rceil. \quad (3.4)$$

Теорема 1. Якщо d_0 парне, то код може одночасно виправляти $(d_0 - 2) / 2$ помилок і виявляти $d_0 / 2$ помилок.

На рис. 3.2 наведена геометрична модель найпростішого коригуючого коду з парним числом одиниць, показана на площині, де всі дозволені КС зображені у вигляді точок, які є центрами кіл з радіусами $d = 1$. Недозволені КС зображені точками на колах, які завжди є загальними для двох суміжних кіл.

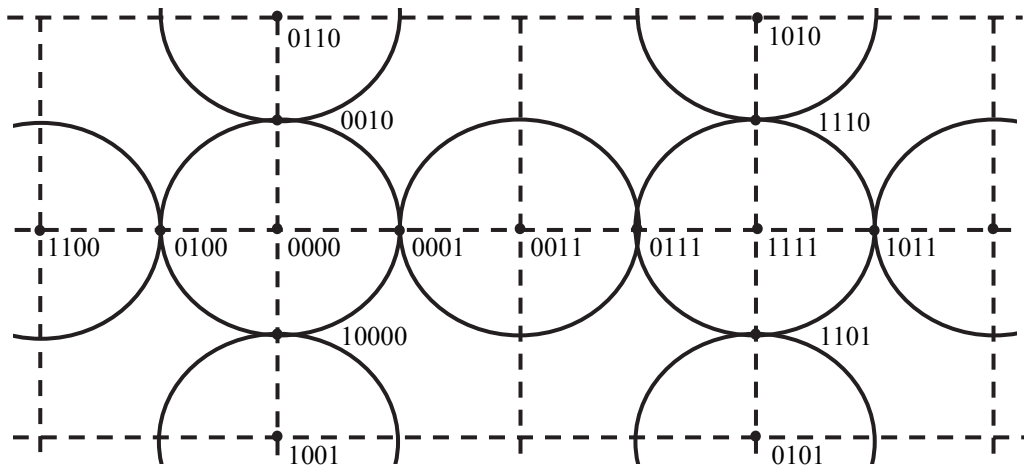


Рисунок 3.2 – Геометрична модель коригуючого коду

Із рис. 3.2 наочно видно, що мінімальна відстань між двома дозволеними КС дорівнює двом одиницям за Хеммінгом, тобто $d_0 = 2$. Тут дозволені КС мають єдине відображення – центри кіл, а кожному недозволеному КС відповідає два дозволені КС, в чому виявляється невизначеність при

їх декодуванні. Принцип виявлення помилок для коду (4, 3) очевидний. Якщо в результаті дії завад вирішене КС «переходить» із центра на коло ($d=1$), то таке спотворення в місці прийому завжди буде виявлене за структурою КС коду з парним числом одиниць. Перехід із одного центра кола в центр будь-якого іншого кола ($d=2$ чи 4) призводить до невиявленої помилки. Такий код, як видно із наведеного рисунка, дозволяє тільки виявляти всі помилки непарної кратності.

Подібно коду (4, 3), на рис. 3.3 наведений фрагмент геометричного подання коду з $d_0=3$ та коду з $d_0=4$. Із наведених рисунків видно, що перший код дозволяє виправити однократні помилки, а другий – дає можливість, крім виправлення однократних помилок, ще й виявляти двократні помилки, що переконує в справедливості виразів (3.3), (3.4).

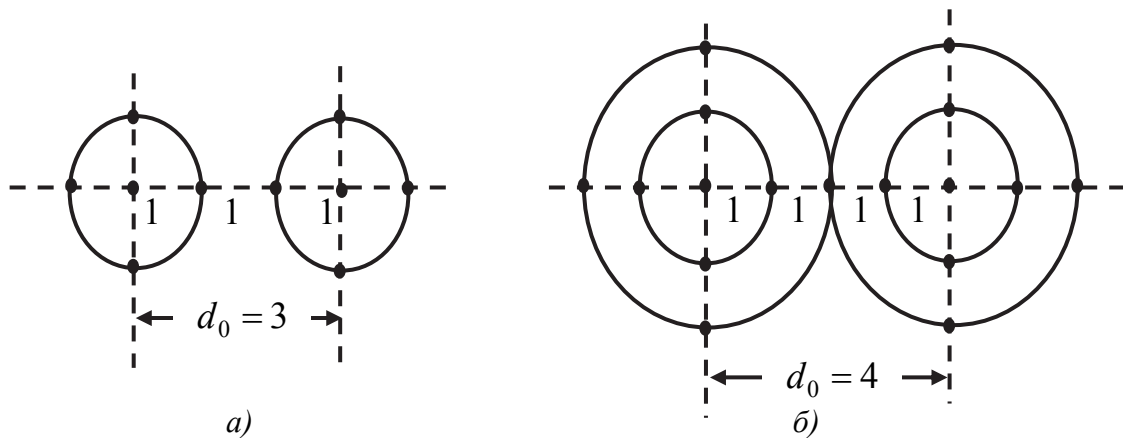


Рисунок 3.3 – Геометричні моделі кодів:
а – що виправляють однократні помилки;
б – що виправляють однократні помилки
та виявляють двократні помилки

Граничні можливості коригуючої здатності лінійних блокових кодів. Як раніше зазначалося, побудова коригуючого коду полягає у формуванні надлишкових (перевірочних) символів b_1, b_2, \dots, b_r за відомими інформаційними символами a_1, a_2, \dots, a_m . При цьому, природно виникає питання про залежність між такими важливими параметрами, як n , $r = n - m$ і d_0 . Розв'язанням цієї важливої задачі займалося багато вчених, однак точної залежності між цими параметрами не знайдено, установлені лише деякі оцінки, що дозволяють зробити висновок про можливість побудови того чи іншого коду із заданими параметрами.

Задача, яка виникає при побудові лінійного n -значного коду, коригуючого незалежні помилки, полягає у визначенні необхідного мінімального числа перевірочних символів r для виправлення t -кратних помилок. Для розв'язання цієї задачі в літературі з кодування є різні граничні співвідношення. Перша оцінка надлишкових символів для двійкових кодів може бути отримана внаслідок використання граничної умови Хеммінга

$$2^{n-m} \geq \sum_{i=0}^{t_{\text{вп}}} C_n^i. \quad (3.5)$$

Значення цього виразу полягає в наступному. Якщо задані основні параметри лінійного коду n і $t_{\text{вп}} = (d_0 - 1)/2$, то можлива мінімальна кількість надлишкових символів $r = n - m$ може бути визначена за допомогою умови (3.5). Для наочності на рис. 3.4 наведені графіки границь Хеммінга згідно з виразом

$$n - m \geq \left\lceil \log_2 \sum_{i=0}^{t_{\text{вп}}} C_n^i \right\rceil \quad d_0 \in 3; 5; 7. \quad (3.6)$$

Тут $\lceil x \rceil$ означає найближче ціле число більше або рівне x . Наприклад, для коду з $t_{\text{вп}} = 1$ і $n = 9$ $n - m \geq \log_2(1 + 10) = 3,46$. Таким чином, $n - m = 4$, що визначає параметри коду (9, 5, 3).

Якщо точка з координатами n і $r = n - m$ знаходиться нижче тієї чи іншої граничної залежності, то коригуючий код з параметрами (n, m, d_0) не існує. В протилежному випадку можливе існування коригуючого коду з такими параметрами.

При цьому слід підкреслити, що рівність (3.6) за будь-яких $t_{\text{вп}}$ вказує тільки теоретичну границю мінімально можливого числа перевірочних символів, але, на жаль, не в усіх випадках можна одержати код з $r' > r$ для практичного використання. Часто при побудові коду з заданими n і $t_{\text{вп}}$ перевірочних символів треба більше, ніж виходить із (3.6).

У зв'язку з цим слід розглянути ще додатково граничну умову Варшавова-Гільберта, яку подамо у вигляді теореми.

У зв'язку з цим слід розглянути ще додатково граничну умову Варшавова-Гільберта, яку подамо у вигляді теореми.

Теорема 2. Якщо при заданих параметрах n , m і d_0 використовується нерівність

$$2^{n-m} \geq \sum_{i=0}^{d_0-2} C_{n-1}^i, \quad (3.7)$$

то існує (n, m, d_0) код, який реалізується за допомогою не більше $n - m$ перевірок на парність.

Для пояснення співвідношень (3.5) і (3.7) розглянемо конкретний приклад побудови коригуючого коду. Нехай треба реалізувати код з

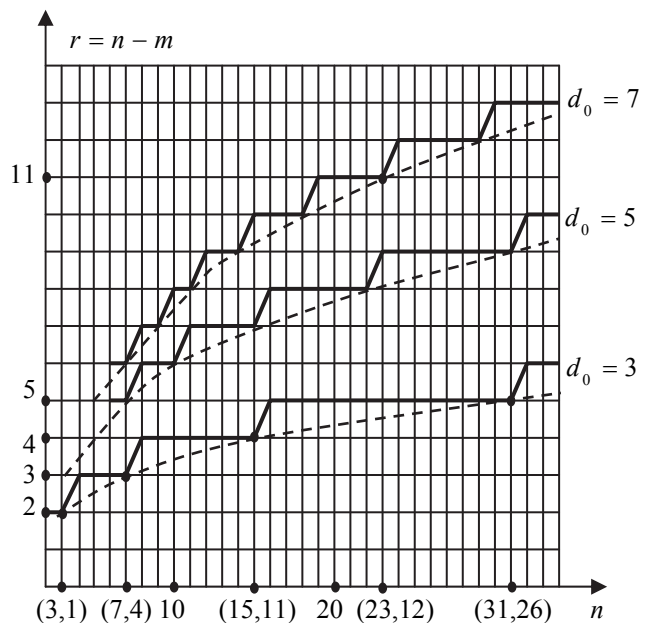


Рисунок 3.4 – Границі Хеммінга для блокових кодів з $d_0 = 3, 5, 7$

$n = 63$, що виправляє двократні помилки $t_{\text{вн}} = 2$ ($d_0 = 5$). Тоді, згідно з (3.5),

$$2^{n-k} \geq \sum_{i=0}^2 C_{63}^i = 1 + 63 + 1953 = 2017.$$

Із нерівності $2^{n-m} \geq 2017$, що відповідає мінімальному значенню кількості перевірюваних вимаганих символів виходить, що $r = n - m = 11$, тому що до числа 2017 найближчий степінь двійки $2^{11} = 2048$. При $n = 63$ і $m = 63 - 11 = 52$ із (3.7) отримуємо твердження тільки про можливість існування коду (63, 52, 5). Однак процедура побудови такого коду невідома. Крім цього, можна зробити висновок, що коди довжиною $n = 63$ з $n - m < 11$ не існують, тому що у цьому випадку умова Хеммінга не виконується.

Звернемося тепер до умови (3.7), яка гарантує побудову коду $n = 63$ і $d_0 = 5$ за деякого значення r , якщо

$$2^{n-m} \geq \sum_{i=0}^3 C_{62}^i = 1 + 62 + 1891 + 37820 = 39774.$$

Із наведеної нерівності бачимо, що у даному випадку $n - m$ повинно дорівнювати 16, тому що 2^{16} є найближчим більшим до числа 39774 ($2^{16} = 65536 > 39774$, а $2^{15} = 32768 < 39774$). Таким чином, найменше число перевірюваних символів в (n, m) коді, для якого виконується гранична умова Варшавова-Гільберта, дорівнює 16. Таким чином, умова (3.7) гарантує можливість побудови коду (63, 47, 5).

Тепер, звертаючись до таблиць відомих коригуючих кодів і зіставляючи в них наведені коди з кодом (63, 47, 5), бачимо, що цей код з точки зору надлишковості є неоптимальним, тому що можлива побудова коду (63, 51, 5) з $n - m = 12$, і очевидно, цей код є кращим, оскільки він близький за своїми параметрами до границі Хеммінга.

Коди, для яких гранична умова Хеммінга виконується зі знаком рівності, називаються *досконалими* або *щільноупакованими*. Найпростішими прикладами таких кодів є всі коди Хеммінга з $d_0 = 3$, для яких $n = 2^r - 1$ і $m = 2^r - r - 1$, при $r = 2, 3, 4, \dots$. Всі досконалі коди володіють мінімальною надлишковістю $\rho = r/n$ для досягнення потрібної коригуючої здатності. Граничні умови Хеммінга для кодів (3, 1), (7, 4), (15, 11), (31, 26), ..., що виконуються зі знаком рівності, можна показати простим виразом

$$2^{n-m} = C_n^0 + C_n^1.$$

Особливий інтерес становить код Голея (23, 12) – єдиний досконалий код, що виправляє помилки першої, другої і третьої кратностей ($d_0 = 7$).

Для цього коду, як і для кодів Хеммінга, умова (3.5) виконується зі знаком рівності

$$\sum_{i=0}^t C_n^i = C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3 = 1 + 23 + 253 + 1771 = 2048 = 2^{11}.$$

Код Голя займає важливе місце в середовищі досконалих кодів і є джерелом для багатьох досліджень в теорії кодування.

Матричне описання блокових кодів. Умови Варшамова при реалізації лінійних кодів. Систематичні лінійні блокові коди компактно задаються породжуючою матрицею $G_{n,k}$ у наведеній ступінчастій формі, ліва частина якої являє собою квадратну одиничну підматрицю $I_{m,m}$, а права – підматрицю перевірочних елементів $B_{(n-m),m}$

$$G_{n,m} = \left\| I_{m,m} B_{(n-m),m} \right\| = \left\| \begin{array}{cccccc} 1 & 0 & 0 & \dots & 0 & 0 & \alpha_{11} & \alpha_{12} & \dots & \alpha_{1(n-m)} \\ 0 & 1 & 0 & \dots & 0 & 0 & \alpha_{21} & \alpha_{22} & \dots & \alpha_{2(n-m)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 & \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{m(n-m)} \end{array} \right\|. \quad (3.8)$$

Процес кодування, з математичної точки зору, означає множення матриці рядка послідовності інформаційних символів $A_k = \|a_1, a_2, \dots, a_k\|$ на породжуючу матрицю $G_{n,m}$. Результатом такого множення є матриця-рядок D_n , яка відповідає КС систематичного (n, m) -коду. Нагадаємо, що множення матриці-рядка A_2 на прямокутну матрицю $G_{3,2}$ виконується наступним чином:

$$\begin{aligned} A_2 \times G_{3,2} &= \|a_1 \ a_2\| \times \left\| \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right\| \times \left\| \begin{array}{cc} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{array} \right\| = \left\| \begin{array}{ccc} (a_1 \cdot 1) & (a_1 \cdot 0) & (a_1 \cdot \alpha_{11}) \\ (a_2 \cdot 0) & (a_2 \cdot 1) & (a_2 \cdot \alpha_{21}) \end{array} \right\| = \\ &= \left\| (a_1 \cdot 1) + (a_2 \cdot 0) \quad (a_1 \cdot 0) + (a_2 \cdot 1) \quad (a_1 \cdot \alpha_{11} + a_2 \cdot \alpha_{21}) \right\| = \|a_1 \ a_2 \ b_1\|. \end{aligned}$$

Із наведеного прикладу видно, що добуток матриці-рядка, який містить m елементів, на прямокутну матрицю розмірності $n \times m$ є матриця-рядок, що складається з n елементів. Таким чином,

$$A_m \times G_{n,m} = \|a_1 \ a_2 \ \dots \ a_m \ b_1 \ b_2 \ \dots \ b_{n-m}\| = D_n,$$

де перевірочні символи b_1, b_2, \dots, b_{n-m} визначаються системою двійкових рівностей

$$b_j \equiv \left(\sum_{i=1}^m a_i \times \alpha_{ji} \right) \text{mod } 2, \quad (3.9)$$

а $j = 1, 2, 3, \dots, n - m$.

деними умовами Варшамова 2, 3 і 4 вибираємо підматрицю $B_{3,3}$ (шляхом вибору лінійно-незалежних рядків) і будуємо породжуючу матрицю

$$G_{6,3} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

яка визначає систематичний код $(6, 3)$ з $d_0 = 3$.

Аналогічно тому, як при кодуванні часто використовується поняття породжуючої матриці $G_{n,m}$, в основу декодування може бути покладена перевірна матриця $H_{n,r}$. Значення назви «перевірна матриця» полягає в тому, що за допомогою цієї матриці виконується перевірка належності прийнятого КС до одного з дозволених.

Перевірна матриця $H_{n,r}$ легко отримується з породжуючої матриці $G_{n,m}$ шляхом транспонування підматриці $B_{(n-m),m}$ і перестановки її місцями з одиничною матрицею

$$H_{n,(n-m)} = \begin{pmatrix} B_{m,(n-m)} & I_{(n-m),(n-m)} \end{pmatrix},$$

де $B_{m,(n-m)}$ – транспонована підматриця перевіричних елементів $B_{(n-m),m}$, тобто така, стовпцями якої є рядки вихідної підматриці, а $I_{(n-m),(n-m)}$ одинична квадратна підматриця розмірності $(n-m)^2$.

У розгорнутому виді перевірна матриця з використанням позначень згідно з (3.8) має вигляд:

$$H_{n,(n-m)} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1m} & 1 & 0 & 0 & \dots & 0 \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2m} & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{(n-m)1} & \alpha_{(n-m)2} & \dots & \alpha_{(n-m)m} & 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Розглянемо побудову перевірної матриці на основі породжуючої матриці коду Хеммінга $(7, 4)$

$$G_{7,4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Перевірна матриця при заданій породжуючій матриці має вигляд

$$H_{7,3} = \begin{vmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}.$$

Результат множення матриці-рядка прийнятого КС $D'_n = (D_n + E_n) \bmod 2$, де $E_n = \|e_1 e_2 e_3 \dots e_n\|$ – матриця-рядок вектора помилок, що містить одиниці тільки на тих позиціях, які створюють кодові символи в прийнятій КК на транспоновану матрицю $H_{n,(n-m)}^T$, називається *синдромом*

$$D'_n \times H_{n,(n-m)}^T = S_{(n-m)}. \quad (3.11)$$

У розгорнутому вигляді вираз (3.11) можна подати так:

$$a'_1 a'_2 \dots a'_m b'_1 b'_2 \dots b'_{n-m} \times \begin{vmatrix} \alpha_{11} & \alpha_{21} & \dots & \alpha_{(n-m)1} \\ \alpha_{12} & \alpha_{22} & \dots & \alpha_{(n-m)2} \\ \dots & \dots & \dots & \dots \\ \alpha_{1m} & \alpha_{2m} & \dots & \alpha_{(n-m)m} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix} = \|s_1 s_2 \dots s_{n-m}\|.$$

Неважко переконатися в тому, що елементи матриці-рядка синдрому визначаються таким чином:

$$s_j \equiv \left(\sum_{i=1}^m a'_i \times \alpha_{ji} + b'_j \right) \bmod 2, \quad (3.12)$$

де $j = 1, 2, \dots, (n - m)$.

Якщо прийняте КС не було піддане дії завад, тобто $E_n = 0$, то $S_{n-m} = 0$. Важливою особливістю синдрому є те, що він не залежить від вигляду переданого КС, а визначається тільки конфігурацією помилок у прийнятому КС. Якщо код використовується для виправлення помилок, то при декодуванні устанавлюється відповідність між видом синдрому і номером спотвореного кодового символу. В двійкових кодах виправлення помилок зводиться до інвертування спотвореного кодового символу перед видачею прийнятого повідомлення споживачу. Якщо кількість помилок у прийнятому КС перевищує величину $t_{\text{пом}} > (d_0 - 1)/2$, то в результаті декодування можуть вноситися хибні виправлення, тобто будуть спотворюватися правильно прийняті символи КС або не виправлятися символи з помилками. Від цього явища не застрахований ні один із відомих лінійних

кодерів при синдромному декодуванні. Питання лише в тому, з якою ймовірністю це явище може відбуватися.

На закінчення необхідно визначити, що матриці $G_{n,m}$ і $H_{n,(n-m)}$ зв'язані таким співвідношенням:

$$G_{n,m} \times H_{n,(n-m)}^T = 0.$$

Тут 0 означає нульову матрицю розмірністю $m \times n - m$.

Проілюструємо це на прикладі простого коригуючого коду (5, 3) з $d_0 = 2$, який має породжуючу $G_{5,3}$ і перевіряючу $H_{5,2}$ матриці:

$$G_{5,3} = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{vmatrix} \text{ и } H_{5,2} = \begin{vmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{vmatrix}.$$

Скориставшись правилом множення матриць, обчислимо добуток матриць

$$G_{5,3} \times H_{5,2}^T = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{vmatrix} \times \begin{vmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 & 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 \\ 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 & 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 \\ 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 & 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 \end{vmatrix} = \begin{vmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{vmatrix}.$$

Коди, в яких як породжуючі матриці вибрані $G_{n,m}$ і $H_{n,r}$, називаються *дуальними*. Так, наприклад, такими є коди (7, 4) з $d_0 = 3$ і (7, 3) з $d_0 = 4$, задані матрицями $G_{7,4}$ і $G_{7,3}$.

3.2. Кодування і декодування в блокових кодах

Основу пристрою реалізації кодера вибраного коригуючого коду складають три блоки: а) блок пам'яті, що являє собою комірки пам'яті (тригери); б) суматори за модулем 2, що мають 2 входи і один вихід; в) пристрій множення та константу c зі значеннями 1 або 0, який реалізується наявністю або відсутністю з'єднання між деякими елементами схеми.

Під *технічною складністю кодера* розуміють кількість елементів, що міститься в ньому. Також не слід забувати про число операцій підсумовування і про перехідні процеси, які визначають швидкодію кодера.

На цей час все частіше знаходиться застосування програмна реалізація кодів коригуючих кодів, яка дозволяє оперативно змінювати параметри

коду і навіть переходити від одного коду до іншого в залежності від каналу зв'язку. Досягається це використанням різних програм, за допомогою яких задається той чи інший код. За програмної реалізації кодеків використовуються комп'ютери, побудовані на базі швидкодіючих мікропроцесорів і таких, що мають обладнання спряження з каналом зв'язку.

Побудова схеми кодера (n, m) коду. Як приклад реалізації розглянемо питання, пов'язане з побудовою кодера найпростішого коду $(7, 4)$ з $d_0 = 3$. Для визначення породжуючої матриці скористаємося теоремою 1.

Кількість стовпців підматриці $B_{(n-r), m}$ визначаємо згідно з умовою Варшамова-Гільберта (3.7):

$$2^{n-m} \geq \sum_{i=0}^{d_0-2} C_{n-1}^i = \sum_{i=0}^1 C_6^i = 1 + 6 = 7.$$

Із нерівності $2^{n-m} > 7$ виходить, що $n - m = 3$.

Перший рядок підматриці $B_{(n-m), m}$ вибираємо довільно з урахуванням пункту 2 умов Варшамова, наприклад, 011, вага якої дорівнює $d_0 - 1 = 2$. Другий рядок також повинен мати дві одиниці, і вибираємо його так, щоб сума за mod 2 цих рядків була не менше $d_0 - 1 = 1$, тобто 101. Як третій і четвертий рядки можна вибрати послідовність символів 110 і 111. Тепер неважко переконатись в тому, що вага суми за (mod 2) двох будь-яких рядків підматриці перевірочних елементів задовольняє вищевказаним умовам, і сума всіх рядків не дорівнює нулю. Об'єднуючи інформаційну $I_{(n-m), (n-m)}$ і перевірочну $B_{(n-m), m}$ підматриці, отримуємо породжуючу матрицю для коду $(7, 4)$

$$G_{7,4} = \left\| I_{4,4} B_{3,4} \right\| = \left\| \begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right\|.$$

Перед тим, як перейти до питання побудови схеми кодера, слід звернути увагу на те, що отримана підматриця $B_{3,4}$ може бути перетворена перестановкою рядків в іншому вигляді. Наприклад, в результаті перестановок другого, третього і четвертого рядків підматриці отримуємо іншу підматрицю, яка також задовольняє всім вказаним вимогам і називається *комбінаторно-еквівалентною*:

$$B_{3,4} = \left\| \begin{array}{ccc} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{array} \right\|.$$

Коди, створені за допомогою комбінаторно-еквівалентних підматриць, які мають різну структуру рядків, називаються *еквівалентними*. Такі коди відрізняються тільки зовнішніми ознаками, тобто розташуванням перевірочних символів у КС, і забезпечують однакову коригуючу здатність.

Використавши співвідношення (3.9) стосовно отриманої раніше матриці $G_{7,4}$, отримаємо систему двійкових рівностей для визначення перевірочних символів b_1, b_2 і b_3 за інформаційними a_1, a_2, a_3, a_4

$$\left. \begin{aligned} b_1 &= a_2 + a_3 + a_4 \\ b_2 &= a_1 + a_3 + a_4 \\ b_3 &= a_1 + a_2 + a_4 \end{aligned} \right\} \text{mod } 2.$$

Алгоритм роботи кодера визначається наведеною вище системою рівностей, яка вказує, в якому поєднанні потрібно підсумовувати інформаційні кодові елементи, щоб сформувані відповідні перевірочні символи КС коду (7, 4). На рис. 3.5 наведена функціональна схема кодера, принцип роботи якої полягає в наступному.

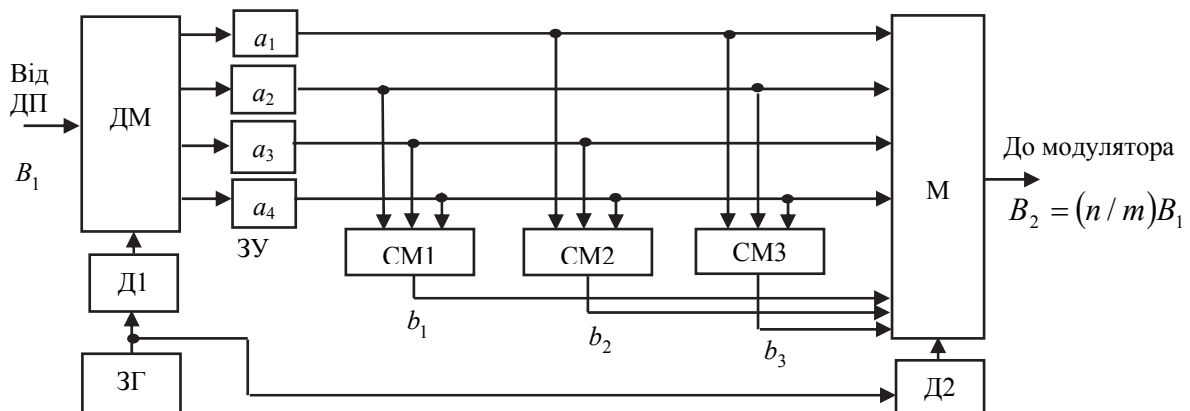


Рисунок 3.5 – Функціональна схема кодера блокового коду (7, 4)

На вхід кодера надходять інформаційні символи a_1, a_2, a_3, a_4 від джерела повідомлень. Як вхідний пристрій використовується демультиплексор ДМ, який призначений для перетворення інформаційних символів із послідовної форми в паралельну. Перевірочні символи формуються за допомогою трьох суматорів за $\text{mod } 2$ – СМ1, СМ2, СМ3, обчислення значень яких виконується за деякий проміжок часу τ . Зворотне перетворення символів одержаного КС $a_1, a_2, a_3, a_4, b_1, b_2, b_3$, тобто із паралельної форми в послідовну здійснюється мультиплексором М, призначення якого полягає в комутації семи кодових елементів і видачі їх послідовно на вхід модулятора.

Ущільнення під час інформаційних і перевірочних символів за час, що дорівнює тривалості кодової комбінації $T_{\text{КК}}$, досягається завдяки застосуванню задаючого генератора (ЗГ), частота якого

$$f_r = \text{НСК}(f_1, f_2),$$

де НСК – найменше спільне кратне; $f_1 = B_1$, $f_2 = B_1 n / m$ і, в свою чергу, B_1 – швидкість модуляції джерела повідомлень. Тактові імпульси з частотами f_1 і f_2 формуються двома дільниками частоти Д1 і Д2 з коефіцієнтами ділення $K_1 = B_1 n / m$ і $K_2 = B_1$. На виході цих дільників утворюються когерентні синхронізуючі імпульси для керування ДМ і М.

На рис. 3.6 наведено послідовність передачі елементів в процесі кодування. Тут a – формат інформаційних символів a_1, a_2, a_3, a_4 ; b – фази перетворення послідовного коду в паралельний за допомогою демультимплектора і запам'ятовуючого пристрою; v – відображено формування перевірочних символів b_1, b_2, b_3 і на діаграмі z – наведено формат КС коригуючого коду (7, 4), швидкість модуляції якого $B_2 = B_1 n / k$

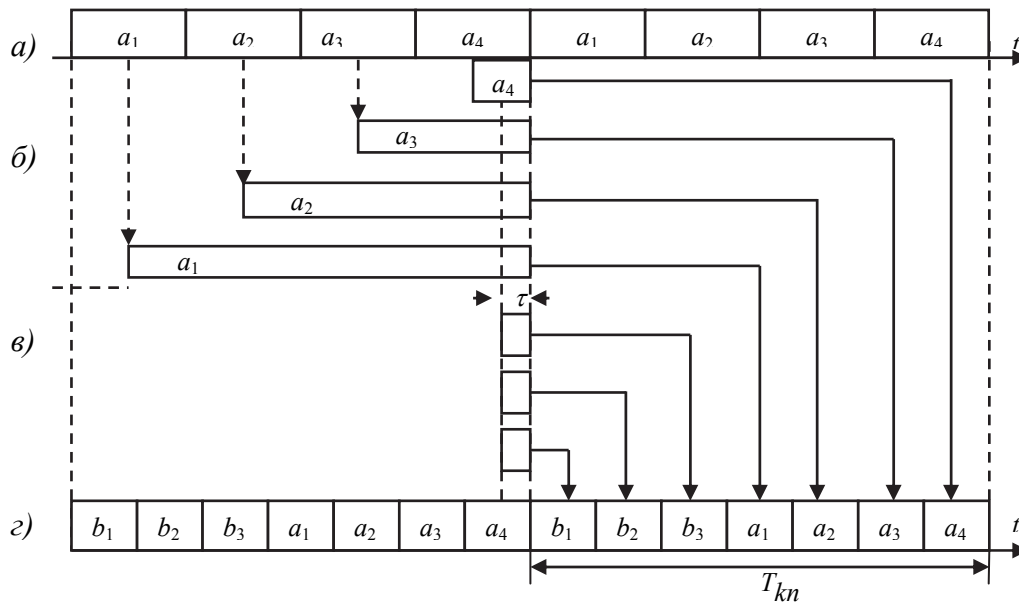


Рисунок 3.6 – Послідовність формування елементів коду (7, 4)

Побудова схеми декодера (n, k) коду. Найбільш очевидним загальним методом декодування коригуючих кодів є метод зіставлення прийнятого КС з усіма дозволеними, які зберігаються в пам'яті декодера. Якщо прийнята КК A_x збігається з однією з дозволених, тобто відстань за Хеммінгом $d(A_x, A_i) = 0$, то після вилучення перевірочних символів інформаційні надходять на вихід декодера і споживачеві надається повідомлення. Якщо ж збіг не виявлено, то обчислюється відстань за Хеммінгом з усіма дозволеними КС і на вихід декодера надходить те КС, яке найбільш близьке до прийнятого. В загальному виді це можна показати таким чином, наприклад, як для коду (7, 4).

Якщо відстань за Хеммінгом між прийнятим КС A_x і одним із дозволених A_i $d(A_x, A_i)=1$, то A_x відповідає A_i . Якщо ж $d(A_x, A_i)=2$ при $i=3, 9$, то це означає, що на інтервалі КС відбулося дві помилки, які не підлягають виправленню.

Цей метод декодування забезпечує мінімальну ймовірність в дискретних каналах з незалежними помилками, де ймовірність підвищення кратності помилки є монотонно спадною функцією. В літературі цей метод називається декодуванням за *мінімумом відстані* або *методом максимальної правдоподібності*. Такий метод знаходить більше застосування при декодування згорткових кодів за алгоритмом Вітербі. Недоліком його при декодуванні блокових кодів є те, що для навіть не дуже великого значення m треба виконувати велике число порівнянь, і тому даний метод може виявитися важко виконуваним за високих швидкостей передавання. Наприклад, при декодуванні КС короткого коду (15,11) треба виконати $2^{11} = 2048$ порівнянь. У зв'язку з зазначеним, для лінійних кодів часто застосовується більш простий метод декодування – *синдромний*.

Розглянемо принцип синдромного декодування з виправленням помилок на прикладі того самого простішого коду (7, 4). Використовуючи вираз (3.12), отримуємо систему двійкових рівностей для обчислення трибітової послідовності, яка є синдромом, або ознакою для корекції помилок:

$$\left. \begin{aligned} s_1 &= a_2 + a_3 + a_4 + b_1 \\ s_2 &= a_1 + a_3 + a_4 + b_2 \\ s_3 &= a_1 + a_2 + a_4 + b_3 \end{aligned} \right\} \text{mod } 2. \quad (3.13)$$

Для полегшення визначення значень синдрому, які відповідають різним однократним помилкам та іншим, будемо вважати, що по каналу передається нульове КС (нагадуємо, що воно завжди відноситься до дозволених для лінійних кодів). У випадку помилково прийнятих кодових комбінацій у синдромі будуть мати місце одиниці. Наприклад, при однократних помилках КС будуть мати вигляд: 1000000, 0100000, 0010000, ..., 0000001; при двократних помилках – 1100000, 1001000 і т.д. Скориставшись КС з однократними і деякими двократними помилками та системою рівностей (3.13), неважко визначити значення синдромів для деяких варіантів помилок. Результати отриманих значень синдромів при однократних і деяких багатократних помилках наведені в табл. 3.1.

Таблиця 3.1 – Таблиця синдромів коду (7, 4)

Можливі спотворені символи КС		a_1	a_2	a_3	a_4	b_1	b_2	b_3	a_1b_1	a_2b_1	$a_2a_4b_2$
Синдром	S_1	0	0	1	1	1	0	0	1	0	0
	S_2	0	1	0	1	1	0	1	0	0	0
	S_3	0	1	1	0	1	0	0	1	1	0

Із табл. 3.1 бачимо, що синдром однозначно відповідає символам тільки при однократних помилках. Так, наприклад, при спотворенні двох кодів символів a_1b_1 утворилась синдромна послідовність 111, яка відповідає синдрому неспотвореного символу a_4 . Але тому що в даному випадку вказаний інформаційний символ прийнято правильно, то, як побачимо далі, при розгляді схеми декодера він буде підданий помилковому виправленню, тобто спотворенню його декодером. Дещо краще складається обставина при декодуванні, коли спотворені символи a_2b_1 , тому що синдром 001, що утворився, відповідає спотворенню перевірного символу b_3 , який після декодування не враховується, і додаткова помилка не виникає. Такого роду багатократні помилки частіш за все виникають при дії в каналі зв'язку імпульсних завад.

Розглянемо тепер питання, пов'язані з побудовою схеми синдромного декодера коду (7, 4). Призначення декодуючого пристрою полягає у виявленні і виправленні помилок в межах коригуючої здатності коду. Процес декодування включає дії: 1) обчислення синдрому прийнятого КС; 2) дешифрування його; 3) виправлення помилки, що відбувається завжди при виконанні умови $d_0 \geq 2t_{\text{вп}} + 1$.

Практична схема декодера для коду (7, 4) наведена на рис. 3.7. Так само, як і в кодері на вході і виході декодера, використовується з тією самою метою демультиплексор (ДМ) і мультиплексор (М). Визначення синдрому виконується за допомогою багатовхідних суматорів за mod 2 – СМ1, СМ2 і СМ3. Підсумовування кодів символів КС виконується з урахуванням системи рівностей (3.12). На виходах вказаних суматорів після прийому кожного КС утворюється синдромна послідовність $s_1 s_2 s_3$. Дешифрування її, тобто визначення спотвореного символу, яка (за умови, що відбулася помилка в одному елементі) здійснюється за допомогою чотирьох дешифраторів – Д1, Д2, Д3 і Д4. Корекція помилок виконується суматорами за mod 2 СМ4, СМ5, СМ6 і СМ7, на інші входи яких подаються одиничні сигнали для інвертування спотворених кодів символів у КС.

З наведеного видно, що синдромне декодування реалізується набагато простіше, ніж декодування за методом максимальної правдоподібності.

В даному випадку не потрібно порівнювати прийняте КС з усіма дозволе-
ними, що ускладнює схему декодера за великої значності коду.

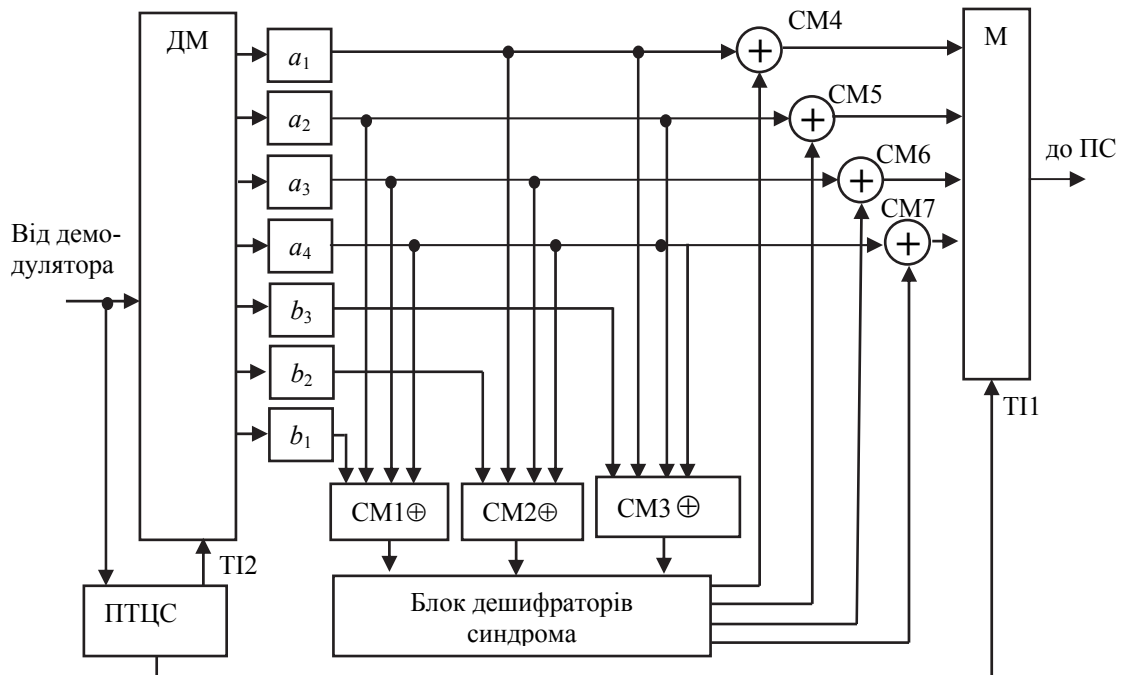


Рисунок 3.7 – Функціональна схема декодера блокового коду (7, 4)

Однак синдромне декодування не позбавлене недоліків. Основний недолік декодування за синдромом полягає в тому, що при корекції багатократних помилок вимагається великий обсяг обчислювальних ресурсів, починаючи зі значності коду $n = 15$. Наприклад, для коду (31, 21) з $d_0 = 5$, який дозволяє виправити дворазові помилки, для розпізнавання всіх з'єднань одно- і двократних помилок потрібний

$$C_{21}^1 + C_{21}^2 = 21 + 210 = 231$$

дешифратор з десятьма входами. Із зазначеного можна зробити висновок, що синдромне декодування блокових кодів доцільно застосовувати для кодів Хеммінга, коригуючих тільки однократні помилки в КС.

Для лінійних блокових кодів, крім синдромного методу декодування, який ми розглянули, існують ще й інші методи, які дозволяють в деяких випадках суттєво спростити процедуру декодування. Одним із них є декодування за стандартною таблицею.

Основні положення про композиційні і каскадні коди. Зупинимося на розгляді найпростішого двовимірного композиційного коду, який володіє високою виявляючою здатністю і тому може бути успішно застосований при передаванні цифрових даних.

Процедура декодування двовимірного композиційного коду полягає в наступному. Інформаційний блок символів записується у вигляді прямокутної таблиці з k_1 стовпцями і k_2 рядками. Символи, записані в рядки,

кодуються будь-яким кодом з параметрами (n_1, k_1, d_{01}) , а символи, що утворюють стовпці, кодуються (n_2, k_2, d_{02}) кодом. У результаті застосування таких кодувань отримується лінійний двовимірний (n, k, d_0) код, де $n = n_1 n_2$, $k = k_1 k_2$ і $d_0 = d_{01} d_{02}$.

Розглянемо найпростіший варіант двовимірного коду з перевіркою на парність за рядками і стовпцями. Блок інформаційних символів з параметрами k і $r = k_1 + k_2 + 1$ утворює кодову комбінацію двовимірного коду, яку в загальному вигляді можна подати таким чином:

a_{11}	a_{12}	a_{13}	\dots	a_{1k_2}	$b_{1(k_2+1)}$	} Горизонтальні перевірки на парність
a_{21}	a_{22}	a_{23}	\dots	a_{2k_2}	$b_{2(k_2+1)}$	
\dots	\dots	\dots	\dots	\dots	\dots	
$a_{k_1 1}$	$a_{k_1 2}$	$a_{k_1 3}$	\dots	$a_{k_1 k_2}$	$b_{k_1(k_2+1)}$	
$b_{(k_1+1)1}$	$b_{(k_1+1)2}$	$b_{(k_1+1)3}$	\dots	$b_{(k_1+1)k_2}$	$b_{(k_1+1)(k_2+1)}$	} Перевірки вер- тикальних і го- ризонтальних перевірок
} Вертикальні перевірки на парність						

Тут перевірочні символи визначаються виразами

$$b_{(k_1+1)j} = \sum_{i=1}^{k_1} a_{ij}, \quad b_{i(k_2+1)} = \sum_{j=1}^{k_2} a_{ij} \quad \text{та} \quad b_{(k_1+1)(k_2+1)} = \sum_{i=1}^{k_1} \sum_{j=1}^{k_2} a_{ij},$$

де j – номер стовпця; i – номер рядка.

Тому що складові коди володіють кодовими відстанями $d_{01} = 2$, $d_{02} = 2$, то кодова відстань композиційного коду $d_0 = 4$. Такий код дозволяє виправляти однократні помилки в кожному прийнятому блоці, а також багатократні помилки, розміщені за діагоналлю прийнятого блока. Не виявляються чотирикратні помилки, що утворюють в інформаційному блоці чотирикутник і шестикутник (показано на рис. 3.8), а також інші помилки певної конфігурації, ймовірність утворення яких надто мала.

До композиційного двовимірного коду застосуємо також і матричний метод опису. Породжуюча матриця двовимірного коду визначається як векторний добуток матриць складових кодів. Нехай їх матриці мають вигляд

$$G_{3,2}^{(1)} = G_{3,2}^{(2)} = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} A_1 \\ A_2 \end{vmatrix},$$

що відповідає найпростішим кодам $(3, 2)$ з перевіркою на парність.

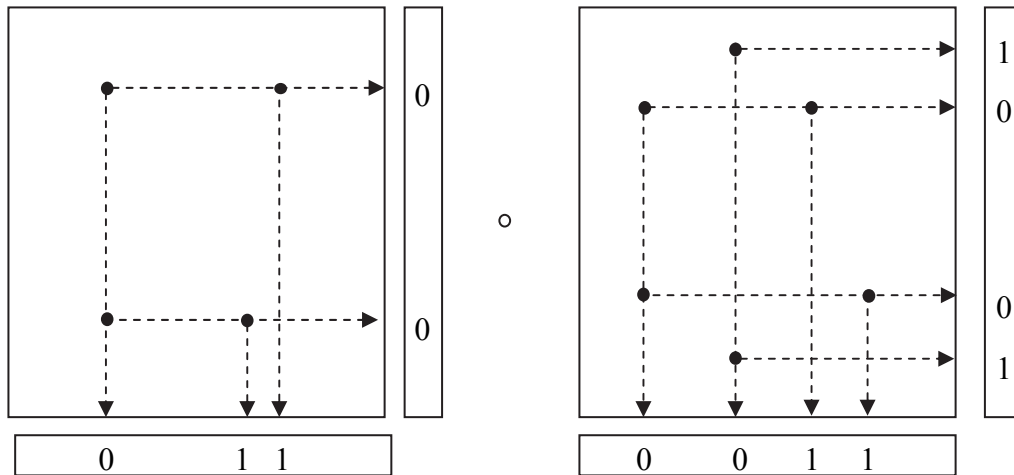


Рисунок 3.8 – Варіанти деяких малоймовірних виявлених, але не виправлених помилок

Тоді

$$G_{3,2}^{(1)} \times G_{3,2}^{(2)} = \begin{Bmatrix} A_1 \\ A_2 \end{Bmatrix} \times \begin{Bmatrix} A_1 \\ A_2 \end{Bmatrix} = \begin{Bmatrix} A_1 \times A_1 \\ A_1 \times A_2 \\ A_2 \times A_1 \\ A_2 \times A_2 \end{Bmatrix} = \begin{Bmatrix} (101) \times (101) \\ (101) \times (011) \\ (011) \times (101) \\ (011) \times (011) \end{Bmatrix} = \begin{Bmatrix} 101\ 000\ 101 \\ 011\ 000\ 011 \\ 000\ 101\ 101 \\ 000\ 011\ 011 \end{Bmatrix} = G_{9,4}.$$

Після виконання лінійних перетворень над рядками, отримаємо породжуючу матрицю коду (9, 4) з $d_0 = 4$ у приведено-ступінчатій формі

$$G_{9,4} = \begin{Bmatrix} 1000 & 10101 \\ 0100 & 10011 \\ 0010 & 01101 \\ 0001 & 01011 \end{Bmatrix}.$$

Композиційний код також може бути побудований на основі більш складних кодів. Взагалі відзначимо це на прикладі двох кодів Хеммінга (31, 26, 3). В результаті утвориться код (961, 676) з $d_0 = 3 \times 3 = 9$, який здатний виправляти помилки кратності $t_{\text{вп}} = 1, 2, 3$ і 4.

Аналогічно композиційним кодам, ідея побудови яких належить П. Елайесу, будуються послідовні каскадні коди Д. Форні. В останніх використовуються дві ступені кодування – зовнішня і внутрішня з перетворенням сигналів модулятором (М) і демодулятором (ДМ), як показано на рис. 3.9. Послідовність двійкових символів, що надходить на вхід зовнішнього кодера (ЗК) зовнішньої ступені, кодується кодом (n_1, k_1) . Внутрішній кодер (ВК) повторно кодує блоки, вважаючи $n_1 = k_2$ більш довгим кодом (n_2, k_2) . В результаті отримуємо каскадний $(n_1 \cdot n_2, k_1 \cdot k_2)$ код з $d_0 = d_1 \cdot d_2$. Декодування на приймальній стороні виконується внутрішнім

(ВнД) і зовнішнім декодером (ЗнД) в зворотному порядку з корекцією помилок на виході каналу зв'язку з завадами.

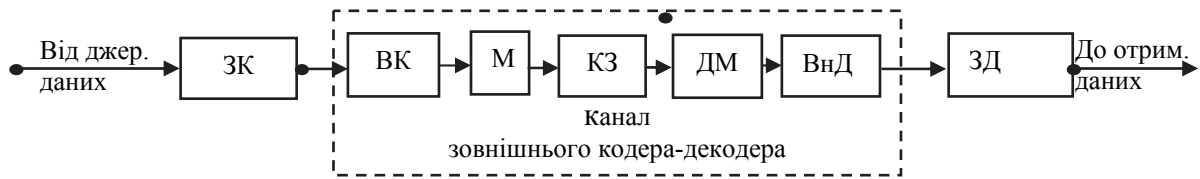


Рисунок 3.9 – Структурна схема декода послідовного складового каскадного коду

Подання кодограм у вигляді векторів n -вимірному простору припускає використання кодової відстані, що відповідає критерію максимуму правдоподібності. Проте у каналах з корельованими завадами, а також при аналізі кодів з високою основою більш доцільно користуватися кореляційним критерієм і оперувати не кодовою відстанню, а коефіцієнтом кореляції між кодограмами.

Двійкові коди для каналів з незалежними помилками. Коефіцієнт кореляції між кодограмами X_j й X_ζ

$$\rho_{j\zeta} = \sum_{v=1}^n a_{vj} b_{v\zeta}, \quad (3.14)$$

де a_j, b_ζ – символи сигнальних конструкцій. Добуток

$$a_{vj} b_{v\zeta} = \begin{cases} +1 & \text{за } a_{vj} = b_{v\zeta}, \\ -1 & \text{за } a_{vj} \neq b_{v\zeta}. \end{cases} \quad (3.15)$$

У якості переданої кодограми X_j фіксується та комбінація, в якій $\rho_{jj} > \rho_{j\zeta}$ для всіх $j \neq \zeta$. Тому що X_j відрізняється від $C_n^1, C_n^2, C_n^3, \dots$ кодограм алфавіту відповідно в 1, 2, 3, ... розрядах, то величина

$$\Delta\rho = \rho_{jj} - \rho_{j\zeta}, \quad (3.16)$$

яка характеризує відстань між кодограмами, завжди парна й $\Delta\rho_{\min} = 2$. Кодограми, в яких значення $\rho_{j\zeta}$ найбільш близьке до ρ_{jj} , будемо називати найближчими й позначати для них коефіцієнт кореляції через $\rho_{j\delta}$. Тоді здатність коду виправляти й виявляти помилки характеризується значенням

$$\Delta\rho_{\min} = \rho_{jj} - \rho_{j\delta} \quad (3.17)$$

Приклад 2. Нехай алфавіт джерела містить 8 повідомлень, відображуваних 3-значними двійковими числами: I - 000, II - 001, III - 010, IV - 011, V - 100, VI - 101, VII - 110, VIII - 111, і нехай по каналу без завад передана кодограма 000. Коефіцієнти кореляції, обчислені на прийманій стороні,

$$\rho_{11} = +3, \quad \rho_{12} = \rho_{13} = \rho_{14} = +1; \quad \rho_{15} = \rho_{16} = \rho_{17} = -1; \quad \rho_{18} = -3.$$

Отже, буде зареєстрована кодограма 000, а величина $\Delta\rho_{\min} = 2$.

Зазначимо, що правила перевірки на парність еквівалентні обчисленню коефіцієнта $\rho_{j\zeta}$. Отже, будь-яка одинична помилка зменшує значення

ρ_{jj} на дві одиниці, а $\rho_{j\delta}$ збільшує на дві одиниці, що зменшує відстань $\Delta\rho_{\min}$. Для виправлення одиничної помилки необхідно, щоб $\rho_{jj} - 2 > \rho_{j\delta} + 2$, звідки відповідно до формули (3.17) величина $\Delta\rho_{\min} = 6$. Для корекції r помилок необхідно мати

$$\Delta\rho_{\min} = 4r + 2.$$

Це ілюструється рис. 3.10. У загальному випадку для виправлення r помилок і виявлення $s = r + \Delta$ помилок необхідно, щоб

$$\Delta\rho_{\min} = 2(2r + \Delta + 1).$$

Для визначення значності коду n можна скористатися методикою А.А. Харкевича. Якщо $\Delta\rho_{\min} = 2\mu$, де $\mu = 3, 5, 7, \dots$, то число інформаційних символів

$$m \leq n - \log_2 \sum_{v=0}^{\alpha} C_n^v, \quad (3.18)$$

де параметр $\alpha = \frac{\mu - 1}{2}$.

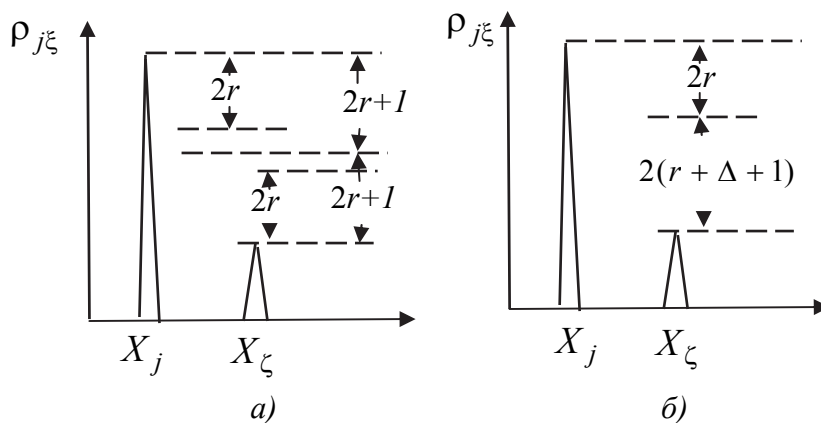


Рисунок 3.10 – Кореляційне трактування виправлення помилок

Якщо $\Delta\rho_{\min} = 2\mu + 2$, то обчислення здійснюються відповідно до виразу (3.18), а потім значення n збільшується на 1.

Приклад 3. Побудуємо код з $k = 2$, що виправляє помилки кратності $r \leq 2$ й виявляє помилки кратності $s = 3$. У нашому випадку $\Delta = 1$, $\Delta\rho_{\min} = 12$, $\mu = 5$, $v = 2$, $n = 8$. Тоді остаточно $n = 9$, отже, необхідно використовувати (9, 2)-код.

Розглянемо кореляційні властивості циклічного коду. При кореляційній обробці прийнята комбінація $Z_j = X_j \oplus U_{\text{ш}}$ помножується на свій

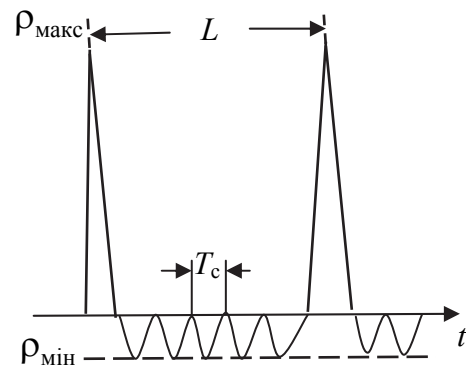


Рисунок 3.11 – До визначення коефіцієнта ρ

еталон X_{e_j} і на інші $2^k - 1$ еталонів робочих кодограм. Циклічно зсуваючи кодограму на задане число тактів T_c , перемножуючи символи й підсумовуючи ці добутки в межах кодограми, отримаємо (рис. 3.11)

$$\rho_{1\text{макс}} = 2^l - 1;$$

$$\rho_{2\text{макс}} = 2^l - 1;$$

$$\rho_{\text{мін}} = -1.$$

Величина $\rho_{\text{макс}}$ відповідає часовому зсуву $\tau = 0$, причому значення $\rho_{2\text{макс}}$ отримується при незвідних поліномах $g(x)$ і $h(x)$, а значення $\rho_{1\text{макс}}$ – при $g(x)$ незвідному й $h(x)$ звідному поліномах. Одинична помилка зменшує $\rho_{\text{макс}}$ на дві одиниці і змінює (зменшує або збільшує при даному τ) $\rho_{\text{мін}}$, тому в найгіршому разі $\Delta\rho_{\text{мін}} = 2^t$ або 2^k й зменшується на 4 одиниці.

Приклад 4. Задано циклічний код з незвідним поліномом $g(x) = 1011$, що належить показнику $n = 7$. Поліном $h(x) = 11101 = (11)(1011)$ – звідний й, отже, $\rho_{\text{макс}} = 7$, $\rho_{\text{мін}} = -1$, $r = 1$.

Двійкові коди для каналів зі стиранням помилок. У випадку каналу зі стиранням символів коефіцієнт кореляції між кодограмами

$$\rho_{j,\zeta} = \sum_{v \neq i \neq t}^n a_{i,j} b_{i,\zeta} + b_{v,\zeta} \delta_{v,j} + a_{t,j} \delta_{t,\zeta}, \quad (3.19)$$

де символ стирання δ задовольняє умові $\delta a_{i,j} = \delta b_{v,\zeta} = 0$. Однократне стирання зменшує $\rho_{j,j}$ на одиницю й збільшує $\rho_{j,\delta}$ на одиницю. Тому для виправлення r помилок, виявлення $s = r + \Delta$ помилок і відновлення ε стертих символів необхідно, щоб

$$\Delta\rho_{\text{мін}} = 2(2r + \Delta + \varepsilon + 1).$$

Коди з основою $a > 2$. При $a > 2$ завада може змінювати значення інформативного параметра на q рівнів, де $q = 1, 2, \dots, m - 1$. Величину q будемо називати показником складності помилки. Для визначення коефіцієнта $\rho_{j,\zeta}$ код необхідно записувати у формі, що максимально забезпечує рівномірний розподіл кодограм із біполярними символами за величиною енергії. Наприклад, при $m = 3$ і $m = 4$ можливі кодограми будуть $(3, -1, 1)$ і $(-3, 1, -1, 3)$. При цьому коефіцієнт

$$\rho_{j\zeta} = \sum_{v=1}^n a_{vj} b_{v\zeta}.$$

Приклад 5. Кодограми коду з параметрами $m = 3$ і $n = 3$ мають вигляд: 1 – $(3, 3, 3)$; 2 – $(3, 3, 1)$; 3 – $(3, 1, 3)$; 4 – $(1, 3, 3)$; 5 – $(3, 3, -1)$; 6 – $(3, -1, 3)$; 7 – $(-1, 3, 3)$; 8 – $(3, 1, 1)$; 9 – $(1, 3, 1)$; 10 – $(1, 1, 3)$; 11 – $(3, -1, -1)$; 12 – $(-1, 3, -1)$; 13 – $(-1, -1, 3)$; 14 – $(3, 1, -1)$; 15 – $(1, 3, -1)$; 16 – $(1, -1, 3)$; 17 – $(3, -1, 1)$; 18 – $(-1, 3, 1)$; 19 – $(-1, 1, 3)$; 20 – $(1, 1, 1)$;

21 – (1, 1, -1); 22 – (1, -1, 1); 23 – (-1, 1, 1); 24 – (1, -1, -1); 25 – (-1, 1, -1); 26 – (-1, -1, 1); 27 – (-1, -1, -1). Тоді коефіцієнти кореляції будуть: $\rho_{1,1} = 27$; $\rho_{2,2} = \rho_{3,3} = \dots = \rho_{7,7} = 19$; $\rho_{8,8} = \rho_{9,9} = \dots = \rho_{19,19} = 11$; $\rho_{20,20} = \rho_{21,21} = \dots = \rho_{27,27} = 3$; $\rho_{1,2} = \rho_{1,3} = \rho_{1,4} = 21$; $\rho_{1,5} = \rho_{1,6} = \dots = \rho_{1,10} = 15$; $\rho_{1,11} = \rho_{1,12} = \dots = \rho_{1,13} = \rho_{1,21} = \rho_{1,22} = \rho_{1,23} = 3$; $\rho_{1,14} = \rho_{1,15} = \dots = \rho_{1,20} = 9$; $\rho_{1,24} = \rho_{1,25} = \dots = \rho_{1,26} = -3$; $\rho_{1,27} = -9$.

Величина $\Delta\rho$ завжди парна. Тому для будь-яких m і q отримаємо

$$\Delta\rho_{\min} = 2q(m-1)(2r + \Delta + \varepsilon + 1)$$

3.3. Поля Галуа. Основи синтезу циклічних кодів

Подальшим кроком на шляху спрощення пристроїв кодування та в деяких випадках декодування є застосування циклічних кодів (ЦК), які дозволяють реалізувати зв'язок зі значно більшою якістю. Для поглибленого розуміння властивостей ЦК, які виправляють неодноразові помилки, і правил їх побудови необхідно познайомитися з низкою положень алгебри кінцевих полів Галуа, об'єктами вивчення якої є *множини*, *групи* і *поля*. Ці питання, на жаль, не входять в програму курсу математики вузів зв'язку і тому, щоб надмірно не завантажувати читача, ми наводимо лише тільки ті відомості, без яких не можна зрозуміти матеріал, пов'язаний з побудовою кодеків для виправлення багаторазових помилок. Виклад цього матеріалу супроводжується необхідним числом прикладів, що, мабуть, надасть можливість легше розібратися в питаннях побудови досить складних кодів, які є узагальненням найбільш простих кодів Хеммінга – кодів Боуза-Чоудхурі-Хоквінгема і Ріда-Соломона, що володіють високою коригувальною здатністю.

Множини, групи, циклічні підгрупи. Множини відносяться до категорії найбільш загальних понять математики та вводяться аксіоматично. Спрощено під *множиною* розуміють сукупність елементів, які володіють деякими властивостями і знаходяться в певних відносинах між собою або з елементами інших множин. Множина задана або визначена, якщо про кожен елемент можна сказати, належить він цій множині чи ні. Найпростіший спосіб завдання множини полягає в перерахуванні всіх елементів, які належать до неї.

Твердження, що множина M складається з a_1, a_2, a_3 елементів і a_4 умовно записується як $M = (a_1, a_2, a_3, a_4)$, а записи $a_1 \in M$ або $a_5 \notin M$, означають належність чи неналежність елементів a_1 і a_5 множині M . *Порядок* множини M визначається кількістю її елементів. У свою чергу, можна розглядати множини множин, тобто розбиття множини M на ряд підмножин M_1, M_2, \dots .

Над елементами множини можуть виконуватися деякі операції, під якими мається на увазі однозначна відповідність між елементами даної множини. Основними операціями є додавання і множення. Операції віднімання і ділення не розглядаються, так як вони є зворотними відповідно по відношенню до додавання і множення. Символічно ці операції зазвичай позначають зірочкою $*$.

Важливою алгебраїчної системою, широко використовуваною в теорії коригувальних кодів, є поняття *групи*.

Визначення 1. Групою D називається множина елементів довільної природи, для якої визначена одна операція (додавання або множення) і виконуються наступні аксіоми:

A1. Для будь-яких двох елементів $a, b \in M$ однозначно визначений елемент $c \in M$ такий, що $a * b = c$ (аксіома замкнутості).

A2. Для будь-якого елемента $a \in M$ існує *нейтральний* елемент $d \in M$ такий, що виконується співвідношення $a * d = a$ (при додаванні $a + d = a$, де $d = 0$ і при множенні $a \times d = a$, де $d = 1$).

A3. Для будь-якого елемента $a \in M$ існує *зворотний* елемент $a^{-1} \in M$, такий, що виконується співвідношення $a * a^{-1} = e$ ($a \neq 0$) (при додаванні $a + a^{-1} = 0$ ($e = 0$), при множенні $a \times a^{-1} = 1$ ($e = 1$)).

A4. Для будь-яких трьох елементів $a, b, c \in M$ виконується співвідношення $(a * b) * c = a * (b * c)$ (аксіома асоціативності).

A5. Додатково для групи може виконуватися аксіома *комутативності*, яка полягає в тому, що $a * b = b * a$.

Групи, в яких виконуються операції додавання або множення, називаються відповідно *адитивними* або *мультиплікативними*. Число елементів, що утворюють групу, називається *порядком*.

У зв'язку з тим, що в групі повинна виконуватися умова замкнутості при додаванні або множенні елементів, то ці операції у звичайному розумінні стають неприйнятними через те, що число елементів груп не буде постійним. Умові замкнутості задовольняють операції так званого *символічного* додавання і множення по модулю деякого числа v . Результатами символічних операцій над елементами a і b є залишки r_1 і r_2 від ділення суми $a + b$ або добутку $a \times b$ в звичайному розумінні на модуль числа v , тобто

$$a + b = c; \quad \frac{c}{v} = q + \frac{r_1}{v}; \quad (a + b) \equiv r_1 \pmod{v}$$

і

$$a \times b = d; \quad \frac{d}{v} = s + \frac{r_2}{v}; \quad (a \times b) \equiv r_2 \pmod{v},$$

де q і s – цілі частини від ділення на v .

Результати наведених операцій називають лишками, а знак рівності у вигляді трьох горизонтальних ліній підкреслює незвичайність цих операцій. Згідно термінології, символ \equiv читається «порівняно з».

Приклад 6. Виконаємо операції символічного додавання чисел 2 і 1 і множення чисел 2 і 2 по mod 3, які є елементами групи $D = (0, 1, 2)$.

Виконуючи ці операції, отримуємо:

$$2 + 1 = 3, \text{ а } 3/3 = 1 + 0/3, \text{ поэтому } (2 + 1) \equiv 0 \pmod{3} \text{ і}$$

$$2 \times 2 = 4, \text{ а } 4/3 = 1 + 1/3 \quad \rightarrow \quad (2 \times 2) \equiv 1 \pmod{3}$$

Приклад 7. Розглянемо множину M порядку 5, тобто яка складається з п'яти елементів $M = (0, 1, 2, 3, 4)$, і перевіримо, чи задовольняє вона основним аксіомам $A1, A2$ і $A3$ за умови, що символічні операції виконуються за модулем числа 5.

Для наочності нижче наведені таблиці додавання (табл. 3.2) і множення (табл. 3.3) елементів множини M за mod 5.

Таблиця 3.2. – Додавання за модулем 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблиця 3.3. – Множення за модулем 5

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

З наведених таблиць видно, що елементи множини M задовольняють аксіомам $A1, A2$ і $A3$. Дійсно, крім цього, всі елементи множини M при операції додавання мають зворотні елементи $0 \leftrightarrow 0, 1 \leftrightarrow 4, 2 \leftrightarrow 3$, і навпаки, тому що 0 є нейтральним елементом щодо операції додавання. При множенні зворотними елементами – $1 \leftrightarrow 1, 2 \leftrightarrow 3, 4 \leftrightarrow 4$, так як 1 є нейтральним елементом щодо операції множення. Виконання умов аксіом $A2$ (асоціативності) і $A5$ (комутативності) очевидно. Отже, на підставі зазначеного можна зробити висновок, що множина M утворює адитивну групу $D_1 = [(0, 1, 2, 3, 4), +]$ і мультиплікативну групу $D_2 = [(0, 1, 2, 3, 4), \times]$ з урахуванням вибору виду символічної операції за модулем $v = 5$.

Приклад 8. Перевіримо, чи утворює множина $M = (0, 1, 2, 3)$ групи щодо операцій додавання і множення за модулем 4?

Для відповіді на поставлене питання складаємо таблиці 3.4 та 3.5 аналогічно попередньому прикладу.

Таблиця 3.4. – Додавання за модулем 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Таблиця 3.5. – Множення за модулем 5

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

У цьому прикладі множина M утворює тільки адитивну групу, так як кожному елементу відповідають нейтральні і зворотні елементи і виконуються умови аксіом $A1$, $A4$ і $A5$. Однак ця ж множина не утворює групу відносно операції множення, тобто мультиплікативну групу тому, що рівняння $2 \times a \equiv 1 \pmod{4}$ не має рішення, тому що $(2 \times 1 \equiv 2, 2 \times 2 \equiv 0, 2 \times 3 \equiv 2) \pmod{4}$, що означає відсутність зворотного елемента у a , який дорівнює двом. Множина елементів утворює групу відносно операції множення тоді, коли модуль v – *просте число*.

При розгляданні групи D деяких елементів природно виникає питання, який полягає в наступному. Чи можна отримати підгрупу H , яка задовольняє обраній раніше груповій операції, взявши не всі елементи, а тільки деякі з них? Відповідь на це питання не завжди може бути позитивною. Підмножина H групи D тоді є підгрупою групи D , коли символічні операції над елементами з H є також і над елементами групи D . Прикладом цього може служити наступне: $H = [(1, 3, 2, 4), \times]$ є підгрупою групи $D = [(0, 1, 2, 3, 4), \times]$, в чому неважко переконатися.

Важливе місце при вивченні ЦК має поняття циклічної підгрупи, яке є досить корисним при розгляді алгебраїчних методів декодування ЦК.

Визначення 2. Підгрупа, утворена степенями будь-якого одного елемента деякої групи D за модулем v , крім $a = 0$ або 1 , називається *циклічною*, а елемент a – утворюючим або примітивним.

Згідно аксіомі замкнутості $A1$, $a \times a = a^2 \in D$, $a^2 \times a = a^3 \in D$, ..., $a^{l-1} \times a = a^l \in D$. Але так як D – кінцева група, то повинні існувати такі показники l і s , що $a^l = a^s$. Таким чином послідовність степенів елемента a за \pmod{v}

$$a^0, a^1, a^2, \dots, a^{l-1}, a^l, a^{l+1}, \dots$$

представляє періодичну послідовність всіх елементів підгрупи H , за винятком нульового та одиничного елементів, періоди яких дорівнюють l .

Приклад 9. Для заданої групи $D = [(0, 1, 2, 3, 4), \times]$ обчислимо послідовність порівнянь степенів третього елемента за $\pmod{5}$.

$$2^0 = 1 \equiv 1, \quad 2^1 = 2 \equiv 2, \quad 2^2 = 4 \equiv 4, \quad 2^3 = 8 \equiv 3,$$

$$2^4 = 16 \equiv 1, \quad 2^5 = 32 \equiv 2, \quad 2^6 = 64 \equiv 4, \quad 2^7 = 128 \equiv 3.$$

З наведеного видно, що множина степенів двійки за $\pmod{5}$ утворює циклічну підгрупу $H_1 = [(1, 2, 3, 4), \times]$ групи D . Аналогічно можна переконатися в тому, що безліч степенів трійки $3^0, 3^1, 3^2, 3^3, 3^4, 3^5, \dots$ за $\pmod{5}$ утворюють ту ж циклічну підгрупу H_1 .

Деякі відомості про кінцеві поля Галуа. Подальше розглядання проблематики теорії і практики кодування і декодування ЦК вимагає знайомства з елементами алгебраїчної структури полів Галуа.

Визначення 3. Полем F називається множина елементів, для яких визначені дві операції – *додавання* і *множення*, виконуються аксіоми $A1$,

A2, A3, A4, A5, а також і умова дистрибутивності, тобто для будь-яких трьох елементів a, b, c мають бути справедливі співвідношення

$$a \times (b + c) = a \times b + a \times c \text{ і } (b + c) \times a = b \times a + c \times a.$$

Поле, як випливає з аксіоми A3, не може містити менше двох елементів, оскільки в ньому мають бути, принаймні, нейтральний елемент 0 – щодо операції додавання і 1 – щодо операції множення. Аналогічно з групами, число елементів у полі так само, як і у групі, називається *порядком* поля. Поле $F = [(0, 1, 2, \dots, v-1), +, \times]$, порядок якого скінченний, називається *кінцевим*. Число v називається *порядком поля* і, як для мультиплікативної групи, обов'язково має бути простим числом. Якщо число елементів полів збігається з порядком, то такі поля називаються *простими*, прикладами яких є

$$F_1 = [(0, 1), +, \times] \ v = 2, \quad F_2 = [(0, 1, 2), +, \times] \ v = 3 \quad \text{і} \quad F_3 = [(0, 1, 2, 3, 4, 5, 6), +, \times] \\ v = 7.$$

У літературі прості поля позначають $GF(v)$, де GF – скорочення слів Galois Field – поля Галуа.

Елементами полів Галуа можуть бути не тільки числа, але, наприклад, многочлени та інші математичні поняття. Якщо елементами поля є многочлени з коефіцієнтами з простого поля порядку v , то таке поле містить число елементів більше v , в цьому випадку його називають *розширеним полем* і позначають такі поля $GF(v^m)$, де v^m називається *порядком розширеного поля*. Тут доречно звернутися до наступної теореми.

Теорема 3. Для кожного простого числа v і довільного цілого $m \geq 1$ існує єдине кінцеве поле $GF(v^m)$.

Далі нас будуть цікавити тільки двійкові розширені поля $GF(2^m)$. Завдання таких полів пов'язане з поняттям незвідних многочленів ступеня m з коефіцієнтами з простого поля $GF(2)$.

Визначення 4. Двійковий многочлен називається незвідним, якщо він не має дільників серед многочленів з коефіцієнтами з поля $GF(2)$, які відрізняються від одиниці і самого себе.

Прикладами деяких незвідних многочленів є:

$$G_1(x) = x + 1, \quad G_2(x) = x^2 + x + 1, \quad G_3(x) = x^3 + x + 1 \quad \text{і} \quad G_4(x) = x^3 + x^2 + 1.$$

Многочлен $G_5(x) = x^2 + x$ не є незвідним, так як його можна розкласти на співмножники $x + 1$ і x .

Для виконання умови замкнутості при множенні двох елементів розширеного поля за аналогією з діями над елементами простого поля використовується символічне множення двох многочленів за модулем третього многочлена, який визначає розширене поле $GF(2^m)$. Результатом такого множення є залишок, отриманий від ділення добутку многочленів у звичайному розумінні, на заданий многочлен, який в даному випадку є модулем. Зазначене можна пояснити наступним чином. Якщо $A(x)$ і $B(x)$ –

многочлени, що відповідають елементам деякого розширеного поля, а $G(x)$ – многочлен, що визначає дане поле, за модулем якого виконується множення, то

$$A(x) \times B(x) = C(x), \quad C(x)/G(x) = Q(x) + R(x)/G(x),$$

де $Q(x)$ – частка, а $R(x)$ – залишок від ділення $C(x)$ на $G(x)$, що і є добутком $A(x)$ і $B(x)$ за модулем $G(x)$. Коротко це позначають записом

$$A(x) \times B(x) \equiv R(x) \pmod{G(x), 2},$$

яка читається так: добуток многочленів $A(x)$ і $B(x)$ порівняно з многочленом $R(x)$ за подвійним модулем $G(x)$ і 2 або простіше: добутком многочленів $A(x)$ і $B(x)$ за подвійним модулем $G(x)$ і 2 є многочлен $R(x)$.

Наведемо ще один приклад, що стосується операції порівняння. Два многочлени $A_1(x)$ і $A_2(x)$, що дають однакові залишки при діленні на $G(x)$, називаються порівнянними за модулем $G(x)$, що коротко фіксується записом

$$A_1(x) \equiv A_2(x) \pmod{G(x)}.$$

Додавання двох або більше многочленів виконується звичайним чином, тобто складаються їхні коефіцієнти при однакових степенях за $\text{mod } 2$. Таким чином, при виконанні операцій множення і додавання досягаються умови замкнутості над елементами розширеного поля.

Додавання таблиць полів $\text{GF}(2^m)$, коли m велике, є трудомісткою задачею. Уникнути труднощів при побудові таких полів можна, якщо врахувати, що елементи кінцевого поля мають властивості, які властиві мультиплікативної групі, тобто замкнутості. Міркування, аналогічні проведеним для циклічної підгрупи, показують, що сукупність всіх ненульових елементів розширеного двійкового поля $\text{GF}(2^m)$ можна визначити як повну систему відрахувань ступенів деякого *утворюючого (примітивного)* елемента a за модулем *примітивного* многочлена $G(x)$. Примітивний многочлен обов'язково є незвідним, проте не кожен незвідний многочлен може бути примітивним для заданого поля.

Визначення 5. Незвідний многочлен $G(x)$ називається *примітивним* ступеня q , якщо він входить у розкладання двочлена $x^q + 1$ і не входить в розкладання двочленів $x^s + 1$, степінь якого $s < q$.

Для пояснення наведемо розкладання двочленів $x^i + 1$ для $1 < i \leq 15$:

$$x^2 + 1 = (x + 1)(x + 1);$$

$$m = 2 \quad x^{2^2-1} + 1 = x^3 + 1 = (x + 1)(x^2 + x + 1),$$

$$x^4 + 1 = (x^2 + 1)(x^2 + 1),$$

$$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1),$$

$$x^6 + 1 = (x^3 + 1)(x^3 + 1);$$

$$\begin{aligned}
m = 3 \quad x^{2^3-1} + 1 = x^7 + 1 &= (x+1)(x^3+x+1)(x^3+x^2+1), \\
x^8 + 1 &= (x^4+1)(x^4+1), \\
x^9 + 1 &= (x+1)(x^2+x+1)(x^6+x^3+1), \\
x^{10} + 1 &= (x^5+1)(x^5+1), \\
x^{11} + 1 &= (x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1), \\
x^{12} + 1 &= (x^6+1)(x^6+1), \\
x^{13} + 1 &= (x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1), \\
x^{14} + 1 &= (x^7+1)(x^7+1);
\end{aligned}$$

$$m = 4 \quad x^{2^4-1} + 1 = x^{15} + 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

З наведених розкладань видно, що двочлену $x^{15} + 1$ ступеня $m = 4$ відповідає тільки два примітивних многочлена, а саме $x^4 + x + 1$ та $x^4 + x^3 + 1$, оскільки решта раніше входили в розкладання двочленів $x^2 + 1$, $x^3 + 1$ і $x^5 + 1$.

При розгляданні розширених полів Галуа прийнято, і це вельми зручно, використовувати іншу символіку для ідентифікації елементів поля. Часто замість фіктивної змінної x використовується буква грецького алфавіту α .

Теорема 4. Кінцеве поле порядку v^m містить примітивний елемент α , степені якого пробігають всі ненульові елементи поля $GF(v^m)$.

Елементи кінцевого розширеного поля $GF(2^3)$, представлені у вигляді многочленів, є класами лишків за подвійним модулем примітивного многочлена $G(\alpha)$ і 2

$$f_i(\alpha) \equiv \alpha^i \pmod{[G(\alpha), 2]}.$$

Розглянемо три способи представлення елементів розширеного поля $GF(2^3)$ з породжуючим многочленом $G_1(\alpha) = \alpha^3 + \alpha + 1$, який є примітивним степені $m = 3$. Елементи такого поля без нульового у двійковому вигляді наведено в табл. 3.6. Визначаються вони пристроєм, схема якого показана на рис. 3.12.

Таблиця 3.6. – Перелік ненульових елементів розширеного поля GF

У вигляді степені породжуючого елемента	У вигляді многочленів $f_i(\alpha)$	У вигляді двійкових кодів символів
α	α	010
α^2	α^2	001
α^3	$\alpha + 1$	110
α^4	$\alpha^2 + \alpha$	011
α^5	$\alpha^2 + \alpha + 1$	111
α^6	$\alpha^2 + 1$	101
α^7	1	100
α^8	α	010

У схемі (рис. 3.12) використовується послідовний регістр зі зворотним зв'язком, а також двійковий суматор, включений між осередками пам'яті відповідно до примітивного многочлена третьої степені $\alpha^3 + \alpha + 1$. Легко переконатись, що послідовність елементів поля (табл. 3.6), яка подана у вигляді двійкових кодових символів, утворюється даною схемою при

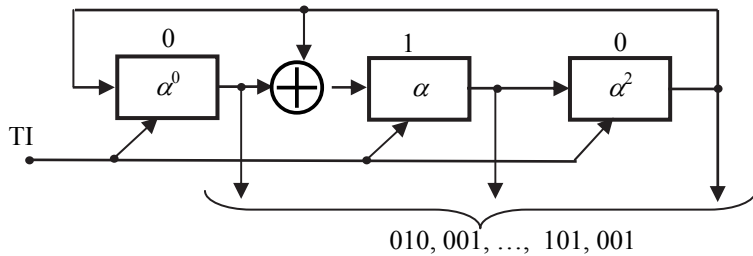


Рисунок 3.12 – Схема генератора елементів розширеного поля $GF(2^3)$ у двійковому поданні

подачі тактових імпульсів, якщо початковий стан регістра 010. Користуючись степенним поданням елементів поля, можна легко переконатися в тому, що кожен елемент $GF(2^3)$ має зворотний елемент, наприклад, α^6 має зворотний елемент α , так як $\alpha \times \alpha^6 = \alpha^7 \equiv 1 \pmod{(\alpha^3 + \alpha + 1)}$. Таким чином, всі ненульові елементи циклічної підгрупи представлені у вигляді степенів, утворюють поле порядку $2^3 - 1$, так як для будь-якого i виконується операція порівняння

$$\alpha^i \times \alpha^{2^3-1-i} \equiv 1 \pmod{G(\alpha)},$$

де $i = 1, 2$ і 3 .

Якщо ж для цієї мети скористатися іншим примітивним многочленом третьої степені $G_2(\alpha) = \alpha^3 + \alpha^2 + 1$, який пов'язаний із $G_1(\alpha) = \alpha^3 + \alpha + 1$ співвідношенням

$$G_1(\alpha) = \alpha^r \times G_2(1/\alpha), \quad (3.20)$$

де r – степінь $G_2(\alpha)$, то отримаємо елементи поля F_2 : $\alpha \rightarrow 010$, $\alpha^2 \rightarrow 100$, $\alpha^3 \rightarrow 101$, $\alpha^4 \rightarrow 111$, $\alpha^5 \rightarrow 001$, $\alpha^6 \rightarrow 110$, $\alpha^7 \rightarrow 001$, $\alpha^8 \rightarrow 010$, В даному випадку поле F_2 є ізоморфним (подібним) полю F_1 . Такі поля відрізняються тільки порядком розташування елементів. Примітивні многочлени, пов'язані співвідношенням (3.20), називаються *взаємними*, або *зворотними*.

Тепер, в якості прикладу, складемо таблицю символічного множення у двох поданнях елементів найпростішого розширеного поля $GF(2^2)$ з породжуючим многочленом $G(\alpha) = \alpha^2 + \alpha + 1$. Ненульовими елементами поля, представленими у вигляді многочленів, є α , $\alpha + 1$ і 1 , а у вигляді двійкових символів – 01 , 11 і 10 . Добуток кожного елемента з кожним за $\text{Modd}[(\alpha^2 + \alpha + 1), 2]$, наведені в табл. 3.7 та 3.8.

Таблиця 3.7 – Таблиця множення елементів поля $GF(2^2)$, поданих у вигляді многочленів

\times	α	$\alpha + 1$	1
α	$\alpha + 1$	1	α
$\alpha + 1$	1	α	$\alpha + 1$
1	α	$\alpha + 1$	1

Таблиця 3.8 – Таблиця множення елементів поля $GF(2^2)$ у двійковому поданні

\times	01	11	10
01	11	10	01
11	10	01	11
10	01	11	10

З наведених табл. 3.7 і 3.8 видно, що елементу поля $GF(2^2)$ $\alpha^3 \equiv 1$ або 10 відповідає зворотний елемент, яким є він же, а елементу α відповідає зворотний елемент $\alpha + 1$ і навпаки, так як

$$\alpha \times (\alpha + 1) = \alpha^2 + \alpha \equiv 1 \pmod{[(\alpha^2 + \alpha + 1), 2]}.$$

Визначимо тепер для порівняння лишок добутку елементів α і $\alpha + 1$ за модулем многочлена, який не є незвідним. Таким найпростішим многочленом є $T(\alpha) = (\alpha + 1)(\alpha + 1) = \alpha^2 + 1$. Перевіримо наявність зворотного елемента у α і $\alpha + 1$

$$\alpha \times (\alpha + 1) = \alpha^2 + \alpha \equiv \alpha + 1 \pmod{[(\alpha^2 + 1), 2]},$$

що незрівнянно з одиницею. Отже, ці елементи в системі лишків за $\text{Modd}[(\alpha^2 + 1), 2]$ не утворюють розширене поле $GF(2^2)$.

Повернемося ще до табл. 3.2.

Тут на закінчення залишається перевірити чи породжують всі ненульові елементи поля $GF(2^4)$ незвідний многочлен $G(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$, що входить до розкладання двочлена $\alpha^{15} + 1$ степені $m = 4$?

$$\left. \begin{array}{l} \alpha \equiv \alpha \quad 0100 \\ \alpha^2 \equiv \alpha^2 \quad 0010 \\ \alpha^3 \equiv \alpha^3 \quad 0001 \\ \alpha^4 \equiv \alpha^3 + \alpha^2 + \alpha + 1 \quad 1111 \\ \alpha^5 \equiv 1 \quad 1000 \\ \alpha^6 \equiv \alpha \quad 0100 \end{array} \right\} \pmod{(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)}$$

Як бачимо з наведеного вище, отримана множина елементів не утворює всі ненульові елементи поля $GF(2^4)$, так як період проходження їх дорівнює 5, що менше $2^4 - 1$. Причиною цього є те, що незвідний многочлен $G(\alpha)$ не є примітивним степені $m = 4$, оскільки він вперше входить у розкладання двочлена $\alpha^5 + 1$.

Алгебраїчна структура кінцевих полів Галуа. Для розуміння властивостей циклічних кодів, правил їх побудови і особливо методів декодування кодів БЧХ необхідно познайомитися з низкою положень, що стосу-

ються алгебри двійкових многочленів. Обговорення структури кінцевих двійкових полів почнемо з розгляду відомої теореми Ферма.

Теорема 5. Будь-який елемент кінцевого поля $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^m-1}$ порядку $2^m - 1$ є коренем рівняння

$$(x^{2^m-1} + 1) \equiv 0 \pmod{[G(\alpha), 2]}, \quad (3.21)$$

де $G(\alpha)$ – примітивний многочлен кінцевого поля.

Дійсно, ця теорема нагадує відоме положення з курсу шкільної математики про те, що алгебраїчне рівняння $f(x) = 0$ має рівно стільки коренів, яка його степінь.

Для елементів кінцевого двійкового поля справедлива теорема Безу, формулювання якої може бути зведена до наступного:

Теорема 6. Якщо многочлен $F(x) \equiv 0 \pmod{[G(x), 2]}$ має своїми коренями елементи кінцевого поля $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^m-1}$, то многочлен $F(x)$ ділиться без залишку на двочлен $(x + \alpha^i)$.

З цього випливає розкладання для циклічної підгрупи поля двочлена $x^{2^m-1} + 1$

$$x^{2^m-1} + 1 = \prod_{i=1}^{2^m-1} (x + \alpha^i). \quad (3.22)$$

Використовуючи положення згідно теореми 5 і 6 можна представити розкладання двочлена $x^7 + 1$ з урахуванням його коренів у вигляді

$$x^{2^3-1} + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^3)(x + \alpha^4)(x + \alpha^5)(x + \alpha^6)(x + \alpha^7).$$

Переконаємося у справедливості рівняння (3.21) і (3.22) на прикладі розширеного поля $GF(2^2)$. Позначивши утворюючий елемент поля символом α а примітивний многочлен, що визначає це поле, можна подати у вигляді $G(\alpha) = \alpha^2 + \alpha + 1$. З табл. 3.7 випливає, що ненульовими елементами такого поля є $\alpha, \alpha + 1$ і $\alpha^{3 \bmod 3} = \alpha^0 = 1$. В даному випадку перевірка полягає в підстановці значень змінної x елементами поля в рівність

$$F(x) = x^{2^2-1} + 1 = x^3 + 1.$$

При: 1) $x = \alpha^0 = 1, f(x) = 1^3 + 1 \equiv 0$;

2) $x = \alpha, f(x) = \alpha^3 + 1 = (\alpha + 1)(\alpha^2 + \alpha + 1) \equiv 0 \pmod{[(\alpha^2 + \alpha + 1), 2]}$;

3) $x = \alpha + 1, f(x) = (\alpha + 1)^3 + 1 = (\alpha^2 + 1)(\alpha + 1) + 1 =$
 $\alpha^3 + \alpha + \alpha^2 + 1 + 1 \equiv$
 $\equiv \alpha(\alpha^2 + \alpha + 1) \equiv 0 \pmod{[(\alpha^2 + \alpha + 1), 2]},$

що і слід було очікувати.

Зауваження. Якщо елементи α^i поля $GF(2^m)$ розглядати в якості коренів двочлена $x^{2^m-1} + 1$ або коренів примітивних многочленів $G(x)$, то корені і многочлени в новій якості зручно позначати іншими символами, наприклад, β^i і $\mu_s(x)$, як це прийнято в літературі по теорії кодування.

Розглянемо тепер задачу розбиття множини коренів $\beta^0, \beta^1, \beta^2, \dots, \beta^{2^m-1}$ на підмножини, що визначають незвідні многочлени, що відіграє важливу роль при виборі *породжуючих* многочленів БЧХ, які дозволяють виправляти багатократні помилки. Зазначене призводить до наступної теореми.

Теорема 7. Нехай $\mu_s(x)$ – незвідний многочлен з коефіцієнтами з поля $\text{GF}(2)$ степені r , а β є коренем многочлена мінімальної степені в полі $\text{GF}(2^m)$, тоді підмножина коренів $\beta, \beta^2, \dots, \beta^{2^m-1}$ утворює сукупність всіх коренів, які визначають $\mu_s(x)$.

Зміст теореми 6 можна подати в загальному вигляді формулою

$$\mu_s(x) = \prod_{i=0}^{r-1} (x + \beta^{2^i \cdot s}), \quad (3.23)$$

де s – індекс мінімального многочлена.

Цінність теореми 6 полягає в тому, що вона однозначно встановлює належність коренів двочлена $x^{2^m-1} + 1$ до незвідних многочленів.

Визначення 6. Незвідний многочлен $\mu_s(x)$, згідно теоремі 6, називається *мінімальним* многочленом елемента β^s , а при $s=1$ коренем першої степені β . Крім умови $\mu_s(\beta) \equiv 0 \pmod{2}$, також виконуються умови

$$\mu_s(\beta^{2^i}) \equiv 0 \pmod{2} \text{ при } i = 1, 2, \dots, r-1. \quad (3.24)$$

Приклад 10. Розглянемо відповідність розподілу коренів мінімальних многочленів $\mu_s(x)$ у полі $\text{GF}(2^3)$.

З урахуванням теореми 6 мінімальний многочлен з індексом $s=1$ $\mu_1(x)$ визначається згідно (3.23) через свої корені в такий спосіб:

$$\mu_1(x) = (x + \beta)(x + \beta^2)(x + \beta^4).$$

Розкриваючи дужки, одержуємо, що

$$\begin{aligned} \mu_1(x) &= x^3 + (\beta + \beta^2 + \beta^4)x^2 + (\beta^2\beta^2\beta + \beta\beta\beta^2)x + \beta\beta^2\beta^4 = \\ &= x^3 + (\beta + \beta^2 + \beta^4)x^2 + (\beta^5 + \beta^4)x + \beta^7. \end{aligned}$$

Переходячи від позначень β^i до α^i і до подання елементів поля у вигляді двійкових кодових символів, згідно табл. 3.2 отримуємо

$\beta + \beta^2 + \beta^4$	$010 + 001 + 011$	$\equiv 000 \rightarrow 0$
$\beta^4 + \beta^5$	$011 + 111$	$\equiv 100 \rightarrow 1$
$\beta^7 \equiv \beta^0 \pmod{7}$	100	$\equiv 100 \rightarrow 1$

Отже, $\mu_1(x) = x^3 + x + 1$, що не є несподіваним результатом.

Покажемо тепер справедливість (3.24). Так як $\mu_1(x) = x^3 + x + 1$, то, підставивши корінь першого степеня β і переходячи до двійкового подання остаточно одержуємо

$\mu_1(\beta) = \beta^3 + \beta + 1$	$\rightarrow 110 \oplus 010 \oplus 100 \equiv 000.$
$\mu_1(\beta^2) = \beta^6 + \beta^2 + 1$	$\rightarrow 101 \oplus 001 \oplus 100 \equiv 000$

$$\mu_1(\beta^4) = \beta^{12} + \beta^4 + 1 \equiv \beta^5 + \beta^4 + 1 \rightarrow 111 \oplus 011 \oplus 100 \equiv 000$$

Корінь мінімального степеня, що не увійшов в період циклічної послідовності $\mu_1(x) \in \beta^3$, який належить мінімальному многочлену $\mu_3(x)$. Тому згідно (3.23), іншими коренями $\mu_3(x)$ будуть $\beta^6, \beta^{12} \equiv \beta^5 \pmod{7}$. Тепер одержуємо, що $\mu_3(x) = (x + \beta^3)(x + \beta^6)(x + \beta^5)$. Аналогічно попередньому перетворенню, можна перекоонатися, що $\mu_3(x) = x^3 + x^2 + 1$. І, нарешті, останній корінь, що не увійшов до розкладання $\mu_1(x)$ і $\mu_3(x)$, $\in \beta^7 \equiv \beta^0 \pmod{7}$. Корінь β^0 відповідає мінімальному многочлену першої степені $\mu_0(x) = x + 1$. Таким чином, на підставі проведених обчислень можна записати, що

$$x^7 + 1 = \mu_0(x) \mu_1(x) \mu_3(x). \quad (3.25)$$

У розглянутих прикладах простежується певна закономірність розкладання двочлена $x^{2^m-1} + 1$ на добуток мінімальних многочленів, яка полягає в тому, що множина цілих чисел i , відповідних степеням β , розпадаються на непересічні підмножини C_s за $\text{mod}(2^m - 1)$, а саме:

$$\begin{aligned} C_0 &= \{0\} && \rightarrow \mu_0(x); \\ C_1 &= \{1, 2, 4\} && \rightarrow \mu_1(x); \\ C_3 &= \{3, 6, 5\} && \rightarrow \mu_3(x). \end{aligned}$$

Підмножини C_s , називаються *циклотомічними* класами. При цьому слід зазначити, що розкладання на циклотомічні класи можна виконувати по будь-якому цілому непарному додатному числу. Останнє можна використовувати при розкладанні на мінімальні многочлени двочлена $x^n + 1$, де $n \neq 2^m - 1$.

Таблиця Марша-Пітерсона для деяких незвідних многочленів над полем. Для розкладання двочленів $x^{2^m-1} + 1$ степені $m < 34$ ($n < 2^{34} - 1$) наведені мінімальні многочлени в вісімковій системі числення із зазначенням степенів мінімальних многочленів в десятковій системі числення. У таблиці вісімковому поданню многочленів відповідає код:

$$0 \rightarrow 000, 1 \rightarrow 001, 2 \rightarrow 010, 3 \rightarrow 011, 4 \rightarrow 100, 5 \rightarrow 101, 6 \rightarrow 110, 7 \rightarrow 111.$$

Після кодового запису мінімального многочлена в таблиці наведені латинські літери, що несуть додаткову інформацію про многочлен. Літери А, В, С, D означають, що розглянутий многочлен непримітивний, а букви Е, F, G, Н відповідають *примітивним* многочленам. Ці ж букви несуть й іншу інформацію, яка для нас в даному випадку не дуже важлива. Для зручності вирішення задач при побудові кодеків БЧХ в табл. 3.9 наведені мінімальні многочлени, що входять до розкладання двочленів степені $m < 11$.

Приклад 11. Виконаємо декодування многочленів степеня $m = 4$.

Умовне позначення першого многочлена 1 23 F свідчить про те, що корінь β має мінімальну степінь, яка дорівнює одиниці, а многочлену в вісімковому поданні 23 відповідає многочлен в двійковій формі 010 011 або

в поліноміальній формі $\mu_1(x) = x^4 + x + 1$. Символ F свідчить про те, що розглянутий многочлен є примітивним. Далі $3\ 37\ D \rightarrow \beta^3$, $011\ 111$, $\mu_3(x) = x^4 + x^3 + x^2 + x + 1$. Многочлен непримітивний і наступний многочлен $5\ 07 \rightarrow \beta^5$, 000111 , $\mu_5(x) = x^2 + x + 1$, відсутність літерного позначення свідчить про те, що многочлен має степінь $r < m$.

Таблиця 4.9 – Таблиця незвідних многочленів ступені $m < 11$

Степінь $m = 2$ ($n = 3$)					
1 7 H					
Степінь $m = 3$ ($n = 7$)					
1 13 F					
Степінь $m = 4$ ($n = 15$)					
1 23 F	3 37 D	5 07			
Степінь $m = 5$ ($n = 31$)					
1 45 E	3 75 G	5 67 H			
Степінь $m = 6$ ($n = 63$)					
1 103 F 21 007	3 127 B	5 147 H	7 111 A	9 015	11 155 E
Степінь $m = 7$ ($n = 127$)					
1 211 E 13 203 F	3 217 E 19 313 H	5 235 E 21 345 G	7 367 H	9 277 E	11 325 G
Степінь $m = 8$ ($n = 255$)					
1 435 E 13 453 F 25 433 B 85 007	3 567 B 15 727 D 27 477 B	5 763 D 17 023 37 537 F	7 551 E 19 545 E 43 703 H	9 675 C 12 613 D 45 471 A	11 747 H 23 543 F 51 037
Степінь $m = 9$ ($n = 511$)					
1 1021 E 13 1167 F 25 1743 H 41 1563 H 73 0013	3 1131 E 15 1541 E 27 1617 H 43 1713 H 75 1773 G	5 1461 G 17 1333 F 29 1553 H 45 1175 E 77 1511 C	7 1231 A 19 1605 G 35 1401 C 51 1725 G 83 1425 G	9 1423 G 21 1027 A 37 1157 F 53 1225 E 85 1267 E	11 1055 E 23 1751 E 39 1715 E 55 1275 E
Степінь $m = 10$ ($n = 1023$)					
1 2011 E 13 2157 F 25 2443 F 37 3543 F 49 3525 C 69 2701 A 85 2707 E 101 2055 E 149 3025 G 341 0007	3 2017 15 2653 B 27 3573 D 39 2107 B 51 2547 B 71 3323 H 87 2311 A 103 3575 G 155 2251 A	5 2415 E 17 3515 G 29 2461 E 41 2745 E 53 2617 F 73 3507 H 89 2327 F 105 3607 C 165 0051	7 3771 G 19 2773 F 31 043 D 43 2431 E 55 3453 D 75 2437 B 91 3265 G 107 3171 G 171 3315 C	9 2257 B 21 3753 D 33 0075 C 453061 C 57 3121 C 77 2413 B 93 3777 D 109 2047 F 173 3337 H	11 2065 A 23 2033 F 35 3023 H 47 3177 H 59 3471 G 83 3623 H 99 0067 147 2355 A 179 3211 G

У табл. 3.9 наводяться тільки основні многочлени, якими є $\mu_1(x)$, $\mu_3(x)$ і $\mu_5(x)$, четвертим є взаємний або зворотний примітивному многоч-

лену $\mu_1(x)$, а п'ятим для всіх степенів m є многочлен першого степеню $\mu_0(x) = x + 1$. Корінь зворотного многочлена до $\mu_1(x)$ визначаються таким чином: $\beta^{-1} = \beta^{0-1} = \beta^{15-1} = \beta^{14}$, далі аналогічно можна отримати, що $\beta^{-2} = \beta^{13}$, $\beta^{-4} = \beta^{11}$ і $\beta^{-8} = \beta^7$. Таким чином $\mu_7(\beta) = (x + \beta^7)(x + \beta^{11})(x + \beta^{13})$, що відповідає в поліноміальній формі $\mu_7(x) = x^4 + x^3 + 1$. В даному випадку примітивному многочлену $x^4 + x + 1$ відповідає мінімальний многочлен $\mu_7(x) = x^4 + x^3 + 1$. Отже,

$$x^{15} + 1 = \mu_0(x) \mu_1(x) \mu_3(x) \mu_5(x) \mu_7(x).$$

3.4. Синтез двійкових циклічних кодів

У цьому підрозділі розглядається важливий підклас лінійних двійкових блокових кодів, в який входять прості, з точки зору розширення циклічні поліноміальні коди Хеммінга, а також більш складні коди Боуза-Чоудхурі-Хоквінгема (БЧХ), які дозволяють виправляти багатократні помилки.

Кодові слова двійкових циклічних кодів $(n, m) = (2^r - 1, 2^r - r - 1)$ компактно подають у поліноміальній формі, тобто у вигляді багаточленів деякої фіктивної змінної x з коефіцієнтами простого поля $GF(2)$. Тому для їх подання будемо користуватися такою формою, а у деяких випадках і у вигляді послідовностей двійкових символів. Прикладом запису двійкової послідовності 1000101 у вигляді багаточлена є

$$F(x) = 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1 = x^6 + x^2 + 1.$$

Далі, при викладенні матеріалу. під багаточленом $A(x) = x^{m-1} + x^{m-2} + \dots + 1$ слід розуміти двійкову послідовність інформаційних символів, яка підлягає кодуванню ЦК, а $F(x) = x^{n-1} + x^{n-2} + \dots + 1$ – є КК в поліноміальній формі ЦК.

Визначення 7. Лінійний блоковий код називається *циклічним*, якщо в ньому, крім багаточлена $F(x)$, що належить йому, містяться ще багаточлени $F_1(x)$, $F_2(x)$ і т.д., утворені циклічними зсувами багаточлена $F(x)$.

Суть циклічного зсуву праворуч полягає в тому, що старший символ КК (він знаходиться праворуч) займає місце молодшого, а молодший і всі наступні – зміщуються на один розряд праворуч. Наприклад, КК 1001011, після циклічного зсуву праворуч на один такт, відповідає послідовності двійкових символів 1100101.

Покажемо, що циклічний зсув праворуч на один розряд символів довільного КС $F(x) = x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + 1$ відповідає символічному множенню за модулем два

$$(x \times F(x)) \bmod [(x^n + 1), 2].$$

Пояснимо сказане на прикладі КС 1001011 $\rightarrow 1 + x^3 + x^5 + x^6$.

$$x \times (1 + x^3 + x^5 + x^6) = \begin{array}{r|l} x + x^4 + x^6 + x^7 & x^7 + 1 \\ \hline \underline{x^7 + 1} & 1 \\ 1 + x + x^4 + x^6 \rightarrow & 1100101 \end{array}$$

Тепер необхідно з'ясувати умови завдання і побудови циклічного коду. Відповідь на це в першу чергу дає теорема 3.

Теорема 8. Циклічний код значності $n = 2^r - 1$, де $r > 1$ – ціле позитивне число, задається породжуючим багаточленом $G(x)$ степеня $s < r$ тоді і тільки тоді, коли він ділить двочлен $x^n + 1$ без остачі.

Ідея побудови найпростіших ЦК, які виправляють тільки однократні помилки або виявляють одно- і двократні помилки, базується на застосуванні в якості $G(x)$ примітивних багаточленів. Нагадаємо тільки те, що є вони незвідним, тобто не мають дільників крім одиниці і самого себе. Якщо ж $G(x)$ є добутком двох і більше незвідних багаточленів, то такий ЦК може виправляти помилки кратності більше одиниці.

Як найпростіший приклад розглянемо побудову всіх основних параметрів можливих ЦК значності $n = 2^3 - 1 = 7$. Для цього необхідно скористатися розкладом двочлена степеня $r = 3$ $x^{2^r - 1} + 1 = x^7 + 1$.

Виходить, що

$$x^7 + 1 = \mu_0(x) \times \mu_1(x) \times \mu_3(x) = 1 \times (x + 1) \times (x^3 + x + 1) \times (x^3 + x^2 + 1).$$

Вибираючи різні співмножники з наведеного розкладу і їх добутки як породжуючі багаточлени, отримуємо різні ЦК значності $n = 7$. Основні параметри цих кодів наведені в табл. 3.10.

Таблиця 3.10 – Параметри ЦК значності $n = 7$

$G_i(x)$	r	(n, k)	ρ	d_0
$G_1(x) = 1$	0	(7, 7)	0	1
$G_2(x) = x + 1$	1	(7, 6)	0,143	2
$G_3(x) = x^3 + x + 1$	3	(7, 4)	0,428	3
$G_4(x) = x^3 + x^2 + 1$	3	(7, 4)	0,428	3
$G_5(x) = G_2(x) \times G_3(x)$	4	(7, 3)	0,571	4
$G_6(x) = G_3(x) \times G_4(x)$	6	(7, 1)	0,857	7

Із табл. 3.10 бачимо, що некоригуючий семизначний код (7, 7) є єдиним випадком ЦК з $\rho = 0$ і $d_0 = 1$, тобто при значенні $G(x) = 1$. Насту-

пний код (7, 6) з породжуючим багаточленом $G(x) = x + 1$ є найпростішим коригуючим кодом з парним числом одиниць, що дозволяє виявляти помилки непарної кратності. Коди (7,4) $d_0 = 3$, отримані на основі багаточленів $G_3(x)$ і $G_4(x)$, називаються *еквівалентними*, тому що їх породжуючі багаточлени взаємні. Ці коди відрізняються тільки порядком розміщення двійкових символів в КК. Якщо як породжуючий багаточлен вибраний багаточлен $G_5(x) = x^4 + x^3 + x^2 + 1$ четвертого степеня, то отримаємо код (7, 3) з $d_0 = 4$, який забезпечує виправлення однократних і виявлення двократних помилок. Максимальною коригуючою здатністю володіє ЦК (7,1) з $G_6(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ і $d_0 = 7$, в якому дозволеними КС є 0000000 і 1111111. На закінчення зазначимо, що з підвищенням степеня $G(x)$ при фіксованому n коригуюча здатність ЦК підвищується.

Циклічні коди Хеммінга. Кодами Хеммінга називають лінійні блокові (n, m) коди з $d_0 = 3$, що задовольняють умові (3.5) зі знаком рівності, тобто $2^r = 1 + C_n^1$, які дозволяють виправляти однократні помилки. Із зазначеного виходить, що для будь-яких додатних $r = n - m$ і $n = 2^r - 1$ існують відмінні коди Хеммінга з $m = 2^r - r - 1$. Для цих кодів як породжуючий багаточлен $G(x)$ може бути вибраний будь-який примітивний багаточлен, що входить в розклад двочлена $x^{2^r - 1} + 1$ або взаємний йому. В табл. 3.11 наведені деякі коди Хеммінга, які задані примітивним багаточленом степеня $r < 11$. Нагадуємо, що вімковому представленню багаточлена 1021 відповідає код 001 000 010 001, якому в свою чергу відповідає багаточлен дев'ятого степеня $x^9 + x^4 + 1$.

Таблиця 3.11 – Параметри деяких ЦК Хеммінга

Вісімковий код $G(x)$	r	$G_i(x)$	(n, m)	$\rho = r/n$
7 H	2	$x^2 + x + 1$	3, 1	0,667
13 F	3	$x^3 + x + 1$	7, 4	0,428
23 F	4	$x^4 + x + 1$	15, 11	0,267
45 E	5	$x^5 + x^2 + 1$	31, 26	0,161
103 F	6	$x^6 + x + 1$	63, 57	0,095
211 E	7	$x^7 + x^3 + 1$	127, 120	0,055
435 E	8	$x^8 + x^4 + x^3 + x^2 + 1$	225, 247	0,031
1021 E	9	$x^9 + x^4 + 1$	511, 502	0,018
2011 E	10	$x^{10} + x^3 + 1$	1023, 1013	0,010

Слід відзначити, що наведений в таблиці код (63, 57) знаходить застосування в міжнародній супутниковій системі морського зв'язку ІНМАРСАТ як складовий каскадний код.

Порівнюючи циклічні коди згідно з табл. 3.11, бачимо, що з підвищенням значності коду зменшується надлишковість $\rho = r/n$ і, отже, за однакових алгоритмів декодування в каналах з незалежними помилками, буде зростати ймовірність помилки на виході декодера. Це пояснюється тим, що зі зростанням n зростає значення ймовірності утворення помилок кратності $t > t_{\text{вп}}$, що виходить із формули Бернуллі

$$P_t = C_n^t p_0^t (1 - p_0)^{n-t}.$$

На рис. 3.13 показана діаграма залежності значень P_t , при $t = 1, 2, 3, \text{ і } 4$, обчислені за вищенаведеною формулою при $p_0 = 10^{-3}$ для кодів значності $n = 7, 15, 31, \text{ і } 63$. Таким чином видно, що для дискретного симетричного каналу (ДСК) кращими можуть бути коди з невеликою довжиною кодового блока. Але в каналі з аддитивним білим гауссівським шумом (АБГШ) і двофазною модуляцією (ФМ-2) в діапазоні відношень енергії біта до спектральної потужності завади $E_b/N_0 = 6 \dots 12$ дБ ймовірність бітової помилки при коді (15, 11) менше, ніж при (7, 4).

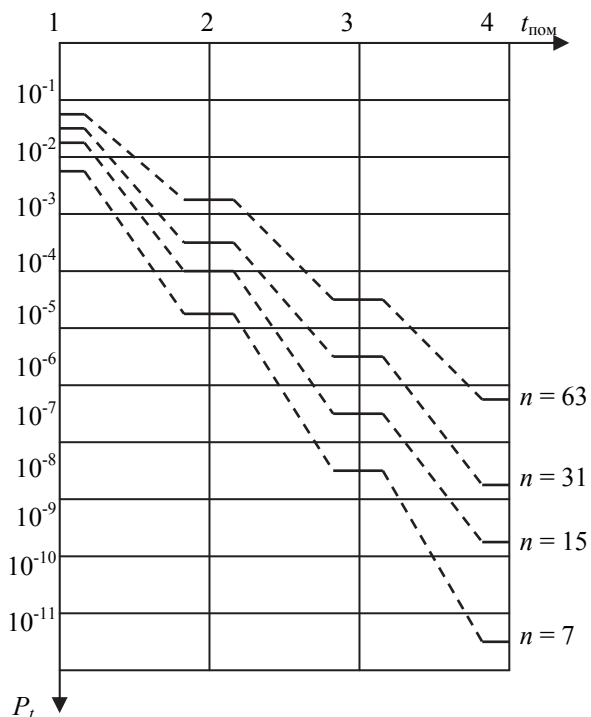


Рисунок 3.13 – Діаграма залежності ймовірності утворення t -кратних помилок при $p_0 = 10^{-3}$

Коди Хеммінга є прикладами небагатьох досконалих кодів, тобто таких, які володіють мінімальною надлишковістю при $d_0 = 3$. Покажемо це на прикладі, порівнюючи з кодом (9, 3) з параметрами $d_0 = 3$ і $\rho = 0,666$. Породжуючий багаточлен цього коду $G(x) = x^6 + x^3 + 1$ входить в розклад двочлена $x^9 + 1$, степінь якого, як видно, не є степенем двійки або одиниці. Порівнюючи надлишковість цього коду з надлишковістю коду (15, 11) бачимо, що в ньому виправлення однократних помилок досягається при більшому числі перевірочних символів, а саме шести замість чотирьох для коду Хеммінга.

Коди Хеммінга легко перетворюються в коди з $d_0 = 4$ шляхом множення породжуючого багаточлена на двочлен $x + 1$, тобто $G_{(n, m-1)}(x) = G_{(n, m)}(x) \times (x + 1)$. Такі коди називають *розширеними* кодами Хеммінга. Їх основні параметри $n = 2^r - 1$, $m = n - r - 1$, тобто (7, 3), (15, 10), (31, 25) і т.д.

Циклічний код, як і будь-який лінійний бло-ковий код, може бути заданий за допомогою *породжуючої* або *перевірочної* матриці. Підматрицю перевірочних елементів $B_{(n-m), m}$ для ЦК (7, 4) можна побудувати шляхом ділення перших чотирьох дозволених КС з однократними помилками $F_1(x) = x^6$, $F_2(x) = x^5$, $F_3(x) = x^4$ і $F_4(x) = x^3$ на $G_1(x) = x^3 + x + 1$.

$$\begin{array}{r} x^6 \\ \underline{x^6 + x^4 + x^3} \\ x^4 + x^3 \\ \underline{x^4 + x^2 + x} \\ x^3 + x^2 + x \\ \underline{x^3 + x + 1} \\ x^2 + 1 \end{array} \rightarrow \begin{array}{l} x^3 + x + 1 \\ x^3 + x + 1 \\ \\ \\ \\ 101 \end{array}$$

$$x^5 \bmod G_1(x) = x^2 + x + 1 \rightarrow 111, \quad x^4 \bmod G_1(x) = x^2 + x \rightarrow 110, \\ x^3 \bmod G_1(x) = x + 1 \rightarrow 011.$$

Таким чином, для ЦК (7, 4) породжуюча матриця має вигляд

$$G_{7,4} = \begin{pmatrix} 1000 & 101 \\ 0100 & 111 \\ 0010 & 110 \\ 0001 & 011 \end{pmatrix}.$$

Перший рядок перевірконої матриці ЦК $H_{7,3}$ визначається виразом $H_1(x) = (x^7 + 1)/G_1(x)$. А саме $(x^7 + 1)/(x^3 + x + 1) = x^4 + x^2 + x + 1$ або у двійковому поданні 0010111. Останні два рядки можуть бути утворені шляхом циклічних зсувів праворуч 0010111. Отже, перевірна матриця даного циклічного коду має вигляд

$$H_{7,3} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{або} \quad H_{7,3} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Таким чином, при розгляді ЦК аналогом породжуючої матриці $G_{7,4}$ є породжуючий багаточлен $G_1(x)$, а перевірконою матрицею $H_{7,3}$ є перевірочний багаточлен $H_1(x)$.

Коди Боуза-Чоудхурі-Хоквінгема. Коди Боуза-Чоудхурі-Хоквінгема (БЧХ) утворюють великий підклас ЦК, які виправляють незалежні помилки кратності $t_{\text{вп}} > 1$, метод побудови яких може бути заданий у неприхованій формі. Інтерес до таких кодів визначається тим, що серед них за невеликих значень значності ($n < 511$) існують порівняно хороші коди. Відомі також прості методи їх декодування. Останнє відноситься до таких кодів, які допускають мажоритарний принцип виправлення помилок.

Характерним для кодів БЧХ є те, що вони є узагальненням розглянутих раніше кодів Хеммінга. Метод побудови кодів БЧХ дає наступна теорема.

Теорема 9. Породжуючий багаточлен $G(x)$ кодів БЧХ с параметрами (n, m) и $d_{\text{БЧХ}} = 2t_{\text{вп}} + 1$ визначається виразом

$$G(x) = \text{НСК} [\mu_1(x), \mu_3(x), \mu_5(x), \dots, \mu_{\text{БЧХ}-2}(x)], \quad (3.26)$$

де НСК – найменше спільне кратне, $\mu_i(x)$ – мінімальні багаточлени елементів β^i , тобто коренів мінімального степеня; $d_{\text{БЧХ}}$ – конструктивна мінімальна кодова відстань (для кодів БЧХ $d_{\text{БЧХ}} \leq d_0$).

Як видно із наведеної теореми, основна задача при виборі того чи іншого ЦК, перш за все, зводиться до визначення породжуючого багаточлена $G(x)$, від вибору якого залежить коригуюча здатність коду. Розглянемо приклад, який дозволяє безпосередньо розв'язати ту або іншу задачу, не використовуючи додаткову літературу.

Приклад 12. Поставимо задачу побудови всіх кодів БЧХ довжиною $n = 31$. Для визначення мінімальних багаточленів можливих кодів БЧХ вказаної значності, дозволяючих виправляти багатократні помилки необхідно виконати наступне:

1) виписати із таблиці Марша-Пітерсона всі основні мінімальні багаточлени, що відносяться до степеня $m = 5$ і перевести їх із вісімкової системи числення в двійкову:

$$1\ 45\ E \rightarrow \beta\ 100\ 101, \quad 3\ 75\ G \rightarrow \beta^3\ 111\ 101, \quad 5\ 67\ H \rightarrow \beta^5\ 110\ 111;$$

2) подати мінімальні функції коренів β , β^3 і β^5 у вигляді багаточленів фіктивної змінної x :

$$\mu_1(x) = x^5 + x^2 + 1; \quad \mu_3(x) = x^5 + x^4 + x^3 + x^2 + 1; \quad \mu_5(x) = x^5 + x^4 + x^2 + x + 1;$$

3) визначити взаємні мінімальні багаточлени до $\mu_1(x)$, $\mu_3(x)$ і $\mu_5(x)$:

$$\begin{aligned} \mu_1^*(x) &= x^5 \times (1 + x^{-2} + x^{-5}) = x^5 + x^3 + 1 \\ \mu_3^*(x) &= x^5 \times (1 + x^{-2} + x^{-3} + x^{-4} + x^{-5}) = x^5 + x^3 + x^2 + x + 1 \\ \mu_5^*(x) &= x^5 \times (1 + x^{-1} + x^{-2} + x^{-4} + x^{-5}) = x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

4) визначити корені оберненого мінімального багаточлена $\mu_1^*(x)$:

$$\begin{aligned} \beta_*^1 = \beta^{-1} = \beta^{0-1} = \beta^{31-1} = \beta^{30}, \quad \beta_*^2 = \beta^{-2} = \dots = \beta^{29}, \quad \beta_*^4 = \beta^{-4} = \dots = \beta^{27}, \\ \beta_*^8 = \beta^{-8} = \dots = \beta^{23}, \quad \beta_*^{16} = \beta^{-16} = \dots = \beta^{15}. \end{aligned}$$

Із обчислених коренів, що належать $\mu_1^*(x)$, виходить, що β^{15} є коренем мінімального степеня мінімального багаточлена $\mu_1^*(x)$. Таким чином, можна записати, що

$$\mu_1^*(x) = \mu_{15}(x) = x^5 + x^3 + 1.$$

Аналогічно знаходимо, що для $\mu_3^*(x) \rightarrow \beta^{-3} = \beta^{28}$, $\beta^{-6} = \beta^{25}$, $\beta^{-12} = \beta^{19}$, $\beta^{-24} = \beta^7$, $\beta^{-48} = \beta^{-17} = \beta^{14}$. Отже,

$$\mu_3^*(x) = \mu_7(x) = x^5 + x^3 + x^2 + x + 1.$$

Продовжуючи далі, отримаємо, що для $\mu_5^*(x) \rightarrow \beta^{-5} = \beta^{26}$, $\beta^{-10} = \beta^{21}$, $\beta^{-20} = \beta^{11}$, $\beta^{-40} = \beta^{-9} = \beta^{22}$. Із наведеного виходить, що

$$\mu_5^*(x) = \mu_{11}(x) = x^5 + x^4 + x^3 + x + 1.$$

Згідно з (3.26) породжуючі багаточлени можливих кодів БЧХ визначаються добутком мінімальних багаточленів з непарними індексами

$$G_{\text{БЧХ}}(x) = \mu_1(x) \times \mu_3(x) \times \mu_5(x) \times \mu_7(x) \times \mu_{11}(x) \times \mu_{15}(x).$$

Основні параметри кодів БЧХ довжини $n = 31$ наведені в табл. 3.12.

Із табл. 3.12 бачимо, що код Хеммінга є окремим випадком кодів БЧХ. Мінімальну кодову відстань наведених в таблиці кодів можна збільшити, вводячи при обчисленні $G(x)$ мінімальний багаточлен $\mu_0(x) = x + 1$, єдиним коренем якого є елемент поля $GF(2^5)$ $\beta^0 \rightarrow 00010$. Наприклад, коду $(31, 15)$ з $d_0 = 8$ відповідає породжуючий багаточлен $G(x) = \mu_0(x) \mu_1(x) \mu_3(x) \mu_5(x)$.

Таблиця 3.12 – Параметри кодів БЧХ довжини 31

n	k	r	$G(x)$	$G(x)$ у вісімковій системі	$d_{\text{БЧХ}}$	d_0	$t_{\text{ВП}}$
31	26	5	$G_1(x) = \mu_1(x)$	45	3	3	1
	21	10	$G_2(x) = \mu_3(x) \times G_1(x)$	3551	5	5	2
	16	15	$G_3(x) = \mu_5(x) \times G_2(x)$	107657	7	7	3
	11	20	$G_4(x) = \mu_7(x) \times G_3(x)$	5423325	9 – 11	11	4 – 5
	6	25	$G_5(x) = \mu_{11}(x) \times G_4(x)$	313365047	13 – 15	15	6 – 7

Основою для побудови кодів БЧХ може слугувати табл. 3.12 незвідних багаточленів. Описана вище процедура дає можливість отримати породжуючі багаточлени примітивних кодів довжини $n = 2^m - 1$, що мають зростаючий степінь $G(x)$ і більш високу коригуючу здатність. Коди БЧХ прийнято ділити на короткі ($n < 127$) і довгі ($n > 127$). Серед коротких кодів код БЧХ $(63, 39)$ з $d_0 = 9$ використовується також у системі ІНМАРСАТ.

3.5. Лінійні блокові коди для каналів із групуванням помилок

У каналах із групуванням помилок недоцільно використовувати лінійні блокові коди, сконструйовані для боротьби з незалежними помилками, тому що при цьому потрібна була б більша надлишковість, використовувана лише для виправлення обмеженого числа помилок у межах пакета. Тому в каналах із групуванням помилок більш ефективними виявляються спеціальні лінійні блокові коди. Розглянемо деякі з них.

Коди Абрамсона. Для таких кодів породжуючий поліном

$$g(x) = (1 + x)p(x),$$

$p(x)$ – незвідний поліном μ степеня. Значність коду

$$n = 2^\mu - 1,$$

а число інформаційних і перевірочних символів

$$k = n - \mu - 1 = 2^\mu - \mu - 2; \quad l = \mu + 1.$$

Такі коди мають $d_0 = 4$ і, отже, дозволяють виправляти всі поодинокі й суміжні подвійні ($l_{\text{п}} = 2$) помилки.

Коди Файра. Ці коди є узагальненням кодів Абрамсона й утворюють найбільш великий клас кодів, що виправляють пакети помилок. Породжуючий поліном таких кодів

$$g(x) = (x^\xi + 1)p(x),$$

де $p(x)$ – незвідний поліном μ степеня. Значність коду n є найменше спільне кратне чисел ξ і $\beta = 2^\alpha - 1$:

$$n = \text{НСК}(2^\alpha - 1, \xi)$$

причому α – величина, пов'язана з довжиною пакета помилок, що виправляється ($\alpha \geq l_{\text{п вп}}$), а $\xi = \alpha - 1$.

Число інформаційних і перевірочних символів

$$k = n - \mu - \xi; \quad l = \mu + \xi.$$

Якщо замінити деякі інформаційні символи нулями, то вийде скорочений код Файра.

Коди Файра дозволяють виправити одиночний пакет помилок довжиною $l_{\text{п вп}}$ й одночасно виявити будь-який пакет помилок довжиною $l_{\text{п в}} \geq l_{\text{п вп}}$, якщо $\xi \geq l_{\text{п вп}} + l_{\text{п в}} - 1$ й $\mu \geq l_{\text{п вп}}$. При використанні таких кодів тільки для виявлення помилок вони дозволяють виявляти будь-який пакет помилок довжиною $l_{\text{п}} \leq \xi + \mu$ або будь-якою комбінацією із двох пакетів помилок, причому довжина найменшого пакета $l_{\text{п мін}} \leq \mu$, сума довжин обох пакетів $l_{\text{п мін}} + l_{\text{п макс}} \leq \xi + 1$.

Синтез кодуєчих пристроїв здійснюється звичайними методами, використовуючи $g(x)$ поліном.

Приклад 13. Побудуємо породжуючий поліном коду Файра, що має такі властивості: $l_{\text{ПВП}} = 3$, $l_{\text{ПВ}} = 0$, $p(x) = 1011$. Величини $\mu = 3$; $\beta = 7$, $\alpha = l_{\text{ПВ}} = 3$; $\xi = 2$; $n = \text{НСК}(7,2) = 14$; $k = 9$; $l = 5$; породжуючий поліном $g(x) = (x^2 + 1) \cdot (x^3 + x + 1) = 100111$.

Кодування методом повторення. Цей спосіб кодування заснований на μ -кратній передачі n -значних кодограм. При цьому найбільшого поширення набули два способи. При першому способі кодограма X_j передається μ разів, у результаті чого послідовність символів має вигляд

$$\frac{x_1 x_2 \dots x_n}{1} \quad \frac{x_1 x_2 \dots x_n}{2} \quad \dots \quad \frac{x_1 x_2 \dots x_n}{\mu}.$$

Такий метод легко реалізується й звичайно використовується в каналах з параметрами, що швидко змінюються. Ефективність його обумовлена тим, що спотворення символів з однаковими номерами часто можна вважати статистично незалежними. Тому такий метод іноді називають *кодуванням з декореляцією помилок*.

При другому способі кожний символ кодограми передається μ разів наспіль, і послідовність символів у каналі буде

$$\frac{x_1 \dots x_1}{\mu} \quad \frac{x_2 \dots x_2}{\mu} \quad \dots \quad \frac{x_n \dots x_n}{\mu}.$$

Цей метод звичайно використовується в каналах з параметрами постійними і які повільно змінюються.

Кодова відстань не залежить від способу передачі й становить

$$d_0 \mu = \mu d_0,$$

де d_0 – мінімальна відстань між кодограмами.

Двократне повторення можна розглядати як лінійний блоковий код з породжуючою й перевіркою матрицями

$$G^{(2)} = \|E_n, E_n\|; \quad H^{(2)} = \begin{vmatrix} E_n \\ E_n \end{vmatrix},$$

де E_n – одинична матриця розміру n . Як видно зі структури матриці $H^{(2)}$, такий код не допускає мажоритарного оброблення прийнятих сигналів, тому що будь-який коректор відповідає двом векторам помилок. Однак код виявляє всі непарні помилки.

При трикратному повторенні матриці коду будуть

$$G^{(3)} = \|E_n E_n E_n\|; \quad H^{(3)} = \begin{vmatrix} E_{2n} \\ E_n E_n \end{vmatrix},$$

де E_{2n} – одинична матриця розміру $2n$. Такий код допускає мажоритарне декодування за принципом «2 з 3». При цьому число помилок, що виправляються, ваги v становить $3^v C_n^v$.

Інформаційна послідовність після оброблення кодограми за методом «2 з 3» еквівалентна символу, переданому один раз, але з імовірністю спотворення p_0^1 . Тому що ймовірності правильного прийому символу при трикратній передачі й у двох випадках із трьох відповідно будуть

$$q_{03} = (1 - p_0)^3; \quad q_{023} = C_3^2 p_0 (1 - p_0)^2,$$

тоді з умови

$$1 - p_0^1 = q_{02} + q_{0,23}$$

Ймовірність

$$p_0^1 = 3p_0^2 - 2p_0^3.$$

Останній вираз дозволяє оцінювати ймовірність помилки декодування при трикратному повторенні комбінацій кодів з надлишковістю.

Становить інтерес оцінка числа $N_r(v)$ векторів помилок ваги v , які після оброблення за принципом «2 з 3» утворять в n -значних кодограмах r -кратні помилки. Очевидно, що при $r = 0$ величина $N_0(v) = 3^v C_n^v$; при $r = 1$

$$N_1(v) = 3^{v-1} C_n^1 C_{n-1}^{v-2} + 3^{v-3} C_n^1 C_{n-1}^{v-3},$$

де перший і другий доданки є число векторів помилок, що викликають збої однойменних символів відповідно при двох і трьох повтореннях. Тоді в загальних випадках при r -кратних помилках

$$N_r(v) = 3^{v-r} C_n^r \sum_{j=0}^{\varepsilon} 3^{-2j} C_r^j C_{n-r}^{v-(2r+j)}, \quad (3.27)$$

де j – число збоїв символів при всіх трьох повтореннях; величина ε задовольняє умовам $\varepsilon \leq r$ і $\varepsilon \leq v - 2r$.

Для відбраковування спотворених кодограм при трикратному повторенні може також використовуватися спосіб підрахунку числа символів, незбійних в усіх трьох повтореннях. Якщо число таких символів досягне деякого граничного значення M_0 , то дана кодограма відбраковується. Нехай $N_r(v)$ – число векторів помилок ваги v , які викликають r -кратні помилки, що виявляються таким способом. Очевидно, що при $0 \leq v < M_0 + r$ величина $N'_r(v) = 0$; при $v \geq M_0 + r$ маємо

$$N'_r(v) = 3^{v-r} C_n^r \sum_{j=0}^{\alpha} 3^{-2j} C_r^j C_{n-r}^{v-(2r+j)}, \quad (3.28)$$

де $\alpha = \left\lfloor \frac{v - r - M_0}{2} \right\rfloor$ – найближче більше ціле число.

Формула (3.28) виходить із (3.27): при $j = 0$ лічильник розбіжності дає відлік $M = v - r$; при $j = \varepsilon$, $M = v - r - 2\varepsilon$. Тому при заданому порозі M_0 будуть виявлятися всі вектори помилок, що входять до формули (3.28) при значенні $0 \leq j \leq \frac{v-r-M_0}{2}$.

Укрупнення символів. З появою пакетів помилок можливо зробити їх декореляцію шляхом укрупнення символів. Так, якщо вихідна кодограма містила n символів a_1, \dots, a_n , а довжина пакета l_{Π} , то після укрупнення одержимо нову комбінацію B_1, \dots, B_N , де укрупнений елемент B_j містить η символів (за винятком може останнього). Це еквівалентно переходу від n -вимірного простору до N -вимірного з незалежними помилками. Якщо пакет помилок охопив два елементи B_{j-1} й B_j , то циклічною перестановкою завжди можна поєднати його з кожним із укрупнених елементів.

Аналогічно попередньому введемо коефіцієнт кореляції між укрупненими кодограмами:

$$p_{j\zeta} = \sum_{v=1} B_{v,j} B_{v,\zeta},$$

де

$$B_{v,j} B_{v,\zeta} = \begin{cases} +1 & \text{за } B_{v,j} = B_{v,\zeta} \\ -1 & \text{за } B_{v,j} \neq B_{v,\zeta} \end{cases}$$

Для визначення значності кодограм повинні бути задані число інформаційних символів k , довжина пакета l_{Π} й необхідне значення $\Delta\rho_{\min}$. Укрупнюючи інформаційні символи, отримаємо

$$k_y \leq n_y - \log_2 \sum_{v=0}^{\alpha} C_{n_y}^v, \quad (3.29)$$

де $k_y = \left\lceil \frac{k}{l_{\Pi}} \right\rceil$ – число укрупнених інформаційних символів; n_y – число укрупнених елементів у кодограмі; параметр $\alpha = \frac{\mu-1}{2}$, якщо

$\Delta\rho_{\min} = 2\mu$ ($\mu = 3, 5, 7, \dots$). При $\Delta\rho_{\min} = 2\mu + 2$ обчислення здійснюються за формулою (3.29), а потім значення n_y збільшується на одиницю (якщо $\Delta\rho_{\min} = 4$, то $n_y = k_y + 1$). Остаточна значність кодограми

$$n = (n_y - 1)l_{\Pi} + k_{y_0},$$

де k_{y_0} – значність останнього укрупненого інформаційного символу.

Приклад 14. Побудуємо код з $k = 3$, що виправляє пакет помилок довжиною $l_{\Pi} = 3$. Тоді $k_y = \left\lceil \frac{k}{l_{\Pi}} \right\rceil = 1$, $n_y = 3$, $n = 9$, $\Delta\rho_{\min} = 6$. Методом перебору знаходимо (9, 3)-код: 1 – 000000000; 2 – 001001001; 3 – 010010010; 4 – 100100100; 5 – 110110110; 6 – 011011011; 7 – 101101101; 8 – 111111111. Знайдений код на два символи коротше, ніж код, рекомендований Метцнером.

Приклад 15. Побудуємо код з $k = 3$, що виправляє пакет помилок довжиною $l_{\Pi} = 2$. Тоді $k_y = 2$, $n_y = 4$, $n = 7$. Методом перебору знаходимо (7, 3)-код з алгоритмом: 1 – 1110011; 2 – 0111010; 3 – 0011101; 4 – 1101110; 5 – 0100111; 6 – 1010100; 7 – 1001001; 8 – 0000000, для якого $\Delta\rho_{\min} = 6$. Нехай прийнята спотворена комбінація $3' = 0010001$.

Тоді $\rho_{3',1} = \rho_{3',3} = \rho_{3',7} = \rho_{3',8} = 0$; $\rho_{3',2} = \rho_{3',4} = -4$; $\rho_{3',5} = \rho_{3',6} = -2$ і винести рішення про передачу кодограму виявляється неможливим. Зробимо циклічну перестановку робочих кодограм: 1 – 1110011; 2 – 0111010; 3 – 0011101; 4 – 1101110; 5 – 0100111; 6 – 1010100; 7 – 1001001; 8 – 0000000. Тепер вже коефіцієнти кореляції будуть:

$$\rho_{3',1} = \rho_{3',5} = \rho_{3',6} = \rho_{3',7} = -2; \quad \rho_{3',2} = \rho_{3',4} = -4; \quad \rho_{3',3} = +2, \quad \rho_{3',8} = 0.$$

Величина $\rho_{3',3} > \rho_{3',j}$, що свідчить про передачу кодограми 0011101.

Приклад 16. Побудуємо код з $k = 57$, що виправляє пакет довжиною $l_{\Pi \text{ вп}} = 3$ або виявляє пакет $l_{\Pi \text{ в}} = 13$ символів. Для виправлення помилок знайдемо $k_y = 19$; $n_y = 23$; $n_{\text{в}} = 69$ і $\Delta\rho_{\min} = 6$. Для виявлення помилок отримаємо: $k_y = 5$; $n_y = 6$; $n_o = 70$ і $\Delta\rho_{\min} = 4$. Тому що $n_o > n_{\text{в}}$, то остаточно вибираємо (70, 57)-код.

Із наведених прикладів випливає, що для виправлення пакета помилок довжиною $l_{\Pi \text{ вп}}$ необхідно мати

$$\Delta\rho_{\min} = 4l_{\Pi \text{ вп}} - 2,$$

а для виявлення пакета помилок

$$\Delta\rho_{\min} = 2l_{\Pi \text{ в}} - 4.$$

Може виявитися доцільним, щоб код виправляв пакети помилок довжиною не більше $l_{\Pi \text{ вп}}$ й виявляв одночасно пакети помилок довжиною $l_{\Pi \text{ в}} > l_{\Pi \text{ вп}}$. У цьому випадку значність коду n необхідно вибирати з умови виправлення пакета помилок $l_{\Pi \text{ вп}}$ і потім з умови виявлення пакета помилок $l_{\Pi \text{ в}}$ визначити нову значність коду n' . Якщо

$$n = n' \geq 2l_{\Pi \text{ в}} - 1, \quad (3.30)$$

то код значності n буде відповідати поставленим вимогам; якщо ж $n - n' < 2l_{\text{ПВП}} - 1$, то значність коду треба збільшити, щоб виконувалася нерівність (3.30). Дійсно, величина n вибирається з умови виправлення пакета помилок $l_{\text{ПВП}}$. Тоді коефіцієнти $\rho_{j\zeta}$

$$\rho_{j\nu} \leq \rho_{jj} - \Delta\rho_{\text{мін}} = n - 4l_{\text{ПВ}} + 2.$$

Якщо тепер необхідно додатково виявляти пакети помилок довжини, більшої, ніж $l_{\text{ПВП}}$, то ці додаткові властивості коду будуть визначатися начебто новою, зменшеною значністю $n' \leq n - 2l_{\text{ПВП}} + 1$, звідки випливає умова (3.30).

Приклад 17. Даний (70, 57)-код, що виправляє пакет помилок $l_{\text{ПВП}} = 3$. Визначимо його виявляючі властивості. Відповідно до формули (3.30) $n' = 65$. Такий (65, 57)-код дозволяє виявляти пакет помилок довжиною $l_{\text{ПВ}} = 8$. Таким чином, (70, 57)-код виправляє пакети помилок $l_{\text{ПВ}} = 3$ і одночасно виявляє пакети помилок $l_{\text{ПВ}} = 8$ або тільки виявляє пакети помилок $l_{\text{ПВ}} = 13$. Це відомий код Файра.

3.6. Коди Ріда-Соломона

Важливою і часто використовуваною підмножиною кодів БЧХ є коди Ріда-Соломона. Це такі коди БЧХ, в яких мультиплікативний порядок алфавіту символів кодового слова ділиться на довжину коду. Таким чином, $m=1$ і поле символів $GF(q)$ збігається з полем локаторів помилок $GF(q^m)$. Звичайно ми будемо вибирати α примітивним, тоді

$$n = q^m - 1 = q - 1.$$

Мінімальний багаточлен над $GF(q)$ елемента β , взятого з того самого поля, дорівнює

$$f_{\beta}(x) = x - \beta.$$

Оскільки поле символів і поле локаторів помилок збігаються, всі мінімальні багаточлени лінійні. У кодї Ріда-Соломона, що виправляє t помилок, звичайно покладається $j_0 = 1$, і тоді, породжуючий багаточлен, записується у вигляді

$$g(x) = (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{2t}).$$

Степінь цього багаточлена завжди дорівнює $2t$, звідки слідує, що параметри коду Ріда-Соломона пов'язані співвідношенням

$$n - k = 2t.$$

У кодї Ріда-Соломона можна вибрати також будь-яке інше значення j_0 , причому за допомогою розумного вибору j_0 іноді вдається спростити кодер. Таким чином,

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1}) \dots (x - \alpha^{j_0+2t-1}).$$

Як приклад знайдемо $g(x)$ для (15, 11)-коду Ріда-Соломона з $t = 2$ над $GF(16)$. Може бути обране кожне j_0 ; ми виберемо $j_0 = 1$. Тоді

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + (z^3 + z^2 + 1)x^3 + (z^3 + z^2)x^2 + z^3x + (z^2 + z + 1) = x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10}.$$

Оскільки степінь $g(x)$ дорівнює 4, $n - k = 4$ і $k = 11$. Інформаційний багаточлен являє собою послідовність одинадцяти символів з $GF(16)$, що еквівалентно 44 бітам.

Як другий приклад знайдемо $g(x)$ для (7, 3)-коду Ріда-Соломона з $t = 2$ над $GF(8)$. Може бути обране кожне j_0 ; ми виберемо $j_0 = 4$. Тоді

$g(x) = (x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^0) = x^4 + (z^2 + 1)x^3 + (z^2 + 1)x^2 + (z + 1)x + z$ (тут використане подання елементів поля $GF(8)$ у вигляді багаточленів від z). Інформаційний багаточлен являє собою послідовність трьох вісімкових символів (що еквівалентно дев'яти бітам). Припустимо, що

$$i(x) = (z^2 + z)x^2 + x + (z + 1).$$

Кодове слово несистематичного коду запишеться у вигляді

$$c(x) = i(x)g(x) = (\alpha^4x^2 + x + \alpha^3)(x^4 + \alpha^6x^3 + \alpha^6x^2 + \alpha^3x + \alpha) = \alpha^4x^6 + \alpha x^5 + \alpha^6x^4 + 0x^3 + 0x^2 + \alpha^5x + \alpha^4,$$

що являє собою послідовність семи вісімкових символів.

Коди Ріда-Соломона є оптимальними в змісті границі Сінглтона.

Теорема 10. Код Ріда-Соломона має мінімальну відстань $n - k + 1$ і є кодом з максимальною відстанню.

Доведення. Нехай $d = 2t + 1$ – конструктивна відстань коду. Мінімальна відстань d^* задовольняє нерівності

$$d^* \geq d = 2t + 1 = n - k + 1,$$

оскільки для кодів Ріда-Соломона $2t = n - k$. Але для будь-якого лінійного коду має місце границя Сінглтона

$$d^* \leq n - k + 1$$

Отже, $d^* = n - k + 1$ і $d^* = d$.

Доведена теорема стверджує, що при фіксованих n і k не існує коду, мінімальна відстань якого більше, ніж у коду Ріда-Соломона. Не слід розуміти це твердження буквально. Часто перевага віддається кодам з такими параметрами (n', k') , за яких не існує коду Ріда-Соломона. У той же час коди Ріда-Соломона завжди виявляються коротше всіх інших циклічних кодів над тим же алфавітом.

Розширені коди Ріда-Соломона. До коду Ріда-Соломона в загальному випадку можна додати дві додаткові компоненти; ми будемо завжди поміщати одну з них на початку, а іншу наприкінці кодового слова. Коди,

отримані шляхом додавання однієї або обох додаткових компонентів, називаються *розширеними кодами Ріда-Соломона*. Кожний з доданих символів може використовуватися і як інформаційний, і як перевірочний, тобто або для збільшення швидкості передавання, або для збільшення мінімальної відстані коду. Ми використовуємо цей менш конкретний термін – розширені коди Ріда-Соломона, хоча ці ж коди можна побудувати збільшенням числа слів у кодах Ріда-Соломона з мінімальною відстанню d^* або подовженням кодів Ріда-Соломона з мінімальною відстанню $d^* - 2$. У кожному разі вийде той самий розширений код Ріда-Соломона.

Треба визначити два нових локатори й відповідно ввести нові позначення. Якщо вихідні компоненти нумеруються елементами поля, то для одного нового компонента можна використовувати нульовий елемент поля, так що залишається визначити ще один додатковий символ для іншої. Звичайно використовується символ ∞ . Якщо вихідні компоненти нумеруються показниками степеня примітивного елемента, то для позначення нового локатора не можна використовувати нуль і необхідно ввести два нових символи. У якості цих двох символів ми будемо користуватися знаками – та +. Таким чином, слово розширеного коду записується у вигляді

$$(c_-, c_0, c_1, c_2, \dots, c_{q^m-3}, c_{q^m-2}, c_+),$$

та $n = q^m + 1$. Вектор, що виходить виключенням символів c_- і c_+ , будемо називати *внутрішнім*. Ми будемо вивчати розширені коди за допомогою властивостей перетворень Фур'є внутрішніх векторів, доповнюючи їх властивостями розширеного векторного простору. Коли ми будемо говорити про спектр кодового слова, то будемо мати на увазі спектр внутрішнього вектора.

Спочатку дамо визначення розширеного циклічного коду, а потім – як окремих випадок – визначення розширеного коду Ріда-Соломона.

Визначення 8. Розширеним циклічним (n, k) -кодом над $GF(q)$ називається лінійний код довжини $n = q^m + 1$, кожне слово якого задовольняє наступним умовам: спектр $(C_0, C_1, \dots, C_{n-3})$ кодового слова $(c_-, c_0, c_1, \dots, c_{n-3}, c_+)$ містить нулі в заданій безлічі $n - k - 2$ позицій з індексами j_1, \dots, j_{n-k-2} , а два спектральні компоненти, що залишилися, задовольняють $C_{j_0} = c_-$, $C_{j_{n-k-1}} = c_+$ рівностям.

Розширений циклічний код у загальному випадку не є циклічним.

Визначення 9. Розширеним кодом Ріда-Соломона називається лінійний код довжини $n = q + 1$ над $GF(q)$, спектр кодових слів $(c_-, c_0, c_1, \dots, c_{n-2}, c_+)$ якого за будь-яких цілих j_0 і t задовольняє таким умовам:

- 1) $C_j = 0$, $j = j_0 + 1, \dots, j_0 + 2t - 2$;
- 2) $C_{j_0} = c_-$;

$$3) C_{j_0+2t-1} = c_+.$$

Число $2t+1$ називається конструктивною відстанню розширеного коду Ріда-Соломона. Визначення містить обмеження, які полягають в тому, що $2t-2$ відповідних спектральних компонент повинні дорівнювати нулю, а компоненти, що обрамляють ці $2t-2$ повинні дорівнювати c_- й c_+ відповідно. Ці дві спеціальні частоти називаються *граничними частотами*.

Порівнянно з кодом Ріда-Соломона, що виходить видаленням c_- і c_+ й дорівнюванням нулю спектральних компонентів C_{j_0} і C_{j_0+2t-1} , розширений код Ріда-Соломона завжди містить два додаткових інформаційних символи при незмінній мінімальній відстані. Згодом ми з'ясуємо, що це означає в частотній області, а спочатку наведемо основане на властивостях матриці Вандермонда доведення факту.

Теорема 11. Розширений код Ріда-Соломона над $GF(q)$ є $(q+1, k)$ -кодом з мінімальною відстанню $2t+1 = n-k+1 = q-k+2$.

Доведення. Спочатку припустимо для простоти, що $j_0 = 0$. Перевірочна матриця коду дорівнює

$$H = \begin{bmatrix} -1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 0 & \alpha & \alpha^2 & \dots & \alpha^{q-2} & \alpha^{q-1} & 0 \\ 0 & \alpha^2 & \alpha^4 & \dots & \alpha^{(q-2)^2} & \alpha^{(q-1)^2} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \alpha^{q-k+1} & \alpha^{(q-k-1)^2} & \dots & \alpha^{(q-k-1)(q-2)} & \alpha^{(q-k-1)(q-1)} & 0 \\ 0 & \alpha^{q-k} & \alpha^{(q-k)^2} & \dots & \alpha^{(q-k)(q-2)} & \alpha^{(q-k)(q-1)} & -1 \end{bmatrix}.$$

Якщо будь-які $d-1$ стовпців цієї перевірконої матриці лінійно незалежні, то мінімальна відстань коду дорівнює щонайменше d . Після виключення першого й останнього стовпців будь-яка безліч з $q-k+1$ стовпців утворить матрицю Вандермонда, яка невироджена, і, отже, будь-які $d-1$ внутрішніх стовпців лінійно незалежні. У випадку ж коли вибрана безліч зі $q-k+1$ стовпців містить перший і останній стовпці, відповідний визначник можна обчислити, розкладаючи його за елементами спочатку першого, а потім останнього стовпців. Це приведе до викидання спочатку першого, а потім останнього рядка, і частина, що залишилася, знову приводить до матриці Вандермонда, визначник якої відмінний від нуля. Отже, будь-які $q-k+1$ стовпців лінійно незалежні, і тому мінімальна відстань коду дорівнює щонайменше $q-k+2$.

Далі, якщо $j_0 \neq 0$, то зміни в перевірконій матриці при незмінних першому й останньому стовпцях полягають у тому, що всі її елементи помножуються на α^{j_0} . Це, однак, ніяк не впливає на проведені вище міркування.

На рис. 3.14 зображений кодер у частотній області для розширеного коду Ріда-Соломона. Ми зможемо краще зрозуміти ці коди, якщо будемо представляти їх кодер як модифікацію кодера в частотній області для звичайного коду Ріда-Соломона з мінімальною відстанню d^* . Останній кодер визначається блоком з $d^* - 1$ послідовних частот, в яких стоять нульові компоненти спектра. Інші компоненти спектра набувають довільних значення інформаційних символів з $GF(q)$.

Для розширення цього коду за рахунок збільшення числа інформаційних символів використовуються дві граничні частоти спектра в блоці перевірочних частот спектра, яким надаються довільні значення двох інформаційних символів, причому в часовій області кодове слово теж доповнюється цими двома символами. У результаті виходить розширений код Ріда-Соломона з тією ж мінімальною відстанню d^* , але з двома додатковими інформаційними символами.

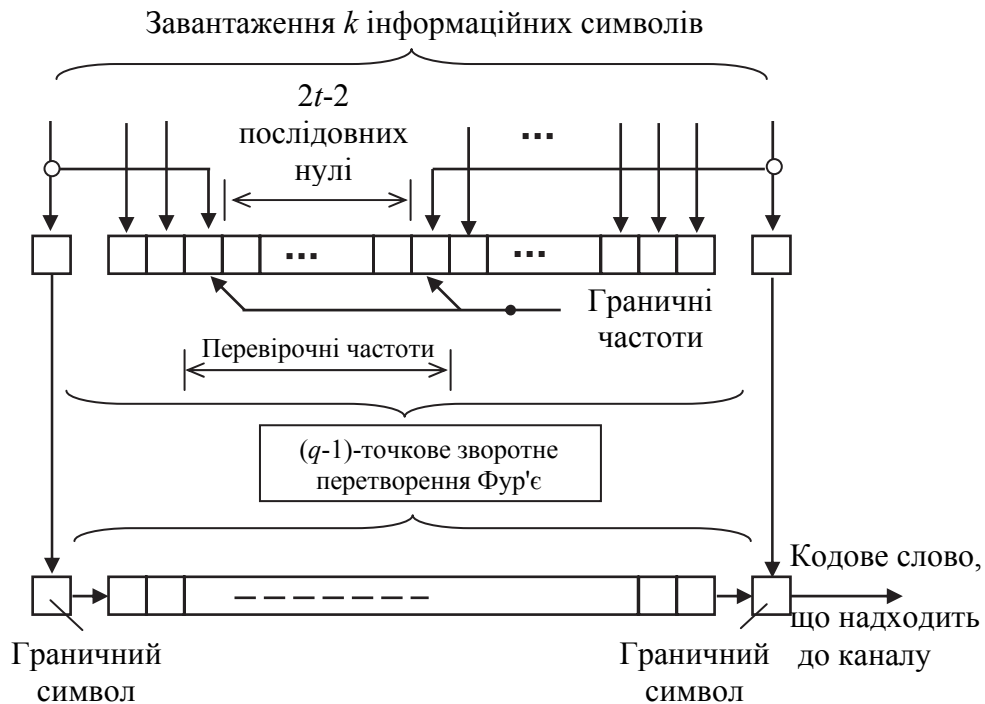


Рисунок 3.14 – Кодер для розширеного коду Ріда-Соломона в частотній області

Якщо ж ми хочемо розширити вихідний код так, щоб збільшити його мінімальну відстань, то два додаткових символи, що приєднуються до блока перевірочних частот, оголошуються новими перевірочними частотами. Значення компонентів цих частот не змінюються, але в часовій області ті ж два символи дописуються до кодового слова. Це призводить до коду з таким самим числом інформаційних символів, як і у вихідного коду, але з мінімальною відстанню $d^* + 2$. Звичайно, ми одержимо той самий розши-

рений код, якщо будемо виходити з коду Ріда-Соломона з мінімальною відстанню $d^* + 2$ й збільшувати в ньому число інформаційних символів.

Кодер розширеного (n, k) -коду Ріда-Соломона в часовій області показаний на рис. 3.15. У цьому випадку розширення розглядається як продовження $(n-2, k)$ -коду Ріда-Соломона з мінімальною відстанню $d^* - 2$ до коду з відстанню d^* . Для кодування k інформаційних символів внутрішнього вектора кодового слова використовується породжуючий багаточлен з коренями $\alpha^2, \dots, \alpha^{2t-1}$. Граничні символи визначаються при цьому відповідно рівностями

$$c_- = \sum_{i=0}^{n'-1} c_i \alpha^i \quad \text{і} \quad c_+ = \sum_{i=0}^{n'-1} c_i \alpha^{2ti}$$

і приєднуються до внутрішнього вектора для формування кодового слова.

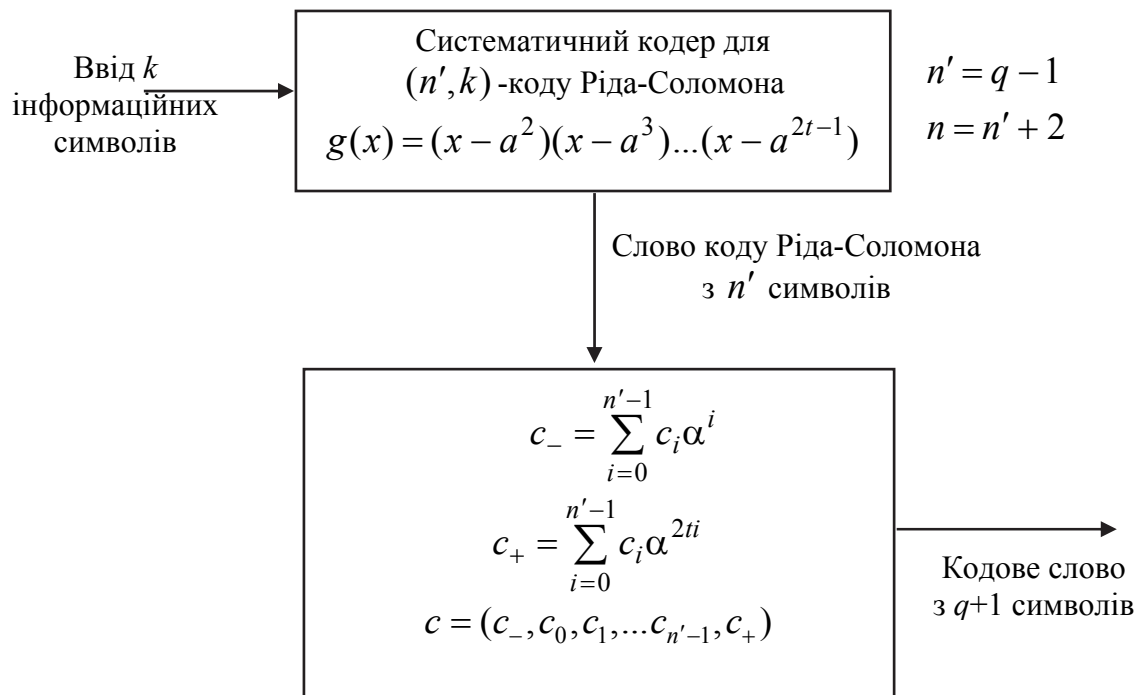


Рисунок 3.15 – Систематичний кодер для розширеного коду Ріда-Соломона

3.8. Декодування за максимумом правдоподібності

Для багатьох блокових і згорткових кодів кодування здійснюється порівняно просто. Значно більш складний процес декодування (n, m) -кодів, виправляючих будь-які з'єднання помилок кратності $r \leq r_0$ за великих значень n і r_0 . Декодуючий пристрій, що реалізує оптимальний алгоритм обробки сигналів, містить дві вирішальні схеми. Перша з них – перший ступінь декодування – слугує для визначення параметра елементарних символів прийнятого кодового слова і входить як складова частина при-

ймального пристрою. В оптимальному випадку сигнал на виході цієї схеми являє собою неперервну випадкову величину, яка містить інформацію про знак і амплітуду випадкового символу. Схема другого ступеня декодування є власно декодуєчим пристроєм, що ототожнює прийняту комбінацію з однією із дозволених кодограм. В оптимальному випадку декодуєчий пристрій повинен мати пам'ять, розраховану на збереження всіх $2m$ кодограм. Декодування полягає в обчисленні $2m$ лінійних сум і визначенні максимальної з них.

Разом з тим тенденція працювати за швидкостей, близьких до пропускної здатності каналу зв'язку, з досить малою ймовірністю помилки викликає необхідність збільшувати значність коду, тому що тільки завдяки кодівці коди мають високу ефективність. Нині в каналах передачі даних часто використовуються коди, які містять блоки по 500 і більше символів. Неважко побачити, що в цьому випадку на кожну кодограму потрібно, принаймні, 2500 операцій.

Методи декодування. Всі методи декодування в залежності від типу вирішальних схем можна поділити на три групи:

1. Схема першого ступеня декодування – неоптимальна, схема другого ступеня – оптимальна.

2. Схема першого ступеня декодування – оптимальна, схема другого ступеня – неоптимальна.

3. Схеми першого і другого ступенів декодування – неоптимальні.

Перша група методів дуже нечисленна. До неї відносяться декодування за максимумом правдоподібності і декодування за допомогою коректора при посимвольному прийомі. Перевага надається тому методу, який вимагає меншого числа операцій, що в свою чергу визначається співвідношенням між числом m інформаційних і r перевірочних символів. Так, якщо $m > r$, то треба здійснювати декодування за допомогою коректора, тому що число операцій в цьому випадку пропорційне $2r < 2m$. Слід підкреслити, що обидва ці методи практично застосовні лише за невеликих довжин кодованих блоків. Схема першого ступеня декодування може також працювати і з великим числом рівнів квантування, але метод декодування за допомогою коректора в цьому випадку не досліджений.

Друга група також містить невелику кількість методів. До них слід віднести метод Вагнера, методи модульного і різницево-модульного декодування, запропоновані Л.Ф. Бородінім, Л.М. Фінком і Б.Д. Каганом.

Найбільш численна третя група, при чому переважного розповсюдження набув посимвольний прийом, коли схема першого ступеня декодування видає сигнали з одним рівнем квантування.

У цьому підрозділі основна увага приділяється методам декодування третьої групи: наведено лише стисла характеристика деяких методів декодування першої і другої групи.

Декодування за максимумом правдоподібності. При передаванні по каналу з шумами кодові слова $X_i = x_1, \dots, x_{n-1}, x_n$, що належить алфавіту A ; на вході приймального пристрою буде деяка комбінація:

$$Z_j = z_1, \dots, z_n = X_i \oplus \Pi_0, \quad (3.31)$$

що належить алфавіту B . Вектор помилок Π_0 буде визначений, якщо для всіх i та j задана матриця умовних ймовірностей $p_{X_i}(Z_j)$ утворена на виході каналу послідовності Z_j , якщо була передана кодограма X_i . Оптимальний приймальний пристрій вибирає в якості рішення ту послідовність X_i , для якої умовна ймовірність $p_{X_i}(Z_j)$ максимальна. Вказаний алгоритм обробки сигналів називається *декодуванням за максимумом апостеріорної ймовірності*.

Згідно з теоремою Байеса, умовна ймовірність:

$$p_{Z_j}(X_i) = \frac{p_{X_i}(Z_j) \cdot p(X_i)}{p(Z_j)}, \quad (3.32)$$

де $p(X_i), p(Z_j)$ – апіорні ймовірності передавання кодограми X_i і отримання послідовності Z_j , ймовірність $p(Z_j)$ можна визначити за формулою повної ймовірності:

$$p(Z_j) = \sum_{X_i \subset A} p_{X_i}(Z_j) p(X_i).$$

Якщо $p(X_i) = \text{const}$, то вираз (3.25а) досягає найбільшого значення лише тоді, коли максимальна ймовірність $p_{X_i}(Z_j)$. Тому в якості розв'язання рівняння необхідно вибирати таку кодограму $X_i \subset A$, яка забезпечує найбільше значення ймовірності $p_{X_i}(Z_j)$. Такий алгоритм оброблення сигналів дістав назву *декодування за максимумом правдоподібності*. Відзначимо, що цей алгоритм справедливий і при нерівномірному законі розподілу повідомлень.

При рівноймовірних повідомленнях декодування за максимумом апостеріорної ймовірності і максимумом правдоподібності оптимальні в тому розумінні, що вони мінімізують ймовірність $P_0(X_i)$ спотворення кодограми X_i і, таким чином, середню ймовірність помилки за ансамблем повідомлень:

$$p_0(A) = \sum_{X_i \subset A} p_0(X_i).$$

Якщо канал симетричний і без пам'яті, то ймовірність:

$$p_{X_i}(Z_j) = \prod_{v=0}^{n-1} p_{x_v}(z_v),$$

де $p_{x_v}(z_v)$ – умовна ймовірність появи символу $z_v \subset Z_j$, при передаванні символу $x_v \subset X_i$. Тому що канал симетричний, то

$$p_{x_v}(z_v) = \begin{cases} p_e & \text{за } z_v \neq x_v, \\ 1 - p_e & \text{за } z_v = x_v. \end{cases}$$

При кількості помилок t_k ймовірність

$$p_{X_i}(Z_j) = p_e^{t_k} (1 - p_e)^{n-t_k},$$

є монотонною спадною функцією r . Тому декодування за максимумом правдоподібності в ДСК зводиться до вибору в якості рішення такої кодограми $X_i \subset A$, яка відстоїть від прийнятої послідовності $Z_j \subset B$ на мінімальній відстані. Тому такий алгоритм оброблення сигналів називається *декодуванням за мінімумом кодової відстані*.

Декодування за допомогою коректора. Розподіл кодових слів за областями рішень, що характеризується нормальною таблицею декодування, дозволяє сформулювати алгоритм оброблення сигналів у такому вигляді: розв'язанням рівняння (3.31) є кодограма $X_i \subset A$, яка знаходиться в тому самому стовбці нормальної таблиці декодування (НТД), що й прийнята послідовність $Z_j \subset B$. Очевидно, що це правило збігається з декодуванням за максимумом правдоподібності і, таким чином, є оптимальним.

Процедура декодування буде аналогічною, якщо використовувати однозначну відповідність між коректорами (синдромами) S_0 і головними елементами відповідних суміжних класів, що містять прийняті послідовності Z_j :

$$S_0 = Z_j \|H_{n,m}\| = \Pi_{0j} \|H_{n,m}\|.$$

За знайденим коректором визначається вектор помилки Π_{0j} і потім передана кодограма $X_i = Z_j \oplus \Pi_{0j}$. Очевидно, що декодування за допомогою коректора збігається з декодуванням за максимумом правдоподібності.

При декодуванні за допомогою коректора найбільш складною в технічному відношенні операцією, що визначає складність усього кодоперетворювача, є визначення відповідного коректора вектора помилок. Ця задача розв'язується порівняно просто тільки для помилок кратності $t_k = 1$, коли всі вектори мають одиничну вагу; в цьому випадку всі коректори збігаються з рядками перевірконої матриці $H_{n,k}$.

Приклад 18. Закодуємо повідомлення $S = 1101$ (7, 4)-кодом з алгоритмом: $x_3=134$, $x_6=124$, $x_7=123$. Тоді кодограма $X = 1101010$. Для послідовності одиничних помилок, починаючи зі старшого розряду, отримаємо коректори $S_{01} = 111$, $S_{02} = 011$, $S_{03} = 101$, $S_{04} = 110$, $S_{05} = 100$, $S_{06} = 010$. Відшукування векторів помилок різко ускладнюється за кратності помилок $t_k > 1$ і за достатньо великих n і t_k для блокових кодів, що не мають властивості циклічності, стає практично неможливим.

Циклічність коду у багатьох випадках суттєво спрощує процедуру побудови коректора, визначення відповідного вектора помилки і виправлення спотвореного символу.

Кодові слова циклічних кодів мають дві властивості, які лежать в основі виявлення і виправлення помилок:

– кодові поліноми $f_j(x)$, відповідні кодограмам, ортогональні перевірочному поліному $h(x)$:

$$f_j(x)h(x) = 0; \quad (3.33)$$

– кодові поліноми $f_j(x)$ діляться без остачі на породжуючий поліном $g(x)$:

$$\frac{f_j(x)}{g(x)} = q(x).$$

Розглянемо декодування циклічних кодів, засноване на множенні на перевірочний поліном.

Дія завади $p_i(x)$ приводить до створення на вході декодуючого пристрою поліному:

$$Z(x) = f_j(x) \oplus p_i(x).$$

При множенні на поліном $h(x)$ з урахуванням (3.33) отримаємо

$$Z(x)h(x) = p_i(x)h(x).$$

Таким чином, кодовий поліном $f_j(x)$ виявився заміненим і утворився поліном:

$$S_{0i}(x) = p_i(x)h(x).$$

Якщо $S_{0i}(x) \neq 0$, то це свідчить про наявність помилок у прийнятій кодограмі; рівність $S_{0i}(x) \neq 0$ вказує на відсутність спотворень. Вираз $S_{0i}(x)$ можна подати

$$S_{0i}(x) = h(x)[p_i(x) \oplus g(x)q(x)].$$

Звідси виходить, що для всіх j добуток:

$$p_{ij}(x) = h(x)[p_i(x) \oplus g(x)q_j(x)] = S_{0i}(x).$$

Тут поліном $p_{ij}(x)$ відображає кодограми суміжного i -го класу, а поліном $S_{0i}(x)$ – головний елемент цього класу. Число поліномів $p_{ij}(x)$ при фіксованому i дорівнює числу $2m$ кодових поліномів $f(x)$. Тому $S_{0i}(x)$ може слугувати коректором, оскільки кожному поліному помилки $p_{ij}(x)$ відповідає свій поліном $S_{0i}(x)$.

Очевидно, що два поліноми помилки $p_1(x)$ і $p_2(x)$ будуть різні при декодуванні, якщо $p_1(x)h(x) \neq p_2(x)$. Припустимо, що різні поліноми помилки $p_i(x)$ $p_t(x)$, де $t = 1, 2, \dots, n - 1$. Тоді поліном коректора:

$$S_{0i}^{(t)}(x) = x^t S_{0i}(x),$$

звідки:

$$S_{0i}(x) = x^{-t}(t)S_{0i}^{(t)}(x).$$

Тут знак мінус в показнику степеня означає циклічний зсув коефіцієнтів поліному $S_{0i}^{(t)}(x)$ на t тактів праворуч, внаслідок чого утворюється поліном $S_{0i}(x)$.

Таким чином, процедура декодування зводиться до наступного:

– прийнята послідовність символів Z_i помножується на перевірочний поліном $h(x)$ і визначається поліномом $S_{0i}^{(t)}(x)$;

– якщо $S_{0i}^{(t)}(x) \neq 0$, то циклічним зсувом його формується поліном $S_{0i}(x)$, що відповідає вектору помилки $p_i(x)$;

– у складі кодоперетворювача є спеціальний пристрій – *селектор*, настроєний на певне значення $S_{0i}(x)$; в момент утворення коректора $S_{0i}(x)$ селектор формує символ 1, що збігається за часом зі спотвореним розрядом комбінації Z_i і підсумовуванням за mod 2, ця помилка усувається.

Приклад 19. Розглянемо роботу декодуючого циклічного (7, 4)-коду множенням на перевірочний поліном $h(x) = 10111$ (рис. 3.66). Спочатку ключ $Кл_1$ установлюється в положення "1", ключ $Кл_2$ розімкнений і кодограма Z уводиться в комірки регістру P_1 багатотактного кодового фільтра. Потім ключ $Кл_2$ замикається і після семи тактів роботи в регістрі P_2 буде записаний поліном $S_{0i}^{(t)}(x) = p_i(x)h(x)$. Потім ключ $Кл_1$ переводиться в положення "2", ключ $Кл_2$ розмикається, і символи кодограми Z починають надходити через суматор C_0 на вихід пристрою. Одночасно в регістрі P_2 здійснюється циклічний зсув поліному $S_{0i}^{(t)}(x)$. Припустимо, що передавалася кодограма $X = 1101001$, прийнята комбінація $Z = 1101101$, а селектор настроєний на комбінацію 0010111.

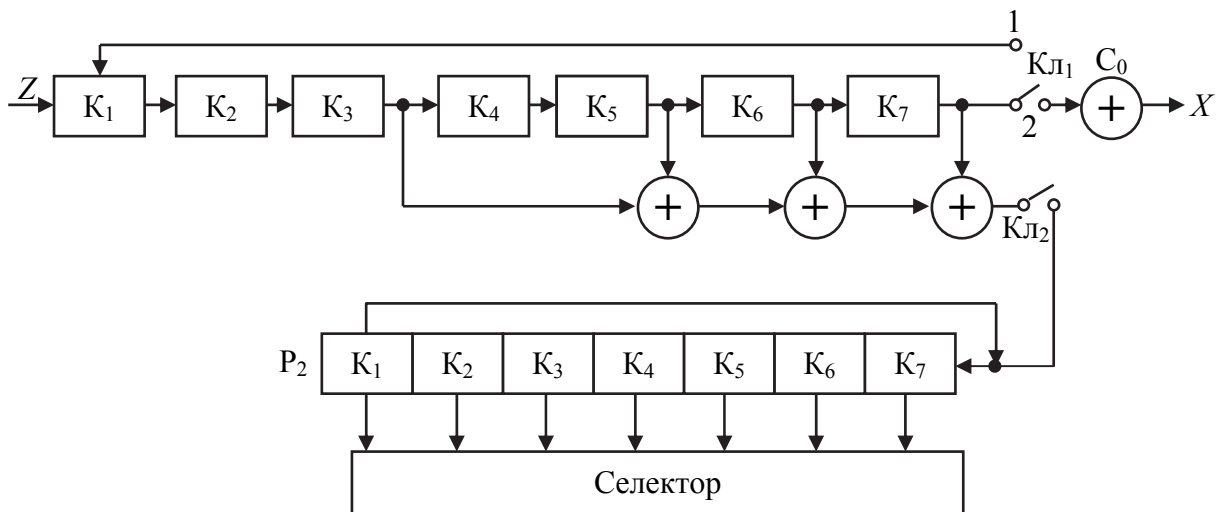


Рисунок 3.16 – Декодуючий пристрій циклічного (7, 4)-коду з множенням на поліном $h(x) = 10111$

Процес роботи схеми ілюструється табл. 3.13, звідки видно, що після 7 тактів роботи в регістрі P_2 буде записаний поліном, а спотворений символ знаходиться в комірці K_3 регістра P_1 . Після $t = 5$ тактів циклічної перестановки в селектор надійде комбінація 0010111, селектор видасть на суматор S_0 символ 1, який збігається за часом із символом 1 комірки K_3 , і помилка буде виправлена.

Розглянемо декодування циклічних кодів, засноване на діленні на породжуючий поліном. Після ділення $Z(x)$ на $g(x)$ отримаємо:

$$[K(x) + Q(x)]g(x) + R(x) = f(x) + p_i(x),$$

де $K(x)$ – інформаційні символи (поліном ненадлишкового коду); $Q(x)$, $R(x)$ – частка і остача від ділення $Z(x)$ на $g(x)$. Умова $R(x) \neq 0$ свідчить про наявність спотворень, а рівність $R(x) = 0$ – про їх відсутність. Оскільки окремо фіксуються лише $K(x) + Q(x)$ і $R(x)$, то корекція помилок зводиться до визначення за остачею $R(x)$ або вектора помилок $p_i(x)$, або поліному $Q(x)$.

Таблиця 3.13 – Ілюстрація роботи схеми згідно з рис. 3.16

Регістр P_1							Регістр P_2						
K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_1	K_2	K_3	K_4	K_5	K_6	K_7
1	0	1	1	0	1	1	0	0	0	0	0	0	0
1	1	0	1	1	0	1	0	0	0	0	0	0	1
1	1	1	0	1	1	0	0	0	0	0	0	1	0
0	1	1	1	0	1	1	0	0	0	0	1	0	1
1	0	1	1	1	0	1	0	0	0	1	0	1	1
1	1	0	1	1	1	0	0	0	1	0	1	1	1
0	1	1	0	1	1	1	0	1	0	1	1	1	0
1	0	1	1	0	1	1	1	0	1	1	1	0	0

Приклад 20. Розглянемо роботу декодуючого пристрою циклічного (7, 4)-коду діленням на породжуючий поліном $g(x) = 1011$ (рис. 3.17). Спочатку ключі $K_{л1}$ та $K_{л2}$ розімкнені і кодограма Z , що приймається, протягом $n = 7$ тактів одночасно надходить до буферного регістру P_1 та до регістру P_2 , де до моменту заповнення комірок регістру P_1 буде записана остача $R(x)$. Потім ключі $K_{л1}$ та $K_{л2}$ замикаються і кодограма через суматор S_0 починає надходити на вихід пристрою. Одночасно в регістрі P_2 відбувається рециркуляція остачі $R(x)$ і в момент формування коректора $S_0(x)$, на який настроєний селектор, на суматор S_0 подається символ 1, і помилка виправляється. Табл. 3.14 ілюструє роботу схеми при $X = 1101001$, $Z = 1101101$ та настроюванні селектора на $S_0 = 100$. Остача $R(x) = 001$ через 5 тактів циркуляції (вектор помилки 0000100) створює комбінацію S_0 .

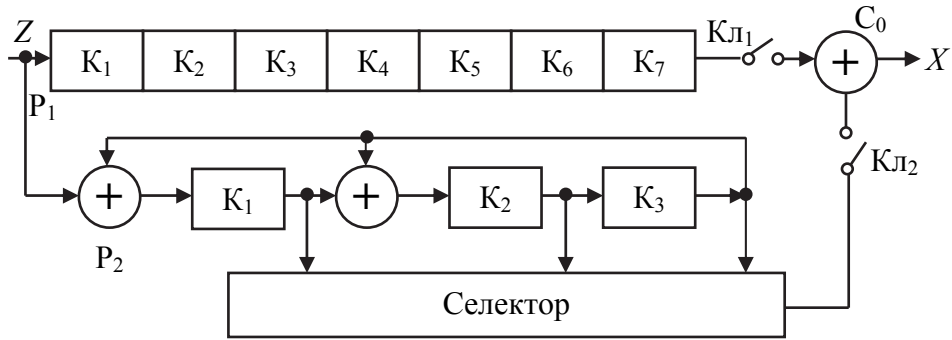


Рисунок 3.17 – Декодуєчий пристрій циклічного (7, 4)-коду з діленням на поліном $g(x) = 1011$

Найбільші ускладнення викликає побудова селектора, складність якого залежить від характеру і числа помилок, що виправляються.

Таблиця 3.14 – Ілюстрація роботи схеми згідно з рис. 3.17

Регістр P ₁							Регістр P ₂		
K ₁	K ₂	K ₃	K ₄	K ₅	K ₆	K ₇	K ₁	K ₂	K ₃
1	0	0	0	0	0	0	1	0	0
1	1	0	0	0	0	0	1	1	0
0	1	1	0	0	0	0	0	1	1
1	0	1	1	0	0	0	0	1	1
1	1	0	1	1	0	0	0	1	1
0	1	1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	0	0	1

Метод декодування Вагнера. Для всіх розглянутих методів декодування виправлення помилок кратності $t_k \leq t_0$ є подією достовірною. На відміну від цього при методі Вагнера помилка виправляються з деякою ймовірністю, залежною від рівня завад в каналі зв'язку. Принцип методу Вагнера полягає в наступному. Двійкова послідовність з виходу схеми першого ступеня декодування перевіряється на парність. Якщо перевірки задовольняються, то кодограма видається отримувачу. Якщо ж виявлена r -кратна помилка, то значення символів, що мають найменшу апостеріорну ймовірність, змінюються на протилежні. Таким чином, перевірки на парність тут слугують тільки для визначення числа спотворених символів, а не для визначення їх номерів. Такий метод дозволяє з високою ймовірністю виправляти помилки кратності $t_k \leq \frac{d_0}{2}$ за достатньо малої надлишковості. Проте технічно реалізувати декодувальний пристрій складно і, крім того, ймовірність правильного рішення залежить від інтенсивності завад. Тому метод Вагнера доцільно використовувати в каналах з низьким рівнем шумів, коли основне значення має швидкість передавання інформації.

Мажоритарне декодування при посимвольному прийомі. Мажоритарний принцип декодування, заснований на ухваленні рішення за більшістю однойменних результатів, являє собою неоптимальний алгебраїчний метод оброблення сигналів і забезпечує суттєве спрощення схемних рішень.

До числа позитивних якостей мажоритарного декодування належать:

- простота схеми приймального кодоперетворювача;
- можливість порівняно простого переходу від виправлення помилок до стирання недостовірних символів;
- здатність виявляти збої і відмови елементів апаратури за рахунок уведення схемної надлишковості кодоперетворювачів.

Разом з тим усі відомі коди, що допускають мажоритарне декодування, не є асимптотично оптимальними, проте при $n \approx 100 \dots 500$ багато з них близькі до оптимальних.

Розділені перевірки. Нехай $X = x_{n-1}, \dots, x_1, x_0$ – кодограма (n, m) -коду. Перевірочні символи виражаються через інформаційні за допомогою лінійно-незалежних співвідношень вигляду:

$$h_{i,n}x_n \oplus h_{i,n-1}x_{n-1} \oplus \dots \oplus h_{i,1}x_1 \oplus, \quad (3.34)$$

де $i = 1, 2, \dots, k$. Коефіцієнти, $h_{i,j} = 0, 1$ утворюють стовпці перевіркової матриці:

$$H_{n,k} = \begin{pmatrix} h_{11} & h_{21} & \dots & h_{k1} \\ \dots & \dots & \dots & \dots \\ h_{1n} & h_{2n} & \dots & h_{kn} \end{pmatrix},$$

що являють собою рівняння перевірок (3.34).

Лінійні комбінації стовпчиків матриці $H_{n,k}$ знов утворюють перевірочні співвідношення. Виконавши μ лінійних операцій над стовпчиками матриці, побудуємо нову матрицю:

$$\Theta_{v,1} = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \dots & \alpha_{1\mu} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{n\mu} \end{pmatrix},$$

що має дві властивості:

- v -й рядок містить тільки одиничні символи;
- будь-який інший рядок містить не більше одного одиничного символу.

Матриця $\Theta_{v,1}$ визначає μ рівнянь перевірок для символу x_v . Додавши рівняння тривіальної перевірки, отримаємо систему $\mu + 1$ рівнянь перевірок.

Згідно з властивостями матриці $\Theta_{v,1}$, будь-який кодовий символ входить не більше ніж в одне рівняння перевірки. Така сукупність перевірок називається системою *розділених (ортогональних) перевірок* (СРП) щодо символу x_v .

Принцип мажоритарного декодування полягає в наступному. Якщо підставити прийняті символи в рівняння перевірок (3.34) для x_v , то за відсутності спотворень всі $\mu + 1$ рівнянь дадуть однакоє правильне значення x_v . Одиначна помилка спотворить тільки одне перевірочне співвідношення: r -кратна помилка спричинить спотворення r рівнянь. Рішення про значення символу x_v будемо приймати за більшістю однойменних результатів перевірок, що фіксуються мажоруючим елементом схеми приймального кодоперетворювача. Отже, символ x_v буде декодований правильно, якщо число помилок $r \leq \frac{\mu}{2}$. При $r = \frac{\mu + 1}{2}$ символ буде декодований правильно, якщо в одному рівнянні перевірки виявилось не менше двох спотворених символів або буде виявлена (але не виправлена) помилка.

Для блокових (n, m) -кодів необхідно побудувати μ (m або n) систем СРП і відповідних їм схем. Якщо кожна з СРП містить не менш $\mu + 1$ розділених перевірок, то кодова відстань d_p , що реалізовується для виправлення помилок, повністю відповідає дійсній відстані d_0 , тобто

$$d_p = d_0 = \mu + 1.$$

Проте за великих значень m або n декодувальний пристрій виходить громіздким. Підкреслимо, що при мажоритарному декодуванні основне значення має кодова відстань, що реалізовується d_p .

Приймальний кодоперетворювач суттєво спрощується для циклічних і згорткових кодів, для яких властивість циклічності кодограм розповсюджується на СРП. Це означає, що якщо відома система нетривіальних перевірок для символу x_v , то для побудови системи нетривіальних перевірок для символу x_{v+1} досить здійснити одночасно циклічний зсув на один такт усіх стовпців матриці θ_{v1} , що відповідає збільшенню індексів всіх символів на одиницю.

Мажоритарний декодуєчий пристрій для циклічних кодів реалізується таким чином. Кодограма, що приймається, записується в регістр зсуву, що містить n комірок. Певні регістри комірки пов'язуються між собою за допомогою суматорів за $\text{mod } 2$, утворюючи $\mu + 1$ схем рівнянь перевірок для символу x_v . Виходи цих схем подаються на мажоруючий елемент (МЕ), що видає значення x_v . При циклічних зсувах символів, записаних в регістрі, на виході МЕ послідовно будуть формуватися символи x_{v+1} , x_{v+2} ...

Приклад 21. Побудуємо мажоритарний приймальний кодоперетворювач циклічного $(7, 3)$ -коду, заданого поліномом $g(x) = 10111$, що використовує розділені перевірки. Перевірочна матриця H_{74} і матриці θ_{v1} для символів x_1 , x_2 , x_3 будуть:

$$H_{7,4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \theta_{1,1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}; \theta_{2,1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}; \theta_{3,1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

звідки рівняння СРП мають вигляд:

$$\begin{aligned} x_1 &= x_1; & x_2 \oplus x_4; & & x_3 \oplus x_7; & & x_5 \oplus x_6 = 1; & & 24; & & 37; & & 56; \\ x_2 &= x_2; & x_3 \oplus x_5; & & x_4 \oplus x_1; & & x_6 \oplus x_7 = 2; & & 35; & & 41; & & 67; \\ x_3 &= x_3; & x_4 \oplus x_6; & & x_2 \oplus x_5; & & x_7 \oplus x_1 = 3; & & 46; & & 25; & & 71. \end{aligned}$$

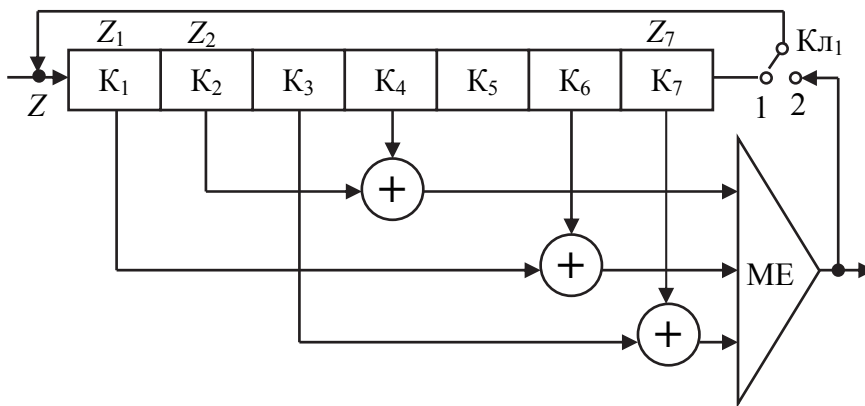


Рисунок 3.18 – Мажоритарний декодуєчий пристрій циклічного (7, 3)- коду з розділеними перевірками

Оскільки число нетривіальних перевірок $\mu = 3$, та кодова відстань $d_p = 4$ і, отже, код виправляє одиночні помилки. Схема кодоперетворювача зображена на рис. 3.18. При положенні «1» ключа $K_{Л1}$ здійснюється циклічний зсув записаних в реєстрі символів. Оскільки декодування відбувається послідовно, то в положенні «2» ключа $K_{Л1}$ в реєстр можуть вводитися виправлені символи замість записаних в ньому спотворених символів.

Розглянутий метод побудови матриць $\theta_{v,1}$ для виправлення помилок легко розповсюдити на канали зі стиранням символів. Для цього досить не враховувати рівнянь перевірок, що містять стерті символи, і приймати рішення за більшістю залишених перевірок. Тоді при r спотвореннях і t стираннях помилка при реєстрації символу x_v буде виправлена, якщо

$$2r + t \leq \mu.$$

Дійсно, t стертих символів входять в $t^* \leq t$ рівнянь перевірок і після їх відкидання залишається $\mu + 1 - t^* \geq \mu + 1 - t \geq 2r + 1$ рівнянь перевірок.

Оскільки r помилок порушують не більше r з залишених рівнянь перевірок, то символ x_v може бути виправлений.

Зв'язні перевірки. Побудувати схему мажоритарного декодування, що реалізовує мінімальну кодову відстань d_0 використовуючи СРП, можна не для будь-яких кодів, оскільки умови, накладені на матрицю $\theta_{v,1}$, дуже жорсткі. Наприклад, не існує СРП для циклічного $(7, 4)$ -коду, заданого поліномом $g(x) = 1011$. В цьому випадку слід відмовитися від СРП, послабивши другу вимогу до матриці $\theta_{v,1}$.

Нехай кожен символ, окрім x_v , може, входити не більше ніж в λ_3 рівнянь перевірок. Тоді одинична помилка спотворить не більше λ_3 рівнянь перевірок, а r -кратна помилка – не більше $r\lambda_3$ рівнянь. Параметр λ_3 називається *коефіцієнтом зв'язності перевірок*, а відповідні системи перевірок – *системами λ_3 -зв'язних перевірок* (СЗП).

При λ_3 -зв'язних перевірках матриця $\theta_{v,\lambda}$ містить в v -му рядку тільки одиничні елементи, а в решті рядків – не більше λ_3 одиничних елементів. Очевидно, що СЗП є узагальненням СРП, для якої $\lambda_3 = 1$.

Для реалізації кодової відстані $d_p = d_0$ досить мати не більше

$$\mu_{\max} = \lambda_3(d_p - 2) + 1$$

нетривіальних рівнянь перевірок. Мінімальна кодова відстань, що реалізується, при зв'язних перевірках:

$$d_{p\min} \geq \left\lfloor \frac{\mu - 1}{\lambda_c} \right\rfloor + 2,$$

де $\lfloor \rfloor$ означає найближче менше ціле число. Якщо за числом помилок, що виправляються $r < d_p - 1$, окрім символу x_v існують r символів, спотворення яких викликає порушення $r\lambda_3$ рівнянь перевірок, то говоритимемо про систему λ_3 -зв'язних перевірок першого типу (СЗП₁); інакше будемо мати систему λ_3 -зв'язних перевірок другого типу (СЗП₂). Для СЗП₂ число порушених рівнянь перевірок не більше, ніж для СЗП₁ за однакових значень r і λ_3 ; при $\lambda_3 = 1$ СЗП₂ не існує. Тому умова для μ_{\max} , залишаючись достатньою, не є необхідною. Дійсно, якщо r -кратна помилка порушує менш $r\lambda_3$ рівнянь перевірок, то при $d_p = 2r + 1$ для виправлення $r_1 \leq r$ помилок потрібно мати $\mu < \lambda_3(d_p - 2) + 1$ рівнянь перевірок.

Приклад 22. Побудуємо мажоритарний декодуючий пристрій циклічного $(7, 4)$ -коду, заданого поліномом $g(x) = 1011$, з використанням системи двозв'язних перевірок. Матриці $H_{7,3}$ і $\theta_{1,2}$ мають вигляд:

$$H_{7,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}; \quad \theta_{1,2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

звідки система нетривіальних перевірок для символу x_1 при $\lambda_3 = 2$ буде:

$$\begin{aligned} x_1 = x_2 \oplus x_3 \oplus x_6; x_3 \oplus x_4 \oplus x_5; x_4 \oplus x_6 \oplus x_7; x_2 \oplus x_5 \oplus x_7 = \\ = 236; 345; 467; 257. \end{aligned} \quad (3.35)$$

У даному випадку $\mu = 4$ і на підставі умови для $d_{0\text{мін}}$ відстань, що реалізується $d_p = d_0 = 3$. Проте згідно з формулою для $\mu_{\text{макс}}$ досить взяти $\mu = 3$ і, отже, одну нетривіальну перевірку можна відкинути, замінивши її тривіальною перевіркою $x_1 = x_1$. Так, у схемі кодоперетворювача, зображеній на рис. 3.19, опущена перевірка $x_1 = x_4 \oplus x_6 \oplus x_7$.

Рівняння перевірок (3.35) лінійно-залежні (сума їх тотожно дорівнює нулю). Тому будь-які три перевірки містять інформацію про четверту перевірку, і відкидання однієї нетривіальної перевірки не знижує в даному випадку коригуючої здатності коду, спрощуючи одночасно схему кодоперетворювача.

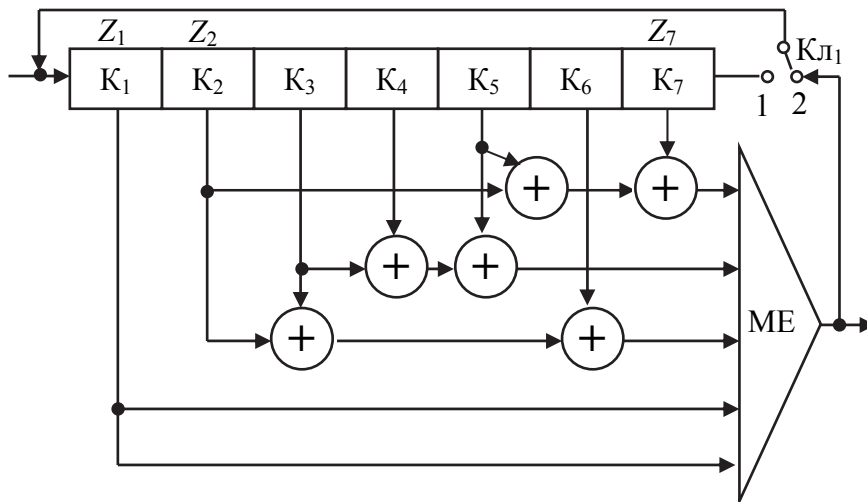


Рисунок 3.19 – Мажоритарний декодуєчий пристрій циклічного (7, 4)-коду з двозв'язними перевірками

Проте не завжди можна відкидати перевірки, які є лінійною комбінацією інших перевірок. У ряді випадків сигнали на вході МЕ повинні залишатися залежними, інакше надлишковість коду використовуватиметься не повністю.

Приклад 23. Для циклічного (15,10)-коду з перевірочним поліномом $h(x) = 10100110111$ можна побудувати нетривіальні трив'язні перевірки для символу x_1 : $x_1 = 2, 3, 5, 6, 9, 11; 2, 4, 5, 8, 10, 12; 2, 5, 7, 12, 13, 14; 3, 4, 7, 9, 14, 15; 3, 8, 9, 10, 12, 13; 4, 6, 11, 12, 13, 15; 6, 7, 8, 10, 11, 14$. Спотворення двох будь-яких символів порушить 4 рівняння перевірок. Тому двократне використання тривіальної перевірки $x_1 = x_1$ дозволяє виправляти всі одиничні і виявляти всі подвійні помилки. Оскільки $k = 5$, то частина нетривіальних рівнянь перевірок лінійно-залежна (наприклад $\mu_3 = \mu_2 + \mu_4 + \mu_5$; $\mu_6 = \mu_1 + \mu_2 + \mu_5$; $\mu_7 = \mu_1 + \mu_2 + \mu_4$).

Проте вилучення будь-якої залежної перевірки знизить коригуючу здатність коду, оскільки при цьому не виявлятимуться всі подвійні помилки.

Квазірозділені перевірки. Більш широкими можливостями для побудови мажоритарних декодуючих пристроїв, що реалізують квазірозділені перевірки (КРП). Вони являють собою рівняння відносно лінійної комбінації (суми за mod 2) v будь-яких символів. Для цього v рядків у матриці $\theta_{v,1}$, що відповідають номерам цих символів, повинні складатися з одних одиничних елементів, а решта рядків повинна містити не більше одного одиничного елемента. Для КРП також зберігається властивість циклічності щодо всіх символів, що входять у визначувану лінійну комбінацію.

Приклад 24. Для циклічного (15, 5)-коду, заданого поліномом $g(x) = 10100110111$, перевірочна матриця (записана в транспонованій формі) має вигляд:

$$H_{15,10}^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Підсумовуючи рядки матриці $H_{15,10}^T$ з номерами 1, 2, 3, 4, 6, 8, 9, 10; 1, 2, 3; 1, 2, 3, 4; 1, 2, 4, 5, 6; 1, 2, 3, 4, 6, 7, 8; 1, 2, 3, 4, 6, 8, 9, отримаємо матрицю $\theta_{2,1}^T$ для суми символів $x_1 \oplus x_2$:

$$\theta_{2,1}^T = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Будь-яка помилка кратності $r \leq 3$ порушить не більше трьох рівнянь і з урахуванням тривіальної перевірки $x_1 \oplus x_2 = x_1 \oplus x_2$ сума цих символів буде визначена правильно. Циклічний зсув утворює системи КРП для сум символів $x_2 \oplus x_3, x_3 \oplus x_4$ і т.д., що дозволяє визначити значення $x_1 \oplus x_2 = a_1, x_2 \oplus x_3 = a_2$ і т.д.

Схема мажоритарного декодування при КРП складніша, ніж при СРП, причому складність її зростає зі збільшенням числа символів v у певній лінійній комбінації. Проте використання суматорів за mod 2 з числом входів більше двох суттєво спрощує схему.

Квазізв'язні перевірки. Найбільш загальним видом перевірок є квазізв'язані перевірки (КЗП), за яких матриця $\theta_{v,\lambda}$ в v рядках містить тільки одиничні елементи, а в решті рядків – не більше λ_3 одиничних векторів. Надалі для укавання системи перевірок будемо використовувати позначення $S(v,\lambda)$, де $S(1,1)$ відповідає СРП, $S(1,\lambda)$ – СЗП, $S(v,1)$ – КРП і $S(v,\lambda)$ – КЗП.

Метод ортогоналізації перевірок у k -кроків. Розглянемо найбільш універсальний метод побудови схеми мажоритарного декодування, що реалізує величину d_0 , називаний методом ортогоналізації перевірок у k -кроків.

Поставимо задачу синтезувати мажоритарний декодуючий пристрій, що реалізує кодову відстань $d_p = d_0$. Нехай задана перевірочна матриця H_{nk} . Якщо не можна скласти систему перевірок $S(1,\lambda)$, то слід побудувати систему $S(v,\lambda)$, що реалізує відстань d_0 . Для цього за допомогою мажоритарних схем заздалегідь необхідно знайти значення сум типу $x_i \oplus x_j = a_\zeta$ (приклад 24). Ці співвідношення можна розглядати як додаткові перевірки, подавши їх матрицею такого вигляду:

$$H_d = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & a_4 & \dots & \dots & \dots & \dots \end{pmatrix}$$

Приєднавши H_d до H_{nk} отримаємо матрицю H'_{nk} з великим значенням μ і знову спробуємо побудувати систему $S(1,\lambda)$. Якщо на даному етапі задача не розв'язується, знаходимо нову систему $S(v,\lambda)$, яка реалізує відстань d_0 , переходимо до матриці H''_{nk} і т.п. Якщо після K кроків отримаємо матрицю H^K_{nk} , яка дозволяє побудувати систему перевірок $S(1,\lambda)$, то процес ортогоналізації перевірок закінчений. Якщо ж за допомогою ма-

триці H_{nk}^ζ не можна побудувати ні систему $S(1, \lambda)$, ні систему $S(v, \lambda)$, то за K кроків неможливо синтезувати мажоритарний декодуєчий пристрій, що реалізує відстань d_0 . Зазначимо, що ортогоналізації в $K=1$ кроків відповідає побудова системи $S(1, \lambda)$ безпосередньо із матриці H_{nk} . Найбільш простий пристрій отримуємо при системі перевірок $S(1, \lambda)$; складність приймального кодоперетворювача швидко зростає зі збільшенням v .

Приклад 25. Для циклічного (15, 5)-коду, заданого поліномом $g(x) = 10100110111$, матриця:

$$H_d = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ a_1 & a_2 & a_3 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_{14} & a_{15} \end{pmatrix}$$

Оскільки в загальному випадку $a_1, a_2, \dots \neq 0$ 16-й рядок матриці відповідає вільним числам перевірки. Приєднуючи матрицю H_d до матриці $H_{15,10}$, отримаємо матрицю $H'_{15,10}$, в якій число рівнянь перевірок $\mu > 10$. Система перевірок $S(1, 1)$ або не існує для всіх символів, або вона існує для будь-якого символу, оскільки матриця $H'_{15,10}$ містить усі циклічні зсуви $S(1, 1)$. Підсумовуючи стовпці матриці $H'_{15,10}$ з номерами 2, 6, 8, 9, 10, 12, 13; 1, 2, 6, 8, 9, 10, 11, 13; 1, 5, 6, 8, 9, 10, 11, 12; 3, 5, 6, 8, 9, 10, 13; 1, 2, 3, 4, 6, 8, 9, 10, 11; 2, 3, 4, 5, 7, 9, 10, 12, отримаємо матрицю $\theta'_{1,1}$, що визначає рівняння перевірок систем $S(1, 1)$ щодо символу x_{15} :

$$\begin{aligned} x_{15} &= x_{15}; & x_5 \oplus a_2 \oplus a_3; & x_6 \oplus a_1 \oplus a_3; & x_7 \oplus a_1 \oplus a_2; & x_9 \oplus a_3; \\ x_{10} \oplus a_1; & x_{13} \oplus a_2 \end{aligned} \quad (3.36)$$

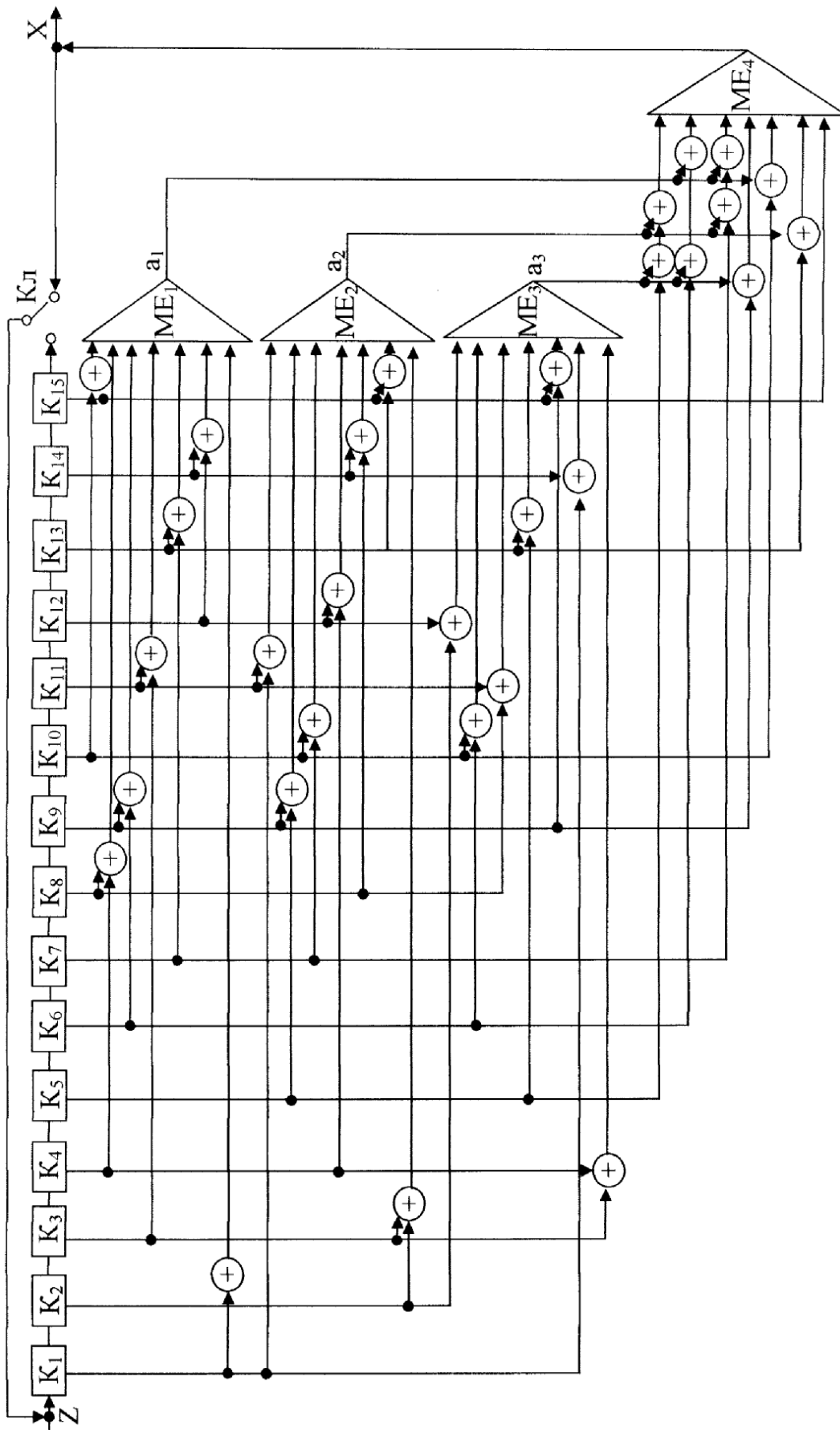


Рисунок 3.20 – Мажоритарний декодувальний пристрій циклічного (15, 5)-коду з ортогоналізацією перевірок у два кроки

Якщо відомі значення a_1, a_2, a_3 , то символ x_{15} можна знайти, використовуючи мажоритарний принцип. Проте для цього необхідні три додаткові мажоруючі елементи. Схема декодуючого пристрою показана на рис. 3.20. За циркуляції в регістрі зсуваються не тільки символи системи (3.36), але і коефіцієнти a_j ; при цьому на виході елемента ME_4 матимемо послідовність символів $x_{14} x_{13}, \dots, x_1$. Якщо число помилок $r \leq 3$, то на виході елементів ME_{1-3} збоїв не буде і, отже, реалізується відстань $d_0 = 7$.

Верхня границя числа перевірок за мажоритарного декодування. Складність схем мажоритарного декодування, що визначається числом перевірок μ , багато в чому залежить від величини відстані d_0 . Проте точні співвідношення між d_0 і μ поки що не знайдені. Тому становить інтерес гранична оцінка відношення $\frac{\mu}{d_0}$. Заздалегідь відзначимо одну властивість

лінійних кодів: будь-яка лінійна комбінація стовпців перевіркової матриці H_{nk} (n, k)-коду є комбінацією так званого *дуального* (n, k)-коду. Гранична оцінка $\frac{\mu}{d_0}$, одержана Ю.М. Штарьковим, має вигляд:

$$\frac{\mu}{\lambda_3} = \frac{n - v - \alpha}{\max \left\{ d_d - v; \left\lfloor \frac{d_d + 1}{2} \right\rfloor \right\}}, \quad (3.37)$$

де параметр

$$\alpha = \begin{cases} \frac{1}{\lambda_3} & \text{при } d_d - \text{непарному та } \frac{v}{d_d} < 0,5; \\ 0 & \text{в інших випадках;} \end{cases}$$

d_d – кодова відстань дуального коду.

Якщо нехтувати значенням $\lambda < 1$, то вираз (3.37) набуде вигляду:

$$\frac{\mu}{\lambda_3} = \begin{cases} \frac{n - v}{d_d - v} & \text{при } \frac{v}{d_d} < 0,5; \\ \frac{2(n - v)}{d_d(1 + \beta)} & \text{при } \frac{v}{d_d} \geq 0,5; \end{cases} \quad (3.38)$$

де

$$\beta = \begin{cases} 0 & \text{при } d_d - \text{парному}; \\ \frac{1}{d_d} & \text{при } d_d - \text{непарному}. \end{cases}$$

Приклад 26. Для циклічного (15, 4)-коду, заданого поліномом $g(x) = x^4 + x^3 + x^2 + 1$, відстань дуального коду $d_d = 3$. Якщо $v = 1$, то $\frac{\mu}{\lambda_3} = 7$ і $d_{p \text{ мін}} = 8$.

Приклад 27. Якщо для (15, 4)-коду відстань $d_d = 4$, то при $v = 1$ відношення $\frac{\mu}{\lambda_3} = \frac{14}{3}$ і залежно від λ_3 $5 \leq d_{p\text{мін}} \leq 6$. Якщо $v = 2$, то при $\lambda_3 = 1$

$$\frac{\mu}{\lambda_3} = \begin{cases} 6,5 & \text{при } \lambda_3 = 1; \\ 5 & \text{при } \lambda_3 > 1. \end{cases}$$

Оскільки μ – ціле, то при $v = 2$ відношення $\frac{\mu}{\lambda_3} \leq 6$ та $d_{p\text{мін}} \leq 7$.

Для того, щоб СЗП₁ реалізовувала задане $d_{p\text{мін}}$, необхідно виконання умови:

$$\left\lfloor \frac{\mu - 1}{\lambda_3} \right\rfloor + 2 \geq 2.$$

У зв'язку з цим вкажемо на помилковість затвердження Дж. Мессі, що СРП ($\lambda_3 = 1$) допускають ортогонізацію в K кроків для будь-якого циклічного коду, реалізуючи при цьому відстань $d_p = d_d$.

При $\lambda_3 = 1$ не існує системи перевірок $S(v, 1)$ а 2-го типу (СЗП₂), а систему перевірок СЗП₁ не можна побудувати для будь-якого коду (наприклад, для (23,11)-, (23,12)- (47,23)- (47,24)-, (31,10)-, (31,11)-кодів та ін.).

При СРП величина

$$\mu \leq \frac{n-1}{d_d-1},$$

де знак нерівності відповідає непарним d_d . Тому для кодів Хеммінга не можна побудувати СРП, що реалізує $d_p = 3$, оскільки $n = 2^\zeta - 1, d_d = 2^{\zeta-1}, \mu < 2$ і $d_{p\text{мін}} = \mu + 1 < 3$.

3.9. Синдромний метод декодування

Декодування з декількома рівнями квантування. За мажоритарного декодування дискретних сигналів при декількох рівнях квантування практичний інтерес становлять два випадки:

– сигнали на виході схеми першого ступеня декодування подані в аналоговій формі (число рівнів квантування нескінченне), що відповідає оптимальному режиму її роботи;

– сигнали на виході схеми першого ступеня декодування дискретні (число рівнів квантування скінченне, але більше одиниці), що відповідає неоптимальному режиму її роботи.

Оптимальний режим роботи схеми першого ступеня декодування. Нехай прийнята деяка кодова комбінація, що утворює на виході демодулятора послідовність $Y = y(t) = y_1, \dots, y_n$. де y_j – неперервна випадкова величина.

Згідно з критерієм максимуму правдоподібності, оптимальний приймач повинен реалізовувати певний алгоритм. Шукатимемо найбільшу функцію правдоподібності $L_{X_r}(Y)$ таким чином. Розіб'ємо всю множину $\{X\}$ дозволених кодограм на дві рівні за потужностями підмножини: $\{X^0\}$, яка містить всі комбінації, що починаються символом 0, і підмножину, що включає кодограми, що починаються символом 1. Визначимо максимальні значення функцій правдоподібності $L_{X_r^0}(Y)$ і $L_{X_l^1}(Y)$ для обох підмножин.

Тоді, якщо відношення правдоподібності

$$\lambda_L = \frac{L_{X_r^0}(Y)|_{\max}}{L_{X_l^1}(Y)|_{\max}} < 1, \quad (3.39)$$

то повинне вноситися рішення про приймання кодограми X_r^0 .

Припустимо, що в каналі діють адитивні нормальні флуктуаційні завади, а передання відбувається з активною паузою ($x_1 = +1$, $x_2 = -1$). Тоді густина розподілу ймовірності послідовності $Y = y_1, \dots, y_n$ буде

$$\omega(y_1, \dots, y_n) = \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left[-\frac{\sum_{j=1}^n (y_j - x_j)^2}{2\sigma_{\text{ш}}^2} \right].$$

Умовна густина ймовірності (функція правдоподібності) для будь-якої кодограми X_v^0 :

$$\begin{aligned} L_{X_v^0}(Y) &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[(y_1 - 1)^2 + \sum_{j=2}^n (y_j - X_{v,j}^0)^2 \right] \right\} = \\ &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[\sum_{j=1}^n (y_j^2 + n - 2y_1) - 2 \sum_{j=2}^n Y_j X_{v,j}^0 \right] \right\} \end{aligned} \quad (3.40)$$

а для кодограми X_l^1 , яка починається з одиниці:

$$\begin{aligned} L_{X_l^1}(Y) &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[(y_1 + 1)^2 + \sum_{j=2}^n (y_j - X_{l,j}^1)^2 \right] \right\} = \\ &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[\sum_{j=1}^n (y_j^2 + n + 2y_1) - 2 \sum_{j=2}^n Y_j X_{l,j}^1 \right] \right\} \end{aligned} \quad (3.41)$$

Підставивши вирази (3.40) і (3.41) в (3.39), після логарифмування отримаємо алгоритм прийому коду:

$$y_1 + \sum_{j=2}^n Y_j X_{r,j}^0 > -y_1 + \sum_{j=2}^n Y_j X_{l,j}^1,$$

де $X_r^0 = 0, x_{r2}, x_{r3}, \dots, x_{rn}$; $X_r^1 = 1, x_{l2}, x_{l3}, \dots, x_{ln}$ – кодограми, що починаються з 0 або 1, для яких сума:

$$S = \sum_{j=2}^n Y_j X_{vj}$$

– максимальна.

Нехай для кожного інформаційного символу (n, m) -коду можна скласти систему з r розділених перевірок, кожна з яких містить тільки два символи:

$$x_i = x_{21} \oplus x_{22}; x_{31} \oplus x_{32}; \dots; x_{r1} \oplus x_{r2}, \quad (3.42)$$

де перший індекс членів у правій частині рівності (3.42) відповідає номеру перевірки, а другий – порядковому номеру символу в рівнянні перевірки.

Очевидно, якщо символ $x_i = 0$, то

$$x_{21} = x_{22}; x_{31} = x_{32}; \dots; x_{r1} = x_{r2},$$

якщо ж $x_i = 1$, то

$$x_{21} = -x_{22}; x_{31} = -x_{32}; \dots; x_{r1} = -x_{r2}.$$

З урахуванням цього, переходячи в сумі для S до індексів, прийнятих в системі (3.42), для підмножини кодограм $\{X^0\}$ отримаємо:

$$S^0 = (y_{21} + y_{22}) \cdot x_{21} + (y_{31} + y_{32}) \cdot x_{31} + \dots + (y_{r1} + y_{r2}) \cdot x_{r1}.$$

Очевидно, що величина S^0 буде максимальною, якщо знаки символів $x_{21}, x_{31}, \dots, x_{r1}$ такі, що всі члени суми S позитивні, тобто знак кожного символу повинен бути однаковим зі знаком суми символів, що стоять в дужках перед цим символом. Оскільки в кодограмі незалежними є лише інформаційні символи, то, суворо кажучи, така максимізація можлива лише за умови, що система перевірок (3.42) дозволяє взяти за символи $x_{21}, x_{31}, \dots, x_{r1}$ у формулі для S^0 інформаційні символи. Тоді

$$S_{\max}^0 = |y_{21} + y_{22}| + |y_{31} + y_{32}| + \dots + |y_{r1} + y_{r2}|.$$

Аналогічно для кодограм підмножини $\{X^1\}$ маємо:

$$S^1 = (y_{21} - y_{22}) \cdot x_{21} + (y_{31} - y_{32}) \cdot x_{31} + \dots + (y_{r1} - y_{r2}) \cdot x_{r1};$$

$$S'_{\max} = |y_{21} - y_{22}| + |y_{31} - y_{32}| + \dots + |y_{r1} - y_{r2}|.$$

Зробивши відповідні підстановки, отримаємо:

$$2y_1 + (|y_{21} + y_{22}| - |y_{21} - y_{22}|) + \dots + (|y_{r1} + y_{r2}| - |y_{r1} - y_{r2}|). \quad (3.43)$$

Таким чином, декодуючий пристрій повинен працювати за наступним алгоритмом. Відповідно до мажоритарної системи перевірок для інформаційного символу x_l знаходяться r сум і r різниць вигляду $y_{i1} + y_{i2}, y_{i1} - y_{i2}$, після чого обчислюється сума, визначувана лівою частиною нерівності (3.32). Якщо ця сума буде позитивною, то приймається рішення $X_l = 0$, а решті символів привласнюються значення, відповідні знакам сум $y_{i1} + y_{i2}$. Якщо ж сума виявиться від'ємною, то виноситься рішен-

ня $x_l = 1$, а решті символів привласнюються значення, відповідні знакам різниць $y_{i1} - y_{i2}$. Отже, декодуванню піддаються відразу всі інформаційні символи.

Приклад 28. Розглянемо (3, 2)-код, для якого $x_3 = x_2 \oplus x_1$. Рівняння перевірок для символу x_1 :

$$x_1 = x_1; x_1 = x_2 \oplus x_3.$$

Якщо $x_1 = 0$, то $x_2 = x_3$ і $S^0 = (y_{21} + y_{22}) \cdot x_{21}$, де $y_{21} = y_2$, $y_{22} = y_3$, $x_{21} = x_2$ (символ x_3 брати не слід, оскільки він є лінійною комбінацією символів x_1 і x_2). Якщо $x_1 = 1$, то $x_2 = -x_3$ і $S^1 = (y_{21} - y_{22}) \cdot x_{21} = (y_2 - y_3) \cdot x_2$. Оскільки суми S містять єдиний незалежний символ x_2 , то максимізація забезпечується, і алгоритм є оптимальним.

Нехай при передачі кодограми $X = 011$ прийнята наступна послідовність: $y_1 = -2$; $y_2 = -0,8$; $y_3 = -0,4$, тобто відбулася помилка на першій позиції. Відповідно до алгоритму декодування маємо:

$$y_2 + y_3 = -1,2; y_2 - y_3 = -0,4; \quad 2y_1 | y_2 + y_3 | - | y_2 - y_3 | = 0,4 > 0.$$

Тому виносяться рішення $x_1 = 0$; $x_2 = 1$, і помилка буде виправлена.

Приклад 29. У системі зв'язку використовується (7, 3)-код, для якого рівняння перевірок на парність мають вигляд:

$$x_4 = x_1 \oplus x_3; x_5 = x_1 \oplus x_2 \oplus x_3; x_6 = x_1 \oplus x_2; x_7 = x_2 \oplus x_3.$$

для символу x_1 маємо систему перевірок:

$$x_1 = x_1; x_3 \oplus x_4; x_2 \oplus x_6; x_7 \oplus x_5.$$

Тоді при $x_1 = 0$ і $x_1 = 1$ відповідно отримаємо:

$$S^0 = (y_3 + y_4) \cdot x_3 + (y_2 + y_6) \cdot x_2 + (y_7 + y_5) \cdot x_7;$$

$$S^1 = (y_3 - y_4) \cdot x_3 + (y_2 - y_6) \cdot x_2 + (y_7 - y_5) \cdot x_7$$

Тут символ x_7 залежний, оскільки, якщо символи x_2 і x_3 вибрані, то $x_7 = x_2 + x_3$. Іншими словами, довільний вибір символу x_7 відповідно до знаку суми $y_7 + y_5$ (або різниці $y_7 - y_5$) недопустимий. Проте алгоритм передбачає саме такі дії, тому в даному випадку він не є оптимальним. Наслідком цього може бути помилкове декодування прийнятої комбінації, тоді як за оптимального декодування цього не відбувається.

Дійсно, нехай, наприклад, при передаванні кодограми $X = 0000000$ відбулися дві помилки на першій і сьомій позиціях і прийнята послідовність має вигляд:

$$y_1 = -0,05; y_2 = 0,3; y_3 = 0,3; y_4 = 0,1; y_5 = 0,2; y_6 = 0,1; y_7 = -0,3.$$

Відповідно до оптимального алгоритму для всіх восьми комбінацій повинні бути обчислені суми:

$$S_i = \sum_{j=1}^n y_j x_{ij}.$$

У результаті розрахунку отримаємо: $X_1 = 0000000$, $S_1 = 0,65$; $X_2 = 0011101$, $S_2 = 0,05$; $X_3 = 0100111$, $S_3 = 0,05$; $X_4 = 0111010$, $S_4 = -0,95$;

$X_5 = 1001110$, $S_5 = -0,05$; $X_6 = 1010011$, $S_6 = 0,55$; $X_7 = 1101001$, $S_7 = 0,55$; $X_8 = 1110100$, $S_8 = -0,85$. Прийнята комбінація ототожнюється з кодограмою, оскільки сума S_1 найбільша, і помилки будуть виправлені.

При декодуванні по алгоритму (3.43) маємо:

$$2y_1 + |y_{21} + y_{22}| - |y_{21} - y_{22}| + |y_{31} + y_{32}| - |y_{31} - y_{32}| + |y_{41} + y_{42}| - |y_{41} - y_{42}| = 2y_1 + |y_3 + y_4| - |y_3 - y_4| + |y_2 + y_6| - |y_2 - y_6| + |y_7 + y_5| - |y_7 - y_5| = -0,1 < 0$$

Відповідно до цього повинні бути винесені такі рішення: $x_1 = 1$; $x_2 = 0$; $x_3 = 0$, тобто декодування відбувається з помилкою. Це є наслідком вибору символу $x_7 = 1$ (згідно з знаком $y_7 + y_5$ або різниці $y_7 - y_5$), тоді як при виборі $x_2 = 0$ і $x_3 = 0$ повинно бути $x_7 = 0$.

Таким чином, при оптимальній схемі першого ступеня декодування мажоритарне декодування за алгоритмом (3.43) має, принаймні, два недоліки:

- можливе декодування кодів, що мають в кожному рівнянні перевірки не більше двох символів;
- якщо число розділених перевірок перевищує число інформаційних символів, то алгоритм декодування неоптимальний, що спричиняє за собою зниження завадостійкості, причому тим більше, чим сильніше це перевищення.

Можна дещо змінити описану процедуру декодування, відмовившись від паралельного визначення всіх інформаційних символів. У цьому випадку обчислення суми (3.43) слугує лише для визначення інформаційного символу x_1 . Потім з використанням системи перевірок для інформаційного символу x_2 обчислюється сума, аналогічна (3.43), і за нею визначається символ x_2 . Цей процес повторюється послідовно стільки разів, скільки інформаційних символів міститься у кодограмі.

3.10. Питання та задачі для самоперевірки

1. Наведіть класифікацію способів кодування дискретних сигналів.
2. Складіть класи залишків чисел A , $A \in 1 \dots 20$ за модулями 5, 7.
3. Дайте визначення групи; наведіть приклади груп.
4. Чи є групами множини цілих чисел відносно операцій цілих чисел, множини векторів відносно операцій векторного множення, множини квадратних матриць відносно операцій множення?
5. Визначте підгрупи $H(2^0)$ і $H(2^5)$ простого (5, 5)-кодера.
6. Дайте визначення кільця і поля; наведіть приклади кілець і полів.
7. Складіть таблицю суміжних класів для групового (5, 2) – коду при дії завад, що викликають одиночні і подвійні помилки.
8. Поясніть взаємозв'язок кодової відстані з виправляючою здатністю коду. Визначте нижню границю значення d для двійкового (7, 3)-коду, користуючись оцінками Хеммінга і Варшамова-Гільберта.

9. Поясніть методику побудови породжуючої і перевіркової матриць групових кодів. Побудуйте матриці H_v і H_p і закодуйте (7, 3)-кодом числа 5 і 6.

10. Поясніть зміст операції перевірки КС на парність.

11. Подайте числа 112 і 57 у формі поліномів змінної X і у вигляді двійкових кодових поліномів; проведіть над ними дії додавання, множення і ділення. Поясніть відмінність понять незведенність і неподільність поліномів.

12. Визначте число поліномів з максимальним періодом при $\rho = 2; n = 5$ і $\rho = 3; n = 3$.

13. Побудуйте породжуючу і перевірочну матриці коду Слепяна, який виправляє всі однократні і двократні помилки для передачі 64 повідомлень, і визначте ймовірність зв'язку, якщо ймовірність спотворень символу $\rho_e = 10^{-3}$.

14. Побудуйте породжуючу і перевірочну матриці коду Хеммінга, який виправляє всі однократні і двократні помилки, для передавання буквенного алфавіту і визначте ймовірність безпомилкового зв'язку, якщо ймовірність спотворень символу $\rho_e = 10^{-3}$.

15. Поясніть алгоритм побудови кодів Ріда-Мюллера. Закодуйте число 9 кодами з параметрами $r = 1, \mu = 3, v = 1$ і $r = 1, \mu = 4, v = 2$.

16. Складіть блок-схеми кодуєчих пристроїв (9, 5)-кодів Слепяна і Хеммінга.

17. Які операції можуть виконувати багатотактові кодові фільтри? Складіть схему БКФ для множення на поліном $g(x) = 1011001$. Напишіть вираз для операторних поліномів цих фільтрів. Визначте вихідну послідовність символів, якщо вхідний сигнал $S(x) = 10111$.

18. Складіть схему лінійного БКФ з вхідними кодами для множення на поліном $g_1(x) = 1100101$ і $g_2(x) = 11001$. Визначте вихідну послідовність символів, якщо вхідні сигнали $S_1(x) = 11001$ і $S_2(x) = 1011$.

19. Складіть схему БКФ для ділення на поліном $h(x) = 10111$. Визначте результат ділення, якщо вхідний сигнал $S(x) = 11001101$.

20. Складіть схему БКФ для одночасного множення на поліном $g(x) = 1101$ та ділення на поліном $h(x) = 11001$. Визначте результат ділення, якщо вхідний сигнал $S(x) = 10011$.

21. Поясніть способи завдання циклічного коду. Побудуйте породжуючу матрицю коду, заданого поліномом $g(x) = 11001$, що належить показнику $n = 15$.

22. Побудуйте перевірочну матрицю циклічного коду за допомогою поліному $h(x)$, якщо породжуючий поліном $g(x) = 1011$ належить показнику $n = 7$.

23. Поясніть способи формування циклічного коду з розділеними і нерозділеними символами. Закодуйте число 23, якщо поліном $g(x) = 10011$.

24. Сформулюйте властивості кодів Хаффмена і Боуза-Чоудхурі.

25. Поясніть принцип побудови скорочених циклічних кодів. Знайдіть поліном $\varphi(x)$ для скороченого циклічного (13, 8)-коду з розділеними і нерозділеними символами, якщо вихідний (15, 10)-код заданий поліномом $g(x) = 101111$

26. Назвіть коди, які використовуються в каналах зв'язку з групуванням помилок. Побудуйте код Файра, який виправляє пакети помилок довжиною $l_{\text{пн}} = 5$ і виявляє пакети помилок довжиною $l_{\text{по}} = 2$. Для яких інших помилок цей код зберігає свою ефективність?

27. Порівняйте правильність зв'язку при використанні коду Хеммінга в режимі однократної і трикратної передачі з мажоритарної обробки прийнятих сигналів, якщо ймовірність спотворення символу $\rho_e = 10^{-2}$.

28. Поясніть принцип рекурентного кодування. Закодуйте число 25 рекурентним (2,1)-кодом Фінка-Хагельбаргера. Намалюйте часові діаграми роботи кодоперетворювачів при одиночних та помилках, що групуються.

29. Поясніть принцип згорткового кодування. Закодуйте число 19 згортковим кодом, якщо $\mu = 4$, $\nu = 3$, а коефіцієнти зв'язку $b_1 = 0110$, $b_2 = 1110$, $b_3 = 1011$ та намалюйте кодове дерево сигналів.

30. Закодуйте число 95 згортковим (3/4)-кодом при довжині утворюючої послідовності $n = 16$, складіть схему кодувального пристрою.

ГЛАВА 4

ТАЙМЕРНІ СИГНАЛЬНІ КОНСТРУКЦІЇ ЯК ІНСТРУМЕНТАРІЙ УКРУПНЕННЯ СИГНАЛІВ ПРИ БЛОКОВОМУ КОДУВАННІ

4.1 Збільшення мірності сигнальних конструкцій при обмеженій довжині кодового слова

Розглянемо структуру приймального пристрою, забезпечуючого оптимальну обробку двійкових сигналів з довільним числом рівнів квантування (рис. 4.1). Як видно із рисунка, між розв'язувальною схемою РС₁, що містить демодулятор сигналів, і схемою РС₂ включено квантизатор КВ, що дозволяє квантувати рівень вихідних сигналів демодулятора. Таким чином, квантизатор перетворює вихідний алфавіт демодулятора $\{y\}$ в новий алфавіт символів $\{z\}$. Імовірнісні зв'язки між символами цих алфавітів описуються перехідними ймовірностями $\{p_{k,l}\}$, що характеризують ймовірність переходу символу $y_k \in Y$ в символ $z_l \in Z$. Ці ймовірності можна представити в матричній формі (рис. 4.2,а) або графічно (рис. 4.2,б).

В залежності від числа рівнів квантування S одержуються різні способи приймання сигналів. Посимвольне приймання реалізується наступним чином. Область вихідних значень сигналів демодулятора Y ділиться порогом U_0 на дві зони – позитивну і від'ємну (рис. 4.3,а). При цьому фіксується лише факт перебування символу кодограми у відповідній зоні, тобто враховується лише його знак. Це рівнозначно тому, що вихідний сигнал демодулятора квантується за амплітудою з одним рівнем квантування. Відмова від використання інформації про рівні сигналів в межах зони квантування понижує завадостійкість приймання.

Очевидно, що першим кроком на шляху підвищення завадостійкості приймання може бути введення ще двох порогів, рівних за величиною і протилежних за знаком (рис. 4.3,б). Ці пороги разом з нульовим розділяють всю ділянку значень вихідних сигналів демодулятора на чотири попарно симетричні зони, що рівнозначно квантуванню сигналів на два рівня. В цьому випадку об'єм інформації про прийнятий сигнал збільшується за рахунок використання відомостей про знаходження сигналу в тій чи іншій зоні, що підвищує завадостійкість зв'язку.

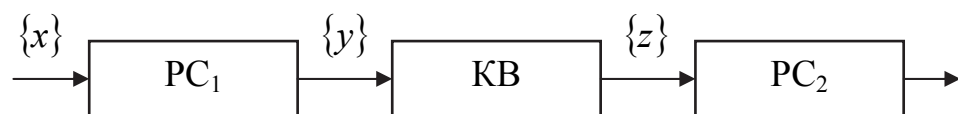


Рис. 4.1. Приймач з довільним числом рівнів квантування сигналів

a)

$$\|p_{k,l}\| = \begin{vmatrix} p_{11} & p_{12} & \dots & p_{1S} \\ \dots & \dots & \dots & \dots \\ p_{m1} & p_{m2} & \dots & p_{mS} \end{vmatrix}$$

б)

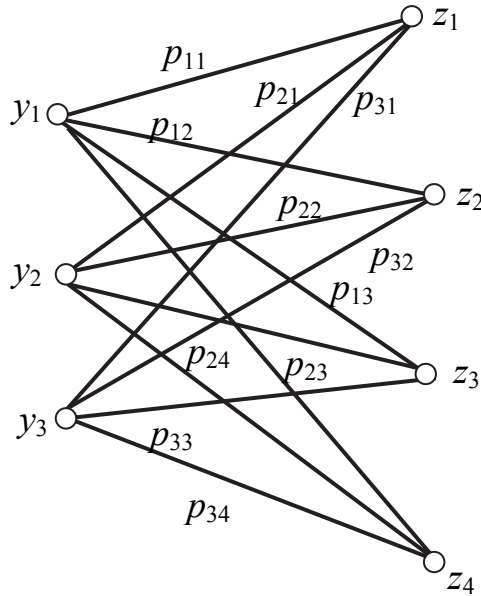


Рис. 4.2. Перехідні ймовірності квантизатора

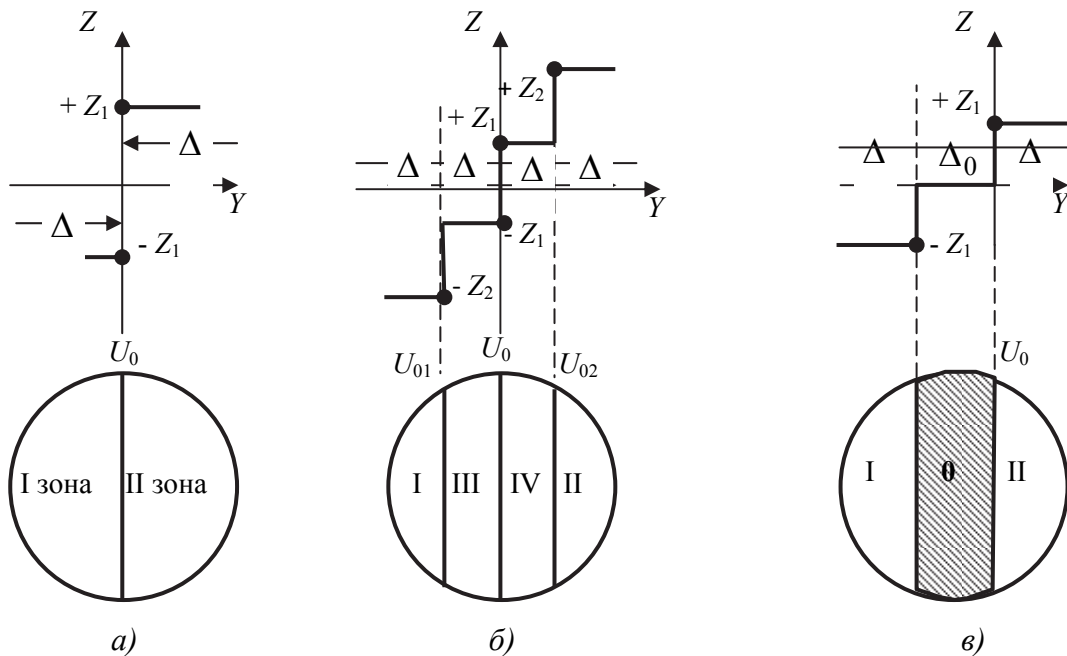


Рис. 4.3. Робочі області сигналів при різних способах приймання

Продовжуючи збільшувати число рівнів квантування, ми все більше будемо підвищувати завадостійкість зв'язку, наближаючись в межі до

завадостійкості оптимального приймання в цілому, являючого собою приймання з нескінченним числом рівнів квантування.

Таким чином можна виділити клас способів приймання, які відрізняються між собою числом рівнів квантування сигналів з виходу демодулятора або, що те ж саме, точністю роботи схеми РС₁. Приймання в цілому і посимвольне приймання є граничними випадками для цього класу.

Оптимальний алгоритм декодування. Алгоритм декодування при довільному числі рівнів квантування безпосередньо витікає із виразу

$$\sum_{k=1}^n x_{r,k} \eta_k > \sum_{k=1}^n x_{l,k} \eta_k .$$

Різниця полягає лише в тому, що якщо функції правдоподібності $L_{п. k}$ і $L_{о. k}$ являють собою густини ймовірностей при правильному і помилковому прийманні, то для будь-якого кінцевого числа рівнів квантування вони повинні бути замінені перехідними ймовірностями q_j і p_j попадання вихідного сигналу демодулятора в j -у зону ($j = 1, 2, \dots, S$) відповідно при вірному і помилковому прийманні. Тоді оптимальний алгоритм декодування при довільному числі рівнів квантування S можна представити у вигляді

$$\sum_{j=1}^S \log \frac{q_j}{p_j} \sum_{k_j} x_{r,k} y_k > \sum_{j=1}^S \log \frac{q_j}{p_j} \sum_{k_j} x_{l,k} y_k , \quad (4.1)$$

де $y_k = \pm 1$ в залежності від знаку k -го символу кодограми; індекс k_j означає, що підсумовування ведеться за тими позиціями кодограми, для яких рівень сигналу знаходився в j -ій зоні квантування, причому

$$\sum_{j=1}^S k_j = n .$$

При $S = 1$ вираз (4.1) переходить в $\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k$.

Поділивши обидві частини нерівності (4.1) на $\log \frac{q_1}{p_1}$, одержимо іншу

форму оптимального алгоритму декодування:

$$\sum_{j=1}^S \gamma_j \sum_{k_j} x_{r,k} y_k > \sum_{j=1}^S \gamma_j \sum_{k_j} x_{l,k} y_k , \quad (4.2)$$

де коефіцієнт

$$\gamma_j = \frac{\log \frac{q_j}{p_j}}{\log \frac{q_1}{p_1}}. \quad (4.3)$$

Згідно алгоритму (4.2) схема РС₁ формує символи, амплітуда яких залежить від того, в якій зоні знаходився рівень сигналу на даній позиції кодограми. Якщо сигнал потрапив у першу зону, то амплітуда символу на виході схеми РС₁ умовно дорівнює одиниці; для j -ої зони амплітуда символу дорівнює коефіцієнту γ_j . Величина γ_j залежить від перевищення сигналу і способу приймання. Схема РС₂ підсумовує символи з урахуванням їх знаків в кодограмі X_v , визначає найбільшу суму і виносить рішення про ототожнення прийнятої комбінації з тією з можливих кодограм X_r , яка відповідає цій найбільшій сумі.

Оптимальний алгоритм декодування при довільному числі рівнів квантування може бути виражений також через кодову відстань між кодограмами. Якщо кодограми X_v і Y співпадають за k_j позиціями, то сума

$$\sum_{k_j} x_{v,k} y_k = k_j;$$

якщо ж на $d_{v,y}^{(j)}$ позиціях символи протилежні, то сума

$$\sum_{k_j} x_{v,k} y_k = k_j - 2d_{v,y}^{(j)}, \quad (4.4)$$

де $d_{v,y}^{(j)}$ – відстань між кодограмами X_v і Y за тими k_j позиціями, де сигнал знаходився в j -ій зоні квантування. Підставивши суму (4.4) в (4.2), після перетворень одержимо

$$\sum_{j=1}^S \gamma_j d_{r,y}^{(j)} < \sum_{j=1}^S \gamma_j d_{l,y}^{(j)}. \quad (4.5)$$

Отже, прийнята комбінація Y повинна ототожнюватися з тією із можливих кодограм X_r , яка віддалена від прийнятої комбінації з урахуванням вагових коефіцієнтів γ_j для різних k_j позицій на мінімальну відстань. Якщо $\gamma_j = \gamma = \text{const}$, то виходить правило $d_{r,y} < d_{l,y}$. для посимвольного приймання з виправленням помилок.

Розглянемо найпростіший випадок приймання двійкових сигналів з одним рівнем квантування (посимвольне приймання). Будемо вважати, що передається кодограма X_0 , яка складається із символів -1 . Це не порушує спільності міркувань в силу властивості симетричності групових кодів. З урахуванням того, що кодограма X_0 відрізняється від будь-якої кодограми

X_v в d_v позиціях, де d_v – вага кодограми X_v , із формули

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k \text{ одержимо умову правильного приймання сигналів}$$

$$-\sum_{d_v} y_k > 0; \quad (4.6)$$

індекс d_v показує, що підсумовування для кожної із кодограм X_v відбувається тільки за тими позиціями, де знаходяться одиниці.

При відсутності помилок кожна сума дорівнює вазі d_v відповідної кодограми. Якщо відбулась одна помилка, то частина сум не змінюється (для тих кодограм, у яких помилки відбулися на позиціях, зайнятих символами -1), а частина сум, де помилки відбулися на позиціях, зайнятих символами $+1$, приймуть значення $d_v - 2$. При двох помилках будуть три значення сум, відповідно рівних.

d_v – для кодограм, де обидві помилки відбулися на позиціях, зайнятих символами -1 ;

$d_v - 2$ – для кодограм, де одна з помилок відбулася на позиції, зайнятій символом $+1$, а друга – на позиції з символом -1 ;

$d_v - 4$ – для кодограм, де обидві помилки відбулися на позиціях, зайнятих символами $+1$.

Таким чином, при r -кратних помилках значення кожної суми визначається розподілом помилок усередині кодограми. Очевидно, що при цьому завжди справедливе відношення

$$-\sum_{d_v} y_k \geq d_v - 2r, \quad (4.7)$$

причому знак рівності буде в самому несприятливому випадку, коли всі помилки відбулися на позиціях кодограми, зайнятих символами $+1$. Звідси виходить, що необхідною і достатньою умовою виправлення всіх можливих сполучень r -кратних помилок, незалежно від їх розподілу всередині кодограми, є виконання нерівності

$$d_0 - 2r > 0, \quad (4.8)$$

де d_0 – мінімальна відстань коду.

Оскільки d_0 і r – цілі числа, то із нерівності (4.8) одержимо умову, що зв'язує мінімальну кодову відстань і максимальну кратність виправляємих кодом помилок :

$$r_0 = \begin{cases} \frac{d_0 - 1}{2} & \text{за } d_0 - \text{непарним,} \\ \frac{d_0 - 1}{2} & \text{за } d_0 - \text{парним.} \end{cases} \quad (4.9)$$

Вирази (4.9) являють собою нижню оцінку виправляючої здатності коду. Якщо r помилок розподілені всередині кодограми таким чином, що у

виразі (4.7) має місце знак рівності, то можливе виправлення помилок кратності $r > r_0$, але не у всіх сполученнях, а тільки в частині сполучень, визначуваних тонкою структурою коду.

Важливо відзначити, що згідно формулі (4.9) виправляюча здатність коду при посимвольному прийманні залежить тільки від його структури.

При прийманні сигналів з довільним числом рівнів квантування одержимо умову правильного приймання кодограми X_0 :

$$-\sum_{j=1}^S \gamma_j \sum_{d_{v,j}} y_k > 0,$$

де $d_{v,j}$ – вага v -ої кодограми за позиціями, що припадають на j -у зону квантування. В цьому випадку також очевидне співвідношення

$$-\sum_{j=1}^S \gamma_j \sum_{d_{v,j}} y_k > \sum_{j=1}^S \gamma_j (d_{v,j} - 2r_j).$$

де r_j – число спотворень символів в j -ій зоні квантування.

Тоді умова, що характеризує нижню границю виправляючої здатності коду при прийманні з довільним числом рівнів квантування буде:

$$\sum_{j=1}^S \gamma_j (d_{v,j} - 2r_j) > 0. \quad (4.10)$$

Звідси виходить, що виправляюча здатність коду при інших рівних умовах залежить від розподілу символів за зонами квантування. Найгіршим буде випадок, коли в будь-якій одній зоні знаходиться більше, ніж $d_0 - 1$ символів, причому всі вони всі вони відповідають $+1$ деякої кодограми (як і раніше передбачаємо, що передавалась кодограма, яка складається із символів -1). Тоді виправляюча здатність коду характеризується формулою (4.9) і буде мінімальною.

Принципова можливість збільшити виправляючу здатність коду при прийманні з довільним числом рівнів квантування $S > 1$ обумовлена наступним. Із формули (4.3) виходить, що при завадах, густина ймовірності яких спадає з ростом їх амплітуди, справедлива нерівність $\gamma_j > \gamma_{j-1}$. Тоді, як впливає із нерівності (4.10), при розподілі символів і помилок за зонами, коли, починаючи з деякої j -ї зони і вище різниця $d_{v,j} - 2r_j > 0$, можна добитися виконання нерівності (4.10), тобто виправлення всіх помилок в нижніх зонах квантування. Це забезпечується вибором відповідних співвідношень коефіцієнтів γ_0 .

Визначимо максимально можливу виправляючу здатність коду і умови її досягнення. Розглянемо випадок, коли r символів, відповідаючих одиночним позиціям, розподілені за двома зонами квантування, причому в

нижній зоні всі вони спотворені, тобто $d_{v(j-\xi)} = r_{j-\xi}$. Тоді із нерівності (4.10) одержимо

$$\gamma_j(d_0 - r_{j-\xi} - 2r_j) - \gamma_{j-\xi}r_{j-\xi} > 0.$$

Отже, в нижній зоні квантування може бути виправлено

$$r_{j-\xi} < \frac{\gamma_j}{\gamma_j - \gamma_{j-\xi}}(d_0 - 2r_j)$$

помилку. Найбільше число виправлених помилок буде при відсутності спотворень у верхній зоні квантування ($r_j = 0$). Тоді

$$r_{j-\xi} < \frac{\gamma_j}{\gamma_j - \gamma_{j-\xi}}d_0 = \frac{\alpha_{j,\xi}}{\alpha_{j,\xi} - 1}d_0, \quad (4.11)$$

де параметр

$$\alpha_{j,\xi} = \frac{\gamma_j}{\gamma_{j-\xi}}. \quad (4.12)$$

Зазначимо, що дріб у правій частині нерівності (4.11) зростає в міру збільшення параметра $\alpha_{j,\xi}$, тобто з його зростанням виправляюча здатність коду збільшується. Крім того, оскільки d_0 і $r_{j-\xi}$ – цілі числа, то із виразу (4.11) виходить, що в нижній зоні квантування будуть виправлятися всі помилки кратності

$$r_{j-\xi} = d_0 - v, \quad (4.13)$$

якщо задовольняється нерівність

$$\frac{\alpha_{j,\xi}}{\alpha_{j,\xi} - 1}d_0 > d_0 - v,$$

яка після перетворень приводиться до виду

$$\alpha_{j,\xi} > \frac{d_0 - v}{v}. \quad (4.14)$$

Вирази (4.13) і (4.14) зв'язують максимальну виправляючу здатність коду з параметрами схеми приймання, які відбиваються величиною $\alpha_{j,\xi}$. Чим більша $\alpha_{j,\xi}$, тим більша кратність помилок, виправляємих кодом в нижній зоні квантування, причому верхня межа

$$r_0 = d_0 - 1 \quad (4.15)$$

і забезпечується за умови, що

$$\alpha_{j,\xi} > d_0 - 1. \quad (4.16)$$

Очевидно, що збільшення $\alpha_{j,\xi}$ над значення, яке визначається нерівністю (4.16), недоцільне, оскільки виправляюча здатність коду при цьому не зростає.

Таким чином, якщо параметри схеми приймання сигналів обрані так, що відношення всіх сусідніх дискретних значень вихідної напруги

підпорядковуються умові (4.16), а число символів в нижніх зонах квантування не більше $d_0 - 1$, то код здатний виправити всі сполучення помилок кратності $r = d_0 - 1$ незалежно від їх розподілу в нижніх зонах квантування.

В окремих випадках в нижніх зонах квантування можуть бути виправлені помилки кратності, більшої, ніж $d_0 - 1$. Для цього необхідно, щоб у верхній зоні квантування знаходився хоча б один вірно прийнятий символ, відповідаючий позиції $+1$ v -ї кодограми. Очевидно, що це можливо лише при деяких сполученнях розміщення символів між зонами, тобто помилки кратності, більшої $d_0 - 1$, будуть виправлятися не у всіх сполученнях. Важливо відзначити, що виконання умови (4.16) достатньо, щоб ці помилки були виправлені. Це виходить з того, що у формулі (4.10) підсумовування ведеться лише за позиціями, що відповідають $+1$; помилки на інших позиціях впливу на суму не мають.

Найбільший інтерес з точки зору простоти технічної реалізації представляє приймання з двома рівнями квантування. В цьому випадку оптимальний алгоритм декодування має вид

$$\gamma d_{r,y}^{(2)} + d_{r,y}^{(1)} < \gamma d_{l,y}^{(2)} + \gamma d_{l,y}^{(1)}, \quad (4.17)$$

де коефіцієнт

$$\gamma = \frac{\log \frac{q_2}{p_2}}{\log \frac{q_1}{p_1}}, \quad (4.18)$$

а умова правильного приймання буде

$$\gamma(d_{v_2} - 2r_2) + (d_{v_1} - 2r_1) > 0. \quad (4.19)$$

При оцінці нижньої границі виправляючої здатності коду слід брати

$$d_{v_2} + d_{v_1} = d_0.$$

Тоді із нерівності (4.19) одержимо рівняння зв'язку між мінімальною відстанню коду d_0 , кратністю повністю виправляємим помилкам $(r_1 + r_2)$ в обох зонах квантування та числом символів в першій зоні d_{v_1} :

$$2r_2 + \frac{2r_1}{\gamma} + d_{v_1} \frac{\gamma - 1}{\gamma} < d_0. \quad (4.20)$$

При $\gamma \rightarrow \infty$ одержимо

$$2r_2 + d_{v_1} < d_0$$

й оскільки всі величини цілочисельні, то

$$2r_2 + d_{v_1} + 1 = d_0. \quad (4.21)$$

Нагадаємо, що величина d_{v_1} є не що інше, як число символів, рівень яких лежить в першій зоні квантування, тобто нижче порога. Отже, вираз

(4.21) встановлює зв'язок між максимальною кратністю виправляємих кодом помилок у другій зоні квантування і мінімальною відстанню коду при наявності d_{v_1} символів з рівнем нижче порогового значення, причому байдуже, правильно чи помилково прийняті ці символи.

4.2. Виправляюча здатність групових кодів при довільному числі рівнів квантування

Розглянемо спочатку найпростіші випадки прийому двійкових сигналів з одним рівнем квантування (посимвольний прийом). Будемо вважати, що передається кодограма X_0 , яка складається із символів -1 . Це не порушує спільності міркувань через властивості симетричності групових кодів. З урахуванням того, що кодограма X_0 відрізняється від будь-якої кодограми X_v в d_v позиціях, де d_v – вага кодограми X_v , із формули

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k \text{ отримаємо умову правильного приймання сигналів}$$

$$-\sum_{d_v} y_k > 0; \quad (4.22)$$

індекс d_v показує, що підсумовування для кожної із кодограм X_v відбувається тільки за тими позиціями, де знаходяться одиниці.

За відсутності помилок кожна сума дорівнює вазі d_v відповідної кодограми. Якщо відбулась одна помилка, то частина сум не змінюється (для тих кодограм, в яких помилки відбулися на позиціях, зайнятих символами -1 , а частина сум, де помилки відбулися на позиціях, зайнятих символами $+1$, набудуть значення $d_v - 2$. При двох помилках будуть три значення сум, відповідно рівних:

– d_v – для кодограм, де обидві помилки відбулися на позиціях, зайнятих символами -1 ;

– $d_v - 2$ – для кодограм, де одна з помилок відбулася на позиції, зайнятій символом $+1$, а друга – на позиції з символом -1 ;

– $d_v - 4$ – для кодограм, де обидві помилки відбулися на позиціях, зайнятих символами $+1$.

Таким чином, при r -кратних помилках значення кожної суми визначається розподілом помилок усередині кодограми. Очевидно, що при цьому завжди справедливе відношення

$$-\sum_{d_v} y_k \geq d_v - 2r, \quad (4.23)$$

причому знак рівності буде в самому несприятливому випадку, коли всі помилки відбулися на позиціях кодограми, зайнятих символами $+1$. Звідси виходить, що необхідною і достатньою умовою виправлення всіх

можливих з'єднань r -кратних помилок, незалежно від їх розподілу всередині кодограми, є виконання нерівності

$$d_0 - 2r > 0, \quad (4.24)$$

де d_0 – мінімальна відстань коду.

Тому що d_0 і r – цілі числа, то із нерівності (4.24) отримаємо умову, що пов'язує мінімальну кодову відстань і максимальну кратність виправляємих кодом помилок:

$$r_0 = \begin{cases} \frac{d_0 - 1}{2} & \text{за } d_0 - \text{непарним,} \\ \frac{d_0 - 1}{2} & \text{за } d_0 - \text{парним.} \end{cases} \quad (4.25)$$

Вирази (4.25) являють собою нижню оцінку виправляючої здатності коду. Якщо r помилок розподілені всередині кодограми таким чином, що у виразі (4.23) має місце знак рівності, то можливе виправлення помилок кратності $r > r_0$, але не в усіх з'єднаннях, а тільки в частині з'єднань, визначуваних тонкою структурою коду.

Важливо відзначити, що згідно з формулою (4.25) виправляюча здатність коду при посимвольному прийманні залежить тільки від його структури.

При прийманні сигналів з довільним числом рівнів квантування отримаємо умову правильного прийманні кодограми X_0 :

$$-\sum_{j=1}^S \gamma_j \sum_{d_{v,j}} y_k > 0,$$

де $d_{v,j}$ – вага v -ї кодограми за позиціями, що припадають на j -ту зону квантування. В цьому випадку також очевидне співвідношення

$$-\sum_{j=1}^S \gamma_j \sum_{d_{v,j}} y_k > \sum_{j=1}^S \gamma_j (d_{v,j} - 2r_j).$$

де r_j – число спотворень символів в j -й зоні квантування.

Тоді умова, що характеризує нижню межу виправляючої здатності коду при прийомі з довільним числом рівнів квантування буде:

$$\sum_{j=1}^S \gamma_j (d_{v,j} - 2r_j) > 0. \quad (4.26)$$

З чого виходить, що виправляюча здатність коду за інших рівних умов залежить від розподілу символів за зонами квантування. Найгіршим буде випадок, коли в будь-якій одній зоні знаходиться більше ніж $d_0 - 1$ символів, причому всі вони відповідають +1 деякої кодограми (як і раніше передбачаємо, що передавалась кодограма, яка складається із символів -1).

Тоді виправляюча здатність коду характеризується формулою (4.25) і буде мінімальною.

Принципова можливість збільшити виправляючу здатність коду при прийомі з довільним числом рівнів квантування $S > 1$ обумовлена наступним. Із формули для γ_j виходить, що при завадах, густина ймовірності яких спадає зі зростанням їх амплітуди, справедлива нерівність $\gamma_j > \gamma_{j-1}$. Тоді, як витікає із нерівності (4.26), при розподілі символів і помилок за зонами, коли, починаючи з деякої j -ї зони і вище різниця $d_{v,j} - 2r_j > 0$, можна досягти виконання нерівності (4.26), тобто виправлення всіх помилок у нижніх зонах квантування. Це забезпечується вибором відповідних співвідношень коефіцієнтів γ_0 .

Визначимо максимально можливу виправляючу здатність коду й умови її досягнення. Розглянемо випадок, коли r символів, що відповідають одиничним позиціям, розподілені за двома зонами квантування, причому в нижній зоні всі вони спотворені, тобто $d_{v(j-\xi)} = r_{j-\xi}$. Тоді із нерівності (4.26) отримаємо

$$\gamma_j(d_0 - r_{j-\xi} - 2r_j) - \gamma_{j-\xi}r_{j-\xi} > 0.$$

Отже, в нижній зоні квантування може бути виправлено

$$r_{j-\xi} < \frac{\gamma_j}{\gamma_j - \gamma_{j-\xi}}(d_0 - 2r_j)$$

помилки. Найбільше число виправлених помилок буде за відсутності спотворень у верхній зоні квантування ($r_j = 0$). Тоді

$$r_{j-\xi} < \frac{\gamma_j}{\gamma_j - \gamma_{j-\xi}}d_0 = \frac{\alpha_{j,\xi}}{\alpha_{j,\xi} - 1}d_0,$$

де параметр

$$\alpha_{j,\xi} = \frac{\gamma_j}{\gamma_{j-\xi}}.$$

Зазначимо, що дріб у правій частині нерівності $r_{j-\xi}$ зростає в міру збільшення параметра $\alpha_{j,\xi}$, тобто з його зростанням виправляюча здатність коду збільшується. Крім того, оскільки d_0 і $r_{j-\xi}$ – цілі числа, виходить, що в нижній зоні квантування будуть виправлятися всі помилки кратності

$$r_{j-\xi} = d_0 - v,$$

якщо задовольняється нерівність

$$\frac{\alpha_{j,\xi}}{\alpha_{j,\xi} - 1}d_0 > d_0 - v,$$

яка після перетворень приводиться до вигляду

$$\alpha_{j,\xi} > \frac{d_0 - v}{v}.$$

Останні вирази пов'язують максимальну виправляючу здатність коду з параметрами схеми прийому, відображуваними величиною $\alpha_{j,\xi}$. Чим більша $\alpha_{j,\xi}$, тим більша кратність помилок, що виправляються кодом у нижній зоні квантування, причому верхня межа

$$r_0 = d_0 - 1$$

і забезпечується за умови, що

$$\alpha_{j,\xi} > d_0 - 1. \quad (4.27)$$

Очевидно, що збільшення $\alpha_{j,\xi}$ на значення $d_0 - 1$, недоцільне, тому що виправляюча здатність коду при цьому не зростає.

Таким чином, якщо параметри схеми прийому сигналів вибрані так, що відношення всіх сусідніх дискретних значень вихідної напруги підпорядковуються умові (4.27), а число символів у нижніх зонах квантування не більше $d_0 - 1$, то код здатний виправити всі з'єднання помилок кратності $r = d_0 - 1$ незалежно від їх розподілу в нижніх зонах квантування.

В окремих випадках у нижніх зонах квантування можуть бути виправлені помилки кратності більшої, ніж $d_0 - 1$. Для цього необхідно, щоб у верхній зоні квантування знаходився хоча б один правильно прийнятий символ, що відповідає позиції $+1$ v -ї кодограми. Очевидно, що це можливо лише за деяких з'єднань розміщення символів між зонами, тобто помилки кратності більшої $d_0 - 1$ будуть виправлятися не в усіх з'єднаннях. Важливо відзначити, що виконання умови (4.27) достатньо, щоб ці помилки були виправлені. Це виходить з того, що у формулі (4.26) підсумовування ведеться лише за позиціями, що відповідають $+1$; помилки на інших позиціях впливу на суму не мають.

Найбільший інтерес з точки зору простоти технічної реалізації становить прийом з двома рівнями квантування. В цьому випадку оптимальний алгоритм декодування має вигляд

$$\gamma d_{r,y}^{(2)} + d_{r,y}^{(1)} < \gamma d_{l,y}^{(2)} + \gamma d_{l,y}^{(1)},$$

де коефіцієнт

$$\gamma = \frac{\log \frac{q_2}{p_2}}{\log \frac{q_1}{p_1}},$$

а умова правильного прийому буде

$$\gamma(d_{v_2} - 2r_2) + (d_{v_1} - 2r_1) > 0. \quad (4.28)$$

При оцінці нижньої межі виправляючої здатності коду слід брати

$$d_{v_2} + d_{v_1} = d_0.$$

Тоді із нерівності (4.28) отримаємо рівняння зв'язку між мінімальною відстанню коду d_0 , кратністю повністю виправлених помилок $(r_1 + r_2)$ в обох зонах квантування та числом символів у першій зоні d_{v_1} :

$$2r_2 + \frac{2r_1}{\gamma} + d_{v_1} \frac{\gamma - 1}{\gamma} < d_0.$$

При $\gamma \rightarrow \infty$ тримаємо

$$2r_2 + d_{v_1} < d_0$$

і тому що величини цілочислені, то

$$2r_2 + d_{v_1} + 1 = d_0. \quad (4.29)$$

Нагадаємо, що величина d_{v_1} є не що інше, як число символів, рівень яких лежить у першій зоні квантування, тобто нижче порога. Отже, вираз (4.29) установлює зв'язок між максимальною кратністю помилок, що виправляються кодом, у другій зоні квантування і мінімальною відстанню коду за наявності d_{v_1} символів з рівнем нижче порогового значення, причому байдуже, правильно чи помилково прийняті ці символи.

У випадку прийому зі стиранням, вираз (4.28) установлює зв'язок між мінімальною відстанню коду, числом стирань і максимальною кратністю не «стертих» помилок, що виправляються кодом.

Підкреслимо, що зв'язок, який установлюється формулою (4.29), залежить тільки від мінімальної відстані коду і справедливий лише при $\gamma \rightarrow \infty$ або, що в даному випадку те ж саме, при $\gamma > d_0 - 1$. У загальному випадку справедлива умова (4.28), яка враховує параметри схеми прийому сигналів. Із цієї умови, зокрема, виходить, що не завжди байдуже, правильно чи помилково прийняті стерті символи. Інакше кажучи, формула (4.29) характеризує, які помилки може виправляти код у відповідності зі своєю структурою, а вираз (4.28) – які помилки код «має право» виправляти з урахуванням параметрів схеми прийому сигналів.

Таким чином, схема прийому сигналів чинить значний вплив на реальну виправляючу здатність коду і, тим самим, на правильність зв'язку.

Для ілюстрації розглянемо схему прийому двійкових сигналів за двох рівнів квантування, зображену на рис. 4.4, де Д – детектори, СВ – схема віднімання, ПП – порогів пристрій, ПФ – пристрій формування сигналів.

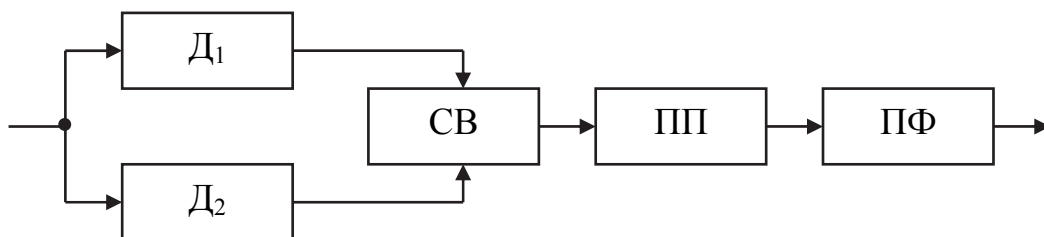


Рисунок 4.4 – Оптимальний приймач сигналів ЧМ з двома рівнями квантування

Обмежимося випадком некогерентного сигналу ЧМ в каналі з релєївськими завмираннями й адитивними шумами. Густина ймовірності сигналів на виході схеми СВ при цьому визначається виразом

$$w(y) = \frac{a^2 - b^2}{2a} e^{-a|y| + by},$$

де параметри

$$a = \frac{\sigma_{\text{сш}1}^2 + \sigma_{\text{сш}2}^2}{4\sigma_{\text{сш}1}^2 \sigma_{\text{сш}2}^2}; \quad b = \frac{\sigma_{\text{сш}1}^2 - \sigma_{\text{сш}2}^2}{4\sigma_{\text{сш}1}^2 \sigma_{\text{сш}2}^2};$$

$\sigma_{\text{сш}j}^2 = (\sigma_{\text{с}}^2 + \sigma_{\text{ш}}^2)_j$ – сумарна середня потужність сигналу ($\sigma_{\text{с}}^2 = P_{\text{с}}$) і шумів ($\sigma_{\text{ш}}^2 = P_{\text{ш}}$) в j -му частотному каналі.

При передаванні позитивного символу x_1 ймовірність попадання напруги y в першу зону квантування за відсутності спотворень

$$q_1 = \int_0^{U_0} w_{x_1}(y) dy,$$

де умовна густина ймовірності вихідної напруги демодулятора за умови, що передавався символ x_1

$$w_{x_1}(y) = \frac{1}{2\sigma_{\text{сш}}^2 (2 + h_{\text{с}0}^2)} \exp \left[\frac{h_{\text{с}0}^2(y)}{4\sigma_{\text{сш}}^2 (1 + h_{\text{с}0}^2)} - \frac{(2 + h_{\text{с}0}^2)|y|}{4\sigma_{\text{сш}}^2 (1 + h_{\text{с}0}^2)} \right];$$

U_0 – порогова напруга; $h_{\text{с}0}^2$ – середнє статистичнє перевищення сигналу.

При спотворенні позитивного символу ймовірність попадання його в першу зону

$$p_1 = \int_{-U_0}^{\infty} w_{x_1}(y) dy.$$

Підставивши значення $w_{x_1}(y)$, після інтегрування отримаємо

$$q_1 = q_0 \left(1 - e^{-\frac{q_{\text{пн}}}{1 + h_{\text{с}0}^2}} \right); \quad p_1 = p_0 \left(1 - e^{-q_{\text{пн}}} \right). \quad (4.30)$$

де нормований поріг

$$q_{\text{пн}} = \frac{U_0^2}{2\sigma_{\text{ш}}^2},$$

а ймовірності помилкового і правильного приймання символів за відсутності порога

$$p_0 = \frac{1}{2 + h_{c0}^2}; \quad q_0 = \frac{1 + h_{c0}^2}{2 + h_{c0}^2}.$$

Ймовірності попадання сигналу в другу зону квантування при правильному і помилковому прийомі відповідно будуть

$$q_2 = q_0 - q_1 = q_0 e^{-\frac{q_{пн}}{1+h_{c0}^2}}; \quad p_2 = p_0 - p_1 = p_0 e^{-q_{пн}}. \quad (4.31)$$

Підставивши ці значення в формулу, отримаємо

$$\gamma = \frac{\log \left[(1 + h_{c0}^2) e^{-\frac{h_{c0}^2}{1+h_{c0}^2} q_{пн}} \right]}{\log \left[(1 + h_{c0}^2) \frac{1 - \exp\left(-\frac{q_{пн}}{1+h_{c0}^2}\right)}{1 - \exp(-q_{пн})} \right]}. \quad (4.32)$$

Криві залежності $\gamma = f(h_{c0}^2; q_{пн})$ показані на рис. 4.5. З рисунка випливає, що нерівність (4.27) може бути забезпечена не за всіх значень h_{c0}^2 і $q_{пн}$, тобто далеко не для всіх кодів за різних умов у каналі зв'язку можна повністю використати їх виправляючу здатність.

Важливо відзначити також, що коефіцієнт γ залежить не від абсолютного, а від нормованого значення порога, тобто на нього дуже впливає рівень шумів. Це означає, що завадостійкість прийому буде визначатися не тільки перевищенням сигналу, але і потужністю шумів.

У зв'язку з цим становлять певний інтерес такі схеми прийому двійкових сигналів, в яких ця залежність була б вилучена. Прикладом може слугувати схема, де сигнали y_1 і y_2 з виходу детекторів не віднімаються, як у схемі рис. 4.4, а обчислюється деяка функція їх відношення

$$z = f(y) = f\left(\frac{y_1}{y_2}\right).$$

Однією із можливих функцій є логарифмічна:

$$f(y) = \log_a \left(\frac{y_1}{y_2} \right); \quad f^{-1}(z) = y = a^z. \quad (4.33)$$

При цьому схема прийому має вигляд рис. 4.4, але детектори повинні мати логарифмічні характеристики. Можна показати, що коефіцієнт визначається виразом

$$\gamma = \frac{\log_a \left[\left(\frac{1-p_0}{p_0} \right) \frac{p_0 + (1-p_0)f^{-1}(U_0)}{(1-p_0) + p_0 f^{-1}(U_0)} \right]}{\log_a \left[\frac{p_0 + (1+p_0)f^{-1}(U_0)}{(1-p_0) + p_0 f^{-1}(U_0)} \right]}. \quad (4.34)$$

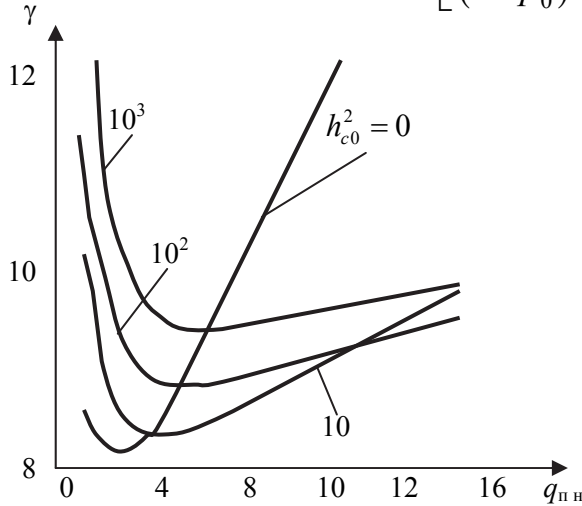


Рисунок 4.5 – Залежність $\gamma = f(h_{c0}^2; q_{пн})$

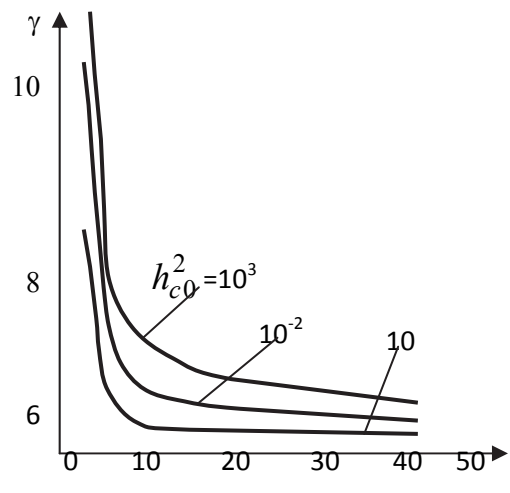


Рисунок 4.6 – Залежність $\gamma = f(a^{U_0})$

У формулу (4.34) входить тільки абсолютна величина порога U_0 , тому завадостійкість прийому залежить лише від перевищення сигналу.

На рис. 4.6 показані криві залежності $\gamma = f(a^{U_0})$, побудовані за формулою (4.34) з урахуванням (4.33). Така схема прийому також не дозволяє забезпечити нерівність $\gamma = d_0 - 1$ за будь-яких умов у каналі зв'язку.

4.3. Подання сигналів через перетини нульового рівня

Сигнали з базою $B = \Delta F \cdot t = 1$ називаються вузькосмуговими. Розглянемо сигнали такого виду:

$$z_s(t) = s(t) + j\hat{s}(t), \quad (4.35)$$

де $\hat{s}(t)$ – сигнал, спряжений сигналу $s(t)$ за Гільбертом.

Очевидно, що

$$\begin{aligned} s(t) &= \text{Re}[z_s(t)], \\ \hat{s}(t) &= \text{Im}[z_s(t)]. \end{aligned}$$

Функція $z_s(t) = s(t) + j\hat{s}(t)$ називається *аналітичним сигналом*, який відповідає вузькосмуговому сигналу $s(t)$.

Слід підкреслити, що вводячи в аналіз, крім власне сигналу $s(t)$, спряжений $\hat{s}(t)$ та аналітичний $z_s(t)$ сигнали, не можна отримати будь-якої нової інформації про сигнал, крім тої, що вже знаходиться у вихідному сигналі $s(t)$. Ці альтернативні моделі відкривають шляхи до систематизації

і спрощення методів дослідження сигналів та процесів, що відбуваються у радіотехнічних колах і системах, особливо у випадку, коли сигнал і сигнал є вузькосмуговими.

Нехай $z_s(t) \leftrightarrow Z_s(f)$ і $\hat{s}(t) \leftrightarrow \hat{S}(f)$. Тоді, можна записати

$$Z_s(f) = S(f) + j\hat{S}(f).$$

$$z_s(t) = |z_s(t)| e^{j\arg z_s(t)} = A(t) e^{j\psi(t)}.$$

За аналогією з повною фазою гармонічного сигналу повну фазу вузько смугового сигналу можна представити як: $\psi(t) = 2\pi f_0 t + \theta(t)$, де f_0 – опорна частота вузькосмугового сигналу; $\theta(t)$ – повільно змінювана функція часу. Підставимо це значення у формулу $z_s(t) = |z_s(t)| e^{j\arg z_s(t)} = A(t) e^{j\psi(t)}$, отримаємо:

$$z_s(t) = A(t) e^{j[2\pi f_0 t + \theta(t)]} = A(t) e^{j\theta(t)} e^{j2\pi f_0 t} = \hat{s}(t) e^{j2\pi f_0 t}.$$

Низькочастотна, повільно змінювана функція часу $\hat{s}(t) = A(t) e^{j\theta(t)}$ називається *комплексною обвідною сигналу* $s(t)$.

Модуль комплексної обвідної дорівнює $A(t)$ містить інформацію лише про амплітудну модуляцію сигналу, а фазовий множник $e^{j\theta(t)}$ – лише про кутову модуляцію сигналу $s(t)$.

Комплексна обвідна містить повну інформацію про сигнал. А це означає, що всю інформацію, яку може переносити вузько смуговий сигнал $s(t)$, зосереджено у його комплексній обвідній.

При аналізі проходження вузькосмугового сигналу через радіотехнічне коло *досить розглянути лише, як при цьому змінюється його комплексна обвідна*.

Таким чином, комплексна обвідна є *низькочастотним аналогом* вузько смугового сигналу.

Координатні функції подання сигналів $\varphi_k(z) = \frac{\sin z}{z}$ не є найкращими. Достоїнство їх полягає у простоті визначення вагових коефіцієнтів A_k . Проте їхній спектр недостатньо швидко спадає зі зростанням z . Функція $\frac{\sin z}{shz}$ має більшу швидкість спадання спектра, що може забезпечити менші перехідні завади у багатоканальних системах.

При розкладанні сигналів координатними функціями можливо також користуватися експонентами:

$$\varphi_{ke}(t) = \psi_k(t - l\Delta t) \exp\left(i \frac{2\pi e t}{\Delta}\right),$$

рознесеними у часі та частоті.

Зазначене розкладання пов'язане з так званими цілими функціями (ЦФ), які є деяким узагальненням визначення полінома нескінченного порядку.

Із сучасної літератури відомо, що цілими функціями описуються сигнали з обмеженою смугою, імпульсні характеристики каналів, спектральні характеристики сигналів з обмеженою тривалістю у часі. Цілі функції можна подавати через нульові перетини осі часу.

Методом такого типу подання сигналів є спектральний аналіз за перетинами нульового рівня, або, точніше, за простими (некратними) дійсними нулями досліджуваного сигналу.

Дійсними нулями сигналу $s(t)$, $0 < t < \tau$ називають точки t_1, t_2, \dots, t_m часового інтервалу $(0, \tau)$, в яких виконується співвідношення:

$$s(t_k) = 0, \quad k = 1, 2, \dots, m.$$

Помноження сигналу $s(t)$ на обмежену функцію $\mu(t)$ ($0 < \mu(t) < \infty$), що не перетворюється на нуль, не призводить до зміни його нулів, тобто нулі сигналів $\mu(t)s(t)$ і $s(t)$ збігаються. Отже, якби існував спосіб відновлення сигналу $s(t)$ за його дійсними нулями, то і спектр цього сигналу, що однозначно визначається перетворенням Фур'є

$$S(\omega) = \int_0^{\tau} s(t) e^{-i\omega t} dt, \quad (4.36)$$

допускав би відновлення за вимірними положеннями нулів t_1, t_2, \dots, t_m .

Способам відновлення сигналів широкого класу за їхніми нулями присвячено багато літератури. Надалі будуть розглядатися лише реальні сигнали спеціального вигляду

$$s(t) = \frac{1}{2} \sum_{k=-n}^n c_k e^{ik\Omega t}, \quad 0 < t < \tau, \quad \Omega = \frac{2\pi}{\tau}, \quad (4.37)$$

де $e^{ik\Omega t}$ – так звані тригонометричні багаточлени, що мають безпосереднє відношення до багатоканальних пристроїв передачі сигналів (ППС).

Незважаючи на те, що вираз (4.37) є експоненціальним багаточленом, в якому фігурують степені експоненти, сигнал $s(t)$ можна представити через формулу Ейлера

$$e^{ik\Omega t} = \cos k\Omega t + i \sin k\Omega t.$$

Задля обґрунтування цього факту нагадаємо, що спектр реального сигналу володіє наступною властивістю: його дійсна частина парна, а уявна – непарна. Стосовно коефіцієнтів Фур'є це означає, що k -й коефіцієнт Фур'є

$$c_k = a_k - ib_k,$$

де $a_k = \operatorname{Re} c_k$, $b_{-k} = -\operatorname{Im} c_{-k}$ і коефіцієнт Фур'є з індексом $-k$

$$c_{-k} = a_{-k} - ib_{-k},$$

де $a_{-k} = \operatorname{Re} c_{-k}$, $b_{-k} = -\operatorname{Im} c_{-k}$, пов'язані співвідношенням $c_k = \bar{c}_{-k}$, $k = 1, 2, \dots, n$, або, що те ж саме $a_k = a_{-k}$, $b_k = b_{-k}$, $k = 1, 2, \dots, n$.

Коефіцієнт c_0 є дійсним числом, тобто $c_0 = a_0 - ib_0$, $b_0 = 0$.

Підставивши наведені значення c_k можна показати, що

$$S(t) = \frac{a_0}{2} + \sum_{k=1}^n (a_k \cos k\Omega t + b_k \sin k\Omega t).$$

Останній вираз можна розглядати як сигнал багатоканального ППС за $\omega_0 = \Omega$, $k = 0$ і $N = n + 1$.

Хоча представлення сигналу $s(t)$ дійсно є тригонометричним, для подальшого особливий інтерес становить початкова формула (4.23 а), бо від неї легко перекинути міст до алгебраїчних багаточленів. Дійсно, ввівши позначення

$$z = e^{i\Omega t},$$

можна записати:

$$s(t) = e^{-in\Omega t} \sum_{k=-n}^n c_k e^{i(k+n)\Omega t} = z^{-n} \sum_{k=-n}^n c_k z^{k+n}.$$

Позначивши по-новому коефіцієнти багаточлена $\alpha_k = c_{k+n}$, отримаємо остаточно

$$s(t) = z^{-n} \sum_{k=0}^{2n} \alpha_k z^k.$$

Вираз $\sum_{k=0}^{2n} \alpha_k z^k$ є алгебраїчним багаточленом порядку $2n$ і має згідно з відомою теоремою алгебри в точності $2n$ коренів (нулів)

$$z_1, z_2, \dots, z_{2n}.$$

За допомогою рівності для z періодичну функцію $e^{i\Omega t}$ (інтервал її періодичності дорівнює $\frac{2\pi}{\Omega} = \tau$) можливо поставити у відповідність числам (кореням) $2n$ нулів багаточлена (4.37)

$$t_1, t_2, \dots, t_{2n}. \quad (4.38)$$

Причому

$$t_k = (1/i\Omega) \ln z_k.$$

Особливий інтерес для практики становлять дійсні нулі багаточлена $s(t)$. Такі нулі можуть бути дуже просто знайдені експериментально шляхом фіксації моментів часу, коли сигнал перетинає нульовий рівень (знаходження комплексних нулів здійснити складніше).

Може здатися, що сигнали з дійсними нулями утворюють лише надто вузький клас, який не має всіх ситуацій, що зустрічаються на практиці, і тому має обмежене значення. Проте це не так. Доведено, що існує дуже просте і витончене перетворення будь-якого багаточлена в багаточлен з дійсними нулями, аналіз якого дозволяє отримати всі

необхідні відомості про початковий багаточлен, у тому числі відтворити його форму.

Важливим питанням для практики є таке: чи можна за дійсними нулями (4.38) відновити безпосередньо багаточлен $s(t)$?

Позитивна відповідь на це питання надається за допомогою дуже простої формули:

$$s(t) = 2^{2n} \prod_{k=1}^{2n} \sin \frac{\Omega}{2} (t - t_k),$$

де t_k , $k = 1, 2, \dots, 2n$ – нулі, що зустрічалися раніше. Тобто відновити багаточлен за його нулями (в окремому випадку дійсними) можливо лише з точністю до постійного множника. Остання формула гарантує точне відновлення багаточлена (4.37) за умови, що $c_{-n} = c_n = 1$.

Для оцінки впливу похибок визначення нулів тригонометричного багаточлена на точність його спектрального аналізу необхідно мати вирази, що пов'язують коефіцієнти багаточлена (4.37) з його дійсними коренями. Незважаючи на те, що одержувачу інформації мають бути направлені коефіцієнти a_k і b_k , $k = 0, 1, 2, \dots, n$ наступні міркування будуть проведені для коефіцієнтів c_k , $k = 0, 1, 2, \dots, n$. Це допустимо через функціональний зв'язок між коефіцієнтами a_k і b_k , $k = 0, 1, 2, \dots, n$, з одного боку, і коефіцієнтами c_k , $k = 0, \pm 1, \pm 2, \dots, \pm n$ – з іншого. Нагадаємо, що $a_k = \operatorname{Re} c_k$, $b_k = -\operatorname{Im} c_k$, $k = 0, \pm 1, \dots, \pm n$. При цьому $|c_k|^2 = a_k^2 + b_k^2$ і, аналогічним чином, квадрат модуля приросту коефіцієнта c_k дорівнює сумі квадратів приростів параметрів a_k і b_k . Тому оцінка коефіцієнтів $\{c_k\}_{k=-n+1}^{n-1}$, що наводиться далі, енергетично еквівалентна оцінці «спільного» відхилення відповідних дійсних і уявних частин.

При виконанні умови $c_n = c_{-n} = 1$ багаточлен (4.37) можна представити у вигляді

$$s(t) = \frac{1}{2} e^{-in\Omega t} (1 - \alpha_1 e^{i\Omega t}) (1 - \alpha_2 e^{i\Omega t}) \dots (1 - \alpha_{2n} e^{i\Omega t}), \quad (4.39)$$

де

$$\alpha_k = e^{-i\Omega t_k}, \quad k = 0, 1, 2, \dots, 2n.$$

Справедливість формули (4.39) випливає з того факту, що числа t_1, t_2, \dots, t_{2n} , які є коренями багаточлена, перетворюють в нуль і праву частину рівності (4.39). Крім того, перемножуючи одночлени виду $(1 - \alpha_k e^{i\Omega t})$, $k = 0, 1, 2, \dots, 2n$, неважко переконатися, що добуток одиниць, які беруть участь у цих одночленах як перший доданок, породжує коефіцієнт c_{-n} , який відповідно до цього припущення, буде дорівнювати одиниці. Далі, після розкриття дужок найменший і найбільший показники

експонент в отриманому багаточлені будуть, як і в (4.37), дорівнювати відповідно $-n\Omega t$ і $n\Omega t$. Отже, праві частини у (4.37) і (4.39), будучи многочленами однакового степеня зі збіжними коренями і рівними коефіцієнтами при $e^{-in\Omega t}$, збігаються.

Для конкретних розрахунків необхідно знати дисперсію відхилень нулів σ^2 . Знайдемо вираз для такої дисперсії за умови, що має місце квантування за відомих положень нулів в інтервалі $(0, \tau)$ у цифровій формі. Ми вже говорили про те, що кожен із нулів сигналу $s(t)$ знаходиться у «своєму» інтервалі завдовжки $\frac{\tau}{2n}$. Пригадавши, що найвища частота у сигналі $s(t) \in n\Omega$, причому $\Omega = \frac{2\pi}{\tau}$, виявляємо, що довжина інтервалу Котельникова збігається з довжиною згаданого вище «власного» інтервалу кожного з нулів:

$$\tilde{\tau} = \frac{1}{2n\Omega/(2\pi)} = \frac{1}{2n(2\pi/\tau)/(2\pi)} = \frac{\tau}{2n}.$$

Для приблизного положення нуля t_k слід вказати інтервал Котельникова, в якому знаходиться цей нуль, для точнішого – відповідний підінтервал довжиною Δ -квант (рис. 4.7). Маючи на увазі двійкове кодування в цифровому процесорі УПС номера цього короткого підінтервалу комбінаціями R -значного коду, вважатимемо, що в інтервалі Котельникова міститься 2^R підінтервалів довжиною Δ . Як відомо, за рівномірного закону розподілу ймовірностей для розподілу точки t_k усередині підінтервалу довжиною Δ дисперсія шуму квантування визначається рівністю

$$\sigma^2 = \frac{\Delta^2}{12},$$

де, як було сказано

$$\Delta = \tilde{\tau} / 2^R.$$

Підставивши значення Δ і $\tilde{\tau}$ для σ^2 , отримаємо

$$\sigma^2 = \frac{\pi^2}{12n^2\Omega^2 2^{2R}}.$$

Передбачимо тепер, що до інформаційного сигналу $x(t)$ додається завада $\xi(t)$, так що суміш, яка подається на обмежувач, має вид

$$S_1(t) = \frac{1}{2} \sum_{k=-n+1}^{n-1} c_k e^{ik\Omega t} + \xi(t) + \cos n\Omega t.$$

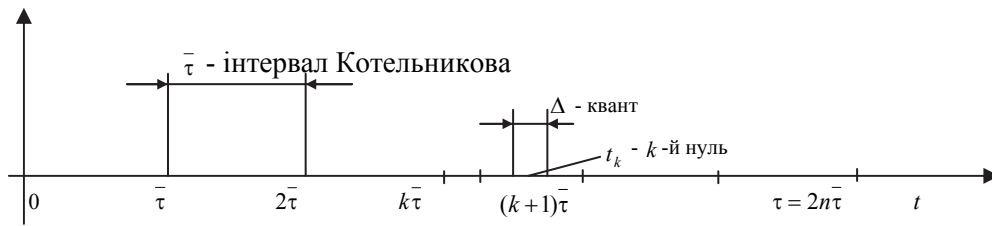


Рисунок 4.7 – Положення нуля t_k на інтервалі Котельникова

Питання, яке нас цікавить, формулюється так: яка чутливість нового методу спектрального аналізу до дії адитивної завади?

Покажемо, що відхилення результатів спектрального аналізу, які викликаються шумом $\xi(t)$, «за нулями» практично збігаються з аналогічними похибками при традиційному методі визначення коефіцієнтів $\{c_k\}_{k=-n+1}^{n-1}$.

Для вирішення сформульованого питання передбачимо, що завада $\xi(t)$ володіє рівномірним спектром і тому може бути подана у виді

$$\xi(t) = \frac{1}{2} \sum_{k=-n}^n \xi_k e^{i\Omega k t}, \quad \xi_k = \bar{\xi}_k, \quad k = 0, 1, 2, \dots, n, \quad (4.40)$$

де $\{\xi_k\}_{k=0}^n$ – випадкові комплексні взаємно незалежні величини, що володіють нульовими середніми значеннями й однаковими дисперсіями σ_3^2 .

Можна показати, що в смуго-обмеженому каналі з верхньою частотою смуги пропускання $n\Omega$ для опису реалізацій білого гауссівського шуму на кінцевому інтервалі $(0, \tau)$ необхідно враховувати також і гармоніки з номерами трохи більшими n . При цьому буде досягнуто точніший опис спектральних властивостей шуму у високочастотній області робочої смуги частот. Проте наближена модель флуктуаційної завади (4.40), яка незначно відрізняється від реальної ситуації, приводить до єдиного опису сигналу з дійсними нулями, що піддається аналізу й адитивній заваді $\xi(t)$ за допомогою тригонометричного багаточлена з максимальним за модулем степенем експоненти $n\Omega t$

$$s(t) = \frac{1}{2} \sum_{k=-n+1}^{n-1} c_k e^{ik\Omega t} + \cos n\Omega t.$$

Користуючись поданням адитивної завади (4.40), запишемо суміш «сигнал плюс шум» $s(t)$ таким чином:

$$s_1(t) = x_1(t) + \cos n\Omega t,$$

де

$$x_1(t) = \frac{1}{2} \sum_{k=-n}^n g_k e^{ik\Omega t},$$

причому

$$g_k = c_k + \xi_k, \quad k = 0, \pm 1, \dots, \pm(n-1),$$

$$g_{-n} = \xi_{-n}, \quad g_n = \xi_n.$$

Введений до розгляду сигнал $x_1(t)$ є по суті зашумленим інформаційним сигналом, коефіцієнти Фур'є якого змінені шумом відповідно до рівності $g_k = c_k + \xi_k$ і, крім того, до якого додана гармоніка шумової компоненти

$$\frac{1}{2}g_{-n}e^{-in\Omega t} + \frac{1}{2}g_n e^{in\Omega t} = |\xi_n| \cdot \cos n\Omega t.$$

Сигнал $s_1(t)$ описується дійсними простими нулями, якщо пікове значення $s_1(t)$ менше одиниці:

$$\max|s_1(t)| < 1, \quad 0 < t < \tau.$$

Вважаючи останню умову виконаною, можна подавати сигнал $s(t)$ на схему, яка здійснить спектральний аналіз сигналу $x_1(t)$ за його дійсними нулями. Результатом аналізу є не самі інформаційні параметри $\{c_k\}_{k=-n+1}^{n-1}$, а їх породжені шумом версії g_k . Оскільки параметри g_k є адитивною сумішшю корисного сигналу c_k і завади ξ_k , що виникає в каналі, то створюється враження, що спектральний аналіз «за нулями» зберігає початкове співвідношення сигнал/шум незмінним, подібно до того, як це робить класичний спектральний аналізатор, що обчислює коефіцієнти Фур'є суми сигналу і завади.

Дисперсія нуль-переходів в реальних бінарних каналах зв'язку. Нехай напруга на виході ФНЧ впливає на пороговий пристрій з характеристикою

$$u_{\Pi}(i) = \begin{cases} 1 & \text{за } u(t) > U_{\Pi} \\ -1 & \text{за } u(t) < U_{\Pi} \end{cases},$$

де $u_{\Pi}(i)$ і $u(t)$ – відповідно вихідна і вхідна напруга порогового пристрою; U_{Π} – рівень порога спрацьовування цього пристрою.

Вважатимемо, як це часто має місце на практиці, що рівень порога лежить посередині корисного сигналу відеоімпульсу. Точніше, приймемо, що при ЧМ і ФМ цей рівень дорівнює нулю (корисні відеоімпульси біполярні), а при АМ

$$U_{\Pi} = \frac{u_1 + u_0}{2},$$

де u_1 і u_0 – відповідно постійні напруги на виході детектора під час передавання посилок двох цифр – «0» і «1».

Такий пороговий рівень близький до оптимального, оскільки забезпечує приблизно однакову ймовірність помилок посилок обох знаків. За відсутності шумів пороговий пристрій даного типу дозволяв би точно

регенерувати відеоімпульс. Зокрема, тривалість відеоімпульсів на виході порогового пристрою дорівнювала б тривалості передаваних сигналів. За рахунок дії шумів зміщуються моменти спрацьовування порогового пристрою (ЗМВ). Це призводить до випадкових зміщень фронтів сигналу на виході порогового пристрою. Крім того, дія шумів призводить до дроблень цих вихідних відеоімпульсів.

Як буде описано нижче, всі ці характеристики суттєво залежать від смуги пропускання ФНЧ детектора. В зв'язку з тим, що на роботі порогових пристроїв різних типів по-різному позначаються зміщення фронтів і дроблення сигналів, що надходять на їх вхід, то слід очікувати, що для кожного типу порогового пристрою існує своє оптимальне значення смуги пропускання ФНЧ – ΔF . Враховуючи це зауваження, будемо визначати які статистичні характеристики спотворень відеоімпульсів для різних значень ΔF , що дозволить надалі визначити оптимальне значення цієї смуги.

Відзначимо також, що робота по реальних каналах не може задовільно протікати при дуже малих значеннях $q_{\text{вих}}$.

Тому, відповідно до потреб практики, ми будемо розглядати спотворення відеоімпульсів лише при $q_{\text{вих}} > 2$. Можна показати, що якщо при $q_{\text{вих}} > 2$ у момент часу t_1 реалізація шумів лежить вище переднього фронту відеоімпульсу, то на ділянці фронту, який відповідає $t < t_1$, вона також буде практично завжди лежати вище. Тому ймовірність того, що зсув фронту відеоімпульсу під дією шумів перевищить величину t_1 ($t_1 < \tau_H / 2$), збігається з імовірністю того, що у момент часу t_1 реалізація шумів лежить нижче кривої – $u(t)$ (рис. 4.8).

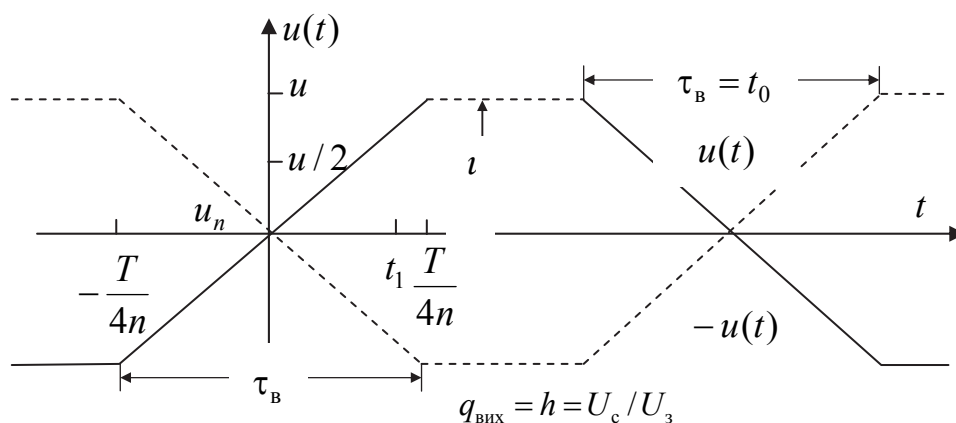


Рисунок 4.8 – Пояснення механізму виникнення зсувів фронтів відеоімпульсів

Отже функція розподілу ймовірностей зсувів фронтів для $t_1 < \frac{\tau_H}{2}$ є нормальною і має вигляд:

$$p_c(l) = \frac{4q_{\text{вих}}n}{\sqrt{2\pi}} e^{-8q_{\text{вих}}^2 n^2 l^2} \quad \text{при } |l| < \tau_{\text{НО}}, \quad (4.41)$$

де l – відносне значення зсуву фронту імпульсу $\left(l = \frac{t_1}{t_0}\right)$; $\tau_{\text{НВ}} = \frac{\tau_{\text{Н}}}{2t_0}$ –

відносна тривалість цього фронту.

На рис. 4.9 показана залежність $p_c(l)$ для різних значень $q \in 2; 3; 4$.

Дані виразу рисунка показують, що зі зростанням n за постійної величини q_1 зсув фронтів відео імпульсів необмежено зменшується. Це пояснюється тим, що зі зростанням n пропорційно зростає крутість фронту відеоімпульсу і зменшується час становлення сигналу на виході $\tau_{\text{в}}$.

Проте при цьому зменшується $q_{\text{вих}}$ і дія перших двох факторів виявляється все-таки переважаючою.

Розглянемо дію сплесків завади. Можна показати, що переважна більшість дроблень повністю розміщена усередині плоскої вершини відеоімпульсу. Кожне з перетинів нульового рівня сигналу слугує початком дроблення, або визначає зсув заднього фронту. З іншого боку, воно слугує початком деякого сплеску шумів над рівнем $q_{\text{вих}}$. Ці сплески (викиди) стимулюють появу дроблень, якщо вони закінчуються всередині плоскої вершини відеоімпульсу (нагадаємо, що переважна більшість дроблень лежить усередині плоскої вершини).

Для обчислення розподілу ймовірностей довжин дроблень при $|l| > \tau_{\text{НВ}}$ розглянемо рівень напруги сигналу – u та сплеск шумів вище рівня сигналу u_0 . Ймовірність попадання точки¹ $t = \frac{\tau_{\text{Н}}}{2}$ усередину такого сплеску збігається з імовірністю того, що напруга шумів у цей момент буде перевищувати u та дорівнювати:

$$\rho_{\text{в}}(q_{\text{вих}}) = \text{erf}(q_{\text{вих}}),$$

($\text{erf}(x)$ – функція помилок).

Нехай тепер точка $t = \frac{\tau_{\text{Н}}}{2}$ попала усередину сплеску шуму, що має тривалість $\tau_{\text{в}}$. Враховуючи, що ця точка може рівномірно займати

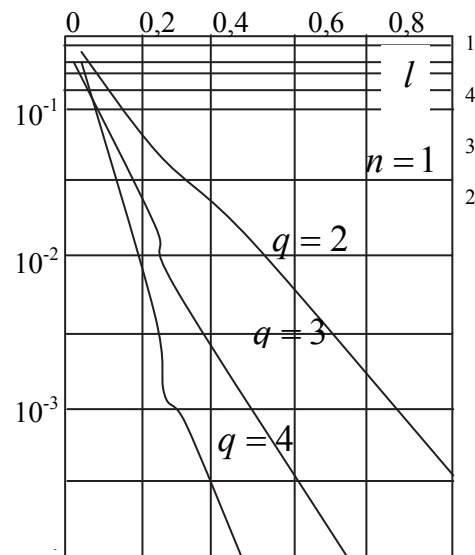


Рисунок 4.9 – Графік функції $p_c(l)$

¹ Під точкою t мається на увазі значення напруги в момент t .

будь-яке положення усередині сплеску, для умовної густини розподілу інтервалу τ_1 між точкою і кінцем викиду можна записати:

$$p_{\tau_1}(\tau/\tau_B) = \begin{cases} \frac{1}{\tau_B} & \text{при } \tau_B > \tau, \\ 0 & \text{при } \tau_B < \tau. \end{cases}$$

Тому

$$p_{\tau_1}(\tau) = \int_{\tau}^{\infty} \frac{1}{\tau_B} p_B(\tau_B) d\tau_B,$$

де $p_B(\tau)$ – розподіл тривалості сплесків шуму, причому, оскільки ми прийняли $\sigma = 1$, слід вважати $h = q_{\text{вих}}$.

Можна показати, що

$$P_c(l) = \begin{cases} F(4q_1\sqrt{nl}) & \text{при } 0 < l < \tau_{\text{HB}}, \\ F\left(\frac{q_1}{\sqrt{n}}\right) Q(l_1) & \text{при } l > \tau_{\text{HB}}, \end{cases}$$

де позначено $l_1 = \frac{l - \tau_{\text{HB}}}{t_0}$; $t_0 = \frac{\tau_B}{T}$;

$$Q(l_1) = \begin{cases} 0,98e^{-0,81l_1^2} - 3,16l_1F(1,27l_1) + 0,02 & \text{при } 0 < l_1 < 1,5, \\ 42[0,34e^{-2,93l_1} + l_1 Ei(-2,93l_1)] & \text{при } l_1 > 1,5; \end{cases} \quad (4.42)$$

$Ei(x)$ – інтегральна показова функція і $q_1 = q_{\text{вих}} \sqrt{n}$.

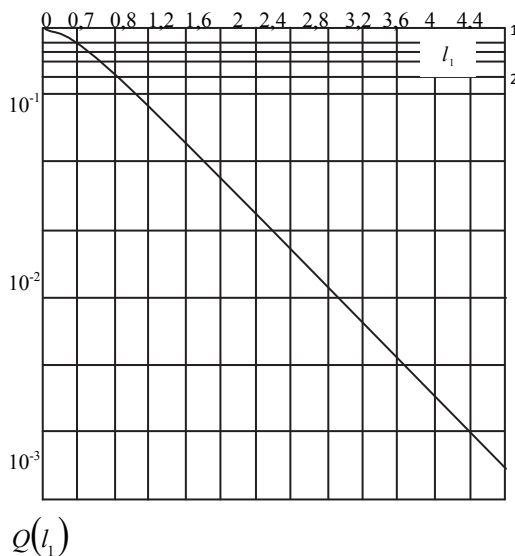


Рисунок 4.10 – Графік функції $Q(l_1)$

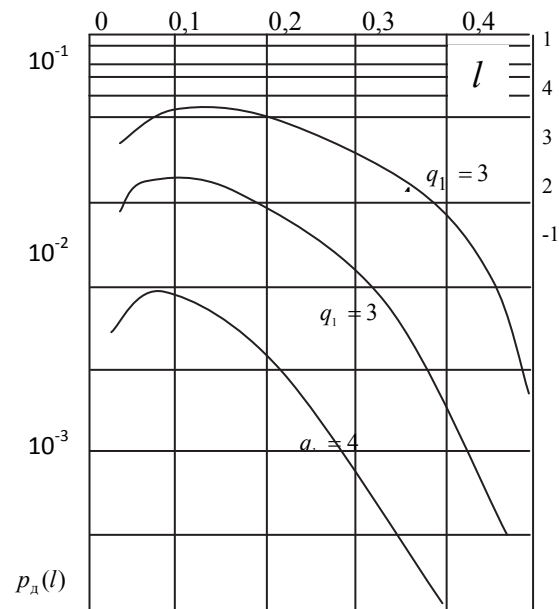


Рисунок 4.11 – Графік функції $p_n(l)$

Величина q_1 введена для зручності порівняння розподілів і є тим відношенням $q_{\text{вих}}$, яке було б, якби смуга пропускання ФНЧ була вибрана відповідною $n = 1$. На рис. 4.10 наведена залежність $Q(l_1)$, розрахована згідно з виразом (4.42).

Враховуючи вираз (4.42) ймовірність появи дроблень різної тривалості визначається:

$$\rho_d = \begin{cases} F\left(\frac{q_1}{\sqrt{n}}\right) [\tau_{\text{пв}} - \Phi(1,27\tau_{\text{пв}})] & \text{при } \tau_{\text{пв}} < 1,5, \\ F\left(\frac{q_1}{\sqrt{n}}\right) [\tau_{\text{пв}} - 1 + 4,87e^{-2,93\tau_{\text{пв}}}] & \text{при } \tau_{\text{пв}} > 1,5, \end{cases}, \quad \tau_{\text{пв}} = \frac{T_{\text{пл}}}{t_0} \quad (4.43)$$

Розподіл ймовірностей нормованої тривалості дроблень складає:

$$p_d(l) = \begin{cases} \delta(l)(1 - \rho_d) + 1,6 \frac{l(\tau_{\text{пв}} - l)}{t_0^3} F\left(\frac{q_1}{\sqrt{n}}\right) e^{-0,8 \frac{l^2}{t_0^2}} & \text{при } 0 \leq l < 1,5t_0 \text{ і } l < \tau_{\text{пв}}, \\ \frac{42(\tau_{\text{пв}} - l)}{t_0^2} F\left(\frac{q_1}{\sqrt{n}}\right) e^{-2,93 \frac{l}{t_0}} & \text{при } l > 1,5t_0 \text{ і } l < \tau_{\text{пв}}, \\ 0 & \text{при } l > \tau_{\text{пв}} \text{ і } l < 0. \end{cases} \quad (4.44)$$

Розподіл $p_d(l)$ для $n = 1$ і деяких h наведено на рис. 4.11 (враховується відносна величина l).

Аналіз виразів (4.43), (4.44) і залежностей $p_d(l)$ свідчить, що зі зростанням n при постійному значенні q_1 ймовірність дроблень збільшується. Це пояснюється зменшенням середньої тривалості сплеску і співвідношення сигнал/завада зі зростанням n .

На закінчення відзначимо, що наведені вище дані про зсув фронтів і дроблення відеоімпульсів під дією шумів добре узгоджуються з результатами експериментальних досліджень.

4.4. Статистичні параметри каналів моделі Гільберта

Розглянемо більш докладно модель Гільберта і визначимо її основні параметри. Дана модель передбачає наявність двох станів дискретного каналу. У «хорошому» стані, або Х-стані, помилок не виникає. У «поганому», або П-стані, можливе виникнення помилок з імовірністю $p_{\text{п}}$. Зміна станів описується ланцюгом Маркова. Поведінка системи може бути представлена графом (рис. 4.12).

Зміна станів моделі визначається матрицею перехідних ймовірностей

$$P = \begin{bmatrix} P_{XX} & P_{X\Pi} \\ P_{\Pi X} & P_{\Pi\Pi} \end{bmatrix}. \quad (4.45)$$

Дискретним кроком системи є одиничний елемент. Сенс перехідної ймовірності – P_{xy} є ймовірністю переходу системи на наступному кроці в стан y , якщо на поточному кроці вона перебувала у стані x . Дана матриця стохастична, тобто сума членів кожного рядка дорівнює одиниці:

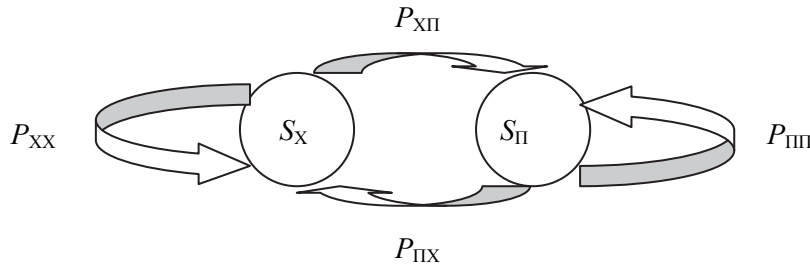


Рисунок 4.12 – Граф станів моделі Гільберта

$$P_{XX} + P_{\Pi X} = 1, P_{\Pi X} + P_{\Pi\Pi} = 1.$$

Фінальні (граничні) ймовірності знаходження у станах визначаються виразами:

$$P_{\Pi} = \frac{P_{X\Pi}}{P_{\Pi X} + P_{X\Pi}}, P_X = \frac{P_{\Pi X}}{P_{\Pi X} + P_{X\Pi}}, \quad (4.46)$$

Середня ймовірність помилкового прийому елемента

$$\overline{p_n} = p_n \cdot P_{\Pi} = p_n \cdot \frac{P_{X\Pi}}{P_{\Pi X} + P_{X\Pi}}. \quad (4.47)$$

Середні довжини поганого і хорошого станів каналу

$$\tilde{l}_X = \frac{1}{P_{X\Pi}}; \tilde{l}_{\Pi} = \frac{1}{P_{\Pi X}}. \quad (4.48)$$

Коефіцієнт групування

$$\alpha = 1 - P_{X\Pi} - P_{\Pi X}. \quad (4.49)$$

Параметри моделі Гільберта визначають середні довжини «хорошого» і «поганого» станів, іншими словами середні довжини пакетів помилок і відстані між ними. Тому можна оцінювати шукані параметри, використовуючи статистику $\tilde{l}_X, \tilde{l}_{\Pi}$, довжин станів. Визначивши середні довжини станів, можна легко оцінити параметри каналу:

$$P_{X\Pi} = \frac{1}{\tilde{l}_X}; P_{\Pi X} = 1 - P_{X\Pi}; P_{\Pi X} = \frac{1}{\tilde{l}_{\Pi}}; P_{XX} = 1 - P_{\Pi X}. \quad (4.50)$$

Визначити ймовірність помилки в П-стані можна, розділивши загальну кількість помилок за час контролю на сумарну довжину поганого стану:

$$p_{\Pi} = N_{\Pi} / \sum_i D_{bi}, \quad (4.51)$$

або, враховуючи відоме співвідношення

$$\overline{p_{\Pi}} = p_{\Pi} \cdot P_{\Pi} = p_{\Pi} \cdot \frac{P_{X\Pi}}{P_{\Pi X} + P_{X\Pi}},$$

отримаємо

$$p_{\Pi} = \frac{\overline{p_{\Pi}}}{P_{\Pi X}} (P_{X\Pi} + P_{\Pi X}) = \overline{p_{\Pi}} \left(1 + \frac{\tilde{l}_X}{\tilde{l}_{\Pi}}\right). \quad (4.52)$$

Принциповим моментом у даній задачі є знаходження меж станів у потоці, що аналізується.

Звичайно пакетом помилок вважається ділянка потоку, що починається і закінчується помилковим елементом, усередині якого відстань між помилками не перевищує деякої величини \hat{k} . У випадку каналу Гільберта поганий стан може починатися і закінчуватися правильно прийнятими елементами, а у деяких випадках може взагалі не містити помилок. Якщо П-стан розглядати як пакет, то можливе штучне заниження величини l_{Π} , що, у свою чергу, призводить до спотворень оцінок усіх інших параметрів моделі. Для виключення даної методичної похибки необхідно збільшувати довжину кожного пакету на деяку величину ρ або зменшувати довжину X-стану.

Визначимо величину максимальної відстані \hat{k} між помилками, що належать одному пакету. Дана величина є змінною і залежить від конкретного набору значень параметрів моделі. Для її визначення розглянемо залежність ймовірності того, що після помилки буде не менше k безпомилкових елементів (рис. 4.13).

Початкова ділянка цієї залежності характеризує розподіл довжин серій безпомилкових елементів в пакетах, а полога відображає відстані між пакетами. Зазначені ділянки зазвичай добре апроксимуються прямими. Точка перетину цих прямих, як показали експерименти, досить задовільно визначає величину \hat{k} – максимальну відстань між помилками у пакеті.

Визначити коефіцієнти рівнянь прямих можна, застосовуючи операцію лінійної регресії точок початкової ділянки для $k = 1..4$ % і пологої ділянки $k = 20..100$ %. У результаті регресії можна отримати рівняння двох прямих

$$P(0^k | 1) = a_1 k - b_1,$$

$$P(0^k | 1) = a_2 k - b_2.$$

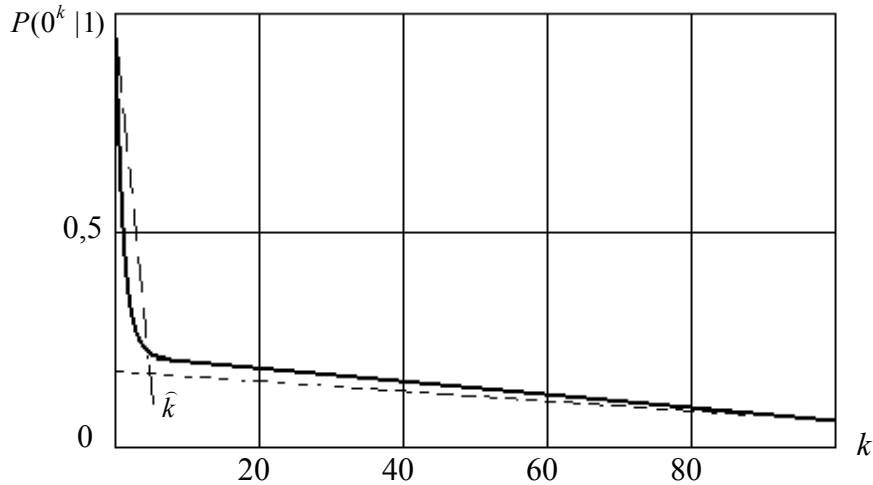


Рисунок 4.13 – Залежність ймовірності серій безпомилкових елементів

Тоді $\hat{k} = \text{ceil} [(b_2 - b_1) / (a_1 - a_2)]$, де $\text{ceil}(x)$ – функція, що повертає найменше ціле число, яке більше або дорівнює x .

Розглянемо існуючі відомі розв'язання задачі обчислення ймовірності появи m помилок у прийнятому блоці довжиною n елементів для дискретного каналу, що описується моделлю Гільберта. Позначимо цю величину через $P(m, n)$. Зважаючи на громіздкість математичних перетворень, які є у роботах Еліота, зупинимося на заключних формулах для $P(m, n)$.

У роботах Еліота для обчислення шуканої ймовірності було отримано такий вираз:

$$P(m, n) = \sum_{k=1}^{n-m+1} p_n P(k) R(m, n-k+1), \quad 1 \leq m \leq n, \quad (4.53)$$

де $p_n = p_n P_{\text{ХП}} / (P_{\text{ХП}} + P_{\text{ПХ}})$ – безумовна ймовірність помилки; $P(k) = P(0^{k-1} | 1)$ – ймовірність появи серії не менше $k-1$ безпомилкового елемента (нулів) після помилки; $R(m, n)$ – ймовірність того, що у $n-1$ символі за помилкою з'явиться ще $m-1$ помилок,

$$R(m, n) = \sum_{k=1}^{n-m+1} p(k) R(m-1, n-k), \quad 2 \leq m \leq n; \quad R(1, n) = P(n),$$

$p(k) = P(0^{k-1} | 1)$ ймовірність того, що довжина серії дорівнює $k-1$.

Для визначення величини $P(k)$ і $p(k)$ звернемося до роботи Гільберта, в якій використовувалися подібні величини $U(K) = P(0^K | 1)$, $V(K) = P(0^{k-1} | 1)$. Для $k \geq 2$ вказані вирази мають вигляд:

$$U(K) = (P_{\text{ХХ}} + hP_{\text{ПП}})U(K-1) + h(P_{\text{ПХ}} - P_{\text{ХХ}})U(K-2);$$

$$U(0) = 1; U(1) = P_{\text{ПХ}} + hP_{\text{ПП}},$$

де $h = 1 - p_n$ – ймовірність вірного прийому елемента у «поганому» стані.

Зв'язок між величинами $U(K)$ і $V(K)$ визначається виразом $V(K) = U(K) - U(K+1)$. Звісно, що $P(k) = U(k-1)$, $p(k) = U(k-1) - U(k)$.

Недоліком цієї методики є значні витрати машинного часу на розрахунок навіть для відносно невеликих довжин блоків. На рис. 4.14 наведена усереднена залежність часу розрахунку $P(5, n)$ у секундах при використанні комп'ютера з процесором Celeron 300 МГц.

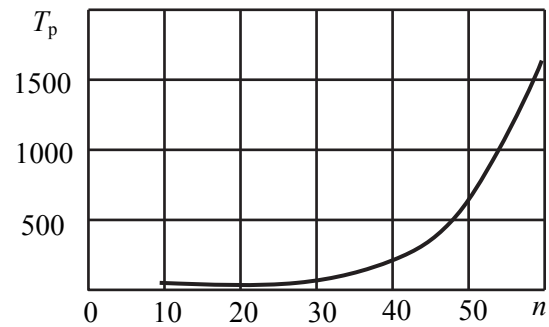


Рисунок 4.14 – Графік залежності витрат машинного часу від довжини блока

З рисунка бачимо, що затрати машинного часу збільшуються у геометричній прогресії при збільшенні довжини блока. Очевидно, що ця методика стає неефективною при аналізі реальних блоків у сотні і тисячі елементів.

Розглянемо більш детально можливі рішення задачі обчислення ймовірності появи помилок m у прийнятому блоці довжиною n елементів для дискретного каналу, що описується моделлю Гільберта. У відповідності з моделлю Гільберта помилки можуть виникати тільки у «поганому» стані каналу, тому перед обчисленням $P(m, n)$ необхідно визначити ймовірності $B(i, n)$ того, що з n елементів блока i елементів були передані у «поганому» стані каналу. При цьому всі ймовірності $B(i, n)$ для $i = 0 \dots n$ будуть несумісними і складати повну групу подій. Це твердження дозволяє зробити перевірку правильності розрахунків, виходячи з

необхідності дотримання умови $\sum_{i=0}^n B(i, n) = 1$, а також отримати інтегральну оцінку похибок при використанні спрощених алгоритмів обчислень.

Після обчислення ймовірностей $B(i, n)$ ймовірність m -кратної помилки у блоці з n елементів можна визначити, використовуючи формулу

$$p(m, n) = \sum_{i=0}^n B(i, n) p(m | i), \quad (4.54)$$

де $p(m | i) = C_i^m p_n^m (1 - p_n)^{i-m}$ – ймовірність m -кратної помилки, якщо число елементів у П-стані дорівнює i ; p_n – ймовірність помилки у П-стані;

$C_i^m = \frac{i!}{m!(i-m)!}$ – число сполучень з i по m .

Основну складність при розв'язанні задачі визначення $P(m, n)$ становить знаходження ймовірностей $B(i, n)$, що відрізняються точністю отримання результату і витратами обчислювальних ресурсів. При передаванні блока довжиною n елементів можлива багаторазова зміна станів каналу. Введемо поняття вектора стану каналу як масиву з n двійкових чисел, в якому нуль відповідає передачі поточного елемента у

«поганому» стані каналу. При фіксованій величині i кількість відповідних векторів стану каналу визначається як число сполучень із n по i . На відміну від каналу з незалежними помилками у даному випадку кожен вектор буде характеризуватися своєю імовірністю. Таким чином, шукана величина $B(i, n)$ являє собою суму ймовірностей усіх векторів стану каналу, довжиною n і вагою i . Для прикладу розглянемо знаходження ймовірності $B(3, 5)$.

Усього можливих векторів станів каналу буде:

$$C_5^3 = \frac{5!}{3!(5-3)!} = 10.$$

Усі вектори станів каналу для даного випадку і відповідні їм ймовірності наведені у таблиці 4.1. Ймовірності, що відповідають векторам станів, визначаються фінальними та перехідними ймовірностями моделі Гільберта. Підсумувавши всі 10 добутків, ми отримаємо ймовірність події $B(3, 5)$.

Ймовірності, що відповідають векторам станів, визначаються фінальними ймовірностями моделі Гільберта. Підсумувавши усі 10 добутків, ми отримаємо ймовірність події $B(3, 5)$.

Зауважимо, що усі розглянуті вектори є двійковими комбінаціями однієї ваги $i = 3$.

Проаналізувавши вектори станів та відповідні їм добутки ймовірностей, можна сформулювати правила переходу від двійкової форми запису до побудови формул для обчислень відповідної ймовірності.

1. Якщо двійкова комбінація починається з 1, то перший множник P_{Π} , якщо 0 – то P_X .
2. Якщо перед поточною 1 була 1, то їй відповідає $P_{\Pi\Pi}$.
3. Якщо перед поточною 1 був 0, то – $P_{X\Pi}$.
4. Якщо перед поточним 0 була 1, то – $P_{\Pi X}$.
5. Якщо перед поточним 0 був 0, то – P_{XX} .

Таблиця 4.1– Вектори станів каналу і відповідні їм ймовірності

Стан	Вектор стану каналу	Ймовірність вектору стану каналу
1	11100	$P_{\Pi} P_{\Pi\Pi} P_{\Pi\Pi\Pi} P_{\Pi X} P_{XX}$
2	01110	$P_X P_{X\Pi} P_{\Pi\Pi} P_{\Pi\Pi} P_{\Pi X}$
3	00111	$P_X P_{XX} P_{X\Pi} P_{\Pi\Pi} P_{\Pi\Pi}$
4	10110	$P_{\Pi} P_{\Pi X} P_{X\Pi} P_{\Pi\Pi} P_{\Pi X}$
5	10011	$P_{\Pi} P_{\Pi X} P_{XX} P_{X\Pi} P_{\Pi\Pi}$
6	11010	$P_{\Pi} P_{\Pi\Pi} P_{\Pi X} P_{X\Pi} P_{\Pi X}$
7	11001	$P_{\Pi} P_{\Pi\Pi} P_{\Pi X} P_{XX} P_{XX}$
8	01011	$P_X P_{X\Pi} P_{\Pi X} P_{X\Pi} P_{\Pi\Pi}$
9	01101	$P_X P_{X\Pi} P_{\Pi\Pi} P_{\Pi X} P_{X\Pi}$
10	10101	$P_{\Pi} P_{\Pi X} P_{X\Pi} P_{\Pi X} P_{X\Pi}$

Отримані правила відповідності дозволяють побудувати досить нескладні алгоритми обчислення ймовірності $B(i, n)$ для будь-яких значень

i та n . В основі даного алгоритму лежить перебір усіх двійкових комбінацій довжини n , вибір з них комбінацій ваги i , заміни обраних комбінацій добутками і підсумовування отриманих добутків. Заміна операції перебору генерацією двійкових чисел заданої ваги дозволить дещо скоротити час роботи програми. На рис. 4.15 наведено графік залежності ймовірності $P(m, n)$ для блоку довжиною 15 елементів.

Оцінка складності обчислення ймовірності m -кратної помилки у блоці довжиною n елементів. Для отримання можливості об'єктивного порівняння витрат обчислювальних ресурсів різних методик необхідно вибрати деякі величини, які кількісно характеризують ці витрати і не залежать від швидкодії процесора і оптимальності алгоритмів. Оберемо в якості таких величин кількість операцій додавання і множення, необхідних для обчислення одного значення ймовірності $P(m, n)$ і проведемо їхню оцінку. Так, для обчислення $P(m, n)$ за методикою Еліота необхідно визначити $(n-m+1)$ значення $R(m, n)$, кожне з яких потребує визначення кількох значень $R(x, y)$ з меншими індексами. На рис. 4.16 наочно показана послідовність обчислення $R(m, n)$ для визначення ймовірності $P(3, 5)$ і логічні зв'язки між ними. Зробивши узагальнення, можна сказати, що для обчислення одного значення $P(m, n)$ необхідно обчислити $(n - m + 1)m$ значень $R(m, n)$.

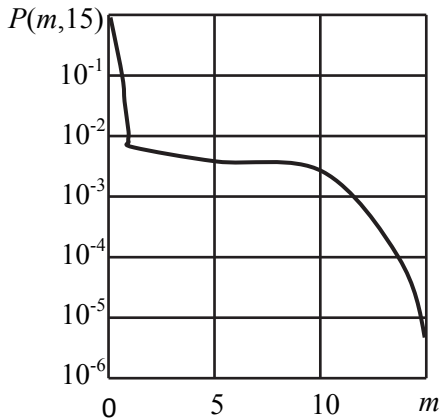


Рисунок 4.15 – Графік ймовірності m -кратної помилки у блоці довжиною 15 елементів

Прийmemo наступні умови:

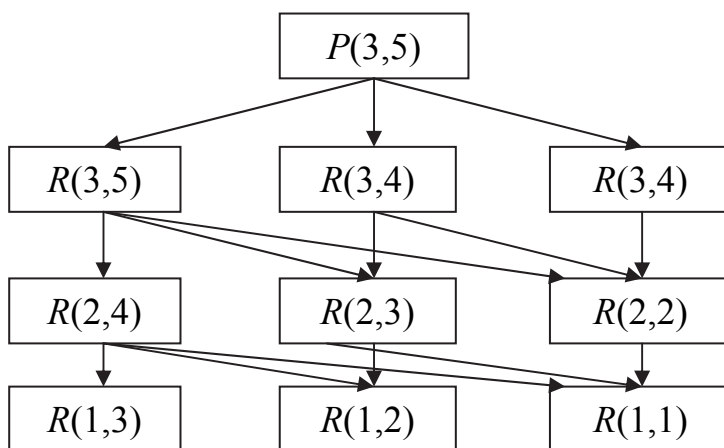


Рисунок 4.16 – До визначення $P(3,5)$

представлення числа n ;

- 1) операція віднімання еквівалентна операції додавання;
- 2) операція ділення еквівалентна операції множення;
- 3) число операцій множення, необхідних для зведення до ступеня, визначатимемо за алгоритмом Аль-Коші:

$$x^n \rightarrow \log_2(n) + W(n),$$

де $W(n)$ – вага двійкового

4) число операцій множення, необхідних для обчислення сполучення

$$C_n^t = \frac{n!}{t!(n-t)!} \text{ дорівнює } 2t + 1, \text{ якщо } n - t > t, \text{ або } 2(n - t) + 1, \text{ якщо } t > n - t.$$

Оцінимо складність обчислення $P(m, n)$. Після чисел і виразів, які одержані внаслідок множення ставитимемо букву «М». В аналогічних випадках для позначення результатів сумування будемо використовувати букву «С».

Для розрахунку за виразом (4.54) потрібно $2(n - m + 1)$ добутків і $(n - m)$ підсумовувань. Обчислення всіх необхідних значень $R(m, n)$ вимагає

$$\left[(m-1) \sum_{i=1}^{n-m+1} i \right] M + \left[(m-1) \sum_{j=1}^{n-m} j \right] C$$

операцій.

Обчислення масиву $P(k)$ вимагає $(n - m + 1)(4M + 4C)$ операцій а масиву $p(k) - (n - m + 1)C$.

Таким чином складність обчислення $P(m, n)$ за алгоритмом Еліота визначається виразом

$$\begin{aligned} C^{El} &= (n - m)C + 2(n - m + 1)M + \left[(m-1) \sum_{i=1}^{n-m+1} i \right] M + \left[(m-1) \sum_{j=1}^{n-m} j \right] C + \\ &+ (n - m + 1)C + (n - m + 1)(4M + 4C) = \left[6(n - m + 1) - 1 + (m-1) \sum_{i=1}^{n-m+1} j \right] C + \\ &+ \left[6(n - m + 1) + (m-1) \sum_{i=1}^{n-m+1} i \right] M. \end{aligned}$$

Користуючись вищенаведеними домовленостями, були отримані витрати операцій обчислення одного значення $P(m, n)$ за спрощеною методикою. На рис. 4.17 наведено залежності при n , що варіюється від 5 до 128, за методикою Еліота і спрощеною методикою при числі врахованих повернь, яке дорівнює 7.

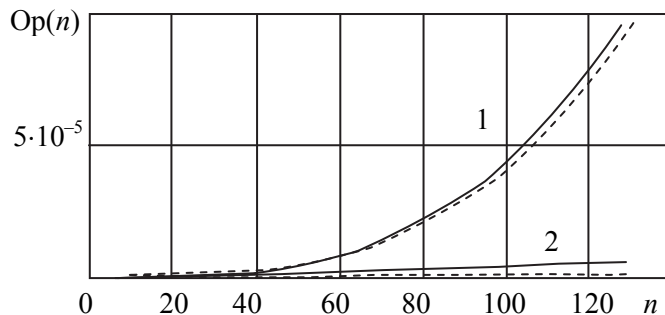


Рисунок 4.17 – Залежності витрат операцій підсумовування і множення на обчислення $(5, n)$ від n : 1 – за методикою Еліота; 2 – за спрощеною методикою

Графіки наочно демонструють перевагу спрощеної методики у діапазоні довжин блоків більше 30. Слід зазначити, що зі зростанням збільшення витрат операцій за спрощеною методикою має лінійний характер, а за методикою Еліота – показники. За такого характеру залежностей виграш за затратами операцій від застосування спрощеної методики буде збільшуватися зі зростанням n .

З принципів побудови алгоритмів обчислення імовірностей $P(\geq t, n)$ коригуючих кодів слід зробити такі висновки: при зростанні кодової відстані d_{\min} , тобто при збільшенні корегувальної спроможності різко збільшується кількість надлишкових елементів (n), що зменшує відносну швидкість передавання інформації. Згідно з таблицею (додаток 7), якісний корегуючий код, що виправляє усі помилки $t_k \in 1 \dots 5$ ($d_{\min} = 11$) за наявності 50 інформаційних елементів повинен мати 40 перевіірочних елементів.

У такому кодї для декодування однієї комбінації необхідно часу близько 2,4 с (суперкомп'ютер Blue Gene/2007, що здійснює 478 трлн. оп/с). Це означає, що при швидкості передавання 1 Мб/с за секунду передається $[10^6 \dots 90 \approx 10^4]$ кодових 100-бітових комбінацій за умови, що оброблення однієї займає до 2,4 с. Таким чином, задача синтезу алгоритмів декодування з меншими затратами часу при простому перебиранні всіх можливих кратностей помилок є задачею затримки інформації.

Встановимо функціональну залежність між параметрами ефективності використання блокових коригуючих РЦК та параметрами узгодженості структури помилок у даному каналі з найбільш імовірними помилками

$$\eta \approx \frac{P(\geq 1, n)}{P(\geq 1, n) - P_{\text{ВП}}(n)}.$$

Для каналів з групуванням помилок аналітичний вираз для імовірності появи помилок на виході декодера

$$P_n[(t_b + 1), n] = \left(\frac{n}{t_b + 1} \right)^{1-\alpha} P_e, \quad (4.55)$$

де α знаходиться експериментально для різних каналів і має значення $0 \leq \alpha \leq 1$.

Формула (4.55) справедлива при $(t_b + 1)/n < 0,3$. Для порівняння значень P_n для каналу з незалежними помилками ($\alpha = 0$)

$$P_{\text{ВП}}[(t_b \pm 1), n] = \sum_{t=t_b+1}^n C_n^t P_e^t (1 - P_e)^{n-t}$$

і значенням згідно з виразом 4.55 на рис. 4.18 показані залежності P_n і $P_{\text{ВП}}$ для каналу з ЧМ при $P_e = 2 \cdot 10^{-3}$ $\alpha = 0,34$ і швидкості передавання $B = 1200$ Бод. Аналіз залежностей показує, що вираз h_n дає занижені значення ймовірностей появи помилок, що не виправляються даним кодом.

Аналітичний вираз для оцінки ефективності коду у режимі виправлення помилок можна подати:

$$h = \frac{P(\geq 1, n)}{P(\geq 1, n) - P[t_B(-1 \div t_{\text{зад}})]}$$

Для каналу з групуванням помилок імовірність появи помилок на виході декодера визначається виразом (4.55). При виконанні умови $n/t_B > 10/3$ зазначену ймовірність можна оцінити наближено:

$$P(t_B > 0, n) = n^{1-\alpha} P_e. \quad (4.56)$$

Поділивши вираз (4.56) на вираз (4.55) отримаємо аналітичний вираз для h_k :

$$h_k = \frac{n^{1-\alpha} P_n}{\left(\frac{n}{t_B + 1}\right)^{1-\alpha} P_n} = (t_B + 1)^{1-\alpha}.$$

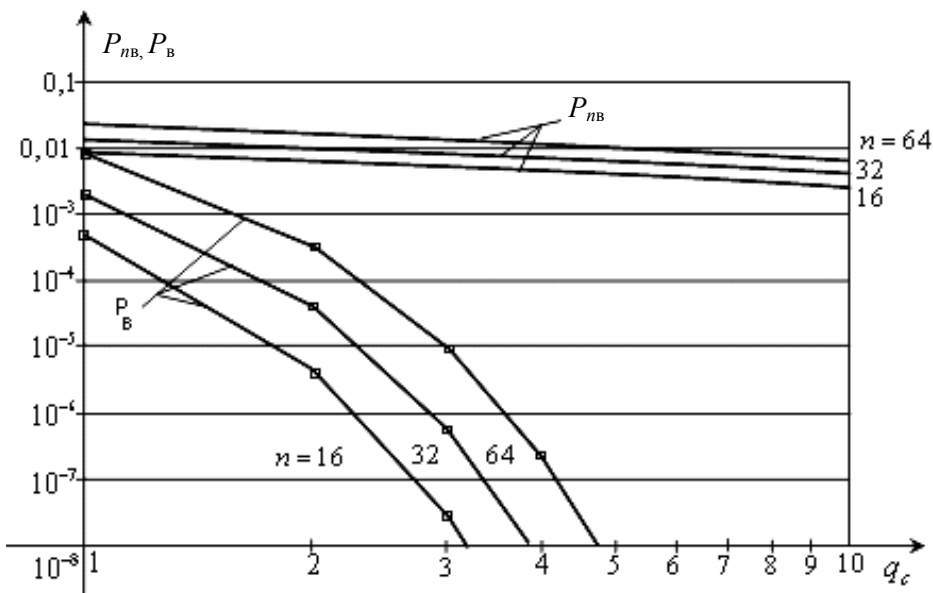


Рисунок 4.18 – Залежність ймовірностей не виправлення помилок від q_c

Отже ефективність коду у першому наближенні можна визначити маючи коефіцієнт групування, так максимальну кратність виправленої помилки (t_B). Наприклад, при $t_B = 8$, $\alpha = 0,5$: $h_k = \sqrt{9}$, тобто такий код підвищує вірність усього втричі.

Розглянемо ефективність коду для випадку відсутності обмеження на кратність виправленої помилки $1 < t_B \leq t_{B3}$. Тоді ймовірність не виправлених помилок визначатиметься:

$$P_{\text{нв}} = P[(t_n > 0, n)] - P[(t_n \leq t_3), n] \quad (4.57)$$

Для ефективності коду будемо мати:

$$h_k = \frac{P[(t_n > 0); n]}{P[(t_n > 0); n] - P[(t_n < t_3); n]} = \left[1 - \frac{P[(t_n < t_3); n]}{P[(t_n > 0); n]} \right]^{-1}, \quad (4.58)$$

$\frac{P[(t_n < t_3); n]}{P[(t_n > 0); n]} = -Z$ і визначає питому вагу значення ймовірності

виправлених помилок. Для реальних каналів це відношення знаходиться у межах 0,5...0,9.

Подамо параметр Z у виді:

$$\frac{P[(t_n < t_3); n]}{P[(t_n > 0); n]} = \frac{P[(t_n \leq t_3); n]}{\sum_i^{N''} P_i} \cdot \frac{\sum_{i=1}^{N''} P_i}{\sum_{i=1}^{N'} P_i} = UP, \quad (4.59)$$

де $p(Z)$ – ймовірність появи i -го ненульового синдрому за умови, що нумерація проведена у межах $P_{i+} \leq P_i$, для будь-якого i ; $N'' = 2^n - 1$ – загальна кількість ненульових синдромів, які є найбільш ймовірними; U – коефіцієнт узгодженості коду з каналом

$$U = \frac{P[(t_n \leq t_3), n]}{\sum_{i=1}^{N''} P_i}, 0 \leq U \leq 1,$$

P – показник найбільш імовірних помилок у каналі зв'язку

$$P = \frac{\sum_{i=1}^{N''} P_i}{\sum_{i=1}^{N'} P_i}, 0 \leq P \leq 1. \quad (4.60)$$

Таким чином ефективність коригуючого коду може визначатися параметрами U і P . На рис. 4.19 наведена номограма для значень ефективності при розрахованих для виразу (4.60) значеннях P . Із номограми видно, що для більшості значень P величина коефіцієнта h є $6 \div 25$, який підтверджує результати наведених вище експериментів отриманих на реальних каналах.

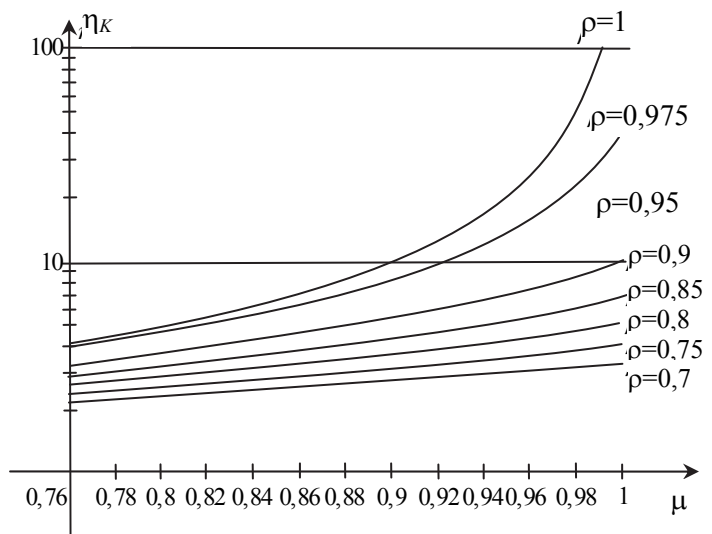


Рисунок 4.19 – Номограма визначення ефективності коду

4.5. Передавання сигналів укрупненими сигнальними конструкціями позиційного кодування

Існує два методи передавання повідомлень – поелементний і укрупненими сигналами. В першому випадку окремі елементи кодових конструкцій, число яких (m) визначається об'ємом (M) алфавіту джерела повідомлень.

$$m = E^+(\log_2 M),$$

де E^+ означає, що у випадках, коли M не дорівнює 2^i (i – ціле число), то береться найближче більше ціле.

При поелементному передаванні m -значні двійкові кодові конструкції (КК) з енергією елементів $mQ_c^2 = BT_{\text{кк}}Q_c^2$ передаються по каналу символ за символом. Частіше за все для цього вибираються ортогональні сигнали

$$U_c(t) = \sum_{i=1}^m \sqrt{Q_c^2} \psi_i(t - it_0), \quad i = 1, 2, \dots, m$$

де $\psi_i(t)$ – нормована за енергією координатна функція.

Таким чином, передавання одного повідомлення займає $T_{\text{кк}}$ секунд. Усі можливі кодові конструкції можна розмістити у вершинах 2^m -вимірного гіперкуба. Тоді ймовірність мінімум однієї помилки в кодовому слові для гауссового каналу буде

$$P_{\text{пкк}} = 1 - (1 - P_e)^m = 1 - (1 - P_e)^{Bt_0}, \quad (4.61)$$

де B – швидкість передавання (модуляції інформаційного параметра).

Ймовірність спотворення елемента кодового слова визначається виразом

$$P_e = \Phi\left(\sqrt{\frac{P_c}{v_{\text{ш}}^2 B}}\right),$$

де $P_e = \Phi(\bullet)$ – символ інтеграла ймовірності.

Прийом елементів КК реалізується послідовно незалежно один від одного з використанням, наприклад, критерію максимуму подібності. Як впливає з виразу (4.61), при заданих P_c і B ймовірність помилкового прийому зростає зі збільшенням елементності кодового слова (m). При фіксованих $T_{\text{кк}}$ ймовірність $P_{\text{пкк}}$ може бути зменшена лише при збільшенні енергії елементарних посилок Q_c^2 (середньої потужності сигналу) або при зменшенні швидкості передавання B (тобто зменшенням елементності коду).

На рис. 4.20, а наведено сигнальну конструкцію 4-елементного кодового слова (1011), яка відповідає числу 11 для

поелементного передавання, а на рис. 4.20, б на одинадцятому місці розміщений інформаційний сигнал, місцезнаходження якого на осі часу відповідає кодовому слову 1011.

Передаваний сигнал характеризується

$$U_{ci} = \sqrt{Q_c^2} \Psi_i(t - it_0), \quad (4.62)$$

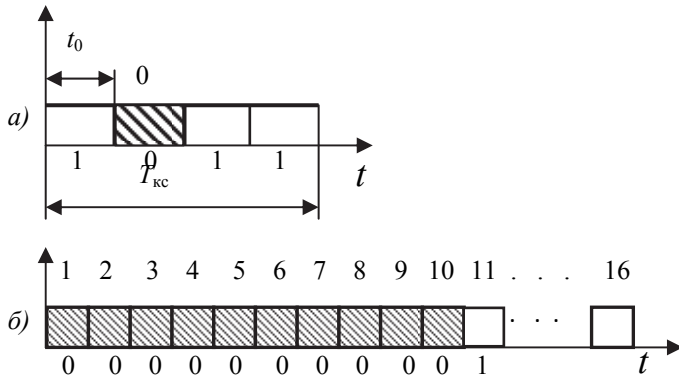


Рисунок 4.20 – Сигнальна конструкція 4-елементної КК для поелементного передавання

де $\Psi_i(t - it_0)$ – нормована за енергією координатна функція з одиничною енергією на інтервалі $t_0 = \frac{T_{кc}}{m}$.

У зв'язку з тим, що величина функції

$$\Phi(h_c^2) < e^{-h_c^2},$$

то ймовірність помилки для $M = 2^m$ рівно-ймовірних ортогональних сигналів з однаковою

енергією обмежена значенням

$$P_e < M e^{-h_c^2}.$$

Підставивши в останній вираз $M = 2^{BT_c}$ і $h^2 = \frac{P_c t_0}{v_{ш}^2}$, отримаємо

$$P_e < \exp \left[-T_c \left(\frac{P_c}{v_{ш}^2} - B \ln 2 \right) \right] \quad (4.63)$$

Із формули (4.63) виходить, що при передачі укрупненими сигналами ймовірність помилки експоненційно зменшується зі збільшенням $T_{ск}$ до тих пір, поки швидкість передачі інформації

$$v_i < v_{i \text{ макс}} = \frac{P_c}{v_{ш}^2 \ln 2} = 1,443 \frac{P_c}{v_{ш}^2}. \quad (4.64)$$

Вираз (4.64) можна подати у вигляді

$$P_{пк} < 2^m e^{-\frac{m Q_c^2}{v_{ш}^2}} = e^{-m(h_c^2 - \ln 2)}. \quad (4.65)$$

Порівняння виразів (4.60) і (4.65) дає змогу зробити висновок, що при посимвольному передаванні $P_{пк} \rightarrow 1$ зі збільшенням m незалежно від h_c^2 , а при передаванні укрупненими сигналами для $h_c^2 > \ln 2$ значення $P_{пк} \rightarrow 0$ зі збільшенням m .

Така відмінність в характері зміни величини $P_{\text{пк}}$ пояснюється наступним: при посимвольному передаванні сигнальні конструкції знаходяться у вершинах m -мірного гіперкуба і відстань між суміжними сигналами, яка дорівнює $2\sqrt{Q_c^2}$, зберігається постійною із збільшенням m , в той час, коли мірність суміжних точок збільшується лінійно. Тому ймовірність попадання сумарного вектору $U_{c\Sigma} = U_c + U_{\text{ш}}$ в суміжну зону рішення зі збільшенням m зростає. При передачі укрупненими ортогональними сигналами відстань між найближчими точками m -вимірного простору визначається виразом $\sqrt{2mQ_c^2}$, тобто зростає пропорційно \sqrt{m} . На жаль розглянута передача укрупненими сигналами зі швидкістю $B = 1,443 \frac{P_c}{v_{\text{ш}}^2}$ для малого значення P_c потребують великих значень t_0 .

Однією із задач при передаванні даних укрупненими сигналами є усунення взаємозв'язків між елементами сигналу. Такого роду зв'язок може бути виражений через кореляцію сигналу. Відсутність взаємозв'язків передбачає відсутність кореляції. Тому процес усунення взаємозв'язків будемо коротко називати декореляцією.

Відомі методи декореляції сигналу: метод передбачення та наведений вище метод укрупнення. Розглянемо нижче метод укрупнення.

Загальна ідея методу полягає в тому, що сигнал розбивається не на елементи, а на відрізки, кожний з яких складається з декількох елементів (елементарних посилянь). Такі відрізки можуть розглядатися як елементи деякого нового сигналу, і можна сказати, що імовірність зв'язків між такими укрупненими елементами більш слабка, ніж між елементами первинного, не укрупненого сигналу. Слід мати на увазі, що при укрупненні сигналу відбувається перетворення, що являється переходом до коду з більш високою основою коду $a_1 = a^r$, де a – первинна основа, а r – число елементів у відрізку. Розглянемо деякі співвідношення, що відносяться до методу укрупнення.

При існуванні взаємозв'язків кількість відомостей виражається через умовні ймовірності появи даного елемента за наявності певних значень попередніх елементів. Розглянемо приклад, коли враховується зв'язок тільки двох сусідніх елементів, тобто коли поява даного елемента залежить лише від попереднього. В цьому випадку:

$$I' = -\sum_{i=1}^m p(i) \sum_{j=1}^m p\left(\frac{j}{i}\right) \log p\left(\frac{j}{i}\right). \quad (4.66)$$

Перетворимо цей вираз за допомогою формули повної імовірності, з якої ми отримаємо для умовної імовірності

$$p(j/i) = \frac{p(ij)}{p(i)}, \quad (4.67)$$

де $p(ij)$ – ймовірність появи пари значень ij . Підставивши (4.67) в (4.66)

$$\begin{aligned} I' &= -\sum_{i=1}^m p(i) \sum_{j=1}^m \frac{p(ij)}{p(i)} \log \frac{p(ij)}{p(i)} = -\sum_{i=1}^m \sum_{j=1}^m p(ij) \log \frac{p(ij)}{p(i)} = \\ &= -\left[\sum_i \sum_j p(ij) \log p(ij) - \sum_i \sum_j p(ij) \log p(i) \right]. \end{aligned}$$

Друга сума спрощується:

$$-\sum_i \sum_j p(ij) \log p(i) = -\sum_i \log p(i) \sum_j p(ij) = -\sum_i p(i) \log p(i) = I_1'.$$

Перша сума спроститься, якщо ми будемо розглядати кожен пару значень ij як новий елемент k . Число таких елементів буде m^2 . Таким чином, для першої суми можна записати:

$$-\sum_i \sum_j p(ij) \log p(ij) = \sum_{k=1}^{m^2} p(k) \log p(k) = I_k'.$$

Отже, $I' = I_k' - I_1'$.

Ми можемо дійсно створити новий, укрупнений сигнал, в якому роль елементів будуть відігравати пари значень ij .

Змістовність укрупненого сигналу

$$I_k' = -\sum_{k=1}^{m^2} p(k) \log p(k). \quad (4.68)$$

Таким чином, описане вище перетворення збільшує змістовність на

$$I_1' = -\sum_{i=1}^m p(i) \log p(i),$$

об'єм сигналу при цьому залишається незмінним. З одного боку об'єм зростає вдвічі через збільшення числа елементів, тобто збільшення основи коду, з іншого боку, спадає в стільки ж разів внаслідок того, що один елемент нового сигналу представляє пару елементів первісного сигналу.

Нехай n та m – число елементів і основа коду для первісного, а n_1 та m_1 – ті ж самі величини, що і для укрупненого сигналу. Тоді

$$V_1 = n_1 \log m_1 = \frac{n}{2} \log m^2 = n \log m = V.$$

Через те, що в укрупненому сигналі $n_1 = \frac{n}{2}$, то повна кількість відомостей до перетворення і після перетворення виражаються відповідно як

$$I = nI_1, I_k = n_1 I'_k = \frac{n}{2} I'_k.$$

Корисний результат укрупнення можна характеризувати відносним збільшенням кількості відомостей, тобто величиною

$$\frac{I_k - I}{I} = \frac{I'_k}{2I'} - 1.$$

Якщо б пари були цілком незалежними, то укрупнений сигнал був би повністю декорельований (у разі якщо кореляція існувала тільки між елементами 1 та 2, 3 та 4, ... l та $l + 1$, ... Тоді між парами 1, 2, 3, 4; ... l , $l + 1$; ... кореляція була б відсутня).

Насправді кореляція може існувати між будь-якими сусідніми елементами. Тому кореляція може бути і між парами. В зв'язку з цим маємо:

$$I'_k = -\sum_{k=1}^{m_2} p(k) \sum_{k=1}^{m_2} p(l/k) \log p(l/k),$$

де l – дана пара, k – попередня пара. Але кореляція між парами слабкіша, ніж між елементами первісного сигналу. Це можна пояснити тим, що лише останній елемент попередньої пари впливає на перший елемент наступної пари. Тому, об'єднавши елементи в пари, ми частково декорелюємо сигнал, та надлишковість R_p для укрупненого сигналу менше, ніж для первісного.

Процес укрупнення відрізків сигналу можна продовжити. Так, наприклад, пари можна з'єднати в чотирьохелементні групи. Це дало б подальшу декореляцію. Якщо повідомлення поділено на відрізки l_s , що складаються з r елементів кожний, і якщо загально можливе число таких відрізків є $m_1 = m^r$, то кількість відомостей на відрізок для повністю декорельованого сигналу є $-\sum_{s=1}^{m_1} p(l_s) \log p(l_s)$, а кількість відомостей на елемент

$$I' = -\frac{1}{r} \sum_{s=1}^{m_1} p(l_s) \log p(l_s).$$

Отже, один з можливих методів декореляції сигналу полягає в тому, що формується новий сигнал, елементами якого є відрізки з того чи іншого числа елементів первісного сигналу. Ця операція зменшує надлишковість тим більше, чим довше беруться відрізки.

Приклад 1. Маємо 2 елементи a та b ($m = 2$). $p(a) = 0,75$, $p(b) = 0,25$; $p(a/a) = 2/3$, $p(b/a) = 1/3$, $p(a/b) = 1$, $p(b/b) = 0$.

Розрахуємо ймовірності пар, тобто $p(ij)$

$$p(ab) = p(a) p(b/a) = 0,25;$$

$$p(ba) = p(b) p(a/b) = 0,25;$$

$$p(aa) = p(a) p(a/a) = 0,5;$$

$$p(bb) = p(b) p(b/b) = 0.$$

Розрахуємо змістовність для сигналу, що складається з пар елементів:

$$I_k' = -\sum_{k=1}^{m^2} p_k \log p_k = -(p(ab) \log p(ab) + p(ba) \log p(ba) + p(aa) \log p(aa) + p(aa) \log p(aa) + p(bb) \log p(bb)) = 1,5$$

$$\text{Повна кількість відомостей } I_k = n_1 I_k' = 0,5 n I_k' = 0,75n.$$

$$\text{Для первісного сигналу } I = -n \sum_{i=1}^m p(i) \sum_{j=1}^m p(j/i) \log p(j/i) = 0,685n.$$

$$\text{Приріст кількості відомостей } I_1 = I_k - I = 0,065n.$$

$$\text{Відносне збільшення кількості відомостей складає: } \frac{I_1}{I} \cdot 100 = 9,5\%.$$

Отриманий частково декорельований сигнал можна піддати подальшому обробленню – кодуванню та модуляції, але по-перше треба нормалізувати розподіл імовірностей.

Приклад 2. Нехай існує джерело повідомлень із продуктивністю $H = H_{\max} = \log_2 l$, а $l \neq 2^m$.

Розглянемо варіант коли $l = 10$ (0, 1, 2 ... 9). Швидкість передавання в такому каналі згідно з теоремою Шеннона може бути як завгодно

$$\text{близькою до } \frac{C}{H} \approx \frac{v}{\log_2 10} = \frac{v}{3,332}.$$

Для передавання по каналу використовується 4-елементний код ($2^4 = 16 > 10$).

$$\text{Надлишковість дорівнює } \frac{4 - 3,332}{4} = 0,167.$$

Після укрупнення сигналу з $l = 10$ до $l_1 = 100$ (00, 01, 02, ..., 99) потрібно буде використати 7-елементний код ($2^7 = 128 > 100$). Отримаємо

$$\text{надлишковість } \frac{(7 - 6,6438)}{7} = 0,05.$$

Наступні укрупнення – $l_2 = 1000$ (000, 001, 002, ..., 999) призведуть до зниження надлишковості до 0,003.

Все вищезазначене справедливе для каналу без завад. У реальних умовах зменшення надлишковості може призвести до неможливості виправлення помилок на прийомі. В разі використання методу укрупнення, формування нового алфавіту і зменшення надлишковості слід використовувати завадостійкі коди.

Як відомо, ентропія, володіє важливою властивістю адитивності. Перехід до укрупнених елементів коду забезпечує збільшення середнього значення ентропії на елемент повідомлення в m разів оскільки середнє

значення ентропії на поліграму дорівнює сумі середніх значень ентропії на елемент поліграми.

Якщо середню ентропію на елемент вихідного повідомлення прийняти рівною h_1 , то після укрупнення середня ентропія на елемент дорівнює $h_2 = rh_1$. Максимальна ентропія повідомлення з укрупненими елементами

$$H_{2\max} = \log_2 N_2 = r \log_2 N_1 = rH_{1\max},$$

де N_2 – об'єм укрупненого алфавіту; N_1 – об'єм первинного алфавіту; $H_{1\max}$ – максимальна ентропія первинного повідомлення. Надлишковість повідомлення з укрупненими елементами

$$k_{i2} = 1 - \frac{H_2}{H_{2\max}} = 1 - \frac{H_1}{H_{1\max}} = k_{i1}, \quad (4.69)$$

де k_{i1} – надлишковість первинного повідомлення.

Вираз (4.69) показує, що укрупнення елементів не забезпечує зменшення надлишковості повідомлень. Це пояснюється тим, що при укрупненні елементів зменшення надлишковості за рахунок ослаблення зв'язків між елементами компенсується збільшенням надлишковості за рахунок більш нерівномірного розподілу ймовірностей елементів.

Необхідно скористатися для подальшої мінімізації середньої кількості кодових символів на один елемент повідомлення оптимальним статистичним кодуванням. Це забезпечить отримання максимально можливої кількості інформації, що передається кодовими комбінаціями при заданій тривалості роботи каналу, тобто пропускної здатності каналу.

Припустимо, що кодуєчий пристрій може формувати різні кодові комбінації з тривалостями t_1, t_2, \dots, t_m .

Задача полягає в тому, щоб встановити таку залежність між тривалостями кодових комбінацій t_i та ймовірностями їх надходження P_i , за якої забезпечується максимальна швидкість передавання інформації.

Нехай для передачі повідомлення тривалістю T необхідно N кодових комбінацій. Тоді повинні бути справедливі наступні рівності:

$$N = \sum_{i=1}^m n_i, \quad (4.70)$$

$$T = \sum_{i=1}^m n_i t_i, \quad (4.71)$$

$$\sum_{i=1}^m p_i = 1, \quad (4.72)$$

$$T = N \sum_{i=1}^m p_i t_i, \quad (4.73)$$

де n_i — середня кількість i -х кодових комбінацій, які використовується при передавання повідомлень.

Повна кількість інформації, що міститься в повідомленні тривалістю T при незалежності появи його елементів має вигляд

$$I = -N \sum_{i=1}^m p_i \log_2 p_i. \quad (4.74)$$

Поставлена задача зводиться до забезпечення максимуму кількості інформації I відповідним вибором величин N і p_i при дотриманні умов (4.72) та (4.73).

Задача може бути розв'язана методом невизначених множників Лагранжа. У відповідності з цим методом складемо нову функцію

$$F = -N \sum_{i=1}^m p_i \log_2 p_i + \lambda_1 \left(1 - \sum_{i=1}^m p_i \right) + \lambda_2 \left(T - N \sum_{i=1}^m p_i t_i \right).$$

Визначимо максимум цієї функції, для чого знайдемо заздалегідь її часткові похідні по N і P_i та прирівняємо їх до нуля

$$\begin{aligned} \frac{\partial F}{\partial N} &= -N \sum_{i=1}^m p_i \log_2 p_i - \lambda_2 \sum_{i=1}^m p_i t_i = 0, \\ \frac{\partial F}{\partial p_i} &= -N \left(\log_2 p_i + \frac{1}{\ln 2} \right) - \lambda_1 - \lambda_2 N t_i = 0, \quad (i = 1, 2, \dots, m). \end{aligned}$$

З другого рівняння знайдемо

$$\log_2 p_i = -\frac{\lambda_1}{N} - \lambda_2 t_i - \frac{1}{\ln 2}, \quad (i = 1, 2, \dots, m) \quad (4.75)$$

і, підставивши цей вираз в перше рівняння, матимемо $\sum_{i=1}^m p_i \left(-\frac{\lambda_1}{N} - \frac{1}{\ln 2} \right) = 0$, звідки $\lambda_1 = -\frac{N}{\ln 2}$.

Підставивши знайдене значення в (4.75), отримаємо $\log_2 p_i = -\lambda_2 t_i$ ($i = 1, 2, \dots, m$), звідки

$$p_i = 2^{-\lambda_2 t_i} \quad (i = 1, 2, \dots, m). \quad (4.76)$$

Цей вираз показує характер залежності між тривалостями кодових комбінацій та ймовірностями їх появи при оптимальному кодуванні. З виразу видно, що кодові комбінації з малою ймовірністю появи повинні мати більшу тривалість і навпаки.

Для з'ясування фізичного значення коефіцієнта λ_2 підставимо (4.76) в (4.74). Оскільки умова (4.76) визначає умову максимізації кількості переданої інформації за заданий час T , то отримаємо

$$-N \sum_{i=1}^m p_i (\lambda_2 t_i) = N \lambda_2 \sum_{i=1}^m p_i t_i = \lambda_2 T = I_{\max},$$

звідки

$$\lambda_2 = \frac{I_{\max}}{T} = c,$$

тобто коефіцієнт λ_2 чисельно дорівнює пропускній здатності каналу передавання інформації. Таким чином,

$$p_i = 2^{-ct_i} \quad (i = 1, 2, \dots, m), \quad (4.77)$$

де

$$t_i = -\frac{\log_2 p_i}{c} \quad (i = 1, 2, \dots, m). \quad (4.78)$$

Вирази (4.77) і (4.78) визначають умови узгодження роботи кодуєчого пристрою зі статистичними властивостями переданих повідомлень. Це забезпечує передавання інформації каналом зі швидкістю, яка практично дорівнює його пропускній здатності.

Для двійкового каналу з відсутністю статистичних зв'язків між символами задовольняє код Шеннона-Фано, який розглянуто в курсі «Теорія електричного зв'язку».

Методика побудови коду Шеннона-Фано для випадку передавання чотирьох символів повідомлення з імовірностями $p(x_1) = 0,5$; $p(x_2) = 0,25$; $p(x_3) = 0,125$; $p(x_4) = 0,125$ ілюструється у табл. 4.2.

Підрахуємо швидкість передавання інформації, яка забезпечується отриманим кодом. Нехай тривалість символів кодових комбінацій дорівнює t_0 . Тоді середня тривалість кодових комбінацій

$$\bar{T} = p(x_1)t_0 + p(x_2)2t_0 + p(x_3)3t_0 + p(x_4)3t_0 = 1,75t_0.$$

Середня ентропія на символ повідомлення

$$H(X) = -\sum_{i=1}^4 p(x_i) \log_2 p(x_i) = 1,75 \frac{\text{дв.од.}}{\text{повід.}}$$

Таблиця 4.2 – Методика побудови коду Шеннона-Фано для випадку передавання чотирьох символів повідомлення при $p(x_1) = 0,5$; $p(x_2) = 0,25$; $p(x_3) = 0,125$; $p(x_4) = 0,125$

Символи повідомлень	Імовірність	Етапи розподілу на підгрупи				Символи кодових комбінацій			
		1	2	3	4	1	2	3	4
x_1	0,5	I				0			
x_2	0,25	II	I			1	0		
x_3	0,125		II	I		1	1	0	
x_4	0,125			II		1	1	1	

Таким чином, швидкість передавання інформації

$$\bar{I}(X) = \frac{1}{t_0} = C \frac{\text{дв.од.}}{c}.$$

Отже, отриманий код в розглянутому випадку дав змогу отримати максимально можливе значення швидкості передавання інформації, тобто

Таблиця 4.3 – Символи та відповідні їм імовірності появи

Символи	x_1	x_2	x_3
Ймовірність	0,2	0,7	0,1

забезпечити повне узгодження статистичних характеристик джерела повідомлень з властивостями каналу. Це вдалося завдяки тому, що в розглянутому прикладі значення імовірностей $p(x_i)$ вибрані такими, що умови поділу на підгрупи вдається виконати точно. У реальних умовах це, як правило, не

забезпечується і швидкість передавання інформації буде менше пропускної здатності каналу.

Ефективність кодування може бути за необхідності збільшена шляхом переходу від кодування одиночних символів повідомлення до кодування груп символів, причому з укрупненням груп ефективність буде підвищуватися. Підвищення ефективності відбувається при цьому за рахунок того, що при укрупненні груп набір імовірностей, що отримується, можна ділити на більш близькі імовірності підгрупи. Методика побудови коду Шеннона-Фано шляхом кодування груп символів повідомлення ілюструється таким прикладом.

Порівняємо швидкість передавання для трьох символів з імовірностями табл. 4.3 при незалежному передаванні і групуванням по два символи. При $m = 3$ довжина коду повинна дорівнювати $n = 2$.

Ймовірні варіанти кодових комбінацій подані в табл. 4.4. Тривалість кодових комбінацій $T = 2t_0 = 2$ мс. Ентропія повідомлення

$$H(X) = -\sum_{i=1}^3 p(x_i) \log_2 p(x_i) = -0,2 \log_2 0,2 - 0,7 \log_2 0,7 - 0,1 \log_2 0,1 = 1,16 \text{ дв.од/с.}$$

Таблиця 4.4 –
Ймовірні варіанти
кодових комбінацій

Символ повідомлення	Код
x_1	00
x_2	01
x_3	10

Швидкість передавання інформації при використанні рівномірного двійкового коду

$$\bar{I}(X) = \frac{H(X)}{T} = \frac{1,16}{2 \cdot 10^{-3}} = 580 \text{ дв.од/с.}$$

Довжина кодових комбінацій для першого і другого випадків наведена в табл. 4.5 і 4.6.

Таблиця 4.5 – Довжина кодових комбінацій при кодуванні одиничних символів

Символ повідомлення	Імовірність	Розподіл на групи		Код	Тривалість кодових комбінацій
		I	II		
x_1	0,7	I		0	t_0
x_2	0,2	II	I	10	$2t_0$
x_3	0,1		II	11	$2t_0$

Таблиця 4.6 – Довжина кодових комбінацій при кодуванні групових символів

Групи символів	Імовірність	Розподіл на групи				Код	Тривалість кодової комбінації		
		I	II	III	IV				
$x_2 x_2$	0,49	I				0	t_0		
$x_1 x_2$	0,14	II	I	I		100	$3t_0$		
$x_2 x_1$	0,14			II		101	$3t_0$		
$x_2 x_3$	0,07	II	II	I	I	1100	$4t_0$		
$x_3 x_2$	0,07				II		1101	$4t_0$	
$x_1 x_1$	0,04			II	II	I		1110	$4t_0$
$x_1 x_3$	0,02					I		11110	$5t_0$
$x_3 x_1$	0,02	II	II	II	I	111110	$6t_0$		
$x_3 x_3$	0,01				II		111111	$6t_0$	

Середня тривалість кодових комбінацій при передаванні групами по 2:

$$\bar{T} = 0,49t_0 + 2 \cdot 0,14 \cdot 3t_0 + 2 \cdot 0,07 \cdot 4t_0 + 0,04 \cdot 4t_0 + 0,02 \cdot 5t_0 + \\ + 0,02 \cdot 6t_0 + 0,01 \cdot 6t_0 = 1,165 \text{ мс.}$$

Швидкість передавання інформації

$$\bar{I}(x) = \frac{1,16}{1,165 \cdot 10^{-3}} = 995 \frac{\text{дв.од.}}{\text{с}}.$$

4.6. Таймерні сигнальні конструкції як інструментарій збільшення питомої ваги інформації на інтервалі найквістового елемента позиційного кодування

У попередніх розділах глави 4 був проведений аналіз причин низької ефективності синтезованих на базі шеннонівської теорії коригуючих кодів для симплексних систем у реальних каналах моделі Гільберта.

Результати статистичних вимірювань використання реальних кодів у реальних умовах передавання свідчать, що основними причинами, які впливають на низьку ефективність є:

1) Багатомірність коригуючих кодових конструкцій, яка при оцінці умов виправлення помилок заданої кратності навіть за відносно малоелементних кодових слів (до 100 елементарних сигналів) потребують потужних процесорів для декодування.

Наприклад, при використанні найбільш часто застосованих методів декодування – синдромного методу, в якому реалізується просте правило розрахунку місця знаходження помилки, потребує 2^{n_i} порівнянь, а також визначення синдрому помилки з урахуванням великої кількості суміжних класів кодів.

У табл. 4.7 наведено число синдромів суміжних класів для кодів різної довжини та заданої кратності виправлення помилок.

2) Відповідно низька потужність процесорів, які використовуються у декодерах коригуючих кодів.

При цьому слід зауважити, що при синтезі кодової множини із заданими параметрами можливі два випадки:

1) довжина кодової конструкції обмежена $T_{\text{кв}} = \text{const}$ і збільшення елементності кодового слова може бути проведено за рахунок зменшення елемента кодового слова $t_e \neq \text{const}$;

2) мінімальна відстань між суміжними моментами модуляції у кожній реалізації не менше найквістового елемента t_0 і збільшення надлишковості коду може тільки збільшувати довжину кодового слова ($T_{\text{кв}}$).

У першому випадку це стосуються широкосмугових каналів з базою $B = t_0 \cdot \Delta F \gg 1$, в другому – для кабельних каналів з базою $B = t_0 \cdot \Delta F = 1$.

Незважаючи на це слід пам'ятати, що надлишковість коду, під якою розуміється введення в кодограму додаткових перевірючих елементів, сама по собі не збільшує завадостійкість, а забезпечує лише перерозподіл відстаней між сигнальними конструкціями. Тому, якщо простий код забезпечує рівну віддаленість всіх кодових слів кодової множини, то введення додаткових елементів не має сенсу, так як завадостійкість в кращому випадку не зменшиться.

Таблиця 4.7 – Кількість синдромів суміжних класів (при $t_{\text{вип}} \leq 5$).

	Кратність виправлення помилок	n						
		15	31	63	127	255	511	1023
$\sum_{i=1}^{t_i} C_n^i$	$t = 1$	15	31	63	127	255	511	1023
	$t = 2$	120	496	2016	8128	32640	130816	523776
	$t = 3$	575	4991	41727	341503	2763775	22239231	178434047
	$t = 4$		36456	637392	10676128	174825280	2830007936	$4,5367 \cdot 10^{10}$
	$t = 5$		206367	7666239	264907903	8812312831	$2,87530 \cdot 10^{11}$	$9,2912 \cdot 10^{12}$
	C_n^i	$t = 1$	15	31	63	127	255	511
$t = 2$		105	465	1953	8001	32385	130305	522753
$t = 3$		455	4495	39711	333375	2731135	22108415	177910271
$t = 4$			31465	595665	10334625	172061505	2807768705	$1,5367 \cdot 10^{10}$
$t = 5$			169911	7028847	254231775	8637487551	$2,84707 \cdot 10^{11}$	$9,2458 \cdot 10^{12}$

Взагалі завадостійкість кодів з надлишковістю при заданій енергії кодового слова залежить тільки від коефіцієнта кореляції кодових слів $\rho_{c,i}$. Цей коефіцієнт дорівнює косинусу кута між векторами кодограм. Для випадку постійної енергії кодового слова ($Q_{\text{кк}} = \text{const}$) імовірність прийому без помилок визначається коефіцієнтом взаємозв'язку відповідних кодограм. Введення додаткових (корегувальних) елементів забезпечує оптимальне їх розміщення для забезпечення максимальної завадостійкості. Для групових (n, m) кодів з основою a (a – число станів інформаційного параметра) встановлено взаємозв'язок

$$\frac{1}{n} \sum_{j=1}^a d_j = 2^{m-1}$$

або при рівності всіх відстаней між кодовими словами

$$\frac{d_0}{n} = \frac{2^{m-1}}{a-1} = \frac{a}{2(a-1)}. \quad (4.79)$$

Зважаючи на те, що

$$\rho_{ci} = \rho(A_c, A_i) = \frac{A_c A_i}{\sigma_{A_c} \sigma_{A_i}} = 1 - \frac{2d_{ci}}{n}. \quad (4.80)$$

Коефіцієнт кореляції

$$\rho = -\frac{1}{a-1}. \quad (4.81)$$

Вираз (4.81) показує відоме співвідношення для симплексних кодів найкращої системи з рівними кодovими відстанями. В зв'язку з виразом (4.81) двійкові коди з ФМ є найкращими з усіх можливих для каналів з постійних параметрами і забезпечують максимальну завадостійкість, яку можна вважати за потенційну.

У теорії широкосмугових сигналів кодові конструкції симплексних коригуючих (n, m) кодів представляють як особливий вид сигналів з базою

$$B_{\text{ск}} = \frac{nt_0}{mt_0} = \frac{n}{m} = \frac{m+k}{m} = 1 + R_i,$$

де R_i – коефіцієнт відносної надлишковості.

Доведено, що для різних значень числа інформаційних елементів (m) завадостійкість буде максимальною

$$B_{\text{ск}} = \frac{2^{m-1}}{m}. \quad (4.82)$$

При синтезі надлишкових коригуючих кодів з позиційним кодуванням в якості бази вибирається добуток довжини елементарного сигналу (t_0) на смугу каналу зв'язку.

Із підрозділів 4.1...4.5 зрозуміло, що суттєвий вплив на ефективність коду при конкретному каналі зв'язку має групування помилок на виході каналу.

У роботах колективу кафедри Інформаційної безпеки і передавання даних отримані аналітичні залежності основних статистичних параметрів потоку помилок від середнього значення спотворених помилок на одне спотворене кодове слово.

– коефіцієнт групування $\alpha = \frac{\ln \bar{t}}{\ln n}$;

– ймовірність появи спотвореного кодового слова із n елементів $P(\geq 1, n) = \frac{n}{\bar{t}} P_e$;

– ймовірність появи спотвореного кодового слова з m і більше помилками

$$P(\geq m, n) = \frac{n}{m} \frac{m^\alpha}{\bar{t}} P_e. \quad (4.83)$$

Отримана функціональна залежність коефіцієнта групування α помилок з коефіцієнтом кореляції

$$\alpha = 1 - \frac{\ln \left\{ 1 - \left[\sum_{i=1}^{n-1} r(a_1, \dots, a_{n-i}, a_{n+1-i}) r(a_1, \dots, a_{n-i}) \prod_{j=n-i+1}^n p(a_j) + \prod_{j=1}^n p(a_j) \right] \right\} - \ln[1 - p(a)]}{\ln n}, \quad (4.84)$$

де $r(a_1, \dots, a_{n+1-i})$, $\sigma(a_1, \dots, a_{n-i})$ – коефіцієнт кореляції помилок і середньоквадратичне відхилення ймовірностей відповідних подій.

Для випадку незалежних помилок

$$\alpha_n = 1 - \frac{\ln[1 - P^n(a)] - \ln[1 - P(a)]}{\ln n}.$$

На основі оброблення результатів статистичних вимірювань на реальних каналах МТМ встановлено, що кусочно-стаціонарна модель вироджується в модель Гільберта з двома станами з відносними термінами існування:

- канал в «хорошому» стані $t_x \geq 0,995 T_{\text{пер}}$;
- канал в «поганому» стані $t_{\text{п}} \leq 0,005 T_{\text{пер}}$.

При цьому в «хорошому» стані ймовірність помилкового приймання елементу визначається

$$P_{\text{ex}} = \frac{1}{2} e^{-\frac{h_c^2}{2}}. \quad (4.85)$$

Ймовірність помилкового приймання елемента кодового слова в «поганому» стані каналу

$$P_{\text{еп}} = \frac{1}{2 + h_{\text{co}}^2}. \quad (4.86)$$

З метою визначення співвідношення (сигнал/завада) в «хорошому» стані були проведені виміри числа викидів зсувів значущих моментів відтворення за величину двох фіксованих зон ($\Delta_1 = \frac{t_0}{14}$, $\Delta_2 = \frac{t_0}{25}$) при роботі по каналу ГТС з частотною модуляцією зі смугою $\Delta F = 1300$ Гц при швидкості модуляції $B = 1000$ Бод ($t_0 = 1$ мс). Вибране співвідношення між ΔF і B враховує нелінійність амплітудно-фазочастотної характеристики. У таблиці 4.8 наведені результати одного фрагмента одночасних вимірів числа зсувів ЗМВ за зазначені зони. При цьому передавалися кодові слова тривалістю $T_c = 8t_0$, які мають по чотири моменти модуляції.

Таблиця 4.8 – Результати одного фрагмента одночасних вимірів числа зсувів ЗМВ за зазначені зони при $T_c = 8t_0$

Величина зони Δ , %	Число кодових слів $N_{\text{КС}}$	Число моментів модуляції $N_{\text{ММ}}$	Число викидів $N(\theta > \Delta)$	$P_{\text{В}}$	σ_c
7,14	73676	294704	326	$1,106 \cdot 10^{-3}$	2,41
4	73676	294704	6982	$2,3 \cdot 10^{-2}$	1,96

Значення середньоквадратичного відхилення σ_c були визначенні через інтеграл ймовірностей

$$\left. \begin{aligned}
 P_{\text{В}} &= \frac{N(\theta > \Delta)}{N_{\text{пер}}} = 1 - 2\Phi(z) \\
 \Phi(z) &= \frac{1}{\sqrt{2\pi}} \int_0^z e^{-\frac{z^2}{2}} dz \\
 z &= \frac{\Delta}{\sigma_c}
 \end{aligned} \right\} \quad (4.87)$$

У результаті розрахунків для вказаного каналу було оцінено дисперсію відновлення значущих моментів відтворення (ЗМВ) на виході каналу в «хорошому» стані ($\sigma_{\text{ЗМ}} \in (0,017 \dots 0,021)t_0$), що обумовило формулювання проблеми *відносної доцільності витрат у двійковому каналі одного найквістового елемента на один біт інформації*. Аналітично обґрунтована можливість отримання більшої середньої правдоподібності в прийманні сигнальної конструкції за меншої енергетичної відстані між КС порівняно з розрядно-цифровими кодами. Через те, що зсув ЗМВ на виході каналу визначався за наявністю не тільки гауссового шуму в «хорошому» стані, але і при перериваннях (канал комутований) число яких за час вимірів більше сотні, то більш близьким до реального значення слід вважати те значення, за якого число викидів набагато більше числа переривань (занижень) сигналу в комутованому каналі, тобто при $\theta = 0,04t_0$.

Враховуючи функціональну залежність середньоквадратичного відхилення і h

$$\sigma = \frac{1}{4h},$$

то можна стверджувати, що на інтервалі «хорошого» стану $h \geq 10$, отже навіть при некогерентному прийманні $P_{\text{ек}} < (10^{-8} \div 10^{-9})$.

Якщо в «поганому» стані ймовірність помилки прямує до 0,5, то середня ймовірність помилкового приймання на виході каналу

$$\bar{P} = k_{\text{п}} \cdot P_{\text{е2}} + k_{\text{х}} \cdot P_{\text{ек}} = 0,01 \cdot 0,5 + 0,99 \cdot 10^{-8} = 5 \cdot 10^{-3},$$

де k_n, k_x – відносна величина часу «поганого» і «хорошого» станів каналу.

Отже, отримані значення P_{ex} і P_{e2} підтверджують, що досліджуваний канал описується моделлю Гільберта.

Проведені численні експерименти на комутованих каналах міської мережі з використанням модему з ЧМ при базі $B = \Delta F \cdot t_0 = 1$ дозволяють зробити наступні висновки:

1. Середня кількість «поганих» станів на 1 годину змінюється для різних з'єднань від 150 до 1300 в залежності від смуги пропускання каналу ΔF (для каналу зі смугою $\Delta F_1 = 1000$ Гц $N_{\Pi} \in 1100 \dots 1200$, а при $\Delta F_2 = 140$ Гц $N_{\Pi} \in 140 \dots 160$).

2. Час перебування в «поганому» стані описується логарифмічно-нормальним законом з середнім значенням $\overline{\lg \tau_{\Pi}}$, яке зменшується в 5–7 разів зі збільшенням смуги ΔF у 8–10 разів (для смуги $\Delta F_1 = 1000$ Гц $\overline{\lg \tau_{\Pi}} \approx 1,775$, а для $\Delta F_2 = 140$ Гц $\overline{\lg \tau_{\Pi}} \approx 8,45$).

3. Середнє значення спотворених елементів на кодове слово визначається, як правило, середнім значенням «поганого» стану і не суттєво змінюється від елементності КС.

4. Помилки на інтервалах часу «поганого» стану групуються, закон розподілу їх на інтервалі 16 посилок після першої помилки апроксимується гіперекспонентою

$$P_{\Pi}(0+i) = \varepsilon_1 e^{-\lambda_1 i} + \varepsilon_2 e^{-\lambda_2 i} \dots + \varepsilon_i e^{-\lambda_i i}, \quad i \in 1 \dots 16, \quad (4.88)$$

де ε, λ – коефіцієнти, які визначаються каналом та видом завад (у межах перших 4-х посилок зосереджено 97,8 % можливих реалізацій помилок).

5. Параметр завадостійкості $\left(h^2 = \frac{u_c^2}{u_s^2} \right)$ в «хорошому» стані для різних каналів знаходиться у межах $h^2 \in 100 \dots 180$, що в десятки разів більше параметра, що забезпечує середню ймовірність помилки в каналі.

З наведених розрахунків впливає, що запас стійкості у «хорошому» стані реального каналу зв'язку на 7 порядків менше середньої ймовірності помилки

$$P_x = \frac{1}{2} \exp\left(-\frac{h^2}{2}\right).$$

Враховуючи відносну тривалість «хорошого» стану з'являється можливість трансформувати якість передавання у кількість переданої інформації (при середній якості не значно менше ніж при розрядно-цифровому кодуванні) з наступним використанням прирощення кількості у нову якість. Для цього скористаємося таймерними сигналами.

Слід зауважити, що послідовний синхронний метод передачі коригуючих блокових кодів передбачає постійність довжини кодового

слова ($T_{\text{кк}} = \text{const}$) і постійність довжини окремих складових кодової конструкції (елементарних посилянь), яка визначається смугою пропускання каналу і при базі $B = 1$ дорівнює

$$\left. \begin{aligned} t_0 &= \frac{1}{2F_0} \\ t'_0 &= \frac{1}{F_0} \end{aligned} \right\}$$

Використання у структурі кодового слова елемента t_0 рівного «найквістовому» не дозволяє отримати в «хорошому» стані каналу ефективної швидкості коду більшої ніж дозволяє відношення кількості інформаційних елементів до загальної кількості елементів у коригуючому помилки кодї:

$$\left. \begin{aligned} n &= m + k \\ R &= \frac{m}{m + k} \end{aligned} \right\}$$

Пояснюється це тим, що посилянню не може бути інформації більше ніж $I(t_0) \leq \log_2 a$, тому при послідовному методі передачі не можна трансформувати високу надійність передачі в «хорошому» стані каналу на кількість переданої інформації з меншою якістю. Розглянуті в попередніх підрозділах 4-ої глави укрупнені сигнали не можуть бути використані для зазначених цілей трансформації, так як вони передбачають передачу декількох елементів кодового слова новим сигналом з довжиною мінімального елемента, що дорівнює «елементу Найквіста».

Наявність елементарного посиляння, яке дорівнює «елементу Найквіста», обмежує не тільки ефективність коду, а і мінімальну кодову відстань між кодограмами простого коду, що унеможливує при заданій елементності коду (n) реалізувати більше сигнальних конструкцій ніж a^n . В ОНАЗ ім. О.С. Попова при формуванні сигнальних конструкцій для ефективності передавання інформації запропоновано два параметри.

Перший параметр обмежує мінімальну енергетичну відстань між дозволеними сигнальними конструкціями. Всупереч методу поелементного кодування, за якого мінімальна енергетична відстань визначається найквістовим елементом, у запропонованих конструкціях мінімальна відстань між ними в декілька разів менше «елемента Найквіста»

$$\Delta = t_0 / s; \quad s \in 1, 2, \dots, k - \text{ціле число.}$$

Саме введення цього елемента дає змогу при обмеженій довжині кодового слова збільшувати число реалізацій. Сам елемент розраховується із забезпеченням доцільної ймовірності приймання одного кодового слова замість переданого на інтервалах «хорошого» стану каналу.

Другий параметр – мінімальна відстань між суміжними значущими моментами модуляції реалізованого кодового слова (τ_{ci} – має нижню межу, що дорівнює найквістовому елементу)

$$\tau_{ci} \geq s\Delta + i\Delta; \quad i \in 0, 1, 2, \dots, z - \text{ціле число.} \quad (4.89)$$

Перший доданок виразу (4.89) відповідає мініальному інтервалу, тобто найквістовому елементу ($t_0 = s\Delta$), а доданок $i\Delta$ показує наскільки τ_{ci} більше найквістового елемента в елементах Δ . При таких обмеженнях кількість реалізованих сигнальних конструкцій

$$N_p = C_{ms-i(s-1)}^i \rightarrow \frac{[ms - i(s-i)]!}{i!(ms - is)!} \quad (4.90)$$

де i – число заданих відрізків сигналу на інтервалі кодового слова довжиною m – найквістових елементів. Наприклад, для $m = 8$ і $s = 7$ при синтезі сигнальної конструкції з 3-х інформаційних відтинків ($i = 3$)

$$N_p = C_{56-3(7-1)}^3 = C_{38}^3 = \frac{38!}{3!35!} = 8436,$$

що у 33 рази більше числа кодових слів при $m = 8$ ($2^8 = 256$). Дякуючи першому доданку виразу (4.90), всі кодові слова можуть бути передані без власних міжсимвольних завад. Підставляючи у вираз (4.90) значення m_{is} розрахуємо число реалізацій при $i \in 1 \div 6$, $s \in 2 \div 12$ і $m \in 4 \div 10$. Результати розрахунків наведено в табл. 4.9.

Аналіз таблиці показує, що:

1) при $m \geq 4$ і $i \geq 2$ за всіх значень $s \geq 4$ число реалізацій більше $N_p > 2^m$;

2) для $m_1 = 4$ і $m_2 = 5$ для $s \geq 3$ число реалізацій для $m = 5$, $N_p(5)$ майже вдвічі більше від $N_p(4)$;

Таблиця 4.9 – Число реалізацій ТСК при зміні i та Δ_c

$i = 1$

$S \backslash m$	4	5	6	7	8	9	10
2	7	9	11	13	15	17	19
3	10	13	16	19	22	25	28
4	13	17	21	25	29	33	37
5	16	21	26	31	36	41	46
6	19	25	31	37	43	49	55
7	22	29	36	43	50	57	64
8	25	33	41	49	57	65	73
9	28	37	46	55	64	73	82
10	31	41	51	61	71	81	91
11	34	45	56	67	78	89	100
12	37	49	61	73	85	97	109

$i = 2$

$S \backslash m$	4	5	6	7	8	9	10
2	15	28	45	66	91	120	153
3	28	55	91	136	190	253	325
4	45	91	153	231	325	435	561
5	66	136	231	351	496	666	861
6	91	190	325	496	703	946	1225
7	120	253	435	666	946	1275	1653
8	153	325	561	861	1225	1653	2145
9	190	406	703	1081	1540	2080	2701
10	231	496	861	1326	1891	2556	3321
11	276	595	1035	1596	2278	3081	4005
12	325	703	1225	1891	2701	3655	4753

$i = 3$

$S \backslash m$	4	5	6	7	8	9	10
2	10	35	84	165	286	455	680
3	20	84	220	455	816	1330	2024
4	35	165	455	969	1771	2925	4495
5	56	286	816	1771	3276	5456	8436
6	84	455	1330	2925	5456	9139	14190
7	120	680	2024	4495	8436	14190	22100
8	165	969	2925	6545	12341	20825	32509
9	220	1330	4060	9139	17296	29260	45760
10	286	1771	5456	12341	23426	39711	62196
11	364	2300	7140	16215	30856	52394	82160
12	455	2925	9139	20825	39711	67525	105995

$i = 4$

$S \backslash m$	4	5	6	7	8	9	10
2	1	15	70	210	495	1001	1820
3	1	35	210	715	1820	3876	7315
4	1	70	495	1820	4845	10626	20475
5	1	126	1001	3876	10626	23751	46376
6	1	210	1820	7315	20475	46376	91390
7	1	330	3060	12650	35960	82251	163185
8	1	495	4845	20475	58905	135751	270725
9	1	715	7315	31465	91390	211876	424270
10	1	1001	10626	46376	135751	316251	635376
11	1	1365	14950	66045	194580	455126	916895
12	1	1820	20475	91390	270725	635376	1282975

$i = 5$

$S \backslash m$	4	5	6	7	8	9	10
2	0	1	21	126	462	1287	3003
3	0	1	56	462	2002	6188	15504
4	0	1	126	1287	6188	20349	53130
5	0	1	252	3003	15504	53130	142506
6	0	1	462	6188	33649	118755	324632
7	0	1	792	11628	65780	237336	658008
8	0	1	1287	20349	118755	435897	1221759
9	0	1	2002	33649	201376	749398	2118760
10	0	1	3003	53130	324632	1221759	3478761
11	0	1	4368	80730	501942	1906884	5461512
12	0	1	6188	118755	749398	2869685	8259888

$i = 6$								
$S \backslash m$	4	5	6	7	8	9	10	
2	0	0	1	28	210	924	3003	
3	0	0	1	84	924	5005	18564	
4	0	0	1	210	3003	18564	74613	
5	0	0	1	462	8008	54264	230230	
6	0	0	1	924	18564	134596	593775	
7	0	0	1	1716	38760	296010	1344904	
8	0	0	1	3003	74613	593775	2760681	
9	0	0	1	5005	134596	1107568	5245786	
10	0	0	1	8008	230230	1947792	9366819	
11	0	0	1	12376	376740	3262623	15890700	
12	0	0	1	18564	593775	5245786	25827165	

3) для $m \geq 5$ відношення числа реалізації при збільшенні інтервалу сигнальної конструкції з $T_c = mt_0$ до $T_c = (m+1)t_0$ відповідає нерівностям:

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} < 2 \text{ при } i < 3;$$

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} > 2 \text{ при } i \geq 3; \quad (4.91)$$

4) побудувавши залежності числа реалізацій від збільшення однієї зі змінних за сталих значень інших можна констатувати їх нелінійність.

5) для всіх значень $m > 4$ при $s > 4$

$$N_p \gg 2^m.$$

Апроксимуючі рівняння мають вигляд:

для $N_p = f(S)$

$$i = 2 \quad \sqrt[2]{N_p(i, m, S)} = 1,416S + 1,045;$$

$$N_p(i, m, S) = (1,416S + 1,045)^2; \quad (4.92)$$

$$i = 3 \quad \sqrt[3]{N_p(i, m, S)} = 0,554S + 1,053;$$

$$N_p(i, m, S) = (0,554S + 1,053)^3; \quad (4.93)$$

для $N_p = f(m)$.

$$i = 2 \quad \sqrt[2]{N_p(i, m, S)} = 3,536m - 6,02;$$

$$N_p(i, m, S) = (3,536m - 6,02)^2; \quad (4.94)$$

$$i = 3 \quad \sqrt[3]{N_p(i, m, S)} = 2,759m - 7,23;$$

$$N_p(i, m, S) = (2,759m - 7,23)^3. \quad (4.95)$$

Приклад 3. Користуючись виразом (4.95) розрахувати кількість реалізацій на інтервалі $m \in 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ при значеннях числа інформаційних моментів модуляції $i = 2; 3; 4; 5$ та різних значень

$$\Delta = \frac{t_0}{s} (s \in 2 \dots 10).$$

З метою оцінки ефективності таймерного кодування порівняємо результати передавання інформації для двох методів кодування:

- а) розрядно-цифровий з реєстрацією у середині посилання (РЦК);
- б) використання таймерних сигналів (ТСК).

Таблиця 4.10 – Вплив довжини конструкції на якість передавання

n	РЦК			ТСК $s = 7$ $i = 3$			
	$N_{\text{пер}}$	$N_{\text{пом}}$	P_n	n	$N_{\text{пер}}$	$N_{\text{пом}}$	P_n
20	100000	700	$7 \cdot 10^{-3}$	17	100000	11,50	$11,5 \cdot 10^{-3}$
40	100000	1500	$15 \cdot 10^{-3}$	$n=33$	100000	1620	$16,2 \cdot 10^{-3}$
10	100000	720	$7,2 \cdot 10^{-3}$	$n=9$	100000	104	$7,1 \cdot 10^{-4}$

Порівняння результатів передавання сигнальних конструкцій при ТСК і РЦК з урахуванням їх довжин показують, що, незважаючи на те, що енергетична відстань при ТСК визначається зоною у сім разів меншою відносно РЦК ($\Delta = t_0/7$), імовірності помилкового приймання КС різняться не суттєво, а в тих випадках, коли T_c (ТСК) < T_c (РЦК), імовірність помилкового приймання при ТСК може бути меншою порівняно з РЦК.

Аналіз причин спотворення сигнальних конструкцій при ТСК буде проведено в главі 5. Відносно даних табл. 4.10, а звернемо увагу тільки на те що, практично, за рівних ймовірностей приймання РЦК і ТСК число реалізацій на ТСК на заданому інтервалі n в десятки разів більше, ніж при РЦК. Наприклад, при $s = 3$, $i = 3$ на інтервалі $T_c = 10t_0$ можлива реалізація $N_p = 22100$ КС (див. табл. 4.9), а при РЦК – $N_p = 1024$ ($2^{10} = 1024$). Коефіцієнт збільшення дорівнює 21,58 (22100:1024). Якщо ж формувати конструкції з п'яти інформаційними ЗММ ($i = 5$), то на інтервалі $T_c = 10 t_0$ можлива реалізація 658008 КС (табл. 4.9), тобто коефіцієнт збільшення відносно РЦК буде дорівнювати 642, 585. Таке збільшення числа реалізацій суттєво збільшує пропускну здатність каналу (навіть при алфавіті каналу $a = 2$). При чому граничне значення пропускну здатності буде визначатися виразом

$$C_{\text{макс}} = \frac{\log_2 N_{\text{p}\Sigma}}{T_{\text{ск}}}, \quad (4.96)$$

де $T_{ск}$ – часовий інтервал сигнальної конструкції в числі найквістових елементів; $N_{p\Sigma}$ – загальна кількість реалізацій, які використовуються з урахуванням кількості ЗММ – i .

4.7. Пропускна здатність каналу при ТСК

Пропускна здатність двійкового каналу, представляючи максимальне значення швидкості передавання інформації за заданих фіксованих меж W_c , визначається

$$C = \sup \left[I(n, W_c) \right] \frac{\text{дв.од.}}{с};$$

$$L_1 \in W_1 \dots; L_i \in W_i, \quad (4.97)$$

де W_i – обмеження на формуючі сигнали. При РЦК – це є границя на довжину одиничного елемента ($t_0 = \frac{1}{2\Delta F}$ або $t_0 = \frac{1}{\Delta F}$).

Із даного виразу виходить, що кількість інформації, яка передається на інтервалі одного двійкового елемента не перевищує

$$I = [1 + P_e \log_2 P_e + (1 - P_e) \log_2 (1 - P_e)]. \quad (4.98)$$

При формуванні сигналів на інтервалі $T_c = mt_0$ за мінімальної довжини елементарного сигналу Δ реалізується $2^{\frac{m}{\Delta}}$ (2^{ms}) сигналів. Щоправда вони далеко не всі задовольняють умові.

З дозволених для передавання ТСК (в яких окремі відрізки $\tau_{ci} \geq s\Delta$, які формуються на проміжку часу $T_c = mt_0$ за вибраної величини Δ будуть СК: $N_p(1)$ – з одним інформаційним ЗММ; $N_p(2)$ – з двома ЗММ, $N_p(m-1)$ – з $(m-1)$ ЗММ і одна СК з m значущими моментами модуляції.

Отже,

$$N_{\Sigma} = N_p = N_p(1) + N_p(2) + \dots + N_p(m-1) + N_p(m).$$

Через те що в сумарному числі N_p різне число кодових комбінацій з i -моментами модуляції, то середнє число моментів модуляції \bar{i} дорівнює

$$\left. \begin{aligned} \bar{i} &= \sum_{i=1}^m P[N_p(i)] i \\ P[N_p(i)] &= \frac{N_p(i)}{N_{p\Sigma}} \end{aligned} \right\}. \quad (4.99)$$

Кожна з таймерних сигнальних конструкцій за рівноймовірних символів на вході може передати H_i біт інформації.

$$H_i = \log_2 N_p.$$

Але, тому що на вході каналу формуються кодові сигнали, які належать різним групам за ознакою числа переходів, то кількість інформації, яка полягає у виборі групи з i -переходами, дорівнює

$$H_r = -\sum_{i=1}^m P[N_p(i)] \log_2 P[N_p(i)] = \sum \frac{N_p(i)}{N_p} \log_2 \left[\frac{N_p(i)}{N_p} \right]. \quad (4.100)$$

Якщо приймач отримав сигнал з i -переходами, то невизначеність у достовірності передавання кожного з них на k -му місці знаходиться умовною ентропією

$$H\left(\frac{Z_i}{K_i}\right) = -\sum_{i=1}^{Z_0} P\left(\frac{Z_i}{K_i}\right) \log_2 P\left(\frac{Z_i}{K_i}\right), \quad (4.101)$$

де $P\left(\frac{Z_i}{K_i}\right)$ – ймовірність отримання переходу на Z_i місці за умови, що він передавався на K_i місці.

Тому що число реалізацій з i переходами дорівнює $N(i)$, то число станів кожного переходу дорівнює

$$Z_0 = i\sqrt{N_p(i)}.$$

Ймовірність $P\left(\frac{Z_i}{K_i}\right)$ при аналізі зі сторони приймача й передавача знаходиться за допомогою каналних матриць. Враховуючи, що потужність просторів окремих груп за числом переходів різні, то загальні втрати інформації $H_\Sigma\left(\frac{Z_i}{K_i}\right)$

$$H_{\Sigma i} = H_\Sigma\left(\frac{Z_i}{K_i}\right) = -\sum_{i=1}^m P(i) i H\left(\frac{Z_i}{K_i}\right).$$

Отже, кількість інформації, яка передається одним словом ТСК в каналі без завад (відсутні дроблення, тому що потужність міжсимвольних завад незначна)

$$I = H_i - H_{\Sigma i} = \log_2 N_p - \sum_{i=1}^m P(i) H\left(\frac{Z_i}{K_i}\right). \quad (4.102)$$

За нерівномірних довжин кодових слів максимальне значення дорівнює $T_c = mt_0$, а мінімальне $T_c = t_0$ (при одному переході), то середня довжина кодового слова дорівнює

$$\bar{m}_\Sigma = \sum_{i=1}^m m(i) P[N_p(i)].$$

За кожного значення i -переходів середній інтервал між ЗМВ знаходиться

$$\bar{m}(i) = it_0 + \frac{mt_0 - it_0}{2}.$$

Звідси виходить

$$\bar{m}_\Sigma = \sum_{i=1}^m \left[it_0 + \frac{mt_0 - it_0}{2} \right] \frac{N_p(i)}{N_p}.$$

Враховуючи значення \bar{m}_Σ і вираз (4.102), знаходимо значення I_0

$$I_0 = \frac{I}{\bar{m}_\Sigma} = \frac{\log_2 N_p - \sum_{i=1}^m iP(i)H\left(\frac{Z_i}{K_i}\right)}{\sum_{i=1}^m \left[it_0 + \frac{mt_0 - it_0}{2} \right] \frac{N_p(i)}{N_p}}.$$

Слід зауважити, що нерівномірні за довжиною сигнали ТСК можливі тільки за наявності ознак кінця кодового слова. Тому, при формуванні простих ТСК краще користуватись кодовими сигналами однакової довжини $T_0 = mt_0$. Отже, для простих кодів ТСК маємо

$$I_0 = \frac{\log_2 N_p - \sum_{i=1}^m iP(i)H\left(\frac{Z_i}{K_i}\right)}{m}. \quad (4.103)$$

З останнього виразу виходить, що пропускна здатність є функція від N_p і достовірності вірного приймання одного переходу. Тому що закон розподілу зміщень ЗМВ можна вважати нормальним, то величина $H\left(\frac{Z_i}{K_i}\right)$ дорівнює

$$H\left(\frac{Z_i}{K_i}\right) = -2\Phi\left(\frac{2h}{S}\right) \log_2 \left[2\Phi\left(\frac{2h}{S}\right) \right] + 2 \sum_{i=1}^{Z_{01}} \left\{ \Phi(2i+1) \left[\frac{2h}{S} \right] - \Phi\left[(2i-1) \frac{2h}{S} \right] \right\} \log_2 \left\{ \Phi\left[(2i+1) \frac{2h}{S} \right] - \Phi\left[(2i-1) \frac{2h}{S} \right] \right\}. \quad (4.104)$$

Через те що вираз (4.104) показує втрати на один значущий момент модуляції і враховуючи, що всі переходи знаходяться в однакових умовах, величина $H\left(\frac{Z_i}{K_i}\right) = \text{const}$. Тому загальні втрати становлять

$$H_{\Sigma i} = +H\left(\frac{Z_i}{K_i}\right) \sum_{i=1}^m P(i) = -H\left(\frac{Z_i}{K_i}\right) \bar{i}. \quad (4.105)$$

Враховуючи (4.103), (4.104), (4.105), пропускна здатність каналу без завад дорівнює

$$I_0 = \frac{\log_2 N_p - \bar{i}H\left(\frac{Z_i}{K_i}\right)}{m}. \quad (4.106)$$

Таким чином, з виразів (4.103), (4.104) виходить, що пропускна здатність каналу без завад визначається числом реалізацій сигналів за заданого значення s або Δ і потужністю міжсимвольних завад.

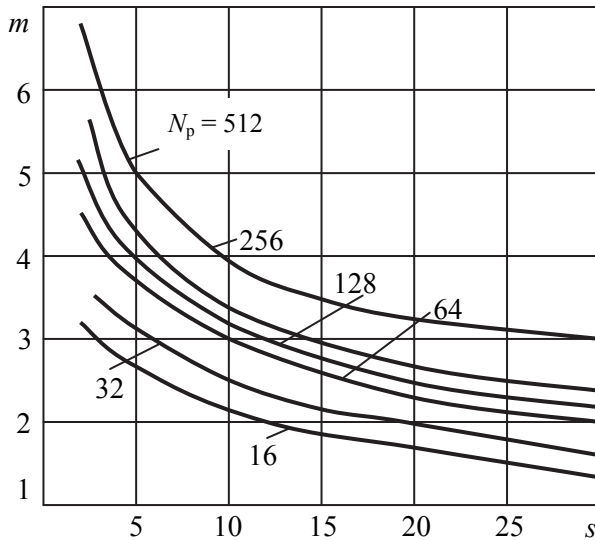


Рисунок 4.21 – Залежності $m = f(s)$ при $N = \text{const}$

З наведеної вище інформації слід зробити висновок, що у двійковому каналі на m -елементному інтервалі часу, за рахунок значення $\Delta(s)$ можливо отримати одне й те саме число сигнальних конструкцій на різних інтервалах часу T_c . Як приклад на рис. 4.21 подано залежності тривалості сигнальних конструкцій за заданої потужності кодових множин і параметра s . З цих залежностей виходить, що при $s > 2$ для отримання $N_p = 2^m$ можна витратити час $T_c < m_0 t_0$. При цьому нерівність тим більша, чим

більше значення s .

При роботі по каналах з гауссівським шумом слід враховувати, що ймовірність помилкового приймання кодової конструкції ТСК (P_{π}) визначається величиною зони Δ , середньоквадратичним відхиленням ЗМВ (σ), що в свою чергу, залежить від співвідношення сигнал/завада, а також числом переходів у слові (i)

$$P_{\pi} = 1 - [\Phi(\Delta / 2\sigma)]^{\bar{i}}, \quad (4.107)$$

де \bar{i} – середнє число ЗММ у кодовому слові,

$$\Phi(x) = \frac{1}{\sqrt{2\sigma}} \int_0^x e^{-\frac{t^2}{2}} dt. \quad (4.108)$$

$\Phi(x)$ – інтеграл імовірностей.

Виходячи з виразів (4.103), (4.106), середнє число переходів у сигнальній конструкції при $i \in (1 \dots m)$

$$\bar{i} = \sum_{i=1}^m \frac{i C_{ms-i(s-1)}^2}{C_{ms-i(s-1)}^i}. \quad (4.109)$$

Враховуючи, що зі збільшенням s зростає не лише число реалізацій N_p , але й імовірність помилкового приймання їх p_n , то для кожного каналу є своє значення Δ_0 , за якого реалізується максимальна пропускна здатність системи. При цьому, кожна із реалізацій сигналу на інтервалі $T_c = m\tau_0$ являє собою одну із реалізацій багатопозиційного сигналу. Тоді значення пропускної здатності

$$C_m = \frac{1}{m} (\log_2 N_{pz} - H_{вт}). \quad (4.110)$$

Тут $H_{вт}$ визначає втрати в каналі через невизначеність у прийманні кодової сигнальної конструкції

$$H_{вт} = - \left[p_B \log_2 p_B + (1 - p_B) \log_2 \frac{1 - p_B}{N - 1} \right], \quad (4.111)$$

$$P_i = [2\Phi(\Delta / 2\sigma)]^i, \quad (4.112)$$

де P_i – ймовірність вірного приймання сигнальної конструкції з i -переходами.

На рис. 4.22 наведено залежності пропускної здатності каналів з різним рівнем флуктуаційних шумів (задано $h = u_c / u_3$) як функцій s (криві 1...3 для $h = 7,5$ і $m = 8, 6, 5$ відповідно, криві 4...6 для $h = 5,5$ і $m = 8, 6, 5$ відповідно).

З рисунка виходить, що для кожного значення h є величина зони, за якої C_m буде максимальним. На практиці оптимальне значення визначається середньоквадратичним відхиленням зміщення фронту сигналу на виході каналу (σ_k)

$$\Delta_{\text{опт}} = (3,8 \dots 5,5); \quad \sigma_k = 3,8 \dots 4,5 / h$$

При цьому розуміється, що в каналі з частотною модуляцією

$$\left. \begin{aligned} \sigma_3 &= 1/4h \\ h &= u_c / u_{ш} \end{aligned} \right\}$$

З принципу формування ТСК зрозуміло, що множина дозволених для передавання КС не є лінійною, тобто серед

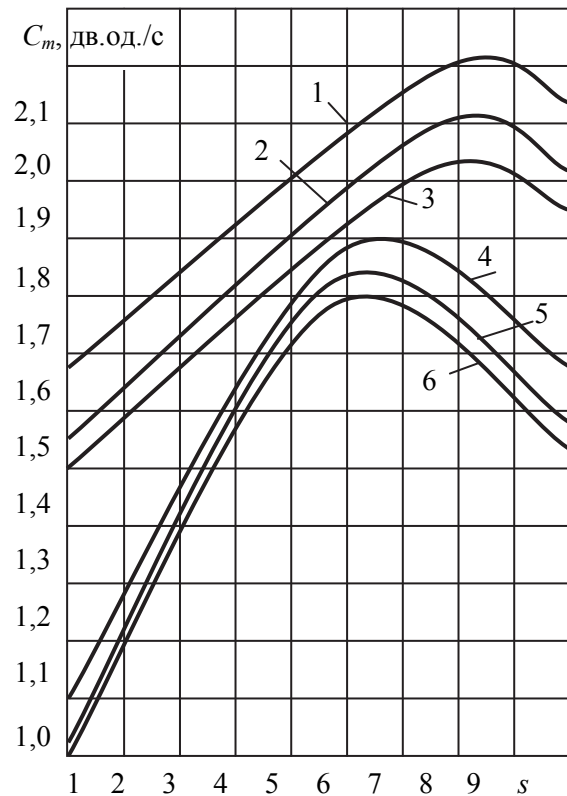


Рисунок 4.22 – Залежності пропускної здатності каналу $C_i = f(s)$ при $h = \text{const}$, $m = \text{const}$

дозволенних сигналів можна знайти пару таких, сума яких може утворити сигнал, в якого відстань між суміжними моментами модуляції менша за $t_0 = s\Delta$. Наприклад, сума двох кодових слів (для $s = 5$):

$$\begin{array}{r} 111110000011111 \\ \oplus \\ 111110000011111 \end{array}$$

дає кодове слово 0000010000100000, в якому число суміжних одиниць менше значення s . У зв'язку з цим використовувати теорію лінійних надлишкових кодів РЦК для виявлення або виправлення помилок при ТСК неможливо.

Приклад 4. Знайдемо кодове слово циклічного коду для початкового слова ТСК при $s = 5$ на інтервалі $m = 3\tau_0$, поданого двійковим числом

$$111110000011111 \rightarrow q(x).$$

За породжуючий багаточлен використаємо біном, що відповідає двійковому поданню $f(x)=127$. Із запису $f(x)$ виходить, що це багаточлен 6-го степеня, отже надлишкових елементів у кодовому слові повинно бути $r = 6$. Візьмемо як породжуючий багаточлен $f(x) \rightarrow x^6 + x^4 + x^3 + 1$. Визначимо доповнення до 15-елементного кодового слова методом ділення двійкового числа 11111000001111100000 на двійкове число 1010111. Оскільки отриманий залишок 110100 має підряд одиниць менше ніж 5, сформульоване двійкове кодове слово не задовольняє умовам ТСК і не може передаватися каналом без міжсимвольних завад.

Синтез ТСК при $a > 2$. Сигнальний алфавіт недвійкових ТСК формується на інтервалі часу $T_c = mt_0$, де t_0 , як і раніше, визначається величиною оберненою до смуги пропускання каналу зв'язку, $n = ms$, $\Delta = t_0/s$ (n і s – цілі позитивні числа). В цьому значенні часова структура недвійкових ТСК збігається з часовою структурою двійкових ТСК. Крім того, при передаванні сигналу в кожний значущий момент використовується одне із $a > 2$ положень (рівнів) модульованого параметра. Із цього випливає, що кодова комбінація недвійкового ТСК визначається не тільки часом зміни інформаційного параметра x_i , але й значенням рівня (позиції) інформаційного параметра.

На рис. 4.23 пояснюється принцип формування недвійкових ТСК.

Пронумеруємо усі рівні від 0 до a , тобто 0, 1, 2, ..., $a-1$. Значення 0 присвоюємо відносному рівню (далі називатимемо його нульовим). Число нульових рівнів у комбінації змінюється від 0 до i (i – число ЗММ). Очевидно, що загальна кількість комбінацій, до яких нуль входить хоча б один раз, буде дорівнювати сумі груп комбінацій, що відрізняються одна від одної кількістю вхідних до них нулів. Отже, число доданків в сумі буде дорівнювати $(i-1)$.

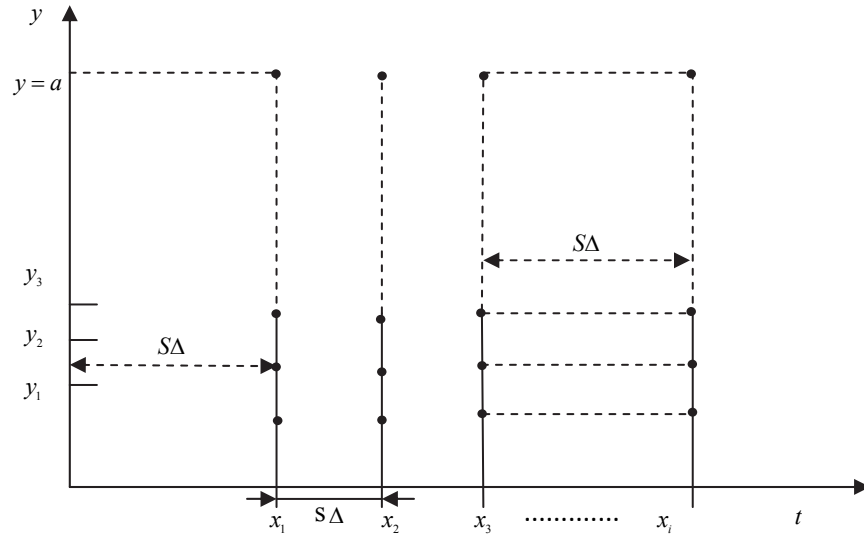


Рисунок 4.23 – Принцип формування недвійкових ТСК

Визначимо число комбінацій в групі. Для цього розглянемо випадок, коли комбінації групи містять лише один нуль. Ненульові члени комбінації можуть набувати $(a - 1)$ значень.

Таких ненульових членів у такого виду груп може бути лише $(i - 1)$, отже загальне число ненульових наборів цифр, що входять до i -розрядної комбінації, яка містить лише один нуль, буде дорівнювати $(a - 1)^{i-1}$.

Визначимо скільки i -розрядних комбінацій буде при кожному фіксованому наборі ненульових членів комбінації. Очевидно, що число таких комбінацій буде дорівнювати числу з'єднань i по $i - 1$, тобто C_i^{i-1} , отже, загальна кількість комбінацій у групі (B_{i-1}) даного виду може бути обчислена як

$$B_{i-1} = (a - 1)^{i-1} C_i^{i-1}. \quad (4.113)$$

Подібні міркування можна навести і для груп, які вміщують i -розрядні комбінації з двома і більше нулями (відносними) значеннями. Тому загальне число i -розрядних комбінацій, до яких відносний рівень входить хоча б один раз, буде визначатися як

$$B = \sum_{k=0}^{i-1} (a - 1)^k C_i^k.$$

Можна показати, що

$$N_p(a > 2) = \sum_{i=1}^m \left[a^i - \sum_{k=0}^{i-1} (a - 1)^k \cdot C_i^k \right] \cdot C_{ms-i(s-1)}^i.$$

Розглянемо перший співмножник під знаком суми у виразі

$$a^i - \sum_{k=0}^{i-1} (a - 1)^k \cdot C_i^k.$$

Даний вираз можна подати у вигляді

$$C_i^0 \cdot a^i \cdot 1^0 + (-1) \cdot \sum_{k=0}^{i-1} (a-1)^k \cdot C_i^k \cdot 1^k.$$

Після включення першого доданка суми під знак підсумовування з урахуванням даного доданка вираз набуває вигляду

$$\sum_{k=0}^i (-1)^k \cdot C_i^k \cdot a^{i-k} \cdot 1^k.$$

Проте сума являє собою не що інше, як розкладання бінома Ньютона виду $(a-1)^i$. Отже можна записати

$$\sum_{k=0}^i (-1)^k \cdot C_i^k \cdot a^{i-k} \cdot 1^k = (a-1)^i.$$

Дійсно розглянемо формулу бінома Ньютона

$$(\alpha + \beta)^i = \sum_{k=0}^i C_i^k \cdot \alpha^{i-k} \cdot \beta^k.$$

Якщо замінити β на $-\beta$, тоді з виразу випливає

$$(\alpha - \beta)^i = \sum_{k=0}^i (-1)^k \cdot C_i^k \cdot \alpha^{i-k} \cdot 1^k.$$

Якщо у попередньому виразі прийняти $\beta = -1$, то

$$(\alpha - 1)^i = \sum_{k=0}^i (-1)^k \cdot C_i^k \cdot \alpha^{i-k} \cdot 1^k,$$

що і потрібно було довести.

З урахуванням наведених міркувань дістаємо кінцевий вираз для потужності сигнального алфавіту (числа реалізацій) недвійкових ТСК:

$$N_p(a > 2) = \sum_{i=1}^m (a-1)^i \cdot C_{ms-i(s-1)}^i. \quad (4.114)$$

Рівність (4.114) показує, що, порівняно з бінарними ТСК, потужність сигнального алфавіту багаторівневих ТСК зростає за біноміальним законом.

При заданому значенні числа інформаційних значущих моментів модуляції i_0 , максимальне число реалізацій буде

$$N_p(a > 2; i = \text{const}) = (a-1)^i C_{ms-i(s-1)}^i.$$

Виходячи з цього максимальне відносне значення пропускну здатності

$$C_{\text{макс}} = \frac{i \log_2(\alpha-1) + \log_2 C_{ms-i(s-1)}^i}{m} = \frac{i \log_2(\alpha-1)}{m} + \frac{\log_2 C_{ms-i(s-1)}^i}{m}. \quad (4.115)$$

Із останнього виразу видно, що введення багатопозиційного сигналу суттєво доповнює складову, яка забезпечується за рахунок розміщення моментів модуляції в точках некратних найквістовому інтервалу.

Приклад 5. Оцінити величину приросту $C_{\text{макс}}$ за умови, що таймерні сигнальні конструкції формуються на інтервалі $T_c = 5$ при $i = 3$, а інформаційний параметр $a = 16$ станів.

Тому що $\log_2(a-1) \approx 4$, то значення першого доданка виразу (4.115) дорівнює $\frac{3 \cdot 4}{5} \approx 2,4$. По відношенню до $C_{\text{макс}}$ для бінарного каналу цей приріст збільшує максимальне значення пропускну здатності майже вдвічі (див. рис. 4.22).

4.8. Теорія синтезу простих ТСК

Задача кодера простого таймерного коду полягає в перетворенні інформації в певну послідовність чисел (x_1, x_2, \dots, x_i) , що задовольняють обмеженням

$$\begin{aligned} Q_1 : x_j &\geq 0; \quad j = 1, \dots, i; \\ Q_2 : \sum_{j=1}^i x_j &\leq n - is - 1, \end{aligned} \quad (4.116)$$

де $n = ms$.

Зазначені умови повинні використовуватись таким чином, щоб декодер міг за прийнятою послідовністю чисел однозначно відновити початкову інформацію. Розв'язання задачі синтезу кодуєчого алгоритму подано в наступній лемі.

Теорема 1. Нерівності

$$\frac{1}{(i-1)!} \sum_{r=0}^{x_i} \prod_{t=0}^{i-2} (n - is - r + t + 1) - N(x) \leq 0 \quad (4.117)$$

та

$$\begin{aligned} &\frac{1}{(k-1)!} \sum_{r=0}^{x_k} \prod_{t=0}^{k-2} (n - is - r + t + 1) + \\ &+ \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-2} \left(n - is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right) - N(x) \leq 0, \end{aligned} \quad (4.118)$$

де $k = 1, \dots, i-1$ дають змогу однозначно надати всім членам $0 \leq N(x) < \binom{n - i(s-1)}{i}$ множини чисел (x_1, x_2, \dots, x_i) , які задовольняють обмеженням Q_1 й Q_2 .

Схема перетворення числа $N(x)$ у множини чисел (x_1, x_2, \dots, x_i) наведена нижче.

Доведення. Подамо інформацію, що підлягає кодуванню, у вигляді десяткового числа $N(x)$, а кодову комбінацію, отриману в результаті кодування, як множини чисел (x_1, x_2, \dots, x_i) . З урахуванням обмежень (4.116) складемо схему перетворення (див. послідовність) й визначення a_k ,

$k \in [1; i]$:

$$a_1 = n - is; \quad a_2 = \frac{1}{2!}(n - is + 1)(n - is); \quad (4.119)$$

$$a_3 = \frac{1}{3!}(n - is + 2)(n - is + 1)(n - is); \quad (4.120)$$

.....

$$a_i = \frac{1}{i!}(n - is + (i - 1))(n - is + (i - 2)) \dots (n - is); \quad (4.121)$$

$$a_k = \frac{1}{k!} \prod_{t=0}^{k-1} (n - is + t) = \frac{1}{(k-1)!} \sum_{r=0}^{n-is-1} \prod_{t=0}^{k-2} (n - is - r + t + 1). \quad (4.122)$$

$N(x)$	$x(i)$	x_{i-1}	\dots	x_2	x_1	
0	0	0	...	0	0	}
1	0	0	...	0	1	
\vdots	\vdots	\vdots	...	\vdots	\vdots	
$n - is - 1$	0	0	...	0	$n - is - 1$	}
$n - is$	0	0	...	1	0	
\vdots	\vdots	\vdots	...	\vdots	\vdots	}
$2(n - is) - 2$	0	0	...	1	$n - is - 2$	
$2(n - is) - 1$	0	0	...	2	0	
\vdots	\vdots	\vdots	...	\vdots	\vdots	}
\vdots	0	0	...	$n - is - 1$	0	
\vdots	\vdots	\vdots	...	\vdots	\vdots	
\vdots	0	1	...	0	0	}
\vdots	0	1	...	0	1	
\vdots	\vdots	\vdots	...	\vdots	\vdots	
\vdots	0	1	...	0	$n - is - 2$	}
\vdots	0	1	...	1	0	
\vdots	\vdots	\vdots	...	\vdots	\vdots	
\vdots	0	$n - is - 1$...	1	0	}
\vdots	1	0	...	0	0	
\vdots	\vdots	\vdots	...	\vdots	\vdots	
$\binom{n-i(s-1)}{i} - 1$	$n - is - 1$	0	...	0	0	}

Таким чином, процес кодування зведено до визначення інтервалу належності $N(x) \in [a_k, a_{k+1}]$, а потім його положення в цьому інтервалі.

Тому, якщо у формулі (4.118) верхня межа суми буде змінною величиною $x_i \in [0, n-is-1]$, то можна буде перейти до нерівності (4.117) і знайти елемент x_i множини чисел (x_1, x_2, \dots, x_i) . Вираз (4.118) складається з трьох членів. Перший, як і у виразі (4.117) – змінний, а другий являє собою накопичення з усіх попередніх елементів x_μ , $\mu = k + 1, \dots, i$. Отже, x_1, x_2, \dots, x_{i-1} визначаються з нерівності. Теорему доведено.

Обернене перетворення є правилом декодування для простого таймерного коду з постійним числом значущих моментів.

Теорема 2. Інформація, подана у вигляді десяткового числа $N(x)$, однозначно відновлюється за значеннями множини чисел (x_1, x_2, \dots, x_i)

$$N(x) = \sum_{\mu=1}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-1} \left(n - is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right). \quad (4.123)$$

Доведення. Оскільки (x_1, x_2, \dots, x_i) відомі, то вираз (4.118) переходить у рівність. Якщо припустити, що $k = 1$, то отримуємо

$$\begin{aligned} & \sum_{r=0}^{x_i} \prod_{t=0}^1 (n - is - r + t + 1) + \sum_{\mu=2}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-2} \left(n - is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right) = \\ & = \sum_{\mu=1}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-2} \left(n - is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right) = N(x). \end{aligned}$$

Теорему доведено.

Інше розв'язання задачі синтезу кодера та декодера простого таймерного коду сформулюємо в наступних теоремах.

Теорема 3. Для чисел множини $0 \leq N(x) \leq \binom{n-i(s-1)}{i}$ нерівності

$$\sum_{r=1}^{i-k} \sum_{l=0}^{x_i+1-r} \binom{n-i(s-1) - \sum_{t=1}^l x_{i-t+1} - l}{i-r+1} + \sum_{l=0}^{x_k} \binom{n-i(s-1) - \sum_{t=0}^{i-k+1} x_{i-t} - l}{k} \leq N(x) \quad (k = \overline{1, i})$$

дають можливість однозначно надати всім числам вектори (x_1, x_2, \dots, x_i) , які задовольняють обмеженням (4.116).

Теорема 4. За значеннями (x_1, x_2, \dots, x_i) однозначно відновлюється $N(x)$:

$$N(x) = \sum_{k=1}^i \sum_{l=1}^{x_k} \binom{n-i(s-1) - \sum_{r=1}^{k-1} x_r - l}{k}.$$

Отже, теореми 3 і 4 є відповідно правилами кодування й декодування таймерного коду довжиною n найквістових елементів з кодовою відстанню $d = 1$ та числом значущих моментів i .

Доведення. Перетворимо вирази (4.119 ... 4.122) в наступні рівності:

$$a_1 = n - is;$$

$$a_2 = \frac{1}{2!}(a_1^2 + 3a_1 + 2);$$

$$a_3 = \frac{1}{3!}(a_1^3 + 6a_1^2 + 11a_1 + 6);$$

.....

$$a_i = \frac{1}{i!} \left(\sum_{k=0}^i S(i, k) a_1^k \right),$$

де $S(i, k)$ – коефіцієнти ряду Стирлінга. З іншого боку, відомо, що:

$$\binom{m}{n} = \frac{1}{m!} \sum_{k=0}^{m+1} S(m+1, k) n^k.$$

Тоді:

$$a_k = \sum_{r=0}^{n-is-1} \binom{n-i(s-1)-r}{k}$$

й подальше доведення зводиться до процедури, аналогічної доведенню попередніх теорем.

Знайдемо залежність потужності $\|L\|$ простого коду від числа значущих моментів та довжини сигнальної конструкції.

Спочатку розглянемо питання визначення числа значущих моментів, що забезпечує максимальну потужність $\|L\|$ простого таймерного коду при заданих m та s .

Теорема 5. Для простого таймерного коду максимальна потужність $\max \|L\| = \binom{ms - i(s-1)}{i}$, якщо $i = \left\lfloor \frac{ms}{s+1} \right\rfloor$, $\forall s > 0$ (множина s більше нуля) та $\forall m \geq 0$. Звідси

$$\max \|L\| > \binom{ms - (i-1)(s-1)}{i-1}, \quad (4.124)$$

$$\max \|L\| > \binom{ms - (i+1)(s-1)}{i+1}. \quad (4.125)$$

Доведення. Теорему буде доведено, якщо доведемо вирази (4.124), (4.125).

Припустимо, що $(ms, s+1) \neq 1$, тоді $i = \left\lfloor \frac{ms}{s+1} \right\rfloor$ й нерівність набуде вигляду

$$\frac{\Gamma\left(\frac{2ms}{s+1} + (s-1) + 1\right)}{\Gamma\left(\frac{2ms}{s+1} + 1\right)} < \frac{\Gamma\left(\frac{2ms}{s+1} + 1\right)}{\frac{ms}{s+1} \cdot \Gamma\left(\frac{ms}{s+1} + 1\right)},$$

де $\Gamma(x)$ – гама-функція. Після перетворень остаточно маємо:

$$\left(\frac{m}{m+1+s}\right) \prod_{k=1}^{s-1} \left(1 + \frac{1}{1 + (s-k)\frac{s+1}{ms}}\right) < 1. \quad (4.126)$$

Дослідимо (4.126) в двох граничних випадках, коли $s \rightarrow 0$ та $s \rightarrow \infty$:

$$\lim_{s \rightarrow 0} \left(\frac{m}{m+1+s}\right) \prod_{k=1}^{s-1} \left(1 + \frac{1}{1 + (s-k)\frac{s+1}{ms}}\right) = \frac{1}{1 + \frac{1}{m}},$$

$$\lim_{s \rightarrow \infty} \left(\frac{m}{m+1+s}\right) \prod_{k=1}^{s-1} \left(1 + \frac{1}{1 + (s-k)\frac{s+1}{ms}}\right) = 0.$$

Отже, доведено вірність нерівності (4.124).

Аналогічно для виразу (4.125) можна записати

$$\frac{\Gamma\left(\frac{2ms}{s+1} - s\right)}{\Gamma\left(\frac{ms}{s+1} - s + 1\right) \cdot \left(\frac{ms}{s+1} + 1\right)} < \frac{\Gamma\left(\frac{2ms}{s+1} + 1\right)}{\Gamma\left(\frac{ms}{s+1} + 1\right)},$$

$$2 \left(\frac{ms + s + 1}{ms - (s-1)(s+1)}\right) \prod_{k=1}^{s-1} \left(1 + \frac{1}{ms - (s-k)(s+1)}\right) > 1.$$

Очевидно, що останній вираз є вірним для $\forall s \geq 0$ при $\forall m \geq 0$, тим самим рівняння (4.125) доведене. Для випадку, коли $(ms, s+1) = 1$, вірність виразів (4.124) і (4.125) впливає із властивостей гама-функції $\Gamma(x)$ при $x \geq 2$.

Теорему доведено.

Особливий інтерес становить аналіз залежності $\|L\|$ простого таймерного коду зі змінним числом значущих моментів від довжини кодової комбінації $n = ms$ за фіксованих значень s . Для блокових кодів, як відомо, збільшення довжини блока на одиницю призводить до подвоєння

потужності; аналогічно для таймерного коду при $s = 1$ маємо $\|L\| = 2^n$, і збільшення n на одиницю веде до подвоєння $\|L\|$.

Розглянемо випадок, коли $s > 1$ та $m \gg s$. Тоді $s(m-i) + i \rightarrow m$, і можна записати

$$\lim_{m \rightarrow \infty} \frac{\sum_{i=0}^{m+1} \binom{s(m-i)+i}{i}}{\sum_{i=0}^m \binom{s(m-i)+i}{i}} = 2.$$

Це свідчить про те, що s впливає лише на швидкість збіжності до граничного значення, тому для $m \approx s$ граничне значення співвідношення потужностей більше двох.

4.9. Питання та задачі для самоперевірки

1. Поясніть значення квантизатора в схемі 4.1.
2. Побудуйте епюри сигналів на виході схем РС1, РС2 і квантизатора при заданому кодовому слові на вході.
3. Чим визначається число входів і виходів квантизатора?
4. Побудуйте графічне представлення перехідних імовірностей квантизатора при числі значень сигналів на вході $x = 3$ і числі вихідних сигналів після квантизатора $y = 5$ (для $P(x_1) = P(x_2) = P(x_3) = 1/3$; $P(y_1) = P(y_2) = P(y_3) = P(y_4) = P(y_5) = 1/5$).
5. Нарисуйте діаграму перехідних імовірностей каналу із «стиранням» отриманого сигналу на виході двійкового каналу.
6. В чому відмінність «нижніх» зон квантування від «верхніх»? В якій зоні буде більше число помилок «нижній» чи «верхній»? Поясніть.
7. Чим визначається можливість виправлення всіх помилок в нижніх зонах квантування?
8. Чим визначається мінімальна кодова відстань корегуючого кода при відомій кратності виправляємих помилок в I і II зонах та числом символів першої зони?
9. Дайте визначення коефіцієнта кореляції двох кодових слів коригувального блокового коду і доведіть, що збільшення числа додаткових елементів (k) при постійному значенні інформаційних дійсно збільшує якість приймання кодового слова.
10. Чим визначається верхня межа можливої імовірності помилкового приймання двійкового коригувального коду?
11. Чим визначається енергетична ефективність приймання з двома рівнями квантування? Які кодові слова мають мінімальну вагу в коригувальному коді?

12. Які параметри каналу моделі Гільберта з двома станами (перевищення сигналу над завадами h^2) в «поганому» та «хорошому» стані?

13. Які імовірнісні параметри існування «поганого» і «хорошого» станів каналу? Яке середнє співвідношення інтервалів існування кожного із станів?

14. Знаючи середнє значення пакету помилок в «поганому» стані каналу, оцінити параметри коригувального коду при значеннях числа інформаційних символів $m_1 = 5$, $m_2 = 8$, припускаючи імовірність невірною приймання елементу кода на інтервалі існування пакету помилок $P_{\text{пом}} = 0,5$.

15. Чому при числі інформаційних відрізків i в ТСК, синтезованих на інтервалі m елементарних посилок, $N_p = 1$ для випадку $m = i$?

16. На якому інтервалі $T_c = mt_0$ при $s = 7$, $i = 4$ можливо синтезувати 2^{16} сигнальних конструкцій?

17. За якого мінімального значення s можна синтезувати 2^{12} сигнальних конструкцій, які мають число інформаційних відрізків $i = 3$ або $i = 4$ за умови, що $m = \text{const} = 6$?

18. Розрахуйте величину середньоквадратичного відхилення ЗМВ (σ_2) для каналу з базою $B = \Delta F \cdot t_0 = 2$, якщо при $B = 1$ $\sigma_1 = 0,02t_0$.

19. Визначте середнє значення плоскої вершини сигналу (рис. 3.17) при передаванні всіх реалізацій ТСК на інтервалі $m = 4$, $s = 4$, $i = 3$ для $B = \Delta F \cdot t_0 = 1$.

20. Побудуйте залежність $\log_2 N_{p\Sigma}$ при зміні $s \in 2 \dots 10$ для $T_c = 5 t_0$.

21. Оцініть при якому значенні s в каналі моделі Гільберта при коефіцієнті $h^2 = 56$ можливо одержати пропускну здатність в 2 рази більшу по відношенню до позиційного кодування.

22. Оцініть при яких значеннях m і s можливо отримати максимальне значення числа реалізацій:

m	4	5	6	7	8	9	10
i	3	2	7	5	2	1	5

23. Оцініть при яких значеннях m (в елементах) при $s = 6$ можливо реалізувати $N_{p_1} = 256$, $N_{p_2} = 512$ сигнальних конструкцій ТСК при $i = 4$.

24. Оцініть значення середньоквадратичного відхилення ЗМВ в «хорошому» стані каналу при ймовірності зміщення $P(\theta \leq 0,5\Delta) = 0,99862572$.

25. Яким чином можливо збільшити число реалізацій ТСК на заданому інтервалі при заданій імовірності помилкового прийому в «хорошому» стані каналу моделі Гільберта?

26. Користуючись додатком оцініть на скільки збільшиться граничне значення пропускної здатності каналу при збільшенні дозволеної множини на інтервалі $m = 7$. За рахунок сумісного використання ТСК з $i = 3$, $i = 4$ та $i = 7$.

27. При умовах задачі 26 оцініть втрати пропускної здатності при середній довжині пакета помилок в «поганому» стані каналу $l_n = 10$ символів.

28. При умові задачі 26 оцініть в якому випадку при $i_1 = 3$ чи $i_2 = 4$ мінімальна енергетична відстань між ТСК більша.

29. Для умови задачі 26 побудуйте на інтервалі $m = 8$ дві стартоstopні таймерні конструкції, які при $i_1 = 3$ та $i_2 = 4$ на інтервалі кодового слова мають стартовий ЗММ та стопову послідовність довжиною $t_{ст} = t_0$. За якою ознакою оцінюється належність одержаної ТСК до дозволеної множини?

30. Яке максимальне значення s доцільно вибирати в синтезованій ТСК при відомому середньоквадратичному значенні зміщень ЗМВ в «хорошому» стані каналу?

Глава 5

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ ТСК В СИСТЕМАХ ПЕРЕДАВАННЯ З БЛОКОВИМ КОДУВАННЯМ

5.1. Синдромні методи оцінки якості передавання

При посимвольному методі прийому кінцевий результат впливу шуму на передану комбінацію $X = (x_1; x_2; \dots; x_n)$ виражається в тому, що на виході декодера утворюється комбінація $\tilde{X} = (\tilde{x}_1; \tilde{x}_2; \dots; \tilde{x}_n)$, частина символів якої, можливо, не збігається з символами комбінації X . Цей процес можна інтерпретувати як результат «покоординатного» складання вектора X з шумовим вектором $E = (e_1; e_2; \dots; e_n)$, тобто вважають

$$\tilde{X} = X + E \quad (5.1)$$

й записати j -й символ прийнятої комбінації \tilde{X} у вигляді

$$\tilde{x}_j = x_j + e_j \quad (5.2)$$

де підсумовування проводиться за правилами поля $GF(b)$.

Число можливих шумових векторів (комбінацій значності n) дорівнює b^n . Кажуть, що шумова комбінація має вагу θ_b , якщо вона містить θ_b ($0 < \theta_b < n$) відмінних від нуля символів.

Вектор шуму ваги θ_b спотворює θ_b символів комбінації X , що призводить до утворення θ_b -кратної помилки в прийнятій комбінації.

Зауважимо, що наведена вище інтерпретація процесу спотворення складних сигналів з найбільшим ефектом може бути використана для вивчення систем, де реалізація того чи іншого вектора E не залежить від того, яка з кодових комбінацій передається.

Метод контрольних чисел. Ідея цього методу стосовно до бінарних кодів з корекцією одиночних помилок була викладена Хемінгом. Потім вона була обґрунтована і розповсюджена на більш складні випадки, в тому числі на не бінарні коди (див. приклад 1). Слід зазначити, що дослідження, які проводяться по цих напрямках різними авторами, відрізняються лише за формою, але не по суті.

Приклад 1.

Нехай задано код

$$x_1 x_2 \dots x_m F_1(x) \dots F_j(x) \dots F_k(x) \quad (5.3)$$

і по каналу передана одна з його комбінацій

$$\alpha_1 \dots \alpha_i \dots \alpha_m \beta_1 \dots \beta_j \dots \beta_k \quad (5.4)$$

де, перевірочний символ

$$\beta_j = \sum_{i=1}^m c_{ij} \alpha_i \quad (5.5)$$

(c_{ij} – коефіцієнт при незалежній змінній x_i в лінійній формі $F_j(x)$).

Припустимо, що прийнята комбінація

$$\tilde{\alpha}_1 \dots \tilde{\alpha}_l \dots \tilde{\alpha}_m \tilde{\beta}_1 \dots \tilde{\beta}_j \dots \tilde{\beta}_k \quad (5.6)$$

Для зручності запишемо вектор шуму у вигляді

$$E = (e_1 \dots e_i \dots e_m s_1 \dots s_j \dots s_m), \quad (5.7)$$

Тоді в повній відповідності (5.1) і (5.2) інформаційні символи комбінації (5.6).

$$\tilde{\alpha}_i = \alpha_i + \tilde{e}_i \quad (5.8)$$

а її перевіірочні символи

$$\tilde{\beta}_j = \beta_j + s_j = \sum_{i=1}^m c_{ij} \alpha_i + s_j \quad (5.8a)$$

Обчислимо значення перевіірочних символів $\tilde{\beta}_j^*$, використовуючи для цієї мети інформаційні символи прийнятої комбінації і співвідношення (5.5):

$$\tilde{\beta}_j^* = \sum_{i=1}^m c_{ij} \tilde{\alpha}_i \quad (5.9)$$

Знайдемо різницю:

$$\begin{aligned} G_1 &= \beta_1^* - \tilde{\beta}_1, \\ G_2 &= \beta_2^* - \tilde{\beta}_2, \\ &\dots\dots\dots \\ G_k &= \beta_k^* - \tilde{\beta}_k. \end{aligned} \quad (5.10)$$

Сукупність елементів G_j називають контрольним числом або синдромом. По виду контрольного числа, як буде показано нижче, можна зробити не тільки висновок про те, чи містить прийнята комбінація трансформовані символи, але і визначити їх місце і характер спотворення¹.

Підставляючи (5.8) і (5.8a) в (5.10) знайдемо

$$\begin{aligned} G_1 &= \sum_{i=1}^m c_{i1} e_i - s_1, \\ G_2 &= \sum_{i=1}^m c_{i2} e_i - s_2, \\ &\dots\dots\dots \\ G_k &= \sum_{i=1}^m c_{ik} e_i - s_k. \end{aligned} \quad (5.11)$$

Звідси видно, що елементи контрольного числа залежать тільки від значення компонент вектора шуму. Іншими словами, контрольне число інваріантно відносно комбінацій коду (5.3).

¹ У бінарному випадку для виправлення помилок достатньо лише знати номер спотвореного символу. У не бінарних кодах кожен символ може бути трансформований $b - 1$ різними способами, тому тут необхідно встановити не лише номер спотвореного символу, але й характер його спотворення

Теорема 1. Всі елементи контрольного числа дорівнюють нулю тоді (і лише тоді), коли прийнята комбінація (5.6) збігається з однією з комбінацій коли (5.3).

Дійсно, з (5.11) випливає, що якщо $G_j = 0$, то

$$s_j = \sum_{i=1}^m c_{ij} e_i, \quad (5.12)$$

тобто символ s_j пов'язаний з першими символами комбінації E співвідношенням, характерним для j -го перевірного символу комбінацій даного коду (5.4). Іншими словами, шумова комбінація E збігається з однією з комбінацій коду, в силу чого і прийнята комбінація належить коду.

Аналіз показує, що якщо у векторі E тільки одна з компонентів $e_j \neq 0$, то

$$G_1 = c_{ij} e_i; \dots; G_j = c_{ij} e_i; \dots; G_k = c_{ij} e_i \quad (5.13)$$

зокрема, при $e_i = 1$

$$G_1 = c_{ij}; \dots; G_j = c_{ij}; \dots; G_k = c_{ik} \quad (5.14)$$

Звідси виходить, що кожному з $b - 1$ можливих спотворень i -го інформаційного символу відповідають контрольні числа, що представляють собою результат множення на e_j компонент вектора G (5.14) (всілякими спотвореннями j -го інформаційного символу, відповідає системі $b-1$ лінійно залежних векторів).

Якщо ж вектор E такий, що лише його компонента $s_j \neq 0$, то

$$G_1 = 0; G_{j-1} = 0; G_j = s_j; G_{j+1} = 0; G_k = 0 \quad (5.15)$$

зокрема, коли s_j збігається з елементом, зворотним одиниці даного поля ($s_j = -1$), ми маємо

$$G_1 = 0; G_{j-1} = 0; G_j = 1; G_{j+1} = 0; G_k = 0 \quad (5.16)$$

Таким чином, номер позиції контрольного числа, на якій розташовується відмінний від нуля елемент, збігається з номером трансформованого перевірного символу, причому G_j є елементом, зворотним s_j .

Випишемо у вигляді матриці коефіцієнти C_{ij} при незалежних змінних x_i в лінійних формах $F_j(x)$ (5.4) і доповнимо її одиничною матрицею, кожен рядок якої помножений на -1 :

$$\left\{ \begin{array}{l} m \\ k \end{array} \right\} \left\| \begin{array}{cccccc} c_{11} & c_{12} & c_{13} & \dots & c_{1k} \\ \dots & \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & c_{m3} & \dots & c_{mk} \\ -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 \end{array} \right\| \quad (5.17)$$

Матрицю (5.17) домовимося називати контрольною, бо перші m її рядків – контрольні числа, відповідно зміни на $+1$ i -го інформаційного символу, а k останніх рядків визначають контрольні числа, відповідні зміни на ту ж величину j -го перевірного символу.

У силу лінійності операцій, використовуваних для обчислення елемента G_j , контрольне число, відповідне різним спотворень символів комбінації, може бути знайдено як деяка нетривіальна сума рядків контрольної матриці.

Теорема 2. Якщо знайти лінійну комбінацію рядків (5.17), таку, що вона буде збігатися з обчисленим контрольним числом, то номери цих рядків співпадуть із номерами спотворених позицій, а коефіцієнти, з якими вони склалися, визначають, як спотворений символ, що стоїть на відповідній позиції. (Для того, щоб виправити спотворений символ, достатньо знайти елемент, протилежний кожному із зазначених коефіцієнтів, і додати його до відповідного символу прийнятої комбінації).

Звернемо увагу на дві обставини. По-перше, число k -значних векторів типу (5.10) дорівнює b^k , і, отже, можливе число коректованих помилок принципово не може бути більше $b^k - 1$. По-друге, кожне контрольне число неоднозначно визначає характер спотворення прийнятої комбінації [одне і те ж контрольне число може бути отримане в результаті різних лінійних комбінацій рядків матриці (5.17)]. Отже, завдання корекції помилок не має однозначного рішення, і в комбінаціях одного, і того ж коду можна виправляти різні безлічі помилок потужністю не більше $b^k - 1$.

В даний час не існує яких-небудь конструктивних методів, що дозволяють визначити повний набір множин помилок, що можуть бути виправлені даним кодом.

З фізичної точки зору ясно, що безліч шумових комбінацій буде коригуватися даним кодом, якщо помилкам, викликаним в кодової комбінації будь-який з них, відповідає своє, відмінне від нуля контрольне число. Виявляється, що для виконання цієї вимоги шумові комбінації повинні задовольняти наступним умовам.

Теорема 3. Безліч шумових комбінацій E_r ($r = 1, 2, \dots, b^k - 1$) коректується даним кодом, якщо, по-перше, не збігається ні з однією з комбінацій даного коду і, по-друге, різниця двох будь-яких векторів E_r і E_s також не утворює комбінацію коду.

Необхідність виконання першої умови очевидна в силу теореми 1. Покажемо, що при виконанні другої умови помилкам, породжуваним в кодової комбінації різними шумовими комбінаціями, відповідають певні і не співпадаючі контрольні числа.

Зафіксуємо два вектор-шуму: $E_s = (e_{1s}; e_{2s}; \dots; e_{ts}; \dots; e_{ns})$ і $E_r = (e_{1r}; e_{2r}; \dots; e_{tr}; \dots; e_{nr})$. Випишемо їх різницю:

$$E_s - E_r = (e_1; e_2; \dots; e_i; \dots; e_n), \quad (5.18)$$

де

$$e_t = e_{ts} - e_{tr}.$$

Контрольні числа, відповідні векторам E_s , E_r та E , визначаються формулами (5.11), причому їх j -ті елементи мають вигляд:

$$\left. \begin{aligned} G_{js} &= \sum_{i=1}^m c_{ij} e_{is} - e_{(m+j)s} \\ G_{jr} &= \sum_{i=1}^m c_{ij} e_{ir} - e_{(m+j)r} \\ G_j &= \sum_{i=1}^m c_{ij} e_i - e_{(m+j)} \end{aligned} \right\} \quad (5.19)$$

де $j = 1, 2, \dots, k$.

Аналіз цих виразів приводить до висновку:

$$G_j = G_{js} - G_{jr}. \quad (5.20)$$

Таким чином, контрольні числа (5.19) не будуть збігатися, якщо серед елементів різницевого контрольного числа (5.20) виявиться хоча б один відмінний від нуля. У нашому випадку ця обставина і має місце, бо різницевий вектор по умові не належить коду, і тому згідно теоремі 1 серед елементів його контрольного числа завжди знайдеться принаймні один відмінний від нуля.

Тільки що доведене положення широко використовується в теорії кодування.

Наслідок 1 (теорема 3). Кожне контрольне число може бути отримане в результаті b^m спотворення символів кодової комбінації.

Дійсно, нехай шумовий комбінації E_1 відповідно деяке контрольне число, тоді те ж саме контрольне число буде отримано і при іншій шумовий комбінації E_2 , якщо

$$E_2 - E_1 = X_l \quad (5.21)$$

або

$$E_2 = E_1 - X_l, \quad (5.21a)$$

де X_l – довільна комбінація даного коду.

При фіксованому векторі шуму E_1 вектор X_l може прийняти b^m різних значень. (Число комбінацій даного коду дорівнює b^m).

Вираз (5.21a) дозволяє однозначно розбити безліч всіх n -значних комбінацій на b^k непересічних підмножин (всього мається b^k різних контрольних чисел). Зауважимо, що одне з цих підмножин буде збігатися з кодом (випадок, коли контрольне число дорівнює нулю). Зазначені підмножини володіють властивостями, властивими так званим в алгебрі класам суміжності. Тому іноді теорема 3 формулюється так: безліч шумових комбінацій коректується даним кодом, якщо кожна з них

належить різним класам суміжності. Таким чином, процес виправлення помилок методом контрольних чисел в загальному випадку протікає так. На приймальному кінці у вигляді таблиці записуються контрольні числа та відповідні їм шумові комбінації (кожному контрольному числу ставиться у відповідність одна і тільки одна шумова комбінація з класу суміжності, визначеного даним контрольним числом). Прийнята комбінація \tilde{Y} запам'ятовується в спеціальному пристрої пам'яті. Потім обчислюється контрольне число, і якщо виявиться, що воно відмінно від нуля, то за допомогою зазначеної таблиці знаходиться відповідна йому шумова комбінація. Остання віднімається з \tilde{Y} , на чому і закінчується процес корекції помилок. Хеммінг на прикладі семизначного бінарного коду з $d=3$ розробив метод, при якому контрольні числа збігаються з двійкової записом номера спотвореного символу. Такі ідеї можуть бути реалізовані стосовно до ряду кодів з підстави $b \geq 3$. Нарешті, зауважимо, що метод контрольних чисел допускає безліч модифікацій, заснованих на структурних особливостях контрольних чисел, відповідних цим або іншим групам помилок, і на те, що для правильного впізнання надісланого повідомлення достатньо виправити помилки в інформаційних символах прийнятої комбінації.

Число всіх множин шумових комбінацій, коректованих даним кодом, дорівнює $(b^m)^{b^k-1}$. Серед них особливий інтерес представляє випадок, коли з кожного класу суміжності вибирається найбільш ймовірна шумова комбінація (що має найменшу вагу для симетричних каналів), що забезпечує максимум ймовірності правильного декодування. Конструктивні методи вирішення такого завдання в загальному випадку навіть для найпростіших каналів в даний час невідомі, а їх пошук ускладнюється тим, що коректують можливості коду (змістовність суміжних класів) залежать не тільки від вибору лінійних форм, але і від способу упорядкування цих форм по позиціях, хоча остання обставина не впливає на d_{kl} .

Приклад 2. Розглянемо семизначний бінарний код:

$$x_1x_2x_3 + x_2x_1 + x_3x_2 + x_3x_1 + x_2 + x_3 \quad (5.22)$$

Комбінації цього коду відрізняються одна від одної точно в чотирьох позиціях ($d=4$) і утворюють нульовий клас суміжності (див. табл. 5.1).

Контрольна матриця аналізованого коду відповідно до (5.17) має вигляд [в поле GF (2) $1 = -1$]

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (5.23)$$

Якщо прийняту комбінацію записати у вигляді

$$\tilde{\alpha}_1 \tilde{\alpha}_2 \tilde{\alpha}_3 \tilde{\beta}_1 \tilde{\beta}_2 \tilde{\beta}_3 \tilde{\beta}_4 \quad (5.23a)$$

то згідно (5.11)

$$\begin{aligned} G_1 &= \tilde{\alpha}_1 \oplus \tilde{\alpha}_2 \oplus \tilde{\beta}_1, \\ G_2 &= \tilde{\alpha}_1 \oplus \tilde{\alpha}_3 \oplus \tilde{\beta}_2, \\ G_3 &= \tilde{\alpha}_2 \oplus \tilde{\alpha}_3 \oplus \tilde{\beta}_3, \\ G_4 &= \tilde{\alpha}_1 \oplus \tilde{\alpha}_2 \oplus \tilde{\alpha}_3 \oplus \tilde{\beta}_4. \end{aligned} \quad (5.24)$$

Контрольні числа вписані у другому рядку табл. 5.1. Під кожним з них наведені елементи відповідного класу суміжності, які визначалися в такий спосіб.

Таблиця 5.1

Номер класу суміжності	0	1	2,	3	4	5	6	7
Контрольне число	0000	1101	1011	0111	1000	0100	0010	0001
Класи суміжності	0000000	1000000	0100000	0010000	0001000	0000100	0000010	0000001
	0010111	1010111	0110111	0000111	0011111	0010011	0010101	0010110
	0101011	1101011	0001011	0111011	0100011	0101111	0101001	0101010
	0111100	1111100	0011100	0101100	0110100	0111000	0111110	0111101
	1001101	0001101	1101101	1011101	1000101	1001001	1001111	1001100
	1011010	0011010	1111010	1001010	1010010	1011110	1011000	1011011
	1100110	0100110	1000110	1110110	1101110	1100010	1100100	1100111
	1110001	0110001	1010001	1100001	1111001	1110101	1110011	1110000

Номер класу суміжності	8	9	10	11	12	13	14	15
Контрольне число	1100	1010	1001	0110	0101	0011	1110	1111
Класи суміжності	0001100	0001010	0001001	0000110	0000101	0000011	0001110	1000010
	0011011	0011101	0011110	0010001	0010010	0010100	0011001	1010101
	0100111	0100001	0100010	0101101	0101110	0101000	0100101	1101001
	0110000	0110110	0110101	0111010	0111001	0111111	0110010	1111110
	1000001	1000111	1000100	1001011	1001000	1001110	1000011	0001111
	1010110	1010000	1010011	1011100	1011111	1011001	1010100	0011000
	1101010	1101100	1101111	1100000	1100011	1100101	1101000	0100100
	1111101	1111011	1111000	1110111	1110100	1110010	1111111	0110011

Спочатку визначалася одна (будь-яка) шумова комбінація, яка призводить до даного контрольного числа, а потім на основі формули (5.21a) знаходилися інші елементи класу суміжності.

Ці операції легко виконуються за допомогою перевірконої матриці (5.23). Перша її рядок збігається з контрольним числом, яке утворюється при спотворенні першого інформаційного символу ($E = 1000000$). Додаючи до знайденої таким чином шумової комбінації всі комбінації коду (5.22) (комбінації нульового класу суміжності), отримуємо всі елементи першого класу суміжності. Другий рядок матриці (5.23) збігається з контрольним числом, відповідним шумовий комбінації 0100000. Використовуючи цю обставину і формулу (5.21a), отримуємо всі елементи другого класу суміжності. Контрольні числа, що визначають класи суміжності з номерами від восьмого і більше, не містяться в контрольній матриці, кожне з них представлено у вигляді деякої суми її рядків. (Це вірно хоча б вже тому, що (5.23) містить одиничну підматрицю). Наприклад, контрольне число 1100 можна отримати складанням четвертого та п'ятого рядків або в результаті підсумовування першого і останнього рядків. Перша ситуація відповідає випадку одночасного спотворення першого і другого перевірочних символів ($E = 0001100$), а друга – одночасного спотворення першого інформаційного та останнього перевірочного символу ($E = 1000001$). Вибираючи будь-яку із зазначених шумових комбінацій і складаючи її з кожною з комбінацій коду, знайдемо всі елементи восьмого класу суміжності і т. д.

У коді (5.22) $k = 4$, тому є можливість коректувати 24-1 різних спотворень символів його комбінацій, наприклад спотворень, викликаних 7 одиничними, 7 подвійними і 1 потрійними помилками (сім класів суміжності табл. 5.1 містять комбінації ваги один, вісім – ваги два, і один, а саме 14-й, – ваги три і більше). При цьому ймовірність правильного прийому комбінації коду в разі симетричного каналу без пам'яті дорівнює

$$Q = (1 - p_0)^7 + 7 p_0(1 - p_0)^6 + 7 p_0^2(1 - p_0)^5 + 7 p_0^3(1 - p_0)^4. \quad (5.25)$$

Якщо символи комбінації спотворюються завадами не незалежно, то серед векторів E ваги два найбільш ймовірними виявляються вектора виду

$$0 \ 0 \ \dots \ 0 \ 1 \ 1 \ 0 \ \dots \ 0 \quad (5.26)$$

Вони породжують так звані подвійні суміжні (парні) помилки. Природно, що такого роду помилки бажано включити в число коректованих. Однак стосовно до коду (5.22) цього зробити не можна, бо комбінації 0001100 та 0110000 належать одному (восьмому) класу суміжності.

Змінимо в (5.22) порядок проходження лінійних форм, що визначають перевірочні символи:

$$x_1x_2x_3 \quad x_1 + x_2 \quad x_2 + x_3 \quad x_1 + x_2 + x_3 \quad x_1 + x_3 \quad (5.27)$$

Таблиця 5.2

Номер класу суміжності	0	1	2	3	4	5	6	7
Контрольне число	0000	1011	1110	0111	1000	0100	0010	0001
Класи суміжності	0000000	1000000	0100000	0010000	0001000	0000100	0000010	0000001
	0010111	1010111	0110111	0000111	0011111	0010011	0010101	0010110
	0101110	1101110	0001110	0111110	0100110	0101010	0101100	0101111
	0111001	1111001	0011001	0101001	0110001	0111101	0111011	0111000
	1001011	0001011	1101011	1011011	1000011	1001111	1001001	1001010
	1011100	0011100	1111100	1001100	1010100	1011000	1011110	1011101
	1100101	0100101	1000101	1110101	1101101	1100001	1100111	1100100
	1110010	0110010	1010010	1100010	1111010	1110110	1110000	1110011

Номер класу суміжності	8	9	10	11	12	13	14	15
Контрольне число	0101	1001	1111	1100	0110	0011	1010	1101
Класи суміжності	1100000	0110000	0011000	0001100	0000110	0000011	0001010	0001101
	1110111	0100111	0001111	0011011	0010001	0010100	0011101	0011010
	1001110	0011110	0110110	0100010	0101000	0101101	0100100	0100011
	1011001	0001001	0100001	0110101	0111111	0111010	0110011	0110100
	0101011	1111011	1010011	1000111	1001101	1001000	1000001	1000110
	0111100	1101100	1000100	1010000	1011010	1011111	1010110	1010001
	1111010	1010101	1111101	1101001	1100011	1100110	1101111	1101000
	0010010	1000010	1101010	1111110	1110100	1110001	1111000	1111111

Таблиця 5.3

Номер класу суміжності	0	1	2	3	4	5	6	7
Контрольне число	000	1111	0111	1011	1000	0100	0010	0001
Класи суміжності	0000000	1000000	1000000	0010000	0001000	0000100	0000010	0000001
	1001111	0001111	1101111	1011111	1000111	1001011	1001101	1001110
	0100111	1100111	0000111	0110111	0101111	0100011	0100101	0100110
	0011011	1011011	0111011	0001011	0010011	0011111	0011001	0011010
	1101000	0101000	1001000	1111000	1100000	0101100	1101010	1101001
	1010100	0010100	1110100	1000100	1011100	1010000	1010110	1010101
	0111100	1111100	0011100	0101100	0110100	0111000	0111110	0111101
	1110011	0110011	1010011	1100011	1111011	1110111	1110001	1110010

Номер класу суміжності	8	9	10	11	12	13	14	15
Контрольне число	1110	1101	1100	1010	1001	0110	0101	0011
Класи суміжності	1000001	1000010	0001100	0001010	0001001	0000110	0000101	0000011
	0001110	0001101	1000011	1000101	1000110	1001001	1001010	1001100
	1100110	1100101	0101011	0101101	0101110	0100001	0100010	0100100
	1011010	1011001	0010111	0010001	0010010	0011101	0011110	0011000
	0101001	0101010	1100100	1100010	1100001	1101110	1101101	1101011
	0010101	0010110	1011000	1011110	1011101	1010010	1010001	1010111
	1111101	1111110	0110000	0110110	0110101	0111010	0111001	0111111
	0110010	0110001	1111111	1111001	1111010	1110101	1110110	1110000

Всі контрольні числа і відповідні їм комбінації класів суміжності цього коду представлені в табл. 5.2.

Перші два рядки контрольної матриці цього коду відрізняються від відповідних рядків (5.23) (ср. контрольні числа, що визначають перший і другий клас суміжності табл. 5.1 і 5.2). Код (5.27), як і код (5.22), дозволяє коригувати 7 одиночних, 7 подвійних і 1 потрійну помилку. Однак всі комбінації виду (5.26) в табл. 5.2 розташовуються в різних суміжних класах, і, отже, в число виправляємих подвійних помилок можуть бути включені всі парні помилки. Таким чином, простою перестановкою лінійних форм отримано код з новою якістю коригування крім всіх одиночних помилок все подвійні суміжні помилки. Нарешті, розглянемо ще один семизначний бінарний код з трьома інформаційними символами:

$$x_1x_2x_3 \quad x_1 + x_3 \quad x_1 + x_2 \quad x_1 + x_2 + x_3 \quad x_1 + x_2 + x_3. \quad (5.28)$$

Всі контрольні числа й обумовлені ними класи суміжності наведені в табл. 5.3: 7 з них містять комбінації ваги один і 8 – ваги 2, а кодова відстань $d = 3$, що на одиницю менше, ніж у двох попередніх кодах. Однак незважаючи на останню обставину, код (5.28) у разі бінарного симетричного каналу забезпечує більшу ймовірність правильного прийому комбінації, бо є можливість виправити в ній, крім всіх одиночних, 8 подвійних помилок (а не 7 подвійних і одну потрійну, як було раніше). Ймовірність правильного прийому

$$Q = (1 - p_0)^7 + 7 p_0(1 - p_0)^6 + 8 p_0^2(1 - p_0)^5. \quad (5.28a)$$

Різниця між цією величиною і (5.25), звичайно, дуже мала, і зазначений факт має лише принципове значення - він є гарною, ілюстрацією положення, згідно з яким оптимізація коду в сенсі максимуму d ще не означає оптимізацію в сенсі максимуму ймовірності правильного прийому.

5.2. Кориговальні коди ТСК в системі залишкових класів

Системою залишкових класів зазвичай називається така непозиційна система числення, в якій будь-яке ціле додатне число подається у вигляді набору найменших додатних залишків (вирахувань) від ділення цього числа на фіксовані цілі додатні числа p_1, p_2, \dots, p_m , які називаються основами (модулями).

Позначимо $a_i = |A|$ – найменший позитивний залишок від ділення цілого числа A на основу p_i . Тоді; число A запишеться в системі залишкових класів у такій формі:

$$A = \{a_1, a_2, \dots, a_m\} \quad (5.29)$$

Будь-якому цілому числу A можна зіставити певний набір $\{a_1, \dots, a_m\}$, але зворотне твердження справедливе лише в тому випадку, коли основи СЗК попарно взаємно прості. Якщо ця умова не виконується, то знайдуться такі набори $\{a_1, \dots, a_m\}$, яким не можна зіставити жодного цілого числа A .

Наприклад, при $p_1 = 4$ і $p_2 = 6$ числа $A = 7$ відповідає набір $\{3, 1\}$, проте набору $\{3, 2\}$ не відповідає жодне з цілих чисел.

Для довільної СЗК існує $M = [p_1, p_2, \dots, p_m]^2$ різних наборів $\{a_1, \dots, a_m\}$, кожному з яких можна зіставити множину цілих чисел виду $A \pm kM$, де $k = 0, 1, 2, \dots$. Якщо всі цілі числа A належать інтервалу, значення якого дорівнює M , то кожному набору $\{a_1, \dots, a_m\}$ відповідає тільки одне число A із заданого інтервалу.

Число M назвемо загальною основою (модулем) системи залишкових класів. Надалі під терміном «основою M » будемо розуміти саме загальну основу системи.

Для запису цілого числа A в СЗК із загальною основою M скористуємося позначенням

$$A = \{a_1, a_2, \dots, a_m\}M \quad (5.30)$$

У позиційних системах числення в основному використовуються два типи дробових чисел – дробу з довільним знаменником A/B і дробу з фіксованим знаменником A/pk , де A і B – довільні цілі числа, p – основа позиційної системи числення, k – ціле додатне число.

Величина k визначається або положенням коми між розрядами числа (для чисел з фіксованою комою), або задається окремим числом (для чисел з плаваючою комою). Обидва типи дробів можна подати у системі залишкових класів.

У першому випадку і чисельник і знаменник подаються окремо в СЗК з основою M :

$$A/B = \{a_1, a_2, \dots, a_m\}M / \{\beta_1, \beta_2, \dots, \beta_m\}M.$$

² $[p_1, p_2, \dots, p_m]$ – найменше спільне кратне чисел p_1, p_2, \dots, p_m . Якщо ці числа попарно взаємно прості, то $[p_1, p_2, \dots, p_m] = p_1, p_2, \dots, p_m$.

У другому випадку в якості знаменника можна використовувати величину, рівну найменшому спільному кратному всіх або частини основ системи. При цьому для зазначення модулів, що входять до складу знаменника, іноді використовують косі дужки. Наприклад, якщо в СЗК з попарно простими основами p_1, p_2, p_3, p_4 знаменник дорівнює $p_1 p_2$, то

$$A/p_1 p_2 = \{/a_1, a_2/, \dots, a_m\}_M,$$

де $A = \{a_1, a_2, a_3, a_4\}_M$.

Однак у даному посібнику використовується інше позначення:

$$A/N = \{a_1, a_2, \dots, a_m\}_M^N = \{A\}_M^N,$$

де N – фіксоване ціле число.

Зокрема, N може дорівнювати найменшому спільному кратному будь-яких основ системи.

Таке подання дробів відповідає числам з фіксованою комою.

У системі залишкових класів немає природного поділу чисел на додатні і від'ємні. Тому існує кілька способів подання від'ємних чисел. Мабуть, найзручніше подавати від'ємні числа у вигляді доповнення абсолютної величини числа до основи системи M (подання, аналогічне додатковому коду в позиційних системах числення):

$$\{-A\}_M = \{0 - A\}_M = \{M - A\}_M.$$

Якщо величина діапазону зміни чисел L дорівнює основі M і сам діапазон симетрично розташований відносно нуля, то додатними є числа, що лежать в інтервалі $(0, M/2)$, а від'ємними – числа в інтервалі $(M/2, M)$.

У загальному випадку при зміні чисел в інтервалі $(-L_1, L_2)$, де $L_1 + L_2 = L M$, додатними вважаються числа, що лежать в інтервалі $(0, L_2]$, а від'ємними – числа в інтервалі $(M - L_1, M)$ ³.

Все вищесказане поширюється і на дробові числа, якщо покласти, що L – діапазон зміни числівників.

Наведемо приклад, який ілюструє подання чисел в СЗК.

Приклад 3. Нехай дана СЗК з основами $p_1 = 4, p_2 = 5, p_3 = 6$ і загальною основою $M = [4, 5, 6] = 60$.

Отже, діапазон зміни чисел, поданих в цій системі числення, не повинен перевищувати 60. Покладемо $L_1 = L_2 = 30$ й подамо у заданій СЗК цілі числа $A = +17, B = -17$:

$$\{A\}_M = \{17\}_M = \{1, 2, 5\}_M; \{B\}_M = \{-17\}_M = \{3, 3, 1\}_M.$$

Модульні операції. Операція, що виконується над групою чисел, називається модульною або непозиційною, якщо значення будь-якого розряду результату залежить тільки від значень відповідних розрядів вихідних чисел. Модульними є, наприклад, операції логічного складання, множення, порівняння та додавання за модулем два, вживані у ЦОМ.

На відміну від позиційних систем числення, де величина певного розряду суми або добутку залежить не тільки від значень відповідних, але і

³ Символом L позначається й сам діапазон зміни чисел та його величина.

від інших розрядів доданків або співмножників, у системі залишкових класів додавання, віднімання і добуток (для цілих чисел) виконуються окремо за кожною основою і переноси між розрядами відсутні.

Отже, ці операції в системі залишкових класів є модульними.

Нехай

$$\{A\}_M = \{a_1, a_2, \dots, a_m\}_M; \{B\}_M = \{\beta_1, \beta_2, \dots, \beta_m\}_M.$$

Тоді

$$\{C\}_M = \{A \underset{M}{\div} B\}_M = \{\gamma_1, \gamma_2, \dots, \gamma_m\}_M, \quad (5.31)$$

де $i = 1, 2, \dots, m$.

Цікаво, формула (5.31) виявляється справедливою для чисел будь-якого знаку. Оскільки для додавання і віднімання чисел таке твердження тривіальне, розглянемо лише операцію множення.

Нехай один із співмножників (A) від'ємний, а інший (B) – додатний.

Тоді

$$\{C\}_M = \{M - |A|\}_M \cdot \{B\}_M = \{B \cdot M - |A| \cdot B\}_M.$$

Але очевидно, що $|BM|_M = 0$. Тому $\{C\}_M = \{M - |A| \cdot B\}_M$. Покладемо тепер, що обидва множники є невід'ємними:

$$\begin{aligned} \{C\}_M &= \{M - |A|\}_M \cdot \{M - |B|\}_M = \\ &= \{M^2 - M \cdot |A| - M \cdot |B|\}_M = \{|A| \cdot |B|\}_M. \end{aligned}$$

Таким чином, множення завжди можна звести до операцій, виконуваних над додатними числами.

Рівність (5.31) справедлива лише у тому випадку, якщо результат операції не виходить за межі інтервалу визначення.

Модульні операції та їхні результати називаються формальними, якщо при виконанні цих операцій нехтують можливим виходом результату за межі діапазону.

До модульних операцій можна віднести і ділення цілих чисел без залишку:

$$\{C\}_M = \{A\}_M / \{B\}_M = \{\gamma_1, \gamma_2, \dots, \gamma_m\}, \quad (5.32)$$

де

$$\gamma_i = \left| \frac{\alpha_i}{\beta_i} \right|_{p_i} = \left| \alpha_i \left| \frac{1}{\beta_i} \right|_{p_i} \right|_{p_i}, \quad i = 1, 2, \dots, m.$$

Таким чином, ділення без залишку двох чисел в СЗК здійснюється шляхом модульного множення дільника на мультиплікативну зворотну величину дільника.

Величина $x = \left| \frac{1}{\beta_i} \right|_{p_i}$ є рішенням порівняння $x\beta_i \equiv 1 \pmod{p_i}$ й однозначно

визначена, якщо β_i і p_i взаємно прості числа.

Нехай для якого модуля p_i залишок β_i дорівнює нулю. Це означає, що p_i є дільником числа B . Але оскільки число A за умовою ділиться на B без

залишку, то основа p_i має бути також дільником A . Отже, $\alpha_i = 0$ і відповідна цифра частки є невизначеною:

$$\gamma_i = \left| \frac{0}{0} \right|_{p_i}.$$

Однак якщо число B ділиться на p_i , то це число заздалегідь не може бути меншим, ніж p_i , і тому $C = (A/B) < (M/p_i)$.

Тому частка C може бути однозначно подана у скороченій СЗК, отриманій шляхом виключення з вихідної СЗК основи p_i (і відповідно невизначеною цифри γ_i). Невизначена цифра частки C може бути однозначно обчислена за значеннями інших залишків частки внаслідок розширення скороченої СЗК.

Якщо β_i і p_i мають найбільший спільний дільник d_i , то залишок α_i також повинен ділитися на d_i . Тоді

$$\left| \frac{\alpha_i}{\beta_i} \right|_{p_i} = \left| \frac{\alpha_i}{d_i} \left| \frac{d_i}{\beta_i} \right|_{\frac{p_i}{d_i}} + \xi_i \frac{p_i}{d_i} \right|_{p_i}.$$

Величина $\xi_i = 0, 1, 2, \dots, d_i - 1$ однозначно визначається рештою цифр частки, оскільки $C \leq (A/d_i) < (M/d_i)$.

Проілюструємо вищесказане прикладами.

Приклад 4. Визначимо суму, різницю й добуток чисел $A = 3$ і $B = 5$, поданих у системі залишкових класів з основами $p_1 = 4$, $p_2 = 5$, $p_3 = 6$, і, крім того, обчислимо результати від ділення добутки цих чисел на кожен із співмножників:

$$\begin{aligned} \{A\}_M &= \{3\}_M = \{3, 3, 3\}_{60}; \{B\}_M = \{5\}_M = \{1, 0, 5\}_{60}. \\ \{C_1\}_M &= \{A + B\}_M = \{|3 + 1|_4; |3 + 0|_5; |3 + 5|_6\}_{60} = \{0, 3, 2\}_{60}; \\ \{C_2\}_M &= \{A - B\}_M = \{|3 - 1|_4; |3 - 0|_5; |3 - 5|_6\}_{60} = \{2, 3, 4\}_{60}; \\ \{C_3\}_M &= \{A \cdot B\}_M = \{|3 \cdot 1|_4; |3 \cdot 0|_5; |3 \cdot 5|_6\}_{60} = \{3, 0, 3\}_{60}; \\ \{C_4\}_M &= \left\{ \frac{C_3}{B} \right\}_M = \left\{ \left| \frac{3}{3} \right|_4; \left| \frac{0}{0} \right|_5; \left| \frac{3}{5} \right|_6 \right\}_{60}; \quad \left| \frac{3}{1} \right|_4 = |3 \cdot 1|_4 = 3; \quad \left| \frac{3}{5} \right|_6 = |3 \cdot 5|_6 = 3. \end{aligned}$$

Зворотні величини $\left| \frac{1}{\beta_i} \right|_{p_i}$ знайдемо з додатку. Оскільки

$C_4 \leq (C_3/5) < (L_1/5) = 6$, то залишки з основами p_1 і p_2 однозначно визначають частку, а, отже невизначену цифру за основою p_2 : $\left| \frac{0}{0} \right|_5 = 3$.

Таким чином

$$\begin{aligned} \{C_4\}_M &= \{A\}_M = \{3, 3, 3\}_{60}. \\ \{C_5\}_M &= \left\{ \frac{C_3}{A} \right\}_M = \left\{ \left| \frac{3}{3} \right|_4; \left| \frac{0}{0} \right|_5; \left| \frac{3}{5} \right|_6 \right\}_{60}; \quad \left| \frac{3}{3} \right|_4 = |3 \cdot 3|_4 = 1; \quad \left| \frac{0}{3} \right|_5 = |0 \cdot 3|_5 = 0 \end{aligned}$$

$$\left| \frac{3}{3} \right|_6 = |1 \cdot 1 + \xi_2 \cdot 2|_6.$$

Оскільки $C_5 < (L_1/3) = 10$, залишки з основами 4 і 5 дозволяють однозначно визначити величину ξ_3 (в даному прикладі вони однозначно визначають всю цифру $|3/3|_6$) $\xi_3 = 2$.

Отже, $\{C_5\}_M = \{B\}_M = \{1, 0, 5\}_{60}$.

Нижче будуть приведені способи обчислення невизначеної цифри частки за значеннями інших залишків.

Визначення позиційних характеристик чисел, поданих у СЗК.

Крім описаних вище модульних операцій, у ЦОМ часто виконуються і такі операції, які вимагають знання величини всього числа в цілому. Так, при визначенні знака, арифметичному порівнянні чисел, діленні та множенні дробів, округленні їх, а також при визначенні наявності переповнення необхідно знати розташування чисел у числовому діапазоні, тобто їх позиційні характеристики.

Розглянемо довільну позиційну систему числення з основами p_1, \dots, p_m , добуток яких дорівнює M . Припустимо, що $(M/p_{m_i}) < M \leq M$. Тоді будь-яке число з діапазону $[0, M]$ можна однозначно подати у даній позиційній системі числення⁴:

$$A = \sum_{i=1}^{m_i} \alpha_i \prod_{j=1}^{i-1} p_j, \quad (5.33)$$

де $\alpha_i = 0, 1, \dots, p_i - 1; i = 1, 2, \dots, m$.

Під позиційною характеристикою числа зазвичай розуміють таку функцію $\pi(A)$, яка залежить лише від символів a_i, a_{i+1}, \dots, a_m , що відповідають старшим розрядам числа. У більшості випадків для виконання різних модульних операцій в ЦОМ достатньо знати позиційну характеристику числа, що відповідає лише його старшому розряду, тобто $\pi(A) = f(a_{m_i})$.

Позначимо добуток основ p_1, \dots, p_i , що відповідають розрядам, які не приймають участі у визначенні позиційної характеристики числа $\pi(A)$ через K . Тоді

$$\pi_K(A) = f\left[\frac{A}{K}\right] = f\left(\frac{A - |A|_K}{K}\right). \quad (5.34)$$

Для чисел, поданих у СЗК з основами p_1, \dots, p_m , із загальною основою M , позиційна характеристика $\pi_K(A)$ є функцією від m змінних: $\pi_K(A) = \pi_K(a_1, \dots, a_m)$.

⁴ Такі системи числення зазвичай називаються узагальненими позиційними системами (УПС), поліадичними або ж системами числення зі змішаними основами (СЗО). Звичайну позиційну систему з основою p можна розглядати як окремий випадок УПС, у якої все основи рівні p .

Область визначення функції $\pi_K(a_1, \dots, a_m)$ значно більша (у K разів) області її зміни. Тому виникає питання, чи можна при обчислення позиційної характеристики використовувати не всі, а лише деякі із залишків a_1, \dots, a_m ; або за рахунок перетворень цих залишків зменшити область визначення π_K ? Проте теорема 4, що наводиться нижче (яка є модифікацією теореми кодування Сабо), показує, що практично будь-які незалежні перетворення окремих змінних a_1, \dots, a_m , у результаті яких можна було б зменшити область визначення позиційної характеристики, призводять до порушень однозначної відповідності між функціями $[A/K]$ й характеристик $\pi_K(A)$. Як буде показано нижче, якщо визначення зазначених характеристик здійснюється за допомогою довільних функціональних перетворювачів від однієї або двох змінних (змінними є вихідні залишки a_1, \dots, a_m , а також вихідні функції перетворювачів), то кількість послідовних перетворень, необхідних для обчислення $\pi_K(A)$, пропорційне кількості основ СЗК. Більш того, будь-які методи визначення позиційних характеристик, за яких не порушується однозначність $\pi_K(A)$, зводяться до переведення чисел із СЗК до УПС.

Доведемо невелику лему.

Лема 1.

Для будь-якого цілого числа $A = (a_1, \dots, a_m)_M$, поданого у СЗК з основами p_1, \dots, p_m , та для будь-якої пари основ p_1 і p_2 , повинна виконуватися умова:

$$|a_i - a_j|_{d_{ij}} = 0, \quad (5.35)$$

де d_{ij} – найбільший спільний дільник для основ p_i і p_j .

Доведення. Будь-яке число A можна подати за допомогою наступних рівностей:

$$A = k_i p_i + a_i = k_j p_j + a_j. \quad (5.36)$$

Визначимо залишок від ділення числа A на модуль d_{ij} , враховуючи, що $|p_i|_{d_{ij}} = |p_j|_{d_{ij}} = 0$.

Тоді $|A|_{d_{ij}} = |a_i|_{d_{ij}} = |a_j|_{d_{ij}}$ або $|a_i - a_j|_{d_{ij}} = 0$, що й потрібно було довести.

Теорема 4. Якщо для будь-якого цілого числа $A = \{a_1, \dots, a_m\}_M$, поданого в СЗК з основами та для будь-якої основи p_i ($i = 1, 2, \dots, m$) визначена функція $g(a_i)$, приймаюча $r_i < (p_i/d_i)$ різних значень, де d_i – найбільший спільний дільник між p_i і добутком інших основ СЗК, то для довільної позиційної характеристики $\pi_K(a_1, \dots, a_m)$ при $K \leq M - p_i$ заміна аргумента p_i на $g(a_i)$ порушить однозначність цієї функції, тобто знайдуться, по крайній мірі, два таких числа A і B що

$$\pi_K(A) = \pi_K(B) \text{ при } [A/K] \neq [B/K].$$

Доведення. Виберемо таке ціле число l , що $M > lK < p_i$. Серед множини чисел з діапазону $[0, M]$ завжди знайдуться такі $A = \{a_1, \dots, a_m\}_M$ і $B = \{\beta_1, \dots, \beta_m\}_M$ із інтервала $[lK, lK + p_i]$, що

$$g(a_i) = g(\beta_i); a_i \neq \beta_i [a_i - \beta_i] d_i = 0.$$

Визначимо число $C = \{\gamma_1, \dots, \gamma_m\}_M$ наступним чином:

$\gamma_j = a_j$ при $j = 1, 2, \dots, m, j \neq i$;

$\gamma_j = \beta_j$ при $j = i$.

Умова (5.35) для числа C у даному випадку виконується, оскільки

$$d_i = \prod_{j=1, j \neq i}^m d_{ij}.$$

Очевидно, в цьому випадку $\pi_K(A) = \pi_K(C)$, оскільки всі аргументи для обох характеристик однакові.

Якщо $0 \leq C_3 < IK$, то $[A/K] > l$, а $[C/K] < l$, тобто $[A/K] \neq [C/K]$, і, отже, теорему доведено.

Розглянемо випадок, коли $C \geq IK$.

Різниця $\{C - B\}_M$ містить нульовий залишок за основою p_i . Тому число $|C - B|_M$ має ділитися на p_i , тобто $|C - B|_M \geq p_i$.

Якщо $C < B$, то $C < IK$. Але оскільки ми прийняли, що $C \geq IK$, то

$$C \geq B + p_i \geq IK + p_i.$$

Розглянемо тепер числа $A - p_i$ і $C - p_i$. Для цих чисел позиційні характеристики рівні, але

$$\left[\frac{A - p_i}{K} \right] < l, \text{ а } \left[\frac{C - p_i}{K} \right] \geq l.$$

Отже, теорему доведено.

Якщо основами СЗК є взаємно прості числа, то для будь-якої основи p_i дільник d_i дорівнює одиниці. Тому будь-яке зменшення інформації про будь-який із залишків унеможливорює однозначне визначення позиційних характеристик.

З теореми 1 виходить, що для чисел, поданих у СЗК зі взаємно простими основами p_1, \dots, p_m , величина області визначення будь-якої позиційної характеристики $\pi_K(A) = \pi_K(a_1, \dots, a_m)_M$ при $K \leq M - p_{\max}$ не може бути меншою, ніж M , де $M = p_1 p_2 \dots p_m$, а p_{\max} – максимальна з основ p_1, \dots, p_m .

Можна припустити, що і для системи залишкових класів, у якої $M = [p_1 \dots p_m] < p_1, \dots, p_m$, величина області визначення позиційних характеристик повинна бути не меншою M , але, на жаль, цього поки довести не вдалося. Тому довелося обмежитися більш скромним наслідком теореми 1.

Наслідок 1.

Величина області визначення будь-якої позиційної характеристики $\pi_K(A) = \pi_K(a_1, \dots, a_m)$ при $K \leq M - [p_2, \dots, p_m]$ не може бути меншою, ніж M/d_1 , де d_1 – найбільший спільний дільник для p_1 і $[p_2, \dots, p_m]$.

Доведення. Основи p_2, \dots, p_m можна розглядати як один складений модуль p_2 , рівний $[p_2, \dots, p_m]$. Тоді вся система містить дві основи p_1 і p_2 з найменшим спільним дільником d_1 .

Утворюємо функції $g_1(a_1)$ і $g_2(a_2, \dots, a_m)$, що набувають відповідно r_1 і r_2 значень. У відповідності з теоремою 1 $r_1 \geq p_1/\tilde{d}_1$ і $r_2 \geq p_2/\tilde{d}_1$. Тоді

величина області визначення $\pi_K(A)$, що дорівнює добутку $r_1 r_2$, не може бути меншою, ніж

$$\frac{p_1 [p_2, \dots, p_m]}{\tilde{d}_1 \tilde{d}_1} = \frac{[p_1, \dots, p_m]}{\tilde{d}_1},$$

що й потрібно було довести.

В якості модуля p_1 можна вибрати будь-яку основу СЗК. Отже, можна вважати, що область визначення $\pi_K(A)$ збігається з діапазоном зміни чисел (або, у крайньому випадку, за наявності загальних дільників у основі має той же порядок). Оскільки зазвичай величина M має порядок $10^6 - 10^{10}$, то табличний метод реалізації довільної функції у даному випадку, звичайно, відповідає.

Тому спробуємо подати позиційну характеристику числа $\pi_K(A)$ за допомогою набору функцій, що залежать не більше ніж від двох змінних (залишків).

Розглянемо деякий вектор $\tilde{A} = (\tilde{a}_1, \tilde{a}_2, \dots, \tilde{a}_m)$, компонентами якого є натуральні числа, що задовольняють умові: $0 \leq \tilde{a}_i \leq p_i - 1$, де $i = 1, 2, \dots, m$; p_1, \dots, p_m – фіксовані натуральні числа.

З іншого боку, розглянемо множину L , що містять L цілих чисел A , таких, що якщо будь-які два числа A_1 і A_2 належать множині L , то й будь-яке число, що лежить між A_1 й A_2 , також належить цій множині. Будемо вважати, що до складу множини L обов'язково входить нуль.

Як було показано, будь-яке число із множини L можна подати в системі остаточної класів із загальною основою $M = [p_1, \dots, p_m]$, якщо $L \ll M$. Кожному числу $A \in L$, поданому у вигляді СЗК, можна поставити у відповідність деякий вектор $A \in P$, але зворотне твердження справедливе лише в тому разі, коли $M = L = P$. При виконанні цієї умови будемо казати про беззбиткове подання чисел у СЗК.

Очевидно, що якщо основи системи залишкових класів не є взаємно простими, то подання чисел у такій СЗК завжди надлишкове, оскільки $M < P$.

Для системи зі взаємно простими основами $M = P$, і тому питання про надлишкове подання чисел залежить від співвідношення між L та M . Ступенем надлишковості подання чисел у СЗК назвемо величину $R = P/L$. Надлишковість подання чисел у СЗК можна використовувати для виявлення та виправлення помилок, які виникають у процесі зберігання, передачі або перетворення інформації.

Коригувальним кодом у системі залишкових класів назвемо підмножину K множини P , що складається з L різних векторів \tilde{A} , кожному з яких відповідає одне й тільки одне число $(A) \in L$. Оскільки множини K та L містять однакоє число елементів, кожному числу $A \in P$ відповідає один і тільки один вектор $\tilde{A} \in K$. Вектори, що належать коду, будемо називати також кодovими словами.

Відповідність між векторами $\tilde{A} \in P$ й числами $A \in L$ можна встановити різними способами. Однак властивості кодів практично не залежать від вибору того чи іншого способу, а в основному визначаються лише числами L , M і P . Тому надалі будемо припускати, що числу $A = \{a_1, \dots, a_m\}$ M відповідає вектор в тому і тільки тому випадку, якщо $a_i = \tilde{a}_i$ для будь-якого $i = 1, 2, \dots, m$. Отже, $\tilde{A} = \{A\}_M$.

Залежно від співвідношення між величинами L , M і P в СЗК всі коригувальні коди можна розбити на три основні класи.

До першого класу відносяться коди, що відповідають СЗК зі взаємно простими основами. Ці коди найбільш придатні для використання у ЦОМ. Такі коди надалі будемо називати R -кодами.

Кодам другого та третього класів відповідають відношення $L = M < P$ й $L < M < P$. У обох випадках основи системи залишкових класів не є взаємно простими. Перші з цих кодів назвемо L -кодами, а другі – RL -кодами.

Нехай, наприклад, є СЗК з основами 3, 4, 5. Якщо $L = 12$, то цій СЗК відповідає R -код, у якого $M = P = 60$; $R = 5$. Системі залишкових класів з основами 3, 4, 6 відповідає L -код, у якого $L = M = 12$; $P = 72$. Врешті-решт системі з основами 3, 4, 5, 6 відповідає RL -код ($L = 12$; $M = 60$; $P = 360$).

Розглянемо тепер деякі загальні поняття для всіх коригувальних кодів у СЗК.

При оцінці ефективності будь-якого коригуючого коду необхідно знати зв'язок між надлишковістю і можливостями виявляти або виправляти помилки. Для визначення цих можливостей найчастіше використовують поняття мінімальної відстані коду, тобто найменшої відстані між двома будь-якими кодовими словами. Відстанню d між будь-якими двома векторами \tilde{A}_1 і \tilde{A}_2 з множини P назвемо число компонент, у яких ці вектори відрізняються один від одного. Безпосередньо із визначення слідує такі властивості даної відстані:

$$\left. \begin{array}{l} 1) d(\tilde{A}_1 \tilde{A}_2) = d(\tilde{A}_2 \tilde{A}_1); \\ 2) d(\tilde{A}_1 \tilde{A}_2) = 0 \text{ тоді і тільки тоді, коли } \tilde{A}_1 = \tilde{A}_2; \\ 3) d(\tilde{A}_1 \tilde{A}_2) \geq 0; \\ 4) d(\tilde{A}_1 \tilde{A}_2) \leq d(\tilde{A}_1 \tilde{A}_2) + d(\tilde{A}_2 \tilde{A}_1) \end{array} \right\} \quad (5.37)$$

Відстань, яке задовольняє наведеним властивостям, часто називають метрикою, а множину елементів, в якому задана метрика, – метричним простором.

Величина відстані між різними векторами множини P змінюється в межах від 1 до m . Цікаво зазначити, що двом сусіднім числам A_1 і A_2 (що відрізняється на одиницю) відповідають вектори \tilde{A}_1 і \tilde{A}_2 , відстань між якими дорівнює m для будь-якої системи залишкових класів.

Визначимо операції додавання, віднімання та множення векторів в просторі P так само, як визначалися формальні модульні операції над числами, поданими в СЗК. Ті вектори, яким відповідають числа, подані в СЗК, одночасно є скалярними величинами. Таким чином, операція множення вектора на скаляр не відрізняється від множення двох векторів. Кожному вектору з множини P можна присвоїти певну вагу. Вагою або ваговою функцією $W(\tilde{A})$ вектора \tilde{A} назвемо число ненульових компонент цього вектора.

Очевидно, що відстань між двома векторами дорівнює вазі їх різниці, тобто

$$d(\tilde{A}_1, \tilde{A}_2) = W(\tilde{A}_1 - \tilde{A}_2). \quad (5.38)$$

Наведемо тепер кілька корисних властивостей вагових функцій, які безпосередньо впливають із співвідношенні, що визначають метрику, і виразу (5.38):

$$W(\tilde{A}_1 + \tilde{A}_2) \leq W(\tilde{A}_1) + W(\tilde{A}_2); \quad (5.39)$$

$$W(\tilde{A}_1 + \tilde{A}_2) = W(\tilde{A}_2) + W(\tilde{A}_1); \quad (5.40)$$

$$W(\tilde{A}) = W(-\tilde{A}), \text{ де } -\tilde{A} = 0 - \tilde{A}; \quad (5.41)$$

$$W(\tilde{A}_1 + \tilde{A}_2) \leq \min(W(\tilde{A}_1), W(\tilde{A}_2)). \quad (5.42)$$

Поняття відстані й ваги, введені вище, дуже корисні при вивченні коригувальних властивостей кодів.

Припустимо, що один із символів кодового слова \tilde{A} змінив своє значення в результаті впливу будь-якої завади. Отриманий в результаті новий (спотворений) вектор \tilde{A}' знаходиться на відстані, рівній одиниці від вектора \tilde{A} . Таку помилку можна виявити лише в тому випадку, коли вектор \tilde{A}' не є кодовим словом. Тому всі кодові слова повинні бути віддалені від вектора \tilde{A}' на відстань, більшу одиниці. Чим більша відстань між кодовими словами, тим більше помилок може виявити і виправити такий код.

Надалі під одиночною помилкою будемо розуміти будь-які спотворення символу, що відповідають якому-небудь одному модулю, а t -кратною помилкою назвемо будь-які спотворення символів, що відповідають довільним t основам. Проте в деяких випадках при розгляданні L -кодів будемо використовувати поняття одиночної і t -кратної двійкових помилок, розуміючи під ними спотворення символів двійкового подання залишків a_1, \dots, a_m . Крім того, будемо вважати, що помилки носять адитивний характер і однозначно визначаються вектором $\{\Delta\}_M$, вага якого дорівнює кратності помилки. Спотворений вектор \tilde{A}' виходить в результаті суми (різниці) кодового слова й вектора помилки:

$$\tilde{A}' = \tilde{A} + \tilde{\Delta}.$$

Зв'язок між мінімальною відстанню коду, тобто найменшою відстанню між кодовими словами, і його коригуючими можливостями встановлюється наступними двома теоремами.

Теорема 5. *Коригувальний код в СЗК може виявити усі сукупності з i або меншого числа помилок лише у тому випадку, якщо мінімальна відстань коду більша l , тобто*

$$d_{\min} \geq l + 1. \quad (5.43)$$

Доведення. Нехай $\tilde{\Delta} = \tilde{A}' - \tilde{A}$ – вектор помилки з вагою, що не перевищує l . Але якщо \tilde{A}' є кодовим словом (а саме в цьому випадку ми але зможемо виявити помилки), то вага різниці $\tilde{A}' - \tilde{A}$ не може бути меншою мінімальної відстані коду, тобто повинна бути більшою, ніж l . Отже, \tilde{A}' не може бути кодовим словом і умова (5.43) є достатньою для виявлення помилок з кратністю, що не перевищує l .

Припустимо тепер що $d_{\min} \leq l$. Тоді знайдуться два таких вектора, що належать коду, різниця яких $\tilde{\Delta} = \tilde{A}' - \tilde{A}$ має вагу, рівну або меншу l . Але оскільки \tilde{A}' є кодовим словом, подібне спотворення вектора \tilde{A} не можна виявити. Отже, умова (5.43) є і необхідною. Таким чином, теорему доведено.

Теорема 6. *Коригувальний код у СЗК може виправити усі сукупності із k або меншої кількості помилок лише у тому випадку, якщо мінімальна відстань коду більша подвоєної кількості помилок, тобто*

$$d_{\min} \geq 2k + 1. \quad (5.44)$$

Доведення. Спотворення у векторі \tilde{A}' поправні лише у тому випадку, якщо кожному спотвореному вектору \tilde{A}' можна зіставити тільки одне кодове слово (і відповідно один вектор помилки). Отже, будь-яка помилка з деякої множини E може бути виправлена коригувальним кодом, якщо для будь-яких векторів $\tilde{\Delta}_1$ і $\tilde{\Delta}_2$, що належать множині E , та будь-яких двох кодових слів \tilde{A}_1 і \tilde{A}_2 справедливий вираз:

$$\tilde{A}_1 + \tilde{\Delta}_2 \neq \tilde{A}_2 + \tilde{\Delta}_1. \quad (5.45)$$

Для умови (5.44) виходить, що вага різниці будь-яких двох кодових слів не може бути меншою, ніж $2k + 1$. У той же самий час, відповідно до формули (5.39), вага різниці будь-яких двох векторів помилок, кожен з яких містить не більше k ненульових компонент, не може бути більшою $2k_0$. Тому для будь-яких кодових слів \tilde{A}_1 і \tilde{A}_2 , а також векторів помилок $\tilde{\Delta}_1$ і $\tilde{\Delta}_2$ з вагою, що не перевищує k , справедливо вираз $W(\tilde{A}_1 - \tilde{A}_2) \neq W(\tilde{\Delta}_2 \pm -\tilde{\Delta}_1)$. Звідси безпосередньо випливає справедливність нерівності (5.45).

Доведемо тепер необхідність виконання умови (5.44) для корекції k -кратних помилок. Якщо мінімальна відстань коду менша, ніж $2k + 1$, то знайдуться, принаймні, два кодових слова \tilde{A}_1 і \tilde{A}_2 , різниця яких має вагу,

що не перевищує $2k$. Відповідно завжди можна знайти два таких вектора помилок $\tilde{\Delta}_1$ і $\tilde{\Delta}_2$, що $\tilde{A}_1 - \tilde{A}_2 = \tilde{\Delta}_1 - \tilde{\Delta}_2$.

Отже, умова (5.45) не виконується і за значенням спотвореного вектора не можна однозначно отримати кодове слово, що й потрібно було довести.

З теорем 5 і 6 виходить, що коригуючий код у СЗК, виправляючий будь-які k помилок й, крім того, виявляючий будь-які $k + l$ помилок, повинен мати мінімальну відстань, рівну $2k + l$. Таким чином, визначивши мінімальну відстань коду, можна отримати уявлення про його коригуючі можливості.

Слід враховувати, що мінімальна відстань є достатньо грубою характеристикою, яка не розкриває повністю структуру й можливості коду. Зокрема, якщо відстань між більшістю кодових слів перевищує мінімальну, то такий код можна використовувати для виявлення більшої частини помилок більш високої кратності порівняно з кратностями, обумовленими теоремами 5 і 6. Тому можна вважати, що мінімальна відстань коду дозволяє встановити гарантований мінімум числа виявлених або виправлених помилок. Мінімальну відстань коду можна визначити, якщо відомі ваги кодових слів.

Теорема 7. *Мінімальна відстань коригуючого коду у системі залишкових класів дорівнює мінімальній вазі ненульових кодових слів, якщо множина L не містить чисел протилежних знаків.*

Доведення. Припустимо, що відстань між кодовими словами \tilde{A}_1 і \tilde{A}_2 є найменшою для даного коду. Оскільки числа A_1 і A_2 мають однакові знаки, повинна виконуватися нерівність $|A_1 - A_2| < L$. Тому один з векторів $\tilde{A}_1 - \tilde{A}_2$ або $\tilde{A}_2 - \tilde{A}_1$ є кодовим словом, вага якого дорівнює $d(\tilde{A}_1, \tilde{A}_2)$, тобто мінімальній відстані коду.

Припустимо тепер, що серед кодових слів знайдеться вектор \tilde{A}_3 , вага якого менша мінімальній відстані коду. Але тоді відстань між вектором \tilde{A}_3 і нульовим кодовим словом виявиться меншою мінімальній, чого, природно, бути не може. Отже, теорему доведено.

Якщо множина L містить числа різних знаків, то мінімальна відстань коду може бути меншою мінімальній ваги кодових слів. Нехай множина L містить L_1 від'ємних чисел. Додамо до кожного кодового слова вектор $\{L_1\}_M$. Отримаємо новий код з попередньою мінімальній відстанню (так як $(\tilde{A} + \tilde{L}_1) - (\tilde{A}_2 - \tilde{L}_1) = (\tilde{A}_1 - \tilde{L}_1)$), але тепер вже такий, що задовольняє умові теореми 7. Визначивши для цього коду значення мінімальній ваги, тим самим знайдемо мінімальну відстань вихідного коду.

Обмеження, що накладаються теоремою 7 на множину L , не належать до L -кодів, так як у цих кодів на відміну від двох інших

коригувальних кодів в СЗК сума, різниця і добуток будь-яких кодових слів обов'язково є кодовими словами.

Коригувальні R -коди. Як слідує з попереднього підрозділу, R -кодом називається такий коригуючий код, векторам якого відповідають числа, подані у СЗК зі взаємно простими основами. Ці коди можуть мати будь-яку мінімальну відстань залежно від ступеня надлишковості, причому, як впливає з наведеної нижче теореми, для будь-якої заданої СЗК величина R однозначно визначає коригувальні можливості коду.

Теорема 8. *Коригувальний R -код має мінімальну відстань d у тому і тільки тому випадку, якщо ступінь надлишковості R не менший добутку будь-яких $d - 1$ основ заданої СЗК:*

$$R \geq \prod_{j=1}^{d-1} p_{q_j}, \text{ де } q_j = 1, 2, \dots, m. \quad (5.46)$$

Доведення.

Поділивши число M на ліву та праву частини нерівності (5.46), отримаємо наступний вираз:

$$L = \frac{M}{R} \leq \frac{M}{\prod_{j=1}^{m-d+1} p_{q_j}} = \prod_{j=1}^{m-d+1} p_{q_j}. \quad (5.47)$$

Число A , що відповідає будь-якому кодовому слову \tilde{A} , за абсолютною величиною менше L і тому не може ділитися ні на який добуток $m - d + 1$ модулів СЗК. Якщо число A ділиться на деякий модуль p_i то відповідна компонента вектора \tilde{A} повинна дорівнювати нулю. Тому число нульових компонент вектора \tilde{A} не може бути більшим $m - d$, і, отже, вага вектора \tilde{A} не менша, ніж d . Якщо всі числа A мають однакові знаки, то з теореми 7 слідує, що d є мінімальною відстанню коду.

Припустимо тепер, що множина L містить L_1 від'ємних чисел. Розглянемо множини цілих додатних чисел B , отриманих шляхом додавання до кожного числа A величини L_1 , тобто $B = \tilde{A} + L_1$. Відповідно до наведеного вище доведенням множина векторів B утворює коригуючий код з мінімальною відстанню d . Але мінімальні відстані отриманого й вихідного кодів повинні бути рівні з побудови. Тому й у випадку різних за знаком чисел A теорема справедлива.

Доведемо тепер необхідність умови (5.46). Припустимо, що добуток деяких $d - 1$ основ СЗК більший, ніж R .

Тоді

$$L > \prod_{j=1}^{m-d+1} p_{q_j}.$$

Тому серед кодових слів знайдуться, принаймні, два вектори \tilde{A}_1 і \tilde{A}_2 , такі, що

$$\tilde{A}_1 - \tilde{A}_2 = \prod_{j=1}^{m-d+1} p_{q_j}.$$

Отже, вектор $\tilde{A}_1 - \tilde{A}_2$ містить $m - d + 1$ нульових компонент, тобто вага його дорівнює $d - 1$. Тому мінімальна відстань коду (у даному випадку відстань між векторами \tilde{A}_1 і \tilde{A}_2) менша d , що суперечить умові теореми. Отже, теорему доведено.

5.3. Основні теореми синтезу корегувальних ТСК в системі залишкових класів

Основна задача при синтезі асиметричних таймерних кодів, які виправляють та виявляють помилки, полягає в тому, що необхідно знайти залежності вагових коефіцієнтів A_k ($k = 1, \dots, i$) та модуля A_0 для виразу (5.44) від заданих властивостей коду.

Нижче доведено дві основні теореми, перша з яких дає можливість синтезувати асиметричні таймерні коди, що виявляють помилки, а друга є основною для побудови кодів з виправленням помилок.

Теорема 9. Якщо коефіцієнти порівняння (5.44) визначені так, що

$$\begin{aligned} A_k &= (e_0 + 1)^{k-1}; & k \in \{1 \dots i\} \\ A_0 &= (e_0 + 1)^i \end{aligned} \quad (5.48)$$

то помилки кратності меншої або рівної i величиною $[-e_0; e_0]$ виявляються з імовірністю 1.

Доведення. Вектор помилки $\vec{E}(e_1, e_2, \dots, e_i)$ і кодове слово $\vec{X}(x_1, x_2, \dots, x_i)$ скалярно складаються та створюють новий вектор $\widehat{X}(\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_i)$. Для цього вектора можна записати

$$\sum_{k=1}^i A_k \widehat{x}_k \equiv \sum_{k=1}^i A_k (x_k + e_k) \equiv \sum_{k=1}^i A_k e_k \pmod{A_0}, \quad (5.49)$$

де $e_k \in [-e_0; e_0]$.

Припустимо $e_k = e_0$. Тоді з урахуванням (5.48) можна записати

$$\sum_{k=1}^i A_k e_0 \equiv e_0 \sum_{k=1}^i (e_0 + 1)^{k-1} \equiv (e_0 + 1)^i - 1 \pmod{A_0}. \quad (5.50)$$

Аналогічно для $e_k = -e_0$ отримуємо

$$-\sum_{k=1}^i A_k e_0 \equiv -[(e_0 + 1)^i + 1] \equiv -A_0 + 1 \pmod{A_0}. \quad (5.51)$$

Беручи до уваги вирази (5.50) і (5.51), отримуємо $\sum_{k=1}^i |A_k e_k| < A_0$, $\forall e_k \in [-e_0; e_0]$, що й треба було довести.

Висновок 1. Код виправляє помилки кратності меншої або рівної i величиною $\left[-\left\lfloor \frac{e_0}{2} \right\rfloor, \left\lfloor \frac{e_0}{2} \right\rfloor \right]$.

Доведення. Для того щоб код виявляв помилки кратності меншої або рівної i величиною $\left[-\left\lfloor \frac{e_0}{2} \right\rfloor, \left\lfloor \frac{e_0}{2} \right\rfloor \right]$ усі синдроми C_s повинні бути різними. Методом математичної індукції покажемо, що всі $\left(2 \left\lfloor \frac{e_0}{2} \right\rfloor \right)^2$ синдроми є різними.

Не втрачаючи загальності викладок, розглянемо випадок, коли e_0 парне. Нехай $e_1 \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right]$, $e_k = 0$ ($k = 2, \dots, i$).

Тоді:

$$e_1 \leq \left| \pm \frac{e_0}{2} \right| \Rightarrow C_s \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right],$$

$$e_2 \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right], \quad e_k = 0 \quad (k = 3, \dots, i);$$

$$e_2 = \mp 1 \Rightarrow C_s \in \left[-\frac{3e_0}{2} - 1, -\frac{e_0}{2} - 1 \right] \cup \left[\frac{e_0}{2} + 1, \frac{3e_0}{2} + 1 \right]$$

.....

$$e_2 = \mp \frac{e_0}{2} \Rightarrow C_s \in \left[-\frac{e_0^2}{2} - e_0, -\frac{e_0^2}{2} \right] \cup \left[\frac{e_0^2}{2}, \frac{e_0^2}{2} + e_0 \right];$$

.....

$$e_k \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right] \quad ;$$

$$e_k = \mp 1 \Rightarrow C_s \in \left[-\frac{3(e_0 + 1)^{i-1} - 1}{2}, -\frac{(e_0 + 1)^{i-1} + 1}{2} \right] \cup \left[\frac{(e_0 + 1)^{i-1} - 1}{2}, \frac{3(e_0 + 1)^{i-1} + 1}{2} \right]$$

.....

$$e_k = \mp \frac{e_0}{2} \Rightarrow$$

$$\Rightarrow C_s \in \left[-(e_0 + 1)^i + 1, -\frac{(e_0 - 1)(e_0 + 1)^{i-1} + 1}{2} \right] \cup \left[\frac{(e_0 - 1)(e_0 + 1)^{i-1} + 1}{2}, (e_0 + 1)^i - 1 \right].$$

Отже, показано, що $C_s \in \left[-(e_0 + 1)^i, (e_0 + 1)^i - 1 \right]$ та всі e_0^i синдроми є різними. Тим самим висновок доведено.

Висновок 2. Якщо вектор помилки $\vec{E}(e_1, e_2, \dots, e_i)$ має вагу $W(\vec{E}) \leq e_0 - 1$, то код виправляє помилки величини $[-(e_0-1), (e_0-1)]$.

Доведення. Враховуючи, що $\sum_{k=1}^i e_k \leq e_0 - 1$, можна записати

$$\begin{aligned} \sum_{k=1}^i A_k e_k &\leq (e_0 + 1)^{i-1} (e_0 - 1) < A_0; \\ C_s &\in [-(e_0 + 1)^{i-1} (e_0 - 1), (e_0 + 1)^{i-1} (e_0 - 1)]; \\ \|C_s\| &= (e_0 - 1)^i - 1 < A_0. \end{aligned}$$

Отже, всі синдроми різні, а число їх менше, ніж кількість залишків A_0-1 , і код виправляє помилки величини $[-(e_0-1), (e_0+1)]$ вагою $W(\vec{E}) \leq e_0 - 1$. Висновок доведено.

Теорема 10. Якщо коефіцієнти A_k порівняння визначено таким чином, що

$$\begin{aligned} A_k &= (2e_0 + 1)^{k-1}; & k \in \{1 \dots i\} \\ A_0 &= (e_0 + 1)^i, \end{aligned} \quad (5.52)$$

то помилки, кратності меншої чи рівної i величиною $[-e_0, e_0]$, виявляються й виправляються з імовірністю 1.

Доведення. Враховуючи, що під впливом вектора помилки $\vec{E}(e_1, e_2, \dots, e_i)$ на кодове слово $\vec{X}(x_1, x_2, \dots, x_i)$ відбуваються зміщення ЗМВ, внаслідок чого на прийомі фіксується кодове слово $\widehat{X}(\widehat{x}_1, \widehat{x}_2, \dots, \widehat{x}_i)$, за умови (5.44), можна зробити висновок, що помилка буде невиявленою у випадку, якщо $\sum A_k e_k = 0 \pmod{A_0}$. Якщо ж $\sum A_k e_k \neq 0 \pmod{A_0}$, тоді, залежно від величини коефіцієнтів A_1, A_2, \dots, A_i , помилки можуть виявлятися або виправлятися. Для виправлення помилок зміщень ЗМВ потрібно, щоб кожному вектору помилки відповідав свій синдром C_s :

$$\frac{\sum A_k e_k}{A_0} = Z + C_s, \quad (5.53)$$

де Z — ціле число, C_s — остача від ділення.

Визначимо потрібне число різних остач за необхідності виправляти i -кратні помилки величиною e_0 . Можливе число зміщень кожного ЗМВ буде $2e_0 + 1$ (коефіцієнт 2 враховує можливі додатні та від'ємні зміщення ЗМВ, а 1 відповідає випадку відсутності зміщень). Таким чином, число різних синдромів, що відповідають різним виправленим помилкам, буде дорівнювати

$$N_C = (2e_0 + 1)^i. \quad (5.54)$$

Значення ж кожного синдрому визначається коефіцієнтами A_1, A_2, \dots, A_i і A_0 .

Коефіцієнт A_1 може бути будь-яким, у тому числі й рівним одиниці. У цьому випадку синдроми, що відповідають зміщенням

першого ЗМВ, займають область $+e_0$; 0 ; $-e_0$. При цьому припускається, що решта ЗМВ не змістилась за межі «своїх» зон.

Значення коефіцієнта A_2 має бути таким, щоб абсолютна величина $|A_2 e_2 - e_1|$ не відповідала синдромам зміщень першого ЗМВ. Легко показати, що для цього коефіцієнт A_2 має задовольняти умові

$$A_2 = 2e_0 + 1. \quad (5.55)$$

Отже, максимальне значення синдрому при зміщеннях першого та другого ЗМВ на величину e_0 дорівнює

$$C_{1+2} = (2e_0 + 1)e_0 + e_0 = 2e_0(e_0 + 1).$$

Виходячи з цього, значення коефіцієнта A_3 буде дорівнювати

$$A_3 = 2C_{1+2} + 1 = 4e_0(e_0 + 1) + 1. \quad (5.56)$$

Неважко помітити, що $A_3 = 2A_2^2 = (2e_0 + 1)^2$.

Розмірковуючи аналогічно, визначимо максимальне значення синдрому при зміщеннях x_1, x_2, x_3 на величину e_0 :

$$C_{1+2+3} = 4e_0^3 + 6e_0^2 + 3e_0.$$

За аналогією одержимо

$$A_4 = 8e_0^3 + 12e_0^2 + 6e_0 + 1 = (2e_0 + 1)^3. \quad (5.57)$$

Узагальнюючи наведені міркування для всіх коефіцієнтів A_k , дійдемо висновку, що в даному випадку всі коефіцієнти A_1, A_2, \dots, A_i вибираються за відповідним правилом.

На основі сказаного устанavimo взаємозв'язок між коефіцієнтами A_k та потрібною кодовою віддаллю d_x у метриці Хеммінга.

У табл. 5.4 подано значення параметрів таймерного коду з трьома ЗММ за різних величин виправлення помилок e_0 : коефіцієнти A_k та мінімальна кодова віддаль d_{\min} . Значення d_{\min} визначені виходячи із коефіцієнтів A_k у відповідності з виразами (5.45) та (5.46). Для порівняння в правій колонці табл. 5.4 подано кодові відстані d_0 , які потрібні для виправлення помилок кратності i величиною e_0 за умови, що помилки не розподілені рівномірно в межах сигнальної конструкції. В цьому випадку кратність помилки t_k та кодова віддаль d_0 будуть такими:

$$\left. \begin{aligned} t_k &= i \cdot e_0 \\ d_0 &= 2t_k + 1 = 2i \cdot e_0 + 1 \end{aligned} \right\} \quad (5.58).$$

Порівнюючи d_{\min} та d_0 , бачимо, що за умови розділу помилок рівномірно в сигнальній конструкції при одному й тому ж значенні виправленої помилки можна зменшити кодову відстань більш ніж у два рази.

Таблиця 5.4 - Параметри бінарних таймерних кодів з трьома ЗММ

e_0	A_1	A_2	A_3	d_{\min}	d_0
1	1	3	9	4	7
2	1	5	25	6	13
3	1	7	49	8	19

Для того, щоб кожному вектору помилок величиною $e \leq e_0$ кратності i відповідав єдиний синдром помилки, достатньо, щоб виконувалась умова:

$$A_0 = 2 \sum_{k=1}^i A_k . \quad (5.59)$$

Аналіз наведених міркувань може привести до запитання про доцільність використання таймерних кодів, які виправляють помилки зсувів замість кодів, що виявляють ці зміщення при більшому значенні Δ . Для відповіді на це запитання розглянемо табл. 5.5, в якій наведено значення числа реалізацій сигнальних конструкцій на різних інтервалах часу для таких кодів:

1. Число сигнальних конструкцій, які реалізовані на інтервалі $T = m\tau_0$ при $s = 3$ та відповідають умові (5.44) при $d = 3$, $A_1 = 1$, $A_2 = 2$, $A_3 = 3$, $A_0 = 7$.

2. Число реалізацій сигнальних конструкцій на інтервалі $T = m\tau_0$ при $s = 9$, відповідності умові (5.44) та виправленні помилок кратності $i = 3$ величиною $e_0 = 1$. При цьому питання про розподіл помилок у межах сигнальної конструкції не обговорюється. Для даного коду $d = 7$, $A_1 = 1$, $A_2 = 6$, $A_3 = 21$, $A_0 = 73$.

3. Число реалізацій сигнальних конструкцій на інтервалі $T = m\tau_0$ при $s = 9$, відповідно до умові (5.44) та виправлення помилок кратності $i = 3$ величини $e_0 = 1$ за умови їх рівномірного розподілу. Для даного коду $d = 4$, $A_1 = 1$, $A_2 = 3$, $A_3 = 9$, $A_0 = 27$.

4. Число реалізацій сигнальних конструкцій на інтервалі $T = m\tau_0$ при $s = 15$, відповідно до умови (5.44) та виправлення помилок кратності $i = 3$ величини $e_0 = 2$ за відсутності обмежень на розподіл помилок. Для даного коду $d = 13$, $A_1 = 1$, $A_2 = 12$, $A_3 = 78$, $A_0 = 487$.

5. Число реалізацій сигнальних конструкцій на інтервалі $T = m\tau_0$ при $s = 15$, відповідно до умови (5.44) та виправлення помилок кратності $i = 3$ величини $e_0 = 2$ за умови їх рівномірного розподілу. Для даного коду $d = 6$, $A_1 = 1$, $A_2 = 5$, $A_3 = 25$, $A_0 = 63$.

Таблиця 5.5 - Число реалізацій сигнальних конструкцій надлишкових таймерних кодів

№ коду	m							
	3	4	5	6	7	8	9	10
1	1	2	12	31	65	117	190	290
2	0	4	20	57	129	223	397	613
3	0	11	58	167	367	684	1144	1776
4	0	2	10	32	82	155	270	419
5	0	11	85	276	631	1207	2060	3241

Значення s для окремих кодів взято з умови, що виправлення спотворень величиною $e_0 = 1$ відповідає збільшенню еквівалентної зони в

три рази, а виправлення спотворень $e_0 = 2$ відповідає збільшенню зони в п'ять разів. Таким чином, еквівалентні зони для усіх п'яти кодів.

З аналізу наведених даних випливає, що виправлення помилок величиною $e_0 = \pm 1$ за відсутності обмеження на розподіл помилок (код №2) збільшує потужність множини до двох разів, а за рівномірного розподілу помилок (код №3) до п'яти разів. Уводити виправлення i -кратних помилок величиною $e_0 = 2$ при нерівномірному їх розподілі у межах сигнальної конструкції недоцільно, тому що потужність множини дозволених сигналів зменшується (код №4). В той самий час за рівномірного розподілу помилок у межах сигнальної конструкції потужність множини на заданому інтервалі суттєво збільшується (код №5).

Висновок 1. Якщо вектор помилки $\vec{E}(e_1, e_2, \dots, e_i)$ має вагу $W(\vec{E}) \leq 2e_0$, то код виявляє помилки величиною $[-2e_0, 2e_0]$.

Доведення. Припустимо, що $e_1 = e_2 = \dots = e_{i-1} = 0$, а $e_i = 2e_0$. Тоді можна записати: $\sum_{k=1}^i A_k e_k = A_i e_i = 2e_0 (2e_0 + 1)^{i-1}$. Очевидно, що $\forall e_0 > 0$

$$2e_0 (2e_0 + 1)^{i-1} < \frac{1}{2} \left((2e_0 + 1)^i + 1 \right) \quad (5.60)$$

і при $A_i \geq \sum_{k=1}^{i-1} A_k$ нерівність (5.60) виконується в усій решті випадків. Тим самим висновок доведено.

Висновок 2. Синдром помилки C_s кратності меншої або рівної i величиною $[-e_0, e_0]$ визначається як

$$C_s = R_{A_0} \left(\sum_{k=1}^i A_k \hat{x}_k \right), \quad (5.61)$$

де \hat{x} – прийняті значущі моменти.

Доведення. Розглянемо три випадки:

а) $\vec{E} \rightarrow \vec{E}(0, \dots, e_j, 0, e_{j+2}, \dots, 0)$; б) $e_k = e_0, k \in [1, i]$; в) $e_k = -e_0, k \in [1, i]$.

$$\begin{aligned} \text{а) } C_s &= \sum_{k=1}^i A_k x_k + A_j e_j + A_{j+2} e_{j+2} - A_0 \left\lfloor \frac{1}{A_0} \left(\sum_{k=1}^i A_k x_k + A_j e_j + A_{j+2} e_{j+2} \right) \right\rfloor = \\ &= pA_0 + A_j e_j + A_{j+2} e_{j+2} - A_0 \left\lfloor \frac{1}{A_0} (A_0 p + A_j e_j + A_{j+2} e_{j+2}) \right\rfloor = A_j e_j + A_{j+2} e_{j+2}, \end{aligned}$$

де p – ціле число;

$$\text{б) } C_s = pA_0 + (A_0 - 1) - \left\lfloor \frac{1}{A_0} (pA_0 - 1) \right\rfloor A_0 = A_0 - 1;$$

$$\text{в) } C = pA_0 - (A_0 - 1) - \left\lfloor \frac{1}{A_0} (pA_0 - (A_0 - 1)) \right\rfloor A_0 = -(A_0 - 1).$$

Отже, $C_s \in [-A_0, A_0]$, $C_s = 0$ лише тоді, коли $e_k = 0$, $k \in [1, i]$. Якщо для $\vec{e} \cdot C_s = C_{s0}$, то для $-\vec{e} \cdot C_s = -C_{s0}$.

Висновок 3. Синдром помилки C_s дає змогу знайти вектор помилки $\vec{E}(e_1, e_2, \dots, e_i)$, при цьому

$$e_k = e_0 - R_{(2e_0+1)} \left(\left\lfloor \frac{C_s + A_0 - 1}{(2e_0 + 1)^{i-k}} \right\rfloor \right). \quad (5.62)$$

Доведення. Покажемо, що формула (5.62) являє собою короткий запис методу перетворення чисел з однієї системи числення в іншу, а саме: з десяткової в e -ту систему. Позначимо $C = C + A_0 - 1$, $C_i = 0,2(A_0 - 1)$ і $e_k = e_k + e_0$,

$$\begin{array}{r} C_i \quad \lfloor 2e_0+1 \\ e_i' \quad C_{i-1} \quad \lfloor 2e_0+1 \\ \quad e_{i-1}' \quad C_{i-2} \\ \quad \quad \quad \vdots \\ \quad \quad \quad C_3 \quad \lfloor 2e_0+1 \\ \quad \quad \quad e_3 \quad C_2 \quad \lfloor 2e_0+1 \\ \quad \quad \quad \quad e_2' \quad C_1 = e_1'. \end{array}$$

$e_k = (0, 2e_0)$. Послідовність перетворення має такий вигляд:

Перетворення показує, що

$$C_{i-1} = \left\lfloor \frac{C_i}{2e_0 + 1} \right\rfloor, \quad e_i' = R_{(2e_0+1)}(C_i);$$

$$C_{i-2} = \left\lfloor \frac{C_{i-1}}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^2} \right\rfloor, \quad e_{i-1}' = R_{(2e_0+1)} \left(\frac{C_i}{2e_0 + 1} \right);$$

.....

$$C_2 = \left\lfloor \frac{C_3}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^{i-1}} \right\rfloor, \quad e_2' = R_{(2e_0+1)} \left(\frac{C_i}{(2e_0 + 1)^{i-2}} \right);$$

$$C_1 = \left\lfloor \frac{C_1}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^i} \right\rfloor, \quad e_1' = R_{(2e_0+1)} \left(\frac{C_i}{(2e_0 + 1)^{i-1}} \right)$$

або

$$C_{k-1} = \left\lfloor \frac{C_i}{(2e_0 + 1)^{i-k+1}} \right\rfloor, \quad e_k' = R_{(2e_0+1)} \left(\frac{C_i}{(2e_0 + 1)^{i-k}} \right),$$

де $k \in [1, i]$, $C_0 = 0$.

Оскільки $\hat{e}_k = e_0 - e_k'$, то висновок доведено.

Пояснимо викладений метод синтезу надлишкових таймерних сигнальних конструкцій на прикладі. Розглянемо надлишковий таймерний

код з параметрами: $i = 3$, $n = 24$, $s = 3$, $e_0 = 3$ та вектор помилки $\vec{E}(-1, 2, -3)$. З формули знаходимо

$$x_1 + 7x_2 + 49x_3 \equiv 0 \pmod{172}. \quad (5.63)$$

Розв'язаннями (5.63) можуть бути кодові слова $\vec{X}_1(3, 7, 20)$, $\vec{X}_2(7, 17, 22)$ тощо. При передаванні вектора \vec{X}_1 на прийомі під впливом завади буде зареєстровано кодове слово $\hat{\vec{X}}_1(2, 9, 17)$. За формулами (5.61) та (5.62) знаходимо

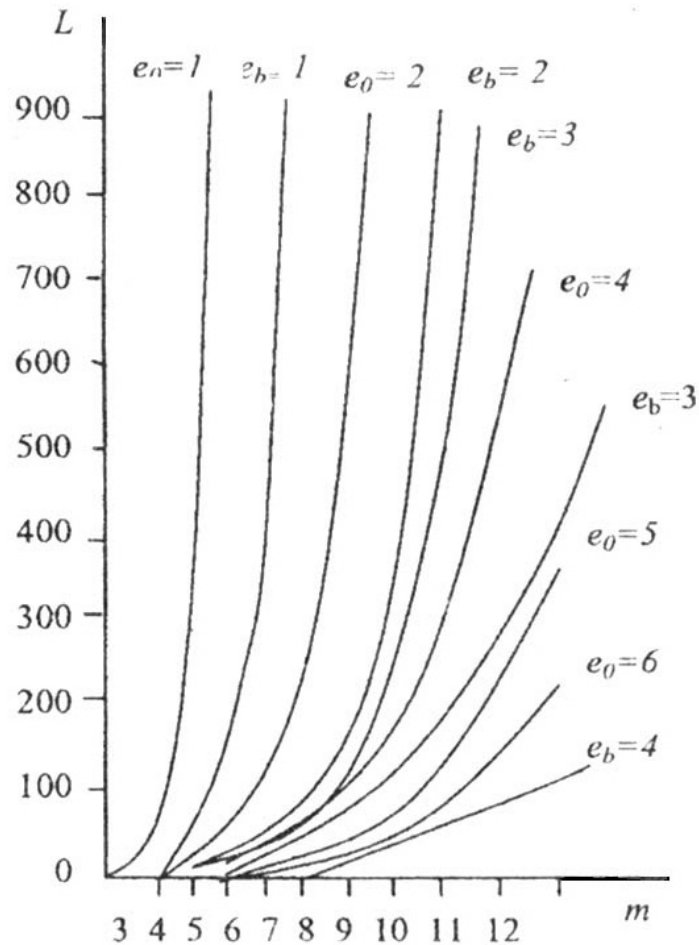


Рисунок 5.1 - Залежності потужності множини таймерного коду від тривалості кодового слова при $s = 10$, $i = 3$

$$C = 38, \quad \hat{e}_1 = 3 - R_7 \left(\left\lfloor \frac{209}{49} \right\rfloor \right) = -1, \quad \hat{e}_2 = 2, \quad \hat{e}_3 = -3.$$

Тоді $\hat{\vec{E}}(-1, 2, -3)$, $\hat{\vec{X}}_1' = \hat{\vec{X}}_1 - \hat{\vec{E}} = (3, 7, 20)$ та $\hat{\vec{X}}_1' = \vec{X}_1$.

Для запропонованих в цьому підрозділі кодів було розраховано залежності потужності множини сигнальних конструкцій від тривалості кодових комбінацій, кількості значущих моментів та коригувальних

властивостей коду. Для прикладу на рис. 5.1 наведено залежності $L = f(m, e)$ для $s = 10, i = 3$.

Прискорений метод формування кодової таблиці надлишкових таймерних кодів. Одним із методів складання кодової таблиці для надлишкових таймерних кодів є метод перебирання. Розглянемо метод, який дає можливість прискорити процес відшукування кодових слів, які задовольняють умові.

Нехай задано таймерний код з $i = 3$:

$$A_1x_1 + A_2x_2 + A_3x_3 = 0 \pmod{A_0}. \quad (5.64)$$

Очевидно, що координати x_k ($k \in \{1, 2, 3\}$) повинні задовольняти умові

$$s + x_{k-1} \leq x_k \leq n - (3 - k)s, \quad k \in \{1, 2, 3\}, \quad (x_0 = 0). \quad (5.65)$$

З урахуванням (5.64) рівняння (5.65) можна звести до такого вигляду:

$$B_1y_1 + B_2y_2 + B_3y_3 + B_0 = 0 \pmod{A_0}, \quad (5.66)$$

де $B_1 = \sum_{k=1}^3 A_k$, $B_2 = \sum_{k=2}^3 A_k$, $B_3 = A_3$, та $0 \leq y_1 \leq n - 3s$, $0 \leq y_2 \leq n - 3s - y_1$,
 $0 \leq y_3 \leq n - 3s - y_1 - y_2$.

Покладемо $y_1 = y_1^0$, $y_2 = y_2^0$, тоді вираз (5.66) набуде вигляду:

$$B_1y_1^0 + B_2y_2^0 + B_3y_3 + B_0 = 0 \pmod{A_0} \quad (5.67)$$

або
$$y_3 = \frac{B_p}{B_3} \pmod{A_0},$$

де $B_p = A_0 - R_{A_0}(B_0 + B_1y_1^0 + B_2y_2^0)$, та $R_x(y)$ - остача від ділення y на x .

Нерівність (5.67) буде мати розв'язок тільки в тому випадку, коли $n = 3s(y_1^0 + y_2^0) \geq \frac{B_p}{B_3}$. Тоді відповідне кодове слово (x_1^0, x_2^0, x_3^0) можна

знайти за такими формулами: $x_1^0 = y_1^0 + s$, $x_2^0 = y_2^0 + s + x_1^0$, $x_3^0 = B_p + x_2^0 + s$ та, варіюючи y_1 та y_2 у зазначених межах, знаходимо всі кодові слова. Принцип методу прискореного перебирання розглянемо на прикладі

Приклад 5. $A_0 = 47, A_1 = 4, A_2 = 11, A_3 = 1, n = 39$ та $s = 6$. Згідно з формулою (5.66), одержимо: $B_1=16, B_2=12, B_3=1, B_0=174$ та $0 \leq y_1 \leq 21$, $0 \leq y_2 \leq 21 - y_1$, $0 \leq y_3 \leq 21 - y_1 - y_2$.

Покладемо $y_1=0, y_2=0$, тоді $B_p=14$ і рівняння $y_3 = \frac{B_p}{B_3} \pmod{A_0}$ перетворюється в $y_3 = 14 \pmod{47}$. Це рівняння має розв'язок, оскільки $0 \leq y_3 \leq 21$. Отже, $x_1^0 = 6, x_2^0 = 12, x_3^0 = 32$.

Далі покладемо $y_1=0, y_2=1$, та аналогічним чином складемо рівняння $y_3 = \frac{B_p}{B_3} \pmod{A_0}$, $y_3 = 2 \pmod{47}$ і знаходимо $x_1^1 = 6$, $x_2^1 = 13$, $x_3^1 = 21$; при $y_1=0, y_2=2$ маємо $y_3 = 37 \pmod{47}$. Враховуючи, що при $0 \leq y_3 \leq 19$, розв'язку немає. Процедура закінчиться, коли y_1 та y_2 набудуть усіх значень $0 \leq y_1 \leq 21$ та $0 \leq y_2 \leq 21 - y_1$.

Визначимо кількість необхідних циклів для складення кодової таблиці таймерного коду методом прискореного перебирання, загальну кількість циклів G одержимо із системи обмежень

$$\left. \begin{array}{l} 0 \leq y_1 \leq n - 3s \\ 0 \leq y_2 \leq n - 3s - y_1 \end{array} \right\}.$$

Бачимо, що для кожного y_1 змінна y_2 набуває ряд значень, при цьому ряд має від одного до $n - 3s + 1$ членів, тому загальне число їх дорівнює

$$C = \sum_{k_2=1}^{n-3s+1} k_2 = \frac{1}{2}(n-3s+1)(n-3s+2).$$

Для оцінки ефективності цього методу, порівняно з простим методом перебирання, так само обчислимо число циклів C , які потрібні для отримання такого самого алфавіту простим методом. З урахуванням умови (5.65) одержимо

$$C' = \sum_{k_1=0}^{n-3s} \sum_{k_2=1}^{n-3s+1-k_1} k_2 = \frac{1}{2}(n-3s+1)(n-3s+2) + \frac{1}{2} \sum_{k_1=1}^{n-3s} (n-3s+1-k_1)(n-3s+2-k_1).$$

Отже, запропонований метод прискореного перебирання зменшує число циклів на $\frac{1}{2} \sum_{k_1=1}^{n-3s} (n-3s+1-k_1)(n-3s+2-k_1)$.

Узагальнимо отримані результати при довільному $i \geq 2$. Рівняння $\sum_{k=1}^i A_k x_k = 0 \pmod{A_0}$ та обмеження $s + x_{k-1} \leq x_k \leq n - (i-k)s$ ($x_0 = 0$) перетворюються у наступну умову:

$$\sum_{k=1}^i B_k y_k + B_0 = 0 \pmod{A_0}, \quad (5.68)$$

де $B_k = \sum_{j=k}^i A_j$; $B_0 = s \sum_{k=1}^i k A_k$; $0 \leq y_k \leq n - is - \sum_{j=1}^{k-1} y_j$; $y_0 = 0$.

Поклавши $y_1 = y_1^0, \dots, y_{i-1} = y_{i-1}^0$, рівність (5.68) зведемо до вигляду

$$y_i = \frac{B_p}{B_i} \pmod{A_0}, \quad (5.69)$$

де $B_p = A_0 - R_{A_0} \left(B_0 + \sum_{k=1}^{i-1} B_k y_k^0 \right)$, i , має розв'язання лише тоді, коли

$$n - is - \sum_{k=1}^{i-1} y_k^0 \geq \frac{B_p}{B_i}, \text{ кодове слово визначається як } x_k^j = y_k^j + s + x_{k-1}^j,$$

$$k \in \{1, \dots, i-1\}, j \in \{1, \dots, i-1\}, x_0^j = 0 \text{ та } x_i^j = B_p + x_{i-1}^j + s.$$

$$\text{Число циклів дорівнює } C = \sum_{k_1=1}^{n-is-1} \sum_{k_2=1}^{n-is+1-k_1} \dots \sum_{k_{i-2}=1}^{n-is+1-k_{i-3}} k_{i-2}.$$

$$\text{Аналогічним чином для простого методу: } C' = \sum_{k_1=1}^{n-is} \sum_{k_2=1}^{n-is+1} \dots \sum_{k_{i-2}=1}^{n-is+1-k_{i-3}} k_{i-2}.$$

Таким чином, число циклів зменшується на

$$C' - C = \sum_{k_0=1}^{n-is} \sum_{k_1=1}^{n-is+1} \dots \sum_{k_{i-2}=1}^{n-is+1-k_{i-3}} k_{i-2}.$$

Отже, ефективність запропонованого методу збільшується при збільшенні числа значущих моментів в ТСК.

Синтез ТСК на базі лінійних розрядно-цифрових кодів. Відомо, що трудомісткість оптимального кодування джерела може бути значно зменшена, якщо існує спосіб простої нумерації повідомлення із заданими властивостями. Викладено метод кодування двійкових незалежних джерел, трудомісткість якого пропорційна l^3 , де l – довжина повідомлення. Суть методу полягає в простій нумерації блоків з l двійкових символів із заданим числом одиниць.

Аналогічним чином задача кодера таймерного коду зводиться до подання кодової комбінації набором i чисел (x_1, \dots, x_i) , які є координатами вектора \vec{X} .

Визначимо умови, яким повинні задовольняти координатами вектора \vec{X} , як систему обмежень Q_3 з початковими умовами $y_0 = 0, x_0 = 0$:

$$0 \leq y_k \leq n - is - \sum_{j=1}^{k-1} y_j; \quad x_k = y_k + x_{k-1+s}, \quad k \in \{1, \dots, i\}.$$

Позначимо алфавіт джерела інформації через V , його елементи – як числа v , тобто $V = v \{v | v \in Z^+\}$. Тоді кодер таймерного коду повинен однозначно здійснювати відображення множини V у множину $L_y = \{ \vec{Y} | \vec{Y} : Q_1 \wedge \vec{Y} : Q_3 \}$ й кодування задається схемою

$$\left. \begin{array}{l} v_1 \rightarrow \vec{Y}_1 \\ v_2 \rightarrow \vec{Y}_2 \\ \vdots \\ v_l \rightarrow \vec{Y}_l \end{array} \right\}.$$

Одне з розв'язань цієї задачі сформулюємо у наступній лемі.

Теорема 11. Якщо елементи y_k ($k \in \{1, \dots, i\}$) задовольняють нерівність

$$\frac{1}{(k-1)!} \sum_{r=0}^{y_k} \prod_{t=0}^{k-2} (n - is - z_k r + t + 1) + \\ + \sum_{\mu=k+1}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{y_\mu} \prod_{t=0}^{\mu-2} \left(n - is - \sum_{j=\mu}^i z_j y_j - z_{\mu r} + t + 1 \right) - v \leq 0,$$

то має місце перетворення

$$v \rightarrow (z_1 y_1, \dots, z_i y_i) \text{ та } \sum_{j=1}^i z_j y_j \leq n - is - 1.$$

Для зворотного перетворення $(y_1, \dots, y_i) \rightarrow v$ або декодування таймерного коду сформулюємо теорему 12.

Теорема 12. Елемент $v \in V$ однозначно відновлюється за елементами (y_1, \dots, y_i) :

$$v = \sum_{\mu=1}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{y_\mu} \prod_{t=0}^{\mu-1} \left(n - is - \sum_{j=\mu}^i z_j y_j - r + t + 1 \right).$$

Таймерні коди, побудовані на основі лінійних кодів мають такі переваги:

- оптимальність розміщення комбінацій в i -вимірному просторі;
- припустимість впровадження виявлення чи виправлення за кожним ЗМВ;
- можливість поелементного оброблення кодової комбінації, не виключаючи оброблення в цілому;
- наявність систематичного правила кодування й декодування;
- фізична реалізованість.

Узагальнимо результати синтезу симетричних таймерних кодів з постійним числом значущих моментів, що ґрунтується на лінійних кодах.

Одним з недоліків вищевикладених методів побудови таймерних кодів є відсутність узгодженості з параметром s чи d . Саме тому асиметричні коди нещільно розміщені у просторі. Для симетричних кодів відсутність узгодженості призводить до того, що в деяких випадках $\|L\|_{s=s_1} \leq \|L\|_{s=s_2}$ при $s_1 > s_2$. Викладемо метод найщільнішого „пакування” таймерних конструкцій, який дозволяє усунути вказаний недолік і повністю узгодити всю сукупність параметрів таймерних кодів.

Нехай: $L = \{ \vec{X} | \vec{X} : Q_1 \wedge \vec{X} \wedge Q_2 \}; Q_1 : x_i > x_{i-1} > x_1;$
 $Q_2 : d_{\min} \geq |dist(\vec{X}_1, \vec{X}_2)|$ і $\vec{X} = (x_1, \dots, x_i).$

Тоді: $L' = \{ \vec{X} | \vec{X} : Q_1 \wedge \vec{X} : Q_2 \wedge \vec{X} : Q_3 \},$
 $Q_3 : x_j = x_{j-1} + s + kd_j,$

де $x_0 = 0$, $k = 0, \dots, \left\lfloor \frac{n - is}{d} \right\rfloor$, $j \in \{1, \dots, i\}$ є оптимальним таймерним кодом в розумінні щільного пакування, виявляє помилки кратності i величиною $\lfloor d_j - 1 \rfloor$ та виправляє помилки кратності i величиною $\left\lfloor \frac{d_j - 1}{2} \right\rfloor$.

Розглянемо принцип побудови оптимального таймерного коду в розумінні щільного пакування на прикладі.

Дано: $n = 30$, $s = 2$, $I = 3$, $d_1 = d_2 = d_3 = 3$. Визначимо кодові слова за умовою $Q_3 : k \in [0, 8]$; $j = [1, 3]$:

$\vec{X}_1 :$	2	4	6	:	:	:	:
$\vec{X}_2 :$	2	4	9	:	:	:	:
$\vec{X}_3 :$	2	4	12	$\vec{X}_{17} :$	2	7	30
:	:	:	:	:	:	:	:
$\vec{X}_9 :$	2	4	30	$\vec{X}_{45} :$	2	26	30
$\vec{X}_{10} :$	2	7	9	$\vec{X}_{46} :$	5	7	9
:	:	:	:	:	:	:	: і т.д.

Принцип виявлення помилок. Нехай $\widehat{X}(\widehat{x}_1, \dots, \widehat{x}_i)$ – прийняте кодове слово, тоді при $c_j = 0$ помилка буде невиявленою, а при $c_j \neq 0$ помилку буде виявлено. Тоді

$$c_j = Rd_j(\widehat{x}_j - js). \quad (5.70)$$

Принцип виправлення помилок. Для прийнятого кодового слова $\widehat{X}(\widehat{x}_1, \dots, \widehat{x}_i)$ маємо

$$\left. \begin{aligned} x_j &= \widehat{x}_j - c_j, & 0 \leq c_j \leq \frac{d_j}{2} \\ x_j &= \widehat{x}_j - c_j + d_j, & \frac{d_j}{2} \leq c_j \leq d_j \end{aligned} \right\}. \quad (5.71)$$

Отже, таймерний код з щільним пакуванням задається умовою Q_1 , Q_2 , Q_3 , а метод виявлення та виправлення помилок – рівняннями (5.70), (5.71).

Подамо інформацію, яка підлягає кодуванню, у вигляді десяткового числа $N(x)$, а процес кодування – як перетворення $N(x) \rightarrow (x_1, \dots, x_i)$. Тоді на підставі одержаних результатів сформулюємо наступні леми.

Теорема 13. Перетворенню $N(x) \rightarrow (x_1, \dots, x_i)$ відповідає схема $x_j = x'_j d + js$, $j \in \{1, \dots, i\}$, де x'_j визначається з нерівності

$$\sum_{r=1}^{i-k} \sum_{l=0}^{j+1-r} \left(\left\lfloor \frac{n-is}{d} + 1 \right\rfloor + i + 1 - \sum_{t=1}^{i-k+1} x'_{i-t+1} - l \right)_{i-r+1} + \sum_{l=0}^{x'_k} \left(\left\lfloor \frac{n-is}{d} + 1 \right\rfloor + i - 1 - \sum_{t=0}^{i-k+1} x'_{i-t} - l \right)_k \leq N(x)$$

де $k = 1, \dots, i$.

Теорема 14. Зворотнє перетворення $(x_1, \dots, x_i) \rightarrow N(x)$ задається так:

$$N(x) = \sum_{k=1}^i \sum_{l=1}^{x'_k} \left(\left\lfloor \frac{n-is}{d} + 1 \right\rfloor + i - 1 - \sum_{r=1}^{k-1} x'_r - l \right)_k,$$

де $x'_j = \frac{(x_j - js)}{d}$, $j = 1, \dots, i$.

Останні теореми не потребують окремого доведення, оскільки аналогічні теореми були доведені раніше.

Визначення нижньої межі потужності для симетричних таймерних кодів є еквівалентним до давно відомої в дискретній геометрії задачі з найщільнішим розміщенням однакових куль об'ємом V_d в i -вимірному просторі об'ємом V_i , причому центри куль відповідають сигнальним точкам, а відстань між будь-якою парою точок не менша, ніж задане значення величини d . Тоді нижня межа являє собою коефіцієнт заповнення простору

$$\rho = \|L\| = \frac{V_i}{V_d}.$$

З обмежень $s + x_{k-1} \leq x_k \leq n - (3 - k)s$, $k \in \{1, 2, 3\}$ ($x_0 = 0$) одержимо

$$V_i = \int_s^{n-(i-1)s} \int_{s+x_1}^{n-(i-2)s} \dots \int_{s+x_{i-1}}^n dx_i dx_{i-1} \dots dx_1.$$

Для $i = 2$:

$$V_2 = \int_s^{n-s} \int_{s+x_1}^n dx_1 dx_2 = \frac{1}{2}(n-2s)^2,$$

для $i = 3$:

$$V_3 = \int_s^{n-2s} \int_{s+x_1}^{n-s} \int_{s+x_2}^n dx_3 dx_2 dx_1 = \frac{1}{6}(n-3s)^3,$$

аналогічно для $I = k$:

$$V_k = \int_s^{n-(k-1)s} \int_{s+x_1}^{n-(k-2)s} \dots \int_{s+x_{k-1}}^n dx_k \dots dx_2 dx_1 = \frac{1}{k!}(n-ks)^k.$$

Відомо, що об'єм i -вимірної кулі радіусом d дорівнює

$$V_d = \frac{\pi^{1/2}}{\Gamma\left(\frac{i}{2} + 1\right)} d^i,$$

де $\Gamma(x)$ – гамма-функція. Отже, в загальному вигляді отримаємо

$$\|L\| \geq \frac{(n - is)^i \Gamma\left(\frac{i}{2} + 1\right)}{i! \pi^{i/2} \cdot d^i}.$$

Враховуючи значення гамма-функції для парних і непарних i , одержимо вираз для потужності $\|L\|$:

$$L = \binom{\left\lfloor \frac{n - is}{d} + 1 \right\rfloor + i - 1}{i},$$

де $d = \min(d_j)$, $j \in [1, i]$.

На рис 5.2. подано графіки залежностей $L = f(s, d)$ для коду з $i = 3$, з яких видно, що залежності являють собою монотонну зростаючу функцію, тобто усунено недолік попереднього коду. На рис. 5.3 подано графіки залежностей потужності від довжини коду $L = f(m, d)$ для випадку $i = 3$, $s = 10$.

Отримані результати свідчать, що потужність $\|L\|$ даних кодів перевищує потужність асиметричних таймерних кодів за одних і тих самих вихідних умов. Розглянемо два випадки:

а) i – парне, тоді $\Gamma\left(\frac{i}{2} + 1\right) = \left(\frac{i}{2}\right)!$, і можна записати

$$\|L\| \geq \frac{(n - is)^i \left(\frac{i}{2}\right)!}{i! \pi^{i/2} d^i}; \quad (5.72)$$

б) i – непарне, тоді $\Gamma\left(\frac{i}{2} + 1\right) = i! \sqrt{\frac{\pi}{2}} 2^{i+1}$, і можна записати

$$\|L\| \geq \frac{(n - is)^i i! \sqrt{\pi}}{i! \pi^{i/2} d^i \sqrt{2}^{i+1}} = \frac{(n - is)^i}{d^i \pi^{(i-1)/2} 2^{(i+3)/2} \left(\frac{i-1}{2}\right)!}. \quad (5.73)$$

Розрахунки за формулами (5.72) та (5.73) свідчать, що запропонована межа є прийнятною для оцінки ефективності.

В додатку проведено оцінку ефективності використання нерівномірних сигнальних конструкцій ТСК.

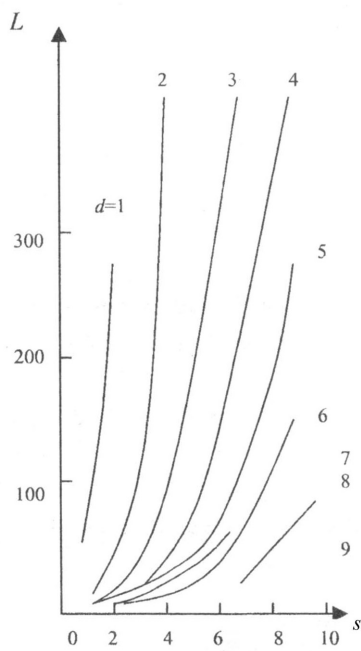


Рисунок 5.2 - Залежності потужності оптимального таймерного коду з $i = 3$ від параметрів s і d

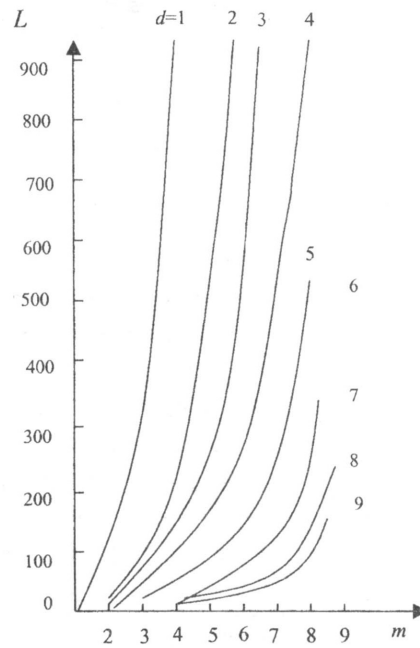


Рисунок 5.3 - Залежності потужності оптимального таймерного коду з $i = 3, s = 10$ від параметрів m і d

5.4. Зв'язок коефіцієнтів рівняння якості $\sum_{i=1}^n A_i x_i = 0 \pmod{A_0}$ з кодовою відстанню

Запишемо рівняння

$$A_1 x_1 + A_2 x_2 + \dots + A_{n-1} x_{n-1} + A_n x_n = \sum_{i=1}^n A_i x_i = 0 \pmod{A_0}. \quad (5.74)$$

Права частина рівняння являє добуток векторів

$$A\bar{X} = 0 \pmod{A_0},$$

при цьому координати векторів $\bar{A}(A_1, A_2, \dots, A_n)$, $\bar{X}(x_1, x_2, \dots, x_n)$ – цілі числа. Можна сформулювати теорему.

Теорема 15. Якщо координати і модуль порівняння A_0 визначені за формулами

$$\left. \begin{aligned} A_n &= 1; \\ A_{n-1} &= d - 1; \\ A_{n-k} &= E^{-\left(\frac{d-1}{2}\right)} A_{n-k+1} + E^{-\left(\frac{d}{2}\right)}, k = 1, 2, \dots, n; \\ A_0 &= E^{-\left(\frac{d+1}{2}\right)} A_1 + E^{-\left(\frac{d}{2}\right)}, \end{aligned} \right\} \quad (5.75)$$

то будь-який вектор \bar{X} , що задовольняє умові $A\bar{X} = 0 \pmod{A_0}$, має вагу $W(X) \geq d$. Відзначимо, що формули (5.75) за парного та непарного d мають вигляд:

$$\left. \begin{aligned} A_n &= 1, \\ A_{n-1} &= d-1, \\ A_{n-k} &= A_{n-k+1} \left(\frac{d}{2} - 1 \right) + \frac{d}{2}, \\ A_0 &= A_1 \frac{d}{2} + \frac{d}{2}, \end{aligned} \right\}, d - \text{парне} \quad (5.76)$$

$$\left. \begin{aligned} A_n &= 1, \\ A_{n-1} &= d-1, \\ A_{n-k} &= A_{n-k+1} \left(\frac{d-1}{2} \right) + \frac{d-1}{2}, \\ A_0 &= A_1 \frac{d+1}{2} + \frac{d-1}{2}, \end{aligned} \right\}, d - \text{непарне} \quad (5.77)$$

При доведенні будемо розглядати координати векторів: $A(A_0, A_1, \dots, A_n)$ і $\bar{X}(x_1, x_2, \dots, x_n)$ як цілі числа. Беручи до уваги формули (5.76) легко перевірити, що за непарного d вектори

$$\left. \begin{aligned} \bar{Y}_1 & \left(1, \frac{d-1}{2}, 0, 0, 0, \dots, \frac{d-1}{2} \right); \\ \bar{Y}_2 & \left(0, -1, \frac{d-1}{2}, 0, 0, \dots, \frac{d-1}{2} \right); \\ \bar{Y}_{n-2} & \left(0, \dots, 0, -1, \frac{d-1}{2}, 0, \frac{d-1}{2} \right); \\ \bar{Y}_{n-1} & \left(0, \dots, 0, 0, -1, \frac{d-1}{2}, \frac{d-1}{2} \right); \\ \bar{Y}_n & \left(0, \dots, 0, 0, 0, -1, \frac{d-1}{2} \right) \end{aligned} \right\} \quad (5.78)$$

ортогональні \bar{A} . Ранг матриці, який складений з координат цих векторів, дорівнює n і визначник не дорівнює нулю. Отже, вектори Y_i являють собою базис для дозволених векторів \bar{X} . Тому будь-який вектор \bar{X} можна розкласти за базисом у вигляді

$$\bar{X} = \sum_{k=1}^n \alpha_k \bar{Y}_k,$$

звідки випливає, що

$$\left. \begin{aligned} P &= -\alpha; \\ x_1 &= -\alpha_2 + \alpha_1 \frac{d+1}{2}; \\ x_3 &= -\alpha_3 + \alpha_2 \frac{d-1}{2}; \\ x_{n-1} &= -\alpha + \alpha_{n-1} \frac{d-1}{2}; \\ x_n &= \frac{d-1}{2} \sum_{k=1}^n \alpha_k + \frac{d-1}{2} \alpha_n + \alpha_1. \end{aligned} \right\}$$

З останніх співвідношень випливає, що координати \bar{X} будуть цілими числами тоді і тільки тоді, коли $\alpha_k, k=1, \dots, n$ — цілі.

Для парних значень d базисом будуть вектори \bar{Y}' :

$$\left. \begin{aligned} \bar{Y}_1 & \quad \left(-1, \quad \frac{d}{2}, \quad 0, \quad 0, \quad \dots, \quad 0, \quad \frac{d}{2}\right); \\ \bar{Y}_2 & \quad \left(0, \quad 1, \quad \frac{d}{2}, \quad 0, \quad \dots, \quad 0, \quad \frac{d}{2}\right); \\ \bar{Y}_{n-2} & \quad \left(0, \quad 0, \quad -1, \quad \frac{d}{2}-1, \quad \dots, \quad 0, \quad \frac{d}{2}\right); \\ \bar{Y}_{n-1} & \quad \left(0, \quad 0, \quad 0, \quad 1, \quad \dots, \quad \frac{d-1}{2}, \quad \frac{d}{2}\right); \\ \bar{Y}_{n-2} & \quad \left(0, \quad 0, \quad 0, \quad 0, \quad \dots, \quad -1, \quad \frac{d}{2}\right). \end{aligned} \right\}$$

Розглянемо послідовність доведення для модуля порівняння A_0 при $n=4$. Рівняння (5.74) набуває вигляду

$$A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 = 0,$$

де коефіцієнти A_i ($i=1, \dots, 4$) вибрані у відповідності з формулами

$$\left. \begin{aligned} A_4 &= 1; A_3 = d-1; \\ A_2 &= E^-\left(\frac{d-1}{2}\right) + E^-\left(\frac{d}{2}\right); \\ A_1 &= \begin{cases} A_2 \frac{d-1}{2} - A_2 \frac{d-3}{2} + 1; d - \text{непарне}; \\ A_2 \left(\frac{d}{2} - 1\right) + \frac{d}{2}; d - \text{парне}. \end{cases} \end{aligned} \right\} \quad (5.79)$$

Базисом у цьому випадку будуть вектори

$$\left. \begin{aligned} \bar{Y}_1(0, & \quad 0, & \quad -1, & \quad d-1); \\ \bar{Y}_2(0, & \quad -1, & \quad E^-\left(\frac{d-1}{2}\right) & \quad E^-\left(\frac{d}{2}\right)); \\ \bar{Y}_3(-1, & \quad \frac{d-1}{2}, & \quad \frac{d-3}{2}, & \quad 1), & \quad d - \text{непарне}; \\ \bar{Y}_4(-1, & \quad \frac{d}{2}-1, & \quad 0, & \quad \frac{d}{2}), & \quad d - \text{парне}. \end{aligned} \right\} \quad (5.80)$$

Кожен із векторів (5.79) має вагу $W(\bar{Y})$ і задовольняє умові ТСК. Однак серед векторів, що мають вагу d можна знайти і такі, лінійна форма яких

$$L(\bar{X}) = A_1x_1 + A_2x_2 + A_3x_3 + A_4x_4 \neq 0.$$

Позначимо через M – множину векторів $Z(z_1, z_2, z_3, z_4)$, до яких ставляться такі вимоги

$$\left. \begin{aligned} W(\bar{Z}) &= d, \\ W(\bar{Z} + \bar{X}) &\geq d. \end{aligned} \right\}$$

Ясно, що в якості модуля A_0 можна взяти будь-яке ціле число. А тому що зі збільшенням A_0 збільшується час, необхідний для отримання заданого N_p , то доцільно обрати

$$A_0 = \min L(Z), \quad Z \in M,$$

що збільшить швидкість передавання.

Для знаходження $\bar{Z}(z_1, z_2, z_3, z_4) \in M$ доведемо теорему.

Теорема 16. Існує такий вектор $Z(z_1, z_2, z_3, z_4) \in M$, координати якого задовольняють будь-якому з таких обмежень:

$$\left. \begin{aligned} -z_2 - z_4 &\leq \frac{d-1}{2}; z_3 - z_4 \leq \frac{d-1}{2}; \\ z_3 - z_2 &\leq \frac{d-5}{2}; \\ z_4 &\leq -1; z_3 \geq 0; z_2 \leq -1; z_1 > 0. \end{aligned} \right\}, \quad (5.81a)$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-5}{2}; z_2 + z_3 \leq \frac{d+1}{2}; \\ z_3 - z_4 &\leq \frac{d+1}{2}; z_2 \geq 0; z_3 \geq 1; \\ z_4 &\leq 0; z_1 \geq 0. \end{aligned} \right\}, \quad (5.81b)$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-7}{2}; -z_3 + z_4 \leq \frac{d+1}{2}; \\ -z_3 - z_2 &\leq \frac{d-1}{2}; z_4 \geq 0; z_3 \leq 1; \\ z_2 &\leq 0; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{B})$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d-1}{2}; z_3 + z_4 \leq \frac{d-1}{2}; \\ z_2 - z_3 &\leq \frac{d+1}{2}; z_3 \geq -1; z_2 \geq 0; \\ z_4 &\leq 1; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{Г})$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d-3}{2}; z_3 + z_4 \leq \frac{d-3}{2}; \\ z_3 - z_2 &\leq \frac{d-3}{2}; z_2 \leq -1; z_3 \geq 0; \\ z_4 &\geq 0; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{Д})$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d+1}{2}; -z_3 + z_4 \leq \frac{d-1}{2}; \\ z_3 + z_2 &\leq \frac{d-3}{2}; z_3 \leq -1; \\ z_2 &\geq 1; z_4 \geq 1; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{Ж})$$

$$\left. \begin{aligned} -z_2 - z_4 &\leq \frac{d-3}{2}; z_3 - z_4 \leq \frac{d+1}{2}; \\ -z_2 - z_3 &\leq \frac{d-3}{2}; z_2 \leq 0; \\ z_3 &\leq -1; z_4 \leq -1; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{З})$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-1}{2}; -z_3 - z_4 \leq \frac{d-3}{2}; \\ z_2 - z_3 &\leq \frac{d-1}{2}; z_2 \geq 1; \\ z_3 &\leq 0; z_4 \leq 0; z_1 > 0. \end{aligned} \right\}, \quad (5.81\text{К})$$

Усі вісім умов доводяться аналогічно теоремі 5. Зазначені умови є обмеженнями багатогранного об'єму в n -вимірному просторі і представляють 8 задач лінійного програмування, розв'язання яких здійснюється при застосуванні симплексного методу.

Доведемо справедливність (5.81б)

$$\left. \begin{aligned} \bar{Y}_5 &= \bar{Y}_2 - \bar{Y}_1; \bar{Y}_5(0; -1; \frac{d+1}{2}; \frac{-d+1}{2}); \\ \bar{Y}_3 + 2\bar{Y} - \bar{Y}_1 &= \bar{Y}_7(-1; \frac{d-5}{2}; \frac{d+3}{2}; 1); \\ L(Y_i) &= 0; i = 5, 6, 7. \end{aligned} \right\} \quad (5.82)$$

За умовою теореми $\bar{Z} \in M$, тобто

$$W(\bar{Z}) = \sum_{k=1}^4 |z_k| = d,$$

$$W(\bar{Z} - \varphi_7) = |z_1 - 1| + \left| z_2 - \frac{d-5}{2} \right| + \left| z_3 - \frac{d+3}{2} \right| + |z_4 - 1| \geq d.$$

Вважаємо з нерівності (5.82)

$$\left. \begin{aligned} z_1 &> 0; 0 \leq z_2 \leq \frac{d-5}{2}; \\ 1 \leq z_3 \leq \frac{d+3}{2}; z_4 &\leq 0; \\ d &\geq 7. \end{aligned} \right\} \quad (5.83)$$

Віднімемо з нерівності (5.82) рівність (5.81б)

$$|z_1 + 1| - |z_1| + \frac{d-5}{2} - 2z_2 + \frac{d+3}{2} - 2z_3 + |z_4 - 1| - |z_4| \geq 0. \quad (5.84)$$

Враховуючи обмеження (3.83) і зауваживши

$$|z_1 + 1| - |z_1| = 1; \quad |z_4 - 1| - |z_4| = 1,$$

після підставлення зазначених різниць у вираз (5.84) та простих перетворень, отримаємо третю з нерівностей (5.78)

$$z_3 - z_4 \leq \frac{d+1}{2}.$$

Другу та першу з нерівностей (3.78) можна вивести, використовуючи замість (5.82)

$$W(\bar{Z} - \varphi_6) \geq d, \quad W(\bar{Z} - \varphi_5) \geq d.$$

Для визначення модуля порівняння A_0 потрібно знайти $\min L(\bar{Z})$ при $\bar{Z} \in M$.

$$\min L(\bar{Z}) = \min(A_1 z_1 + A_2 z_2 + A_3 z_3 + A_4 z_4), \bar{Z} \in M.$$

Враховуючи, що коефіцієнти лінійної функції пов'язані співвідношеннями $A_4 \leq A_3 \leq A_2 \leq A_1$, то для знаходження найменшого значення лінійної функції $L(\bar{Z})$ будемо вибирати такі вектори \bar{Z} , в яких найбільші значення мають координати з великими номерами. Після простих перетворень для непарних d отримаємо:

$$\left. \begin{aligned} A_0 = L(\bar{Z}_1) &= A_1 \frac{d-1}{2} + \frac{5d-1}{2}; d \geq 5; \\ A_0 = L(\bar{Z}_2) &= A_1 \frac{d-1}{2} - A_3 \frac{d-1}{2} + 1; d \geq 7; \\ L(\bar{Z}_1) &> L(\bar{Z}_2). \end{aligned} \right\} \quad (5.85)$$

З виразів (5.85) видно, що вираз для A_0 залежить не тільки від n , а й від величини d . Зі збільшенням d можна знайти інші (менші) значення модуля порівняння A_0 , ніж ті, що визначаються загальною теоремою кодування. Зокрема, для $n = 4$ і $d \geq 5$ можна довести теорему.

Приклад 6. Визначити кількість кодових конструкцій, які задовольняють умові при $i = 3$, $d = 4$, $s = 7$, $m = 5$.

Для заданих параметрів m, i, s визначимо загальну кількість таймерних сигналів $N_p = 680$.

Згідно з виразом (5.75) значення коефіцієнтів A_i в рівнянні (5.74) $A_3 = 1$ $A_2 = 3$ $A_1 = 5$ $A_0 = 12$. Число реалізацій, які відповідають умові (5.74), буде $N_p \left(\sum A_i x_i = 0 \right) = \frac{680}{12} \approx 56$.

Таймерні сигнальні конструкції використовуються в каналах моделі Гільберта, які відрізняються тим, що мають два робочих стану: «хороший», що займає не менше 99,5% часу передачі сигналу, і «поганий», що займає не більше 0,5% часу передачі сигналу. При цьому, в «хорошому» стані середньоквадратичне відхилення ЗМВ становить $\sigma \leq 0,02t_0$. Для відмінності «хорошого» і «поганого» станів каналу використовується рівняння якості, в якому взаємопов'язані довжини відрізків сигнальних конструкцій:

$$A_1 x_1 + \dots + A_{n-1} x_{n-1} + A_n x_n = 0 \text{ mod } A_0 \quad (5.86)$$

або $A \cdot X = 0 \text{ mod } A_0$, при цьому елементи векторів $A (A_1, \dots, A_n)$ и $X (x_1, \dots, x_n)$ – цілі числа.

Для заданих коефіцієнтів справедлива наступна теорема:

Теорема 17. Якщо коефіцієнти A_i і A_0 модуль порівняння визначені за формулами

$$A_n = 1,$$

$$\begin{aligned}
A_{n-1} &= d - 1, \\
A_{n-k} &= \left\lfloor \frac{d-1}{2} \right\rfloor A_{n-k+1} + \left\lfloor \frac{d}{2} \right\rfloor, k = 2, \dots, n-1, \\
A_0 &= \left\lfloor \frac{d+1}{2} \right\rfloor A_1 + \left\lfloor \frac{d}{2} \right\rfloor, d \geq 3, d - \text{нечетн.}
\end{aligned} \tag{5.87}$$

то будь-який вектор x , що задовольняє умові (8), має вагу

$$W(x) = \sum_{k=1}^n |x_k| \geq d \tag{5.88}$$

Доведення:

Відзначимо, що формула (5.87) при d парному і непарному записується відповідно:

d - парне $A_n = 1$ $A_{n-1} = d - 1$ $A_{n-k} = \left(\frac{d}{2} - 1\right) A_{n-k+1} + \frac{d}{2},$ $k = 2, \dots, n - 1$ $A_0 = \left(\frac{d}{2}\right) A_1 + \left(\frac{d}{2}\right)$	d - непарне $A_n = 1$ $A_{n-1} = d - 1$ $A_{n-k} = \left(\frac{d-1}{2}\right) A_{n-k+1} + \frac{d-1}{2},$ $k = 2, \dots, n - 1$ $A_0 = \left(\frac{d+1}{2}\right) A_1 + \left(\frac{d-1}{2}\right)$	$\left. \vphantom{\begin{matrix} A_n \\ A_{n-1} \\ A_{n-k} \\ k \\ A_0 \end{matrix}} \right\} \tag{5.89}$
--	--	---

Наведемо доведення теореми для d – непарного.

Зважаючи формули (5.89), легко перевірити, що вектори

$Y_1 \left(1, \frac{d+1}{2}, 0, 0, 0, \dots, \frac{d-1}{2} \right)$ $Y_2 \left(0, -1, \frac{d-1}{2}, 0, 0, \dots, \frac{d-1}{2} \right)$ $Y_{n-2} \left(0, \dots, 0, -1, \frac{d-1}{2}, 0, \frac{d-1}{2} \right)$ $Y_{n-1} \left(0, \dots, 0, 0, -1, \frac{d-2}{2}, \frac{d-1}{2} \right)$ $Y_n \left(0, \dots, 0, 0, -1, d-1 \right)$	$\left. \vphantom{\begin{matrix} Y_1 \\ Y_2 \\ Y_{n-2} \\ Y_{n-1} \\ Y_n \end{matrix}} \right\} \tag{5.90}$
---	---

ортогональні \bar{A} .

Будь який вектор \bar{x} , що задовольняє умові (5.90), представляється у

вигляді $\bar{x} = \sum_{k=1}^n \alpha_k Y_k$, звідки випливає

$$\left. \begin{aligned}
 p &= -\alpha_1 \\
 x_1 &= -\alpha_2 + \alpha_1 \frac{d+1}{2} \\
 x_2 &= -\alpha_3 + \alpha_2 \frac{d-1}{2} \\
 x_{n-1} &= \alpha_n + \alpha_{n-1} \frac{d-1}{2} \\
 x_n &= \frac{d-1}{2} \sum_{k=1}^n \alpha_k + \frac{d-1}{2} \alpha_n + \alpha_1
 \end{aligned} \right\} (5.91)$$

З значень змінної x_i (5.91) випливає, що координати будуть цілими числами тоді і тільки тоді, коли α_k – цілі.

При проведенні подальших міркувань будемо вважати, що α_k – цілі числа. Розглянемо випадок, коли всі α_k мають однаковий знак, тоді з (5.91) отримаємо

$$W(x) = \sum_{k=1}^n |x_k| \geq |x_n| \geq d. \quad (5.92)$$

Нехай тепер у ряді чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ мається, принаймні дві зміни знаку.

Нехай α_i і α_{i+1} , α_k і α_{k+1} мають різні знаки. Тоді

$$W(x) \geq |x_{i-1}| + |x_{k-1}| \geq |d_{i+1}| + |\alpha_i| \frac{d-1}{2} + |\alpha_{k+1}| + |\alpha_k| \frac{d-1}{2} > d.$$

Припустимо, що в ряді коефіцієнтів $\alpha_1, \alpha_2, \dots, \alpha_n$ одна зміна знаків

$$\text{sign} \alpha_k \neq \text{sign} \alpha_{k+1}.$$

Тоді

$$|x_k| = |\alpha_{k+1}| + \alpha_k \frac{d-1}{2}, k = 2, 3, \dots, n-1. \quad (5.93)$$

Якщо при цьому $|\alpha_k| \geq 2$, то з (5.93) випливає

$$W(x) \geq |x_k| \geq 1 + 2 \cdot \frac{d-1}{2} = d.$$

за умови $|\alpha_k| = 1$ можна показати, що

$$|x_{k-1}| = -1 + \alpha_{k-1} \frac{d-1}{2},$$

якщо $|\alpha_{k-1}| \geq 2$, $|x_k| \neq 0$ для цілого α_{k-1}

$$W(x) \geq |x_k| + |x_{k-1}| \geq 1 + 1 \cdot \frac{d-1}{2} + 2 \cdot \frac{d-1}{2} \geq d.$$

Остання нерівність і є доказом сформульованої вище теореми. Аналогічне доказ можна провести для випадку, коли $|\alpha_{k-1}| = 1$ відповідає $|x_{k-2}|$ або, якщо все $|\alpha_{k-1}| = |\alpha_{k-1}| = \dots = |\alpha_2| = 1$.

В результаті отримаємо

$$W(x) \geq |x_k| + |x_1| \geq 1 + \frac{d-1}{2} - 1 + \frac{d+1}{2} = d. \quad (5.94)$$

Для передачі по каналу зв'язку кодового слова при наявності завад рівняння сигналу з перешкодою на виході каналу буде мати вигляд:

$$A_1(x_1 + e_1) + \dots + A_{n-1}(x_{n-1} + e_{n-1}) + A_n(x_n + e_n) = 0 \text{ mod } A_0,$$

або

$$(A_1x_1 + \dots + A_{n-1}x_{n-1} + A_nx_n) + (A_1e_1 + \dots + A_{n-1}e_{n-1} + A_n e_n) = 0 \text{ mod } A_0 \quad (5.95)$$

У цьому випадку існує ймовірність того, що вектор перешкоди буде розпізнано, оскільки його сума по модулю A_0 , також як і вектора сигналу, буде дорівнює нулю.

Наприклад, при $i = 3$, $S = 7$ і коефіцієнтах A_i , рівних $A_1 = 2$; $A_2 = 3$; $A_3 = 7$; $A_0 = 19$, можливі координати перешкоди, що забезпечують появу нульового вектора приймуть вигляд

$$\begin{aligned} E_{0_1}(0) &\rightarrow \pm 3; \mp 2; 0 \quad w = 5, \\ E_{0_2}(0) &\rightarrow \pm 2; \pm 1; \mp 1 \quad w = 4, \\ E_{0_3}(A_0) &\rightarrow \mp 1; 0; \pm 3 \quad w = 4, \end{aligned} \quad (5.96)$$

де w – вага вектора.

Знаючи координат нульових векторів і значення середньоквадратичного відхилення σ , можна оцінити ймовірність появи такої завади. Наприклад, для вектора перешкоди E_{0_2} ймовірність невиявленої помилки складе

$$P_{\text{невияв}} = 0,5 \cdot P(2) \cdot P(1) \cdot P(1), \quad (5.97)$$

де множення на 0,5 враховує зміну знака третього зміщення по відношенню до перших двох.

Ймовірності того, залишиться елемент в своїй зоні або ж зміститься на величини 1Δ , 2Δ , 3Δ , відповідно, будуть рівні

$$\begin{aligned} P(0) &= 2\Phi(0,5\Delta/\sigma), \\ P(1) &= \Phi(1,5\Delta/\sigma) - \Phi(0,5\Delta/\sigma), \\ P(2) &= \Phi(2,5\Delta/\sigma) - \Phi(1,5\Delta/\sigma), \\ P(3) &= \Phi(3,5\Delta/\sigma) - \Phi(2,5\Delta/\sigma), \end{aligned} \quad (5.98)$$

де функція $\Phi(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_0^x e^{-\frac{z^2}{2}} dz$ – значення інтеграла ймовірності.

Як було зазначено вище, в «хорошому» стані каналу середньоквадратичне відхилення ЗМВ становить $\sigma \leq 0,02t_0$. Для параметра $S = 7$ ширина зони $\Delta = 1/7 \approx 14,28\%$. Тоді отримаємо

$$\begin{aligned}
P(0) &= \Phi(0,5 \cdot 0,14 / 0,02), \\
P(1) &= \Phi(1,5 \cdot 0,14 / 0,02) - \Phi(0,5 \cdot 0,14 / 0,02), \\
P(2) &= \Phi(2,5 \cdot 0,14 / 0,02) - \Phi(1,5 \cdot 0,14 / 0,02), \\
P(3) &= \Phi(3,5 \cdot 0,14 / 0,02) - \Phi(2,5 \cdot 0,14 / 0,02).
\end{aligned} \tag{5.99}$$

У цьому випадку ймовірність появи нульового вектора E_{0_2} буде

$$\begin{aligned}
P &= 0,5((\Phi(2,5 \cdot 0,14 / 0,02) - \Phi(1,5 \cdot 0,14 / 0,02)) \cdot (\Phi(1,5 \cdot 0,14 / 0,02) - \Phi(0,5 \cdot 0,14 / 0,02))) \times \\
&\times (\Phi(1,5 \cdot 0,14 / 0,02) - \Phi(0,5 \cdot 0,14 / 0,02)) < 10^{-8}.
\end{aligned} \tag{5.100}$$

Таким чином, отримані сумарні ймовірності не виявлення викривлень ТСК $P_{\text{нв}} < 10^{-8}$, що також підтверджується проведеними експериментами в реальному каналі ГТС.

5.5. Завадостійкість систем з реєстрацією нульового рівня

Важливою відмінністю симплексного методу передавання від дуплексного є відсутність можливості запиту спотворених завадами СК. У сукупності зі значною складністю задачі декодування за максимумом правдоподібності, яка відноситься до класу NP повних, визначає низьку ефективність класичних асинхронних симплексних СПД.

Розглянемо роботу бінарної системи з реєстрацією 0 рівня сигналу, що відповідає таймерному методу надання інформації.

При цьому будемо вважати що прийняті сигнали мають амплітуди $+\sqrt{U}$ або $-\sqrt{U}$. Крім цього припустимо, що величина r_b характеризує число відліків дискретизації на базовий елемент інформації в повідомленні й що шум характеризується рівномірним розподілом між піками в межах $\pm \bar{\sigma}$.

Якщо величина $\bar{\sigma}^2$ менше ніж U , тоді невизначеність при прийманні сигналів і розв'язання завдання винесення розв'язання про прийнятий елемент тривіальна. По цьому будемо розглядати випадок коли $\bar{\sigma}^2 > U$.

Апостеріорна ймовірність того, що був переданий $+\sqrt{U}$ після отримання відліку y_j з номером j :

$$p(\sqrt{U} | (y_1 \dots y_{r_b})) = \begin{cases} 1, & y_j > \bar{\sigma} - \sqrt{U} \\ 1/2, & -(\bar{\sigma} - \sqrt{U}) < y_j < (\bar{\sigma} - \sqrt{U}) \\ 0, & y_j < \bar{\sigma} - \sqrt{U} \end{cases} \tag{5.101}$$

Розташувавши елементи відповідно до їхньої апостеріорної ймовірності, усі можливі отримані сигнали можна поділити на три окремі діапазони. Позначимо ці діапазони +1, 0, -1 відповідно. При передаванні

елемента $z + \sqrt{U}$, умовна ймовірність того, що всі відліки дискретизації y_j перебувають у діапазоні $|y_j| < \bar{\sigma} - \sqrt{U}$, може бути визначена як:

$$p(0|\sqrt{U}) = \left(1 - \sqrt{\frac{U}{\bar{\sigma}^2}}\right)^{r_b}. \quad (5.102)$$

Тому що величина будь-якого y_j не може набувати значення менше ніж $-(\bar{\sigma} - \sqrt{U})$:

$$\begin{aligned} p(-1|\sqrt{U}) &= p(+1|-\sqrt{U}) = 0, \\ p(+1|\sqrt{U}) &= p(-1|-\sqrt{U}) = 1 - \left(1 - \sqrt{\frac{U}{\bar{\sigma}^2}}\right)^{r_b}. \end{aligned} \quad (5.103)$$

Позначення через +1, 0, -1 трьох рівнів при передаванні інформації є оптимальним. Кінцева величина ентропії у повідомленні визначається:

$$H = 1 - \left(1 - \sqrt{\frac{U}{\bar{\sigma}^2}}\right)^{r_b}. \quad (5.104)$$

Проведемо порівняння з оптимальною системою, в якій приймання елементів здійснюється шляхом «інтегрування», без урахування інформації про нульові значення сигналу. Система з інтегруванням працює наступним чином. Якщо сума $\sum y_i$ позитивна, то приймач реєструє «+1», якщо сума $\sum y_i$ негативна, реєструється «-1».

При передаванні сигналу $+\sqrt{U}$, у випадку приймання $\sum y_i < 0$ розв'язання про реєстрацію буде невірним. Визначимо новий набір змінних z^p_j так, що $z^p_j = y_j - \sqrt{U}$. Можливі значення z^p_j перебувають у діапазоні $|z^p_j| \leq \bar{\sigma}$. Тоді умовою помилкової реєстрації, коли переданий $+\sqrt{U}$, буде:

$$\sum_{i=1}^r z^p_j < -r_b \sqrt{U}. \quad (5.105)$$

Для $r_b = 1$ імовірність для неправильної реєстрації буде дорівнювати

$$p(-1|\sqrt{U}) = \frac{\bar{\sigma} - \sqrt{U}}{2\bar{\sigma}} = \frac{1}{2} \left(1 - \sqrt{\frac{U}{\bar{\sigma}^2}}\right). \quad (5.106)$$

Для $r_b = 2$ $p(0|+\sqrt{U})$ може бути визначена геометричним шляхом. Область можливого приймання показана у вигляді квадрата на рис. 5.4. Область неправильної реєстрації заштрихована щільним штрихуванням.

Отже,

$$p(-1|\sqrt{U}) = \frac{\text{Заштрихована площа}}{\text{Загальна площа}} = \frac{1}{2} \left(1 - \sqrt{\frac{U}{\bar{\sigma}^2}}\right)^2. \quad (5.107)$$

Для $r_B > 2$ імовірність $p(-1|\sqrt{U})$ може бути отримана шляхом відображення на геометричному r_B -вимірному просторі. У цьому випадку, простором можливої реєстрації прийнятого сигнал буде r_B -вимірний куб. Простір неправильної реєстрації – кут, виключений з r_B -вимірного куба $(r_B - 1)$ -вимірною гіперповерхнею $-r_B \sqrt{P}$.

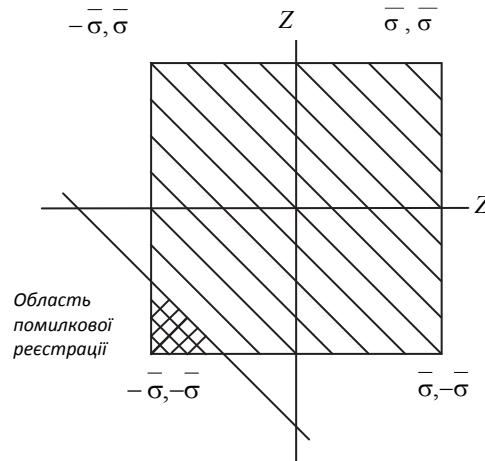


Рисунок 5.4 - Зона помилкової реєстрації при фіксації нульових значень сигналів

Якщо величина U перебуває в діапазоні:

$$\bar{\sigma}^2 > U > \left(\frac{r_B - 2}{r_B} \right)^2 \bar{\sigma}^2,$$

Зону помилкової реєстрації можливо обчислити як:

$$V_l(-1|\sqrt{U}) = \frac{r_B^{r_B}}{r_B!} (\bar{\sigma} - \sqrt{U})^{r_B}. \quad (5.108)$$

У такий спосіб

$$p(-1|\sqrt{U}) = \frac{V_l(-1|\sqrt{U})}{\text{загальний об'єм}}, \quad (5.109)$$

або,

$$p(-1|\sqrt{U}) = \left(\frac{r_B}{2} \right)^{r_B} \cdot \frac{1}{r_B!} \left\{ 1 - \sqrt{\frac{U}{\bar{\sigma}^2}} \right\}^{r_B}. \quad (5.110)$$

Для невеликих значень r_B визначимо:

$$r_B > 4 \text{ і } \left(\frac{r_B - 2}{r_B} \right) > \left(\frac{U}{\bar{\sigma}^2} \right) > \left(\frac{r_B - 4}{r_B} \right)^2. \quad (5.111)$$

Результати для $p(-1|\sqrt{U})$ можуть бути отримані аналогічним способом зі співвідношення (5.110), за винятком одного додаткового члена, який необхідно відняти:

$$\left(\frac{r_B}{2}\right)^{r_B} \cdot \frac{1}{r_B!} \left[r_B \left(\frac{r_B - 2}{r_B} - \sqrt{\frac{U}{\sigma^2}} \right) \right]. \quad (5.112)$$

У такий же спосіб результати для $r_B > 6$,

$$\left(\frac{r_B - 4}{r_B}\right) > \left(\frac{U}{\sigma^2}\right) > \left(\frac{r_B - 6}{r_B}\right)^2, \quad (5.113)$$

результати для $p(-1/\sqrt{U})$ аналогічні співвідношенню (5.111), за винятком додаткового елемента, який необхідно додати:

$$\left(\frac{r_B}{2}\right)^{r_B} \cdot \frac{1}{r_B!} \left[\frac{r_B(r_B - 1)}{2} \left(\frac{r_B - 4}{r_B} - \sqrt{\frac{U}{\sigma^2}} \right)^{r_B} \right]. \quad (5.114)$$

Ці результати можуть бути компактно записані у формі, яка виконується для всіх r_B .

$$p(-1|\sqrt{U}) = \left(\frac{r_B}{2}\right)^{r_B} \cdot \frac{1}{r_B!} \sum_{\vartheta=0}^{\vartheta_m} (-1)^{\vartheta} \frac{r_B!}{\vartheta!(r_B - \vartheta)!} \cdot \left[\frac{r_B - 2\vartheta}{r_B} - \sqrt{\frac{U}{\sigma^2}} \right], \quad (5.115)$$

де

$$\vartheta_m \leq \frac{r}{2} \left(1 - \sqrt{\frac{U}{\sigma^2}} \right). \quad (5.116)$$

Простим методом виправлення спотворених кодових слів на прийманні є метод повторного передавання. Але у класичному вигляді потребує не менш як 3-кратного повтору для винесення мажоритарного рішення, що значною мірою знижує швидкість передавання.

Розв'язання завдання коригування спотворених кодових слів на прийманні, досягається за рахунок формування надлишковості у словнику на передаванні. У першу чергу, це можливо за рахунок візуально-аналітичного розподілу кодових слів на дозволені і недозволені. При цьому, функція:

$$f(x_1, x_2, x_3) = \begin{cases} x = x_1 + e_0 \cos(\theta) \cos(\varphi); \\ y = x_2 + e_0 \sin(\theta) \cos(\varphi); \\ z = x_3 + e_0 \sin(\theta), \end{cases} \quad (5.117)$$

де $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, $\varphi \in [0, 2\pi]$, x_j – положення ЗММ задає тримірне просторове відображення кодових слів ТСК зі значенням $i = 3$. За даного способу відображення на осях $0-X$, $0-Y$, $0-Z$ відкладаються значення першого x_1 , другого x_2 та третього x_3 ЗММ. На рис. 5.5 приведено взаємне розміщення кодових слів відібраних за заданим критерієм.

Виправлення помилок зміщення ЗММ відносно дійсних положень на прийманні можливе за допомогою рівняння якості:

$$\sum_{j=1}^i A_j x_j \equiv Z \pmod{A_0}, \quad (5.118)$$

де A_j – коефіцієнти, що забезпечують необхідні відстані між дозволеними конструкціями;

Z – один з можливих залишків.

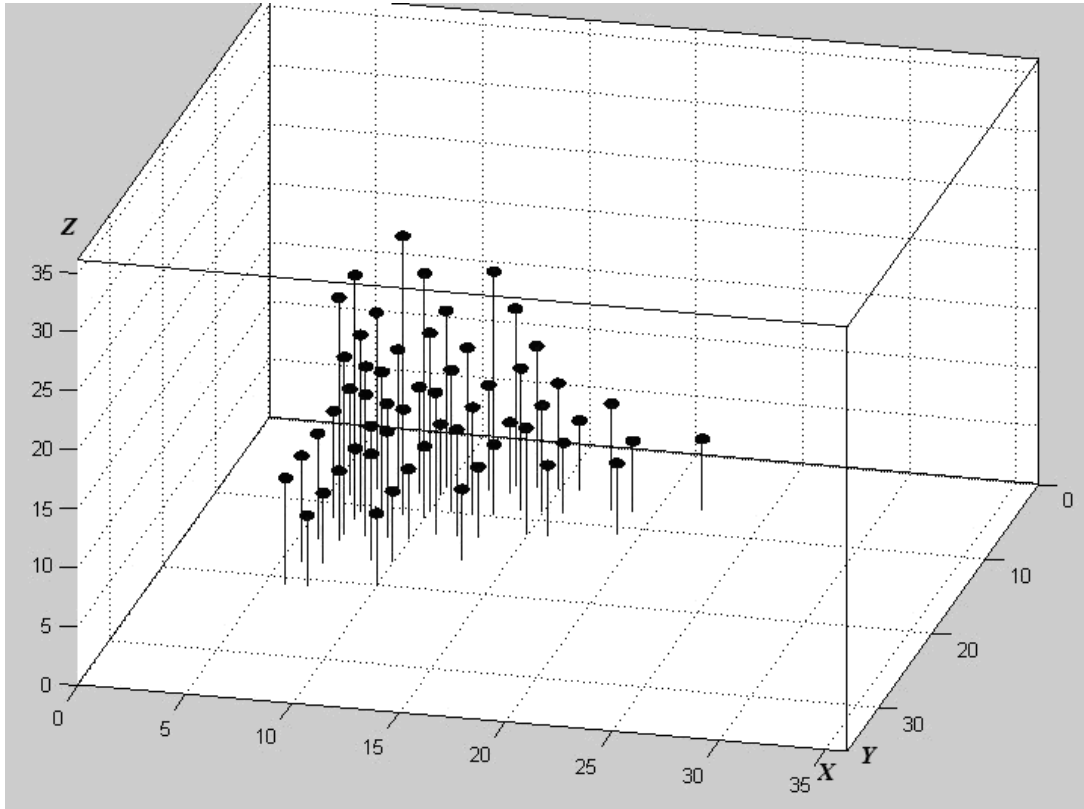


Рисунок 5.5 - Просторове відображення ТСК з $i = 3$ відібраних за заданим критерієм

Якщо коефіцієнти рівняння (5.117) визначені так, що

$$A_0 = (e_0 + 1)^i, A_j = (e_0 + 1)^{j-1}; \quad j \in \{1 \dots i\}, \quad (5.119)$$

то помилки кратності меншої або рівної i величиною $[-e_0; e_0]$ виявляються з імовірністю 1.

Якщо коефіцієнти A_j рівняння (5.120) визначено таким чином, що

$$A_0 = (2e_0 + 1)^i, A_j = (2e_0 + 1)^{j-1}; \quad j \in \{1 \dots i\}, \quad (5.120)$$

то помилки, кратності меншої чи рівної i величиною $[-e_0; e_0]$ виявляються й виправляються з імовірністю 1.

При цьому слід зауважити, що за умови вибору вищезазначених коефіцієнтів, векторам помилок будуть відповідати синдроми рівняння якості, зведені у табл. 5.6.

Таблиця 5.6 - Група векторів для виправлення помилок коефіцієнтами $A_i \in 2, 3, 7$ і $A_0 = 19$ $X_1 - 1, X_2 - 2, X_3 -$ відповідні синдроми (С) рівняння якості

x1	x2	x3	C	x1	x2	x3	C	x1	x2	x3	C	x1	x2	x3	C	x1	x2	x3	C
0	0	0	0	0	-1	1	4	1	2	-1	1	2	0	0	4	-1	-2	1	18
0	0	1	7	0	0	-1	12	-2	-2	-1	2	-2	0	0	15	-2	2	1	9
0	1	-1	15	0	0	2	14	2	-2	0	17	2	0	1	11	2	2	1	17
0	1	0	3	0	1	-2	8	1	2	0	8	-2	0	1	3	-1	-2	2	6
0	1	1	10	1	-2	-2	1	-2	-2	0	9	-2	0	2	10	-1	-1	-2	0
1	-1	-1	11	0	1	2	17	2	-2	1	5	-2	1	-2	4	-2	2	2	16
1	-1	0	18	0	2	-2	11	1	2	1	15	2	0	2	18	2	2	2	5
1	-1	1	6	1	-2	-1	8	-2	-2	1	16	2	1	-2	12	-1	-1	2	9
1	0	-1	14	0	2	-1	18	2	-2	2	12	-2	1	-1	11	-1	0	-2	3
1	0	0	2	1	-2	0	15	2	-1	-2	6	2	1	-1	0	-1	0	2	12
1	0	1	9	0	2	0	6	1	2	2	3	-2	1	0	18	-1	1	-2	6
1	1	-1	17	1	-2	1	3	-2	-2	2	4	2	1	0	7	0	-2	-2	18
1	1	0	5	0	2	1	13	-2	-1	-2	17	-2	1	1	6	-1	1	2	15
1	1	1	12	1	-2	2	10	2	-1	-1	13	2	1	1	14	-1	2	-2	9
-1	-1	-1	7	1	-1	-2	4	-2	-1	-1	5	-1	-2	-2	16	0	-2	-1	6
-1	-1	0	14	0	2	2	1	2	-1	0	1	-2	1	2	13	-1	2	-1	16
-1	-1	1	2	1	-1	2	13	-2	-1	0	12	-2	2	-2	7	-1	2	0	4
-1	0	-1	10	1	0	-2	7	2	-1	1	8	2	1	2	2	0	-2	0	13
-1	0	0	17	1	0	2	16	-2	-1	1	0	2	2	-2	15	0	-2	1	1
-1	0	1	5	1	1	-2	10	2	-1	2	15	-1	-2	-1	4	-1	2	1	11
-1	1	-1	13	2	-2	-2	3	2	0	-2	9	-2	2	-1	14	0	-2	2	8
-1	1	0	1	1	1	2	0	-2	-1	2	7	2	2	-1	3	0	-1	-2	2
-1	1	1	8	1	2	-2	13	-2	0	-2	1	-2	2	0	2	-1	2	2	18
0	-1	-1	9	-2	-2	-2	14	2	0	-1	16	2	2	0	10	0	-1	2	11
0	-1	0	16	2	-2	-1	10	-2	0	-1	8	-1	-2	0	11	0	0	-2	5

Невиявленими будуть такі помилки, що перетворюють (5.118) у 0. Наприклад, при $A_i \in 2, 3, 5$ і $A_0 = 17$ можливо отримати наступні нульові вектори з вагою W :

$$E'_{03}(0) \rightarrow \pm 1; \pm 1; \mp 1, W = 3,$$

$$E'_{05}(0) \rightarrow \pm 2; \pm 1; \pm 2, W = 5,$$

$$E'_{06}(0) \rightarrow \pm 2; \pm 2; \mp 2, W = 6$$

Якщо коефіцієнти рівняння якості обрано як прості числа, то такі конструкції можливо представити у вигляді системи залишкових класів з набором взаємно простих модулів $(A_1, A_2, A_3, \dots, A_i)$ та

добутком $A = \prod_{i=1}^i A_k$ так, що кожному цілому x із множини $[0, A - 1]$

відповідає набір залишків (x_1, x_2, \dots, x_i) . «Китайська» теорема про залишки гарантує однозначність відтворення для чисел множини $[0, A - 1]$.

Отже, вибираючи таким чином кодові слова за наявності одного вірно прийнятого положення ЗММ, можливо відтворити усе кодове слово.

Таблиця 5.7 - Група векторів для виправлення помилок коефіцієнтами $A_i \in \{1, 3, 9\}$ і $A_0 = 27$ $X_1 - 1, X_2 - 2, X_3 -$ відповідні синдроми (С) рівняння якості

x1	x2	x3	С	x1	x2	x3	С	x1	x2	x3	С	x1	x2	x3	С	x1	x2	x3	С
0	0	0	0	0	-1	1	6	1	2	-1	25	2	0	0	2	-1	-2	1	2
0	0	1	9	0	0	-1	18	-2	-2	-1	10	-2	0	0	25	-2	2	1	13
0	1	-1	21	0	0	2	18	2	-2	0	23	2	0	1	11	2	2	1	17
0	1	0	3	0	1	-2	12	1	2	0	7	-2	0	1	7	-1	-2	2	11
0	1	1	12	1	-2	-2	4	-2	-2	0	19	-2	0	2	16	-1	-1	-2	5
1	-1	-1	16	0	1	2	21	2	-2	1	5	-2	1	-2	10	-2	2	2	22
1	-1	0	25	0	2	-2	15	1	2	1	16	2	0	2	20	2	2	2	26
1	-1	1	7	1	-2	-1	13	-2	-2	1	1	2	1	-2	14	-1	-1	2	14
1	0	-1	19	0	2	-1	24	2	-2	2	14	-2	1	-1	19	-1	0	-2	8
1	0	0	1	1	-2	0	22	2	-1	-2	8	2	1	-1	23	-1	0	2	17
1	0	1	10	0	2	0	6	1	2	2	25	-2	1	0	1	-1	1	-2	11
1	1	-1	22	1	-2	1	4	-2	-2	2	10	2	1	0	5	0	-2	-2	3
1	1	0	4	0	2	1	15	-2	-1	-2	4	-2	1	1	10	-1	1	2	20
1	1	1	13	1	-2	2	13	2	-1	-1	17	2	1	1	14	-1	2	-2	14
-1	-1	-1	14	1	-1	-2	7	-2	-1	-1	13	-1	-2	-2	2	0	-2	-1	12
-1	-1	0	23	0	2	2	24	2	-1	0	26	-2	1	2	19	-1	2	-1	23
-1	-1	1	5	1	-1	2	16	-2	-1	0	22	-2	2	-2	13	-1	2	0	5
-1	0	-1	17	1	0	-2	10	2	-1	1	8	2	1	2	23	0	-2	0	21
-1	0	0	26	1	0	2	19	-2	-1	1	4	2	2	-2	17	0	-2	1	3
-1	0	1	8	1	1	-2	13	2	-1	2	17	-1	-2	-1	11	-1	2	1	14
-1	1	-1	20	2	-2	-2	5	2	0	-2	11	-2	2	-1	22	0	-2	2	12
-1	1	0	2	1	1	2	22	-2	-1	2	13	2	2	-1	26	0	-1	-2	6
-1	1	1	11	1	2	-2	16	-2	0	-2	7	-2	2	0	4	-1	2	2	23
0	-1	-1	15	-2	-2	-2	1	2	0	-1	20	2	2	0	8	0	-1	2	15
0	-1	0	24	2	-2	-1	14	-2	0	-1	16	-1	-2	0	20	0	0	-2	9

Мінімізація впливу корельованих з сигналом завад. При аналізі каналів із флуктуаційними параметрами досить зручним є геометричне зображення випадкових величин з різним ступенем взаємної кореляції.

Реалізацію коливання $U_{рк} = U_{ск} + U_{шк}$ на вході приймача можна представити як n -мірний вектор, який дорівнює сумі векторів реалізації сигналу $U_{ск}$ адитивної реалізації завади $U_{шк}$ (рис. 5.7,а).

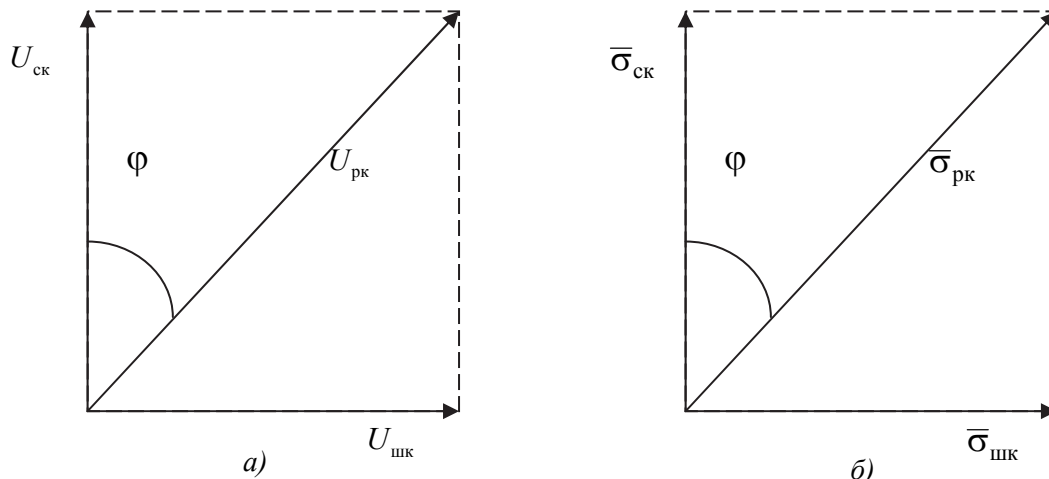


Рисунок 5.7 - Зображення сигналів у векторному виді

У прийнятному пристрої приймається рішення про реєстрацію того сигналу, який найбільш близько розташований до коливання, що приймається. Тому в якості критерію прийому можна взяти деяке значення φ_0 кута φ між векторами $U_{ск}$ і $U_{рк}$. Якщо вектор $U_{рк}$ вийде за межі кута φ_0 , то відбудеться помилка.

Коефіцієнт кореляції між векторами $U_{ск}$ та $U_{рк}$ визначається:

$$\rho_{ср} = \frac{E[U_{ск}U_{рк}]}{\sqrt{E[U_{ск}^2]E[U_{рк}^2]}}, \quad (5.121)$$

де математичне сподівання двовимірного розподілу:

$$E[U_{ск}U_{рк}] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} U_{ск}U_{рк} \omega(U_{ск}U_{рк}) dU_{ск} dU_{рк}, \quad (5.122)$$

а математичне сподівання квадратів складових

$$E[U_{ск}^2] = \sigma_{ск}^2; \quad E[U_{рк}^2] = \sigma_{рк}^2 = \sigma_{ск}^2 + \sigma_{шк}^2. \quad (5.123)$$

Тому що вектори $U_{ск}$ та $U_{шк}$ не залежать один від одного, то

$$\rho_{ср} = \frac{\sigma_{ск}}{\sigma_{рк}} = \frac{\sigma_{ск}}{\sqrt{\sigma_{ск}^2 + \sigma_{шк}^2}}. \quad (5.124)$$

Звідси випливає, що векторна діаграма випадкових векторів $U_{ск}$, $U_{шк}$ та $U_{рк}$ (рис. 5.7, а) еквівалентна векторній діаграмі не випадкових векторів $\bar{\sigma}_{ск}$, $\bar{\sigma}_{шк}$ та $\bar{\sigma}_{рк}$ (рис. 5.7, б), а коефіцієнт кореляції чисельно дорівнює косинусу кута φ між не випадковими векторами $\bar{\sigma}_{ск}$ та $\bar{\sigma}_{шк}$.

Взаємна кількість інформації між випадковими векторами U_c та U_p з нормальним законом розподілу можна виразити через коефіцієнт кореляції між однойменними їх складовими:

$$I(U_c; U_p) = -0,5 \sum_{k=1}^n \log_2(1 - p_k^2).$$

Тоді пропускна здатність каналу

$$C = -\frac{1}{T} \sum_{k=1}^n \log_2(1 - P_k^2) = -\Delta f_k \log_2(1 - P_k^2). \quad (5.125)$$

При використанні однопроменевих каналів перший сигнал, що має мінімальну затримку, можна розглядати як робочий сигнал з потужністю P_c , а решту затриманих сигналів – як заваду з потужністю $P_{ш}$, корельовану з сигналом. Крім того, в каналі діють адитивні шуми з потужністю $P_{ш}$.

Векторна діаграма для цього випадку представлена на рис. 5.8, а, де $\bar{\sigma}_c$, $\bar{\sigma}_{ш}$ і $\bar{\sigma}_{ш}$ – вектори, що чисельно дорівнюють середнім квадратичним значенням сигналу, корельованої завади та адитивних шумів.

Розкладемо корельовану заваду на дві складові

$$\bar{\alpha}_1 = \rho_{\text{сш}} \bar{\sigma}_{\text{ш}}, \quad \bar{\alpha}_2 = \sqrt{1 - \rho_{\text{сш}}^2} \bar{\sigma}_{\text{ш}}.$$

Синфазна складова $\bar{\alpha}_1$, жорстко корельована з сигналом, утворює сумарний сигнал $U_{\text{со}} = \bar{\sigma}_c + \rho_{\text{сш}} \bar{\sigma}_{\text{ш}}$, а ортогональна складова $\bar{\alpha}_2$, некорельована сигналом, утворює сумарну заваду

$$U_{\text{шо}} = \sqrt{\bar{\sigma}_{\text{ш}}^2 + (1 - \rho_{\text{сш}}^2) \bar{\sigma}_{\text{ш}}^2}.$$

Результуюче коливання

$$U_p = \sqrt{U_{\text{со}}^2 + U_{\text{шо}}^2}.$$

Коефіцієнт кореляції між $U_{\text{со}}$ та U_p буде

$$\rho_{\text{ср}} = \cos \varphi_2 = \frac{U_{\text{со}}}{\sqrt{U_{\text{со}}^2 + U_{\text{шо}}^2}}. \quad (5.126)$$

Підставивши вираз (5.125) у (5.126), отримаємо вираз для пропускної здатності однопроменевого каналу з корельованими шумами:

$$C = \Delta f_k \log_2 \left(\chi + \frac{P_c}{P_{\text{п}} + P_{\text{ш}}} \right), \quad (5.127)$$

де

$$\chi = \frac{\left(1 + \rho_{\text{сш}} \sqrt{\frac{P_{\text{п}}}{P_c}} \right)^2}{1 - \rho_{\text{сш}} \frac{P_{\text{п}}}{P_{\text{п}} + P_{\text{ш}}}}. \quad (5.128)$$

Наявність кореляції між шумом і сигналом характеризується векторною діаграмою рис. 5.8, б, де $\bar{\sigma}_c$, $\bar{\sigma}_{\text{шк}}$ – вектори, що чисельно дорівнюють середнім квадратичним значенням сигналу і корельованих шумів; $\rho_{\text{сш}} = \cos \varphi_1$ – коефіцієнт кореляції між сигналом і шумами; $\bar{\alpha}_1$, $\bar{\alpha}_2$ – синфазна та ортогональна складові шумів; $U_{\text{со}}$ – сумарний сигнал; U_p – результуюче коливання на вході приймального пристрою.

Коефіцієнт кореляції між $U_{\text{со}}$ та U_p , що чисельно характеризується $\cos \varphi_2$, буде:

$$\rho_{\text{ср}} = \frac{1}{\sqrt{1 + \frac{(1 - \rho_{\text{сш}}^2) P_{\text{шк}}}{\sqrt{P_c} + \rho_{\text{сш}} \sqrt{P_{\text{шк}}}}}}. \quad (5.129)$$

Тоді пропускна здатність каналу

$$C = \Delta f_k \log_2 (1 + \chi h_{\text{сш}}^2), \quad (5.130)$$

де

$$\chi = \frac{\left(1 + \frac{\rho_{\text{сш}}}{\sqrt{h_{\text{сш}}^2}}\right)^2}{1 - \rho_{\text{сш}}^2}; \quad (5.131)$$

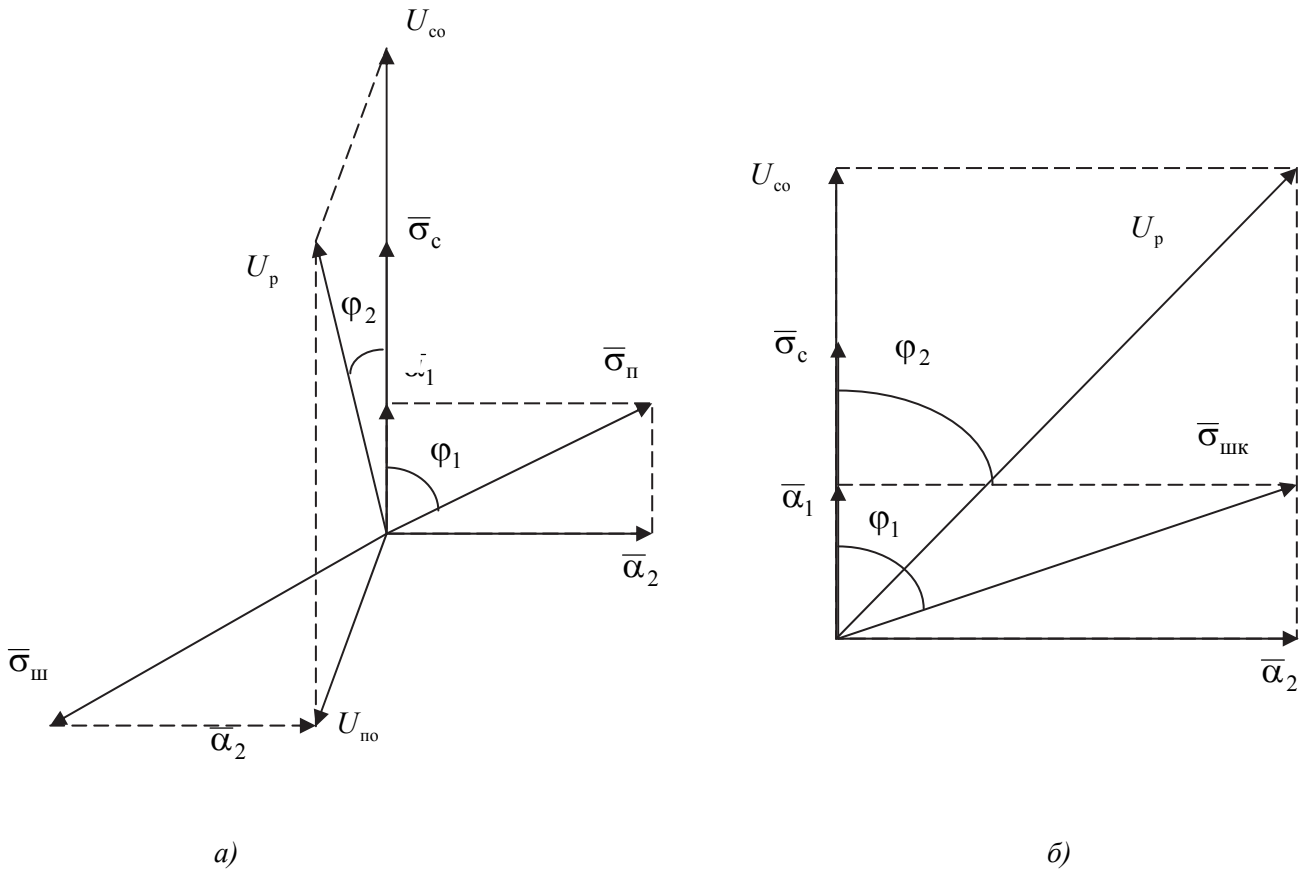


Рисунок 5.8 - Векторні моделі однопроменевих каналів:
 а) канал з адитивними шумами і корельованими завадами;
 б) канал з корельованими завадами

$$h_{\text{сш}}^2 = \frac{P_{\text{с}}}{P_{\text{шк}}}. \quad (5.132)$$

Подання кодових слів у вигляді векторів m -вимірному простору припускає використання кодової відстані d , відповідної максимуму правдоподібності. Коефіцієнт кореляції між двома кодовими словами визначаємо за формулою:

$$\rho_{jz} = \sum_{v=1}^m a_{vj} b_{vz}, \quad (5.133)$$

де a_j й b_z – елементи кодових слів, а добуток елементів:

$$a_{vj}b_{vz} = \begin{cases} +1, & a_{vj} = b_{vz} \\ -1, & a_{vj} \neq b_{vz} \end{cases} \quad (5.134)$$

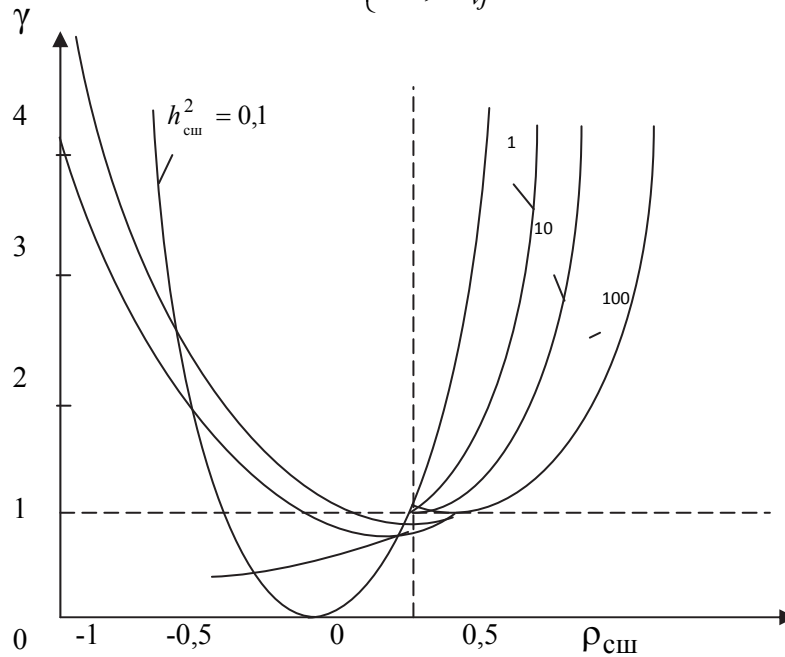


Рисунок 5.9 - Графіки $\gamma(\rho_{cш}; h_{cш})$

На прийманні фіксується кодове слово, в якого $\rho_{jj} > \rho_{jz}$ для $j \neq z$, якщо прийняте кодове слово відрізняється від кодових слів алфавіту в різних розрядах, величина $\Delta\rho$ – характеризує відстань між кодовими словами:

$$\Delta\rho = \rho_{jj} - \rho_{jz}. \quad (5.135)$$

Кодові слова, у яких значення ρ_{jz} найбільш близьке до ρ_{jj} , будемо називати найближчими й позначати $\rho_{j\bar{b}}$. Здатність коду виправляти й виявляти помилки характеризується значенням:

$$\Delta\rho_{\min} = \rho_{jj} - \rho_{j\bar{b}}. \quad (5.136)$$

Для виправлення одиничної помилки необхідно, щоб $\rho_{jj} - 2 > \rho_{j\bar{b}} + 2$, звідси $\Delta\rho_{\min} = 6$. Для корекції r помилок необхідно:

$$\Delta\rho_{\min} = 4r + 2. \quad (5.137)$$

У загальному випадку для виправлення r помилок і виявлення $g = r + w$ необхідно щоб:

$$\Delta\rho_{\min} = 2(2r + w + 1). \quad (5.138)$$

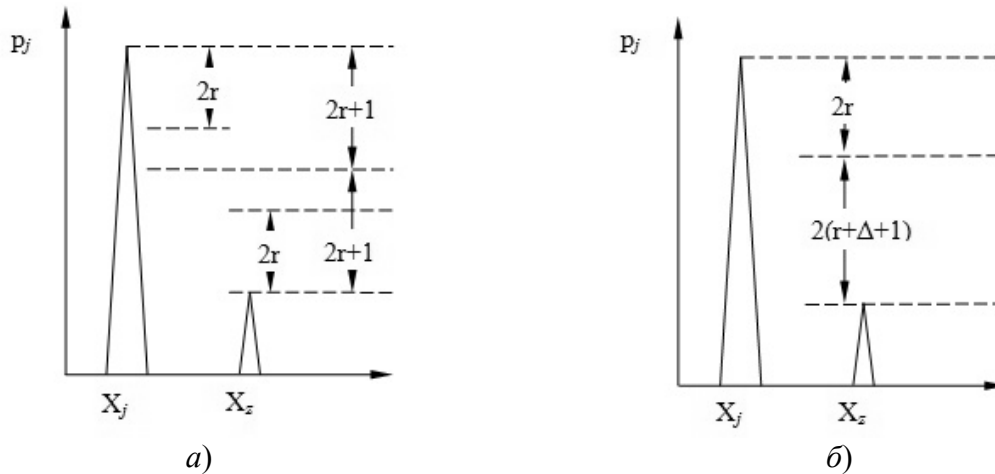


Рисунок 5.10 - Кореляційне трактування виправлення помилок

5.6. Ефективність використання наднайквістової швидкості модуляції при позиційному кодуванні

Оцінимо ефективність використання ТСК на прикладах використання їх для різних систем передачі.

Приклад 7. Оцінимо ефективність перетворення якості передавання у «хорошому стані» бінарного каналу у швидкість передавання для каналу з ЧМ ($P_e = 10^{-8}$) при базі сигналу, що дорівнює 1, в якому діє гауссівська завада.

Порівняємо два способи збільшення швидкості передавання інформації за рахунок використання швидкості модуляції в бінарному каналі більше найквістової або за рахунок використання бінарних ТСК.

Розглянемо випадок, коли за рахунок збільшення швидкості модуляції зменшується тривалість одиничного елемента при розрядно-цифровому коді.

Припустимо, що на вході каналу зі смугою $(0, \Omega)$ формується кодова послідовність. Поставимо задачу визначення дисперсії міжсимвольної завади, або, інакше кажучи, дисперсію помилки відновлення переданої інформаційної послідовності за швидкістю модуляції, що перевищує межу Найквіста. При цьому для зручності будемо припускати, що верхньою частиною смуги пропускання каналу Ω можна варіювати, обираючи її меншою за Ω_c . Очевидно, що величина $\mu = \frac{\pi}{\Omega}$ показує, у скільки разів швидкість передавання елементарних посилок через «ідеальний» фільтр зі смугою пропускання $(0, \Omega)$ за тривалістю $T = 1$ с більша за найквістову граничну швидкість для цього фільтра.

Як відомо, імпульсна реакція смуго-обмеженого каналу зі смугою пропускання $(0, \Omega)$ та його передатна функція $H(\omega)$ пов'язані співвідношенням

$$h_{\Omega}(t) = \frac{1}{2\pi} \int_{-\Omega}^{\Omega} H_{\Omega}(\omega) e^{i\omega t} d\omega. \quad (5.139)$$

Якщо на вхід такого каналу подати сигнал, що являє собою δ -імпульсну послідовність, то на його виході дістанемо напругу

$$z(k) = \sum_{l=-\infty}^{\infty} x_l h_{\Omega}(k-l), \quad k = 0; \pm 1; \dots, \quad H(\omega) = \begin{cases} 1 & |\omega| \leq \pi \\ 0 & |\omega| > \pi \end{cases}. \quad (5.140)$$

Отже, сигнал помилки при передаванні корисного сигналу визначається виразом

$$z(k) = \sum_{l=-\infty}^{\infty} x_l u(k-l) - \sum_{l=-\infty}^{\infty} x_l h_{\Omega}(k-l) = \sum_{l=-\infty}^{\infty} x_l [u(k-l) - h_{\Omega}(k-l)], \quad (5.141)$$

де $u(k) = \begin{cases} 1, & k = 0, \\ 0, & k \neq 0. \end{cases}$ – дискретна імпульсна реакція ідеального фільтра у

випадку, коли інтервал дискретизації дорівнює 1 с. Відзначимо, що при використанні умови

$$h_{\Omega}(0) = 1, \quad (5.142)$$

$$\frac{1}{2\pi} \int_{-\Omega}^{\Omega} H_{\Omega}(\omega) d\omega = 1. \quad (5.143)$$

Останнє співвідношення очевидно виходить із виразів (5.142) та (5.139).

Припустимо, що випадкова інформаційна послідовність $x(K)$ є стандартною в широкому розумінні і має автокореляційну функцію, чи, точніше, автокореляційну послідовність

$$B(m) = M \{x_n, x_{n+m}\}, \quad m = 0, \pm 1, \dots, \quad (5.144)$$

де M – операція усереднення за множиною реалізацій та нульовим математичним сподіванням. Енергетичний спектр (спектр густини потужності) розглядуваної випадкової залежності дорівнює

$$P(e^{i\omega}) = \sum_{m=-\infty}^{\infty} B(m) e^{-i\omega m}, \quad -\pi \leq \omega < \pi. \quad (5.145)$$

Відповідно до відомих співвідношень для перетворення енергетичного спектра лінійною системою, спектр густини потужності випадкової послідовності

$$Q(e^{i\omega}) = P(e^{i\omega}) |\sigma(e^{i\omega})|^2, \quad (5.146)$$

де

$$\sigma(e^{i\omega}) = \sum_{k=-\infty}^{\infty} [u(k) - h_{\Omega}(k)] e^{-i\omega k} = 1 - \sum_{k=-\infty}^{\infty} h_{\Omega}(k) e^{-i\omega k} = 1 - H_{\Omega}(e^{i\omega}), \quad (5.147)$$

$-\Omega \leq \omega \leq \Omega$

Причому, як відомо, спектр відліків імпульсної реакції

$$H_{\Omega}(e^{i\omega}) = \sum_{p=-\infty}^{\infty} H_{\Omega}(\omega - p2\pi). \quad (5.148)$$

Оскільки дисперсію випадкової послідовності можна знайти діленням на 2π її енергетичного спектра, дисперсія міжсимвольної завади, що нас цікавить, обчислюється за допомогою наступного співвідношення, що випливає з рівностей (5.145) та (5.147):

$$\sigma_z^2 = \frac{1}{\pi} \int_{-\pi}^{\pi} Q(e^{i\omega}) d\omega = \frac{1}{2\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) \left[1 - \sum_{p=-\infty}^{\infty} H_{\Omega}(\omega - p2\pi) \right]^2 d\omega. \quad (5.149)$$

Оскільки, за припущенням $H_{\Omega}(\omega) = 0$ при $|\omega| > \Omega$ на величину інтеграла в останньому виразі впливає лише один доданок нескінченної суми (при $p = 0$). У зв'язку з чим величину (5.149) можна перетворити до вигляду

$$\sigma_z^2 = \frac{1}{2\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) [1 - H_{\Omega}(\omega)]^2 d\omega \quad (5.150)$$

З урахуванням парності підінтегрального виразу з формули (5.150) та смугової обмеженості $H_{\Omega}(\omega)$, можемо записати остаточно

$$\sigma_z^2 = \frac{1}{\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) [1 - H_{\Omega}(\omega)]^2 d\omega + \frac{1}{\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) d\omega. \quad (5.151)$$

Оцінимо значення σ_z^2 для випадку передавання так званого випадкового телеграфного сигналу, який набуває з однаковою ймовірністю два можливих значення (+1) та (-1) і має функцію автокореляції

$$B(\tau) = e^{-2\lambda_0|\tau|}, \quad -\infty < \tau < \infty, \quad (5.152)$$

де λ_0 – середнє число перетинів нульового рівня за одиницю часу.

Енергетичний спектр

$$P(\omega) = \int_{-\infty}^{\infty} B(\tau) e^{-i\omega\tau} d\tau = \frac{4\lambda_0}{4\lambda_0 + \omega^2}; \quad -\infty < \omega < \infty. \quad (5.153)$$

Оскільки кореляційна послідовність відліків випадкового телеграфного сигналу має вигляд $B(m) = e^{-2\lambda_0|m|}$, $m = 0, \pm 1, \dots$, а її дискретне перетворення Фур'є (спектр густини потужності)

$$P(e^{i\omega}) = \sum_{p=-\infty}^{\infty} P(\omega - p2\pi) = \frac{4\lambda_0}{4\lambda_0 + (\omega - p2\pi)^2} \sum_{p=-\infty}^{\infty}, \quad -\pi \leq \omega < \pi, \quad (5.154)$$

то можна показати, що

$$\sigma_{z_1}^2 = \frac{(1 - \pi / \Omega)^2}{\pi \lambda_0} \int_0^{\Omega} \sum_{p=-\infty}^{\infty} \frac{1}{1 + \left[\frac{\omega - p2\pi}{2\lambda_0} \right]^2} d\omega + \frac{1}{\pi \lambda_0} \int_{\Omega}^{\pi} \sum_{p=-\infty}^{\infty} \frac{1}{1 + \left[\frac{\omega - p2\pi}{2\lambda_0} \right]^2} d\omega \quad (5.155)$$

При розрахунках за формулою (5.155) з'являється похибка через скінченні значення членів суми, яку визначають за виразом

$$\begin{aligned} \xi^2(n) &= \frac{(1 - \pi / \Omega)^2}{\pi \lambda_0} \int_0^{\Omega} \frac{2\lambda_0^2}{\pi^2} \left(\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right) d\omega + \frac{1}{\pi \lambda_0} \int_{\Omega}^{\pi} \frac{2\lambda_0}{\pi^2} \left(\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right) d\omega = \\ &= \frac{2\lambda_0(\pi - \Omega)}{\pi^2 \Omega} \left[\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right]. \end{aligned} \quad (5.156)$$

Амплітуда міжсимвольної завади визначається

$$u_{мз} = \sqrt{\sigma_z^2}. \quad (5.157)$$

Величина $\pi / \Omega = \mu$ показує, у скільки разів швидкість передавання посилок більша за найквістову граничну швидкість для даного каналу.

Абсолютне значення похибки для дисперсії, яку визначають за виразом (5.157), становить 5 ... 10%.

Результати розрахунків σ^2 та $u_{мз}$ при $\lambda = 0,4$ за формулами (5.141) та (5.143) наведено нижче:

m	1,1	1,2	1,4	1,6,
s_2	0,04	0,1	0,18	0,42,
$u_{мс}$	0,2	0,32	0,42	0,64.

Якщо для розглядуваного каналу зв'язку відношення сигнал/завада має певне значення $h = \frac{u_c}{u_3}$, то з урахуванням міжсимвольної інтерференції, викликаної поза-найквістовою швидкістю передавання, зменшенням сигналу в $\sqrt{\mu}$ разів, відношення сигнал/завада

$$h^* = \frac{u_c}{\sqrt{\mu(u_3^2 + u_{мз}^2)}}. \quad (5.158)$$

Як бачимо, відношення сигнал/шум в каналі зменшується через з'явлену міжсимвольну інтерференцію. Це зменшення ілюструється графіком $h^* = f(h)$ для різних μ (див. рис. 5.11).

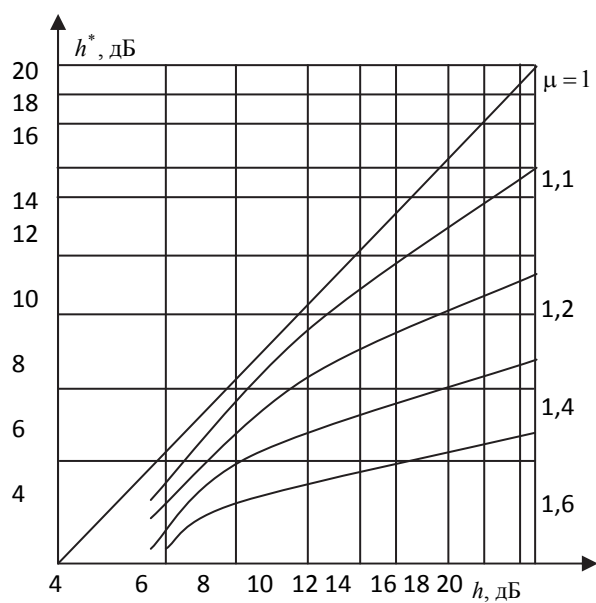


Рисунок 5.11 – Вплив флукуційного шуму на момент спрацьовування безінерційного реле

Наслідком зниження величини відношення сигнал/шум є зменшення завадостійкості переданої інформації. На графіках рис. 5.12 показано залежність ймовірності помилкового приймання елемента p_e , визначену для двійкової системи передавання з ЧМ за когерентного приймання відповідно до виразу

$$p_e = \left[1 - \Phi(h^*) \right], \quad (5.159)$$

де $\Phi(h^*)$ – функція Крампа. На рис. 5.12 показана залежність ймовірності помилки елемента за рахунок його скорочення в μ разів, а на рис. 5.13 – з урахуванням міжсимвольних спотворень при зростанні μ .

Передаванню зі швидкістю, яка дорівнює граничній швидкості Найквіста, відповідає лінія $p_n = f(p_n(\mu = 1))$.

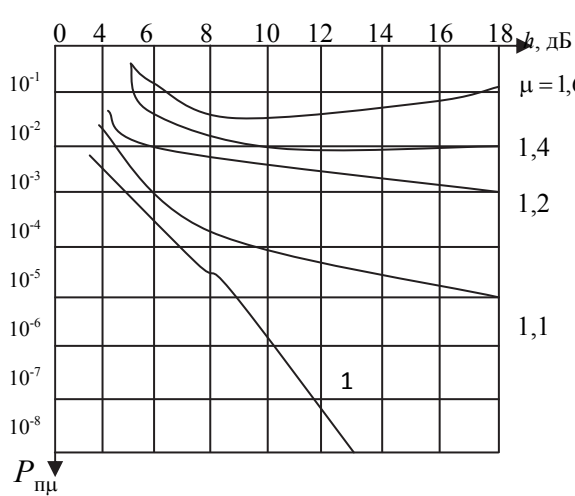


Рисунок 5.12 – Графік залежності ймовірності помилкового приймання елемента

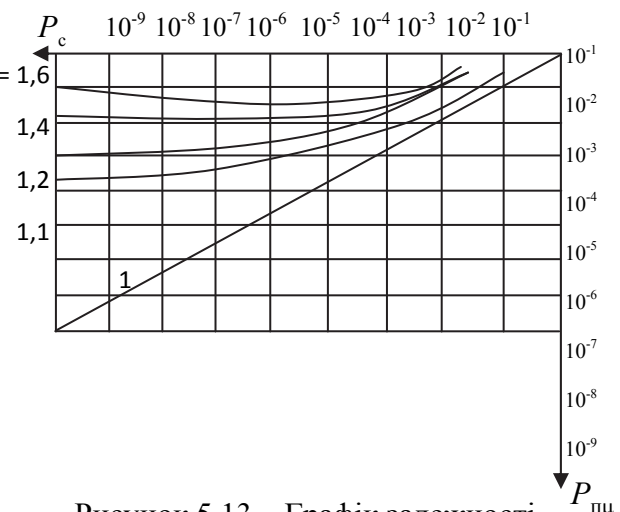


Рисунок 5.13 – Графік залежності ймовірності помилки елемента

Залежності $p_{пц} = f(p_e)$ для $\mu = 1,1; 1,2; 1,4; 1,6$ лежать вище за пряму $p_{пц} = |p_e|$, що саме й свідчить про зменшення завадостійкості. Слід підкреслити, що втрати завадостійкості тим більші, чим вище μ .

З іншого боку, збільшення швидкості передавання утворює можливість сформуванню на тому самому часовому інтервалі, що й раніше, більшу кількість реалізацій, тобто утворити можливості для збільшення пропускної здатності каналу:

$$C = \mu \left[1 + p_n \log_2 p_n + (1 - p_n) \log_2 (1 - p_n) \right]. \quad (5.160)$$

На рис. 5.14 наведено залежності $C = f(\mu)$ для значень $h = 2; 3; 4; 5$. Таким чином, показано, що зменшення тривалості елементарних сигналів за розрядно-цифрового кодування по відношенню до найквістового елемента в μ разів приводить до збільшення пропускної здатності каналу зв'язку, з одного боку, і до зменшення завадостійкості – з іншого боку. В зв'язку з цим доцільно дослідити можливості використання зекономленого

за час передавання однієї кодової комбінації розрядно-цифрового коду часового інтервалу для введення надлишковості з метою підвищення завадостійкості. Наприклад, при $\mu = 1,2$ на інтервалі $T_c = 10t_0$ довжина нової кодової комбінації становитиме $n(\mu) = 12$ елементів, $\tau_1 = \tau_0/\mu$, при цьому до 10 використаних раніше інформаційних розрядів додаються $r = 2$ надлишкових. Знаючи величину $n(\mu)$ та r , можна знайти мінімальну кодову відстань d_{\min} , що визначає коригуючі здатності коду.

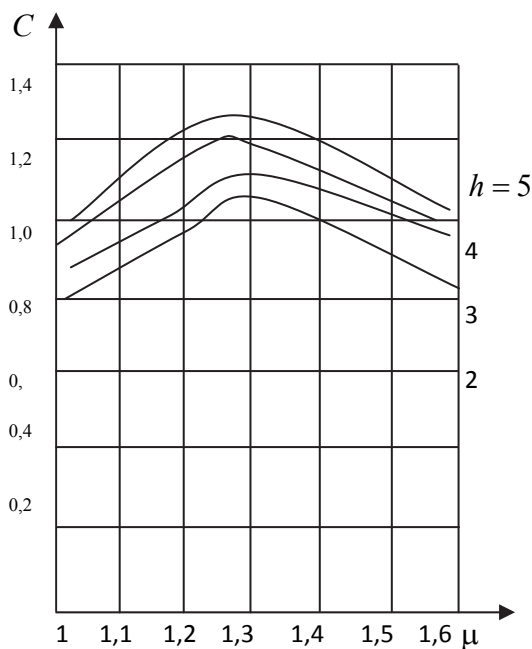


Рисунок 5.14 – Залежності $C = f(\mu)$

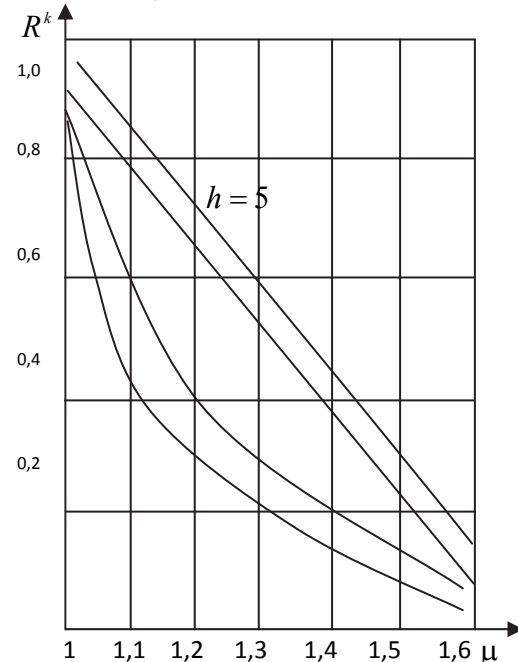


Рисунок 5.15 – Графіки залежностей $R^k = f(\mu)$

У табл. 5.8 подано значення параметрів $n(\mu)$, r , d_{\min} та t_b надлишкових кодів для різних значень μ .

Таблиця 5.8 - Значення параметрів надлишкових кодів для різних значень μ

Параметри	μ			
	1,1	1,2	1,4	1,6
$n(\mu)$	11	12	14	16
r	1	2	4	6
d_{\min}	2	2	3	4
t_b	1	1	2	3

Як відомо, ефективність надлишкового коду можна оцінити за допомогою ефективної ймовірності помилкового приймання елемента

$p'_{\text{пц}} = p_{\text{пц}} / n(\mu)$, де $p_{\text{пц}}$ – ймовірність помилкового приймання кодової

комбінації коду, який використовує елементарний сигнал $\tau_1 = \tau_0 / \mu$. Для кодів, що виявляють помилки,

$$p_{\text{пц}} = \sum_{i=d_{\text{min}}}^{n(\mu)} C_{n(\mu)}^i p_{\text{пц}}^i (1 - p_{\text{пц}})^{n(\mu)-i}, \quad (5.161)$$

а для кодів, що виправляють помилки кратності $t_{\text{вп}}$,

$$p_{\text{пц}} = \sum_{i=t_{\text{вп}}+1}^{n(\mu)} C_{n(\mu)}^i p_{\text{пц}}^i (1 - p_{\text{пц}})^{n(\mu)-i}. \quad (5.162)$$

На рис. 5.15 показана залежність швидкості передавання R^k від μ з урахуванням числа надлишкових елементів згідно з табл. 5.8.

Як бачимо, застосування кодів, що виправляють помилки за рахунок найквістової швидкості модуляції, зменшує ймовірність помилкового приймання елемента, але не компенсує втрату завадостійкості повністю.

Таким чином, застосування понаднайквістової швидкості модуляції з метою збільшення швидкості передавання не дає бажаного ефекту завдяки виникненню додаткової завади у вигляді міжсимвольної інтерференції.

5.7. Ефективність корегуючи ТСК в адаптивних системах з вирішальним зворотним зв'язком (ВЗЗ)

Передавання сигналів запиту та повторювання кодових слів створює надлишковість в системах з ВЗЗ і змінює середню швидкість передавання інформації порівняно з системами зв'язку одnobічної дії. Оцінювання впливу завад та запізнювання сигналів зводиться до відшукування залежностей

$$\begin{aligned} P_{0\text{к}} &= f(P_{\text{в.п}}, P_{\text{нп}}, q_{\text{в.з}}, \mu_0, N_{\text{кп}}); \\ \bar{\mu} &= f(P_{\text{в.п}}, P_{\text{нп}}, q_{\text{в.з}}, q_{\text{з.з}}, \mu_0, N_{\text{кп}}), \end{aligned} \quad (5.163)$$

де $P_{0\text{к}}$ – ймовірність спотворювання кодового слова; $P_{\text{в.п}}, P_{\text{нп}}$ – ймовірності з'явлення помилок, виявлюваних та невиявлювальних у прямому каналі; $q_{\text{з.з}}, q_{\text{в.з}}$ – ймовірності зникнення та виникнення нового помилкового сигналу запиту в зворотному каналі; $N_{\text{кп}}$ – кількість повторюваних кодових послідовностей, витрачених на виправлення помилки; $\bar{\mu}$ – середнє значення числа повторюваних кодових слів на одне запрошення.

Процес передавання інформації в системах з ВЗЗ відрізняється значною складністю. Тому нерідко впроваджують спрощені припущення стосовно логіки роботи системи, впливу завад та запізнювання сигналів та ін. Найбільш серйозним за своїми наслідками є припущення про ідеальний зворотний зв'язок: воно призводить до помилок в оцінюванні технічних показників систем, зростаючих зі збільшенням рівня завад, швидкості передавання та протяжності каналів зв'язку.

Як приклад оцінимо завадостійкість та швидкість передавання інформації в системі з безінерційним ВЗЗ. За відсутності завад у зворотному каналі безпомилковість передачі визначається можливістю з'явлення невиявлюваних помилок. Тому ймовірність

$$P_{0K_1} = P_{н.в} + \sum_{v=1}^{\infty} P_{в.п}^v P_{н.п} = P_{н.п} \sum_{v=1}^{\infty} P_{в.п}^v = \frac{P_{н.п}}{1 - P_{в.п}}. \quad (5.164)$$

В разі виявлення помилок у прямому каналі та придушення сигналу в зворотному каналі станція А продовжуватиме передавати наступні слова, тоді як реєструвальний пристрій станції В блокується на час $T_{\text{бл}} = N_{к.п} T_k$, де T_k – тривалість кодового слова. Як наслідок слова, які надходять впродовж часу блокування $T_{\text{бл}}$, втрачаються, що є еквівалентно до їхнього спотворення з імовірністю

$$\begin{aligned} P_{0K_2} &= N_{к.п} = \left(\frac{P_{в.п}}{N_{к.п}} + \frac{P_{в.п}^2}{N_{к.п}^2} + \frac{P_{в.п}^3}{N_{к.п}^3} + \dots \right) q_{3.3} = \\ &= N_{к.п} \left[\sum_{v=0}^{\infty} \frac{P_{в.п}^v}{N_{к.п}^v} - 1 \right] q_{3.3} = N_{к.п} q_{3.3} \frac{P_{в.п}}{N_{к.п} - P_{в.п}}. \end{aligned} \quad (5.165)$$

У цьому виразі враховано, що за довжини циклу повторювання $N_{к.п} T_k$ ймовірність виявлення помилки зменшується в $N_{к.п}$ разів через зменшення в $N_{к.п}$ разів кількості перевірочних елементів повідомлення. Тоді повна ймовірність помилки

$$P_{0к} = P_{0K_1} + P_{0K_2} = \left[1 + \left(\frac{1 - P_{в.п}}{N_{к.п} - P_{в.п}} \right) \frac{P_{в.п} q_{3.3}}{P_{н.п}} N_{к.п} \right] P_{0K_1} \left(\frac{P_{н.п}}{1 - P_{в.п}} \right). \quad (5.166)$$

Якщо за сигнал $S_{п}$ використовується одне з дозволених кодових слів, то $P_{н.п} = q_{3.3}$ та ймовірність

$$P_{0к} = \left(1 + \frac{1 - P_{в.п}}{N_{к.п} - P_{в.п}} N_{к.п} P_{в.п} \right) P_{0K_1}. \quad (5.167)$$

У реальних каналах $P_{в.п} \ll 1$ та ймовірність $P_{0к} \approx P_{0K_1}$.

Позначимо через $T_{к.о}$ середню тривалість сигналів у системі з ВЗЗ із врахуванням їхнього повторення. Величина

$$T_{к.о} = T_k + N_{к.п} T_k P_{в.п} + N_{к.п} T_k P_{в.п}^2 + \dots = T_k \left(1 + \frac{P_{в.п}}{1 - P_{в.п}} N_{к.п} \right) > T_k. \quad (5.168)$$

Коефіцієнт

$$\eta_v = \frac{T_{к.о}}{T_k} = \frac{1 + (N_{к.п} - 1) P_{в.п}}{1 - P_{в.п}} \quad (5.169)$$

характеризує збільшення часу (зниження швидкості) передавання інформації в системах зі зворотним зв'язком порівняно з односторонніми

системами. Коефіцієнт η_9 зменшується зі збільшенням імовірності $P_{в.п}$ та зменшенням запізнення сигналів.

Ефективність використання каналу при застосуванні виявлювального коду буде

$$\eta = \frac{m}{n} \frac{(1-p_0)^n + p_0}{1 + N_{к.п} [1 - (1-p_e)^n - p_e]}. \quad (5.170)$$

Надлишковість систем з ВЗЗ. За аналогією із завадостійкими кодами надлишковість у системах з ВЗЗ можна схарактеризувати коефіцієнтом повної надлишковості

$$R_{зб} = \frac{\bar{n}_0 - m}{\bar{n}_0}, \quad (5.171)$$

де \bar{n}_0 – середня кількість кодових символів, витрачених в обох каналах на передавання k одиниць інформації. За нульової пропускної здатності зворотного каналу $\bar{n}_0 = \bar{n}_1$, де \bar{n}_1 – середня кількість кодових символів, витрачених у прямому каналі на передавання k одиниць інформації. За відсутності повторювання $\bar{n}_1 = n$ та $R_{зб} = \frac{m}{n}$. Величина $R_{зб}$ залежить від типу зворотного зв'язку та логіки роботи системи.

Коефіцієнт $R_{зб}$ можна подати у вигляді

$$R_{зб} = R_{зк} + R_{зп} = \frac{n_1 - n}{\bar{n}_0} + \frac{\bar{n}_п}{\bar{n}_0}, \quad (5.172)$$

де $R_{зк}$ – коефіцієнт надлишковості, зумовлений завадостійким кодуванням за однократного передавання кодового слова; $R_{зп}$ – коефіцієнт збитковості, зумовлений повторенням спотворених кодових слів; n_1 – кількість кодових символів, витрачених в одному циклі роботи на передавання k одиниць інформації з урахуванням сигналів корекції; $\bar{n}_п$ – середня кількість кодових символів, витрачених на виправлення виявленої помилки при повторенні сигналів з урахуванням їхнього запізнення й логіки роботи системи.

У системах з ВЗЗ, де зменшення ємності зворотного каналу за рахунок надсилання сигналу запиту часто можна не враховувати, за позначкової перевірки $n_1 = n$, $n_0 = n_1$ та коефіцієнти

$$R_{зк} = \frac{n - m}{n + (\bar{\mu} - 1)m_0}; \quad R_{зп} = \frac{(\bar{\mu} - 1)}{m + (\bar{\mu} - 1)m_0}, \quad (5.173)$$

де $m_0 = nN_{к.п}$ – загальна кількість кодових символів, витрачених на виправлення виявленої помилки за кожного повторювання.

За рахунок збиткових кодових символів та повторення сигналів швидкість передавання інформації знижується відповідно у

$$\eta_{91} = \frac{n_1}{m} = \frac{n}{m} \text{ та } \eta_{92} = \frac{\bar{n}_1}{n_1} = \frac{n + (\mu - 1)m_0}{n} \quad (5.174)$$

разів. Тому коефіцієнт

$$\eta_9 = \eta_{91} \eta_{92} = \frac{1}{1 - R_{36}} = \frac{n + (\mu - 1)m_0}{m}. \quad (5.175)$$

Тоді коефіцієнт надлишковості у системі з ВЗЗ

$$R_{36} = 1 - \frac{k}{n + (\bar{\mu} - 1)m_0} = 1 - \frac{m}{n[1 + (\bar{\mu} - 1)N_{к.п}]}. \quad (5.176)$$

Вирази (5.173) та (5.176) є справедливими також за посимвольної та групової перевірок. За $\bar{n}_0 = \bar{n}_1$ та посимвольної перевірки $R_{3,к} = 0$ та $R_{36} = R_{3,п}$, що свідчить про добре узгодження джерела з каналом. Цьому режимові роботи відповідають найменші порівняно з іншими видами перевірок значення $\bar{\mu}$ та m_0 .

Аналіз систем з ВЗЗ показує, що швидкість передавання R може змінюватися і є функцією двох коефіцієнтів: кодової швидкості γ_k і коефіцієнт повторення γ_p :

$$R_{ср} = K = \gamma_k \cdot \gamma_p = \frac{m}{n} \cdot \frac{1}{1 + \frac{M \cdot P_{ст}(n)}{1 - P_{ст}(n)}}, \quad (5.177)$$

де m – кількість інформаційних елементів у кодовому слові довжиною n -елементів, M – кількість повторюваних кодових слів при одному повторенні.

При виборі коригуючого позиційного коду для систем з ВЗЗ необхідно пам'ятати, що підвищення імовірності використовується груповий (n, m) -код, і після декодування можливі три різні результати:

- видається кодова комбінація, ідентична переданій ($P_{пр}(n)$);
- видається кодова комбінація, відмінна від переданої ($P_{пом}(n)$);
- формується сигнал стирання (комбінація з виявленою помилкою ($P_{ст}(n)$)).

Ці три імовірності складають повну групу подій і тому

$$P_{пр}(n) + P_{пом}(n) + P_{ст}(n) = 1,$$

при чому імовіроності $P_{пр}(n)$, $P_{пом}(n)$ та $P_{ст}(n)$ визначають корегувальні властивості (n, m) -кодів.

В табл. 5.9 і 5.10 приведено результати вимірювання основних параметрів систем із зворотнім зв'язком при корегувальних кодах з елементністю кодових слів $n \in 15, 31, 63, 127$ при значеннях додаткових елементів $k \in 5, 7$ для двох каналів зв'язку: $P_{n1} = 7 \cdot 10^{-4}$, $\alpha_1 = 0,545$; $P_{n2} = 1,98 \cdot 10^{-3}$, $\alpha_2 = 0,318$, де α – коефіцієнт групування.

Таблиця 5.9 – Основні параметри системи із зворотнім зв'язком

n	$n-m$	d_{\min}	$p(\geq 1, n) \cdot 10^{-3}$	$P_{\text{пом.екс}} \cdot 10^{-5}$	$h = \frac{P(\geq 1, n)}{P[(> t_{\text{об}} + 1); n]}$	$R = \frac{m}{n}$	$R_{\text{експ}}$	$\Delta_{\text{повт}}$
15	5	3	2,49	4,25	57,17	0,666	0,66	0,006
	7	4		1,14	213	0,53	0,527	0,003
31	5	3	3,22	1,24	253	0,83	0,825	0,075
	7	5		0,21	1500	0,774	0,763	0,011
63	7	3	4,53	2,07	218	0,888	0,894	0,06
127	7	3	5,6	4,42	126	0,94	0,874	0,066

Об'єм вибірки $25128 \cdot 10^3$ – символів, $P_{n2} = 1,98 \cdot 10^{-3}$, $\alpha_2 = 0,318$.

Таблиця 5.10 – Основні параметри системи із зворотнім зв'язком

n	$n-m$	d_{\min}	$p(\geq 1, n) \cdot 10^{-3}$	$P_{\text{пом.екс}} \cdot 10^{-5}$	$h = \frac{P(\geq 1, n)}{P[(> t_{\text{об}} + 1); n]}$	$R = \frac{m}{n}$	$R_{\text{експ}}$	$\Delta_{\text{повт}}$
15	5	3	7,82	11,3	500	0,666	0,635	0,025
	7	4		1,49	827	0,527	0,507	0,027
31	5	3	13,2	21,5	61,4	0,838	0,770	0,068
	7	5		4,49	293	0,774	0,710	0,064
63	7	3	22,9	1,35	1696	0,888	0,775	0,113
127	7	3	39,6	8,54	126	0,94	0,763	0,177

Аналіз проведених розрахунків дозволяє зробити висновки:

- наявність зворотнього каналу забезпечує синтез позиційних коригуючих кодів, які збільшують якість передачі в діапазоні від декількох десятків разів, до декількох сотень (в залежності від параметрів завад в каналі);

- із збільшенням елементності кодового слова виправляюча ефективність позиційного коду збільшується від 0,66 до 0,94;

- втрати на повторення змінюються від частки процентів до десятків процентів в залежності від структури коду і параметрів завад;

- кодова відстань наведена в табл. 5.9 та 5.10 дозволяє виявляти в основному 2-х кратні помилки.

Збільшення мінімальної кодової відстані веде до збільшення коефіцієнта ефективності за рахунок суттєвого зменшення кодової швидкості передачі. Наприклад, при $n = 127$ і виявленні помилок кратності 13 число інформаційних елементів буде 85, а ефективна швидкість

складатиме $\sqrt{R} = \frac{85}{127} = 0,66$ в порівнянні з наведеною в таблицях 0,94.

Розглянемо ефективність використання коригуючих таймерних сигналів для коду $n = 15$ $m = 8$ ($r \in n - m = k = 7$) табл. 5.9. Інформаційна частина цього коду відповідає одному байту. Основна відмінність таймерних сигнальних конструкцій від кодових слів позиційного кодування полягає в відсутності розподілу значущих моментів модуляції на інформаційні та коригуючі (додаткові). Кожне кодове слово складається

з декількох “ i ” значущих моментів модуляції (ЗММ), інтервали між якими i передають інформацію відносно передаваного символу.

На рис. 5.16 представлено декілька таймерних кодових конструкцій з трьома ЗММ:

- 1) кодове слово при позиційному кодуванні ($T_{СК} = 5t_0$);
- 2) таймерне кодове слово з трьома ЗМВ з інтервалами кратними t_0 ;
- 3) Таймерне кодове слово при $i = 3$ з інтервалами між суміжними ЗММ $\tau_{ci} = t_0 + k\Delta$; $k \in 1 \dots c$.
- 4) четверте кодове слово ТСК із зміщенням двох ЗММ на величину Δ .

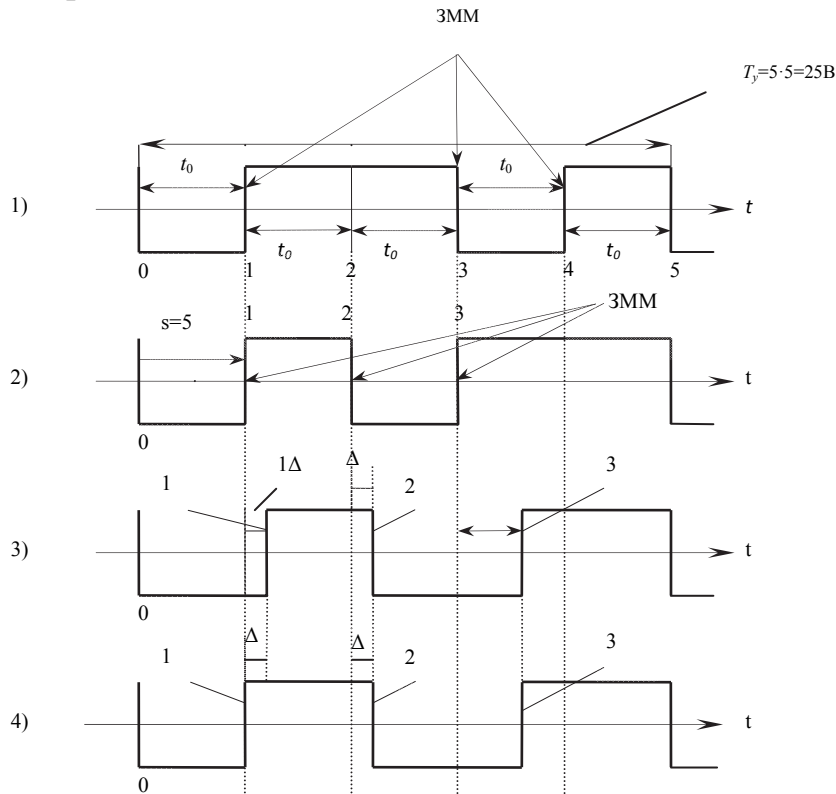


Рисунок 5.16 – Структура таймерних сигнальних конструкцій при $i = 3$, $s = 5$

Таким чином в таймерних конструкціях відстань між суміжними ЗММ визначається:

$$\tau_{i,i+1} = t_0 + \Delta k \quad (k \in 0, 1, 2, 3) \quad (5.178)$$

Перший додаток в виразі (5.178) забезпечує відсутність міжсимвольних завад в даному КС, а другий забезпечує зменшення мінімальної відстані між кодовими конструкціями до величини Δ .

Аналізуючи потужності таймерних кодових слів при заданому інтервалі реалізації слід визначити:

1. Задане число значущих моментів модуляції (ЗММ) i в кодовому слові синтезованому на інтервалі t елементів довжиною t_0 впливає на потужність множини ТСК реалізованих на інтервалі $T = mt_0$.

2. Інтервал Δ забезпечує необхідну мінімальну імовірність помилкового приймання в «хорошому» стані каналу $\tau_c \geq t_0 + z\Delta$ ($z \in 1, 2, 3, \dots$) і визначає мінімальну енергетичну відстань між КСК.

3. Реалізована на інтервалі $T_k = mt_0$ множина є нелінійна, так як не завжди сума двох ТСК утворює нову ТСК, яка відповідає рівнянню (5.178).

Таким чином інформація відносно переданого десятинного числа в ТСК визначається довжинами декількох (i) відтинків сигналів τ_i між суміжними ЗММ і їх взаємними положеннями.

Для сигналів з вказаними властивостями одержані основні параметри.

Потужність множини (число реалізацій):

$$N_p = F(m, s, i) = \frac{[s(m-i) + i]!}{i! [s(m-i)]!} \quad (5.179)$$

Максимальна кількість інформації, яка передається на інтервалі одного найквістового елемента t_0 :

$$V = \frac{[s(m-i) + i]!}{mi! [s(m-i)]!} \quad (5.180)$$

В табл. 5.11 представлено максимальні значення питомої ваги інформації на один найквістовий елемент для ТСК з $i=3$ при $m = 4; 5; 7; 10$ обрхованих згідно рівнянь (5.179), (5.180).

Таблиця 5.11 – Значення питомої ваги інформації на один найквістовий елемент

$m \backslash S$	2	3	4	5	6	7	8	9	10
4	0,83	1,08	1,282	1,452	1,598	1,727	1,842	1,945	2,04
5	1,026	1,278	1,473	1,632	1,766	1,882	1,984	2,075	2,158
7	1,052	1,261	1,417	1,541	1,645	1,733	1,811	1,88	1,942
10	0,941	1,098	1,213	1,304	1,379	1,443	1,499	1,548	1,592

Із таблиці слідує, що при ($9 \leq m \leq 11$) питома вага на елемент більше двох, а при $m < 9$ зменшується.

З метою можливості оцінки якості прийому кодових конструкцій із загальної множини $N_{рт}$ для передачі вибираються тільки сигнальні конструкції, в яких відстані між суміжними ЗММ задовольняють умові:

$$A_1x_1 + A_2x_2 + A_3x_3 = 0 \pmod{A_0}, \quad (5.181)$$

де A_i – коефіцієнти (краще прості числа), які визначають відстань між кодовими словами; x_1, x_2, x_3 – відстань між суміжними ЗММ в конкретній ТСК (ці відстані краще обчислювати в елементах Δ); A_0 – модуль системи залишкових класів, який забезпечує необхідне число синдромів для виправлення помилок.

З метою оцінки параметрів окремих станів каналів міської телефонної мережі м. Одеси були проведені експерименти: передача даних проводилася зі швидкістю модуляції $B = 1000$ Бод при смузі пропускання $\Delta F = 1300$ Гц (величина ΔF більше швидкості модуляції на 30% з урахуванням нелінійності АЧХ і ФЧХ). З метою оцінки ефективності окремих синдромів для виправлення відповідних помилок на прийомі була забезпечена реєстрація всіх відхилень значущих моментів відновлення (ЗМВ) на прийомі. Сигнальні конструкції ТСК були синтезовані при $\Delta = 1/7 t_0$ ($\Delta = 0,1428 t_0$) з реєстрацією елементів Δ в середній частині кожного. Якість передачі оцінювалась перевіркою рівняння якості (5.181):

$$2x_1 + 3x_2 + 7x_3 = 0 \pmod{19}, \quad (5.182)$$

де: коефіцієнти 2; 3; 7 забезпечують відповідну відстань між кодовими словами; x_i – інформаційні відрізки ($i = 3$) сигналів відповідної ТСК; i – номери інформаційних відтинків: ($i = 3$).

Статистичні параметри одного фрагменту передачі наведені в табл. 5.11а.

Таблиця 5.11а - Статистичні параметри одного фрагменту передачі

Передано кодових слів	90000
Прийнято вірно КС	89349
Прийнято КС із зміною числа ЗМВ	133
Прийнято помилкові КС при наявності на прийомі 3-х ЗМВ серед яких один має зміщення на величину ($\theta = 1\Delta$)	518
В 133 КС прийнятих з дробленням не змінили місця модуляції сформовані на передачі ЗММ: - перший ЗММ - другий ЗММ - третій ЗММ	в 13 конструкціях в 52 конструкціях в 65 конструкціях
Зареєстровано кодових слів при $i = 3$ із $N(\theta > 1\Delta) = 0$	

З урахуванням одержаних статистичних параметрів оцінимо ймовірність вірного прийому ЗМВ в «хорошому» стані:

$$P_b = \frac{(90000 - 133) \cdot 3 - 518}{(90000 - 133) \cdot 3} = \frac{269083}{269601} = 0,9980.$$

Враховуючи, що в «хорошому» стані каналу появлялись зміщення в одному ЗМВ на величину, які виправляються синдромним методом, то помилка можлива лише у випадку завади, яка не змінює рівняння (5.182).

Ймовірність вірного прийому (в своїй зоні) визначається інтегралами ймовірностей:

$$P_b(\Delta) = 2 \frac{1}{\sqrt{2\sigma_0}} \int e^{-dz} = 2\Phi\left(\frac{\Delta}{2\sigma_0}\right) = 0,9980$$

$$2 \frac{1}{\sqrt{2\sigma_0}} \int_0^z e^{-t^2/2} dt = 2\Phi\left(\frac{\Delta}{2\sigma_0}\right),$$

де $\Phi(Z)$ – інтеграл імовірностей.

Для даного значення P_B параметр $Z = \Delta/2\sigma_0$ відповідає значенню $Z = 3,13$. Згідно таблиць інтеграла ймовірностей при $Z = 3,13$:

$$Z = \frac{\Delta}{2\sigma_0} = 3,13,$$

$$\sigma_0 = \frac{0,1428}{2 \cdot 3,13} = 0,022t_0.$$

Зважаючи на те, що для каналу з ЧМ $\sigma_0 = \frac{1}{4h}$, $\left(h = \frac{u_c}{u_{ш}}\right)$. Для даного

каналу $h = \frac{1}{4\sigma_0} = \frac{1}{0,088} = 11,36$, $h^2 = 129$. Дане перевищення сигналу

відповідає каналам моделі Гільберта.

Знаючи значення σ_0 і Δ визначимо імовірність зміщення ЗМВ на величину $0,5\Delta \leq \Theta_{зм} \leq 1,5\Delta$, що відповідає зміщенню на 1Δ .

$$P_{зм}(1\Delta) = \Phi(1,5\Delta) - \Phi(0,5\Delta) = 0,99999 - 0,9988 = 1,2 \cdot 10^{-3}$$

Згідно статистики експерименту кількість ЗМВ із зміщенням ($\theta = 1\Delta$) становить 518, тому $P_{зм}(1\Delta) = \frac{518}{(90000 - 133)3} = 1,92 \cdot 10^{-3}$, що в межах допустимої вірності.

Слід зазначити, що одержане значення $P_{зм}(1\Delta) = 1,1 \cdot 10^{-3}$ дозволяє розрахувати значення появи 2-х і 3-х зміщень ЗМВ на величину $\theta = 1\Delta$ в одному КС.

$$P_2 = C_3^2 (1,1 \cdot 10^{-3})^2 \cdot 0,9981 \approx 3,6 \cdot 10^{-6}$$

$$P_3(1\Delta) = C_3^3 (1,1 \cdot 10^{-3})^3 \approx 1,3 \cdot 10^{-9}$$

Імовірність розрахованих зміщень 2-х і 3-х ЗМВ в кодових словах на 3 і 6 порядків менша по відношенню до однократних.

В зв'язку з тим, що при позиційному кодуванні для $n = 15$ значення інформаційної частини коду ($m = 8$), то і при формуванні кодової таблиці ТСК необхідно передбачити можливість реалізації відповідної кодової множини $M_1 = 2^8 \cdot 19 = 4864$ кодових слів.

Всі ТСК множини M_1 мають по три ЗММ і тільки 256 із них задовольняють рівнянню якості. Слід звернути увагу, що кількість інформаційних відтинків ТСК в десятки і сотні разів менше елементності позиційного коду (n).

Слід звернути увагу на те, що число інформаційних відтинків ТСК в десятки і сотні разів менше елементності позиційного коду. Не виявленою

помилка рівняння якості буде тільки в тому випадку коли завада E проведе зміни стану відповідних координат так, що рівняння не буде порушено

$$\begin{cases} 2(x_1 + e_1) + 3(x_2 + e_2) + 7(x_3 + e_3) = 0(\text{mod}19) \\ 2x_1 + 3x_2 + 7x_3 = 0(\text{mod}19) \\ 2e_1 + 3e_2 + 7e_3 = 0(\text{mod}19) \end{cases} \quad (5.183)$$

Такими векторами, які не змінюють рівності можуть бути

$$E_0(1) \rightarrow \pm 3; \mp 2; 0 \text{ з вагою } W = 5;$$

$$E_0(2) \rightarrow \pm 2; \pm 1; \pm 1; 0 \text{ з вагою } W = 4;$$

$$E_0(3) \rightarrow \pm 1; 0; \pm 3 \text{ з вагою } W = 4.$$

З метою визначення співвідношення сигнал/шум в «хорошому» стані були проведені вимірювання числа викидів зміщень значущих моментів

відтворення за величину двох фіксованих зон ($\Delta = \frac{t_0}{14}$), ($\Delta = \frac{t_0}{25}$) при

роботі по каналу МТМ з частотною модуляцією з полозою $\Delta F = 1300$ Гц при швидкості модуляції $B = 1000$ Бод.

Таблиця 5.12 – Результати одного фрагменту одночасних вимірювань числа зміщень ЗМВ за вказаних зон при $T_c = 8t_0$

Величина зони Δ від t_0 , %	Число кодових слів	Число моментів модуляції $N_{\text{мом}}$	Число викидів $N(\theta > \Delta)$	$P_{\text{п}}$	σ_0
7,14	73676	294701	326	$1,106 \cdot 10^{-3}$	2,18
1	73676	294701	6982	$2,3 \cdot 10^{-2}$	1,86

За результатами статистики було визначено значення середньоквадратичного відхилення ЗМВ (σ).

$$P(\theta > \Delta) = \frac{2}{\sqrt{2\pi}} \int_{\Delta}^{t_0} \exp(-z^2 / 2) dz = 1 - 2\phi(z), \quad (5.184)$$

де $\phi(z)$ – інтеграл імовірності.

Підставимо значення $N(\theta > \Delta)$ і знаючи число ЗМВ в кодових словах отримуємо:

$$\Delta = 7,14\% \quad P(\theta > 7,14\% t_0) = 1 - 2\sigma(0,0714t_0) = 1,1 \cdot 10^{-3};$$

$$\sigma_1 = 2,18; \quad \sigma_2 = 1,86.$$

Так зміщення ЗМВ на виході каналу визначалось при наявності не тільки гауссівського шуму в «хорошому» стані, а і при перериваннях (комутований канал), число яких за час вимірювання більше ста, тим більше близьке до реального значення σ слід вважати те значення, при якому число викидів набагато більше числа переривань(занижень) сигналу в комутованому каналі, тобто при $\theta = 0,04t_0$ ($\sigma_2 = 1,86$).

Так для каналу з ЧМ середньоквадратичне відхилення функціонально зв'язане із співвідношенням сигнал/шум h

$$\sigma = \frac{1}{4h}. \quad (5.185)$$

Звідси, можна стверджувати, що на інтервалі «хорошого» стану $h \geq 10$, з цього виходить, що навіть при некогерентному прийомі $P_{\text{ex}} < (10^{-8} \div 10^{-9})$.

Якщо в «поганому» стані імовірність помилки прагне до 0,5 то середня імовірність помилкового прийому на виході каналу:

$$\bar{P} = k_{\text{п}} P_{\text{п}} + k_{\text{х}} P_{\text{х}} = 0,001 \cdot 0,5 + 0,99 \cdot 10^{-8} = 5 \cdot 10^{-3}, \quad (5.186)$$

де $k_{\text{х}}$, $k_{\text{п}}$ – відносна величина часу «поганого» і «хорошого» стану каналу.

Отже, отримані значення $P_{\text{п}}$ і $P_{\text{х}}$ показують, що канал, який досліджується описується моделлю Гільберта.

З сказаного вище, слідує, що запас стійкості в «хорошому» стані реального каналу зв'язку на 5-7 порядків менше середньої імовірності помилки.

Проведені численні експерименти на комутованих каналах міської мережі з використанням модему з ЧМ при базі сигналу $B = \Delta B \cdot t_0 = 1$ дозволяють зробити наступні висновки:

Середня кількість поганих станів на 1 годину змінюється для різних з'єднань від 150 до 1300 в залежності від смуги пропускання і виду комутаційного обладнання каналу ΔF (для каналу зі смугою $\Delta F_1 = 1000$ Гц $N \in 1100 \dots 1200$, а при $\Delta F_2 = 140$ Гц $N \in 140 \dots 160$).

Час перебування в «поганому» стані описується логарифмічним-нормальним законом з середнім значенням $\overline{\lg \tau_{\text{п}}}$, яке зменшується в 5-7 раз із збільшення смуги ΔF в 8-10 раз (для полоси $\Delta F_1 = 1000$ Гц $\overline{\lg \tau_{\text{п}}} = 1,775$, а для $\Delta F_2 = 140$ Гц $\overline{\lg \tau_{\text{п}}} = 8,45$).

Середнє значення спотворених елементів на кодове слово визначається, як правило, середнім значенням «поганого» стану і не суттєво змінюється від елементності КС.

Помилка на інтервалах часу «поганого» стану групується, закон розподілення їх на інтервалі 16 посилок після першої помилки апроксимується гіперекспонентою:

$$P_{\text{п}}(0+1) = \varepsilon_1 e^{-\lambda_1} + \varepsilon_2 e^{-\lambda_2} + \dots + \varepsilon_i e^{-\lambda_i} \quad i \in \dots 16, \quad (5.187)$$

де ε , λ – коефіцієнти, які визначаються каналом і вилом помилок (в границях перших 4-х посилок зосереджено 97,8% можливих реалізацій помилок).

Параметр завадостійкості $h^2 = \frac{U_c^2}{U_3^2}$ в «хорошому» стані для різних

каналів знаходиться в межах $h \in 100 \dots 180$, що в десятки разів більше параметра забезпечуючого середню імовірність помилки в каналі.

Середньоквадратичне відхилення σ_0 в хорошому стані каналу дають близькі результати ($\sigma_0 = (0,02 \div 0,023)t_0$; $\left(\frac{U_c}{U_3}\right)^2 > 180$), що відповідає моделі Гільберта.

Із наведених результатів розрахунку середньоквадратичного відхилення σ_0 в «хорошому» стані каналу дають близькі результати $\sigma_0 = (0,02 \div 0,023)t_0$; $\left(\frac{U_c}{U_3}\right)^2 > 180$, що відповідає моделі Гільберта.

Недоліком позиційного кодування являється значення мінімальної відстані між змінами інформаційного параметра. Воно може бути відмінним від найквістового елемента тривалістю $\tau_0 = t_0$. Так як мінімальний час між змінами інформаційного параметра не може бути менше найквістового елемента, то синхронні системи не можуть забезпечувати на обмеженому (заданому) інтервалі n -елементного коду число реалізацій $N_p > a^n$. Для вирішення цієї задачі необхідно змінити мінімальну кодову відстань між сигнальними конструкціями на величину $\Delta\tau_0 < t_0$, що реалізується в таймерних сигнальних конструкціях.

В третій частині даного посібника для оцінки ефективності коригуючих позиційних кодів введено коефіцієнт підвищення достовірності (η):

$$\eta = \frac{p(\geq 1, n)}{p(\geq 1, n) - P_B(n)},$$

де $p(\geq 1, n)$ – імовірність помилкового приймання кодового слова; $P_{B(n)}$ – імовірність виправленої частини помилок. Для порівняння позиційного та таймерного кодування необхідно знайти вказані вище імовірності для ТСК в «поганому» та «хорошому» станах каналу.

В якості позиційного коригуючого коду виберемо 15-елементний код (в якому на 8 інформаційних елементів додається 7 перевірючих забезпечуючих кодову відстань $d = 3$; 4. Позитивним в порівнянні двох методів кодування являється передача в кожній комбінації коригуючого коду 1 байта інформації.

Відмінність таймерних сигнальних конструкцій від сигналів позиційного кодування полягає в відсутності відстані між суміжними ЗММ елемента Найквіста t_0 , який визначається ефективною полосою передачі $\Delta F_{\text{кан}} (t_0 = \frac{1}{\Delta F})$. В запропонованих ТСК відстань між суміжними ЗММ кратна частині цього елемента $\Delta = \frac{t_0}{s}$ ($s \in 1, 2, \dots, s$). При формуванні кодової конструкції з метою зменшення міжсимвольних спотворень

відстань між суміжними ЗММ не може бути менше найквістового елемента:

$$\tau_i = s\Delta + k\Delta \quad k \in 1, 2, \dots, k;$$

де τ_i гарантує, що відстань не менше t_0 , а другий являється інформаційним.

Наявність двох складових в параметрі τ_i забезпечує довжину окремих відстаней між суміжними ЗММ в заданім кодовім слові не менше t_0 , і мінімальну відстань між різними кодовими словами простих ТСК рівною одному елементу Δ ($\Delta = \frac{t_0}{s}$).

Основними задачами при формуванні необхідної потужності множини простих ТСК являються:

- в множині, що формується, M_1 повинна бути підмножина M_2 кодових слів відповідаючих рівнянню 5.181 [$N_{\text{реал}}(M_2) = 2^8$];
- друга частина множини M_1 відповідає залишкам $P(\theta_{\text{зал}} \neq 0)$;
- число залишків в системі залишкових класів визначається модулем A_0 (один з яких узгоджується рівнянням якості 5.182);
- величина базового елемента A вибирається із розрахунку зміщення ЗМВ в «хорошому» стані каналу на величину $\theta_3 > 0,5\Delta$ з імовірністю не більше середнього значення помилкового приймання кодового слова.

Зважаючи, що кодове слово при позиційному коригуючому коді при $n = 15$ має 8 інформаційних елементів дорівнює $M_1 = 2^8 \cdot A_0 = 4864$, де $A_0 = 19$.

Із цієї кодової множини кодових слів необхідно вибрати тільки $2^8 = 256$ кодових слів, які задовольняють рівнянню якості 2.18а при коефіцієнтах $A_1 = 2$, $A_2 = 3$, $A_3 = 7$, а $A_0 = 19$.

Із додатка 7 виходить, що при $s = 7$; $i = 3$ на інтервалі $T = 7t_0$ можливо реалізувати 4495 кодових конструкцій, що на 369 реалізацій менше M_1 ($4864 - 4495 = 369$). В цьому розрахунку взято значення s , при якому проводився експеримент.

Оцінимо на скільки потрібно збільшити інтервал реалізації необхідної множини при якому потужність простого ТСК буде мінімально більшою від $M_1 = 4864$ (якщо не рівною). Одержана раніше аналітична залежність між потужністю множини конструкцій простих ТСК параметрами коду (m ; s ; i) має вид:

$$N_p = \frac{[m - s(s - 1)!]}{i![m - is]!}.$$

Так як при $s = 7$, $i = 3$ кожний елемент Найквіста відповідає ($t_0 \rightarrow 7\Delta$) семи елементам Δ , а інтервал $7\Delta = 49$.

Розрахуємо яку кількість реалізацій можливо отримати якщо $T_p = 7t_0 + \Delta = 7 \cdot 7 + \Delta = 50\Delta$,

$$\frac{[50 - 3(7 - 1)]}{3!29!} = \frac{30 \cdot 31 \cdot 32}{1 \cdot 2 \cdot 3} = 4960,$$

що на 96 реалізацій більше ($4960 - 4864 = 96$). Таким чином збільшення інтервалу реалізацій на 1Δ збільшило число реалізацій на ($4960 - 4495$) 465 реалізацій. Так, враховуючи, що в «поганому» стані каналу в реалізаціях змінюється число ЗМВ ($i \neq 3$), то оцінка прийнятого кодового слова по числу ЗМВ є надійним критерієм помилкового приймання.

Оцінимо імовірність невиявленої помилки при прийманні в «хорошому» стані каналу. Зрозуміло, що не виявленою може бути помилка коли вектор завади в зміщених окремих ЗМВ відповідає нульовому вектору, тобто зміщення окремих ЗМВ з урахуванням коефіцієнтів A_i породжують зміщення задовольняючих рівняння якості

$$A_1x_1 + A_2x_2 + A_3x_3 = 0 \pmod{A_0}.$$

Для прийнятих коефіцієнтів $A_1 = 2, A_2 = 3, A_3 = 7, A_0 = 19$, нульовими векторами можуть бути:

$$E_0(0) \rightarrow \pm 3; \pm 2; 0 \text{ з вагою } W = 5;$$

$$E_0(0) \rightarrow \pm 2; \pm 1; \mp 1; W = 4;$$

$$E_0(A_0) \rightarrow \mp 1; 0; \pm 3; W = 4.$$

Легко показати, що для гауссової завади в «хорошому» стані каналу:

$$P(1) = \Phi\left(\frac{1,5\Delta}{\sigma_0}\right) - \Phi\left(\frac{0,5\Delta}{\sigma_0}\right);$$

$$P(0) = 2\Phi\left(\frac{\Delta}{2\sigma_0}\right);$$

$$P(d-1) = \Phi\left[\frac{(d-0,5)\Delta}{\sigma_0}\right] - \Phi\left[\frac{(d-1,5)\Delta}{\sigma_0}\right];$$

де σ_0 – середнє квадратичне відхилення ЗМВ в «хорошому» стані каналу. Зрозуміло що при $\sigma_0 \approx 0,02t_0$ імовірність появи завад, які призводять до нульових векторів менше 10^{-7} таким чином передача за допомогою таймерних сигналів зменшує час передачі одного байта інформації в $\frac{15}{7,14} = 2,1$ рази із підвищенням якості передачі на 4 порядки.

Переходячи від систем із зворотним зв'язком, в яких наявність зворотного каналу дозволяє приймальній стороні інформувати відносно якості одержаного кодового слова, до симплексних систем.

5.8. Таймерні сигнальні конструкції як інструментарій укрупнення сигналів при блоковому кодуванні

Шеннонівська теорія інформації стверджує, що побудова хороших каналів зв'язку економічно недосяжна – вигідно використовувати коди, що

виправляють помилки. Революційні ідеї Шеннона викликали переворот в свідомості інженерів-зв'язківців – до публікації цієї теорії вважалось, що єдиною можливістю підвищення завадостійкості приймання сигналів в односторонніх (симплексних системах) є збільшення потужності передавача або багатократна передача одного й того ж повідомлення.

Багаточисленні роботи другої половини ХХ століття були направлені на вирішення наступних проблем позиційного блокового кодування:

- синтезу кодів з високими коригуючими властивостями;
- синтезу алгоритмів декодування при незначній складності;
- узгодження структури кодів, що корегують помилки, видів модуляції, алгоритмів декодування та характеристик каналів зв'язку.

В цьому напрямі каталізатором ланцюгової реакції появи нових блокових кодів були роботи М.Дж. Гоше, Р. Хемінга, І.С. Ріда, Г. Форні, В.Д. Колесника, Е.Т. Мирончикова. Американський вчений Д. Слепян одержав суттєві результати в розробці строгої теорії лінійних блокових кодів використовуючи математичну теорію груп. І незважаючи на значні досягнення в теорії синтезу корегуючих блокових кодів слід вважати, що питома вага перевірочних елементів в кодових словах на сьогодні є великою.

Статистична обробка результатів вимірювань дозволила визначити основні закономірності розподілу відстаней між помилковими кодовими словами:

- закон відстаней логарифмічно-нормальний;
- імовірність появи суміжних спотворених кодових слів (по два слова) – $(2...3) \cdot 10^{-5}$;
- імовірність суміжних спотворених кодових слів (три слова) – 10^{-5} .

Середнє значення логарифмів інтервалів в значеннях Δ між спотвореними кодовими словами $M(\ln l) = 10,89$. Середньоквадратичне відхилення $\delta(\ln(l)) = 0,33202$. Головним результатом проведених вимірювань є підтвердження факту, що всі спотворені таймерні кодові слова в «поганому» стані каналу призводять до збільшення значущих моментів відтворення в порівнянні з переданими.

З метою оцінки параметрів каналу в хорошому стані був проведений експеримент, що полягав в оцінці якості передачі таймерних структур з постійним числом значущих моментів модуляції (ЗММ).

Довжини сигналів τ_i між ЗММ складали

$$\tau_i = t_0 + i\Delta; \quad i \in 0 \div z, \quad 0 < z - \text{ціле число } t_0 = \frac{1}{2} \Delta F; \quad \Delta = \frac{t_0}{7}.$$

Результати передачі одного фрагменту по каналу МТМ з числом ЗММ в кодовому слові $i = 3$ наведені нижче:

- кількість переданих кодових слів – 90000;
- кількість прийнятих кодових слів із зміною кількості ЗММ – 133;

– кількість кодів слів із зміщенням одного ЗМВ на величину $\Delta - 512$;

– кількість зареєстрованих кодів слів із зміщенням двох ЗМВ на величину $(\theta = 1\Delta) - 14$.

Одержані результати експерименту свідчать, що ймовірність появи спотвореного кодового слова із зміною числа ЗМВ знаходиться в межах $(1,4 \dots 1,6) \cdot 10^{-3}$.

Користуючись межею Варшмова – Гільберта визначені границі оцінки числа додаткових елементів симплексних корегуючих кодів для $d \in (1 \dots 21)$ та $m \in (1 \dots 60)$, забезпечуючих відповідну ймовірність помилкового (вірного) приймання в «хорошому» стані каналу. Слід зауважити, що значний результат в підвищенні ефективності коригуючих позиційних кодів дає узгодження параметрів кодів з параметрами завод. При вирішенні проблеми узгодження завод та параметрів в коригуючих кодах необхідно враховувати, що число послідовностей довжини « n » з елементами із двійкового поля ваги i визначається

$$y_{ij} = \begin{cases} 0, & \text{при } i > j, \\ 0, & \text{при } i = 1, j > 1, \\ 1, & \text{при } i = 0, j = 0, \\ n, & \text{при } i = 1, j = 1, \\ C_{j-2}^{i-2}(n-j+1) & \text{при } i > 1, j \geq i. \end{cases}$$

Незважаючи на успіхи в теорії синтезу коригуючих блокових позиційних кодів слід відмітити що підвищити їх ефективність можливо тільки при елементності не менше $n \geq 100 \div 500$ при кодовій швидкості $R_k \geq 0,5$.

Для підвищення якості передачі символу в односторонніх системах часто використовується алгоритм i -кратного повторення кодового слова. Цей спосіб кодування заснований на μ -кратній передачі n -значних кодограм. При цьому найбільшого поширення набули два способи. При першому способі кожна кодограма X_j передається μ разів, у результаті чого послідовність символів має вигляд:

$$\frac{x_1 x_2 \dots x_n}{1} \quad \frac{x_1 x_2 \dots x_n}{2} \quad \frac{x_1 x_2 \dots x_n}{\mu}$$

Такий метод легко реалізується і, звичайно, використовується в каналах з параметрами, що швидко змінюються. Ефективність його обумовлена тим, що спотворення символів з однаковими номерами часто можна вважати статистично незалежними. Тому такий метод іноді називають кодуванням з декореляцією помилок.

При другому способі кожний символ кодограми передається n разів поспіль, і послідовність символів у каналі має вигляд:

$$\frac{x_1 \dots x_1}{\mu} \quad \frac{x_2 \dots x_2}{\mu} \quad \frac{x_3 \dots x_3}{\mu}.$$

Цей метод звичайно використовується в каналах з постійними параметрами, або в каналах, які повільно змінюються.

Кодова відстань не залежить від способу передачі й становить:

$$d_0(\mu) = \mu d_0,$$

де d_0 – мінімальна відстань між кодовими словами.

Двократне повторення можна розглядати як лінійний блоковий код з породжуючою й перевіркою матрицями:

$$G^{(2)} = \|E_n, E_n\|; \quad H^{(2)} = \left\| \begin{array}{c} E_n \\ E_n \end{array} \right\|,$$

де E_n – одинична матриця розміру n .

Як видно зі структури матриці $H^{(2)}$ такий код не дозволяє мажоритарне оброблення прийнятих кодових слів, тому що будь-який коректор відповідає двом векторам помилок. Проте код виявляє всі непарні помилки.

При трикратному повторенні кодового слова матриці коду будуть:

$$G^{(3)} = \|E_n E_n E_n\| \quad H^{(3)} = \left\| \begin{array}{c} E_{2n} \\ E_n E_n \end{array} \right\|,$$

де E_{2n} – одинична матриця розміру $2n$. Такий код допускає мажоритарне декодування за принципом «2 із 3». При цьому число помилок, що виправляються, ваги ν становить $3^\nu C_n^\nu$.

Результати оброблення кодограми за методом «2 із 3» еквівалентна символу, переданому один раз, але з імовірністю спотворення P_0^1 . Пов'язане це з тим, що ймовірність правильного прийому символу при трикратній передачі має складові:

$$q_{03} = (1 - p_0)^3 \quad q_{023} = C_3^2 p_0 (1 - p_0)^2.$$

Враховуючи, що

$$1 - p_0^1 = q_{02} + q_{023}$$

P_0^1 становитиме

$$p_0^1 = 3p_0^2 - 2p_0^3.$$

Останній вираз дозволяє оцінювати ймовірність помилки декодування при трикратному повторенні для кодових слів з надлишковістю при позиційному кодуванні.

З метою оцінки ефективності повторення кодових конструкцій, синтезованих на базі коригуючих таймерних сигналів була організована по тому ж каналу МТМ передача з двократним повторенням таймерних

кодових структур, в яких відстані між ЗММ задовольняють наступній умові:

$$A_1x_1 + A_2x_2 + A_3x_3 = 0(\text{mod } A_0)$$

при значущих коефіцієнтах A_i : $A_1 = 2$; $A_2 = 3$; $A_3 = 7$; $A_0 = 19$.

При 256 реалізаціях кодових слів з трьома ЗММ задовольняючих умові при значенні $S = 7$ достатньо інтервал реалізації інформаційної частини кодової конструкції $T_c = 7,5t_0$, на якому можливо реалізувати (256×19) простих ТСК. Враховуючи закон розподілу інтервалів між спотвореними кодовими словами (і його параметрів), ймовірність появи 2-х або 3-х спотворених суміжних конструкцій при експерименті в якості захисного інтервалу повторення вибрано інтервал $K = 4$ кодового слова.

З метою оцінки питомої ваги «плохого» та «хорошого» станів каналу, визначення алгоритмів оброблення сигналів при коригуючи ТСК з різними параметрами було закодовано три бінарні послідовності різної елементності при РЦК: $n_1 = 15$; $n_1 = 30$; $n_1 = 63$.

При цьому в першому випадку кодове слово складалося з 5 ЗММ; у другому – з 10; у третьому – з 21.

Для можливих визначень початку нового блоку в кінці передавалося по два відмінних за місцем знаходження інформаційних переходи, які виконували функцію кадрового синхросигналу.

Помилковим вважався блок, в якому

- будь-який з переходів змістився на величину $\delta > \Delta/2$;
- змінилося число переходів у сигнальній конструкції;
- спотворився кадровий синхросигнал.

Таблиця 5.13 – Результати вимірювань при передаванні кожного блока

Характер спотворень	$B = 200$ Бод			$B = 600$ Бод		
	$n = 17$	$n = 33$	$n = 65$	$n = 17$	$n = 33$	$n = 65$
$N_{п.б.}$	607	936	1583	448	720	11287
$N_{п.з.}$	351	452	777	297	431	617
$N(i+2)$	220	401	656	131	241	456
$N(i+4)$	25	69	102	17	31	78
$N_{др}$	445	470	758	1489	278	534
$N(i-x)$	3	5	9	2	4	7

Результати вимірювань при передаванні кожного блока 100000 разів при швидкості модуляції 200, 600 Бод для смуги $\Delta F = 700$ наведені в табл. 5.13 – 5.14.

В табл. 5.13 позначено: $N_{п.б.}$ – число одержаних помилкових блоків; $N_{п.з.}$ – число помилкових блоків, в яких відбулося зміщення ЗМВ на величину $0,5\Delta \leq \theta \leq 1,5\Delta$; $N(i+2)$ – число помилкових блоків, в яких

кількість переходів збільшилося на два; $N(i+4)$ – число помилкових блоків, в яких кількість переходів збільшилося на чотири; $N_{др}$ – число блоків, в яких є дроблення $t_d \leq t_0/2$; $N(i-x)$ – число блоків, в яких число переходів стало менше i .

В табл. 5.14 наведені частоти появи помилкових блоків зі зміщенням ЗМВ з урахуванням їхньої кратності при швидкостях $B = 200$ Бод, $B = 600$ Бод і зазначених довжинах блоків n .

Таблиця 5.14 – Частота появи помилкових блоків зі зміщення ЗМВ

Кратність зміщення	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
600, $n = 17$	224	60	10	3	-	-
600, $n = 33$	250	131	29	9	1	-
600, $n = 65$	368	181	55	12	1	-
600, $n = 17$	198	107	35	9	1	-
600, $n = 33$	246	145	52	12	2	-
200, $n = 65$	438	217	99	19	3	1

З цих таблиць слідує, що навіть для такого поганого каналу як комутований канал МТМ відносний час «поганого» стану менше $T_{II} \leq 0,01T_{пер}$.

Наприклад, при швидкості 600 Бод та довжині блока $n = 17$ спотворених сигналів ЗМВ з урахуванням кратності зміщень і дроблень $N_c = 623$.

Враховуючи, що при експерименті передано $N_{II} = 100000 \cdot 17 = 17 \cdot 10^5$ ЗММ. Вага помилкових сигналів складає $\frac{623}{17 \cdot 10^5} = 36 \cdot 10^{-5} < 0,01$.

Враховуючи, що в результаті експерименту через зміщення число спотворених ЗМВ лише

$$224 \times 1 + 60 \times 2 + 10 \times 3 + 3 \times 4 = 386.$$

З урахуванням значень $\Delta = \frac{1}{s} t_0 = \frac{1}{7} t_0 = 0,14 t_0$ для ймовірності помилкового приймання ЗМВ маємо $p_{оз}$:

$$p_{оз} = 0,5 - \Phi\left(\frac{\Delta}{2\sigma}\right) = \frac{386}{17 \cdot 10^5} = 2,3 \cdot 10^{-4},$$

$$\Phi\left(\frac{\Delta}{2\sigma}\right) = 0,4996,$$

$$\frac{\Delta}{2\sigma} = 4; \quad \sigma = \frac{\Delta}{8} = \frac{0,14 t_0}{8} = 0,017 t_0.$$

Встановлено, що для каналу з ЧМ $\sigma = \frac{1}{4h}$; $h = \frac{u_c}{u_{ш}} > 12$ ($h^2 > 120$, що

відповідає моделі Гільберта).

В табл. 5.16 наведено значення імовірності вірного приймання повторюваного кодового слова після переданого з спотворенням.

Безумовну сумісну ймовірність помилки для двох кодових слів, що повторюються через i кодових слів, подано нижче:

	$i = 0$	$i = 1$	$i = 2$	$i = 3$	$i = 4$
$P_{\text{пом}}$	8,9E-05	1,3E-06	2,8E-07	2,2E-07	3,8E-07

Таким чином при повторенні через 4 кодових слова одної й той самої сигнальної конструкції можна зменшити ймовірність помилкового прийому знака $P_{\text{пом}}$ знака значно більше ніж чотири порядки.

Крім вибору оптимальної відстані повторення надлишкових СКК необхідно забезпечити захист кожної із них при умові приймання на інтервалі хорошого стану. Для цього необхідно вирішити вибір параметрів повторюваних ТСК:

- значення величини Δ ;
- значення модуля порівняння (A_0);
- число інформаційних значущих моментів модуляції.

В розглянутих в даному розділі матеріалах випробувано на реальних каналах ТСК при $S = 7$; $A_1 = 2$; $A_2 = 2$, $A_3 = 7$, $A_0 = 19$.

Таблиця 5.15 – Априорні ймовірності помилкового прийняття кодових слів ТСК на інтервалі «хорошого» стану каналу за умови, що величина $\sigma \approx 2\%$, $i = 3$ та різних значеннях параметра S .

S	7	8	9	10	11	12
$i = 3$						
P_1^1	$3,55 \cdot 10^{-4}$	$1,77 \cdot 10^{-3}$	$5,41 \cdot 10^{-3}$	$1,21 \cdot 10^{-2}$	$2,19 \cdot 10^{-2}$	$3,45 \cdot 10^{-2}$
P_2^1	$1,26 \cdot 10^{-7}$	$3,16 \cdot 10^{-6}$	$2,98 \cdot 10^{-5}$	$1,52 \cdot 10^{-4}$	$5,19 \cdot 10^{-4}$	$1,33 \cdot 10^{-3}$
P_3^1	$4,48 \cdot 10^{-9}$	$5,62 \cdot 10^{-9}$	$1,64 \cdot 10^{-7}$	$1,92 \cdot 10^{-6}$	$1,22 \cdot 10^{-5}$	$5,16 \cdot 10^{-5}$

З табл. 5.15 виходить, що навіть виправлення помилок зміщення одного ЗММ на величину $0,5\Delta \leq \theta \leq 1,5\Delta$ підвищує ймовірність безпомилкового прийому на інтервалі «хорошого» стану каналу майже на три порядки. Досягнути це можливо шляхом вибору коефіцієнтів рівняння якості, що забезпечують надлишковість, та таке векторне поле, в якому зміщення одного ЗММ не приводять до невиявленої помилки через різні синдроми (табл. 5.17).

Дослідження ефективності 2-х кратного повторення коригуючих ТСК. В процесі дослідження використовувався «шлейфний» метод вимірювання. Комплекс складався з каналу зв'язку МТМ, ЧМ-2 модему та аналого-цифрового перетворювача персонального комп'ютера (ПК) або електронно-обчислювальної машини (ЕОМ). У ролі АЦП було обрано лінійний вхід звукової карти за частотою дискретизації 96 кГц. Таке АЦП забезпечує похибку для параметрів $S = 7$ та при смузі у $\Delta F = 1300$ Гц, величиною меншою за 1%. У ролі генератора тестової послідовності використовувався вихід звукової карти, що являє собою цифро-аналоговий перетворювач (ЦАП). Структурна схема наведена на рис. 5.17.

Квантування імпульсів виробляється за допомогою внутрішнього генератора імпульсів вбудованого в звукову карту ЕОМ.

Загальна схема модему може бути представлена у вигляді рис. 5.18.

До основних елементів модему можна віднести СФ – смуговий фільтр, ПС – підсилювач, Обм – обмежувач, ЧД – частотний детектор, вирішальний пристрій та ключ.

Аналіз імпульсів «поганого» стану за тривалістю при передаванні тестової сигнальної конструкції або сигналів з несучими коливаннями, що відповідають «1» або «0», виробляються за допомогою ЕОМ. По закінченню запису та розподілу на неперервні зони відбувається збереження масиву тривалостей у пам'ять ЕОМ з подальшим виводом результатів розрахунків на екран у графічному вигляді.

На першій стадії експерименту фіксувалася структура прийнятих помилкового кодових слів з $S = 1$, при цьому кожний елемент було рівномірно розбито на сім часових відтинків. Фіксувалися номери вражених завадами кодових слів.

Дані одного фрагмента передавання наступні:

1. Тривалість кодового слова дорівнює $8t_0$.
2. Число переданих кодових слів – 360000.
3. Число прийнятих кодових слів зі спотворенням – 364.

Таблиця 5.18 - Аналіз прийнятих кодових слів зі спотворенням

Кратність помилки	Кількість кодових слів	Імовірність появи
1	244	0,67
2	102	0,28
3	16	0,0446
4	1	0,0027
5	1	0,0027

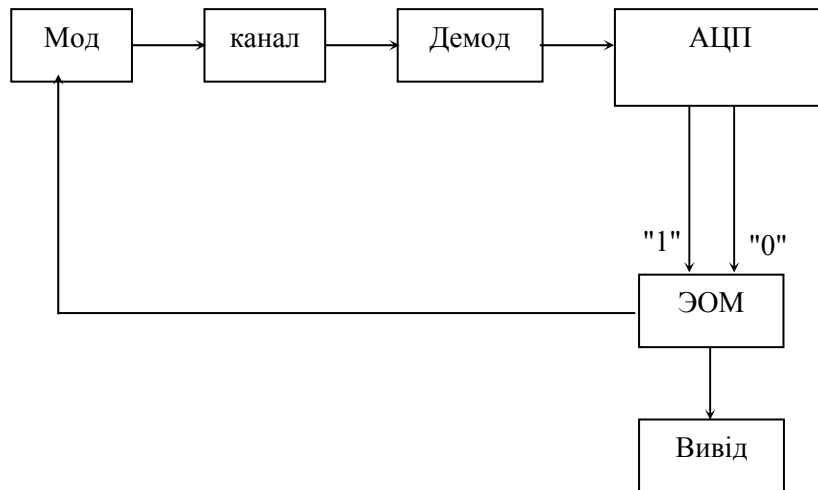


Рисунок 5.17 - Схема вимірювального комплексу

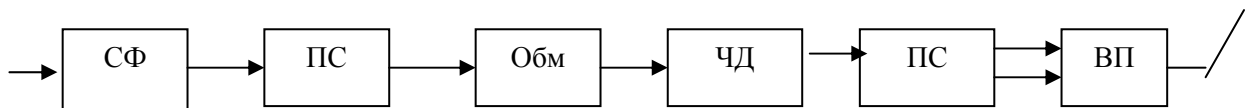


Рисунок 5.18 - Загальна схема модема

Отримані статистичні дані дозволяють визначити коефіцієнт групування помилок, що характеризує питому вагу спотворених елементів у кодовому слові, за формулою:

$$\alpha_{\text{гр}} = \frac{\ln \bar{t}}{\ln m}, \quad (5.188)$$

де \bar{t} – середня кількість спотворених елементів у кодовому слові; m – кількість елементів у кодовому слові.

Коефіцієнт групування дорівнює $\alpha_{\text{гр}} = 0,66$. Крім того аналіз структури прийнятих кодових слів та критерію, що характеризує «поганий» стан каналу, наведеного вище, дозволяє стверджувати, що лише на інтервалі «поганого» стану каналу, завади змінюють кількість ЗММ прийнятого сигналу.

Розглянемо результати вимірювання в якості передавання надлишкових ТСК каналом МТМ з ЧМ, в яких імовірність помилкового прийому одного байта при позиційному кодуванні складає $p(t_0 \geq 1,8) = 1,08 \cdot 10^{-2}$, а параметри рівняння якості задовольняли умові $2x_1 + 3x_2 + 7x_3 = 0 \pmod{19}$.

Таблиця 5.19 – Результати вимірювання якості передавання ТСК

1	Передано кодових слів	73676
2	Прийнято кодових слів (відсутність зміщень ЗМВ величиною $ \theta \geq 1/2 \Delta$ і наявність трьох ЗМВ)	72835
3	Кількість помилкових кодових слів	834
4	Кількість кодових слів з дробленням	54
5	Кількість кодових слів, виправлених синдромним методом	780

З наведених даних виходить:

1) незважаючи на те, що відстань між сигнальними конструкціями визначається енергією елемента (а не інтервалом t_0) ймовірність помилкового приймання слова дорівнює $834/73676 = 7,3 \cdot 10^{-4}$, що несуттєво перевищує значення, отримане при передаванні кодових слів при позиційному кодуванні.

2) середня відстань між «поганими» станами (в кодових конструкціях) $76676/54 = 1419$.

Численні експерименти на різних каналах МТМ характеризуються інтервалом «поганих» станів. В табл. 5.20 наведено результати спотворень у «поганому» стані на інтервалі 756 КС з наведеною статистикою спотворених КС в «хорошому» стані.

Таблиця 5.20 – Розподіл однократних помилок зі зміщенням на Δ

Номера кодових слів із дробленням (в «поганому» стані)	Кодові слова зі зміщенням на Δ (в «хорошому» стані)		Відношення кількості однократних помилок до інтервалу між спотвореними кодовими словами з дробленням
	Номер кодового слова	Який перехід змістився	
756	825	3	0,00252
1549	1067	1	
1549 2383	1649	3	0,006
	1695	3	
	2017	3	
	2030	1	
	2305	1	
2383 3131	2461	3	0,008
	2543	1	
	2576	3	
	2717	1	
	2936	1	
	3042	3	
3131 3643	3339	1	0,0078
	3408	1	
	3486	1	
	3530	1	
3643 4444	3723	1	0,0062
	3768	2	
	3838	1	
	3991	3	
	4040	1	
4444 5052	4916	3	0,0032
	4972	1	

5052	5138	3	0,0036
5881	5508	1	
	5847	3	
5881	6089	1	0,005
6677	6101	1	
	6215	1	
	6453	1	
6677	7437	2	0,0013
7453			

Реалізація вузлів системи з повторенням двох коригуючих ТСК.

Аналіз спотворень на виході каналу дозволяє синтезувати простий програмний метод корекції помилок на прийомі в окремих парах. Це дає можливості для реалізації низки функцій пристрою обміну даними, які можуть бути легко впроваджені шляхом програмування в електронну пам'ять. Впровадження програмної реалізації методу дозволяють реалізувати багато функцій опрацювання сигналів на підставі елементарного набору мікропроцесорних команд. Використання послідовності операцій та команд при реалізації методів завадостійкого кодування, синтезу сигнальних конструкцій на стороні передавання, оброблення сигналів забезпечується прозорими бульовими наборами функцій, які впроваджені у логіку обчислювальної техніки та виконують функцію схемотехнічних рішень.

Такий підхід дозволяє мінімізувати об'єм необхідних ресурсів пам'яті, тому що не потребує постійного завантаження. У процесі виконання елементів програми, що відповідають вузлам емітованої схеми, програмне середовище, що виконує дану програму, запускає по черзі, шляхом звернення та передавання необхідних даних, що у фізичному еквіваленті є значення амплітуди, фази напруги чи струму у даний момент часу, номер кодового слова, кількість спотворених елементів та іншу інформацію у блок-файл, який проводить його оброблення, яке еквівалентне фізичній або логічній дії, необхідній даному типу даних.

Отже, першочерговим завданням, при розробці програмної реалізації є формування блока процедур опрацювання фізичних величин та реалізація вузлів.

Розглянемо детальніше метод обробки інформації на стороні приймання. В процесі приймання інформація записується у регістр зсуву.

Такий підхід передбачає можливість використання байтових елементів пам'яті зовнішніх постійного або оперативного запам'ятовуючого пристроїв для оброблення одночасно двох або більше кодових конструкцій.

Далі проходить етап перевірки кожного кодового слова на ураження завадами на інтервалі «поганого» стану каналу. Функціонально дану схему

легко реалізувати за допомогою регістра (1), схеми суматора (2) та визначення модуля i . Приклад такої реалізації наведено на рис. 5.19.

Після перевірки інформації, щодо того чи прийняте кодове слово на інтервалі «хорошого» стану, воно передається на оброблення за рівнянням якості. Реалізацію перевірки за даним виразом легко уявити у вигляді схеми, представленій на рис. 5.20.

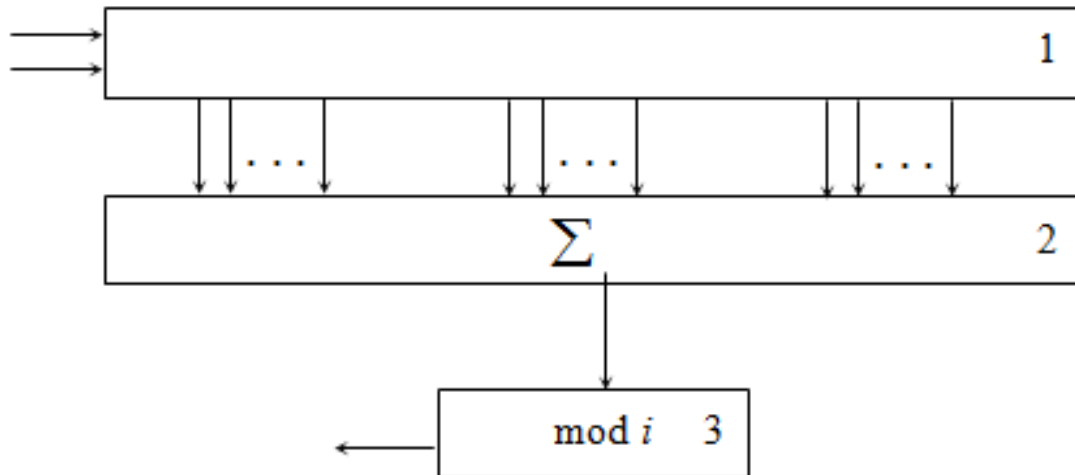


Рисунок 5.19 - Блок перевірки кодового слова на належність до приймання на інтервалі «хорошого» або «поганого» стану

До основних вузлів даної схеми входять: 1 – кодоперетворювач, даний блок формує послідовність у вигляді зручному для подальшої подачі інформації щодо розміщення ЗММ у кодовій конструкції на блок множення с заданими коефіцієнтами – 2. Блок 2 – схожий за своєю структурою на блок синдромного декодера. Наступним етапом методу перевірки кодової конструкції на зміну структури під дією завади на інтервалі «хорошого» стану, є обробка отриманих множників суматором 3. На останньому етапі сума перевіряється на залишок від ділення у блоці 4. У випадку ненульового залишку кодовому слову додається позначка, що вказує на наявність спотворення. У випадку, коли обидва з кодових слів прийняті зі спотвореннями, які виявлені, вірним обирається таке, яке можливо виправити рівнянням якості, вектором найменшої ваги, враховуючи значення ймовірностей помилкового прийому.

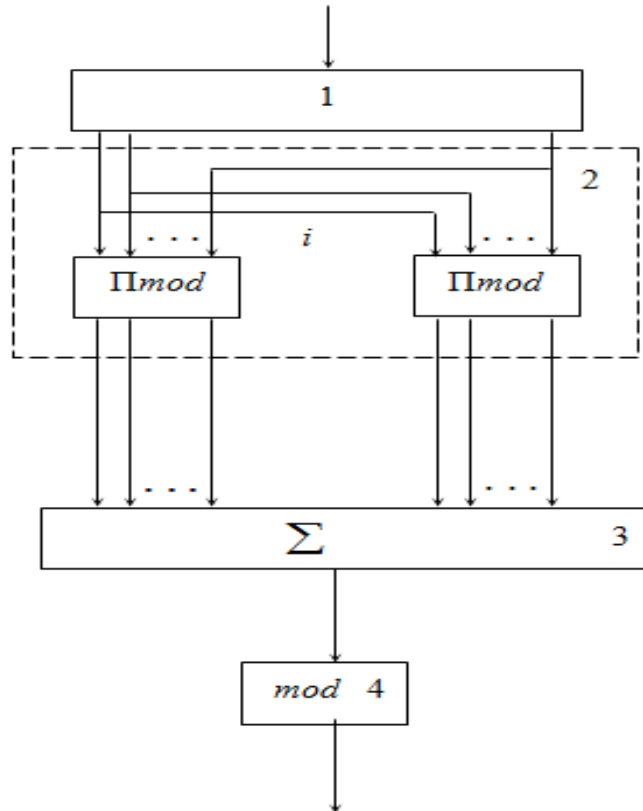


Рисунок 5.20 - Блок перевірки кодового слова за рівнянням якості

Експериментальна перевірка ефективності 2-х кратної передачі коригуючи ТСК. При синтезі сигнальних конструкцій вибрані наступні характеристики:

- $m = 8$, $\Delta = 0,14t_0$ ($S = 7$), $i = 3$;
- вагові коефіцієнти – прості числа : $A_1 = 2$; $A_2 = 3$; $A_3 = 7$; $A_0 = 19$.

Такі коефіцієнти здатні виправляти помилки зміщення одного ЗММ на величину $0,5\Delta \leq \theta \leq 1,5\Delta$.

Перевірка положень алгоритму проводилася на реальному каналі комутованої МТМ. Передача даних проводилася ЧМ модемом методом «шлейфу» у смузі пропускання $\Delta F = 1300$ Гц зі швидкістю модуляції $B = 1000$ Бод (30% різниця величини ΔF та швидкості модуляції обрано з урахуванням спотворень АЧХ і ФЧХ).

Як прикінцева апаратура була обрана ЕОМ, яка імітує роботу передавального і приймального пристрою, здійснює оброблення отриманих даних.

Нижче наведена статистика одного із фрагментів вимірів тривалістю 5 год. Було передано 2000000 кодових слів (6 000 000 ЗМВ), які відповідають

1 000 000 пар з двократним повторенням на відстані 3 ТСК. В табл. 5.21 наведено численні значення умов прийняття окремих пар при різних спотвореннях, наведених в інформації до таблиці

Таблиця 5.24 - Структура помилково прийнятих кодових слів ТСК, група № 4

№ кк	Точка аналізу	Структура кодового слова
57928	На прийманні	0000000010000000000100
	На прийманні	00000000100000000000010000000000000000000000000000000100100110000000000000001
	На передаванні	0000000010000000000001000
16965	На прийманні	000000001000000000011000010110000000010000010000000000001000000000001000000000
	На прийманні	0000000001001000000000001000000000
	На передаванні	000000001000100000000001000000000

Таблиця 5.25 - Структура помилково прийнятих кодових слів ТСК, група № 5

№ кк	Точка аналізу	Структура кодового слова
97713	На прийманні	00000000001000000100
	На прийманні	00000000001000000010000000000000000000000000000000001000000000000000000000000000
	На передаванні	0000000000100000001000
168236	На прийманні	00000000001000000100
	На прийманні	00000000001000000100
	На передаванні	0000000000100000001000

Оцінимо питому вагу із збільшенням ЗМВ, що відповідає індексу «3». Основна статистика кодових ТСК із збільшенням числа ЗМВ 3077. При цьому змінилося число ЗМВ лише в одному ТСК із даної пари. Питома вага «поганого» стану каналу не більше значення $3077/10^6 = 1,5 \cdot 10^{-3}$.

5.9. Питання та задачі для самоперевірки

1. Дайте характеристику поля $GF(b)$.
2. Перерахуйте умови рівності нулю всіх елементів контрольованого числа.
3. Яка потужність виправляємих помилок коригуючим кодом з параметрами m і k ?
4. Який зв'язок між кількістю пересічних підмножин надлишкового коду m і k ?
5. Чим визначається потужність множин класів суміжності?
6. Розрахуйте потужність i -кратних помилок в кодi $n = m + k$, за $m = 10 \dots 15$, $k = 5 \dots 7$, $i = 3, 5, 7$.
7. В якому випадку набір залишків одного і той самого десятичного числа N_{10} при різних модулях однозначно характеризує N_{10} ?
8. Які операції відносяться до модульних в системi залишкових класів?
9. Розв'язати задачу 3 при зміні значень P_i : $P_1 = 5$, $P_2 = 7$, $P_3 = 4$.

10. Які характеристики заданого числового діапазону називаються узагальненими позиційними?

11. Чим визначається відстань між двома векторами з різним числом членів?

12. Доведіть справедливість нерівності $\sum_{k=1}^i |A_k e_k| < A_0$ при значенні модуля $A_0 = (e_0 + 1)^i$.

13. Як розраховано значення d_{\min} і d_0 для таймерних кодів табл. 5.4?

14. Для кодів табл. 5.4 визначте значення модулів A_0 .

15. За рахунок яких операцій в синтезі кодової таблиці коригуючих кодів зменшуються затрати часу?

16. Чому для парних і непарних d різні аналітичні вирази для модулів порівняння?

17. Як визначається ранг матриць (5.76), (5.77), (5.78)?

18. Яка особливість векторів 5.80 дозволяє бути базисом?

19. Наведіть послідовність розрахунку умов (5.81a) ... (5.81к) з використанням лінійного програмування.

20. Як впливає значення кодової відстані d на потужність корегуючого ТСК?

21. Якими параметрами характеризується завада в рівнянні 5.106?

22. Чим обмежена зона помилкової реєстрації у виразі (5.108)?

23. Який зв'язок кодової відстані корегуючого ТСК і ваги нульового вектору?

24. На основі табл. 5.13 побудуйте таблицю повторюваності синдромів С.

25. При якому мінімальному значенні A_0 для табл. 5.13 повторення синдромів С буде відсутнє?

26. Проведіть оцінку витрат на синтез коригуючого коду в системі з ВЗЗ і на повторення спотворених кодових слів (табл. 5.14).

27. Побудуйте залежності максимально можливого значення передачі інформації на один найквістовий елемент для ТСК $i = 3; s = 5, 7, 12; m = 6 \dots 10$.

28. Оцініть при якому значенні середньоквадратичного відхилення ЗМВ імовірності зміщення одного ЗМВ на величину $\theta = 1\Delta$ і двох ЗМВ $\theta_1(1\Delta) = \theta_2(1\Delta)$ відрізняються не більше ніж на порядок.

29. Оцініть ефективність використання числа ЗМВ в коригуючому коді ТСК згідно статистичних даних наведених в табл. 5.11а.

30. Оцініть імовірність спотворення однієї з повторюваних коригуючих ТСК при збільшенні відстані між ними в межах $T_{\text{від.повт.}} \in [3 \dots 10] T_{\text{кс}}$.

Література

1. Аксенов Б.Е. Повышение эффективности передачи информации в автоматизированных системах управления / Б.Е. Аксенов, А.М. Александров, В.И. Ключко. – Л., 1983. – С. 332.
2. Аршинов М.Н. Коды и математика / М.Н. Аршинов, Л.Е. Садовський. – (Библиотека “Квант”, вып. 30). – М.: Наука, 1983. – 143 с.
3. Балан Н.М. Определение зоны искажений синхронного звукового вещания в диапазоне ОВЧ / Н.М. Балан, Ш.Г. Искендерзаде, С.В. Хомич // Цифрові технології. – 2011. – Вип. 9. – С.101 – 111.
4. Берликэмп Э. Алгебраическая теория кодирования / Берликэмп Э.; пер. с англ.; под ред. С.Д. Бирмана. – М.: Мир, 1971. – 477 с.
5. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р.; пер с англ. – М.: Мир, 1986. – 576 с.
6. Блох Э.Л. Модели источника ошибок в каналах передачи цифровой информации / Блох Э.Л., Попова О.В., Турин В.Я. – М.: Связь, 1971. – 312 с.
7. Боккер П. Передача данных. Техника связи в системах телеобработки данных / Боккер П.; ПЕР. с нем.; под ред. Д.Д. Кловского. – М.: Связь, 1980. – Т. 1: Основы. – 264 с.
8. Борисов Ю.П., Основы многоканальной передачи информации / Борисов Ю.П., Пенин П.И. – М.: Связь, 1967. – 436 с.
9. Бородин Л.Ф. Введение в теорию корректирующих кодов / Бородин Л.Ф. – М.: Сов. радио, 1968. – 408 с.
10. Буга Н.Н. Основы теории связи и передачи данных / Буга Н.Н. – Ч. 4. – Л.: ЛВИКА им. А.Ф. Можайского, 1970. – 704 с.
11. Буга Н.Н. Основы теории связи и передачи данных / Буга Н.Н. – Ч. I. – Л.: ВИКА им. А.Ф. Можайского, 1968. – 542 с.
12. Варакин Л.Е. Теория систем сигналов / Варакин Л.Е. – М.: Сов. радио, 1978. – 304 с.
13. Васильев В.И. и др. Системы связи: Учеб. пособие для ВТУЗов. – М.: Высшая школа, 1987. – 280 с.
14. Вентцель Е. С. Теория вероятностей. – М.: Наука, 1969. – 328 с.
15. Витерби А.Д. Принципы цифровой связи и кодирования / А.Д. Витерби, Д.К. Омура. – М., Радио и связь, 1982. – 320 с.
16. Возенкрафт Дж., Джекобе И. Теоретические основы техники связи. – М.: Мир, 1969. – 640 с.
17. Возенкрафт Дж., Рейфен Б. Последовательное декодирование. – М.: Изд-во иностр. лит., 1963. – 153 с.
18. Ворон А.А. О спектрах псевдослучайных двоичных последовательностей / Ворон А.А. // Труды ЛВИКА А.Ф. Можайского. – Вып. 472, 1964.
19. Гаджиев М.М. The iteration algorithm of the harmonic equalizer parameters optimization by coordinatewise descent method / М.М. Гаджиев, М.М. Balan, Ш.Н. Isgandarzada, О.С. Kuznetsova // Учебн. пособ. ОНАЗ ім. О.С. Попова. – 2010. – С. 16.
20. Гаджиев М.М. Аналитическая модель сквозного канала гетерогенной сети / С.А. Нестеренко, М.М. Гаджиев, Т.М. Мансуров, Л.В. Иванова // Научные статьи. Азербайджанский технический университет. – Баку (Азербайджан), 2013. – №1 XII (45). – С. 93-97.
21. Гаджиев М.М. Аналіз, синтез і оптимізація мереж зв'язку // Математичні основи оптимізації телекомунікаційних систем: підручник [для студ. вищ. техн. навч. закл.]

- / [М.В. Захарченко, М.М. Гаджиев, С.М. Горохов та ін.]; під ред. М.В. Захарченко. – Одеса, ОНАЗ ім. О.С. Попова. – 2010. – Разд. 8 – С. 94-144.
22. Гаджиев М.М. Методика расчета пропускной способности безпроводного сегмента сети на основе регрессионного анализа / С.А. Нестеренко, М.М. Гаджиев, Т.М. Мансуров, Л.В. Иванова // Научные статьи. Азербайджанский технический университет. – Баку (Азербайджан), 2013. – №2 XII (45). – С. 95-99.
 23. Гаджиев М.М. Оптимизация опорных сигналов при корреляционной обработке при наличии в канале аддитивных помех / М.М.Гаджиев // Матеріали 66-ї НТК професорсько-викладацького складу науковців молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова, Одеса. – 2011. – С. 7.
 24. Галлагер Р. Теория информации и надежная связь: Пер с англ. / Галлагер Р.; под ред. М.С. Пинскера и Б.С. Цыбакова. – М.: Сов. радио, 1974. – 720 с.
 25. Гитлиц М.В. Теоретические основы многоканальной связи / Гитлиц М.В., Лев А.Ю. – М.: Радио и связь, 1985. – 248 с.
 26. Гойхман Э.Ш. Передача информации в автоматизированных системах управления / Гойхман Э.Ш., Лосев Ю.И. – М., 1971. – 160 с.
 27. Дельгадо Э.В., Лещук И.А. Об одном алгоритме реализации циклического кода / Помехоустойчивость и эффективность системы передачи информации: Сб. науч. тр. Одес. электротехн. ин-та связи. – 1983. – № 21 – С. 36–37.
 28. Драганов А.В., Гринь А.А. Эффективность систем зі зворотним зв'язком при таймерному кодуванні // Системы и средства передачи и обработки информации: Тр. VI Междунар. науч.–практич. конф. 3–8 сентября 2002 г. – Одесса, 2002. – С. 79–80.
 29. Драганов О.В. Оптимізація базового елемента багатопозиційних часових кодів при зміні параметрів каналу // Наук. праці ОНАЗ ім. О.С. Попова, 2002. – №1. – С. 104–107.
 30. Захарченко В.М. Синтез багатопозиційних часових кодів / Захарченко В.М. – К.: Техніка, 1999. – 281 с.
 31. Захарченко В.Н. Оптимизация систем с парциальным кодированием : учеб. пособие / Захарченко В.Н., Кисель А.В., Михайлов В.К. – Одесса: УГАС им. А.С. Попова, 2000. – 193 с.
 32. Захарченко В.Н. Расчет мощности избыточного кода при многопозиционных временных сигналах // В.Н. Захарченко / Сб. науч. трудов Информатика и связь: УГАС им. А.С. Попова. – К.:Техніка, 1997. – С. 194-196.
 33. Захарченко В.Н. Уменьшения числа запросов в системе РОС на базе МВК / В.Н. Захарченко // Информатика и связь: сб. науч. трудов УГАС им. А.С. Попова. – К. : Техніка, 1996. – С. 161-165.
 34. Захарченко М.В. Порівняння синдромних методів для коригуючих блокових позиційних і таймерних кодів / М.В. Захарченко, М.М. Гаджиев, Б.К. Радзімовський, Ю.С. Горохов, Д. О. Шпак // Восточно-Европейский журнал передовых технологий. – 2014. – № 2/9(68). – С. 4–8, 67.
 35. Захарченко М.В. Алгебраїчний алгоритм декодування бінарних сигналів з енергетичною віддаллю менше Найквістової / М.В. Захарченко, С.В. Хомич, Ю.В. Белова, К.О. Осадчук // Матеріали II міжн. наук.-практ. конф. [“Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки”], (Чернівці, 25–27 жовтня 2012 р.) – Чернівці, 2012. – С. 86.
 36. Захарченко М.В. Вплив корельованих завад на пропускну здатність каналу та швидкість передачі інформації при обмеженій якості / М.В. Захарченко, В.Й. Кільдїшев, С.В. Хомич, Ю.В. Белова // Вестник НТУ «ХПИ». – 2012. – Вип. 33. – С. – 62–88.

37. Захарченко М.В. Эффективность корегулирующих ТСК в односторонних системах передачи / М.В. Захарченко, М.М. Гаджієв, С.В. Хомич, М.П. Кучеренко // Східно-європейський журнал передових технологій. – 2012. – Вип. 1/9. – С. 33–36.
38. Захарченко М.В. Комп'ютерна програма «Відображення кодових слів таймерних сигнальних конструкцій у тривимірному просторі» / М.В. Захарченко, М.М. Балан, С.В. Хомич, Ш.Г. Іскендерзаде // Свідectво про реєстрацію авторського права на твір №44856. Комп'ютерна програма.
39. Захарченко М.В. Компенсація надлишковості в блокових коректуючих кодах за рахунок таймерних сигналів / М.В. Захарченко, В.Й. Кільдішев, С.В. Хомич, О.Г. Пришляк // Вісник Хмельницького національного університету. – 2011. – Вип. 2. – С.178 – 185.
40. Захарченко М.В. Корреляционный метод декодирования таймерных сигнальных конструкций / М.В. Захарченко, С.В. Хомич, Ю.В. Белова // Матеріали 66-ї наук.-техн. конф. проф.-виклад. складу, науковців, аспірантів та студентів (Одеса, 5 – 8 грудня 2011 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2012. – С. 38– 39.
41. Захарченко М.В. Оценка параметров надежности многоканальных сегментов сложных информационных систем / [М.В. Захарченко, Д.Ю. Ильин, С.В. Хомич, Ж.А. Торк] // Вестник НТУ «ХПИ». – 2012. – Вип. 9. – С. – 58–62.
42. Захарченко М.В. Порівняльний аналіз *i*-кратної передачі сигнальних кодових конструкцій РЦК і таймерних кодів / М.В. Захарченко, С.В. Хомич // Матеріали 66-ї наук.-техн. конф. проф.-виклад. складу, науковців, аспірантів та студентів, (Одеса, 5 – 8 грудня 2011 р.) – Одеса: ОНАЗ ім. О.С. Попова, 2012. – С. 36– 38.
43. Захарченко Н. В. Метод синтеза шумового сигнала гауссова типа на основе систем с динамическим хаосом / Н. В. Захарченко, Б. К. Радзимовский, В. В. Корчинский // Восточно-Европейский журнал передовых технологий. – 2012. – № 2/10(56). – С. 25–27.
44. Захарченко Н. В. Метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов в системах передачи конфиденциальной информации/ Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім. О. С. Попова. –2011. – № 2. – С. 3–7.
45. Захарченко Н. В. Многопользовательский доступ в системах передачи с хаотическими сигналами / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 5/9(53). – С. 26–29.
46. Захарченко Н. В. Оценка информационной скрытности таймерных сигнальных конструкций в системах передачи конфиденциальной информации / Н.В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім. О. С. Попова. – 2011. – № 1. – С. 3–8.
47. Захарченко Н. В. Случайные числа и последовательности на основе систем с динамическим хаосом / Н. В. Захарченко, Б. К. Радзимовский, В. В. Корчинский // Збірник наукових праць ОНАЗ ім. О. С. Попова. –2012. – № 1. – С. 8–11.
48. Захарченко Н. В. Структурная скрытность таймерных сигналов в системах с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 2/9(50). – С. 7–9.
49. Захарченко Н. В. Эффективность использования таймерных сигнальных конструкций в системах передачи с кодовым разделением каналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Наукові праці ДонНТУ. – 2011. – Випуск № 20(182). – С. 145–151.

50. Захарченко Н.В. Выбор узлов аппаратуры передачи данных ч.І. учебное пособие / Захарченко Н.В., Нудельман П.Я. // Одесский электротехнический институт связи им. А.С. Попова. – Одесса, 1980. – 92 с.
51. Захарченко Н.В. Выбор узлов аппаратуры передачи данных: учеб. пособие / Н.В. Захарченко, П.Я. Нудельман // Одесский электротехнический институт связи им. А.С. Попова. – Одесса, 1985. – Ч. 1. – 88 с.
52. Захарченко Н.В. Ефективність корегуючих ТСК в односторонніх системах передачі / М.В. Захарченко, М.М. Гаджиев, С.В. Хомич, М.П. Кучеренко // Східно-європейський журнал передових технологій. – 2012. – Вип. 1/9. – С. 36–39.
53. Захарченко Н.В. О возможности уменьшения избыточности блочных кодов для каналов с группированием ошибок / Захарченко Н.В. // Тр. УНИИРТ. – 1997. – №3. – С. 73-77.
54. Захарченко Н.В. Односторонние системы передачи: метод. пособие / Н.В. Захарченко, А.С. Крысько. – Одесса: ОНАС им.А.С. Попова, 2007. – 88 с.
55. Захарченко Н.В. Оптимизация параметров избыточных блочных кодов по критерию обнаружения асинфазного состояния приемника / Захарченко Н.В., Мамедов М.А., Гаджиев М.М. // Восточно-европейский журнал передовых технологий. – Харьков. – 2006. – № 2/2 (20). – С. 53 – 56.
56. Захарченко Н.В. Оптимизация синдромного метода исправления ошибок в адаптивных системах / Н.В. Захарченко, М.М. Гаджиев, С.И. Лысенко, Д.В. Талакевич // Восточно-европейский журнал передовых технологий. – 2013. – №5/2 (65) – С. 13-18.
57. Захарченко Н.В. Основы кодирования: учеб. пособие / Захарченко Н.В., Захарченко В.Н., Крысько А.С. – Одесса, УГАС им. А.С. Попова, 1999. – 240 с.
58. Захарченко Н.В. Основы передачи дискретных сообщений / Захарченко Н.В., Нудельман П.Я., Кононович В.Г. – М.: Радио и связь, 1990. – 240 с.
59. Захарченко Н.В. Параметры потока ошибок на выходе кодопреобразователя МВЦ-РЦК / Н.В. Захарченко, С.М. Горохов, А.В. Драганов. // Наукові праці УДАЗ ім. О.С. Попова. – 2001. – №4. – С. 51-61.
60. Захарченко Н.В. Пропускная способность каналов при таймерных сигнальных конструкциях / Н.В. Захарченко, М.М. Гаджиев, А.А. Русаловская // Матеріали XII міжнародної науково-технічної конференції ОНАЗ ім. О.С. Попова, Одеса. – 2013. – С. 186-188.
61. Захарченко Н.В. Совместная минимизация аддитивного шума и межсимвольных помех / Н.В. Захарченко, М.М. Гаджиев, А.О. Мамедов // Наукові праці ДонНТУ. – Вип. 106, 2006. – С. 66 – 70.
62. Захарченко Н.В. Сравнение сигнальных конструкций разрядно-цифровых и многопозиционных временных кодов / Захарченко Н.В., Захарченко В.Н., Кузьминов А.В. // Информатика и связь: сб. науч. трудов. – Одесса, 1996. – С. 13-21.
63. Захарченко Н.В. Теоретические основы оптимизации узлов и сетей / Захарченко Н.В., Мамедов М.А., Гаджиев М.М.; под ред. Н.В. Захарченко. – Баку: ЭЛМ. – 2007. – 272 с.
64. Захарченко Н.В. Эффективность использования многопозиционных кодов в низовых системах ПДИ. МС СССР / Захарченко Н.В. – Одесса: ОЭИС, 1984. – 92 с.
65. Захарченко Н.В. Эффективность компенсации избыточности кода при использовании таймерных сигналов / Н.В. Захарченко, В.Е. Басов // Моделювання та інформаційні технології: зб. наук праць. – Вип. 31. – К.: 2005. – С. 6–13.
66. Захарченко Н.В. Эффективность компенсации избыточности кода при использовании таймерных сигналов / Н.В. Захарченко, В.Е. Басов // Моделювання та інформаційні технології: зб. наук праць. – Вип. 31. – К., 2005 р. – С. 6 – 13.

67. Захарченко Н.В. Эффективность применения корректирующих блоковых таймерных кодов в адаптивных системах с решающей обратной связью / Н.В. Захарченко, М.М. Гаджиев, Е.Н. Мартынова, С.И. Лысенко // Вестник НТУ «ХПИ» – 2013. – №38 (1011). – С. 140 – 145.
68. Злотник Б.М. Помехоустойчивые коды в системах связи / Злотник Б.М. – М.: Радио и связь, 1989. – 232 с.
69. Зюко А.Г., Фалько А.И., Банкет В.Л., Иващенко П.В. Помехоустойчивость и эффективность систем передачи информации / Под ред. А.Г. Зюко.- М.: Радио и связь, 1985.-304 с.
70. Зяблов В.В. Дистанционные свойства турбо-кодов с различными перемежителями / В.В. Зяблов, М.А. Цветков // Информационные процессы. – 2003. – Т. 3, № 2. – С. 83-96.
71. Ибрагим С.Х. и др. Особенности построения систем при использовании многопозиционных временных бинарных сигналов // Эффективные системы связи: Сб. науч. тр. ОЭИС. – Одесса, 1988. – С. 93–95.
72. Ибрагим С.Х., Юнес А.А. вероятность ошибочного приема элемента при сверхнаиквистовой передаче // Помехоустойчивость системы связи: Сб. научн. тр. ОЭИС. – Одесса, 1990. – С. 76–79.
73. Игнатов В.А. Теория информации и передачи сигналов / Игнатов В.А. – М.: Сов. радио, 1979. – 280 с.
74. Клар Дж.мл. Кодирование с исправлением ошибок в системах цифровой связи / Клар Дж.мл., Кейн Дж.; пер. с англ.; под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.
75. Коган И.М. Прикладная теория информации / Коган И.М. – М: Радио и связь, 1981.
76. Колесник В.Д. Декодирование циклических кодов / В.Д. Колесник, Е.Т. Мирончиков. – М.: Связь, 1968. – 251 с.
77. Коричнев Л.П. Статистический контроль каналов связи / Л.П. Коричнев, В.Д. Королев. – М.: Радио связь, 1989. – 240 с.
78. Котельников В.А. Теория потенциальной помехоустойчивости / Котельников В.А. – М.: Госэнергоиздат, 1956. – 152 с.
79. Котов П.А. Повышение достоверности передачи цифровой информации / Котов П.А. – М.: Связь, 1966, – 185 с.
80. Коханов О.Б. Оптимальное синхронное линейное детектирование РАМ сигналов с компенсацией фазового сдвига / Коханов О.Б., Захарченко Н.В., Перекрестов И.С. // Зб. наукових праць ОНАЗ ім. О.С. Попова. – 2006. – № 1. – С. 18 – 22.
81. Кошевой А.А. Телеметрические комплексы / Кошевой А.А. – М.: Машиностроительные, 1975.
82. Купер Дж., Макгиллем К. Вероятностные методы анализа сигналов и систем / Пер. с англ. – М.: Мир, 1989. – 376 с.
83. Курицин С.А. Теоретические основы построения адаптивных систем: учеб. пособие. / Курицин С.А. – Л.: ЛЭИС, 1983. – 64 с.
84. Лосев В.В. Поиск и декодирование сложных дискретных сигналов / Лосев В.В., Бродская Е.Б., Коржик В.И.; под ред. В.И. Коржика. – М.: Радио и связь, 1988. – 224 с.
85. Мазин И.А. Передача информации в сетях с коммутацией сообщений / Мазин И.А., Уринсон Л.С., Хромешен Г.К. – М.: Связь, 1977. – 326 с.
86. Мазурков М.И. Алгоритмы рекуррентного декодирования в целом кодов Рида–Соломона / М.И. Мазурков, С.В. Миц, В.Я. Чечельницкий // Радиоэлектроника. 2003. – №6. – С. 34-38. (Изв. высш. учебн. заведений).

87. Мазурков М.И. Метод вероятностного декодирования циклических кодов Рида – Соломона / М.И. Мазурков, С.В. Миц // Радиоэлектроника. 1999. – 7. – С. 17-23. (Изв. высш. учеб. заведений).
88. Мазурков М.И. Рекуррентный алгоритм скользящего корреляционного декодирования циклических кодов / Мазурков М.И. // Радиоэлектроника. – 2000. – № 1. – С. 53-59. (Изв. высш. учеб. заведений).
89. Мазурков М.И. Цифровые методы в радиосистемах передачи информации. – Одесса: ОПИ, 1984. – 101 с.
90. Мазурков М.И. Основи теорії передавання інформації / Мазурков М.И. – Одеса. Наука і техніка 2004. – 168 с.
91. Макаров С.Б., Цикин И.А. Передача дискретных сообщений по радиоканалам с ограниченной полосой пропускания. – М.: Радио и связь, 1988. – 340 с.
92. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь 1979. – 732 с.
93. Мандзій Б.А., Желяк Р.І. Основи теорії сигналів: навч. посіб. для студентів вищих технічних закладів України / Б.А. Мандзій, Р.І. Желяк; за ред. д.т.н., проф. Мазія Б.А. – Львів: НВП “НОВИЙ ТЕЗАУРУС”, 2001. – 152 с.
94. Мановиев А.П. Основы теории радиотелеметрии / Мановиев А.П. – М.: Энергия, 1973. – 592 с.
95. Математичні основи оптимізації телекомунікаційних систем. Свідectво про реєстрацію авторського права на твір України №40340. / М.В. Захарченко, М.М. Гаджиев, С.М. Горохов та ін. // Дата реєстрації 10.10.2011.
96. Мережі та системи телекомунікацій. ЄНЗУ. Аналогові та комп'ютерні мережі [М.В. Захарченко, Г.С. Гайворонська, А.І. Єщенко, Л.А. Никитюк та ін.]. – за ред. М.В. Захарченка. – К.: Техніка, 2000. – 304 с.
97. Мережі та системи телекомунікацій: у 4 т. / [М.В. Захарченко, Г.С. Гайворонська, А.І. Єщенко]; за ред. М.В. Захарченка. –Т.1: Інформаційні мережі. Стандарти та рекомендації. ЄНМЗУ. Аналогові та комп'ютерні мережі.– К.: Техніка, 2000 р. – 2000 р. – 304 с.
98. Методи підвищення ефективності використання каналів зв'язку / [Захарченко В.М., Гайдар В.П., Улеєв О.П., Липчпнський О.І.]. – К.: Техніка, 1998. – 248 с.
99. Методы и коды сжатия информации / [Мазурков М.И., Ямпольский Ю.С., Бондарь В.И., Чечельницкий В.Я.]. – Одесса: ЛИТО ОНПУ, 1999. – 68 с.
100. Методы повышения эффективности использования каналов связи / Захарченко Н.В., Гайдар В.П., Улеєв А.П., Липчанский А.И.. – К.: Техніка, 1998. – 248 с.
101. Мешковский К.А. Кодирование в технике связи / К.А. Мешковский, Н.Е. Кириллов. – М.: Связь, 1966. – 340 с.
102. Митряев Е.В. Контроль верности информации в морской радиосвязи / Митряев Е.В., Ростовцев Ю.Г., Рышков Ю.П. – Л.: Судостроение, 1979. – 164 с.
103. Михайлов А.В. Высокоэффективные оптимальные системы связи. – М.: Связь, 1980. – 344 с.
104. Морев В.Л. Передача данных по телефонным каналам в информационно-вычислительных системах. – М.: Связь, 1971. – 46 с.
105. Мсеновуев А.П. Введение в цифровую телеметрию / Мсеновуев А.П.. – М.: Энергия, 1967. – 344 с.
106. Основы теории электросвязи. Телекоммуникационные системы коммутации и передачи информации : [учебник] ; под ред. Н.В. Захарченко. – Том 1: Системы электросвязи. – К.: Техніка, 1998. – 303 с.

107. Передача дискретных сообщений: [учебник для вузов] / В.П. Шувалов, Н.В. Захарченко, В.О. Шварцман и др.; под ред. В.П. Шувалова. – М.: Радио и связь, 1990. – 464 с.
108. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / У. Питерсон, Э Уэлдон; пер. с англ.; под ред. Р.Л. Добрушина, С.И. Самойленко. – М.: Мир, 1976. – 594 с.
109. Повышение скрытности передачи конфиденциальной информации на базе хаотических сигналов и таймерных сигнальных конструкций / Н. В Захарченко, В. В. Корчинский, Б. К. Радзимовский, В. Й. Кильдишев // Восточно-Европейский журнал передовых технологий. – 2012. – № 3/9(57). – С. 45–49.
110. Повышение эффективности блочного кодирования при работе по нестационарным каналам связи / Н.В. Захарченко, С.М. Горохов, В.Н. Захарченко, М.М. Гаджиев, А.С. Крысько, М.А. Мамедов и др.; под ред. Н.В. Захарченко. – Баку: ЭЛМ. – 2009. – 362 с.
111. Помехоустойчивость и эффективность систем передачи информации / [А.Г. Зюко, А.И. Фалько, И.П. Панфилов, В.Л. Банкет и др.]; под ред. А.Г. Зюко. – М.: Радио и связь, 1985. – 272 с.
112. Пухов Г.Е. Вычислительные устройства на таймерных скаляторах / Пухов Г.Е., Бордаченко В.П., Королев Ю.П. – К.: Техніка, 1991. – 215 с.
113. Радзимовский Б. К. Бинарные последовательности на основе систем с динамическим хаосом / Б. К. Радзимовский // Збірник наукових праць ОНАЗ ім. О. С. Попова. – 2012. – № 2. – С. 82–86.
114. Системы передачи документальной электросвязи : учеб. пособие / Н.В. Захарченко, Б.С. Владишевский, И.А. Киреев, А.П. Улеев и др.; под ред. Н.В. Захарченко. – Одесса: УГАС им. А.С. Попова, 2000. – 327 с.
115. Системы подвижной радиосвязи / [Пышкин И.М., Дежурный И.И., Талызин В.Н., Чвилев Г.Д.]. – М.: Радио и связь, 1986. – 328 с.
116. Системы радио-, телевизионного вещания и документальной электросвязи; под ред. Н.В. Захарченко. – Том 2: Системы электросвязи. – К.: Техніка, 1998 р. – 240 с.
117. Системы частотного мультиплексирования: учеб. пособ.; под ред. Н.В. Захарченко. – К.: Техніка, 2006 р. – 264 с.
118. Системы электросвязи: [учебник для вузов] / [В.П. Шувалов, С.И. Горшкова, Г.П. Катунин и др.]; под ред. В.П. Шувалова. – М.: Радио и связь, 1987.
119. Скрытность передачи в системах связи с хаотическими сигналами / Н. В Захарченко, С. М. Горохов, В. В. Корчинский, Б. К. Радзимовский // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2013. – № 3. – С. 161–164.
120. Сосин А.М., Захарченко В.Н., Шкуренко А.С. Пропускная способность канала при неравномерных МВС // Информатика и связь: Сб. Укр. гос. акад. связи им. А.С. Попова. – К.: Техніка, 1997. – С. 37–40.
121. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі. К.: Техніка, 2001. – 385 с.
122. Теория кодирования / [Касами Т., Такура Н., Ивадари Е., Инагаки Я.]; пер с япон.; под ред. Б.С. Цыбакова и С.И. Гельфанда. – М.: Мир, 1978. – 576.
123. Теория передачи сигналов: учебник для вузов / [Зюко А.Г., Кловский Д.Д., Назаров М.В., Финк Л.М.]. – М.: Радио и связь, 1986. – 304 с.
124. Теория электрической связи: учебн. для вузов / [Зюко А.Г., Кловский Д.Д., Коржик В.И., Назаров М.В.]; под ред. Д.Д. Кловского. – М.: Радио и связь, 1999. – 432 с.
125. Финк Л.М. Теория передачи дискретных сообщений / Финк Л.М. – М.: Сов. радио, 1970. – 726 с.

126. Харкевич А.А. Очерки общей теории святы / Харкевич А.А. – М.: Гостехиздат, 1955. – 268 с.
127. Хомич С.В. Корегування частини помилок у адаптивних систем із вирішальним зворотнім зв'язком на базі таймерних сигнальних конструкцій // С.В. Хомич, Ю.В. Белова, К.О. Осадчук // Матеріали 67-ї наук.-техн. конф. профес.-виклад. складу, науковців, аспірантів та студентів, (Одеса, 5 – 7 грудня 2012 р.) – Одеса, ОНАЗ ім. О.С. Попова, 2012. – С. 133– 135.
128. Хомич С.В. Корреляционный метод декодирования таймерных сигнальных конструкций / С.В. Хомич // Вестник НТУ «ХПИ». – 2011. – Вип. 58. – С. – 143–148.
129. Хомич С.В. Порівняльний аналіз обчислювального навантаження при декодуванні ТСК та блокових кодів / С.В.Хомич // Матеріали II міжн. наук.-практ. конф. [«Інфокомунікації – сучасність та майбутнє»]. – Ч. 2, (Одесса, 11–12 жовтня 2012 р.) – Одеса, 2012. – С. 152 – 154.
130. Цымбал В.П. Теория информации и кодирования / Цымбал В.П. – К.: Вища школа, 1977. – 288 с.
131. Шеннон К. Математическая теория святы. Роботы по теории информации и кибернетике / Шеннон К.; пер с англ.; под ред. Р.Л. Добрушина и О.В Лупанова. – М.: ИЛ, 1963. – 830 с.
132. / Эффективные системы передачи информации / Н.В. Захарченко, Е.М. Рудый, А.А. Варакин, М.А. Мамедов, М.М.Гаджиев; под ред. Н.В. Захарченко. – Баку: ЭЛМ. – 2007. – 568 с.

ДОДАТОК 1

I. Значення інтегралу імовірності

$$\Phi(x) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_0^x e^{-\frac{z^2}{2}} dz$$

x	Φ(x)	x	Φ(x)	x	Φ(x)
1.000	0.341344746068543	2.000	0.477249868051821	3.000	0.498650101968370
1.010	0.343752354978745	2.010	0.477784405570569	3.010	0.498693761551231
1.020	0.346135769627265	2.020	0.478308306232353	3.020	0.498736126572328
1.030	0.348494997211656	2.030	0.478821730357328	3.030	0.498777231306408
1.040	0.350830049669019	2.040	0.479324837133930	3.040	0.498817109256896
1.050	0.353140943624104	2.050	0.479817784594296	3.050	0.498855793168977
1.060	0.355427700336090	2.060	0.480300729590623	3.060	0.498893315042591
1.070	0.357690345644061	2.070	0.480773827772483	3.070	0.498929706145321
1.080	0.359928909911231	2.080	0.481237233565062	3.080	0.498964997025197
1.090	0.362143427967965	2.090	0.481691100148341	3.090	0.498999217523386
1.100	0.364333939053617	2.100	0.482135579437183	3.100	0.499032396786782
1.110	0.366500486757253	2.110	0.482570822062343	3.110	0.499064563280486
1.120	0.368643118957269	2.120	0.482996977352367	3.120	0.499095744800178
1.130	0.370761887759982	2.130	0.483414193316395	3.130	0.499125968484368
1.140	0.372856849437202	2.140	0.483822616627834	3.140	0.499155260826541
1.150	0.374928064362850	2.150	0.484222392608909	3.150	0.499183647687171
1.160	0.376975596948657	2.160	0.484613665216074	3.160	0.499211154305625
1.170	0.378999515578982	2.170	0.484996577026268	3.170	0.499237805311933
1.180	0.380999892544799	2.180	0.485371269224011	3.180	0.499263624738446
1.190	0.382976803976891	2.190	0.485737881589331	3.190	0.499288636031355
1.200	0.384930329778292	2.200	0.486096552486501	3.200	0.499312862062084
1.210	0.386860553556023	2.210	0.486447418853580	3.210	0.499336325138560
1.220	0.388767562552165	2.220	0.486790616192744	3.220	0.499359047016340
1.230	0.390651447574308	2.230	0.487126278561398	3.230	0.499381048909613
1.240	0.392512302925413	2.240	0.487454538564053	3.240	0.499402351502066
1.250	0.394350226333145	2.250	0.487775527344955	3.250	0.499422974957609
1.260	0.396165318878700	2.260	0.488089374581453	3.260	0.499442938930975
1.270	0.397957684925181	2.270	0.488396208478096	3.270	0.499462262578170
1.280	0.399727432045558	2.280	0.488696155761447	3.280	0.499480964566793
1.290	0.401474670950252	2.290	0.488989341675589	3.290	0.499499063086214
1.300	0.403199515414390	2.300	0.489275889978324	3.300	0.499516575857616
1.310	0.404902082204761	2.310	0.489555922938049	3.310	0.499533520143892
1.320	0.406582491006528	2.320	0.489829561331280	3.320	0.499549912759408
1.330	0.408240864349719	2.330	0.490096924440836	3.330	0.499565770079618
1.340	0.409877327535548	2.340	0.490358130054642	3.340	0.499581108050550
1.350	0.411492008562598	2.350	0.490613294465161	3.350	0.499595942198136
1.360	0.413085038052915	2.360	0.490862532469427	3.360	0.499610287637418
1.370	0.414656549178033	2.370	0.491105957369663	3.370	0.499624159081600
1.380	0.416206677584986	2.380	0.491343680974483	3.380	0.499637570850967
1.390	0.417735561322331	2.390	0.491575813600654	3.390	0.499650536881662
1.400	0.419243340766229	2.400	0.491802464075404	3.400	0.499663070734323
1.410	0.420730158546608	2.410	0.492023739739266	3.410	0.499675185602581
1.420	0.422196159473454	2.420	0.492239746449446	3.420	0.499686894321419
1.430	0.423641490463261	2.430	0.492450588583691	3.430	0.499698209375391
1.440	0.425066300465673	2.440	0.492656369044651	3.440	0.499709142906709

1.450	0.426470740390352	2.450	0.492857189264728	3.450	0.499719706723184
1.460	0.427854963034106	2.460	0.493053149211376	3.460	0.499729912306037
1.470	0.429219123008315	2.470	0.493244347392859	3.470	0.499739770817573
1.480	0.430563376666668	2.480	0.493430880864453	3.480	0.499749293108720
1.490	0.431887882033275	2.490	0.493612845235057	3.490	0.499758489726432
1.500	0.433192798731142	2.500	0.493790334674224	3.500	0.499767370920964
1.510	0.434478287911084	2.510	0.493963441919587	3.510	0.499775946653009
1.520	0.435744512181064	2.520	0.494132258284667	3.520	0.499784226600705
1.530	0.436991635536022	2.530	0.494296873667049	3.530	0.499792220166519
1.540	0.438219823288188	2.540	0.494457376556917	3.540	0.499799936483993
1.550	0.439429241997941	2.550	0.494613854045933	3.550	0.499807384424364
1.560	0.440620059405207	2.560	0.494766391836444	3.560	0.499814572603067
1.570	0.441792444361447	2.570	0.494915074251009	3.570	0.499821509386095
1.580	0.442946566762246	2.580	0.495059984242229	3.580	0.499828202896254
1.590	0.444082597480531	2.590	0.495201203402874	3.590	0.499834661019280
1.600	0.445200708300442	2.600	0.495338811976281	3.600	0.499840891409843
1.610	0.446301071851880	2.610	0.495472888867033	3.610	0.499846901497426
1.620	0.447383861545748	2.620	0.495603511651879	3.620	0.499852698492093
1.630	0.448449251509911	2.630	0.495730756590910	3.630	0.499858289390124
1.640	0.449497416525896	2.640	0.495854698638964	3.640	0.499863680979554
1.650	0.450528531966352	2.650	0.495975411457242	3.650	0.499868879845580
1.660	0.451542773733277	2.660	0.496092967425147	3.660	0.499873892375862
1.670	0.452540318197053	2.670	0.496207437652314	3.670	0.499878724765715
1.680	0.453521342136280	2.680	0.496318891990825	3.680	0.499883383023185
1.690	0.454486022678450	2.690	0.496427399047600	3.690	0.499887872974018
1.700	0.455434537241457	2.700	0.496533026196959	3.700	0.499892200266523
1.710	0.456367063475968	2.710	0.496635839593331	3.710	0.499896370376326
1.720	0.457283779208671	2.720	0.496735904184109	3.720	0.499900388611024
1.730	0.458184862386405	2.730	0.496833283722642	3.730	0.499904260114731
1.740	0.459070491021193	2.740	0.496928040781349	3.740	0.499907989872526
1.750	0.459940843136183	2.750	0.497020236764945	3.750	0.499911582714799
1.760	0.460796096712517	2.760	0.497109931923774	3.760	0.499915043321502
1.770	0.461636429637129	2.770	0.497197185367235	3.770	0.499918376226297
1.780	0.462462019651483	2.780	0.497282055077299	3.780	0.499921585820616
1.790	0.463273044301274	2.790	0.497364597922095	3.790	0.499924676357621
1.800	0.464069680887074	2.800	0.497444869669572	3.800	0.499927651956075
1.810	0.464852106415961	2.810	0.497522925001214	3.810	0.499930516604120
1.820	0.465620497554110	2.820	0.497598817525811	3.820	0.499933274162970
1.830	0.466375030580372	2.830	0.497672599793268	3.830	0.499935928370511
1.840	0.467115881340836	2.840	0.497744323308458	3.840	0.499938482844817
1.850	0.467843225204386	2.850	0.497814038545087	3.850	0.499940941087581
1.860	0.468557237019247	2.860	0.497881794959595	3.860	0.499943306487466
1.870	0.469258091070534	2.870	0.497947641005060	3.870	0.499945582323366
1.880	0.469945961038800	2.880	0.498011624145106	3.880	0.499947771767598
1.890	0.470621019959591	2.890	0.498073790867812	3.890	0.499949877889004
1.900	0.471283440183998	2.900	0.498134186699616	3.900	0.499951903655982
1.910	0.471933393340228	2.910	0.498192856219194	3.910	0.499953851939444
1.920	0.472571050296163	2.920	0.498249843071324	3.920	0.499955725515688
1.930	0.473196581122945	2.930	0.498305189980723	3.930	0.499957527069211
1.940	0.473810155059547	2.940	0.498358938765843	3.940	0.499959259195442
1.950	0.474411940478362	2.950	0.498411130352635	3.950	0.499960924403402
1.960	0.475002104851780	2.960	0.498461804788262	3.960	0.499962525118309
1.970	0.475580814719778	2.970	0.498511001254762	3.970	0.499964063684097
1.980	0.476148235658492	2.980	0.498558758082660	3.980	0.499965542365885
1.990	0.476704532249788	2.990	0.498605112764508	3.990	0.499966963352371
2.000	0.477249868051821	3.000	0.498650101968370	4.000	0.499968328758167

x	$\Phi(x)$	x	$\Phi(x)$	x	$\Phi(x)$
4.000	0.499968328758167	5.000	0.499999713348428	6.000	0.499999999013412
4.010	0.499969640626073	5.010	0.499999727849823	6.010	0.499999999072383
4.020	0.499970900929288	5.020	0.499999741642602	6.020	0.499999999127915
4.030	0.499972111573560	5.030	0.499999754760082	6.030	0.499999999180201
4.040	0.499973274399281	5.040	0.499999767234077	6.040	0.499999999229429
4.050	0.499974391183526	5.050	0.499999779094968	6.050	0.499999999275771
4.060	0.499975463642034	5.060	0.499999790371761	6.060	0.499999999319392
4.070	0.499976493431132	5.070	0.499999801092149	6.070	0.499999999360449
4.080	0.499977482149612	5.080	0.499999811282566	6.080	0.499999999399087
4.090	0.499978431340552	5.090	0.499999820968243	6.090	0.499999999435446
4.100	0.499979342493088	5.100	0.499999830173259	6.100	0.499999999469658
4.110	0.499980217044132	5.110	0.499999838920594	6.110	0.499999999501844
4.120	0.499981056380049	5.120	0.499999847232172	6.120	0.499999999532123
4.130	0.499981861838282	5.130	0.499999855128911	6.130	0.499999999560605
4.140	0.499982634708927	5.140	0.499999862630766	6.140	0.499999999587393
4.150	0.499983376236270	5.150	0.499999869756771	6.150	0.499999999612585
4.160	0.499984087620281	5.160	0.499999876525079	6.160	0.499999999636275
4.170	0.499984770018052	5.170	0.499999882953003	6.170	0.499999999658550
4.180	0.499985424545209	5.180	0.499999889057050	6.180	0.499999999679492
4.190	0.499986052277273	5.190	0.499999894852960	6.190	0.499999999699179
4.200	0.499986654250984	5.200	0.499999900355737	6.200	0.499999999717684
4.210	0.499987231465586	5.210	0.499999905579684	6.210	0.499999999735077
4.220	0.499987784884075	5.220	0.499999910538435	6.220	0.499999999751422
4.230	0.499988315434405	5.230	0.499999915244980	6.230	0.499999999766782
4.240	0.499988824010668	5.240	0.499999919711701	6.240	0.499999999781214
4.250	0.499989311474225	5.250	0.499999923950395	6.250	0.499999999794774
4.260	0.499989778654816	5.260	0.499999927972299	6.260	0.499999999807511
4.270	0.499990226351627	5.270	0.499999931788121	6.270	0.499999999819476
4.280	0.499990655334330	5.280	0.499999935408057	6.280	0.499999999830713
4.290	0.499991066344087	5.290	0.499999938841820	6.290	0.499999999841267
4.300	0.499991460094529	5.300	0.499999942098660	6.300	0.499999999851177
4.310	0.499991837272697	5.310	0.499999945187383	6.310	0.499999999860482
4.320	0.499992198539962	5.320	0.499999948116374	6.320	0.499999999869218
4.330	0.499992544532909	5.330	0.499999950893617	6.330	0.499999999877419
4.340	0.499992875864199	5.340	0.499999953526709	6.340	0.499999999885117
4.350	0.499993193123401	5.350	0.499999956022884	6.350	0.499999999892342
4.360	0.499993496877799	5.360	0.499999958389024	6.360	0.499999999899123
4.370	0.499993787673173	5.370	0.499999960631679	6.370	0.499999999905486
4.380	0.499994066034554	5.380	0.499999962757081	6.380	0.499999999911456
4.390	0.499994332466958	5.390	0.499999964771158	6.390	0.499999999917057
4.400	0.499994587456092	5.400	0.499999966679552	6.400	0.499999999922311
4.410	0.499994831469043	5.410	0.499999968487626	6.410	0.499999999927240
4.420	0.499995064954938	5.420	0.499999970200482	6.420	0.499999999931863
4.430	0.499995288345588	5.430	0.499999971822974	6.430	0.499999999936198
4.440	0.499995502056112	5.440	0.499999973359714	6.440	0.499999999940263
4.450	0.499995706485530	5.450	0.499999974815090	6.450	0.499999999944075
4.460	0.499995902017353	5.460	0.499999976193271	6.460	0.499999999947648
4.470	0.499996089020140	5.470	0.499999977498221	6.470	0.499999999950998
4.480	0.499996267848039	5.480	0.499999978733708	6.480	0.499999999954138
4.490	0.499996438841321	5.490	0.499999979903313	6.490	0.499999999957082
4.500	0.499996602326875	5.500	0.499999981010438	6.500	0.499999999959840

4.510	0.499996758618713	5.510	0.499999982058315	6.510	0.49999999962424
4.520	0.499996908018431	5.520	0.499999983050017	6.520	0.49999999964846
4.530	0.499997050815677	5.530	0.499999983988461	6.530	0.49999999967115
4.540	0.499997187288588	5.540	0.499999984876418	6.540	0.49999999969240
4.550	0.499997317704220	5.550	0.499999985716520	6.550	0.49999999971231
4.560	0.499997442318961	5.560	0.499999986511268	6.560	0.49999999973096
4.570	0.499997561378926	5.570	0.499999987263033	6.570	0.49999999974842
4.580	0.499997675120350	5.580	0.499999987974071	6.580	0.49999999976477
4.590	0.499997783769952	5.590	0.499999988646519	6.590	0.49999999978008
4.600	0.499997887545298	5.600	0.499999989282410	6.600	0.49999999979442
4.610	0.499997986655145	5.610	0.499999989883669	6.610	0.49999999980784
4.620	0.499998081299780	5.620	0.499999990452127	6.620	0.49999999982040
4.630	0.499998171671336	5.630	0.499999990989519	6.630	0.49999999983215
4.640	0.499998257954110	5.640	0.499999991497492	6.640	0.49999999984316
4.650	0.499998340324856	5.650	0.499999991977608	6.650	0.49999999985345
4.660	0.499998418953081	5.660	0.499999992431350	6.660	0.49999999986308
4.670	0.499998494001322	5.670	0.499999992860124	6.670	0.49999999987210
4.680	0.499998565625416	5.680	0.499999993265263	6.680	0.49999999988053
4.690	0.499998633974755	5.690	0.499999993648031	6.690	0.49999999988841
4.700	0.499998699192546	5.700	0.499999994009629	6.700	0.49999999989579
4.710	0.499998761416043	5.710	0.499999994351191	6.710	0.49999999990269
4.720	0.499998820776784	5.720	0.499999994673797	6.720	0.49999999990914
4.730	0.499998877400815	5.730	0.499999994978468	6.730	0.49999999991517
4.740	0.499998931408906	5.740	0.499999995266172	6.740	0.49999999992081
4.750	0.499998982916758	5.750	0.499999995537828	6.750	0.49999999992608
4.760	0.499999032035204	5.760	0.499999995794303	6.760	0.49999999993101
4.770	0.499999078870404	5.770	0.499999996036423	6.770	0.49999999993561
4.780	0.499999123524027	5.780	0.499999996264969	6.780	0.49999999993992
4.790	0.499999166093434	5.790	0.499999996480679	6.790	0.49999999994394
4.800	0.499999206671848	5.800	0.499999996684254	6.800	0.49999999994770
4.810	0.499999245348521	5.810	0.499999996876358	6.810	0.49999999995120
4.820	0.499999282208893	5.820	0.499999997057619	6.820	0.49999999995448
4.830	0.499999317334747	5.830	0.499999997228631	6.830	0.49999999995755
4.840	0.499999350804357	5.840	0.499999997389959	6.840	0.49999999996041
4.850	0.499999382692628	5.850	0.499999997542135	6.850	0.49999999996308
4.860	0.499999413071236	5.860	0.499999997685664	6.860	0.49999999996558
4.870	0.499999442008757	5.870	0.499999997821024	6.870	0.49999999996791
4.880	0.499999469570797	5.880	0.499999997948668	6.880	0.49999999997008
4.890	0.499999495820112	5.890	0.499999998069022	6.890	0.49999999997211
4.900	0.499999520816723	5.900	0.499999998182492	6.900	0.49999999997401
4.910	0.499999544618035	5.910	0.499999998289461	6.910	0.49999999997578
4.920	0.499999567278938	5.920	0.499999998390292	6.920	0.49999999997743
4.930	0.499999588851916	5.930	0.499999998485327	6.930	0.49999999997897
4.940	0.499999609387146	5.940	0.499999998574890	6.940	0.49999999998041
4.950	0.499999628932592	5.950	0.499999998659287	6.950	0.49999999998175
4.960	0.499999647534102	5.960	0.499999998738810	6.960	0.49999999998300
4.970	0.499999665235492	5.970	0.499999998813732	6.970	0.49999999998417
4.980	0.499999682078634	5.980	0.499999998884312	6.980	0.49999999998526
4.990	0.499999698103538	5.990	0.499999998950795	6.990	0.49999999998628
5.000	0.499999713348428	6.000	0.499999999013412	7.000	0.49999999998722

x	$\Phi(x)$	x	$\Phi(x)$	x	$\Phi(x)$
7.000	0.49999999998722	8.000	0.500000000000051	9.000	0.49999999999237
7.010	0.49999999998811	8.010	0.500000000000051	9.010	0.49999999999212
7.020	0.49999999998893	8.020	0.500000000000052	9.020	0.49999999999188
7.030	0.49999999998970	8.030	0.500000000000052	9.030	0.49999999999163
7.040	0.49999999999042	8.040	0.500000000000052	9.040	0.49999999999137
7.050	0.49999999999108	8.050	0.500000000000052	9.050	0.49999999999111
7.060	0.49999999999171	8.060	0.500000000000052	9.060	0.49999999999085
7.070	0.49999999999229	8.070	0.500000000000052	9.070	0.49999999999058
7.080	0.49999999999283	8.080	0.500000000000052	9.080	0.49999999999031
7.090	0.49999999999333	8.090	0.500000000000051	9.090	0.49999999999003
7.100	0.49999999999380	8.100	0.500000000000051	9.100	0.49999999998975
7.110	0.49999999999424	8.110	0.500000000000051	9.110	0.49999999998946
7.120	0.49999999999465	8.120	0.500000000000051	9.120	0.49999999998917
7.130	0.49999999999503	8.130	0.500000000000050	9.130	0.49999999998888
7.140	0.49999999999538	8.140	0.500000000000049	9.140	0.49999999998858
7.150	0.49999999999571	8.150	0.500000000000049	9.150	0.49999999998827
7.160	0.49999999999602	8.160	0.500000000000048	9.160	0.49999999998797
7.170	0.49999999999631	8.170	0.500000000000047	9.170	0.49999999998766
7.180	0.49999999999658	8.180	0.500000000000046	9.180	0.49999999998734
7.190	0.49999999999682	8.190	0.500000000000045	9.190	0.49999999998702
7.200	0.49999999999706	8.200	0.500000000000044	9.200	0.49999999998670
7.210	0.49999999999727	8.210	0.500000000000043	9.210	0.49999999998637
7.220	0.49999999999747	8.220	0.500000000000041	9.220	0.49999999998604
7.230	0.49999999999766	8.230	0.500000000000040	9.230	0.49999999998570
7.240	0.49999999999784	8.240	0.500000000000039	9.240	0.49999999998536
7.250	0.49999999999800	8.250	0.500000000000037	9.250	0.49999999998502
7.260	0.49999999999815	8.260	0.500000000000035	9.260	0.49999999998467
7.270	0.49999999999829	8.270	0.500000000000033	9.270	0.49999999998432
7.280	0.49999999999843	8.280	0.500000000000031	9.280	0.49999999998397
7.290	0.49999999999855	8.290	0.500000000000029	9.290	0.49999999998361
7.300	0.49999999999866	8.300	0.500000000000027	9.300	0.49999999998325
7.310	0.49999999999877	8.310	0.500000000000024	9.310	0.49999999998289
7.320	0.49999999999887	8.320	0.500000000000022	9.320	0.49999999998252
7.330	0.49999999999896	8.330	0.500000000000019	9.330	0.49999999998215
7.340	0.49999999999905	8.340	0.500000000000016	9.340	0.49999999998178
7.350	0.49999999999913	8.350	0.500000000000013	9.350	0.49999999998141
7.360	0.49999999999921	8.360	0.500000000000010	9.360	0.49999999998103
7.370	0.49999999999928	8.370	0.500000000000006	9.370	0.49999999998065
7.380	0.49999999999935	8.380	0.500000000000003	9.380	0.49999999998027
7.390	0.49999999999941	8.390	0.499999999999999	9.390	0.49999999997988
7.400	0.49999999999947	8.400	0.499999999999995	9.400	0.49999999997950
7.410	0.49999999999952	8.410	0.499999999999991	9.410	0.49999999997911
7.420	0.49999999999957	8.420	0.499999999999987	9.420	0.49999999997872
7.430	0.49999999999962	8.430	0.499999999999982	9.430	0.49999999997833
7.440	0.49999999999966	8.440	0.499999999999977	9.440	0.49999999997794
7.450	0.49999999999971	8.450	0.499999999999972	9.450	0.49999999997755
7.460	0.49999999999975	8.460	0.499999999999967	9.460	0.49999999997715
7.470	0.49999999999978	8.470	0.499999999999962	9.470	0.49999999997676
7.480	0.49999999999982	8.480	0.499999999999956	9.480	0.49999999997636
7.490	0.49999999999985	8.490	0.499999999999950	9.490	0.49999999997597
7.500	0.49999999999988	8.500	0.499999999999944	9.500	0.49999999997557
7.510	0.49999999999991	8.510	0.499999999999938	9.510	0.49999999997517
7.520	0.49999999999994	8.520	0.499999999999932	9.520	0.49999999997478

7.530	0.499999999999997	8.530	0.499999999999925	9.530	0.499999999997439
7.540	0.499999999999999	8.540	0.499999999999918	9.540	0.499999999997399
7.550	0.500000000000002	8.550	0.499999999999911	9.550	0.499999999997360
7.560	0.500000000000004	8.560	0.499999999999903	9.560	0.499999999997321
7.570	0.500000000000006	8.570	0.499999999999895	9.570	0.499999999997282
7.580	0.500000000000008	8.580	0.499999999999887	9.580	0.499999999997244
7.590	0.500000000000010	8.590	0.499999999999879	9.590	0.499999999997205
7.600	0.500000000000012	8.600	0.499999999999870	9.600	0.499999999997167
7.610	0.500000000000014	8.610	0.499999999999862	9.610	0.499999999997129
7.620	0.500000000000015	8.620	0.499999999999852	9.620	0.499999999997091
7.630	0.500000000000017	8.630	0.499999999999843	9.630	0.499999999997054
7.640	0.500000000000019	8.640	0.499999999999833	9.640	0.499999999997017
7.650	0.500000000000020	8.650	0.499999999999823	9.650	0.499999999996981
7.660	0.500000000000022	8.660	0.499999999999812	9.660	0.499999999996945
7.670	0.500000000000023	8.670	0.499999999999802	9.670	0.499999999996909
7.680	0.500000000000025	8.680	0.499999999999791	9.680	0.499999999996874
7.690	0.500000000000026	8.690	0.499999999999779	9.690	0.499999999996840
7.700	0.500000000000027	8.700	0.499999999999767	9.700	0.499999999996806
7.710	0.500000000000029	8.710	0.499999999999755	9.710	0.499999999996773
7.720	0.500000000000030	8.720	0.499999999999743	9.720	0.499999999996740
7.730	0.500000000000031	8.730	0.499999999999730	9.730	0.499999999996709
7.740	0.500000000000032	8.740	0.499999999999717	9.740	0.499999999996678
7.750	0.500000000000033	8.750	0.499999999999704	9.750	0.499999999996647
7.760	0.500000000000034	8.760	0.499999999999689	9.760	0.499999999996618
7.770	0.500000000000035	8.770	0.499999999999675	9.770	0.499999999996589
7.780	0.500000000000036	8.780	0.499999999999661	9.780	0.499999999996562
7.790	0.500000000000037	8.790	0.499999999999646	9.790	0.499999999996535
7.800	0.500000000000038	8.800	0.499999999999630	9.800	0.499999999996510
7.810	0.500000000000039	8.810	0.499999999999615	9.810	0.499999999996485
7.820	0.500000000000040	8.820	0.499999999999598	9.820	0.499999999996462
7.830	0.500000000000041	8.830	0.499999999999582	9.830	0.499999999996440
7.840	0.500000000000042	8.840	0.499999999999565	9.840	0.499999999996418
7.850	0.500000000000043	8.850	0.499999999999547	9.850	0.499999999996399
7.860	0.500000000000044	8.860	0.499999999999530	9.860	0.499999999996380
7.870	0.500000000000044	8.870	0.499999999999512	9.870	0.499999999996363
7.880	0.500000000000045	8.880	0.499999999999493	9.880	0.499999999996348
7.890	0.500000000000046	8.890	0.499999999999474	9.890	0.499999999996334
7.900	0.500000000000046	8.900	0.499999999999455	9.900	0.499999999996321
7.910	0.500000000000047	8.910	0.499999999999435	9.910	0.499999999996310
7.920	0.500000000000047	8.920	0.499999999999414	9.920	0.499999999996301
7.930	0.500000000000048	8.930	0.499999999999394	9.930	0.499999999996293
7.940	0.500000000000049	8.940	0.499999999999373	9.940	0.499999999996288
7.950	0.500000000000049	8.950	0.499999999999351	9.950	0.499999999996284
7.960	0.500000000000050	8.960	0.499999999999329	9.960	0.499999999996282
7.970	0.500000000000050	8.970	0.499999999999307	9.970	0.499999999996281
7.980	0.500000000000051	8.980	0.499999999999284	9.980	0.499999999996283
7.990	0.500000000000051	8.990	0.499999999999260	9.990	0.499999999996288
8.000	0.500000000000051	9.000	0.499999999999237	10.00	0.499999999996294

II. Апроксимація інтегралу ймовірності з похибкою $\delta < 0,02$

$$\Phi(x) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_0^x e^{-\frac{z^2}{2}} dz \approx 0,5 - 0,65[-0,44(x + 0,75)^2]$$

ДОДАТОК 2

Алгебраїчні структури та поля Галуа

Пошук хороших кодів, що контролюють помилки, значною мірою пов'язаний зі структурами сучасної алгебри. Багато знайдених важливих кодів засновані на структурах кілець багаточленів і полів Галуа. Крім того, ці алгебраїчні поняття та методи є необхідним робочим інструментом для конструювання кодерів та декодерів. Розглянемо основні розділи алгебри, які важливі для теорії кодів, що контролюють помилки.

Бінарне і 16-елементне поле. Дійсні числа утворюють відому множину математичних об'єктів, які можна додавати, множити, віднімати і ділити. Аналогічно комплексні числа утворюють множину об'єктів, які можна складати, додавати, множити і ділити. Обидві ці арифметичні системи є найважливішою основою всіх інженерних дисциплін. Усі множини математичних арифметичних систем об'єктів складаються із множин і операцій над елементами цих множин. Такими операціями є – «додавання», «віднімання», «множення» і «ділення». Вони не обов'язково відповідають операціям елементарної арифметики.

Існуючі в сучасній алгебрі арифметичні системи класифікуються відповідно до ускладнення їхньої математичної структури. Наведемо формальну класифікацію таких систем. Дамо основні визначення:

1) *абелева група*: множина математичних об'єктів, які можна «додавати» і «віднімати»;

2) *кілець*: множина математичних об'єктів, які можна «додавати», «віднімати» і «множити»;

3) *поле*: множина математичних об'єктів, які можна «додавати», «віднімати», «множити» і «ділити».

Зауважимо, що назви цих операцій взяті в лапки тому, що, взагалі кажучи, вони не є прийнятими арифметичними операціями; ці назви вживаються через їхню подібність з прийнятими.

Перш ніж переходити до формальних понять, виконаємо деякі обчислення в найпростішому із усіх можливих полів, а саме в полі, що складається тільки з двох елементів. (Поле дійсних чисел містить незчисленну кількість елементів). Позначимо через 0 і 1 два елементи поля та визначимо операції додавання й множення рівностями

$$\begin{aligned}0 + 0 &= 0, & 0 \cdot 0 &= 0, \\0 + 1 &= 1, & 0 \cdot 1 &= 0, \\1 + 0 &= 1, & 1 \cdot 0 &= 0, \\1 + 1 &= 0, & 1 \cdot 1 &= 1.\end{aligned}$$

Так визначені додавання й множення називаються *додаванням за модулем 2* і *множенням за модулем 2*. Зазначимо, що із рівності $1 + 1 = 0$ слідує, що $-1 = 1$, а із рівності $1 \cdot 1 = 1$ – що $1^{-1} = 1$. Використовуючи це, легко

перевірити, що, за винятком ділення на нуль, віднімання та ділення завжди визначені. Алфавіт із двох символів 0 та 1 разом з додаванням за модулем 2 та множенням за модулем 2 називається *полем із двох елементів* і позначається через $GF(2)$.

У зазначеній арифметичній системі можна здійснювати відомі алгебраїчні операції. Прикладом є наступна система рівнянь над полем $GF(2)$:

$$\begin{aligned} X + Y + Z &= 1, \\ X + Y &= 0, \\ X + Z &= 1. \end{aligned}$$

Цю систему можна розв'язати відніманням третього рівняння із першого, що дає $Y = 0$. Тоді із другого рівняння отримуємо $X = 0$, а із першого рівняння $Z = 1$. Підстановкою отриманого розв'язання у вихідну систему рівнянь перевіряємо, що воно вірне.

Щоб отримати інший спосіб розв'язання, припустимо, що можна довести можливість застосування звичайних методів лінійної алгебри над полем $GF(2)$. Визначник системи обчислюється таким чином:

$$\begin{aligned} D &= \det \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - 1 \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \\ &= 1 \cdot 1 - 1 \cdot 1 - 1 \cdot 1 = -1 = 1. \end{aligned}$$

Цю систему рівнянь можна розв'язати за правилом Крамера:

$$\begin{aligned} X &= D^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = 0, & Y &= D^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = 0, \\ Z &= D^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = 1. \end{aligned}$$

Другим прикладом поля є 6-10-поле. Це поле містить 16 елементів, які ми позначимо символами 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Таблиці додавання та множення в цьому полі вписані на рис. 1. Зазначимо, що тут правила додавання та множення значно відрізняються від відомих правил додавання й множення дійсних чисел; у той самий час ці таблиці мають внутрішню закономірність і дозволяють здійснювати віднімання та ділення. Для ділення слід взяти $x: y = x \cdot (y^{-1})$, де y^{-1} – елемент поля, що задовольняє умові $y \cdot y^{-1} = 1$. Перегляд таблиці множення показує, що кожний ненульовий елемент має зворотний, а, отже, ділення завжди визначене, за винятком ділення на нуль.

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

a

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

б

Рисунок 1 – 6-10-поле: *a* – таблиця додавання; *б* – таблиця множення.

Більшість методів лінійної алгебри, так само як і матричні операції, переносяться на випадок довільного поля. Саме тому поля з кінцевим числом елементів виявились дуже корисними. Ми будемо вивчати ці поля й знайдемо способи побудови таблиць, додавання та множення, які породжують поле навіть для значної кількості елементів. Згодом ми побачимо, що поля з q елементами можна побудувати тоді й тільки тоді, коли q дорівнює p^m , де p – просте, а m – довільне позитивне ціле число. Але перш за все ми повинні ввести поняття груп і кілець.

Групи. Група – це збиральна назва деяких алгебраїчних структур. Хоча існують багато конкретних прикладів цікавих груп, у математиці введено абстрактне поняття групи, тому що легше одночасно досліджувати всі математичні системи із загальною структурою, ніж досліджувати кожен з них окремо.

Визначення 1. Групою G називається множина елементів із визначеною для кожної пари елементів операцією (позначеною $*$), що володіє такими чотирма властивостями:

1) *замкненість*: для кожної пари a і b із множини елемент $c = a * b$ належить множині;

2) *асоціативність*: для всіх a, b і c із множини

$$a * (b * c) = (a * b) * c;$$

3) *існування одиниці*: у множині існує елемент e , який називається одиничним елементом і такий, що

$$a * e = e * a = a$$

для будь-якого елемента a множини;

4) *існування зворотних елементів*: для будь-якого a із множини існує деякий елемент b із множини, який називається зворотним елементу a і такий, що

$$a * b = b * a = e.$$

Якщо група G містить кінцеве число елементів, то вона називається *кінцевою групою*, а число елементів в G називається *порядком* G .

Деякі групи володіють тією додатковою властивістю, що для будь-яких a і b із групи

$$a * b = b * a.$$

Ця властивість називається *комутативністю*. Групи, що володіють цією додатковою властивістю, називаються *комутативними* або *абелевими групами*. За винятком деякого матеріалу цього додатка ми завжди будемо мати справу з абелевими групами.

У випадку абелевих груп групова операція позначається символом $+$ і називається додаванням (навіть тоді, коли вона не є звичайним арифметичним додаванням). У цьому випадку одиничний елемент називається нулем і позначається 0 , а зворотний елементу a елемент записується у вигляді $-a$, отже

$$a + (-a) = (-a) + a = 0.$$

Іноді групова операція позначається символом \cdot і називається множенням (навіть тоді, коли вона не є звичайним арифметичним множенням). У цьому випадку одиничний елемент називається одиницею і позначається 1 , а зворотний елементу a елемент записується у вигляді a^{-1} ; отже

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Теорема 1. Одиничний елемент у кожній групі є єдиним. Для кожного елемента групи зворотний елемент також є єдиним, і $(a^{-1})^{-1} = a$.

Доведення. Припустимо, що e і e' – одиничні елементи групи; тоді $e = e * e' = e'$. Далі припустимо, що b і b' – елементи, зворотні елементу a ; тоді

$$b = b * (a * b') = (b * a) * b' = b'.$$

Нарешті, $a^{-1}a = aa^{-1} = 1$, отже a – зворотний елементу a^{-1} . Але в силу єдиності зворотного елемента $(a^{-1})^{-1} = a$.

Існує безліч прикладів груп. Більшість груп містять нескінченну кількість елементів. Прикладами є цілі числа відносно додавання, позитивні раціональні числа відносно множення. Багато інших груп містять лише кінцеве число елементів. Прикладами є двоелементна множина $\{0, 1\}$ відносно операції «виняткового або» (додавання за модулем 2), множина $\{0, 1, \dots, 8, 9\}$ відносно додавання за модулем 10 і т.д.

Як більш складний приклад побудуємо кінцеву неабелеву групу, тобто менш відому структуру. Одним із способів побудови груп з цікавою алгебраїчною структурою є дослідження перетворень простих геометричних фігур і алгебраїчна інтерпретація цих перетворень. Наприклад, рівносторонній трикутник з вершинами A , B і C (пронумерованими за годинниковою стрілкою) можна обертаням або віддзеркаленням відносно осі відобразити на себе точно шістьма різними способами, причому кожне з цих обертань і віддзеркалень має зворотне перетворення. Використовуючи деякі очевидні факти, можна швидко побудувати алгебраїчну групу. Позначимо ці шість перетворень символами $1, a, b, c, d$ і e таким чином:

- $1 = (ABC \rightarrow ABC)$ (немає змін),
- $a = (ABC \rightarrow CAB)$ (обертання проти годинникової стрілки),
- $b = (ABC \rightarrow BCA)$ (обертання за годинниковою стрілкою),
- $c = (ABC \rightarrow ACB)$ (віддзеркалення відносно бісектриси кута A),
- $d = (ABC \rightarrow CBA)$ (віддзеркалення відносно бісектриси кута B),
- $e = (ABC \rightarrow BAC)$ (віддзеркалення відносно бісектриси кута C),

де перетворення $ABC \rightarrow BCA$ означає, що вершина A переходить у вершину B , вершина B переходить у вершину C , а вершина C переходить у вершину A . Таким чином, трикутник повертається на 120° . Нехай група $(G, *)$ визначається множиною

$$G = \{1, a, b, c, d, e\}$$

і $y*x$ є елементом групи, що позначає перетворення, яке отримується послідовним виконанням спочатку перетворення x , а потім перетворення y ; наприклад,

$$a*d = (ABC \rightarrow BCA) * (ABC \rightarrow CBA) = (ABC \rightarrow BAC) = e.$$

Діючи таким чином, можна побудувати таблицю для $x*y$:

$x \backslash y$	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	d	e	c
b	b	1	a	e	c	d
c	c	e	d	1	b	a
d	d	c	e	a	1	b
e	e	d	c	b	a	1

Оскільки таблиця побудована, можна забути про її геометричне походження. Таблиця сама визначає групу. Підкреслимо, що це приклад неабелевої групи, тому що $a*c \neq c*a$. Зауважимо також, що кожний елемент з'являється один раз у кожному стовпці й у кожному рядку. Для кінцевих груп це виконується завжди.

Нашим останнім прикладом групи є група перестановок n літер. Нехай X є множина $\{1, 2, \dots, n\}$. Взаємно-однозначне відображення цієї множини на самого себе називається *перестановкою*. Всього є $n!$ таких перестановок, і можна визначити групу, яка називається симетричною групою й позначається через S_n , елементами якої є перестановки на множині X . (Спочатку може трохи турбувати та обставина, що елементами групи є оператори – оператори перестановок на множині X . Насправді в прикладі перетворень рівностороннього трикутника мова також іде про групу перестановок). Якщо взяти перестановку на вибраних цілих числах і переставити їх ще раз, то вийде інша перестановка на цих цілих числах. Виберемо як групову операцію $*$ таку композицію перестановок і візьмемо, наприклад, $n = 4$. Всього є $4! = 24$ перестановок в групі S_4 . Типовий елемент групи S_4 дорівнює

$$a = [(1\ 2\ 3\ 4) \rightarrow (3\ 1\ 4\ 2)]$$

і є перестановкою, яка заміняє 1 на 3, 2 на 1, 3 на 4 і 4 на 2. Іншою такою перестановкою є

$$b = [(1\ 2\ 3\ 4) \rightarrow (4\ 1\ 3\ 2)].$$

Тоді добуток $b*a$ в групі S_4 дорівнює перестановці, яка отримується у результаті застосування спочатку a , а потім b :

$$b*a = [(1\ 2\ 3\ 4) \rightarrow (2\ 3\ 4\ 1)],$$

що є елементом групи S_4 . З таким визначенням множення група перестановок S_4 є неабелевою групою, що містить 24 елементи.

Нехай G – група, і нехай H – деяка підмножина в G . Тоді H називається підгрупою групи G , якщо вона є групою щодо обмеження

операції $*$ на H . Для того щоб перевірити, що непуста множина H є підгрупою групи G , необхідно тільки перевірити, що для всіх a і b із H елемент $a*b$ належить H (замкненість) і що елемент, зворотний до a із H , також належить H . Інші групові властивості наслідуються із групи G . Як згодом ми побачимо при розгляданні циклічних підгруп, у випадку кінцевих груп із властивості замкненості автоматично впливає навіть властивість існування зворотного елемента.

Наприклад, множина всіх парних чисел і множина чисел, кратних 3, є підгрупами у множині всіх цілих чисел (додатних, від'ємних і нуля) відносно операції додавання.

Один із шляхів побудови підгрупи H кінцевої групи G полягає у виборі довільного елемента h групи H і формуванні H як множини елементів, утворених множенням h на самого себе довільне число разів. Таким чином, будуюмо послідовність елементів

$$h, h*h, h*h*h, h*h*h*h, \dots,$$

позначаючи їх для зручності через h, h^2, h^3, h^4, \dots . Так як G кінцева, то тільки кінцеве число цих елементів різне, так що з деякого моменту послідовність почне повторюватися. Першим повторюваним елементом повинен бути сам елемент h , тому що якщо два різних елементи h^i і h^j рівні, то їх можна помножити на елемент, зворотний h , і отримати, що h^{i-1} і h^{j-1} також рівні. Далі зазначимо, що якщо $h^j = h$, то $h^{j-1} = 1$, одиничному елементу групи. Множина H називається *підгрупою*, породженою елементом h . Число c елементів в H називається *порядком* елемента h . Множина елементів $h, h^2, h^3, \dots, h^c = 1$ називається *циклом*. Цикл є підгрупою, тому що добуток двох елементів такого виду знову є елементом цього виду, а елемент, зворотний елементу h^i , дорівнює h^{c-i} і, отже, є одним із елементів циклу. Група, що складається із усіх степенів одного з її елементів, називається *циклічною групою*.

Для заданих кінцевої групи G і підгрупи H існує важлива операція, що установлює деякі взаємозв'язки між G і H і називається *розкладанням групи G на суміжні класи по H* . Позначимо через h_1, h_2, h_3, \dots елементи з H , причому через h_1 позначимо одиничний елемент. Побудуємо таблицю таким чином. Перший рядок складається з елементів підгрупи H , причому першим зліва виписаний одиничний елемент h_1 і кожний елемент із H записаний у рядку один і тільки один раз. Виберемо довільний елемент групи G , що не міститься в першому рядку. Назвемо його g_2 і використаємо як перший елемент другого рядка. Інші елементи другого рядка отримуються множенням зліва елементів підгрупи на цей перший елемент. Аналогічно будуюмо третій, четвертий і п'ятий рядки: щоразу як елемент першого стовпця вибираємо не використаний на попередніх кроках елемент групи G . Побудова закінчується тоді, коли після деякого кроку виявляється, що кожний елемент групи записаний в якомусь місці

таблиці. Процес обривається через скінченність G . Внаслідок отримується така таблиця:

$$\begin{array}{cccccc}
 h_1 = 1 & h_2 & h_3 & \cdots & h_n & \\
 g_2 * h_1 = g_2 & g_2 * h_2 & g_2 * h_3 & \cdots & g_2 * h_n & \\
 g_3 * h_1 = g_3 & g_3 * h_2 & g_3 * h_3 & \cdots & g_3 * h_n & \\
 \vdots & \vdots & \vdots & \vdots & & \\
 g_m * h_1 = g_m & g_m * h_2 & g_m * h_3 & \cdots & g_m * h_n & .
 \end{array}$$

Перший елемент зліва у кожному рядку називається *лідером суміжного класу*. Кожний рядок таблиці називається *лівим суміжним класом*, а у випадку абелевої групи – просто *суміжним класом*. Якщо при побудові розкладання групи на суміжні класи використати праве множення на елементи групи G замість лівого, то рядки називаються *правими суміжними класами*. Внаслідок зазначених вище правил побудови розкладання на суміжні класи завжди подається прямокутною таблицею, всі рядки якої повністю заповнені. Доведемо тепер, що завжди отримується таблиця, в якій кожний елемент групи зустрічається точно один раз.

Теорема 2. У розкладанні групи G на суміжні класи кожний елемент із G зустрічається один і тільки один раз.

Доведення. Кожний елемент з'явиться хоча б один раз, тому що в протилежному випадку процес не зупиниться. Доведемо тепер, що кожний елемент не може з'явитися двічі в одному і тому ж рядку і що той самий елемент не може з'явитися у двох різних рядках.

Припустимо, що два елементи одного і того ж рядка, $g_i * h_j$ і $g_i * h_k$, рівні. Тоді множення зліва кожного з них на g_i^{-1} дає рівність $h_j = h_k$. Це суперечить тому, що кожний елемент підгрупи виписаний в першому рядку тільки один раз.

Припустимо, що два елементи різних рядків $g_i * h_j$ і $g_k * h_l$ рівні і що $k < i$. Множення справа на h_j^{-1} приводить до рівності $g_i = g_k * h_l * h_j^{-1}$. Тоді g_i породжує k -й суміжний клас, тому що елемент $h_l * h_j^{-1}$ належить підгрупі. Це суперечить вказаному вище правилу вибору лідерів суміжних класів.

Наслідок. Якщо H – підгрупа групи G , то число елементів у H ділить число елементів у G . Таким чином, (Порядок H)(Число суміжних класів G по H) = (Порядок G).

Доведення виходить безпосередньо із прямокутності таблиці розкладання на суміжні класи.

Теорема 3. Порядок кінцевої групи ділиться на порядок кожного з її елементів.

Доведення. Група містить циклічну підгрупу, породжену будь-яким з її елементів; таким чином, твердження теореми витікає з наслідку.

Кільця. Наступною необхідною нам алгебраїчною структурою є кільце. Кільце являє собою абстрактну множину, яка є абелевою групою і наділена додатковою структурою.

Визначення 2. Кільцем R називається множина з двома визначеними на ній операціями: перша називається додаванням (позначається $+$), друга називається множенням (позначається сусіднім розміщенням), причому мають місце такі аксіоми:

- 1) стосовно додавання ($+$) R є абелевою групою;
- 2) замкненість: добуток ab належить R для будь-яких a і b з R ;
- 3) закон асоціативності:

$$a(bc) = (ab)c;$$

- 4) закон дистрибутивності:

$$a(b+c) = ab+ac, \quad (b+c)a = ba+ca.$$

Додавання в кільці завжди комутативне, а множення не обов'язково повинне бути комутативним. *Комутативне кільце* – це кільце, в якому множення комутативне, тобто $ab = ba$ для всіх a і b з R .

Закон дистрибутивності у визначенні кільця пов'язує операції додавання й множення. Цей закон має декілька безпосередніх наслідків, як, наприклад, наведена нижче теорема.

Теорема 4. Для довільних елементів a і b у кільці R

I. $a0 = 0a = 0$.

II. $a(-b) = (-a)b = -(ab)$.

Доведення.

I. $a0 = a(0+0) = a0 + a0$. Віднімаючи з обох частин рівності $a0$, отримаємо $0 = a0$. Друга частина твердження I доводиться аналогічно,

II. $0 = a0 = a(b-b) = ab + a(-b)$. Отже, $a(-b) = -(ab)$.

Друга частина твердження II доводиться аналогічно.

Операція додавання в кільці має одиничний елемент, називаний нулем. Операція множення не обов'язково має одиничний елемент, але якщо він є, то є єдиним. Кільце, що містить єдиний елемент відносно множення, називається *кільцем з одиницею*. Цей одиничний елемент називається одиницею й позначається символом 1. Тоді для всіх a з R має місце рівність

$$1a = a1 = a.$$

Відносно операції додавання кожний елемент кільця має зворотний. Щодо операції множення елемент, зворотний даному елементу, не обов'язково існує, але в кільці з одиницею зворотні елементи можуть існувати. Це означає, що для даного елемента a може існувати елемент b , такий, що $ab = 1$. Якщо це так, то b називається *правим зворотним до a* . Аналогічно, якщо існує елемент c такий, що $ca = 1$, то c називається *лівим зворотним до a* .

Теорема 5. У кільці з одиницею

I. Одиниця єдина.

II. Якщо елемент a має як правий зворотний b , так і лівий зворотний c , то елемент a називається зворотним, причому зворотний йому елемент є єдиним (і позначається через a^{-1}).

III. $(a^{-1})^{-1} = a$.

Доведення. Міркування аналогічні проведеним при доведенні теореми 1.

Зворотний елемент кільця називається *одиницею*. Множина всіх одиниць у кільці замкнена відносно множення, тому що, якщо a і b – одиниці, то $c = ab$ має зворотний елемент, що дорівнює $c^{-1} = b^{-1}a^{-1}$.

Теорема 6.

I. Множина одиниць кільця утворює групу відносно множення в кільці.

II. Якщо $c = ab$ і c – одиниця, то a має правий зворотний, а b – лівий зворотний елемент.

Доведення. Безпосередня перевірка.

Є багато відомих прикладів кілець, і нижче наводяться деякі із них. Є повчальним проілюструвати цими прикладами теореми 5 і 6.

1. Множина всіх дійсних чисел утворює комутативне кільце з одиницею відносно звичайних додавання й множення. Кожний ненульовий елемент кільця є одиницею.

2. Множина всіх цілих чисел (додатних, від'ємних і нуля) утворює комутативне кільце з одиницею відносно звичайних додавання та множення. Це кільце прийнято позначати через Z ; його одиницями є тільки ± 1 .

3. Множина всіх квадратних $(n \times n)$ -матриць, елементами яких є дійсні числа, утворює некомутативне кільце з одиницею відносно матричного додавання й множення. Одиницею є одинична $(n \times n)$ -матриця. Одиницями в кільці слугують усі невивроджені матриці.

4. Множина всіх квадратних $(n \times n)$ -матриць, елементами яких є цілі числа, утворює некомутативне кільце з одиницею відносно матричного додавання і множення.

5. Множина всіх багаточленів від x із дійсними коефіцієнтами утворює комутативне кільце з одиницею відносно додавання і множення багаточленів. Одиницею кільця є багаточлен нульового ступеня $p(x) = 1$.

Поля. Отже, абелевою групою є множина, в якій можна додавати й віднімати, а кільцем – множина, в якій можна додавати, віднімати та множити. Більш складною алгебраїчною структурою, названою полем, є множина, в якій можна додавати, віднімати, множити і ділити.

Визначення 3. Полем називається множина з двома визначеними на ньому операціями – додаванням та множенням, причому мають місце такі аксіоми:

- 1) множина утворює абелеву групу за додаванням;
- 2) поле замкнене відносно множення, і множина ненульових елементів утворює абелеву групу за множенням;

3) закон дистрибутивності:

$$(a + b) c = ac + bc \text{ для будь-яких } a, b, c \text{ із поля.}$$

Одиничний елемент відносно додавання прийнято позначати через 0 і називати нулем, адитивний зворотний елементу a елемент $-a$; одиничний елемент відносно множення позначати через 1 і називати одиницею, мультиплікативний зворотний до елемента a елемент a^{-1} . Під відніманням $(a - b)$ розуміється $a + (-b)$; під діленням (a / b) розуміється $b^{-1}a$.

Достатньо відомі такі приклади полів:

R : множина дійсних чисел;

C : множина комплексних чисел;

Q : множина раціональних чисел.

Усі ці поля містять нескінченну множину елементів. Ми цікавимося полями, що містять кінцеве число елементів. Поле з q елементами, якщо воно існує, називається *кінцевим полем* або *полем Галуа* і позначається через $GF(q)$.

Що являє собою найменше поле? Воно обов'язково містить нульовий елемент і одиничний елемент. Насправді цього вже достатньо при таких таблицях додавання та множення:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Це поле $GF(2)$. Перевірка показує, що не існує іншого поля з двома елементами. Зараз ми наведемо два прості приклади й опишемо їх таблицями додавання та множення (віднімання і ділення неявно визначаються цими ж таблицями).

Поле $GF(3) = \{0, 1, 2\}$ з операціями

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Поле $GF(4) = \{0, 1, 2, 3\}$ з операціями

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Відзначимо, що множення в полі $GF(4)$ не є множенням за модулем 4 і додавання не є додаванням за модулем 4.

Існує багато інших полів Галуа. Навіть для цих прикладів дуже маленьких полів не так легко за допомогою простої перевірки встановити, що вони мають зазначену структуру.

Помітимо, що поле $GF(2)$ міститься в $GF(4)$, тому що в полі $GF(4)$ два елементи 0 і 1 додаються й множаться так само, як вони додаються і множаться в полі $GF(2)$. Однак $GF(2)$ не міститься в $GF(3)$.

Визначення 4. Нехай F – деяке поле. Підмножина в F називається *підполем*, якщо воно саме є полем відносно наслідуваних із F операцій додавання й множення. В цьому випадку вихідне поле F називається *розширенням поля*.

Для того щоб довести, що підмножина кінцевого поля є підполем, необхідно довести тільки, що воно містить ненульовий елемент і що воно замкнене відносно додавання та множення. Всі інші необхідні властивості наслідуються із F . Зворотні елементу β по додаванню або множенню елементи містяться в породженій β циклічній групі відносно операції додавання або множення.

Поле володіє всіма властивостями кільця, а також важливою додатковою властивістю – в ньому завжди можливе скорочення. Скорочення є слабка форма ділення й означає, що якщо $ab = ac$, то $b = c$.

Теорема 7. Якщо в довільному полі $ab = ac$ і $a \neq 0$, то $b = c$.

Доведення. Помножити на a^{-1} .

Деякі кільця можуть також задовольняти цій умові скорочення, але все ж таки не бути полями. Простим прикладом слугує кільце цілих чисел. У цьому кільці скорочення можливе, але наведене для теореми 7 доведення не проходить, так як в цьому кільці не існує елемента a^{-1} . Кільця, в яких завжди можливе скорочення, мають спеціальну назву.

Визначення 5. Комутативне кільце, в якому $b = c$, якщо $ab = ac$ і елемент a відмінний від нуля, називається *областю цілісності*.

Векторні простори. Відомий приклад векторного простору дає тривимірний евклідов простір, що фігурує в багатьох фізичних задачах. Його узагальненням є n -вимірний векторний простір над полем дійсних чисел. Поняття n -вимірного простору тісно пов'язане з ідеями лінійної алгебри і теорії матриць та відіграє важливу роль у багатьох додатках.

Для довільного поля можна дати абстрактніше визначення векторних просторів.

Визначення 6. Нехай F – деяке поле. Назвемо елементи із F *скалярами*. Множина V називається векторним простором, і його елементи називаються векторами, якщо для пар елементів із V визначена така операція векторного додавання (позначається плюсом), а для елементів із V і елементів із F визначена така операція *множення на скаляри* (позначається плюсом), що результат виконання операції дає елемент із V , причому мають місце такі аксіоми:

1) V є абелевою групою щодо векторного додавання;

2) *закон дистрибутивності*: для кожної пари векторів v_1, v_2 та скаляра c виконується рівність

$$c(v_1 + v_2) = cv_1 + cv_2;$$

3) *закон дистрибутивності*: для довільного вектора v і довільних скалярів c_1 і c_2 , виконуються рівності

$$1v = v \quad \text{і} \quad (c_1 + c_2)v = cv_1 + cv_2;$$

4) *закон асоціативності*: для довільного вектора v і довільних скалярів c_1 і c_2 виконується рівність

$$(c_1 c_2)v = c_1(c_2v).$$

Нульовий елемент із V називається початком координат простору V і позначається через $\mathbf{0}$.

Відзначимо, що ми використовували символ $+$ двома різними способами: для векторного додавання і для додавання в полі. Відзначимо також, що ми використовували символ 0 для позначення нульового елемента поля і символ $\mathbf{0}$ для позначення початку координат векторного простору.

Як менш відомий приклад векторного простору V можна назвати множину багаточленів від x з коефіцієнтами із $GF(q)$. Векторами цього простору слугують багаточлени. Векторне додавання збігається з додаванням багаточленів, а множення на скаляр – з множенням багаточленів на елементи поля.

У векторному просторі V сума вигляду

$$u = a_1v_1 + a_2v_2 + \dots + a_kv_k,$$

де a_i – скаляри, називається *лінійною комбінацією* векторів v_1, \dots, v_k . Множина векторів v_1, \dots, v_k називається *лінійно залежною*, якщо існує множина не всіх рівних нулю скалярів $\{a_1, \dots, a_k\}$, така, що

$$a_1v_1 + a_2v_2 + \dots + a_kv_k = \mathbf{0}.$$

Множина векторів, яка не є лінійно залежною, називається *лінійно незалежною*. Ніякий вектор із множини лінійно незалежних векторів не може бути представленим у вигляді лінійної комбінації інших векторів цієї множини. Зазначимо, що нульовий вектор $\mathbf{0}$ не може належати лінійно незалежній множині; кожна множина, що містить $\mathbf{0}$, є лінійно залежною.

Про множину векторів говорять, що вона породжує векторний простір, якщо кожен вектор простору дорівнює хоча б одній лінійній комбінації векторів із цієї множини. Векторний простір, породжуваний кінцевою множиною векторів, називається *кінцевовимірним векторним простором*. Ми в першу чергу цікавимося кінцевовимірними векторними просторами.

Теорема 8. Якщо векторний простір V породжений кінцевою множиною з k векторів $A = \{ v_1, \dots, v_k \}$ і V містить m лінійно незалежних векторів $B = \{ u_1, \dots, u_m \}$, то $k \geq m$.

Доведення. Ми опишемо правило побудови послідовності множин $A_0, A_1, A_2, \dots, A_m$, таких, що кожна із множин породжує V , кожна із множин містить k елементів, вибраних із A та B , і множина A_r містить u_1, \dots, u_r . Таким чином, серед k елементів множини A_m будуть мати місце u_1, \dots, u_m , і, отже, $k \geq m$.

Тому що ніяка лінійна комбінація векторів із B з ненульовими коефіцієнтами не дорівнює нулю, то ніякий елемент із B не може бути представлений у вигляді лінійної комбінації інших елементів із B . Якщо множина A_{r-1} не містить u_r і породжує V , то повинен бути спосіб подання u_r у вигляді лінійної комбінації елементів з A_{r-1} , що включає хоча б один вектор із A (скажемо, v_j), що не належить множині B . Рівняння, що задає цю лінійну комбінацію, можна дозволити відносно v_j , представивши v_j у вигляді лінійної комбінації із u_r й інших елементів з A_{r-1} .

Ця побудова здійснюється таким чином. Нехай $A_0 = A$. Якщо A_{r-1} містить u_r , то вважаємо $A_r = A_{r-1}$; в протилежному випадку u_r не належить множині A_{r-1} , але може бути представлений у вигляді лінійної комбінації елементів із A_{r-1} , що містить деякий елемент v_j із A , що не належить B . Множину A_r утворимо із множини A_{r-1} заміною v_j на u_r .

Довільний вектор v дорівнює деякій лінійній комбінації елементів з A_{r-1} і, отже, також елементів із A_r , якщо вилучити вектор v_j , використовуючи лінійну комбінацію, що зв'язує v_j і u_r з іншими векторами із A_{r-1} . Отже, множина A_r породжує V , а із A_{r-1} ми побудували A_r з бажаними властивостями. Таким чином, множина A_m може бути побудована, і доведення закінчено.

Теорема 9. Дві множини лінійно незалежних векторів, що породжують той самий векторний простір, містять однакову кількість векторів.

Доведення. Якщо одна множина містить m векторів, а інша k векторів, то за теоремою 8 $m \geq k$ і $k \geq m$, і, отже, $m = k$.

Число лінійно незалежних векторів у множині, що породжує кінцевовимірний векторний простір V , називається *розмірністю* простору V . Множина k лінійно незалежних векторів, що породжує k -вимірний векторний простір, називається *базисом* цього простору. Згідно з теоремою

8, у k -вимірному векторному просторі кожна множина, що містить більше, ніж k векторів, є лінійно залежною.

Теорема 10. В k -вимірному векторному просторі V будь-які k лінійно незалежних векторів утворюють базис простору V .

Доведення. Нехай $\{v_1, \dots, v_k\}$ – довільна множина k лінійно незалежних векторів із V . Якщо вона не породжує V , то у V знайдеться такий вектор v , що він не дорівнює ніякій лінійній комбінації векторів v_1, \dots, v_k . Множина $\{v, v_1, \dots, v_k\}$ містить $k + 1$ лінійно незалежних векторів з V , що суперечить теоремі 8. Отже, множина $\{v_1, \dots, v_k\}$ породжує V і є базисом.

Якщо множина лінійно незалежних векторів k -вимірного простору не є базисом, то вона повинна містити менше k векторів. Доповнення такої множини векторами так, щоб воно перетворилося в базис, називається *поповненням базису*.

Теорема 11. Задана множина лінійно незалежних векторів у кінцевовимірному векторному просторі завжди може бути доповнена до множини, що утворює базис.

Доведення. Якщо дана множина не є базисом, то деякий вектор простору не є лінійною комбінацією векторів даної множини. Виберемо такий довільний вектор і приєднаємо його до вихідної множини, збільшивши об'єм множини на одиницю. Якщо отримана множина все ще не є базисом, повторимо процес. Процес обов'язково обірветься, тому що число лінійно незалежних векторів у множині не може перевищувати розмірність простору. Отримана по завершенню процесу множина векторів задовольняє умовам теореми.

Непуста підмножина векторного простору називається *векторним підпростором*, якщо вона також є векторним простором відносно вихідних операцій векторного додавання і множення на скаляр. Відносно операції векторного додавання векторний простір є групою, а векторний підпростір підгрупою. Щоб установити, що непуста підмножина векторного простору утворює підпростір, достатньо перевірити тільки замкненість підмножини відносно векторного додавання і множення на скаляри. Замкненість відносно множення на скаляри гарантує, що нульовий вектор належить підмножині; інші необхідні властивості успадковуються з вихідного простору.

Теорема 12. Множина всіх лінійних комбінацій множини векторів $\{v_1, \dots, v_k\}$ довільного векторного простору V утворює підпростір у V .

Доведення. Кожна лінійна комбінація векторів v_1, \dots, v_k є вектором із V , і тому множина W усіх лінійних комбінацій утворює підмножину простору V . Вона не пуста, тому що 0 належить W . Ми повинні показати, що W є підпростором. Якщо $w = b_1v_1 + \dots + b_kv_k$ і $u = c_1v_1 + \dots + c_kv_k$ – два довільних елементи підмножини W , то $w + u = (b_1 + c_1)v_1 + \dots + (b_k + c_k)v_k$ також належить W . Далі, для довільного вектора w скалярне кратне

вектору w , $aw = ab_1v_1 + \dots + ab_kv_k$ також належить W . Тому що W замкнено відносно векторного додавання і множення на скаляр, то воно є векторним підпростором.

Теорема 13. Якщо розмірність векторного підпростору W кінцевовимірного векторного простору V дорівнює розмірності V , то $W = V$.

Доведення. Позначимо розмірність обох просторів через k . Виберемо у W базис. Він утворить множину k лінійно незалежних векторів простору V , тому є базисом у V . Отже, кожний вектор із W належить також V .

Для заданого поля F величина (a_1, a_2, \dots, a_n) , яка складена з елементів поля, називається n -послідовністю елементів поля. Відносно операцій покомпонентного додавання і покомпонентного множення на скаляри множина n -послідовностей елементів поля F утворює векторний простір, який позначається через F^n . За допомогою вибору базису v_1, \dots, v_k будь-який кінцевовимірний векторний простір можна перетворити в простір n -послідовностей, представляючи кожний вектор $v = a_1v_1 + \dots + a_nv_n$ n -послідовністю його коефіцієнтів (a_1, \dots, a_n) . Отже, ми можемо обмежитися розглядом тільки векторних просторів n -послідовностей.

Скалярний добуток двох n -послідовностей з F^n :

$$u = (a_1, \dots, a_n) \quad \text{і} \quad v = (b_1, \dots, b_n)$$

дорівнює скаляру, визначеному так:

$$u \cdot v = (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = a_1b_1 + \dots + a_nb_n.$$

Можна відразу ж перевірити, що $u \cdot v = v \cdot u$, $(cu) \cdot v = c(u \cdot v)$ і $w \cdot (u + v) = (w \cdot u) + (w \cdot v)$. Якщо скалярний добуток двох векторів дорівнює нулю, то вони називаються *ортогональними*. Ненульові вектори над $GF(q)$ можуть бути ортогональні самі собі. Вектор, ортогональний до кожного елемента множини, називається *ортогональним до множини*.

Теорема 14. Нехай V – векторний простір n -послідовностей над деяким полем F , і нехай W – деякий його підпростір. Множина векторів, ортогональних до W , також утворить підпростір.

Доведення. Позначимо через U множину всіх векторів, ортогональних до W . Тому що 0 належить U , то U не пуста. Нехай w – довільний вектор із W , а u_1 і u_2 – два довільних вектори із U . Тоді $w \cdot u_1 = w \cdot u_2 = 0$ і $w \cdot u_1 + w \cdot u_2 = 0 = w \cdot (u_1 + u_2)$, отже $u_1 + u_2$ належить U . Також $w \cdot (cu_1) = c \cdot (w \cdot u_1) = 0$, і, отже, cu_1 і належить U . Таким чином, U є підпростором.

Множина векторів, ортогональних до W , називається *ортогональним доповненням W* і позначається через W^\perp . У випадку кінцевовимірних векторних просторів над полем дійсних чисел перетин W і W^\perp містить тільки нульовий вектор, але над полем $GF(g)$ підпростір W^\perp може мати нетривіальний перетин з W або може навіть належати W , або містити W . У дійсності можна навіть побудувати приклади підпросторів, які самі є

своїми ортогональними доповненнями. Наприклад, в GF^2 (2) підпростір $\{00, 11\}$ збігається зі своїм ортогональним доповненням.

Теорема 15. Вектор, ортогональний до кожного вектора множини, що породжує W , належить ортогональному доповненню простору W .

Доведення. Припустимо, що множина $\{w_1, \dots, w_n\}$ породжує W . Вектор w із W можна записати у вигляді $w = c_1 w_1 + \dots + c_n w_n \dots$ Тоді

$$w u = (c_1 w_1 + \dots + c_n w_n) \cdot u = c_1 w_1 u + \dots + c_n w_n u \dots$$

Якщо u ортогональний до кожного w_i , то він ортогональний до кожного w із W .

Якщо розмірність підпростору W у векторному просторі n -послідовностей дорівнює k , то розмірність ортогонального доповнення W^\perp дорівнює $n - k$.

Теорема 16. Нехай W – підпростір у просторі n -послідовностей, і нехай W^\perp – його ортогональне доповнення. Тоді W є ортогональне доповнення підпростору W^\perp .

Доведення. Нехай розмірність W дорівнює k . Тоді розмірність W^\perp дорівнює $n - k$, а розмірність ортогонального доповнення простору W^\perp дорівнює k . Але кожний вектор із W ортогональний до W^\perp . Отже, W міститься в ортогональному доповненні до W^\perp і має ту ж саму розмірність, отже ці підпростори збігаються.

ДОДАТОК 3

Основи теорії матриць

Ми коротко викладемо матеріал частково в плані огляду і частково для доведення того, що відомі методи залишаються справедливими над довільним полем (а іноді навіть над довільним кільцем).

Визначення 7. $(n \times m)$ -матрицею A над кільцем R називається прямокутна таблиця, що складається з n рядків і m стовпців та містить nm елементів з кільця R :

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} = [a_{ij}].$$

У більшості додатків кільце R в дійсності є полем, і ми обмежимося цим випадком. Як правило, ми будемо розглядати матриці над кінцевим полем $GF(q)$.

Множина елементів a_{ij} , для яких номер рядка збігається з номером стовпця, називається *головною діагоналлю*. Якщо n дорівнює m , то матриця називається *квадратною матрицею*. $(n \times n)$ -матриця, всі елементи головної діагоналі якої дорівнюють одиничному елементу поля, а інші елементи дорівнюють нульовому елементу поля, називається *одиничною $(n \times n)$ -матрицею*. Одинична матриця позначається через I . Прикладами одиничних матриць є

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ та } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Дві $(n \times m)$ -матриці A і B над полем $GF(q)$ можна додавати за правилом

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1m} + b_{1m} \\ \vdots & \vdots & & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nm} + b_{nm} \end{bmatrix},$$

$(n \times m)$ -матрицю A можна помножити на елемент поля β за правилом

$$\beta A = \begin{bmatrix} \beta a_{11} & \beta a_{12} & \cdots & \beta a_{1m} \\ \vdots & \vdots & & \vdots \\ \beta a_{n1} & \beta a_{n2} & \cdots & \beta a_{nm} \end{bmatrix},$$

$(l \times n)$ -матрицю A можна помножити на $(n \times m)$ -матрицю B , отримавши результуючу $(l \times m)$ -матрицю C , за правилом

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}, \quad i = 1, \dots, l, \quad j = 1, \dots, m.$$

Цей добуток матриць позначається через

$$C = AB.$$

Як легко перевірити, множина квадратних $(n \times n)$ -матриць утворює кільце відносно так визначених множення й додавання матриць. Це кільце некомутативне, але має одиницю, а саме одиничну $(n \times n)$ -матрицю.

Матрицю можна розбити на блоки за правилом

$$A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right],$$

де A_{11} , A_{12} , A_{21} і A_{22} – менші матриці, розміри яких очевидним чином доповнюють один одного до розмірів матриці A . А саме сума числа рядків матриці A_{11} (або A_{12}) і числа рядків матриці A_{21} (або A_{22}) дорівнює числу рядків матриці A ; аналогічне твердження виконується для стовпців. Матриці можна перемножити поблочно, а саме якщо

$$A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right] \quad B = \left[\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array} \right]$$

і $C = AB$, то за умови коректного вибору розмірів блоків (коректного в тому розумінні, що всі добутки й суми матриць визначені)

$$C = \left[\begin{array}{c|c} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ \hline A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{array} \right].$$

Таке розкладання можна отримати як простий наслідок аксіом асоціативності та дистрибутивності основного поля.

Транспонованою до $(n \times m)$ -матриці A називається $(m \times n)$ -матриця A^T , така що $a_{ij}^T = a_{ji}$. Таким чином, рядками матриці A^T слугують стовпці матриці A , а стовпцями матриці A^T слугують рядки матриці A . *Зворотною* до квадратної матриці A називається квадратна матриця A^{-1} (якщо вона існує), така що $A^{-1}A = AA^{-1} = I$. Як можна відразу перевірити, множина всіх зворотних $(n \times n)$ -матриць утворює групу відносно операції множення. Отже, якщо матриця має зворотну, то зворотна матриця єдина. Матриця, що має зворотну, називається *невиродженою*; в протилежному випадку вона називається *виродженою*. Якщо $C = AB$, то за умови, що A і B зворотні, $C^{-1} = B^{-1}A^{-1}$, тому що $(B^{-1}A^{-1})C = I = C(B^{-1}A^{-1})$. Згодом ми побачимо, що якщо у A або у B немає зворотної матриці, то й у C немає зворотної матриці.

Визначення 8. Нехай задане поле F . Визначник квадратної $(n \times n)$ -матриці A для кожного $n \in \mathbb{N}$ функцією на множині всіх $(n \times n)$ -матриць над F зі значеннями в полі F , позначається через $\det(A)$ і задається формулою

$$\det(A) = \sum \xi_{i_1 \dots i_n} a_{1i_1} a_{2i_2} \dots a_{ni_n},$$

де i_1, i_2, \dots, i_n – перестановка на множині цілих чисел $\{1, 2, \dots, n\}$, $\xi_{i_1 \dots i_n}$ дорівнює ± 1 залежно від парності чи непарності перестановки, а сумарність ведеться за всіма перестановками.

Непарна перестановка визначається як добуток непарного числа транспозицій (транспозицією називається перестановка двох членів). Парна перестановка визначається як перестановка, що не може бути отримана непарним числом транспозицій.

Один зі способів зробити це визначення наочним полягає в розгляданні множин усіх матриць, які можна отримати з матриці A перестановкою рядків. Для кожної з таких матриць візьмемо добуток усіх членів, що лежать на головній діагоналі (якщо перестановка була непарною, то змінимо знак добутку), і додамо всі отримані таким чином добутки. Звичайно, обчислювати таким чином визначник не варто, але це дає хороший спосіб установлення властивостей визначників.

У наведеній нижче теоремі перелічені властивості функції $\det(A)$, що впливають безпосередньо з її визначення.

Теорема 17.

I. Якщо всі елементи деякого рядка квадратної матриці дорівнюють нулю, то визначник цієї матриці дорівнює нулю.

II. Визначник матриці дорівнює визначнику транспонованої матриці.

III. Якщо два рядки матриці поміняти місцями, то її визначник змінить знак.

IV. Якщо два рядки матриці рівні, то її визначник дорівнює нулю.

V. Якщо всі елементи одного рядка матриці помножити на елемент поля c , то визначник нової матриці буде дорівнювати визначнику вихідної матриці, помноженої на c .

VI. Якщо, матриці A і B відрізняються тільки i -м рядком, то сума їхніх визначників дорівнює визначнику матриці C , i -й рядок якої дорівнює сумі i -х рядків матриць A і B , а інші рядки дорівнюють відповідним рядкам матриці A або B .

VII. Якщо до елементів деякого рядка матриці k разів додати відповідні елементи деякого іншого її рядка, то визначник матриці не зміниться. Доведення: використати властивості (IV), (V) і (VI).

VIII. Визначник матриці відмінний від нуля тоді й тільки тоді, коли її рядки (стовпці) лінійно незалежні.

Якщо в квадратній матриці видалити рядок і стовпець, що містять елемент a_{ij} , то визначник квадратної таблиці, що залишилася, $n-1$ розміру називається *мінором елемента a_{ij}* і позначається через M_{ij} . *Алгебраїчне доповнення*, позначуване тут через C_{ij} , визначається рівністю

$$C_{ij} = (-1)^{i+j} M_{ij}.$$

Зі способу подання визначника матриці виходить, що алгебраїчне доповнення елемента a_{ij} є коефіцієнтом при a_{ij} в розкладанні визначника:

$$\det(A) = \sum_{k=1}^n a_{ik} C_{ik} .$$

Це відома формула Лапласа для розкладання визначників. Вона дає вираз визначника $(n \times n)$ -матриці через визначники $(n-1) \times (n-1)$ -матриць. Формула розкладання Лапласа лежить в основі рекурентного способу обчислення визначників.

Якщо a_{ik} замінити на a_{jk} , то вийде сума $\sum_{k=1}^n a_{jk} C_{ik}$, яка дорівнює визначнику нової матриці, отриманої зі старої заміною елементів i -го рядка елементами j -го рядка; цей визначник дорівнює нулю, якщо $j \neq i$. Таким чином,

$$\sum_{k=1}^n a_{jk} C_{ik} = \begin{cases} \det(A), & i = j, \\ 0 & i \neq j. \end{cases}$$

Тому якщо $\det(A) \neq 0$, то матриця $A = [a_{ij}]$ має зворотну, яка дорівнює

$$A^{-1} = \left[\frac{C_{ji}}{\det(A)} \right].$$

Якщо $\det(A) = 0$, то зворотної матриці не існує.

Рядки $(n \times m)$ -матриці A над $GF(q)$ можна розглядати як множину m -вимірних векторів над $GF(q)$. *Простір рядків* матриці A визначається як множина всіх лінійних комбінацій векторів-рядків матриці A . Розмірність простору рядків називається *рангом матриці за рядками*. Аналогічно стовпці матриці A можна розглядати як множину n -вимірних векторів над $GF(q)$. *Простір стовпців* матриці A визначається як множина всіх лінійних комбінацій векторів-стовпців матриці A , а розмірність простору стовпців називається *рангом матриці за стовпцями*. Множина всіх векторів v , таких як що $Av^T = 0$, називається *нульовим простором матриці* A . Зрозуміло, що нульовий простір є підпростором в $GF^n(q)$. Зокрема, нульовий простір є ортогональним доповненням простору рядків матриці A , тому що нульовий простір можна задати як множину всіх векторів, ортогональних до всіх векторів простору рядків.

Елементарними операціями над рядками матриці називаються такі дії:

1. Перестановка двох довільних рядків.
2. Множення довільного рядка на нульовий елемент поля.
3. Заміна довільного рядка на суму його самого й деякого кратного будь-якого іншого рядка.

Кожна елементарна операція над рядками зворотна, і зворотна операція має такий самий вигляд. Кожна елементарна операція над

рядками $(n \times n)$ -матриці A може бути виконана шляхом лівого множення A на відповідним чином підбрану так звану *елементарну* $(n \times n)$ -матрицю F . Елементарні матриці визначаються як одна з наступних модифікацій одиничної матриці:

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & 1 & & & \\ & & & \ddots & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \ddots & & & & \\ & & & a & & & \\ & & & & \ddots & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \text{ або } \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & a & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

Елементарні операції над рядками використовуються для надання матриці стандартного вигляду, названого *канонічним ступінчастим виглядом* і визначаються таким чином:

1. Провідний ненульовий елемент кожного ненульового рядка дорівнює одиниці.
2. Усі інші елементи кожного стовпця, що містить такий провідний елемент, дорівнюють нулю.
3. Провідний елемент будь-якого рядка знаходиться правіше будь-якого провідного елемента будь-якого розміщеного вище рядка. Нульові рядки розміщені нижче всіх ненульових рядків. Прикладом матриці, приведеної до канонічного ступінчастого вигляду, є

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Зазначимо, що нульовий рядок розміщений знизу і якщо видалити останній рядок, то всі стовпці одиничної (3×3) -матриці з'являться серед стовпців матриці, але в розкиданому вигляді. У загальному випадку, якщо є k ненульових рядків і щонайменше така сама кількість стовпців, то матриця в канонічному ступінчастому вигляді завжди буде мати всі стовпці одиничної матриці розміру k . Окремим випадком канонічної ступінчастої форми матриці є матриця вигляду

$$A = [I : P],$$

де I – одинична матриця. За допомогою елементарних операцій над рядками кожна матриця, що має щонайменше стільки ж стовпців, скільки й

рядків, може бути приведена до канонічного ступінчастого вигляду, але не до вказаного вище його окремого випадку.

Теорема 18. Якщо матриці A і A' отримуються одна з іншої за допомогою елементарних операцій, то простори рядків цих матриць збігаються.

Доведення. Кожний рядок з A' є деякою лінійною комбінацією рядків матриці A . Отже, кожна лінійна комбінація рядків матриці A' також є лінійною комбінацією рядків матриці A , і, таким чином, простір рядків матриці A містить простір рядків матриці A' . Але матриця A отримується з матриці A' за допомогою зворотних елементарних операцій, і, отже, простір рядків матриці A' міститься в просторі рядків матриці A . Таким чином, A та A' мають один й той самий простір рядків.

Теорема 19. Якщо матриці A і A' пов'язані між собою послідовністю елементарних операцій над рядками, то будь-яка множина лінійно незалежних стовпців у A лінійно незалежна і в A' .

Доведення. Через те, що для елементарних операцій над рядками першого й другого виду теорема очевидна, то досить довести її тільки для елементарної операції третього виду. Отже, припустимо, що A' отримується із A додаванням кратного рядка α до рядка β . У будь-якій лінійно залежній комбінації стовпців матриці A' елементи рядка α повинні давати нуль і, отже, не здійснювати ніякого впливу на рядок β . Таким чином, розглянута множина стовпців у матриці A також є лінійно залежна.

Теорема 20. $(k \times n)$ -матриця A , k рядків якої лінійно незалежні, містить k лінійно незалежних стовпців.

Доведення. Приведемо A до канонічного ступінчастого вигляду A' . Через те, що рядки лінійно незалежні, то жоден з них не є нульовим. Отже, для кожного рядка існує стовпець, елемент якого в цьому рядку дорівнює одиниці, а в кожному іншому рядку дорівнює нулю. Множина з k таких стовпців матриці A' лінійно незалежна, і, отже, згідно з теоремою 19 ця сама множина стовпців лінійно незалежна в A .

Теорема 21. Ранг матриці A за рядками дорівнює її рангу за стовпцями і дорівнює розміру найбільшої квадратної підматриці, визначник якої відмінний від нуля. (Тому дана величина називається просто *рангом матриці*.)

Доведення. Достатньо показати, що ранг матриці A за рядками дорівнює розміру найбільшої квадратної підматриці з ненульовим визначником. Таке саме доведення стосовно до транспонованої матриці дає доведення твердження для рангу матриці за стовпцями, і, таким чином, можна довести, що ранг за рядками дорівнює рангу за стовпцями.

Підматриця матриці A отримується викиданням з A деякого числа рядків і стовпців. Нехай M – не вироджена квадратна підматриця матриці A найбільшого розміру. Відповідно до теореми 17 (VIII), рядки матриці M лінійно незалежні, і, отже, їхнє продовження до рядків матриці A також

повинно бути лінійно незалежними. Отже, ранг матриці A за рядками не менше розміру матриці M .

З іншого боку, виберемо довільну множину з k лінійно незалежних рядків матриці A . Згідно з теоремою 21, матриця, утворена такими рядками, має k лінійно незалежних стовпців. Таким чином, визначник матриці, складеної з розміщених на перетині цих k стовпців і цих k рядків елементів, буде відмінний від нуля. Отже, розмір найбільшої невивродженої підматриці не менше рангу матриці A за рядками. Це завершує доведення.

Нехай A – квадратна $(n \times n)$ -матриця з ненульовим визначником. Тоді, згідно з теоремами 18 і 21, її канонічна ступінчаста форма є $(n \times n)$ -матрицею, всі рядки якої відмінні від нульового, і, отже, є одиничною матрицею. Тому що A може бути отримана з I перетворенням послідовності елементарних операцій над рядками, то A можна записати через елементарні матриці:

$$A = F_1 F_2 \dots F_r.$$

Теорема 22. Якщо в кільці $(n \times n)$ -матриць над полем F $C = AB$, то $\det(C) = \det(A) \det(B)$.

Доведення. Крок 1. Спочатку покажемо, що якщо $\det(A)$ або $\det(B)$ дорівнюють нулю, то й $\det(C)$ дорівнює нулю. Припустимо, що $\det(B)$ дорівнює нулю; тоді згідно з теоремою 17 (VIII) рядки матриці B лінійно залежні. Але рядки матриці C є лінійними комбінаціями рядків матриці B . Отже, рядки матриці C лінійно залежні і $\det(C)$ дорівнює нулю. Аналогічно досліджується випадок, коли $\det(A)$ дорівнює нулю.

Крок 2. Припустимо, що $\det(A)$ не дорівнює нулю. Тоді матрицю A можна записати у вигляді добутку елементарних матриць:

$$A = F_1 F_2 \dots F_r.$$

Кожна з матриць F_l відповідає елементарній операції над рядками матриці A , і, отже, згідно з (III), (V) і (VII) теореми 17, маємо

$$\det(AB) = \det[(F_1 F_2 \dots F_r) B] = \det[F_1 (F_2, \dots, F_r B)] = (\det F_1) \det(F_2 \dots \dots F_r B) = (\det F_1) (\det F_2) \dots (\det F_r) (\det B).$$

При $B = I$ це дає

$$\det(A) = (\det F_1) (\det F_2) \dots (\det F_r).$$

Підставляючи останню рівність у формулу для випадку довільної B , отримуємо $\det(AB) = \det(A) \det(B)$, що й потрібно було довести.

Один із наслідків цієї теореми полягає в тому, що якщо $C = AB$, то матриця C зворотна тоді й тільки тоді, коли обидві матриці A і B зворотні, тому що квадратна матриця має зворотну тоді й тільки тоді, коли її визначник відмінний від нуля.

Теорема 23. Якщо розмірність підпростору W векторного простору всіх n -послідовностей дорівнює k , то розмірність його ортогонального доповнення W^\perp дорівнює $n - k$.

Доведення. Нехай $\{g_1, \dots, g_k\}$ – базис підпростору W ; визначимо матрицю G рівністю

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_k \end{bmatrix},$$

де рядками є базисні вектори. Ранг цієї матриці дорівнює k , і розмірність простору стовпців матриці G дорівнює k . Вектор v належить W^\perp , якщо

$$Gv = 0,$$

тому що в цьому випадку він ортогональний до кожного базисного вектора. Нехай, $\{h_1, \dots, h_r\}$ – базис підпростору W^\perp . Доповнимо цей базис до базису всього простору $\{h_1, \dots, h_r, f_1, \dots, f_{n-r}\}$. Тепер вектор v із простору стовпців матриці G запишеться у вигляді $v = Gb$, де вектор b є деякою лінійною комбінацією базисних векторів. Отже, кожний вектор у просторі стовпців матриці G повинен записуватися у вигляді лінійної комбінації векторів $\{Gh_1^T, Gh_2^T, \dots, Gh_r^T, Gf_1^T, \dots, Gf_{n-r}^T\}$.

Покажемо тепер, що вектори $\{Gf_1^T, \dots, Gf_{n-r}^T\}$ утворюють базис просторів стовпців матриці G . Тому що $Gf_i^T = 0$, то ця множина породжує простір стовпців матриці G . Далі, ці вектори лінійно незалежні, тому що якщо

$$a_1(Gf_1^T) + \dots + a_{n-r}(Gf_{n-r}^T) = 0,$$

то

$$G(a_1f_1^T + \dots + a_{n-r}f_{n-r}^T) = 0,$$

і тому $a_1 = a_2 = \dots = a_{n-r} = 0$, оскільки єдиною лінійною комбінацією векторів f_1, \dots, f_{n-r} , що належить до нульового простору матриці G , є нульовий вектор 0 . Отже, $\{Gf_1^T, \dots, Gf_{n-r}^T\}$ утворюють базис простору стовпців матриці G . Таким чином, $n - r = k$, що й доводить теорему.

ДОДАТОК 4

Таблиця незвідних поліномів та їх періодів

<i>n</i> = 3	<i>L</i>	<i>n</i> = 8	<i>L</i>	<i>n</i> = 9	<i>L</i>
1101	7	100101011	255	1001101111	511
<i>n</i> = 4	<i>L</i>	100101101	255	1001110111	511
10011	15	100111001	17	1001111101	511
11001	15	100111111	85	1010000111	511
11111	5	101001101	255	1010010101	511
<i>n</i> = 5	<i>L</i>	101011111	255	1010011001	73
100101	31	101100011	255	1010100011	511
101001	31	101100101	255	1010100101	511
101111	31	101101001	255	1010101111	511
110111	31	101110001	255	1010110111	511
111011	31	101110111	85	1010111101	511
111101	31	101111011	85	1011001111	511
<i>n</i> = 6	<i>L</i>	110000111	255	1011010001	511
1000011	63	110001011	85	1011011011	511
1001001	9	110001101	255	1011110101	511
1010111	21	110011111	51	1011111001	511
1011011	63	110100011	85	1100000001	73
1100001	63	110101001	255	1100010011	511
1100111	63	110110001	51	1100010101	511
1110011	63	110111101	85	1100011111	511
1110101	21	111000011	255	1100100011	511
<i>n</i> = 7	<i>L</i>	111001111	255	1100110001	511
10000011	127	111010111	17	1100111011	511
10001001	127	111011101	85	1101001001	73
10001111	127	111100111	255	1101001111	511
10010001	127	111110011	51	1101011011	511
10011101	127	111110101	255	1101100001	511
10100111	127	111111001	85	1101101011	511
10101011	127	<i>n</i> = 9	<i>L</i>	1101101101	511
10111001	127	1000000011	73	1101110011	511
10111111	127	1000010001	511	1101111111	511
11000001	127	1000010111	73	1110000101	511
11001011	127	1000011011	511	1110001111	511
11010011	127	1000100001	511	1110100001	73
11010101	127	1000101101	511	1110110101	511
11100101	127	1000100001	511	1110111001	511
11101111	127	1000101101	511	1111000111	511
11110001	127	1000110011	511	1111001011	511
11110111	127	1001001011	73	1111001101	511
11111101	127	1001011001	511	1111010101	511
<i>n</i> = 8	<i>L</i>	1001011111	511	1111011001	511
100011011	51	1001100101	73	1111100011	511
10011101	255	1001101001	511	1111101001	511
				1111111011	511

<i>n</i> = 10	<i>L</i>	<i>n</i> = 10	<i>L</i>	<i>n</i> = 10	<i>L</i>
10000001001	1023	10110000101	1023	11100001111	341
10000001111	341	10110001111	1023	11100010001	341
10000011011	1023	10110010111	1023	11100010111	1023
10000011101	341	10110011011	341	11100011101	1023
10000100111	1023	10110100001	1023	11100100001	1023
10000101101	1023	10110101011	341	11100101011	93
10000110101	93	10110111001	341	11100110101	341
10001000111	341	10111000001	341	11100111001	1023
10001010011	341	10111000111	1023	11101000111	1023
10001100011	341	10111100101	1023	11101001101	1023
10001100101	1023	10111110111	1023	11101010101	1023
10001101111	1023	10111111011	1023	11101011001	1023
10010000001	1023	11000010011	1023	11101100011	1023
10010001011	1023	11000010101	1023	11101111011	341
10010011001	341	11000100011	33	11101111101	1023
10010101001	33	11000100101	1023	11110000001	341
10010101111	341	11000110001	341	11110000111	341
10011000101	1023	11000110111	1023	11110001101	1023
10011001001	341	11001000011	1023	11110010011	1023
10011010111	1023	11001001111	1023	11110101001	341
10011100111	1023	11001010001	341	11110110001	1023
10011101101	341	11001011011	1023	11111000101	341
10011110011	1023	11001111001	1023	11111011011	1023
10011111111	1023	11001111111	1023	11111101011	341
10100001011	93	11010000101	93	11111110011	1023
10100001101	1023	11010001001	1023	11111111001	1023
10100011001	1023	11010100111	93	11111111111	11
10100011111	341	11010101101	341		
10100100011	1023	11010110101	1023		
10100110001	1023	11011111111	341		
10100111101	1023	11011000001	1023		
10101000011	1023	11011001101	341		
10101010111	1023	11011010011	1023		
10101100001	93	11011011111	1023		
10101100111	341	11011110111	341		
10101101011	1023	11011111101	1023		

ДОДАТОК 5

Алгоритми формування кодів Слепяна

(n, k) -код	Норма перевірочних символів							
	1	2	3	4	5	6	7	8
5,2	12	2	1					
6,3	12	12	23					
7,4	134	124	123					
8,4	134	124	123	1234				
9,5	1345	1245	1235	1234				
10,5	1345	1245	1235	1234	12345			
10,6	1345	1245	12356	12346				
11,5	123	124	134	234	125	135		
11,6	13456	12456	12356	12346	12345			
11,7	1345	12457	12356	123467				
12,5	123	124	234	1235	45	1245	1345	
12,6	12456	2356	1346	1345	124	123		
12,7	13456	12456	123567	123467	123457			
12,8	1235678	12346	12457	13458				
13,5	123	124	134	125	135	245	345	12345
13,6	13456	1256	1246	1236	1245	1235	1234	
13,7	23567	3467	2457	2456	1235	1234		
14,6	1235	1246	1346	156	2346	256	356	456
14,8	34678	4578	13568	3567	12346	12345		
15,9	2345	1234	245	4789	15789	1459		
16,10	1245	4579	24689	124510	134610	35610		

ДОДАТОК 6

Помилки, які виправляються кодами Слепяна

(n, k) -код	Число N_r помилок, які виправляються, кратності r			(n, k) -код	Число N_r помилок, які виправляються, кратності r				(n, k) -код	Число N_r помилок, які виправляються, кратності r		
	N_1	N_2	N_3		N_1	N_2	N_3	N_4		N_1	N_2	N_3
5,2	5	2		12,5	12	63	52		14,6	14	91	150
6,3	6	1		12,6	12	50	1		14,8	14	49	
7,4	7			12,7	12	19			15,9	15	48	
8,4	8	7		12,8	12	3			16,10	16	47	
9,5	9	6		13,5	13	78	152	12				
10,5	10	21		13,6	13	72	42					
10,6	10	5		13,7	13	50						
11,5	11	46	6									
11,6	11	20										
11,7	11	4										

Залежність кількості коригуючих елементів від значення інформаційних m і кодової відстані

d	m																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	3	3	3	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5
4	3	5	5	6	6	7	7	7	7	8	8	8	8	8	8	9	9	9	9	9
5	4	7	8	8	9	9	10	10	10	11	11	11	12	12	12	12	12	12	13	13
6	5	9	10	11	11	12	12	13	13	14	14	14	15	15	15	15	16	16	16	16
7	6	11	12	13	14	15	15	16	16	17	17	17	18	18	18	19	19	19	19	20
8	7	13	14	15	16	17	18	18	19	19	20	20	21	21	21	22	22	22	23	23
9	8	15	16	18	19	20	20	21	22	22	23	23	24	24	24	25	25	25	26	26
10	9	17	19	20	21	22	23	24	24	25	25	26	26	27	27	28	28	29	29	29
11	10	19	21	22	23	24	25	26	27	28	28	29	29	30	30	31	31	31	32	32
12	11	21	23	24	26	27	28	29	29	30	31	31	32	33	33	34	34	34	35	35
13	12	22	25	27	28	29	30	31	32	33	33	34	35	36	36	36	37	37	38	38
14	13	25	27	29	30	32	33	34	35	35	36	37	37	39	39	39	40	40	41	41
15	14	27	29	31	33	34	35	36	37	38	39	39	40	41	41	42	42	43	44	44
16	15	29	31	33	35	36	38	39	40	40	41	42	43	44	44	45	45	46	46	47
17	16	31	33	36	37	39	40	41	42	43	44	45	46	47	47	47	48	49	49	50
18	17	33	36	38	40	41	42	43	44	45	46	47	48	49	49	50	51	51	52	52
19	18	35	38	40	42	43	45	46	47	48	49	50	51	52	52	53	53	54	55	55
20	19	36	40	42	44	46	47	48	49	50	51	52	53	55	55	55	56	57	57	58
21	20	38	42	44	46	48	49	51	52	53	54	55	56	57	57	58	59	59	60	61

<i>d</i>	<i>m</i>																			
	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
4	9	9	9	10	10	10	10	10	10	10	10	10	10	10	10	11	11	11	11	11
5	13	13	13	13	14	14	14	14	14	14	14	14	14	15	15	15	15	15	15	15
6	17	17	17	17	17	17	18	18	18	18	18	18	18	19	19	19	19	19	19	19
7	20	20	20	21	21	21	21	21	22	22	22	22	22	22	23	23	23	23	23	23
8	23	23	24	24	24	24	25	25	25	25	25	26	26	26	26	26	27	27	27	27
9	26	27	27	27	28	28	28	28	29	29	29	29	29	30	30	30	30	30	31	31
10	30	30	30	30	31	31	31	32	32	32	32	33	33	33	33	33	34	34	34	34
11	33	33	33	34	34	34	35	35	35	35	36	36	36	36	37	37	37	37	38	38
12	36	36	36	37	37	37	38	38	38	39	39	39	39	40	40	40	41	41	41	41
13	39	39	39	40	40	41	41	41	42	42	42	42	43	43	43	44	44	44	44	45
14	42	42	42	43	43	44	44	44	45	45	45	46	46	46	47	47	47	47	48	48
15	44	45	45	46	46	47	47	47	48	48	48	49	49	49	50	50	50	51	51	51
16	47	48	48	49	49	50	50	50	51	51	52	52	52	53	53	53	54	54	54	54
17	50	51	51	52	52	53	53	53	54	54	55	55	55	56	56	56	57	57	57	58
18	53	54	54	55	55	55	56	56	57	57	58	58	58	59	59	59	60	60	61	61
19	56	56	57	57	58	58	59	59	60	60	61	61	61	62	62	63	63	63	64	64
20	59	59	60	60	61	61	62	62	63	63	64	64	64	65	65	66	66	66	67	67
21	61	62	62	63	63	64	65	65	66	66	66	67	67	68	68	69	69	69	70	70

<i>d</i>	<i>m</i>																				
	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
3	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	7	7	7	
4	11	11	11	11	11	11	11	11	11	11	11	11	11	12	12	12	12	12	12	12	
5	15	15	15	15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	17	17	
6	19	19	20	20	20	20	20	20	20	20	20	20	21	21	21	21	21	21	21	21	
7	23	23	24	24	24	24	24	24	24	24	25	25	25	25	25	25	25	25	25	25	
8	27	27	27	28	28	28	28	28	28	28	29	29	29	29	29	29	29	29	30	30	
9	31	31	31	31	32	32	32	32	32	32	32	33	33	33	33	33	33	33	34	34	
10	34	35	35	35	35	36	36	36	36	36	36	36	37	37	37	37	37	37	37	38	
11	38	38	38	39	39	39	39	39	40	40	40	40	40	40	41	41	41	41	41	41	
12	41	42	42	42	42	43	43	43	43	43	44	44	44	44	44	44	45	45	45	45	
13	45	45	45	46	46	46	46	46	47	47	47	47	48	48	48	48	48	48	49	49	
14	48	48	49	49	49	49	50	50	50	50	51	51	51	51	51	52	52	52	52	52	
15	52	52	52	52	53	53	53	53	54	54	54	54	55	55	55	55	55	56	56	56	
16	55	55	55	56	56	56	56	57	57	57	57	58	58	58	58	59	59	59	59	60	
17	58	58	59	59	59	59	60	60	60	61	61	61	61	62	62	62	62	63	63	63	
18	61	62	62	62	62	63	63	63	64	64	64	64	65	65	65	65	66	66	66	66	
19	64	65	65	65	66	66	66	67	67	67	67	68	68	68	69	69	69	69	70	70	
20	67	68	68	68	69	69	69	70	70	70	71	71	71	72	72	72	72	73	73	73	
21	71	71	71	72	72	72	73	73	73	74	74	74	75	75	75	75	76	76	76	77	

Навчальне видання

*Захарченко М.В.,
Кільдішев В.Й.,
Мартінова О.М.,
Ільїн Д.Ю.,
Трінтіна Н.А.*

**Системи передавання даних
Т.1: Ефективність блокового кодування**

Навчальний посібник
для студентів вищих технічних навчальних закладів,
які навчаються за напрямками:
6.050903 «Телекомунікації»;
6.050904 «Мережі та системи поштового зв'язку»;
6.050801 «Радіотехніка»

За авторською редакцією