

**Міністерство транспорту та зв'язку України
Одеська національна академія зв'язку ім. О.С. Попова**

М.В. Захарченко

СИСТЕМИ ПЕРЕДАВАННЯ ДАНИХ

Том 1. Завадостійке кодування

Підручник

Рекомендовано Міністерством транспорту та зв'язку України для студентів, які навчаються за напрямками 6.050903 "Телекомунікації", 6.050904 "Мережі та системи поштового зв'язку".

Лист № 6778/23/14–08 від 22.09.2008

Одеса
Фенікс
2009

УДК 61.394; 621.397
ББК 32.811.4
З–38

*Друкується відповідно до постанови
Вченої ради Одеської
національної академії зв'язку
ім. О.С. Попова,
протокол № 10 від 30 травня 2008 р.*

Рецензенти:

д.т.н. проф. **Климаш М.М.**, Львівський національний політехнічний університет;

д.т.н. проф. **Семенко А.І.**, Державний університет інформаційно-комунікаційних технологій

Захарченко М.В. Системи передавання даних. – Т. 1: Завадостійке 3-38 кодування : підручник [для студентів вищих технічних навчальних закладів] / М.В. Захарченко. – Одеса : Фенікс, 2009. – 448 с.

ISBN 978-966-438-236-3

У систематизованому вигляді розглянуті характеристики джерел і повідомлень, завад і каналів зв'язку, проблеми побудови блокових кодів, методи їх декодування: оптимізація структури сигнальних конструкцій, кодуючих та декодуючих пристроїв, алгоритмів синтезу, конструкцій виявляючих та виправляючих помилки кодів із заданими ймовірнісними характеристиками.

Побудова неперервних кодів розглянута на прикладі згорткових кодів: сформульовані принципи формування породжуючих багаточленів, алгоритми реалізації кодерів і декодерів, структури турбокодів, методи визначення їхніх імовірнісних характеристик. У роботі розглянуті питання збільшення пропускну здатності нестационарних каналів за рахунок зменшення енергетичної відстані між сигнальними конструкціями.

Для самоперевірки рівня засвоєння матеріалу в кінці кожної глави наведені відповідні питання та задачі.

ISBN 978-966-438-236-3

© М.В. Захарченко, 2009

ЗМІСТ

ВСТУП	5
СПИСОК АБРЕВІАТУР	11
ЧАСТИНА 1 ІНФОРМАЦІЙНІ ХАРАКТЕРИСТИКИ ДЖЕРЕЛ ПОВІДОМЛЕНЬ, СИГНАЛІВ, ЗАВАД ТА КАНАЛІВ ЗВ'ЯЗКУ	13
Глава 1.1. Інформаційні характеристики джерел повідомлень, сигналів	13
1.1.1. Інформація та її виміри. Ентропія повідомлення	13
1.1.2. Інформаційні характеристики джерел повідомлень. Оптимальне кодування	26
1.1.3. Властивості спектрів сигналу. Характеристики лінійних систем	47
1.1.4. Канонічне розкладання сигналів	61
1.1.5. Модель сигналу з обмеженим спектром	71
1.1.6. Питання та задачі для самоперевірки	77
Глава 1.2. Інформаційні характеристики каналу зв'язку	79
1.2.1. Модель каналів зв'язку з обмеженою смугою пропускання	79
1.2.2. Пропускна здатність каналу	84
1.2.3. Спотворення елементарних сигналів кодових конструкцій	90
1.2.4. Реєстрація сигналів кодових конструкцій	102
1.2.5. Статистика помилок на виході дискретного каналу. Моделі потоку помилок	108
1.2.6. Питання та задачі для самоперевірки	121
ЧАСТИНА 2 ЗАВАДОСТІЙКЕ КОДУВАННЯ	123
Глава 2.1. Блокові коди	123
2.1.1. Основні характеристики блокових кодів, їхнє описання та властивості	123
2.1.2. Кодування і декодування при блокових кодах	135
2.1.3. Кореляційне трактування завадостійких кодів	143
2.1.4. Способи побудови двійкових циклічних кодів	146
2.1.5. Технічні засоби кодування і декодування циклічних кодів	153
2.1.6. Лінійні блокові коди для каналів із групуванням помилок	156
2.1.7. Кодування в реальному масштабі часу	161
2.1.8. Коди Ріда-Соломона	168
2.1.9. Декодування блокових надлишкових кодів	173
2.1.10. Ефективність декодування при квантуванні інформаційного параметра на виході каналу	195
2.1.11. Питання та задачі для самоперевірки	213

Глава 2.2. Неперервні коди	216
2.2.1. Синтез згорткових кодів	216
2.2.2. Породжуючі багаточлени згорткового коду	224
2.2.3. Побудова кодерів та декодерів згорткових кодів	228
2.2.4. Зображення згорткових кодів та оцінка їхньої кодової відстані	242
2.2.5. Методи декодування згорткових кодів	251
2.2.6. Характеристики турбо-кодів	269
2.2.7. Питання та задачі для самоперевірки	279

ЧАСТИНА 3 ПОБУДОВА НАДЛИШКОВИХ БЛОКОВИХ КОДІВ ПРИ БАГАТОПОЗИЦІЙНИХ СИГНАЛАХ 281

Глава 3.1. Ймовірнісні характеристики якості приймання надлишкових блокових кодів	281
3.1.1. Пропускна здатність каналу з алфавітом $a > 2$	281
3.1.2. Побудова недвійкових надлишкових кодів	284
3.1.3. Композиційний метод побудови q -ічних коректуючих кодів	287
3.1.4. Ефективність використання алфавіту каналу при $q > 2$	297
3.1.5. Статистичні параметри БЧМ	303
3.1.6. Ймовірнісні параметри БЧМ	306
3.1.7. Параметричне кодування як метод збільшення алфавіту каналу	313
3.1.8. Порівняння посимвольного приймання кодових слів та приймання сигналів у цілому	321
3.1.9. Питання та задачі для самоперевірки	324

Глава 3.2. Ефективність таймерних сигнальних конструкцій при роботі в реальних каналах зв'язку	327
3.2.1. Принцип формування таймерних сигнальних конструкцій	327
3.2.2. Параметри зміщень нуль-переходів на виході бінарного каналу	336
3.2.3. Пропускна здатність каналу при ТСК	347
3.2.4. Зв'язок коефіцієнтів A_i з кодовою відстанню	355
3.2.5. Теореми синтезу простих ТСК	364
3.2.6. Теореми синтезу надлишкових ТСК	369
3.2.7. Ефективність наднайквістової швидкості модуляції	376
3.2.8. Ефективність використання ТСК для трансформації якості у швидкість передавання	382
3.2.9. Питання та задачі для самоперевірки	406

Література	409
Додаток 1. Значення інтегралу імовірності	414
Додаток 2. Алгебраїчні структури та поля Галуа	420
Додаток 3. Основи теорії матриць	437
Додаток 4. Таблиця незвідних поліномів та їх періодів	445
Додаток 5. Алгоритми формування кодів Слепяна	447
Додаток 6. Помилки, які виправляються кодами Слепяна	447

*Світлій пам'яті мого
вчителя, друга, колеги – професора
Василя Купріяновича Стеклова
присвячується*

ВСТУП

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 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 побаченим. 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 телеграфічних 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 багатofункційними, 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. Стенфорд отримав медичну консультацію з офісу BBN). Слід зауважити, що таким режимом (чата) користувались телеграфісти при настроюванні телеграфних каналів.

Починаючи з 1983 р. кількість абонентів мережі ARPANET щорічно збільшується 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. функціонує 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 пере-

давання майже на порядок, а пропускна здатність збільшилась на ту саму величину.

Незважаючи на зростання пропускну здатності і зменшення цін на послуги передавання інформації, 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 використувати 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 адаптивних систем передавання.

Проблеми надійного й ефективного передавання інформації пов'язані з використанням ефективних кодів. Розвинена в роботах В.А. Котельникова і К.С. 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., Зігангірову К., Блоху Є., Зяблову В., Золотарьову В., Овечкіну Г.

Перший том підручника "Системи передавання даних" присвячений основам синтезу надлишкових блокових і неперервних кодів. 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 частина першого тому присвячена інформаційним характеристикам джерел повідомлень, завад 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 першій главі другої частини цього тому розглядаються проблеми синтезу блокових кодів: структури сигнальних конструкцій лінійних кодів,

технічні засоби кодування та декодування циклічних кодів, особливості кодів Ріда-Соломона та вимоги до синтезу кодів для роботи в реальному масштабі часу та реальних каналах зв'язку.

У другій главі другої частини розглянуті питання синтезу неперервних кодів на прикладі згорткових: сформульовані принципи синтезу породжуючих багаточленів згорткових кодів, алгоритми синтезу кодерів та декодерів їх, структура турбокодів і методи визначення їхніх імовірнісних характеристик.

У третій частині підручника 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 зв'язку.

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 підручника надано шість додатків:

1. Значення інтегралу ймовірності.
2. Алгебраїчні структури та поля Галуа.
3. Основи теорії матриць.
4. Таблиця незвідних поліномів та їх періоди.
5. Алгоритми формування кодів Слепяна.
6. Класи помилок, які виправляються кодами Слепяна.

Широке коло та складність проблем синтезу сигнальних конструкцій різних кодів, оптимальних методів декодування у різних системах зв'язку не дозволили в рамках одного тому викласти всі питання передавання даних. Тому підручник структурно складається з двох томів. У другому томі викладені алгоритми та протоколи адаптивних систем передавання. Написання цього підручника стало можливим завдяки творчим дискусіям і наукової підтримки, наданої мені колективом кафедри інформаційної безпеки та передавання даних.

Вважаю своїм обов'язком висловити подяку докторам технічних наук Є.М. Рудому, С.М. Горохову, кандидатам технічних наук, доцентам О.О. Вараксіну, М.М. Балану, порадами яких я користувався. Необхідно відзначити активну допомогу в розробці алгоритмів систем на базі таймерних сигналів, проведенні експериментів та оформленні роботи докторантів

кафедри Гаджисва М.М., Басова В.Є. та аспірантів Мартинової О.М., Белової Ю.В., Русаловської О.А., Шинкарчук Т.М., результати роботи яких відображені в спільно написаному розділі 3.2.8 «Ефективність використання таймерних сигнальних конструкцій».

Особливо вдячний докторам наук Климашу М.М. і Семенку А.І., які взяли на себе нелегку працю рецензування рукопису.

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 ВКА ім. А.Ф. Можайського – М.М. Буга, А.А. Вороніна, С.В. Митряєва; ВІА ім. Ф. Е. Держинського – А.А. Кошевого, А.П. Мановцева; ВКАЗ ім. Будьонного – М.Я. Теплова, П.А. Китова.

СПИСОК АБРЕВІАТУР

- АМ – амплітудна модуляція
- ЧМ – частотна модуляція
- ФМ – фазова модуляція
- АІМ – амплітудно-імпульсна модуляція
- ЧРК – частотне розділення каналу
- КХ – короткі хвилі
- КПС – канал постійного струму
- ЗММ – значущий момент модуляції
- ЗМВ – значущий момент відтворення
- ДСК – двійковий симетричний канал
- ВФМ – відносна фазова модуляція
- МАТС – міська автоматична телефонна станція
- СПДП – система передачі дискретних повідомлень
- КК – кодові комбінації
- КПВ – коди з постійною вагою
- ЦК – циклічні коди
- МДК – мажоритарно декодовані коди
- ЗК – згорткові коди
- ОЗК – самоортогональні згорткові коди
- КС – кодове слово
- М – модулятор
- ДМ – демодулятор
- БЧХ – код Боуза-Чоудхурі-Хоквінгема
- АБГШ – аддитивний білий гауссівський шум
- ЩС – імпульс циклової синхронізації
- СРП – система розділених (ортогональних) перевірок
- СЗП – система λ_c -зв'язних перевірок
- КРП – квазірозділені перевірки
- ЕБ – елементарний блок
- ЕВК – енергетичний виграш кодування
- АЕВК – асимптотичний енергетичний виграш кодування
- РСЗК – рекурсивні систематичні згорткові коди
- МАІ – максимуму апостеріорної імовірності
- АПІ – апостеріорна імовірність

АВМР – алгоритм Вітербі з м'яким розв'язанням

БЧМ – багатопозиційна частотна модуляція

ДЧМ – двійкові канали з ЧМ

ТСК – таймерні сигнальні конструкції

РЦК – розрядно-цифровий код

ФНЧ – фільтр нижніх частот

СК – сигнальні конструкції

ДКК - дозволені кодові комбінації

ЧАСТИНА 1

ІНФОРМАЦІЙНІ ХАРАКТЕРИСТИКИ ДЖЕРЕЛ ПОВІДОМЛЕНЬ, СИГНАЛІВ, ЗАВАД ТА КАНАЛІВ ЗВ'ЯЗКУ

Глава 1.1. Інформаційні характеристики джерел повідомлень, сигналів

1.1.1. 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, аніж 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.

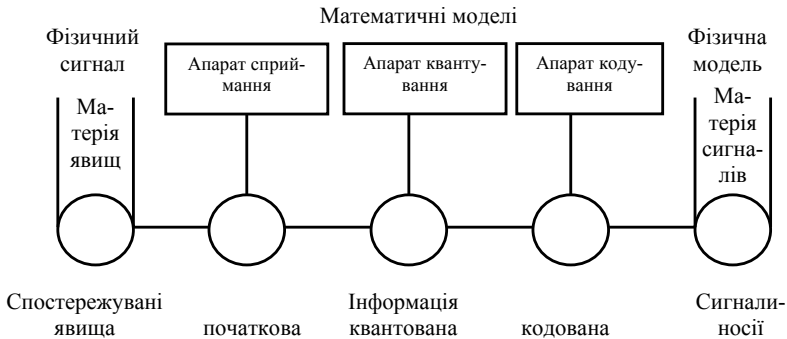


Рисунок 1.1 – Перетворення інформації при передаванні

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 діставати, 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 розрізняти за галузями знань (біологічна, технічна, економічна), за фізичною природою сприйняття (зорова, слухова, смакова 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 комплексів.

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:

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

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

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

Можливе число розміщень з повтореннями по l з h елементів

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

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 апіорних 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 діт = 3,32193 біт.

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

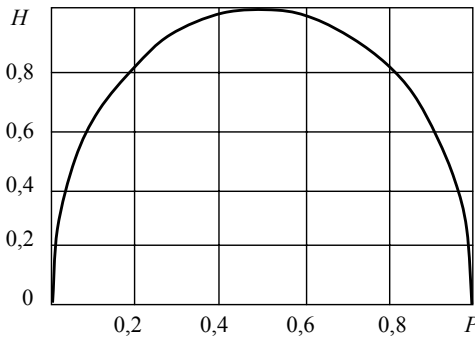


Рисунок 1.3 – Залежність ентропії від імовірності виникнення подій

Кількість інформації та надлишковість. Кількість інформації лише тоді дорівнює ентропії, коли невизначеність в результаті досліду 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:

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

Відносна надлишковість

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

Визначимо відносну надлишковість для двох джерел.

Приклад 1. Повна шкала вимірювання містить $H_{\max} = 1000$ 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.

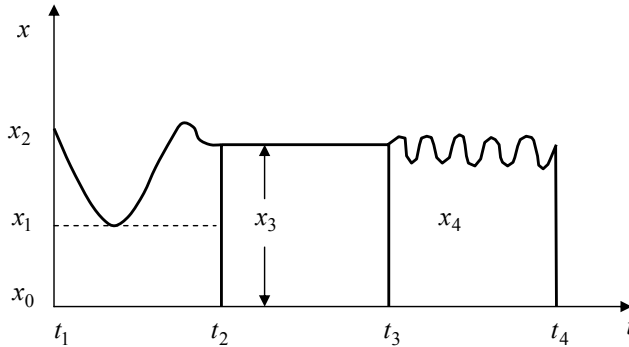


Рисунок 1.4 – Зміни неперервної величини у часі

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 :

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

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

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-

рервно 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 впливає 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 переконалися 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'єданий 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'єданий 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

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

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 дослідних u 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 дослідних u відносно випадкових подій x , дорівнює кількості інформації, що міститься у випадкових подіях x відносно результату дослідів u .

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 автотручки 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 найкращою 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 перероблюваних відомостей (інформації), їхня ймовірність і втрати за різних перетворень.

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

1.1.2. Інформаційні характеристики джерел повідомлень. Оптимальне кодування

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. Неважко переконатися 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 словесний 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 знайдено 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 інший 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 – $p(x_i, x_j)$.

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

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

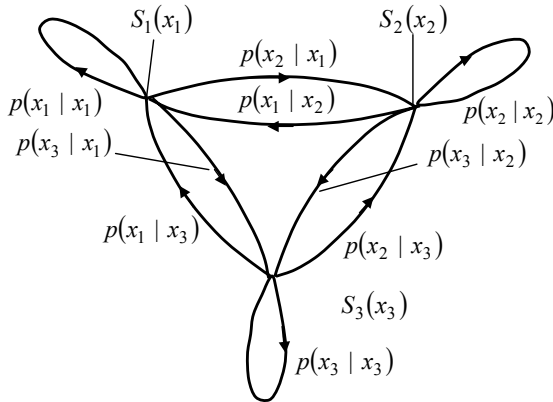


Рисунок 1.6 – Приклад джерела для випадку $n = 3$

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

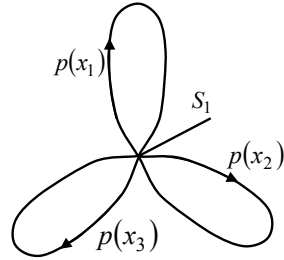


Рисунок 1.5 – Діаграма переходу для джерела, що має один характерний стан S_1 і виробляє три різних символи – x_1, x_2 і x_3

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, ресстрації 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:

в прикладі 7 $R = 0$,

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

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 *потокотом 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 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 за даною 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 однопольосного 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 двопольосної роботи запис того самого числа наведено на рис. 1.7, *б*.

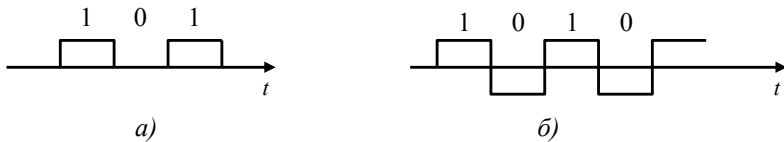


Рисунок 1.7 - Передавання двійкових чисел

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 кодї 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.

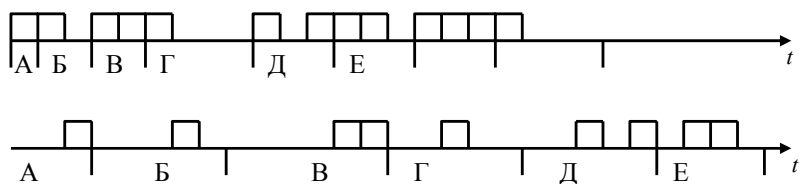


Рисунок 1.8 – Кодові сигнальні конструкції

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 кожну комбінацію до максимально можливої кількості елементарних посилок – п'яти і дістанемо двійковий п'ятизначний рівномірний код. Виникає питання: з якого боку слід розміщувати елементарні посилки, яких бракує, – ліворуч чи праворуч від записаної комбінації – і який стан («0» чи «1») повинен мати ці відсутні елементарні посилки?

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 відрахувувати на станціях передавання та приймання однакові відліки часу. Ці функції виконують розподільвачі 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 прогалин, потрібно в середньому близько $9,5 t_0$ на кожний знак, де t_0 – тривалість елементарної посилки. Переваги коду Морзе – легка запам'ятовуваність, можливість запису найпростішими засобами та приймання на слух у разі сильних завад.

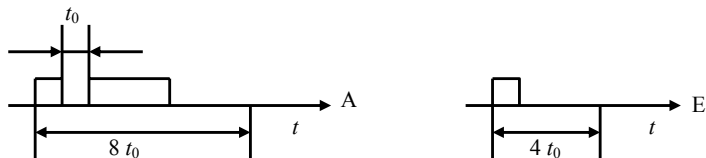


Рисунок 1.9 - Сигнальні кодові конструкції при двопозиційних сигналах

У кабельному кодi (рис. 1.10) точка записується позитивною посилюючою, 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 рівномірною. 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.

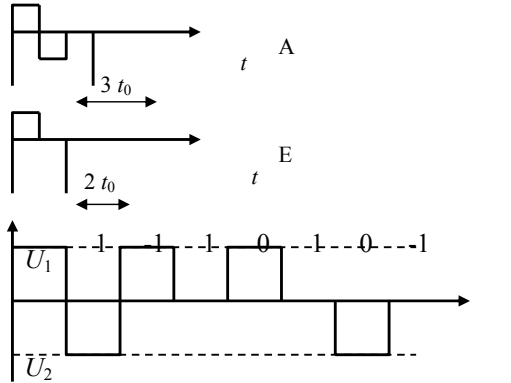


Рисунок 1.10 - Сигнальні кодові конструкції за різної позиційності

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 рівномірними 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 чотирьолітерний 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).

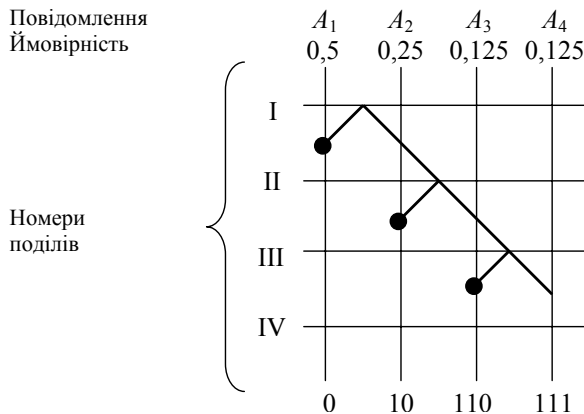


Рисунок 1.11 – Формування слів оптимального коду

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

$$\begin{aligned}
 l_{\text{сеп}} &= \sum_{i=1}^m l_i p_i = 1 \cdot 0,5 + 2 \cdot 0,25 + 3 \cdot 0,125 + 3 \cdot 0,125 = \\
 &= 0,5 + 0,5 + 0,75 = 1,75 \frac{\text{дв. од.}}{\text{знак}},
 \end{aligned}$$

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 відповідень 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.

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 рівномірними комбінаціями слугує n -вимірний *гіперкуб* з одиничними ребрами, вершини якою відповідають кодовим комбінаціям. Відстань між кодовими векторами чисельно дорівнює числу розрядів, в яких різняться між собою кодові комбінації. Враховуючи властивості додавання за 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

$$d = \max |x(t) - z(t)|, \quad (1.28б)$$

часто використовується в різних схемах селекції сигналів за максимумом різничевої 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 *коректуючими*.

Принцип побудови коректуючих 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

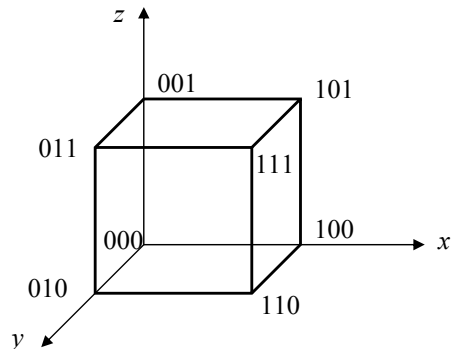


Рисунок 1.12 – Геометрична модель триелементного коду

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.

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 (двократно помилка) одна дозволена комбінація перетворюється на іншу, також дозволену комбінацію. Отже, двократно помилка не виявляється.

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

Для того щоб однократно 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_{\min} пов'язані формулою $d_{\min} = 2t_{\text{вп}} + 1$.

Таким чином, ідея двійкових коректуючих 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, коректуючі 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.

1.1.3. Властивості спектрів сигналу. Характеристики лінійних систем

Поняття спектра сигналу. У техніці зв'язку використовуються сигнали $x(t)$ різної форми: прямокутні, трикутні, косинус-квадратні ($x(t) = \cos^2 \frac{\pi}{T} t$; $-T/2 < t < T/2$) (рис. 1.13) та ін. Кожному сигналу зіставляють спектр за допомогою перетворення Фур'є (точніше, прямого перетворення Фур'є)

$$X(\omega) = \int_{-T/2}^{T/2} x(t) e^{-i\omega t} dt. \quad (1.31)$$

Для сигналів довільної (у тому числі і нескінченної) тривалості останню формулу пишуть у більш загальному вигляді:

$$X(\omega) = \int_{-\infty}^{\infty} x(t) e^{-i\omega t} dt. \quad (1.32)$$

Інтеграли (1.31) і (1.32) для всіх частот $-\infty < \omega < \infty$ визначають комплексну функцію $X(\omega)$ – спектр, фізичний сенс якого стає відомим з доведеної в курсі математичного аналізу формули зворотного перетворення Фур'є

$$x(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} X(\omega) e^{i\omega t} d\omega,$$

$-\infty < t < \infty$.

Дійсно, в останньому співвідношенні можна приблизно – відповідно до методу прямокутників, згідно з яким інтегрована функція наближається послідовністю прямокутників (рис. 1.14), – підмінити інтеграл сумою та переписати це співвідношення таким чином:

$$x(t) \approx \frac{\Delta\omega}{2\pi} \sum_{k=-\infty}^{\infty} X(k\Delta\omega) e^{ik\Delta\omega t} = \frac{\Delta\omega}{2\pi} \sum_{k=-\infty}^{\infty} X(k\Delta\omega) \cos k\Delta\omega t +$$

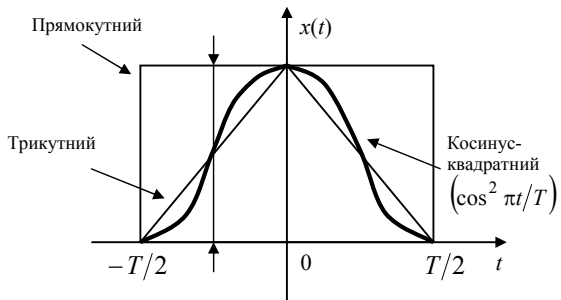


Рисунок 1.13 – Форми сигналів

$$+ i \frac{\Delta\omega}{2\pi} \sum_{k=-\infty}^{\infty} X(k\Delta\omega) \sin k\Delta\omega t. \quad (1.33)$$

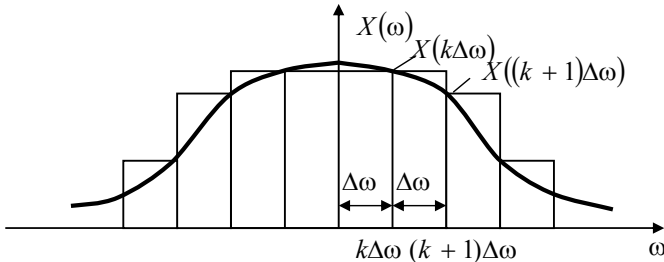


Рисунок 1.14 – Метод прямокутників

При записі результату (1.33) було використане співвідношення Ейлера

$$e^{iz} = \cos z + i \sin z.$$

Рівність (1.33) показує, що довільний сигнал $x(t)$ представимо у вигляді нескінченного набору (суми) косинусоїд і синусоїд з частотами $k\Delta\omega$ і, взагалі кажучи, комплексними коефіцієнтами. Якщо відійти від постійного для всіх значень номера k множника $\Delta\omega/2\pi$, то цими коефіцієнтами при функціях $\sin k\Delta\omega t$ і $\cos k\Delta\omega t$ слугують відлікові значення спектра $X(k\Delta\omega)$. Отже, кожен сигнал «складається» з косинусоїд і синусоїд (точніше, є їх сумою) з відповідним чином підібраними коефіцієнтами.

Іноді можна відмовитися від ейлерового представлення комплексної експоненціальної функції $e^{ik\Delta\omega t}$ й обмежитися наведеним вище представленням сигналу

$$x(t) \approx \frac{\Delta\omega}{2\pi} \sum_{k=-\infty}^{\infty} X(k\Delta\omega) e^{ik\Delta\omega t},$$

яке переходить в зворотне перетворення Фур'є при наближенні $\Delta\omega$ до нуля ($\Delta\omega \rightarrow 0$).

Визначення. Сукупність усіх коефіцієнтів $X(k\Delta\omega)$, $-\infty < k < \infty$, точніше їх граничних значень при $\Delta\omega \rightarrow 0$, тобто функція $X(\omega)$, $-\infty < \omega < \infty$, називається *спектром сигналу* $x(t)$.

Експоненціальні функції $e^{i\omega_1 t}$ і $e^{i\omega_2 t}$, $\omega_1 \neq \omega_2$ володіють хорошою властивістю – ортогональністю на осі $-\infty < \omega < \infty$.

Визначення. Дві в загальному випадку комплексні функції $F(x)$ і $G(x)$, $a < x < b$ називаються *ортогональними на інтервалі* (a, b) , якщо виконується рівність

$$\int_a^b F(x) \overline{G(x)} dx = 0, \quad (1.34)$$

де рискою позначено перехід до комплексно-зв'язаної величини. Зрозуміло, для дійсних $F(x)$ і $G(x)$ рівність (1.34) переписується без риски над $G(x)$:

$$\int_a^b F(x)G(x)dx = 0.$$

Цій умові ортогональності задовольняють, зокрема, косинусоїди і синусоїди різних частот за $a = -\infty$, $b = \infty$:

$$\int_{-\infty}^{\infty} \cos \omega_1 t \cos \omega_2 t dt = 0, \quad \int_{-\infty}^{\infty} \sin \omega_1 t \sin \omega_2 t dt = 0, \quad \omega_1 \neq \omega_2.$$

Таким чином, подання сигналів за допомогою зворотного перетворення Фур'є є по суті ортогональними розкладами. Властивість ортогональності полегшує процес відшукування цих коефіцієнтів.

Повернемося до спектрів сигналів. Припустимо, що комплексну функцію частоти $X(\omega)$ – спектр сигналу $x(t)$ – можна подати у вигляді

$$X(\omega) = |X(\omega)|e^{-i\varphi(\omega)}, \quad (1.35)$$

де відповідно до теорії комплексних функцій $|X(\omega)|$ – модуль спектра, а $\varphi(\omega)$ – його аргумент зі зворотним знаком. При цьому

$$|X(\omega)| = \sqrt{A^2(\omega) + B^2(\omega)},$$

$$\varphi(\omega) = -\operatorname{arctg} \frac{B(\omega)}{A(\omega)},$$

де $A(\omega)$ – реальна частина $X(\omega)$ ($A(\omega) = \operatorname{Re} X(\omega)$); $B(\omega)$ – уявна частина $X(\omega)$ ($B(\omega) = \operatorname{Im} X(\omega)$), тому

$$X(\omega) = A(\omega) + iB(\omega).$$

Геометричний зміст наведених вище співвідношень ілюструє рис. 1.15.

Наділяючи $|X(\omega)|$ і $\varphi(\omega)$ фізичним змістом, $|X(\omega)|$ іноді називають *амплітудно-частотною характеристикою* сигналу (АЧХ), а $\varphi(\omega)$ – його *фазо-частотною характеристикою* (ФЧХ). Така термінологія є доречною; дійсно, якщо розглянути довільно вибрану частотну компоненту (при $\omega = \omega_0$)

$$\begin{aligned} \text{сигналу } X(\omega_0) e^{-i\varphi(\omega_0)t} = \\ = |X(\omega_0)| e^{-i\varphi(\omega_0)t} \times e^{i\omega_0 t} = X(\omega_0) e^{-i\varphi(\omega_0)t}, \end{aligned}$$

то стає зрозумілим, що $|X(\omega_0)|$ визначає її амплітуду, а $\varphi(\omega_0)$ – початкову фазу (зі зворотним знаком).

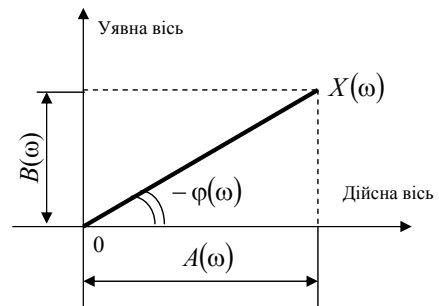


Рисунок 1.15 – Геометричний зміст спектра сигналу

Приклад 11. Як приклад досліджуємо спектр прямокутного імпульсу (див. рис. 1.13). Відповідно до (1.31)

$$\begin{aligned} X(\omega) &= \int x(t)e^{-i\omega t} dt = \int 1 \cdot e^{-i\omega t} dt = \frac{e^{-i\omega t}}{-i\omega} \Big|_{-T/2}^{T/2} = \frac{e^{-i\omega T/2} - e^{i\omega T/2}}{-i\omega} = \\ &= 2 \frac{\sin T/2\omega}{\omega}. \end{aligned}$$

Побудуємо графік одержаного спектру (рис. 1.16). Звернемо увагу на те, що цей спектр є дійсною функцією частоти (цією властивістю володіють спектри всіх парних сигналів). Можна відзначити, що максимальне значення функція $X(\omega)$ набуває в точці $\omega = 0$ (воно дорівнює, як легко перевірити, розкривши невизначеність за правилом Лопітала T); іншими словами, найбільший «внесок» при «побудові» прямокутного імпульсу вносить функція $e^{i\omega t}$ нульової частоти, так звана постійна складова. Найменший (нульовий) «внесок» роблять комплексні експоненти з частотами $\omega = k(2\pi/T)$, $k = \pm 1; \pm 2; \dots$; коефіцієнти в них $X(k(2\pi/T))$ дорівнюють нулю. Вплив на форму прямокутного сигналу експоненціальних функцій $e^{i\omega t}$ при $\omega \rightarrow \pm\infty$ стає все меншим. Дійсно, спектр цього сигналу наближається до 0 зі зростанням частоти: $\lim_{\omega \rightarrow \pm\infty} 2(\sin(T/2\omega)/\omega) = 0$.

Властивості спектрів. Наведемо без доказу низку добре відомих і важливих для подальшого властивостей спектрів:

1. Амплітудно-частотна характеристика і реальна частина спектра $X(\omega)$ довільного речовинного сигналу $x(t)$ є парними функціями частоти, а його уявна частина і фазочастотна характеристика – непарними, тобто

$$\begin{aligned} A(\omega) &= A(-\omega); \quad |X(\omega)| = |X(-\omega)|; \\ B(\omega) &= -B(-\omega); \quad \varphi(\omega) = -\varphi(-\omega). \end{aligned}$$

2. **Теорема 2** (масштабів). Нехай сигнал $x(t)$ має спектр $X(\omega)$. Тоді сигнал $x(\alpha t)$, де α - довільне дійсне число, має спектр $\frac{1}{|\alpha|} X\left(\frac{\omega}{\alpha}\right)$.

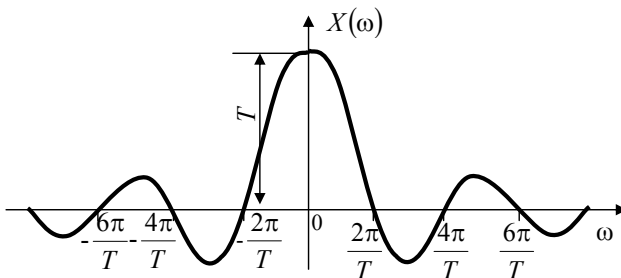


Рисунок 1.16 – Графік спектру прямокутного імпульсу

Цю теорему ілюструє рис. 1.17, де зображені прямокутні сигнали $x(t)$ і $x(\alpha t)$, $\alpha = 2$ (рис. 1.17, а) і відповідні до них спектри $X(\omega)$ і $\frac{1}{|\alpha|} X\left(\frac{\omega}{\alpha}\right)$ (рис. 1.16, б).

Наслідок. Перехід від дійсного сигналу $x(t)$ до інвертованого в часі сигналу $x(-t)$ призводить до перетворення спектру початкового сигналу $X(\omega)$ в комплексно-зв'язаний спектр $\bar{X}(\omega)$.

Це твердження впливає безпосередньо з теореми масштабів і наведеної вище властивості спектрів 1, внаслідок якого $\text{Re } X(\omega)$ – парна функція, а $\text{Im } X(\omega)$ – непарна. Дійсно, спектр сигналу $x(-t)$ має вигляд

$$\frac{1}{|-1|} X\left(\frac{\omega}{-1}\right) = \text{Re } X(-\omega) + i \text{Im } X(-\omega) = \bar{X}(\omega).$$

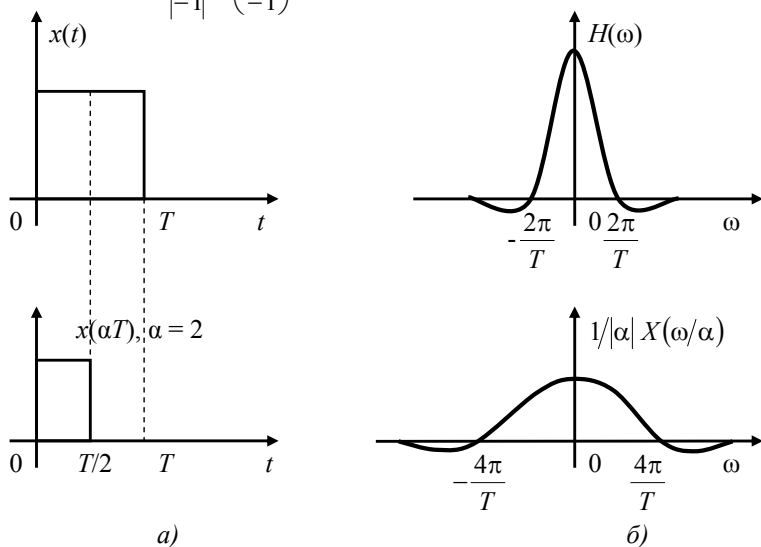


Рисунок 1.17 – Прямокутні сигнали $x(t)$ і $x(\alpha t)$, $\alpha = 2$

і відповідні до них спектри $X(\omega)$ і $\frac{1}{|\alpha|} X\left(\frac{\omega}{\alpha}\right)$

3. **Теорема 3** (Релея-Парсеваля). Енергія сигналу дорівнює енергії його спектра, поділеної на 2π :

$$\int_0^{\infty} x^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |X(\omega)|^2 d\omega.$$

Зауваження. Із останньої рівності виходить, що енергія сигналу не залежить від його фазочастотної характеристики, оскільки остання «не бере участі» в правій частині.

4. **Теорема 4** (затримки). Нехай сигнал $x(t)$ має спектр $X(\omega)$. Тоді сигнал $x(t - \tau)$ (початковий сигнал $x(t)$, що затримався на якийсь час τ) має спектр $X(\omega)e^{-i\omega\tau}$.

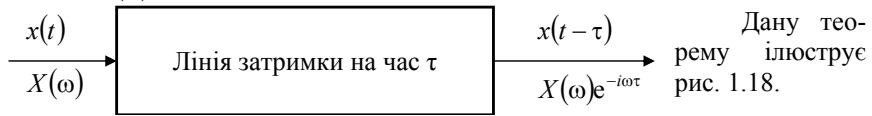


Рисунок 1.18 – Проходження сигналу через лінію затримки на час τ

5. **Теорема 5** (В. А. Котельникова). Довільний сигнал $x(t)$, спектр якого $X(\omega)$ поза смугою частот $-\Omega < \omega < \Omega$ дорівнює 0 (такі сигнали називають смуго-обмеженими), може бути відновлений за своїми дискретними значеннями (відліками), узятими через інтервал часу, з

$$T = \pi/\Omega$$

(інтервал Котельникова), або з подвоєною верхньою частотою, оскільки періоду відповідає частота дискретизації

$$f_d = \frac{1}{T} = \frac{\Omega}{\pi} = \frac{2\pi f_B}{\pi} = 2f_B,$$

де f_B – верхня частота в спектрі сигналу $x(t)$, Гц. Формула відновлення сигналу має вигляд

$$x(t) = \sum_{k=-\infty}^{\infty} x(kT) \frac{\sin \Omega(t - kT)}{\Omega(t - kT)}.$$

На рис. 1.19, *a* наведено модуль спектра смуго-обмеженого сигналу, а на рис. 1.19, *б* наведено його дискретні значення, взяті відповідно до теореми В.А. Котельникова.

Зуваження. Можна показати, що сума квадратів усіх «котельниковських» відліків сигналу $x(kT)$, $k = 0, \pm 1, \pm 2, \dots$ пов'язана з його енергією співвідношенням

$$T \sum_{k=-\infty}^{\infty} x^2(kT) = \int_{-\infty}^{\infty} x^2(t) dt.$$

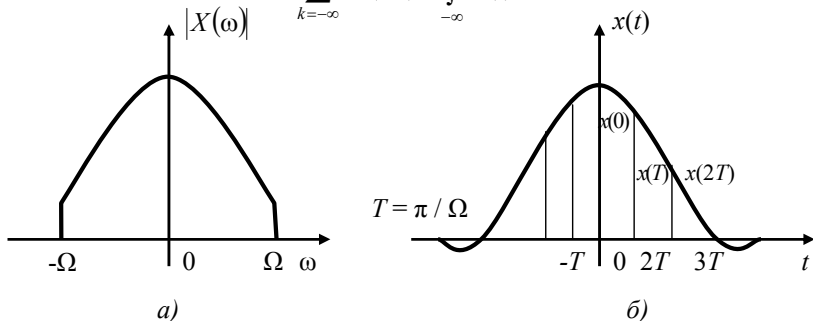


Рисунок 1.19 – Модуль спектра смуго-обмеженого сигналу та його дискретні значення

6. **Теорема 6** (щодо згортки). Нехай маємо два сигнали $u(t)$ і $v(t)$. Введемо третій сигнал $w(t)$ за допомогою так званої формули згортки

$$w(t) = \int_{-\infty}^{\infty} u(\tau)v(t - \tau)d\tau.$$

Тоді спектри сигналів $u(t)$, $v(t)$ та $w(t)$ пов'язані співвідношенням $W(\omega) = U(\omega)V(\omega)$.

7. **Теорема 7** (диференціювання). Якщо сигнал $x(t)$ має спектр $X(\omega)$, то похідна сигналу

$$x'(t) = \frac{d}{dt}x(t)$$

має спектр $i\omega X(\omega)$.

8. **Теорема 8** (зсуви спектра). Множення сигналу $x(t)$ зі спектром $X(\omega)$ на функцію $2 \cos \omega_0 t$ або $2 \sin \omega_0 t$ призводить до таких результатів:

$$\int_{-\infty}^{\infty} x(t)2 \cos \omega_0 t e^{-i\omega t} dt = X(\omega + \omega_0) + X(\omega - \omega_0);$$

$$\int_{-\infty}^{\infty} x(t)2 \sin \omega_0 t e^{-i\omega t} dt = iX(\omega + \omega_0) - iX(\omega - \omega_0).$$

Передавальні функції та імпульсні реакції лінійних систем.

Визначення. Лінійною системою (ланцюгом) називають «чорний ящик» (пристрій з входом і виходом, внутрішня структура якого може бути невідомою) (рис. 1.20), що задовольняє умовам:

1) якщо сигнал $x(t)$ на вході «чорного ящика» породжує сигнал $y(t)$ на його виході, то при подачі на вхід сигналу $\alpha x(t)$, $\alpha = \text{const}$, на виході одержимо $\alpha y(t)$;

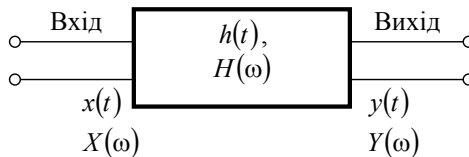


Рисунок 1.20 – Лінійна система

2) якщо сигнали $x_1(t)$ і $x_2(t)$ на вході «чорного ящика» породжують на виході сигнали $y_1(t)$ і $y_2(t)$ відповідно, то при подачі на вхід сигналу $x_1(t) + x_2(t)$ на виході одержимо $y_1(t) + y_2(t)$.

Якщо лінійна система задовольняє умові стаціонарності, тобто її властивості і параметри незмінні в часі, то сигнали на її вході $x(t)$ і на виході $y(t)$ пов'язані згадуваним вище співвідношенням згортки

$$y(t) = \int_{-\infty}^{\infty} x(\tau)h(t - \tau)d\tau = \int_{-\infty}^{\infty} h(\tau)x(t - \tau)d\tau,$$

де $h(t)$ – імпульсна реакція цієї системи. Нагадаємо, в чому суть поняття «імпульсна реакція».

Визначення. Імпульсною реакцією називають відгук системи (рис. 1.21, б) на вхідну дію у вигляді δ -функції (рис. 1.21, а) - нескінченно короткого імпульсу нескінченно великої амплітуди, що має одиничну площу (див. рис. 1.22, на якому зображена послідовність прямокутних імпульсів зростаючої амплітуди k/T й спадної тривалості T/k , $k = 1, 2, \dots$, які переходять у межу за $k \rightarrow \infty$ в δ -функцію).

Якщо імпульсна реакція характеризує поведінку лінійної системи в часовій області, то для її опису в частотній області використовують передавальну функцію.

Визначення. Перетворення Фур'є від імпульсної реакції називають передавальною функцією

$$H(\omega) = \int_{-\infty}^{\infty} h(t)e^{-i\omega t} dt.$$

Через згадану вище теорему про згортання між вхідним і вихідним спектрами лінійної стаціонарної системи (таку систему часто називають системою з інваріантними в часі параметрами) існує надто простий зв'язок (див. рис. 1.20):

$$Y(\omega) = X(\omega)H(\omega).$$

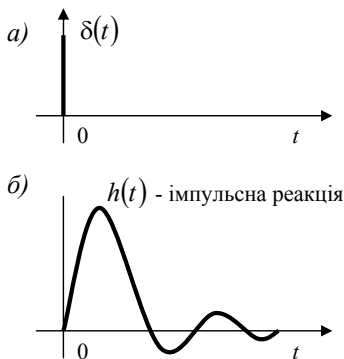


Рисунок 1.21 – Імпульсна реакція

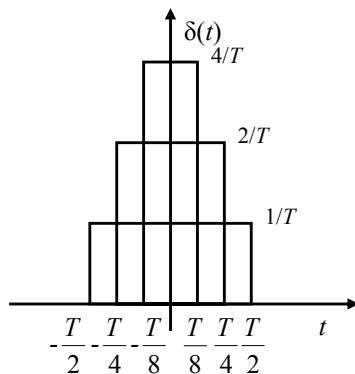


Рисунок 1.22 – Послідовність прямокутних імпульсів

Зауваження. Іноді передавальну функцію вводять за допомогою останньої рівності, визначаючи цю функцію як відношення спектра на виході лінійної стаціонарної системи до спектра на вході цієї системи:

$$H(\omega) = Y(\omega) / X(\omega).$$

Зауваження. Безпосередньо перевіркою можна установити, що парній імпульсній реакції $h(t)$ відповідає парна дійсна передавальна функція $X(\omega)$, а непарній імпульсній реакції – уявна передавальна функція. За аналогією з амплітудно- і фазочастотними характеристиками, якими характеризується спектр довільного сигналу, для передавальної функції лінійної системи

$$H(\omega) = |H(\omega)| e^{-i\varphi(\omega)}$$

вводять амплітудно-частотну характеристику (АЧХ) $|H(\omega)|$ і фазочастотну характеристику (ФЧХ) $\varphi(\omega)$.

Оскільки неспотворююча (ідеальна) передавальна функція повинна тотожно дорівнювати 1 (при цьому спектри, а значить і сигнали, на виході лінійної системи збігаються):

$$H_{\text{ід}}(\omega) = 1, \quad -\infty < \omega < \infty,$$

то для неспотворюючих АЧХ, ФЧХ і ГЧП одержуємо співвідношення

$$\left. \begin{aligned} |H_{\text{ід}}(\omega)| &= 1, \quad -\infty < \omega < \infty, \\ \varphi_{\text{ід}}(\omega) &= 0, \quad -\infty < \omega < \infty, \\ \tau_{\text{ід}}(\omega) &= 0, \quad -\infty < \omega < \infty. \end{aligned} \right\}$$

Проте на практиці, посиленням (послабленням), а також запізнюванням сигналу (при збереженні його форми незмінною) у багатьох випадках можна нехтувати і систему з передавальною функцією $Ae^{-i\omega\tau_0}$, $A = \text{const}$, $\tau_0 = \text{const}$ вважати неспотворюючим ланцюгом. Тому за «ідеальні» часто розглядають характеристики, наведені на рис. 1.23:

$$\left. \begin{aligned} |H_{\text{ід}}(\omega)| &= A, \quad -\infty < \omega < \infty, \\ \varphi_{\text{ід}}(\omega) &= \omega\tau_0, \quad -\infty < \omega < \infty, \\ \tau_{\text{ід}}(\omega) &= \frac{d(\omega\tau)}{d\omega} = \tau_0, \quad -\infty < \omega < \infty, \\ \tau_0 &= \text{const}. \end{aligned} \right\}$$

Якщо порушується хоча б одна із цих умов, вихідний сигнал відрізняється формою від вхідного. Так, спотворення АЧХ типу «завал» високих частот призводить до подовження часу наростання фронтів імпульсів (фронти стають пологими). До збільшення тривалості фронтів призводять також спотворення ФЧХ або ГЧП. Характерною ознакою спотворень ФЧХ або ГЧП є поява асиметрії вихідного сигналу за умови, що вхідний сигнал був чітко симетричним. Зупинимось докладніше на питанні дії на сигнали, що передаються, спотворень АЧХ і ФЧХ (так званих лінійних спотворень).

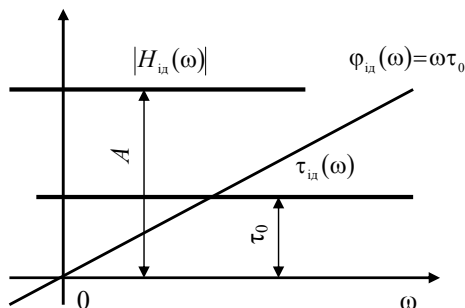


Рисунок 1.23 – «Ідеальні» характеристики

Зважаючи дія спотворень АЧХ. Виникаючі в реальних ситуаціях спотворення АЧХ різноманітні. Нижче ми вивчимо (в ідеалізованому вигляді) один із найпоширеніших видів спотворень АЧХ – «завал» високих частот. На практиці при передаванні дискретної інформації значно використовуються сигнали прямокутної форми. Що відбувається з сигналом такого типу при проходженні через так званий «ідеальний» фільтр нижніх частот (АЧХ цього фільтра показана на рис. 1.24). Фазочастотну характеристику «ідеального» фільтра вважають рівною 0, отже, фазочастотних спотворень фільтр не вносить.

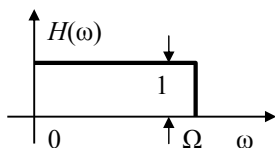


Рисунок 1.24 – АЧХ «ідеального» фільтра нижніх частот

Проте його АЧХ, що дорівнює 1 в інтервалі $0 < \omega < \Omega$, обертається в 0 для всіх частот, більш ніж Ω . Вхідні сигнали позбавляються високих частот при проходженні через такий фільтр, що призводить до характерних змін форми, наприклад, прямокутного імпульсу (рис. 1.25, де наведено вхідний $x(t)$ і вихідний $y(t)$ сигнали «ідеального» фільтра). Фронт вихідного імпульсу виявляється пологим, формула для тривалості фронту має вигляд

$$t_{\text{фр}} = 1/2f_{\text{в}}, \quad (1.36)$$

де $f_{\text{в}}$ - верхня частота смуги пропускання, тобто $f_{\text{в}} = \Omega/2\pi$. Оскільки інтервал часу T , яким відокремлені один від одного відліки смугообмеженого сигналу з верхньою частотою $f_{\text{в}}$ взяті відповідно до теореми Котельникова, визначається рівністю $T = 1/2f_{\text{в}}$, то співвідношення (1.36) можна переписати так: $t_{\text{фр}} = T$. Остаточний висновок можна сформулювати таким чином: тривалість фронту на виході «ідеального» фільтра дорівнює інтервалу Котельникова. Позначена буквою a амплітуда так званого першого викиду складає 9% сталого значення; вона не залежить від вели-

чини f_v : зі зростанням f_v частота коливань на вершині прямокутного імпульсу зростає (вона дорівнює $2f_v$), а амплітуда залишається незмінною – так виявляється добре відоме явище Гіббса (див. рис. 1.25). Відзначимо, що незалежність амплітуди першого викиду від f_v має місце лише для прямокутних імпульсів достатньо великої тривалості, коли перехідні процеси, породжені кожним із фронтів імпульсу, не роблять помітного впливу один на одного. Згадана незалежність a від f_v виконується в точності у перехідній характеристиці «ідеального» фільтра. В зв'язку з цим нагадаємо поняття перехідної характеристики.

Визначення. Перехідною характеристикою $p(t)$ називається відгук лінійної системи на включення напруги – «сходинку», тобто сигнал

$$x(t) = \begin{cases} 0, & t < 0, \\ 1, & t \geq 0. \end{cases}$$

Відзначимо, що іноді перехідну характеристику визначають як граничну реакцію системи на прямокутний імпульс, фронт якого з'являється в нульовий момент часу, а зріз прагне до «плюс нескінченності».

Відомо, що імпульсна реакція системи є першою похідною її перехідної характеристики

$$h(t) = dp(t)/dt.$$

Для передачі даних і телеграфії особливо важливу роль відіграє формула (1.36), оскільки вона обмежує знизу тривалість використовуваних одиничних інтервалів або зверху швидкість модуляції. Дійсно, при використанні посилок (одиничних елементів), коротших, ніж $t_{\text{фр}}$, на виході «ідеального» фільтра з частотою зрізу f_v стає значення сигналу M , що відповідає його плоскій вершині, взагалі не може бути досягнуто. Ця ситуація породжує добре відомі в телеграфії характерні спотворення.

Вплив першого викиду, що заважає, позначається не стільки при передачі телеграфних сигналів, скільки при трансляції рухомих і нерухомих зображень (телебачення і фототелеграф). Цей вплив виявляється в характерній окантовці ліній, що знаходяться на межі чорного і білого.

Заважаюча дія спотворень ФЧХ. Розглянемо рис. 1.26, а, де наведено парно-симетричну щодо точки $t = t_0$ імпульсну реакцію, і порівняємо її із зображеною на рис. 1.26, б імпульсною реакцією, що не володіє подіб-

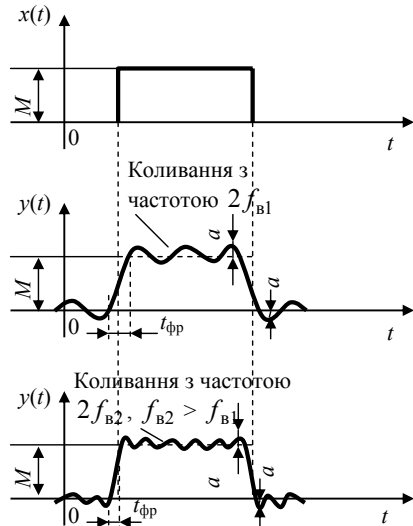


Рисунок 1.25 – Явище Гіббса

ною симетрією. Що можна сказати про частотні характеристики лінійних систем з такими імпульсними реакціями?

Лінійна система з імпульсною реакцією, яка позбавлена парної симетрії, має спотворюючу ФЧХ. Ця властивість імпульсної реакції дозволяє легко «діагностувати» спотворення ФЧХ.

Надто важливим є характер впливу спотворень ФЧХ на максимальне за абсолютною величиною значення імпульсної реакції. Справедливе наступне твердження: максимальне за абсолютною величиною значення імпульсної реакції системи з лінійною ФЧХ ωt_0 (воно реалізується за $t = t_0$, див. рис. 1.26, а) $h(t_0) = |h(t_0)|^5$ більше або рівне максимальному значенню модуля імпульсної реакції $h_{\text{сп}}(t)$ (рис. 1.26, б) лінійної системи з тією ж АЧХ, але з довільно вибраною спотворюючою ФЧХ, тобто

$$h_{\text{макс сп}} \leq h(t_0),$$

де

$$h_{\text{макс сп}} = \max_{-\infty < t < \infty} |h_{\text{сп}}(t)| = |h_{\text{сп}}(t_1)|.$$

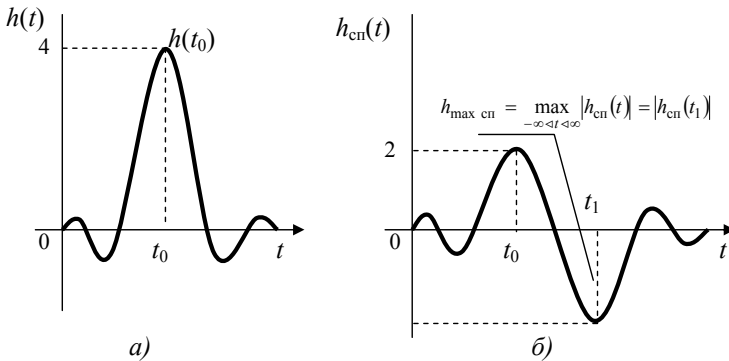


Рисунок 1.26 – Парно-симетрична щодо точки $t = t_0$ імпульсна реакція

Це явище істотно впливає на високошвидкісне передавання дискретної інформації, оскільки максимальне значення відгуку еквівалентного каналу зв'язку (що містить разом з дійсним каналом формуючий фільтр передавача і узгоджений фільтр приймача) є звичайно «переносієм» інформації. Тому зменшення за абсолютною величиною цього значення викликає зменшення відношення сигнал-шум, тобто зниження достовірності.

З позицій передавання телеграфних посилок зменшення максимуму (пікового значення) імпульсної реакції також небажане через збільшення тривалості їхніх фронтів. Дійсно, тривалість фронту обернено пропорційна його крутизні, тобто першій похідній, яка дорівнює максимальному значенню імпульсної реакції.

⁵ Можна показати, що максимальне за абсолютною величиною значення імпульсної реакції системи з лінійною ФЧХ завжди позитивне.

Перейдемо до ще одного важливого ефекту, що породжується спотвореннями ФЧХ. Для його викладу знадобляться наступні, добре відомі факти. По-перше, енергія імпульсної реакції дорівнює енергії передавальної функції поділений на 2π):

$$\int_{-\infty}^{\infty} h^2(t) dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |H(\omega)|^2 d\omega. \quad (1.37)$$

По-друге, для смуго-обмежених лінійних систем зі смугою пропускання $(0, \Omega)$, $\Omega = 2\pi f_b$ енергія імпульсної реакції може бути знайдена за її відліками $h(kT)$, взятих відповідно до теореми Котельникова:

$$\int_{-\infty}^{\infty} h^2(t) dt = T \sum_{k=-\infty}^{\infty} h^2(kT), \quad T = \frac{\pi}{\Omega} = \frac{1}{2f_b}, \quad k = 0, \pm 1, \pm 2, \dots$$

Із наведених двох рівностей виходить, що

$$T \sum_{k=-\infty}^{\infty} h^2(kT) = \frac{1}{2\pi} \int_{-\Omega}^{\Omega} |H(\omega)|^2 d\omega.$$

Останнє співвідношення показує, що сума квадратів відліків імпульсної реакції, взятих з подвоєною верхньою частотою f_b , визначається інтегралом від квадрата АЧХ, але не залежить від форми ФЧХ.

Відзначене вище зменшення максимального абсолютного значення імпульсної реакції каналу з нульовою ФЧХ при появі спотворень ФЧХ призведе до зростання, принаймні, деяких із відліків імпульсної реакції для ненульових відлікових моментів $t = kT, k = \pm 1, \pm 2, \dots$. Лише при цьому сума $h^2(kT) \quad k = 0, \pm 1, \dots$ зможе зберегтися незмінною. Даний факт має важливу фізичну інтерпретацію: нелінійна ФЧХ породжує міжсимвольну інтерференцію, тобто «хвіст» з відлікових значень, що йдуть слідом за імпульсним сигналом і впливають на подальший імпульсний сигнал (рис. 1.27).

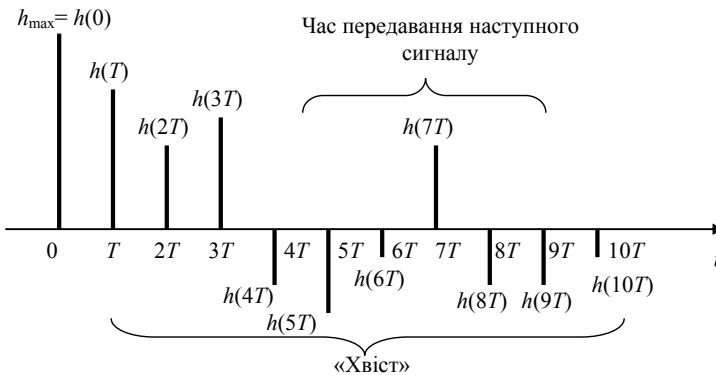


Рисунок 1.27 – Міжсимвольна інтерференція

У процесі розвитку техніки формування сигналів пропонувались різноманітні моделі електричних сигналів та інформаційних каналів. Спочатку при аналізі лінійних електричних кіл в усталеному режимі роботи застосовувалась надто спрощена аналітична модель: сигнали й завади подавались у формі гармонічного коливання певної частоти чи сукупності незначної кількості гармонічних коливань різних частот. Потім сигнали й завади стали описувати за допомогою ряду чи інтеграла Фур'є, проте їхній випадковий характер не враховувався.

Як зазначено вище, детермінована, тобто попередньо відома функція часу не може слугувати як переносій інформації. Тому інформаційні процеси в каналах зв'язку принципово потребують використання ймовірнісних моделей. Випадковий часовий процес $f(t)$ являє собою множину функцій параметра t із заданою на цій множині ймовірнісною мірою. Випадкові процеси можна класифікувати за різноманітними ознаками.

Скажімо, за *часовою структурою* розрізняють дискретні й неперервні процеси; за *ступенем стійкості ймовірнісних характеристик у часі* – стаціонарні й нестаціонарні процеси; за *ступенем відповідності числових характеристик за множиною й за часом* – ергодичні й неергодичні процеси тощо.

На початку 30-х років минулого сторіччя В.І. Сіфоров уперше використав апарат теорії ймовірностей для розв'язання завдання завадостійкості зв'язку. 1933 року В.А. Котельниковим було введено більш складну стаціонарну модель сигналів з обмеженим спектром. При цьому було використано лінійну модель інформаційного каналу типу фільтра нижніх частот.

Розвинення кібернетики спричинилося глибоким впровадженням ймовірнісних методів у теорію зв'язку. К. Шеннон запропонував розглядати процес передавання інформації як випадкове вибирання реалізацій сигналів з алфавіту джерела; при цьому власне сигнал та канал зв'язку описувались моделлю Котельникова.

Наприкінці 50-х років ХХ сторіччя була запропонована нестаціонарна модель електричних сигналів та лінійну модель інформаційного каналу з обмеженим власним інтервалом кореляції.

Одне із провідних положень теорії зв'язку полягає в тім, що сигнал $u_c(t)$ розглядається як випадковий процес, утворений кінцевою множиною детермінованих функцій часу $\{u_{ck}(t)\}$, названих *реалізаціями сигналу*. Кожна реалізація характеризується ймовірністю появи P_k ($k=1,2,\dots,m$), а ансамбль реалізацій утворює скінченну систему подій.

Подібна модель є цілковито слушна й для завод.

У дискретних каналах реалізація сигналу $u_{ck}(t)$ являє собою n -цифрові послідовності елементарних сигналів тривалістю t_0 , які відбивають кодові символи, тобто набувають з певною ймовірністю одне з m значень основи коду. За математичного опису елементарного сигналу вважа-

тимемо його за випадкову функцію часу, задану на інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$,

тобто будемо проводити відлік часу від середини даного елемента. Змінювання станів елементарних сигналів (змінювання значення m) являє собою процес *маніпулювання сигналом*. Скажімо так, літера К за міжнародним кодом № 2 для стартстопних телеграфних апаратів має сигнальну реалізацію $u_{ck}(t) = 10011$, а літера Ф – реалізацію $u_{cl}(t) = 01110$.

Кількість елементарних сигналів, що передаються за 1 с, характеризує *швидкість модуляції*, вимірювану в бодах:

$$B = \frac{1}{t_0}. \quad (1.38)$$

Якщо, наприклад, $t_0 = 10$ мс, то $B = 100$ Бод. Зазначимо, що величина B описує швидкість передавання сигналів; поряд з цим слід розрізнявати швидкість передавання інформації V_i , яка у загальному випадку не збігається з B .

Прості й складні сигнали. Переважна більшість існуючих дискретних систем зв'язку використовує *прості сигнали*, в яких елементарні сигнали є відліки гармонічних коливань:

$$u_{ck} = U_{c\max} \cos(\omega t + \varphi), \quad 0 \leq t \leq t_0.$$

Внаслідок модуляції можуть змінюватися амплітуда (системи АМ), частота (системи ЧМ), фаза коливань (системи ФМ). Для двійкових систем реалізації елементарних сигналів мають вигляд:

для систем АМ

$$u_{cl} = U_{c\max} \cos(\omega t + \varphi); \quad u_{c2}(t) = 0; \quad (1.39)$$

для систем ЧМ

$$u_{cl} = U_{c\max} \cos(\omega_1 t + \varphi); \quad u_{c2}(t) = U_{c\max} \cos(\omega_2 t + \varphi); \quad (1.40)$$

для систем ФМ

$$u_{cl} = U_{c\max} \cos(\omega t + \varphi); \quad u_{c2}(t) = U_{c\max} \cos(\omega_2 t + \varphi + \pi) = -u_{cl}(t). \quad (1.41)$$

Трапляється іноді, що елементарний сигнал не є відлік гармонічного коливання, а є відлік модульованого за певним законом коливання. Сигнали, утворені такими елементами, будемо називати *складними сигналами*. До них належать сигнали в каналах із завмираннями, сигнали в системах АІМ, сигнали з модуляцією несучої частоти за лінійним законом та ін.

1.1.4. Канонічне розкладання сигналів

Розвиток техніки зв'язку супроводжується все ширшим використанням сигналів складної форми. Такі сигнали дозволяють послабити ефект багатопроменевого поширення радіохвиль, передавати мовні сигнали каналами зі смугою пропускання десятки-сотні герц, підвищувати енергетичну прихованість каналів зв'язку, здійснювати з високою точністю вимі-

рювання відстаней та швидкостей відносного переміщення різноманітних об'єктів та ін.

При аналізованні таких сигналів надто зручним стає метод канонічних розкладань, розроблений В.С. Пугачовим.

Випадковий процес може бути подано у вигляді скінченної чи нескінченної суми *елементарних випадкових функцій* вигляду

$$v_0(t) = A\psi(t), \quad (1.42)$$

де A – випадкова величина; $\psi(t)$ – детермінована функція часу.

Для випадкової функції $v_0(t)$ є притаманно, що особливості випадкового процесу – випадковість та залежність від часу – розділено: перша визначається величиною A , а друга – детермінованою функцією $\psi(t)$.

Математичне сподівання функції $v_0(t)$ буде

$$E[v_0(t)] = E[A]\psi(t),$$

де $E[A]$ – математичне сподівання випадкової величини A .

Якщо $E[A] = 0$, то $E[v_0(t)] = 0$ й випадкова функція $v_0(t)$ має назву *центрована*. Кожну функцію $v_0(t)$ можна центрувати шляхом впровадження нової функції $v(t) = v_0(t) - E[v_0(t)]$, тому в подальшому будемо розглядати лише центровані випадкові функції часу.

Нехай функція $v(t)$, яка піддається певному лінійному перетворенню, описуваному оператором L_0 . Тоді

$$L_0[v(t)] = AL_0[\psi(t)].$$

Отже, лінійне перетворення елементарної випадкової функції зводиться до лінійного перетворення її детермінованої складової. Ця властивість наочно відбиває аналітичну зручність методу канонічних розкладань: випадковий процес, який піддається лінійному перетворенню, подається у вигляді суми елементарних випадкових функцій, які піддаються потім заданому перетворенню.

Подання сигналу $u_c(t)$ у вигляді

$$u_c(t) = \sum_{k=0}^N A_k \psi_k(t) \quad (1.43)$$

має назву *розкладання сигналу*, випадкові величини $\{A_k\}$ – *коефіцієнти розкладання* (вагові коефіцієнти), а детерміновані функції $\{\psi_k(t)\}$ – *координатні функції*.

Розподіл сигналу, за якого коефіцієнти $\{A_k\}$ є некорельовані, а функції $\{\psi_k(t)\}$ є ортогональні, має назву *канонічне розкладання сигналу*.

Координатні функції слід обирати в такий спосіб, щоб кожний сигнал та заваду можна було подати збіжним рядом (1.43), щоб вони були зручні з точки зору виконання математичних операцій і мали спектр практично скінченної ширини.

За розкладання випадкової функції $u_c(t)$ в ряд (1.43) слід враховувати точність апроксимації. Помилковим є вважати, що за довільних $u_c(t)$ та $\{\psi_k(t)\}$ різниця

$$u_c(t) - \sum_{k=1}^N A_k \psi_k(t) \quad (1.44)$$

Тотожно буде прагнути до нуля зі збільшенням кількості доданків, оскільки у загальному випадку функція $u_c(t)$ може не відповідати вимогам аналітичності, тобто може бути розривною разом з похідними будь-якого порядку. Тому практично накладають певні обмеження на функцію $u_c(t)$, наприклад, вважають, що ширина її спектра є скінченна, й задаються точністю розкладання за обмеженої кількості $\{\psi_k(t)\}$.

Одним із широко використовуваних на практиці критеріїв оцінювання різниці (1.44) є мінімальна величина інтеграла

$$I = \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} \left| u_c(t) - \sum_{k=1}^N A_k \psi_k(t) \right|^2 dt.$$

Вагові коефіцієнти розкладання визначаються з рівняння

$$\frac{dI}{dA_k} = 0.$$

Диференціюючи і помножуючи обидві частини цього рівняння на функцію $\psi_l(t)$, де $l=1,2,\dots,N$, дістанемо

$$2 \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} \left[u_c(t) - \sum_{k=1}^N A_k \psi_k(t) \right] \psi_l(t) dt = 0.$$

Оскільки множина $\{\psi_k(t)\}$ є ортогональна, то коефіцієнт

$$A_k = \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_c(t) \psi_k(t) dt.$$

Отже, канонічне розкладання забезпечує мінімальну середню квадратичну помилку при подаванні сигналів та завад.

Легко впевнитися, що подавання сигналів та завад рядом Фур'є є канонічне розкладання, коли за координатні функції $\{\psi_k(t)\}$ використовуються тригонометричні функції. В теорії зв'язку широко використовуване подавання сигналів рядом Котельникова також є канонічне розкладання з координатними функціями $\frac{\sin 2\pi F_c(t - k\Delta t)}{2\pi F_c(t - k\Delta t)}$ та ваговими коефіцієнтами,

порівнюваними миттєвим значенням сигналу в точках $k\Delta t$, де інтервал Δt визначається граничною частотою спектра сигналу F_c .

Очевидно, що завади також можуть бути подані в канонічній формі.

Реальні сигнали й завади є дійсними функціями часу. Проте для їхнього опису використовуються комплексні функції. При цьому реальний сигнал можна подати у два способи. За першого способу сигнал виражається у вигляді суми елементарних складових, кожна з яких є комплексною функцією часу. За другого способу, надто зручному для опису вузько смугових сигналів, сам сигнал розглядається як комплексна функція часу.

У канонічній формі сигнал має вигляд

$$u_c(t) = \sum_{k=-\infty}^{\infty} A_k \psi_k(t), \quad (1.45)$$

причому лінійно незалежні координатні функції $\{\psi_k(t)\}$ можуть бути дійсними й комплексними. Сигнал $u_c(t)$ буде дійсним, якщо лише кожен комплексний доданок $A_k \psi_k(t)$ має комплексно-спряжений доданок $A_k^* \psi_k^*(t)$. Для дійсних функцій $\psi_k(t) = \psi_{-k}(t)$ і в цьому разі $\psi_k(t)$ визначає половину внеску k -го доданка в канонічному розкладанні сигналу (за винятком є доданок $\psi_0(t)$, який є завжди дійсним і зустрічається в розкладанні одноразово).

Нехай $A_k^* = A_{-k}$ та $\psi_k^*(t) = \psi_{-k}(t)$. Ця умова означає, що вся інформація про реальний сигнал $u_c(t)$ міститься в доданках з індексами $k \geq 0$. Підсумовуючи ці члени, дістанемо комплексний сигнал

$$\dot{u}_c(t) = \sum_{k=0}^{\infty} A_k \psi_k(t) = u_c(t) + i u_c^*(t),$$

де спряжені реалізації

$$u_c(t) = \sum_{k=0}^{\infty} (a_k \cos k\omega_c t + b_k \sin k\omega_c t);$$

$$u_c^*(t) = \sum_{k=0}^{\infty} (-b_k \cos k\omega_c t + a_k \sin k\omega_c t)$$

дістаються одна з одної змінюванням фаз усіх складових на 90° . Очевидно, що енергетичні спектри $u_c(t)$ та $u_c^*(t)$ збігаються.

Дістати безпосередньо комплексний сигнал $\dot{u}_c(t)$ з дійсного сигналу $u_c(t)$ можливо лише за певних обмежень, які накладаються на уявну частину сигналу $\dot{u}_c(t)$. Одне з обмежень полягає в тім, що сигнал $\dot{u}_c(t)$ має бути аналітичною функцією (тобто мати похідні, будь-якого порядку) й може бути розкладений у степеневий ряд комплексного змінного $S = t + i\xi$ у півплощині S , яка містить дійсну вісь t . При цьому дійсна та уявна частини комплексного сигналу є взаємно пов'язані перетворенням Гільберта. За

прикладі аналітичних функцій слугують $\cos x$, $\log x$ та $\frac{1}{x}$ (функцію $\frac{1}{x}$ можна розкласти в ряд Тейлора відносно кожної точки, яка не лежить на початку координат, де вона є сингулярна); функція $|x| = \sqrt{t^2 + \xi^2}$ є неаналітична, оскільки $|x|$ не можна подати степеневим рядом за змінною x .

Виникає питання: яке практичне значення має поняття аналітичного сигналу, якщо реально існують лише дійсні сигнали? Нехай $u_{1r}(t)$ та $u_{1l}(t)$ – дійсні сигнали на вході лінійної системи. При цьому на її виході також будуть дійсні сигнали $u_{2r}(t)$ та $u_{2l}(t)$. Тоді, згідно з принципом суперпозиції, вхідний сигнал $u_1(t) = u_{1r}(t) \pm u_{1l}(t)$ повинен утворити на виході системи сигнал $u_2(t) = u_{2r}(t) \pm u_{2l}(t)$, а комплексно-спряжений сигнал $u_1^*(t)$ повинен викликати комплексно-спряжений сигнал $u_2^*(t)$. Ця властивість лінійних систем дістала назву *спряженої симетрії*. Тому можна розглядати проходження аналітичного сигналу через лінійну систему, тимчасово нехтуючи його комплексно-спряженим двійником і пам'ятаючи, що відповідний реальний сигнал являє собою дійсну частину аналітичного сигналу. З виразу (1.44) випливає, що потужність аналітичного сигналу дорівнює подвоєній потужності реального сигналу. Отже, аналітичні сигнали можуть існувати лише у вигляді комплексно-спряжених пар, сума яких завжди є дійсна. Якщо передатна функція лінійної системи дорівнює відношенню комплексних амплітуд вихідного та вхідного сигналів, то при аналізованні проходження аналітичного сигналу через ланцюжок лінійних ланок потрібна операція звичайного множення, а не згортки. У цьому полягає велика зручність аналітичних сигналів.

Поняття аналітичного сигналу дозволяє подати нове тлумачення сигналу як інформаційного процесу. При розкладанні сигналу в ряд Фур'є амплітуди, частоти й фази його гармонічних складових виходять різними, але вони припускаються незмінними на всій осі часу. В дійсності, обвідна та миттєва частоти сигналу змінюються у часі. Для вузькосмугових сигналів та завд, в яких середня частота спектра f_0 є значно менша за його ширину Δf , обвідна та миттєва частоти є повільно змінюваними функціями часу порівняно з $\cos \varphi(t)$, а отже, порівняно із самою функцією $u_c(t)$. Це є велика зручність при аналізованні таких процесів. Виокремлення обвідної сигналу, миттєвих значень частоти й фази здійснюється нелінійними пристроями – амплітудними, частотними й фазовими детекторами, які для оптимального виконання власних функцій мають бути безінерційними.

Модель аналітичного сигналу стосовно флуктуаційних процесів використовувалась С. Райсом. Пізніше В.І. Бунімович докладно вивчив її властивості й розвинув способи її застосування для розв'язання різноманітних завдань. Зокрема, при передаванні сигналу $u_c(t) = U_c(t) \cos \omega t$ та наяв-

ності в каналі шумів $u_{\text{ш}}(t) = U_{\text{ш}}(t) \cos[\omega t + \varphi(t)]$ результуюче коливання на вході приймача буде

$$u_p(t) = u_c(t) + u_{\text{ш}}(t) = \sqrt{U_c^2(t) + U_{\text{ш}}^2(t) + 2U_c(t)U_{\text{ш}}(t)\cos\varphi} \times \\ \times \cos\left(\omega t + \arctg \frac{U_{\text{ш}}(t)\sin\varphi}{U_c(t) + U_{\text{ш}}(t)\cos\varphi}\right).$$

Впроваджуючи різноманітні гіпотези щодо властивостей $u_c(t)$ та $u_{\text{ш}}(t)$, можна дістати статистичні характеристики амплітуди й фази такого коливання.

Ортогональні сигнали. За подавання сигналів та завад рядом Фур'є кількість ненульових коефіцієнтів розкладання зазвичай є скінченна й ряд Фур'є перероджується у тригонометричну суму вигляду

$$u_c(t) = \sum_{k=k_1}^{k_2} (a_k \cos k\omega_c t + b_k \sin k\omega_c t). \quad (1.46)$$

Для реалізації сигналів $u_{cr}(t)$ та $u_{cl}(t)$, надаваних в інтервалі $\left(\frac{k_1}{t_0}, \frac{k_2}{t_0}\right)$ сумою (1.46), згідно з теоремою Парсеваля, слушним є співвідношення

$$\frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_{cr}(t) u_{cl}(t) dt = \frac{1}{2} \sum_{k=k_1}^{k_2} (a_{rk} a_{lk} + b_{rk} b_{lk}).$$

Звідси випливає, що для однієї реалізації ($r = l$)

$$\frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_c^2(t) dt = \frac{1}{2} \sum_{k=k_1}^{k_2} (a_k^2 + b_k^2),$$

тобто середня потужність сигналу дорівнює сумі потужностей його складових за розкладання в ряд Фур'є.

Права частина передостаннього виразу є скалярний добуток певних векторів U_s зі складовими $\frac{a_{sk}}{\sqrt{2}}$ та $\frac{b_{sk}}{\sqrt{2}}$ ($S = r, l$). Тому інтеграл в лівій частині виразу комплексного сигналу можна назвати *скалярним добутком реалізації сигналу* $u_{cs}(t)$, де $S = r, l$.

У теорії зв'язку значну роль відіграють *ортогональні сигнали*, для яких скалярний добуток

$$\frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_{cr}(t) u_{cl}(t) dt = \begin{cases} c & \text{за } r = l; \\ 0 & \text{за } r \neq l. \end{cases} \quad (1.47)$$

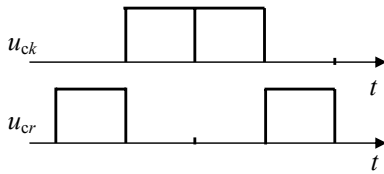
Зауважимо, що таке визначення дещо відрізняється від вживаного в теорії функцій, де до умови (1.47) додається друга умова:

$$\frac{1}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} u_{cr}^2(t) dt \neq 0 \text{ за кожного } r.$$

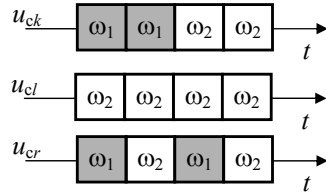
Якщо всі реалізації сигналів множини $\{u_{ck}(t)\}$ є ортогональними парами, то множина $\{u_{ck}(t)\}$ називається *ортогональною*.

Наведемо приклади систем зв'язку з ортогональними сигналами.

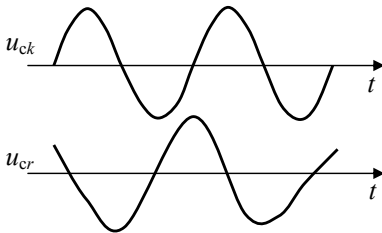
Приклад 12. Системи зв'язку АМ (рис. 1.28, а). Проте в такому випадку умова (1.47) не задовольняється їй, отже, ортогональність таких систем в певному розумінні є умовна.



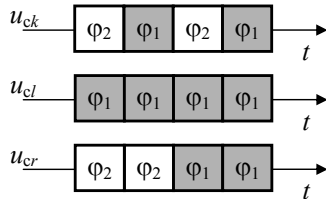
а)



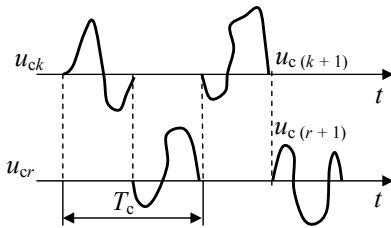
з)



б)



д)



е)

Рисунок 1.28 – Ортогональні сигнали

Приклад 13. Системи зв'язку зі спряженими сигналами (рис. 1.28, б). Неважко побачити, що в такому разі сума в правій частині наведеного вище виразу дорівнює нулеві.

Приклад 14. Системи зв'язку з ЧРК. У таких системах сигнали не перекриваються в часі (рис. 1.28, в) й інтеграл (1.47) тотожно дорівнює нулеві.

Приклад 15. Двійкові системи ЧМ (рис. 1.28, г), в яких надсилання можуть передаватися водночас, але їхні частоти ω_1 та ω_2 підпорядковуються співвідношенням

Насправді, вважаючи у формулі зворотного перетворення Фур'є для спрощення $\varphi = 0$, з (1.47) дістанемо

$$\frac{\omega_1 + \omega_2}{2\pi} t_0 = n_1; \quad \frac{\omega_1 - \omega_2}{2\pi} t_0 = n_2,$$

де n_1 та n_2 – цілі числа.

$$\begin{aligned} \frac{U_{\text{с макс}}^2}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} \cos \omega_1 t \cos \omega_2 t dt &= \frac{U_{\text{с макс}}}{2t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} [\cos(\omega_1 + \omega_2)t + \cos(\omega_1 - \omega_2)t] dt = \\ &= \frac{U_{\text{с макс}}^2}{2t_0} \left[\frac{\sin(\omega_1 + \omega_2)t_0}{\omega_1 + \omega_2} + \frac{\sin(\omega_1 - \omega_2)t_0}{\omega_1 - \omega_2} \right] = \\ &= \frac{U_{\text{с макс}}^2}{2t_0} \left[\frac{\sin 2\pi n_1}{\omega_1 + \omega_2} + \frac{\sin 2\pi n_2}{\omega_1 - \omega_2} \right] = 0. \end{aligned}$$

1. Двійкові системи зв'язку ФТ (рис.1.28, д), в яких фази надсилань φ_1 та φ_2 підпорядковуються співвідношенням

$$\varphi_2 = \varphi_1 + \pi \text{ та } t_0 = \frac{2\pi}{\omega} n,$$

де n – ціле число. Обчислюючи інтеграл (1.47), з урахуванням (1.41) дістанемо

$$\begin{aligned} \frac{U_{\text{с макс}}^2}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} \cos(\omega t + \varphi_1) \cos(\omega t + \varphi_2) dt &= \\ &= \frac{U_{\text{с макс}}}{2t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} [\cos(2\omega t + \varphi_1 + \varphi_2) + \cos(\varphi_1 - \varphi_2)] dt = 0. \end{aligned}$$

Сигнали $u_{cr}(t)$ та $u_{cj}(t)$, які задовольняють умові ортогональності, в разі заміни однієї з реалізацій на спряжену називаються *ортогональними в посиленому розумінні* (ортогональними за Гільбертом):

$$\frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_{cr}(t) u_{cl}^*(t) dt = 0.$$

За Л.М. Фінком, такі сигнали мають найбільшу завадостійкість в каналах з флюктуючими параметрами і в приймальному пристрої має використовуватися властивість їхньої ортогональності в посиленому розумінні.

Зауважимо, що достатньою для ортогональності в посиленому розумінні реалізацій сигналів $u_{cr}(t)$ та $u_{cl}(t)$ є умова неперекриваності їхніх рядів Фур'є, за якої коефіцієнти розкладання $a_{rk} \neq 0$, $b_{rk} \neq 0$, $a_{lk} = b_{lk} = 0$. Проте можуть існувати сигнали, для яких дотримується рівність (1.47), але не виконується остання рівність. Наприклад, ортогональні сигнали ЧМ та ФМ також є ортогональні в посиленому значенні, а спряжені сигнали $u_{cr}(t)$ та $u_{cr}^*(t)$ не задовольняють останній умові.

Розкладання сигналів та завад за ортонормованими функціями. Якщо множина координатних функцій $\{\psi_k(t)\}$ в канонічному розкладанні сигналу

$$u_{cr}(t) = \sum_{k=k_1}^{k_2} A_k \psi_k(t) \quad (1.48)$$

є ортогональна, то ряд (1.48) є ортогональним. Помноживши обидві частини виразу (1.48) на $\psi_l(t)$ й проінтегрувавши на інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$, дістанемо

$$A_l = \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_{cr}(t) \psi_l(t) dt = \sum_{k=0}^N A_k \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} \psi_k(t) \psi_l(t) dt$$

отже всі члени суми, за винятком l -го, дорівнюють нулеві внаслідок ортогональності множини $\{\psi_k(t)\}$, а l -й член дорівнює A_l внаслідок його нормованості.

Одержаний вираз є формули Фур'є, вагові коефіцієнти A_l – коефіцієнти розкладання Фур'є $u_{cr}(t)$ за системою координатних функцій $\{\psi_k(t)\}$, а ряд (1.48) – ряд Фур'є.

Для математичного опису сигналів та завад стає зручним розкладання їх за *ортонормованими* (одичними ортогональними) координатними функціями,

$$\psi_{2k-1}(t) = \sqrt{2} \sin k\omega_c t; \quad \psi_{2k}(t) = \sqrt{2} \cos k\omega_c t,$$

які мають властивості

$$\psi_0(t) = 1; \quad \frac{1}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} \psi_k^2(t) dt = 1; \quad \frac{1}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} \psi_k(t) \psi_l(t) dt = 0 \text{ за } k \neq l.$$

При цьому коефіцієнти розкладання є

$$\left. \begin{aligned} A_0(t) &= \frac{1}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} u_c(t) dt = 1; \\ A_{2k-1}(t) &= \frac{\sqrt{2}}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} u_c(t) \sin k\omega_c t dt = 1; \\ A_{2k}(t) &= \frac{\sqrt{2}}{t_0} \int_{\frac{t_0}{2}}^{\frac{t_0}{2}} u_c(t) \cos k\omega_c t dt = 1. \end{aligned} \right\}$$

Реалізація флукуаційної завади на інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$ також може бути подана рядом (1.48), де коефіцієнти розкладання $\{A_k\}$ набирають випадкових значень. Поклавши $A_k = c_0 \theta_k$, перепишемо вираз (1.48) для завади у вигляді

$$u_{\text{ш}}(t) = c_0 \sum_{k=k_1}^{k_2} \theta_k \psi_k(t),$$

де c_0 – сталий множник; θ_k – вагові коефіцієнти, розподілені за нормальним законом з параметрами $E[\theta_k] = 0$ та $D[\theta_k] = 1$.

Визначимо c_0 з умови, що питома потужність шумів дорівнює заданій величині $v_{\text{ш}}^2$. Середня потужність реалізації у смузі F_c становить

$$P_{\text{ш}} = c_0^2 \sum_{k=k_1}^{k_2} \theta_k^2.$$

Математичне сподівання

$$E[P_{\text{ш}}] = c_0^2 \sum_{k=k_1}^{k_2} E[\theta_k^2] = 2F_c t_0 c_0^2.$$

Насправді, математичне сподівання $E[\theta_k^2] = 1$, а смуга пропускання F_c практично завжди є обмежена і становить

$$F_c = \frac{k_2 - (k_1 - 1)}{t_0}$$

де k_2, k_1 – цілі числа. Тому в розкладанні $u_{ш}(t)$ можна обмежитися скінченною кількістю членів, відповідною до частот, розташованих у межах смуги F_c . Кількість таких частот дорівнює $k_2 - (k_1 - 1)$, причому кожній з них відповідають два члени розкладання вигляду $A_{2k-1}\Psi_{2k-1}(t)$ та $A_{2k}\Psi_{2k}(t)$, які містять відповідно синусоїдні компоненти з непарними індексами та косинусоїдні компоненти з парними індексами. Отже, загальна кількість членів розкладання є $2[k_2 - (k_1 - 1)] = 2F_c t_0$.

Питома потужність шумів

$$v_{ш}^2 = \frac{E[P_{ш}]}{F_c} = c_0^2 2t_0. \quad (1.49)$$

звідки множник $c_0 = \sqrt{\frac{v_{ш}^2}{2T_c}}$.

Наведенні вище канонічні розкладання використовуються в теорії потенційної завадостійкості.

1.1.5. Модель сигналу з обмеженим спектром

В основу розглядуваної моделі сигналів, запропонованої В.А. Котельниковим покладено такі припущення:

- сигнал $u_c(t)$ являє собою стаціонарний випадковий процес;
- спектр сигналу є суцільний та обмежений певною частотою F_c , за межами якої він тотожно дорівнює нулеві.

Ця модель використовує добре розроблений математичний апарат стаціонарних випадкових процесів, дозволяє сформулювати низку принципово важливих положень і має фундаментальне значення в теорії ІЕС.

Теорема Котельникова в часовому поданні. Для сигналів з обмеженим спектром В.А. Котельниковим доведено таку теорему: реалізація випадкового процесу $u_{cr}(t)$, задана в інтервалі $(-\infty < t < \infty)$, яка має спектр, обмежений смугою частот $(0, F_c)$, визначається послідовністю дискретних значень у точках, рівновіддалених одна від одної на інтервал часу

$$\Delta t = \frac{1}{2F_c}. \quad (1.50)$$

При цьому сигнал може бути подано рядом

$$u_{cr}(t) = \sum_{k=-\infty}^{\infty} u_{cr}(k\Delta t) \frac{\sin[2\pi F_c(t - k\Delta t)]}{2\pi F_c(t - k\Delta t)}. \quad (1.51)$$

Вираз (1.51) є канонічне розкладання сигналу за координатними функціями

$$\Psi_k(t) = \frac{\sin[2\pi F_c(t - k\Delta t)]}{2\pi F_c(t - k\Delta t)}$$

з ваговими коефіцієнтами

$$A_k = u_{cr}(k\Delta t)$$

порівнюваними миттєвим значенням сигналу в моменті часу $k\Delta t = \frac{k}{2F_c}$.

Підкреслимо, що теорема Котельникова не накладає жодних обмежень щодо виду спектра функції $u_{cr}(t)$ у середині частотного інтервалу $(0, F_c)$.

Якщо позначити $\theta = t - k\Delta t$, тобто з'єднати початок координат з моментом відліку $k\Delta t$, то координатна функція

$$\psi_k(\theta) = \frac{\sin 2\pi F_c \theta}{2\pi F_c \theta}.$$

Ця функція, зображена на рис. 1.29, називається *функцією відліку* і являє собою реакцію ідеального фільтра нижніх частот зі смугою пропускання F_c і сталим коефіцієнтом передавання на одиничний імпульс. Тоді реалізацію $u_{cr}(t)$, описувану виразом (1.51), можна розглядати як реакцію

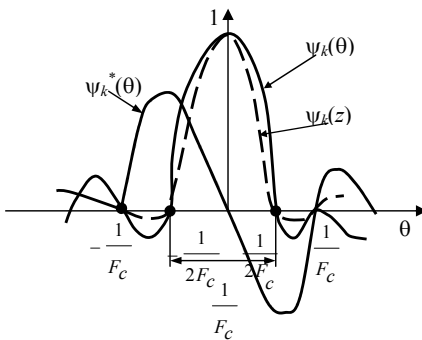


Рисунок 1.29 – Координатні функції

чень, які визначають сигнал на цьому проміжку, є

$$B_c = \frac{t_0}{\Delta t} = 2F_c t_0. \quad (1.52)$$

Отже, для відтворення функції з обмеженим спектром на інтервалі часу $(0, t_0)$ достатньо передати $2F_c t_0$ незалежних значень параметрів сигналу, однозначно пов'язаних з його формою. Такими параметрами можуть бути амплітуда, частота чи фаза спектральних складових. Тому величину B_c названо *базою сигналу*, або *кількістю ступенів мірності сигналу*.

База сигналу відіграє важливу роль в теорії зв'язку. Зокрема, збільшення B_c в низці випадків підвищує завадостійкість каналів, надає сигналам енергетичної утаємниченості тощо.

такого фільтра на послідовність коротких імпульсів тривалістю $t_0 \ll \Delta t$, узятих з ваговими коефіцієнтами A_k , які слідуєть один за одним через проміжки часу $\Delta t = \frac{1}{2F_c}$. Згідно з формулою

(1.51), напруга на виході фільтра є сумою напруг-реакцій $u_{cr}(k\Delta t) \psi_k(\theta)$. Це ілюстровано рис. 1.30.

Якщо тривалість сигналу є t_0 , то кількість дискретних значень,

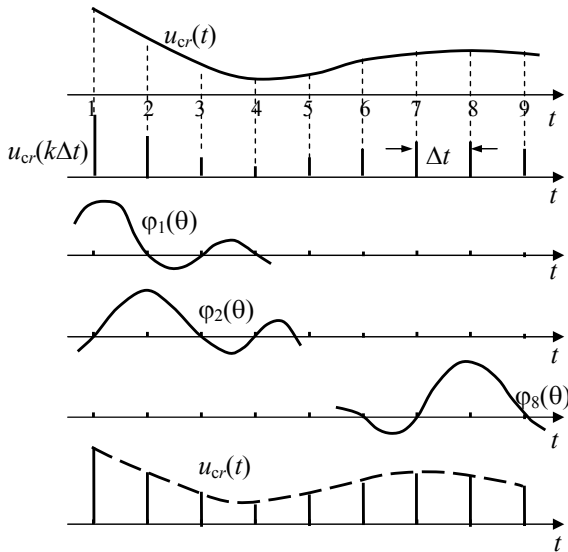


Рисунок 1.30 – Геометрична модель теореми Котельникова

Підкреслимо, що випадковість, яка лежить в основі інформаційних процесів, виявляється в значеннях $u_{cr}(k\Delta t)$. Для отримувача інформації функція $u_{cr}(t)$ є лише одна із можливих реалізацій сигналу, задана власною апіорною ймовірністю.

Отже, в цій моделі сигнали розглядаються як елементи множини детермінованих функцій часу з обмеженим спектром; для подання реалізацій сигналів використовується ряд (1.51). Випадкова для отримувача поява символів алфавіту джерела й відповідних до них реалізацій сигналів утворює в сукупності стаціонарний процес.

Теорема Котельникова в частотному поданні. Вираз (1.51) описує розкладання сигналів у часовій області. Аналогічна теорема є слухна стосовно спектра сигналів: якщо функцію $u_{cr}(t)$ розміщено в інтервалі (t_1, t_2) , то її комплексна спектральна густина визначається послідовністю дискретних значень, рівновіддалених одне від одного на інтервал $\frac{1}{t_2 - t_1}$ Гц.

Зокрема, якщо інтервал $(t_1, t_2) = \left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$, то

$$S_{cr}(if) = \sum_{k=-\infty}^{\infty} S_{cr}\left(k \frac{2\pi}{T_c}\right) \frac{\sin\left(\frac{\omega t_0}{2} - k\pi\right)}{\frac{\omega t_0}{2} - k\pi}. \quad (1.53)$$

Розглянемо взаємозв'язок між теоремою Котельникова в частотному поданні й звичайним рядом Фур'є. Функція $u_c(t)$, задана на інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$, може бути подана на цьому інтервалі інтегралом Фур'є. Якщо $u_c(t)$ має комплексну спектральну густину $S_c(f)$, то її можна розкласти в ряд Фур'є

$$\begin{aligned} u_c(t) &= \sum_{k=-\infty}^{\infty} c_k e^{-ik\omega_c t} = \sum_{k=-\infty}^{\infty} \frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} u_c(t) e^{-ik\omega_c t} dt = \\ &= \sum_{k=-\infty}^{\infty} \frac{1}{t_0} S_c(ik\omega_c) e^{ik\omega_c t}, \end{aligned} \quad (1.54)$$

де $\omega_c = \frac{2\pi}{t_0}$. Цей ряд, як зазначалося раніше, визначає $u_c(t)$ лише в інтервалі $\left(-\frac{t_0}{2}, \frac{t_0}{2}\right)$, а приведений інтеграл, є слушним для кожних значень t . Вироз (1.52) свідчить, що розкладання функції $u_c(t)$ в ряд Фур'є визначає її через значення спектральної густини в точках відліку, рівновіддалених на осі частот на $\frac{1}{t_0}$.

Теорема Котельникова в часовому поданні для радіосигналів. Розглянемо модульований високочастотний сигнал $u_c(t)$, спектр якого є обмежений смугою частот $F_c = F_2 - F_1$.

Використовуючи подавання реального сигналу через аналітичний сигнал, маємо

$$u_c(t) = \frac{1}{\pi} \int_{\Omega_1}^{\Omega_2} S_c(i\omega_c) e^{i\omega_c t} d\omega_c = \frac{1}{\pi} \int_{\Omega_1}^{\Omega_2} a(\omega_c) \cos \omega_c t d\omega_c + \frac{1}{\pi} \int_{\Omega_1}^{\Omega_2} b(\omega_c) \sin \omega_c t d\omega_c \quad (1.55)$$

та спряжений до нього сигнал

$$u_c^*(t) = \frac{1}{\pi} \int_{\Omega_1}^{\Omega_2} b(\omega_c) \cos \omega_c t d\omega_c - \frac{1}{\pi} \int_{\Omega_1}^{\Omega_2} a(\omega_c) \sin \omega_c t d\omega_c.$$

За С. Гольдманом, вираз (1.55) являє собою перетворення Гільберта.

Знайдемо перетворення Гільберта координатної функції, подавши її у вигляді

$$\Psi_k(\theta) = \frac{\sin \Omega_c \theta}{\Omega_c \theta},$$

де $\Omega_c = 2\pi F_c$. Тоді коефіцієнт

$$a(\omega_c) = \int_{-\infty}^{\infty} \psi_k(\theta) \cos \omega_c \theta d\theta = \frac{1}{2} \int_{-\infty}^{\infty} \frac{\sin(\omega_c + \Omega_c)\theta}{\Omega_c \theta} d\theta - \frac{1}{2} \int_{-\infty}^{\infty} \frac{\sin(\omega_c - \Omega_c)\theta}{\Omega_c \theta} d\theta = \frac{1}{2} (I_1 + I_2).$$

Інтегралі

$$I_1 = \begin{cases} \frac{\pi}{\Omega_c} & \text{за } \omega_c > -\Omega_c; \\ -\frac{\pi}{\Omega_c} & \text{за } \omega_c < -\Omega_c; \end{cases}$$

$$I_2 = \begin{cases} \frac{\pi}{\Omega_c} & \text{за } \omega_c > \Omega_c; \\ -\frac{\pi}{\Omega_c} & \text{за } \omega_c < \Omega_c. \end{cases}$$

Отже, коефіцієнт

$$a(\omega_c) = \begin{cases} \frac{\pi}{\Omega_c} & \text{за } -\Omega_c < \omega_c < \Omega_c; \\ 0 & \text{за інших } \omega_c. \end{cases}$$

Коефіцієнт

$$b(\omega_c) = 0,$$

якщо $\psi_k(0)$ – парна функція. Тоді спряжена координатна функція буде мати вид

$$\psi_k^*(0) = -\frac{1}{\pi} \int_0^{\Omega_c} \frac{\pi \sin \omega_c \theta d\theta}{\Omega_c} = -\frac{\sin^2 0,5\Omega_c \theta}{0,5\Omega_c \theta}.$$

Графік функції $\psi_k^*(0)$ подано на рис. 1.29.

Розклавши $S_c(i\omega_c)$ в ряд Фур'є, після перетворення для радіосигналу дістанемо

$$u_c(t) = \sum_{k=-\infty}^{\infty} u_c\left(\frac{k}{F_c}\right) \frac{\sin\left[\pi F_c\left(t - \frac{k}{F_c}\right)\right]}{\pi F_c\left(t - \frac{k}{F_c}\right)} \cos\left[\Omega_0\left(t - \frac{k}{F_c}\right) - \varphi\left(\frac{k}{F_c}\right)\right], \quad (1.56)$$

де $\Omega_0 = 2\pi\left(\frac{F_1 + F_2}{2}\right)$ – середня кругова частота спектра сигналу;

$u_c\left(\frac{k}{F_c}\right) = A_k$ – ваговий коефіцієнт, який визначає миттєве значення амплі-

туди (обвідної) радіосигналу в k -й точці відліку; $\varphi\left(\frac{k}{F_c}\right)$ – миттєве значення фази радіосигналу в k -й точці відліку.

Для визначення числових значень A_k та $\varphi\left(\frac{k}{F_c}\right)$ обвідну $U_c(t)$ й фазу $\varphi(t)$ радіосигналу доцільно подати у вигляді неперервних функцій часу (рис. 1.31, а, б).

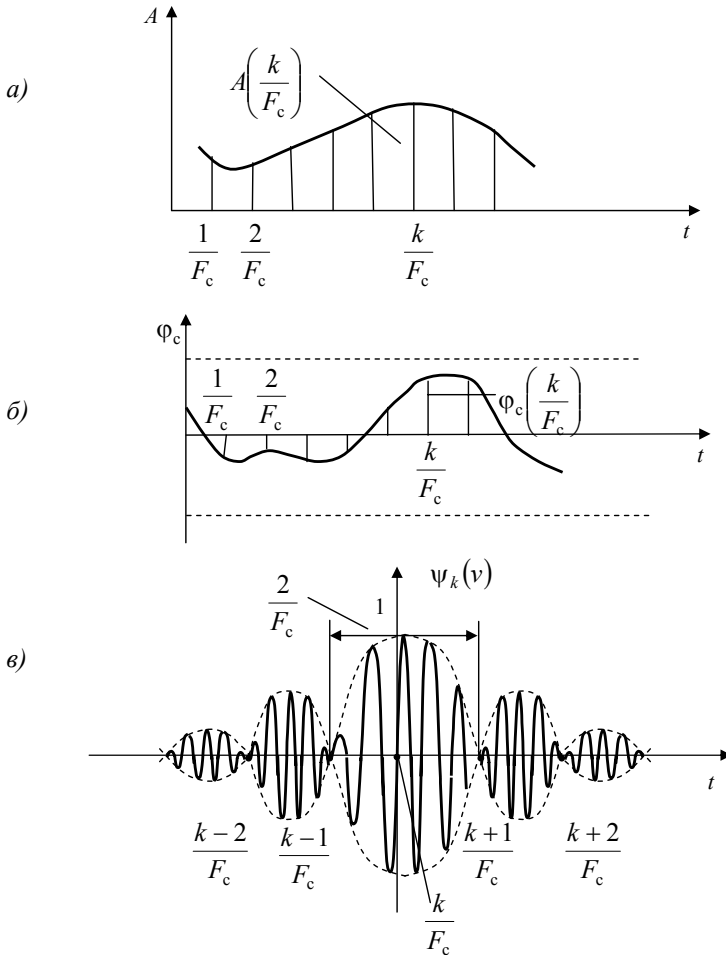


Рисунок 1.31 – Розкладання радіосигналу в ряд Котельникова: а – обвідна сигналу; б – фаза сигналу; в – координатна функція

На рис. 1.31, v подано координатну функцію $\psi_k(v)$ канонічного розкладання (1.56), де $v = t - \frac{k}{F_c}$. Обвідна функції $\psi_k(v)$ визначається множителем $\frac{\sin 2\pi F_c v}{2\pi F_c v}$, аналогічним до координатної функції $\psi_k(0)$ низькочастотного сигналу з тією лише різницею, що точки відстані перебувають на віддалі на осі часу вдвічі далше. Множник $\cos \left[\Omega_0 \theta - \varphi \left(\frac{k}{F_c} \right) \right]$ описує високочастотну структуру $\psi_k(v)$, визначається середньою частотою спектра сигналу Ω_0 та його фазою і є зсунений за часом у точку відліку.

Отже, радіосигнал $u_c(t)$ можна розглядати як наслідок суперпозиції сукупності модульованих координатних функцій, кожна з яких має частоту Ω_0 і належить до відповідної точки відліку. Вагові коефіцієнти A_k й фази $\varphi \left(\frac{k}{F_c} \right)$ описують в k -х точках значення $u_c \left(\frac{k}{F_c} \right)$ та $u_c^* \left(\frac{k}{F_c} \right)$, які, своєю чергою, визначають сигнал $u_c(t)$.

1.1.6. Питання та задачі для самоперевірки

1. Яка зі структурних мір інформації адекватна передачі різними комбінаціями електричних сигналів?
2. Яка міра інформації відповідає ентропійному підходу визначення кількості переданої інформації?
3. В яких випадках інформація вимірюється в бітах, нітах, дітах?
4. Що характеризує середня взаємна ентропія складної системи?
5. Що характеризує відносна та абсолютна надлишковість? Яка похибка буде для прикладу 1, якщо всю шкалу поділити на 25 квантів?
6. Розрахуйте значення D_B для прикладу 2, коли точки t_2 і t_3 об'єднуються в одну.
7. Яким параметром характеризується об'єднаний ансамбль складної фізичної системи?
8. Які недоліки сучасної теорії інформації, що базується на статистичних характеристиках подій?
9. Які джерела називаються ергодичними? В якому випадку ергодична послідовність є типовою?
10. Розрахуйте значення ентропії для прикладу 6, коли залежність між x_4 і x_3 буде відсутня.
11. Для прикладу 7 введіть вісім рівно ймовірних символів та розрахуйте ентропію $H(x)$.

12. Розрахуйте ентропію для прикладу 8 для випадку, коли після символу x_3 завжди передається символ x_4 .
13. Якому розподілу ймовірностей окремих повідомлень відповідає значення H_{\max} у виразі (1.24)?
14. Який параметр характеризується швидкістю створення інформації джерелом?
15. Запишіть числа 0; 1; 2; 3; 4; 5; 6; 7; 8; 9 у системах числення $m_c = 2; 3; 5; 10$.
16. Побудуйте код при $m_c = 3$, якщо передається 27 команд з рівними ймовірностями.
17. Проведіть аналіз методів виділення окремих кодових слів при нерівномірних їхніх довжинах.
18. Для прикладу 10 визначте надлишковість рівномірного коду мінімальної елементності.
19. Дайте визначення метричному простору. Що таке метрика векторного простору? Наведіть приклади метрик різних просторів сигналів.
20. Яка метрика відповідає координатному гільбертовому простору?
21. Що характеризують пряме та зворотне перетворення Фур'є?
22. Проведіть аналіз окремих властивостей спектрів.
23. Дайте визначення імпульсної реакції лінійної системи. Від чого залежить відстань між моментами перетину нульового рівня (рис. 1.21)?
24. Опишіть фізичну природу впливу нелінійності ФЧХ на спотворення сигналу.
25. Опишіть послідовність перетворення сигналу в канонічне представлення з координатними функціями $\frac{\sin x}{x}$.
26. Дайте визначення ортогональності сигналів. Чому сигнали на рис. 1.28, а не задовольняють ортогональності?
27. Чим забезпечується ортогональність сигналів двійкової системи з ЧМ, коли $n_1 = \frac{\omega_1 + \omega_2}{2\pi} t_0$, $n_2 = \frac{\omega_1 - \omega_2}{2\pi} t_0$ (приклад 15)?
28. Що називається функцією відліку?
29. Чим визначається кількість ступенів мірності сигналу?
30. Поясніть відмінність між спотвореннями дискретних сигналів і одержаних при реєстрації помилок.
31. Поясніть вплив коефіцієнта групування помилок на величину надлишковості коду, забезпечуючого задану якість прийому.

Глава 1.2. Інформаційні характеристики каналу зв'язку

1.2.1. Модель каналів зв'язку з обмеженою смугою пропускання

Стационарній моделі сигналу з обмеженим спектром відповідає модель каналу зв'язку у вигляді ідеального лінійного фільтра нижніх частот з амплітудною характеристикою

$$K(f) = \begin{cases} K_0 & \text{за } f \leq F_c; \\ 0 & \text{за } f > F_c. \end{cases} \quad (1.57)$$

Лінійна система може відігравати роль каналу зв'язку, якщо вона не вносить детермінізму у випадковий процес $u_c(t)$, поданий на її вхід. Для виконання цієї вимоги потрібне дотримання певних умов. Нехай на вході каналу з коефіцієнтом передавання за потужністю $K_p(f)$ діє сигнал $u_c(t)$ з енергетичним спектром $G_{c1}(f)$. Тоді спектр цього сигналу на виході каналу буде

$$G_{c2}(f) = K_p(f)G_{c1}(f).$$

Використовуючи умову недетермінованості випадкового процесу, на вході каналу дістанемо

$$\int_{-\infty}^{\infty} \frac{|\lg K_p(f)|}{1+f^2} df < \infty. \quad (1.58)$$

Цей вираз являє собою *критерій фізичної реалізації лінійного фільтра*. Отже, умова реалізації лінійної системи як інформаційного каналу зводиться до виконання умови її фізичної здійсненності.

Якщо канал є лінійний, то

$$K_p(f) = |K(f)|^2,$$

де $K(f)$ – амплітудна характеристика каналу (коефіцієнт передавання за напругою), тоді критерій фізичної здійсненності буде

$$\int_{-\infty}^{\infty} \frac{|\lg |K_p(f)||}{1+f^2} df < \infty. \quad (1.59)$$

Критерій фізичної здійсненності означає дотримання принципу причинності: реакція реального електричного кола на сигнал не може виникнути раніше за момент подання цього сигналу на її вхід. Якщо, наприклад, амплітудна характеристика кола має вигляд прямокутної чи гауссівської кривої

$$K(f) = e^{-f^2},$$

то реакція кола на сигнал у вигляді одиничної функції буде

$$h(t) = \frac{1}{2\sqrt{\pi}} \int_{-\infty}^t e^{-\frac{t}{4}} dt; \quad h(t) = \frac{1}{\pi} \int_{-\infty}^t \frac{\sin z}{z} dz.$$

Ці функції подано на рис. 1.32, *a*, *б*, з якого випливає, що реакція кола спостерігається за $t < 0$. Причина цього полягає в помилковому припущенні, що фільтри такого типу є фізично здійсненні, тому що для них інтеграл (1.59) розходиться. Реальні фільтри можуть мати скільки завгодно велике загасання лише на скінченному інтервалі частот; при цьому швидкість загасання не повинна перевищувати e^{-f^2} .

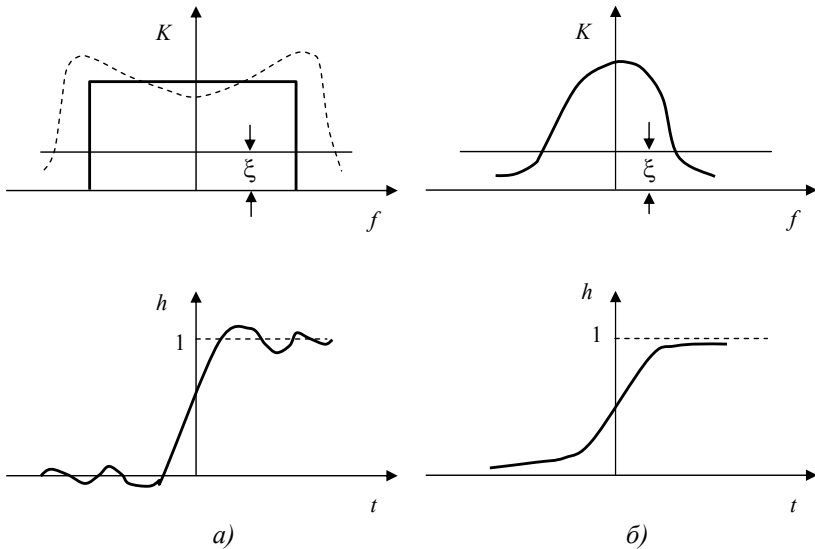


Рисунок 1.32 – Фізично нереалізовані лінійні фільтри:
a – ідеальний прямокутний; *б* – дзвоноподібний

Отже, електричне коло у вигляді ідеального фільтра нижніх частот не може використовуватися як інформаційний канал, тому що він руйнує сигнал, роблячи випадковий процес на виході каналу детермінованим. Крім того, таке коло не може бути фізично реалізовано й на практиці використовуються фільтри з характеристикою, поданою на рис. 1.32, *a* штриховою лінією. Однак при цьому виникає питання: на якому рівні ξ здійснювати обмеження частоти F_c або, інакше кажучи, що слід розуміти під смугою частот сигналу й смугою пропускання каналу зв'язку. Звичайно користуються суб'єктивною оцінкою, відраховуючи смугу залежно від призначення системи на рівні 0,1 чи 0,5, чи 0,7, вважаючи, що за межами смуги частот енергія сигналу є мала й нею можна знехтувати. Проте при цьому можуть інколи виникати небажані для практики складнощі. Нехай, наприклад, амплітудна характеристика каналу зв'язку має вигляд

$$K(f) = K_0 \frac{\sin z}{z},$$

де $z = \frac{\pi f}{2F_0}$. Якщо знехтувати значеннями $K(f) \leq 0,05 \leq K_0$, то смуга пропускання каналу буде $\Delta f_1 \approx 26F_0$; якщо ж пред'явити більш тверді вимоги й задати рівень відліку $K(f) \leq 0,01K_0$, то дістанемо $\Delta f_2 \approx 130F_0$. Це надає оцінюванню смуг пропускання каналу зв'язку якісний характер.

Як окремий випадок слід виділити модель електричних сигналів з обмеженим інтервалом кореляції.

Наведені вище суперечності, притаманні стаціонарній моделі сигналу з обмеженим спектром та моделі інформаційного каналу з обмеженою смугою пропускання, призвели до розроблення нової моделі сигналів. В основу цієї моделі сигналів покладено такі припущення:

- сигнал $u_c(t)$ являє собою недетермінований квазістаціонарний процес;
- тривалість сигналу t_0 є скінченна;
- спектр сигналу є суцільний і відмінний від нуля на всій осі частот, за винятком, можливо, окремих точок;
- інтервал кореляції сигналу $\tau_c \ll t_0$;
- миттєва потужність сигналу є обмежена й не може змінюватися стрибком.

Перші три властивості зумовлено власне фізичною природою електричних сигналів. Інтервал кореляції визначає кількість некорельованих елементів сигналу

$$N_c = \frac{t_0}{\tau_c} \quad (1.60)$$

і характеризує його як переносія інформації. Очевидно, що найпотужніші можливості, з точки зору кількості переносимої інформації, мають сигнали, в яких N_c є максимальне. За приклад можуть слугувати сигнали з функцією автокореляції у вигляді рівнобедреного трикутника:

$$\Psi_{11}(\tau_c) = \begin{cases} \sigma_c^2 \left(1 - \frac{|t|}{\tau_c}\right) & \text{за } -\tau_c \leq t \leq \tau_c; \\ 0 & \text{за інших } t. \end{cases}$$

Припущення, що $\tau_c \ll t_0$ означає наявність у сигналу значимої кількості некорельованих елементів, що також відповідає реальним сигналам. Наприклад, для телефонних сигналів $\tau_c \approx 1 \dots 2$ мс, тому навіть для коротких сигналів $N_c \geq 10^3 \dots 10^4$ елементів. Виконання умови $\tau_c \ll t_0$ робить квазістаціонарні сигнали практично стаціонарними та ергодичними.

Тривалість реальних сигналів завжди є обмежена певним інтервалом $(0, t_0)$. Тому сигнал на виході каналу апроксимується відліком ряду Котельникова

$$u_c^{(N)}(t) = \sum_{k=1}^{2F_c t_0} u_c(k\Delta t) \frac{\sin 2\pi F_c(t - k\Delta t)}{2\pi F_c(t - k\Delta t)} = \sum_{k=1}^{2F_c t_0} A_k \Psi_k(t), \quad (1.61)$$

де $\Delta t = \frac{1}{2F_c}$; A_k – випадкові величини, пов’язані з сигналом, що передається; $\{\Psi_k(t)\}$ – множина невідповідних ортогональних функцій. При цьому виникають питання:

- який критерій безпомилковості відтворення сигналів доцільно обирати?
- чи існує певна «середня» вірність відтворення для ансамблю реалізації сигналів?
- яка є вірність відтворення квазістаціонарних сигналів рядом Котельникова?

За критерій вірності відтворення реалізації сигналу $u_{cr}(t)$ рядом Котельникова $u_c^N(t)$ доцільно обрати величину

$$\xi_r = \frac{1}{T_c} \int_{-\frac{T_c}{2}}^{\frac{T_c}{2}} [u_c^{(N)}(t) - u_{cr}(t)]^2 dt = \frac{1}{T_c} \int_{-\frac{T_c}{2}}^{\frac{T_c}{2}} \Delta_r^2(t) dt, \quad (1.62)$$

яка фактично визначає середньоквадратичну похибку відтворення, де $\Delta_r(t)$ – «сигнал помилки» для r -ї реалізації сигналу. Такий критерій має істотні переваги при розгляданні завдань теорії зв’язку. По-перше, за $\xi_r = 0$ сигнали $u_c(t)$ та $u_c^N(t)$ буде розпізнано оптимальним (у розумінні Котельникова) приймальним пристроєм як тотожні. По-друге, критерій $\xi_r = 0$ водночас слугує за міру загубленої в каналі інформації (в розумінні Шеннона).

З використання канонічного розкладання (1.61) кожній з реалізацій сигналу $u_{cr}(t)$ відповідає власна тотожність ξ_r . Наприклад, при доволі великій тривалості сигналів вірність кожної реалізації сигналу є скільки завгодно близька до значення

$$\xi_0 = \frac{1}{t_0} \int_{-\frac{t_0}{2}}^{\frac{t_0}{2}} E[\Delta_r^2(t)] dt. \quad (1.63)$$

У разі квазістаціонарних сигналів

$$\xi_0 = 1 - \frac{2}{\Delta t} \int_0^{\tau_c} \Psi_{11}(\tau_0) \frac{\sin \frac{\pi t}{\tau_c}}{\frac{\pi t}{\tau_c}} dt. \quad (1.64)$$

Отже, модель сигналів з обмеженим інтервалом кореляції в жодному разі не заперечує моделі сигналів з обмеженим спектром, про що свідчить узагальнення теореми Котельникова в новому формулюванні: квазістаціонарний сигнал з необмеженим спектром визначається послідовністю його миттєвих значень, які прямують одне за одним через інтервал $\Delta t = \frac{1}{2F_c}$, з точністю, скільки завгодно близькою до граничного значення ξ_0 , якщо $\Delta t \leq \tau_c$, а тривалість сигналу $t_0 \gg \tau_c$.

Ефективна смуга частот. Оскільки реальні сигнали мають нескінченно протяжний енергетичний спектр, то для оцінювання його ширини треба ввести величину, яка має кількісну визначеність. Нехай енергетичний спектр сигналу сягає максимального значення $G_{c\text{макс}}$ на частоті $f = f_0$. Побудуємо біля цієї точки прямокутник висотою $G_{c\text{макс}}$ з площею, порівнюваною площею, що обмежена кривою $G_c(f)$ та віссю частот (рис. 1.33). Основа прямокутника

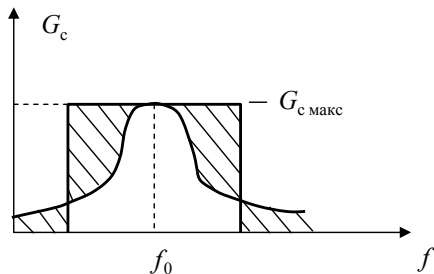


Рисунок 1.33 – До визначення ефективності смуги частот

$$F_{cc} = \frac{1}{G_{c\text{макс}}} \int_0^{\infty} G_c(f) df \quad (1.65)$$

чисельно характеризує *ефективну смугу частот сигналу* (ефективну ширину енергетичного спектра).

Функція автокореляції стаціонарного сигналу з обмеженим спектром перетворюється на нуль у точках $\tau_0 = k\tau_c$ ($k = 1, 2, \dots$), де

$$\tau_c = \frac{1}{2F_{cc}}. \quad (1.66)$$

Інтервал кореляції сягає мінімально можливого значення

$$\tau_{c\text{мін}} = \frac{1}{2F_{cc}}, \quad (1.67)$$

коли енергетичний спектр сигналу є рівномірний.

Для квазістаціонарних процесів мінімальна величина інтервалу кореляції

$$\tau_{c\text{мін}} = \frac{1}{2F_{cc}}$$

й не залежить від тонкої структури сигналу.

1.2.2. Пропускна здатність каналу

Припустимо, що нам відома деяка сукупність фіксованих обмежень, що накладаються на інформаційний канал. До фіксованих обмежень ми будемо відносити: параметри каналу зв'язку й, зокрема, тривалість переданих символів сигналу, використовуваний код, методи декодування сигналів і заборони, що накладаються у зв'язку з цим, і т.п.

Назвемо *пропускною здатністю* інформаційного каналу максимальне значення (точніше, верхню межу) швидкості передавання інформації при заданих фіксованих обмеженнях, тобто

$$C = \sup_{\substack{a_1 \in B_1 \\ \dots \\ a_i \in B_i \\ \dots}} \{ \bar{I}(W, X) \} \quad \text{дв.од/с} \quad (1.68)$$

У даній рівності позначення \sup вказує, що обчислюється верхня межа, а запис $a_i \in B_i$ говорить про те, що параметр a_i задовольняє заданому фіксованому обмеженню, тобто лежить у деякій області B_i .

Спосіб відшукування верхньої межі залежить від того, яка сукупність фіксованих обмежень задана.

Якщо інформаційний канал визначений повністю, то верхня межа повинна відшукуватися за статистичними характеристиками джерела повідомлень, тобто відшукуються розподіл ймовірностей повідомлень і корелятивні зв'язки між ними, за яких швидкість передавання інформації буде найбільшою.

Таким чином, *пропускна здатність є характеристика каналу* й не залежить від фактичної швидкості передачі інформації від даного джерела.

Якщо сукупність заданих фіксованих обмежень не повністю визначає канал, а є можливість зміни тих або інших параметрів, наприклад, тривалості символів, способу декодування та ін., то останні вибираються з умови одержання найбільшої швидкості передавання інформації. В усіх випадках відшукуються оптимальні статистичні характеристики джерела, за яких швидкість передавання інформації максимальна.

Аналогічно тому, як це було зроблено для інформаційного каналу, можна визначити пропускну здатність каналу зв'язку

$$C = \sup_{\substack{a_1 \in B_1 \\ \dots \\ a_i \in B_i \\ \dots}} \{ \bar{I}(Z, Y) \} \quad \text{дв.од/с}, \quad (1.69)$$

де

$$\bar{I}(Z, Y) = \lim_{T \rightarrow \infty} \frac{I(Z_T, Y_T)}{T}. \quad (1.70)$$

При цьому Z_T й Y_T – сигнали тривалістю T відповідно на виході й вході каналу зв'язку.

Канал зв'язку є частиною інформаційного каналу. Розглядаючи канал зв'язку окремо й визначаючи його пропускну здатність, ми можемо не накладати ніяких фіксованих обмежень на спосіб кодування, вид модуляції й структуру сигналів на його вході. Тим самим створюються можливості використання оптимальних сигналів, за яких швидкість передавання інформації буде гранично великою. Побудова реального інформаційного каналу неминує пов'язана із введенням тих або інших додаткових фіксованих обмежень, що призводить до недовикористання пропускну здатності каналу зв'язку. Таким чином, звичайно

$$C_c > C.$$

Якщо пропускну здатність каналу зв'язку визначати з урахуванням всіх фіксованих обмежень, що накладаються роботою кодуєчих і декодуєчих пристроїв, то ми одержимо⁶

$$C = C_c.$$

Це положення впливає з тієї обставини, що пристрої, які кодують та декодують, у найкращому разі можуть бути побудовані таким чином, щоб у них не відбувалася втрата інформації. При цьому вся інформація, що вилучається із сигналу на виході каналу зв'язку, буде передана до одержувача повідомлення. Очевидно, що зворотної нерівності ($C > C_c$) бути не може.

Якщо кількість обмежень, що фіксуються, досить велика так, що їхня сукупність повністю визначає реальний канал, то пропускну здатність часто називають *реальною*. Якщо ж фіксуються лише самі загальні показники, а саме: смуга частот переданого сигналу, середня або пікова потужність передавального пристрою, характер і рівень завад, то пропускну здатність іноді називають *ідеальною* або *граничною*.

За відсутності шумів у каналі можна вважати, що $z = y$, а $w = x$ й, отже, для повідомлень, переданих за час T , $Z_T = Y_T$ і $W_T = X_T$. З огляду на властивості кількісної міри інформації, вивчені раніше, одержимо

$$I(W_T, X_T) = I(X_T, X_T) = H(X_T)$$

та

$$I(Z_T, Y_T) = I(Y_T, Y_T) = H(Y_T).$$

У такому разі з огляду на (1.69) одержимо

$$C = \sup \left\{ \lim_{T \rightarrow \infty} \frac{H(X_T)}{T} \right\}, \quad (1.71)$$

а з (1.69) і (1.70)

$$C_c = \sup \left\{ \lim_{T \rightarrow \infty} \frac{H(Y_T)}{T} \right\}. \quad (1.72)$$

⁶ У цьому випадку, визначаючи, наприклад $I(Z_T, Y_T)$, ми враховуємо, яким способом сигнал Z_T буде реально декодуватись.

⁷ У подальшому ми будемо опускати вказівку про те, що верхню межу шукають при заданих фіксованих обмеженнях.

Позначимо через $N(T)$ кількість усіх можливих послідовностей повідомлень тривалістю T . Із властивостей ентропії, розглянутих раніше, випливає, що $H(X_T)$ буде максимальна, якщо будь-які послідовності повідомлень рівноймовірні. Це максимальне значення може бути визначене й дорівнює $\log N(T)$. З (1.71) тоді треба, що для заданого інформаційного каналу

$$C = \lim_{T \rightarrow \infty} \frac{\log N(T)}{T}. \quad (1.73)$$

Розглядаючи один лише канал зв'язку, аналогічно одержимо

$$C_c = \lim_{T \rightarrow \infty} \frac{\log N_c(T)}{T}, \quad (1.74)$$

де $N_c(T)$ – число всіх можливих послідовностей кодованих сигналів тривалістю T .

Співвідношення (1.73) і (1.74) звичайно використовують як визначення пропускної здатності дискретного каналу без шумів.

Обчислення пропускної здатності дискретних каналів. Знайдемо пропускну здатність деяких дискретних каналів.

Приклад 1. Канал А. Для передавання повідомлень використовується код з основою a (тобто з a різними символами), тривалість усіх символів коду однакова й дорівнює t_0 . Інші фіксовані обмеження відсутні.

Для обчислення C_c розглянемо послідовність із M символів, тривалість такої послідовності дорівнює $T = Mt_0$. При $T \rightarrow \infty$ число символів в одній послідовності $M \rightarrow \infty$. Очевидно, що всього можна утворити a^M послідовностей довжиною в M символів, отже, $N_c(Mt_0) = a^M$ і з (1.74) одержимо

$$C_c = \lim_{M \rightarrow \infty} \frac{\log a^M}{Mt_0}$$

або

$$C_c = \frac{1}{t_0} \log a. \quad (1.75)$$

Потрібно відзначити, що якщо розглядати вихід кодуєчого пристрою, як джерело повідомлень $\log a$, тобто ентропія цього джерела, тобто $\log a = H(Y)$, в якого корелятивні зв'язки між символами відсутні й ймовірності передавання різних символів однакові. Звідси випливає важливе зворотне твердження: для того щоб у розглянутому каналі швидкість передавання була максимальною, необхідно, щоб ймовірності передавання різних символів були однаковими.

При використанні двійкового коду $a = 2$ з (1.75) одержуємо, що

$$C_c = \frac{1}{t_0} \text{ дв.од/с}, \quad t_0 = \frac{1}{B}, \quad (1.76)$$

де B – швидкість передавання, що виражається в бодах.

Приклад 2. Канал Б. Символи коду (або окремі повідомлення) мають однакову тривалість, яка дорівнює t_0 . На припустиму послідовність символів накладаються деякі фіксовані заборони.

При обчисленні C_c будемо розглядати кодуючий пристрій, як джерело інформації.

Розглянемо сигнал Y_T тривалістю $T_c = nt_0$. Ентропія цього сигналу

$$H(Y_T) = nH(Y),$$

де $H(Y)$ – ентропія джерела, що обчислюється з урахуванням накладених фіксованих заборон.

Очевидно, що швидкість передавання інформації в такому каналі

$$\bar{I} = \frac{H(Y_T)}{T_c} = \frac{H(Y)}{t_0}, \quad (1.77a)$$

а пропускна здатність

$$C_c = \frac{H(Y)_{\max}}{t_0}, \quad (1.77б)$$

де $H(Y)_{\max}$ – максимально можливе значення ентропії кодованого сигналу з урахуванням викладених заборон.

Приклад 3. Симетричний небінарний канал. Нехай по симетричному каналу передаються m -позиційні символи з імовірністю помилкового прийому p_e . Тому що величина p_e не залежить від того, який символ передавався, то імовірність зареєструвати символ u_{cl} , якщо передавався символ u_{ck} , буде

$$p(u_{cl}/u_{ck}) = \begin{cases} 1 - p_e & \text{за } l = k; \\ \frac{p_e}{m-1} & \text{за } l \neq k. \end{cases}$$

Пропускна здатність каналу описується формулою

$$C = B[H(U_c) - H(U_c/U_p)]_{\max} = B[H(U_p) - H(U_p/U_c)]_{\max} \quad (1.78)$$

Умовна ентропія

$$\begin{aligned} H(U_p/U_c) &= -\sum_{k=1}^m \sum_{j=1}^m p(u_{pj}; u_{ck}) \log_2 p(u_{pj}/u_{ck}) = \\ &= -\sum_{k=1}^m \sum_{j=1}^m p(u_{ck}) p(u_{pk}/u_{ck}) \log_2 p(u_{pk}/u_{ck}) - \\ &= -\sum_{k=1}^m \sum_{j=1(j \neq k)}^m p(u_{ck}) p(u_{pj}/u_{ck}) \log_2 p(u_{pj}/u_{ck}) = \\ &= -(1 - p_e) \log_2 (1 - p_e) - p_e \log_2 \frac{p_e}{m-1}, \end{aligned}$$

де $p(u_{ck})$ апіорна ймовірність символу u_{ck} . Тоді

$$C = B \left[H(U_p)_{\text{макс}} + (1 - p_e) \log_2(1 - p_e) + p_e \log_2 \frac{p_e}{m-1} \right].$$

Тому що $H(U_p)_{\text{макс}} = \log_2 m$, то остаточно

$$C = B \left[\log_2 m + (1 - p_e) \log_2(1 - p_e) + p_e \log_2 \frac{p_e}{m-1} \right]. \quad (1.79)$$

Приклад 4. Симетричний бінарний канал. Вважаючи в (1.79) $m = 2$, одержимо

$$C = B[1 + (1 - p_e) \log_2(1 - p_e) + p_e \log_2 p_e]. \quad (1.80)$$

Вираз (1.80) подано графічно на рис. 1.34 у вигляді функції

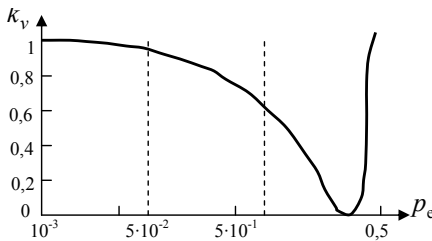


Рисунок 1.34 – Пропускна здатність бінарного симетричного каналу

$k_v = f(p_e)$, де $k_v = \frac{C}{B}$. За від-

сутності завад $k_v = 1$, тобто кожний символ переносить за одну секунду (1 с) одну двійкову одиницю (1 дв. од.) інформації. Якщо $p_e = 0,5$, то $k_v = 0$, оскільки прийнятий сигнал з однаковою ймовірністю може вважатися вірним або помилковим. При подальшому збільшенні p_e величина k_v зростає й при $p_e = 1$ знову $k_v = 1$. Це пояснюється тим, що формально при $p_e > 0,5$ інформацію із прийнятих сигналів можна витягати, виносячи щораз рішення u_{c1} при прийманні символу u_{p2} й рішення u_{c2} у випадку символу u_{p1} .

Формула (1.80) характеризує максимальну швидкість передавання інформації при заданій вірності зв'язку по симетричному каналу типу ЧМ або ФМ. Для несиметричних каналів, наприклад АМ, вона справедлива, якщо $p(U_{c1}) = p(U_{c2})$ й $p_{e1} = p_{e2}$.

Приклад 5. Несиметричний небінарний канал. Нехай канал заданий матрицею

$$M_k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 - p_e & p_e \\ 0 & p_e & 1 - p_e \end{pmatrix}. \quad (1.81)$$

Символ u_{c1} має апіорну ймовірність $p(u_{c1}) = p$ і передається без спотворювань, а символи u_{c2} й u_{c3} мають однакові апіорні ймовірності $p(u_{c2}) = p(u_{c3}) = q$ й при передаванні спотворюються симетрично. Подібну матрицю може мати, наприклад, трійковий канал ЧМ при селективних завмираннях або трійковий канал АМ при нерівномірному законі розподілу символів алфавіту.

Тому що ймовірності $p(u_{p1}) = p$, $p(u_{p2}) = p(u_{p3}) = q$, то ентропії

$$H(U_c) = -p \log_2 p - 2q \log_2 q;$$

$$H(U_c/U_p) = pH(U_c/u_{p1}) + qH(U_c/u_{p2}) + qH(U_c/u_{p3}).$$

Оскільки

$$H(U_c/u_{p1}) = 0;$$

$$H(U_c/u_{p2}) = H(U_c/u_{p3}) = -p_e \log_2 p_e - (1 - p_e) \log_2 (1 - p_e),$$

то, позначивши

$$\xi = -p_e \log_2 p_e - (1 - p_e) \log_2 (1 - p_e),$$

для кількості переданої по каналу інформації одержимо

$$I(U_c; U_p) = H(U_c) - H(U_c/U_p) = -p \log_2 p - 2q \log_2 q + 2q\xi.$$

Пропускна здатність каналу відповідає верхній межі $I(U_c; U_p)$ при додатковій умові $p + 2q = 1$. Для визначення її застосуємо метод Лагранжа.

Із цією метою утворимо допоміжну функцію

$$L = I(U_c; U_p) + \lambda(p + 2q)$$

і з рівнянь

$$\frac{dL}{dp} = 0; \quad \frac{dL}{dq} = 0,$$

знайдемо значення параметра λ , яке максимізує її. Відповідна система рівнянь має вигляд:

$$\frac{dL}{dp} = -\log_2 p + \lambda - \frac{1}{\ln 2} = 0;$$

$$\frac{dL}{dq} = -2 \log_2 q + 2\lambda + 2\xi - \frac{2}{\ln 2} = 0,$$

звідки після виключення параметра λ маємо

$$p = \frac{\alpha}{2 + \alpha}; \quad p = \frac{\alpha}{2 + \alpha},$$

де $\alpha = 2^{-\xi}$.

Тоді пропускна здатність каналу

$$C = B \left[\log_2 (2 + \alpha) 2^{\frac{2\xi}{2+\alpha}} \alpha^{-\frac{\alpha}{2+\alpha}} \right]. \quad (1.82)$$

Розглянемо два окремі випадки.

1. Завади в каналі відсутні. При цьому $p_e = 0$, $\xi = 0$, $\alpha = 1$, $p = q = 1/3$ і $C = B \log_2 3$ дв.од/с Цей результат збігається з величиною C , обчисленої за формулою (1.80) при $m = 3$ й $p_e = 0$, тому що канал став симетричним.

2. Завади викликають спотворення символів з ймовірністю $p_e = 0,5$. При цьому $\xi = 1$, $\alpha = 0,5$, $p = 0,5$, $q = 0,4$ і $C = B \log_2 5$ дв.од/с. Тепер канал став несиметричним, а символи u_{c2} й u_{c3} нерозрізнені.

1.2.3. Спотворення елементарних сигналів кодових конструкцій

Поняття про спотворення посилок. Кодові посилки надходять в канал зв'язку від передавача кінцевої апаратури з достатньо високим ступенем точності за тривалістю (похибка не перевищує 1–2% від тривалості елементарної посилки). При проходженні по каналу зв'язку на точність відтворення тривалості переданих елементарних сигналів (посилок) чинить вплив велике число чинників: загасання сигналу, обмеження його спектра, різні перетворення сигналу (модуляція, демодуляція тощо), вплив завад, і т.п. Через те, що з виходу каналу постійного струму дискретні сигнали надходять обмеженими за амплітудою, то всі ці впливи призводять до зміни (спотворення) тривалості прийманих посилок постійного струму по відношенню до переданих.

Розрізняють два види спотворень кодових посилок – спотворення довжини зміщення країв посилок та дроблення. Під *крайовими спотвореннями* розуміють зміщення в часі країв (границь) посилок, внаслідок якого прийняті посилки виявляються нерівними за тривалістю. *Дробленнями* називають спотворення, що полягають у зміні полярності прийманого сигналу в межах як однієї елементарної посилки, так і декількох посилок, що йдуть підряд.

На рис. 1.35 зображено послідовності переданих і прийнятих посилок, причому останні відтворюються на виході каналу постійного струму з певним запізненням, зумовленим часом розповсюдження електромагнітної енергії по каналу зв'язку, перехідними процесами в каналоутворювальній апаратурі та різного виду завадами. Якщо всі границі посилок відтворюються з однаковим запізненням (рис. 1.35, б), яке дорівнює величині деякого запізнення сигналів у даному каналі $t_{сеп}$ ($t_1 = t_2 = t_3 = t_4 = t_{сеп}$), тоді тривалість усіх прийнятих посилок дорівнює тривалості переданих (рис. 1.35, а), і крайові спотворення дорівнюють нулю. Якщо ж ця умова не виконується, то приймані посилки відтворюються зі спотворенням.

Величина відхилення запізнення даної границі посилок в той чи інший бік від значення $t_{сеп}$ називається індивідуальним крайовим спотворенням.

Розрізняють абсолютну величину спотворень посилок, яка виражається в одиницях часу, і відносну величину – у відсотках від тривалості елементарної послілки. Наприклад, початок першої послілки на рис. 1.35, *в* має абсолютну величину індивідуального крайового спотворення

$$\theta_1 = t_1' - t_{\text{сер}}, \text{ другого –}$$

$$\theta_2 = t_2' - t_{\text{сер}}, \text{ третього}$$

$$\theta_3 = t_3' - t_{\text{сер}} \text{ і четвертого}$$

$$\theta_4 = |t_4' - t_{\text{сер}}| \text{ (області по-}$$

силок, що відповідають спотворенням, заштриховано). Відносна величина індивідуальних спотворень дорівнює

$$\delta_i = \frac{\theta_i}{t_0} \cdot 100\% .$$

Як бачимо на рис.1.35, *в* відлік величини крайових спотворень виконується від значення $t_{\text{сер}}$. Це значення залежить від багатьох чинників і знаходження його величини інколи пов'язане з певними труднощами. Крім того, при вимірюваннях спотворень значної сукупності меж прийманих посилок часто інтерес становить не величина спотворень окремих посилок, а максимальна величина індивідуальних спотворень. Тому вводять поняття загальних спотворень.

При порівнянні великого числа границь сприйманих посилок з границями переданих посилок (рис. 1.36, *а*) можна виділити зону між максимальним зміщенням країв $t_{\text{макс}}$ і мінімальним зміщенням країв $t_{\text{мін}}$ (рис. 1.36, *б*). Ця зона відповідає абсолютній величині загальних крайових спотворень $\theta = t_{\text{макс}} - t_{\text{мін}}$.

Умовно вважаючи, що $t_{\text{сер}}$ розміщується посередині даної зони, можна визначити відносну величину загальних крайових спотворень δ_0 як половину величини зони, віднесеної до всієї тривалості елементарної послілки:

$$\delta_0 = \frac{\theta}{2} \cdot \frac{1}{t_0} 100\% = \frac{t_{\text{макс}} - t_{\text{мін}}}{2t_0} \cdot 100\% .$$

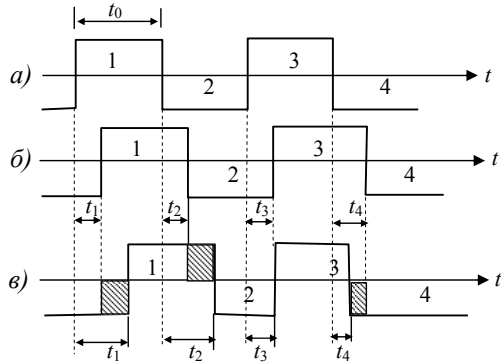


Рисунок 1.35 – Послідовності переданих і прийнятих посилок, які відтворюються на виході каналу постійного струму з певним запізненням

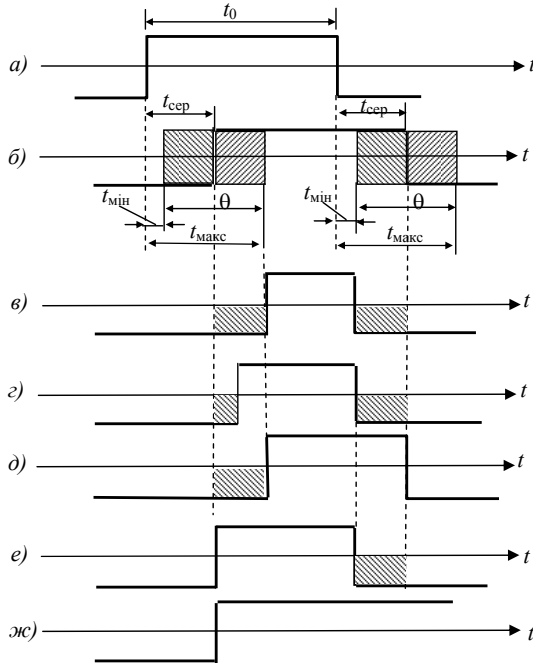


Рисунок 1.36 – Виділення ідеальних моментів відновлення сигналу

Отже відносна величина загальних спотворень не може бути більше 50%. Крім того, дане визначення припускає, що значення $t_{\text{макс}}$ і $t_{\text{мін}}$ можуть належати як одному й тому самому посиланню, так і різним посиланням.

Класифікація спотворень. Спотворення кодових посилок поділяють на дві групи. До першої групи відносять спотворення кодових посилок, які належать до детермінованих (регулярних) процесів. Такі спотворення називають *систематичними*. Систематичні спотворення викликаються, здебільшого, невідповідністю електричних характеристик каналу параметрам посилок, що передаються, і проявляється частіше за все в зміщенні країв посилок, що приймаються. У свою чергу систематичні спотворення поділяються на характеристичні крайові спотворення і крайові спотворення типу переважання. У зв'язку з регулярністю процесів, що викликають систематичні спотворення, величина їх може бути розрахована та занормована.

До другої групи відносяться спотворення, що належать до випадкових процесів і тому називаються *випадковими*. Випадкові спотворення залежать від випадкових чинників: різного роду завади, переривання рівнів сигналу тощо. В залежності від амплітуди завад і тривалості переривань у посиланнях, що приймаються, можуть з'являтися як випадкові крайові спотворення, так і дроблення.

Основним джерелом спотворення посилок є випадкові спотворення. Внаслідок випадковості процесів, що викликають ці спотворення, їхній розрахунок, вимірювання та нормування викликає певні труднощі.

Характеристичні спотворення довжини посилок. Характеристичні спотворення проявляються при передаванні каналами зв'язку послідовності посилок різної структури. Величина характеристичних спотворень у каналах зв'язку залежить від швидкості передавання, ширини смуги пропускання каналу, форми амплітудно-частотних і фазочастотних характеристик каналу та інших чинників. Якщо електричні характеристики каналу не відповідають вибраній швидкості телеграфування, тоді при передаванні посилок, що рівномірно чергуються, різної полярності типу 1:1 спотворення будуть відсутні, а при передаванні періодичних несиметричних послідовностей посилок типу 1:5, 1:6 і т.п. з'являться крайові спотворення, величина яких буде сталою.

З характеристичними спотвореннями доводиться рахуватися при передаванні посилок постійного струму по з'єднувальних лініях і кабельних жилах з великою зосередженою або розподіленою ємністю. Для цього випадку наведемо розрахунок характеристичних спотворень, припустивши, що передавання здійснюється двополярними послітками, а наростання і спадання струму в колі телеграфування відбувається за експоненціальним законом.

Принцип утворення характеристичних спотворень ілюструється на рис. 1.37. Суцільними лініями показані передані (рис. 1.37, а) і прийняті послітки (рис. 1.37, з) при передаванні комбінації 1:1, пунктирними лініями – комбінації 3:1 (рис. 1.37, б, д). Як впливає з рис. 1.37, в, при передаванні точок струм не встигає досягнути усталеного значення I_0 за час елементарної послітки t_0 , але завдяки однаковому характеру кривих наростання і спадання струму крайові спотворення відсутні (рис. 1.37, з). У той самий час приймання комбінації 3:1 відбулося зі спотвореннями: четверта послітка кодового слова скоротилася на початку на величину θ_1 , а в кінці θ_2 .

Для розрахунку величини спотворень визначимо закони спадання струму в обох розглянутих випадках. При усталеному режимі струм спадання i_2 (рис. 1.37, в, д) змінюється згідно з рівнянням

$$i_2 = 2I_0 e^{-\frac{t}{\tau}} - I_0 = I_0 (2e^{-\frac{t}{\tau}} - 1), \quad (1.83)$$

де τ – стала часу кола телеграфування.

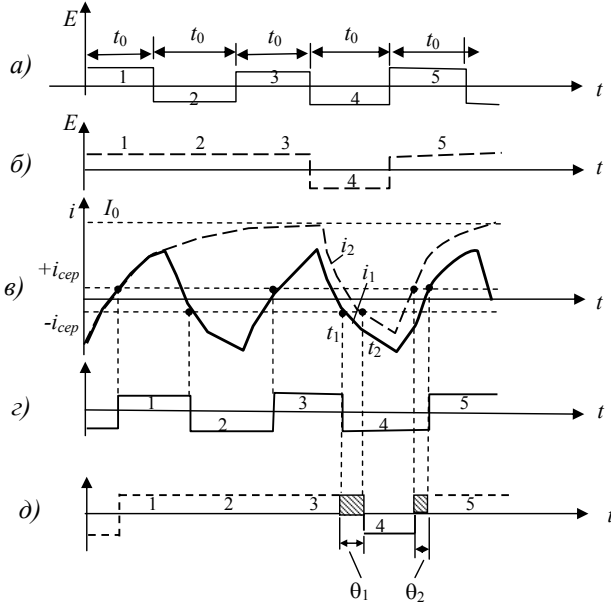


Рисунок 1.37 – Принцип утворення характеристичних спотворень

Для визначення характеру зміни струму i_1 використаємо метод суперпозиції. Припустимо, що в момент часу $t = -t_0$ (рис. 1.38, а) відбувається перемикання джерела живлення з напруги $-E$ на $+E$. У проміжок часу від $t = -t_0$ до $t = 0$ існує струм

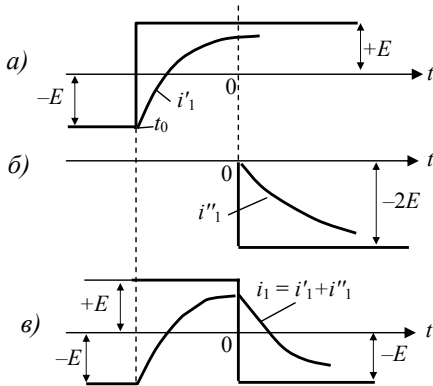


Рисунок 1.38 – Метод суперпозиції

$$i'_1 = I_0(1 - 2e^{-\frac{t+t_0}{\tau}}).$$

У момент часу $t = 0$ вмикається струм $2E$ (рис.1.38, б) і у колі з'являється додатковий струм

$$i''_1 = 2I_0(e^{-\frac{t}{\tau}} - 1).$$

Таким чином, починаючи з моменту $t = 0$ в колі буде існувати два струми, що зумовлені перемиканням джерел струму. Загальний струм i дорівнює сумі цих струмів (рис.1.38, в):

$$i_1 = i'_1 + i''_1 = I_0(2e^{-\frac{t}{\tau}} - 2e^{-\frac{t+t_0}{\tau}} - 1) \quad (1.84)$$

Величина параметрів спотворень дорівнює $\theta_1 = t_2 - t_1$. Підставивши час t_1 та t_2 у рівняння (1.83) і (1.84), одержимо:

$$-i_{\text{сеп}} = I_0(2e^{-\frac{t}{\tau}} - 1);$$

$$-i_{\text{сеп}} = I_0(2e^{-\frac{t_1}{\tau}} - 2e^{-\frac{t_1+t_0}{\tau}} - 1).$$

З цих рівнянь знайдемо

$$t_1 = \tau \ln \frac{2I_0(1 - e^{-\frac{t_0}{\tau}})}{I_0 - i_{\text{сеп}}}; \quad t_2 = \tau \ln \frac{2I_0}{I_0 - i_{\text{сеп}}}.$$

і остаточно

$$\theta_1 = t_2 - t_1 = \tau \ln \frac{1}{1 - e^{-\frac{t_0}{\tau}}}.$$

Відносна величина характеристичних спотворень дорівнює

$$\delta_r = \frac{\theta_1 + \theta_2}{2t_0} \cdot 100\% \quad (1.85)$$

Передбачивши, що $\theta_1 = \theta_2$, визначимо

$$\delta_r = \frac{\theta_1}{t_0} \cdot 100 = \frac{\tau}{t_0} \ln \frac{1}{1 - e^{-\frac{t_0}{\tau}}} \cdot 100\% \quad (1.86)$$

Із формули (1.86) виходить, що відносна величина характеристичних спотворень залежить лише від сталої часу кола τ та тривалості елементарної послілки t_0 і не залежить від інших параметрів (I_0 , $i_{\text{сеп}}$).

З метою зменшення величини характеристичних спотворень необхідно зменшувати сталу часу становлення сигналу або збільшити тривалість елементарних послілок (зменшити швидкість модуляції).

Крайові спотворення типу переваг. Порушення симетрії параметрів сигналу, що мають постійний характер, призводить до постійних переваг. При цьому послілки однієї полярності подовжуються або укорочуються на одну і ту саму величину по відношенню до послілки іншої полярності.

На рис. 1.39 показано, що в прийнятих послілках усі позитивні послілки укорочені спочатку з кінця на одну й ту саму величину $\theta_1 = \theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6 = \theta_{\text{пр}}$, а всі від'ємні подовжені ту й саму величину.

Відносна величина крайових спотворень від переваг дорівнює

$$\delta_p = \frac{2\theta_{\text{пр}}}{2t_0} \cdot 100\% = \frac{\theta_{\text{пр}}}{t_0} \cdot 100\%.$$

Порушення симетрії деяких параметрів сигналу, що мають змінний характер, викликає так звані змінні переваги. Наприклад, однією із причин появи змінних переваг при роботі по КХ радіохвилям просторовою хвилею є вибірні завмирання, тобто завмирання однієї із частот при ЧМ. У цьому

випадку внаслідок установлювальних процесів у вузькосмуговій частині приймача радіолінії умови прийому посилок, частота яких піддається завмиранню, погіршуються і посліжки приймаються зі спотворенням.

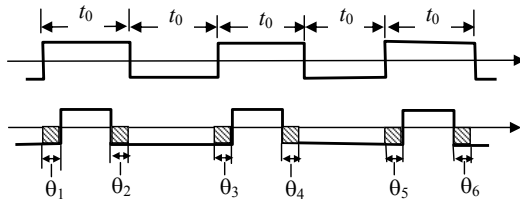


Рисунок 1.39 – Відновлення бінарного сигналу при спотвореннях типу переваг

На рис. 1.40 наведено графіки, що пояснюють причини появи крайових спотворень при зосередженнях завмирання радіосигналів. При однакових амплітудах обвідної високочастотної напруги ($U_A=U_B$), показаних на рис. 1.40, б, посліжки, що приймаються, (рис. 1.40, в) будуть зміщені у часі по відношенню до переданих посилок (рис. 1.40, а) на одну й ту саму величину запізнювання $t_{\text{сер}}$, і крайові спотворення відсутні. Якщо амплітуда однієї із частот, наприклад, частоти Б (рис. 1.40, з), буде менше амплітуди другої частоти, то внаслідок різного характеру установлювальних процесів частот А і Б краї посилок, що приймаються (рис. 1.40, д), будуть спотворюватись. При цьому початок посилок, частота яких завмирає, спотворюються в бік запізнення на величину θ_{1p} , а кінець посилок зміщується в бік випередження на величину θ_{2p} , тобто ці посліжки отримають двосторонні спотворення.

Випадкові спотворення. Випадкові спотворення викликаються, здебільшого, зовнішніми впливами на електричний сигнал під час його проходження по каналу зв'язку. При телеграфуванні по проводах, джерелом сторонніх напруг можуть бути перехідні напруги від сусіднього проводу, вплив високовольтних ліній, будь-якого роду атмосферні впливи (грозові розряди, північні сяйва, магнітні бурі тощо).

У провідних і радіоканалах сторонні напруги виникають від впливу завод, особливо імпульсних, та з інших причин. Крім того, випадкові спотворення з'являються при зміні деяких параметрів каналу: стрибкоподібні зміни рівня сигналу, що приймається, короткочасні переривання в каналі та ін.

Усі вищезазвані впливи, що називаються завадами, випадковим чином підсумовуються, накладаються на сигнал і призводять до випадкових крайових спотворень, якщо амплітуда завод не перевищує рівень сигналу, або до дроблення посилок, що приймаються, у випадку перевищення амплітуди завод над рівнем сигналу.

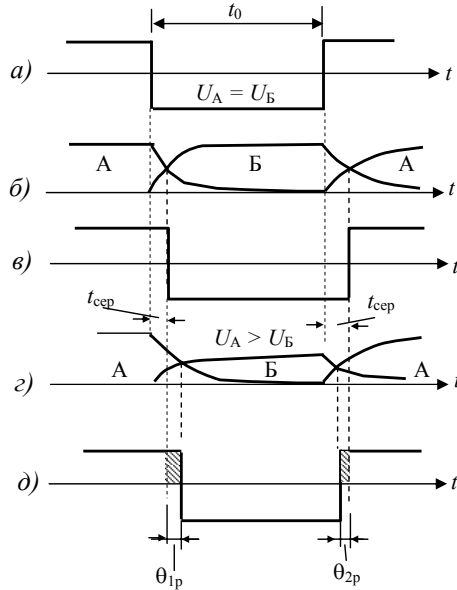


Рисунок 1.40 – Причини появи крайових спотворень при зосереджених завмираннях радіосигналів

Для пояснення фізики процесу накладання завад на основний сигнал розглянемо випадок безпосереднього передавання послідовного постійного струму (рис.1.41, а) по з'єднувальних лініях або кабельних жилах при двополярній роботі. Оскільки вхідний пристрій завжди спрацьовує під впливом струму, то завади можна характеризувати струмом завад I_s (рис. 1.41, б). Характер зміни струму завад випадковий і тому миттєві значення його невідомі, але амплітуду струму завад можна визначити. Позначимо амплітуду позитивних значень струмів завад через $+I_s$, а від'ємних через $-I_s$. При

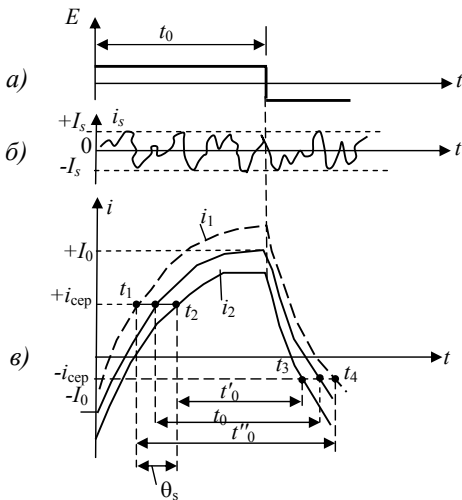


Рисунок 1.41 – Процес накладання завад на основний сигнал

цьому будемо вважати, що $I_s < I_0$, де I_0 – усталене значення струму в колі телеграфування. Для простоти зображення графіків передбачається, що запізнення сигналів в розглядуваному випадку дорівнює нулю.

Сумісний вплив сигналу і струмів завад можна показати шляхом накладання амплітуди струму завад на криву вхідного струму (пунктирні криві на рис. 1.41, в). Тоді граничні зміни струмів в колі вхідного пристрою запишемо так:

$$i_1 = I_0(1 - 2e^{-\frac{t}{\tau}}) + I_s;$$

$$i_2 = I_0(1 - 2e^{-\frac{t}{\tau}}) - I_s.$$

При впливі завад вхідний пристрій може спрацювати у гіршому випадку або в моменти t_1, t_4 , і тоді послілка, що приймається, подовжиться до величини t_0'' , або в моменти t_2, t_3 , і при цьому послілка скоротиться до t_0' .

Абсолютна величина випадкових спотворень буде дорівнювати $\theta_s = t_2 - t_1 = t_4 - t_3$. Для визначення t_1 і t_2 підставимо ці значення у вирази, які наведені вище:

$$i_{\text{сеп}} = I_0(1 - 2e^{-\frac{t_1}{\tau}}) + I_s;$$

$$i_{\text{сеп}} = I_0(1 - 2e^{-\frac{t_2}{\tau}}) - I_s.$$

Розв'язавши ці рівняння відносно t_1 і t_2 , отримаємо:

$$t_1 = \tau \ln \frac{2I_0}{I_0 + I_s - i_{\text{сеп}}};$$

$$t_2 = \tau \ln \frac{2I_0}{I_0 - I_s - i_{\text{сеп}}}.$$

Тоді

$$\theta_s = t_2 - t_1 = \tau \ln \frac{I_0 + I_s - i_{\text{сеп}}}{I_0 - I_s - i_{\text{сеп}}}.$$

Прийнявши $S = \frac{I_s}{I_0 - i_{\text{сеп}}}$, отримаємо

$$\theta_s = \tau \ln \frac{1+S}{1-S}. \quad (1.87)$$

Відносна величина випадкових крайових спотворень дорівнює

$$\delta_s = \frac{\theta_s}{2t_0} \cdot 100\% = \frac{\tau}{2t_0} \ln \frac{1+S}{1-S} \cdot 100\%. \quad (1.88)$$

Із формули (1.88) випливає, що випадкові спотворення збільшуються зі збільшенням постійної часу, струму завад і струму спрацьовування і зі зменшенням установленого значення вхідного струму. Тому з метою змен-

шення величини випадкових спотворень підвищують чутливість вхідного пристрою та вибирають значення $I_0 = (3...4)I_s$.

Вираз (1.88) справедливий при $S < 1$, тобто при рівні завад, що менший за рівень сигналу.

При впливі завад, амплітуда яких сумірна або перевищує рівень сигналу, можуть виникати дроблення. Дроблення з'являються в будь-якій частині посилок (рис. 1.42, *a*), в тому числі і на краях, збільшуючи величину крайових спотворень. На рис.1.42, *б* показана прийнята послідовність з одним дробленням, абсолютна величина якого дорівнює $\theta_{др}$. Відносна величина дроблення визначається по відношенню до тривалості елементарної послілки, тобто

$$\delta_{др} = \frac{\theta_{др}}{t_0} \cdot 100\%.$$

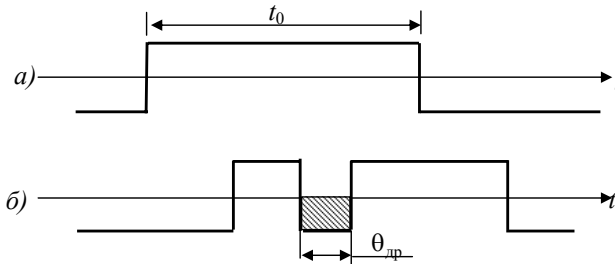


Рисунок 1.42 – Вплив дроблення на бінарний сигнал

Загальний вплив наведених вище завад призводить до того, що закон розподілу зміщення границь одиничних елементів близький до нормально-го (див. рис. 1.44, *a*):

$$f(\delta) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(\delta-a)^2/2\sigma^2}, \quad (1.89)$$

де δ – випадкова величина спотворень, %; a – математичне очікування величини спотворень; σ – середньоквадратичне відхилення δ від значення a .

При інтенсивних імпульсних завадах і короткочасних перериваннях зв'язку крім крайових спотворень спостерігаються дроблення, які визначаються як короткочасні довільні зміни значень позиції всередині одиничного елемента (рис. 1.43).

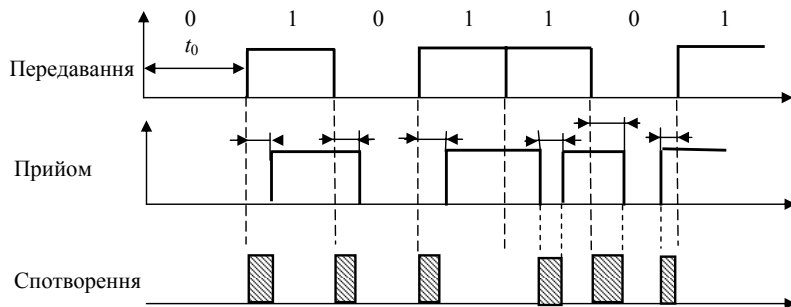


Рисунок 1.43 – Сумісний вплив дроблення та крайових спотворень

Імпульси дроблень характеризуються інтенсивністю виникнення та тривалістю. Криві розподілу тривалості дроблень близькі до логарифмічно-нормального закону (рис. 1.44, б)

$$\varphi(\tau_{др}) = \frac{1}{\tau_{др} \sigma_{\tau} \sqrt{2\pi}} e^{-(\ln \tau_{др} - m)^2 / 2\sigma^2 \tau}, \quad (1.90)$$

де $\tau_{др}$ – випадкова тривалість дроблень; m – математичне очікування випадкової величини $\ln \tau_{др}$ тривалості дроблень; σ_{τ} – середньоквадратичне відхилення випадкової величини $\ln \tau_{др}$.

У реальних дискретних каналах крайові спотворення та дроблення частіше за все групуються. Тоді спостерігається процес пакетування спотворень одиничних елементів. При цьому зручніше розглядати сумарне спотворення одиничних елементів, що характеризуються величиною спотворень і зоною їхньої дії за тривалістю одиничних елементів.

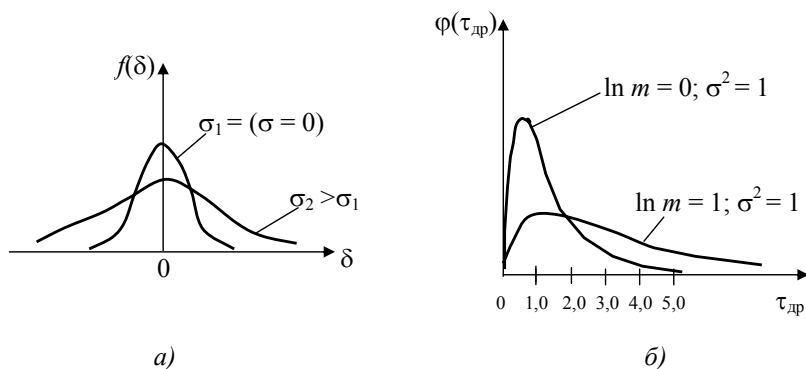


Рисунок 1.44 – Закони розподілу:
а – нормальний; б – логарифмічно-нормальний

Густина розподілу ймовірності сумарних спотворень за величиною, що показує частоту з'явлення одиничних елементів з різним ступенем спотворення (подана на рис. 1.45 для низькошвидкісних каналів), апроксимується таким виразом:

$$p(\delta) = \varepsilon_1 e^{-\lambda_1 \delta} + \varepsilon_2 e^{-\lambda_2 \delta}, \quad (1.91)$$

де δ – величина сумарних спотворень одиничних елементів, $\varepsilon_1 + \varepsilon_2 = 1$ – нормувальні коефіцієнти. Дві складові виразу (1.91) відповідають двом станам каналу – нормальному та «пакетному».

Густина розподілу ймовірності сумарних спотворень за тривалістю одиничних елементів (залежність ймовірності помилок від зони реєстрації), що показує частість спотворень у певній зоні тривалості одиничних елементів (наведена на рис. 1.46 для низькошвидкісних каналів), апроксимується кривою Персона типу 1:

$$p(\delta_t) = \tilde{p}(1 + \delta_t / l_1)^{q_1} (1 - \delta_t / l_2)^{q_2}, \quad (1.92)$$

де $l_1 + l_2$ – зони урахування сумарних спотворень, %; q_1, q_2 – коефіцієнти кривої розподілу.

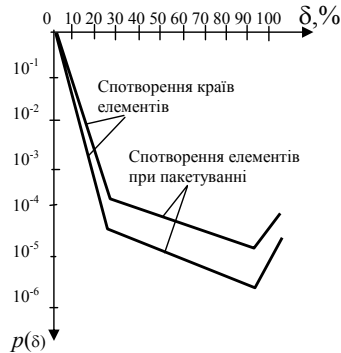


Рисунок 1.45 – Густина розподілу ймовірності сумарних спотворень за величиною δ

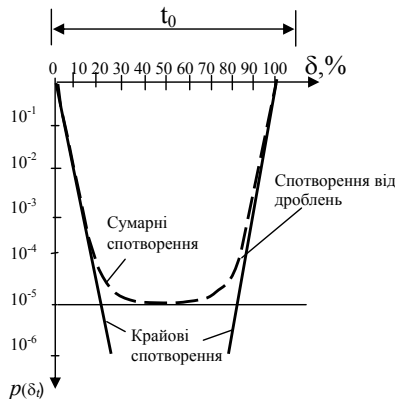


Рисунок 1.46 – Густина розподілу ймовірності сумарних спотворень за тривалістю одиничних елементів

1.2.4. Реєстрація сигналів кодових конструкцій

Знання характеристик крайових спотворень і дроблень в КПС дозволяє оцінити якість каналу зв'язку з точки зору його придатності для передавання дискретних повідомлень. При цьому немаловажливий той факт, що оцінка величин спотворень та інтенсивності дроблень можлива в процесі передавання інформації по каналу зв'язку.

Сигнал, що надходить з виходу КПС, повинен бути ототожнений з «0» або «1». Необхідно провести також запам'ятовування значущої позиції сигналу даних. Процес визначення і запам'ятовування значущої позиції сигналу даних називається *реєстрацією*. Пристрій реєстрації сигналів, що забезпечує мінімальну ймовірність помилкового прийому $p_{\text{пом}}$, назовемо *оптимальним*. Реалізація оптимального пристрою реєстрації викликає певні труднощі, і тому на практиці застосовують спрощені методи реєстрації, які хоча і програють у завадостійкості оптимальному, але простіші в реалізації. До числа найбільш поширених методів реєстрації відносяться методи стробування та інтегральний.

При реєстрації *методом стробування* вид елемента («0», «1»), що приймається, визначається на основі аналізу знаку імпульсу постійного струму (сигналу на виході КПС) у середині одиничного інтервалу. Будь-яке зміщення моменту реєстрації відносно середини одиничного інтервалу призводить до збільшення ймовірності вірної реєстрації сигналу.

Структурна схема пристрою, здійснюючого реєстрацію посилок методом стробування, наведена на рис. 1.47, а часові діаграми, що пояснюють принцип роботи – на рис. 1.48.

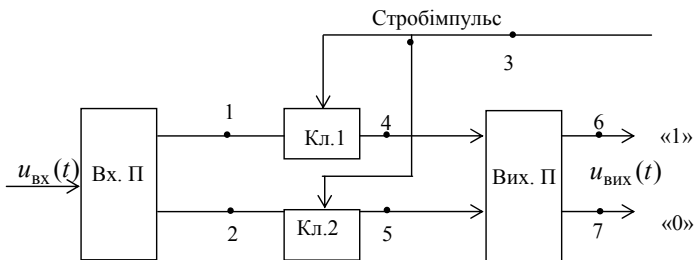


Рисунок 1.47 – Реєстрація методом стробування

Передається послідовність 10101. На виході вхідного пристрою Вх.П імпульси постійного струму мають прямокутну форму, але спотворені за тривалістю (штриховою лінією показано неспотворені сигнали). Ключі Кл.1 і Кл.2 відкриваються одночасно на час надходження стробімпульсу. Надходження імпульсів стробування u_5 в моменти, що відповідають сере-

дині одиничних інтервалів, забезпечуються застосуванням пристроїв елементарної синхронізації. При цьому сигнал u_4 (u_5) з'являється або на виході Кл.1 (точка 4), або Кл.2 (точка 5). У залежності від цього вихідний пристрій Вих.П фіксує «1» або «0». Якщо зміщення ЗМ відносно ідеального положення не перевищує $0,5\tau_0$, то елемент сигналу ресструється вірно. Величина, на яку допускається зміщення ЗМ, яке не викликає помилкового прийому, визначає виправляючу здатність приймача (або телеграфного апарата).

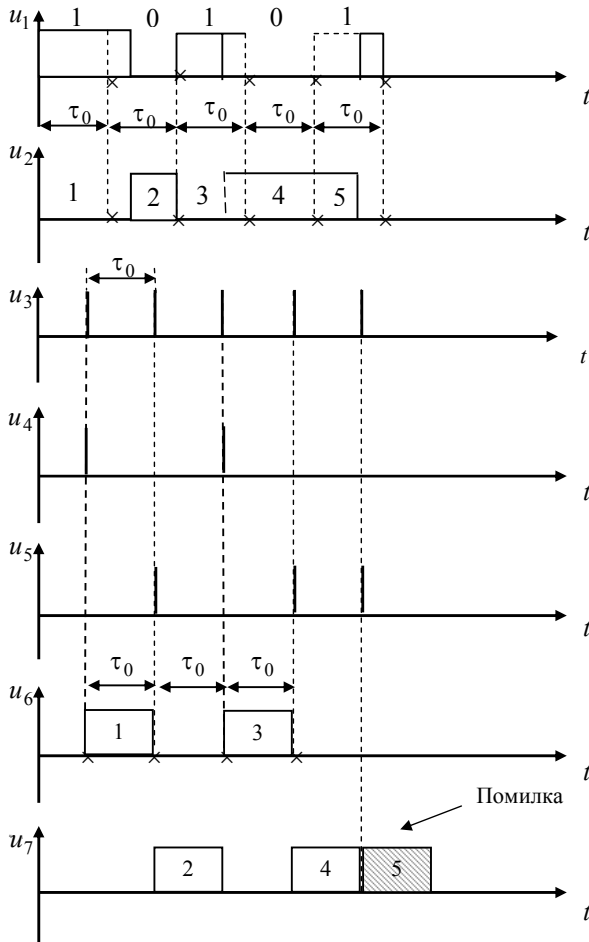


Рисунок 1.48 – Діаграми, що пояснюють принцип ресстрації методом стробування

У нашому випадку виправляюча здатність (теоретична) дорівнює $0,5\tau_0$ або 50%. Із рис. 1.48 видно, що через зміщення ЗМ відносно ідеального положення на величину, що перевищує $0,5\tau_0$, п'ятий елемент приймається невірно.

При *інтегральному методі* реєстрації рішення про вид прийнятого елемента вноситься на підставі аналізу сигналу $u_{\text{вих}}$, визначуваного виразом

$$u_{\text{вих}} = \frac{1}{\tau_0} \int_0^{\tau_0} u_{\text{вх}}(t) dt,$$

де $u_{\text{вх}}(t)$ – сигнал на вході реєструючого пристрою (виході КПС). Цей сигнал є дискретною функцією неперервного часу.

Інтегрування здійснюється на інтервалі, що відповідає неспотвореному елементу. Нехай $u_{\text{вх}}(t)$ приймає на інтервалі аналізу як значення $u_{\text{вх}}(t)=0$, так і $u_{\text{вх}}(t)=1$. Тоді рішення про приймання «1» повинно вноситься, якщо $u_{\text{вих}}(t) \geq \frac{1}{2}$. Очевидно, що помилка при передаванні «1» буде в тому випадку, коли $u_{\text{вих}}(t) < \frac{1}{2}$.

Інтегральний метод часто реалізується на основі багаторазового стробування сигналу $u_{\text{вх}}(t)$ в N точках. Схема, що пояснює принцип дії такого пристрою реєстрації, наведено на рис. 1.49. Сигнал $u_1(t)$ (точка 1) керує ключем Кл. При відкритому ключі, коли $u_{\text{вх}}(t)=1$, а імпульси $u_5(t)$ (стробімпульси) проходять на вхід лічильника Лч. За час дії неспотвореної тактової послідовності $u_1(t)$ (на інтервалі τ_0) на виході Кл. (точка 3) з'являється N тактових імпульсів. Якщо на виході Кл. на одиничному інтервалі з'явиться $N/2+1$ і більше стробімпульсів, то можна дійти висновку про те, що прийнята «1». Ємність лічильника досить взяти рівною $N/2+1$. Вкінці одиничного інтервалу, визначуваного за допомогою пристрою поелементної синхронізації, показання лічильника зчитуються і він обнулюється. Часові діаграми, які ілюструють роботу схеми, наведені на рис. 1.50. Тут невірно реєструється друга послідовність.

Порівняємо завадостійкість методів стробування та інтегрального при дії крайових спотворень. Оскільки при реєстрації методом стробування послідовності реєструються усередині, то допускається зміщення будь-якого із ЗМ на величину, що не перевищує величину $0,5\tau_0$. При реєстрації інтегральним методом сумарне зміщення границь не повинно перевищувати $0,5\tau_0$. Очевидно, що остання умова виконується з меншою ймовірністю, тобто $p_{\text{ек}}^{(i)} > p_{\text{ек}}^{(c)}$, де $p_{\text{ек}}^{(i)}$, $p_{\text{ек}}^{(c)}$ – відповідно ймовірності невірного прийому при крайових спотвореннях і реєстрації інтегральним методом та методом стробування.

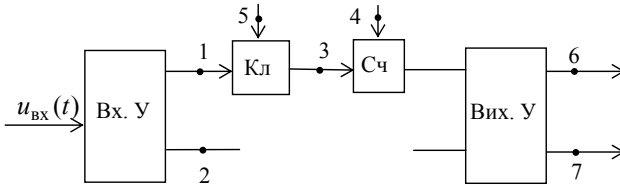


Рисунок 1.49 – Реєстрація інтегральних методів

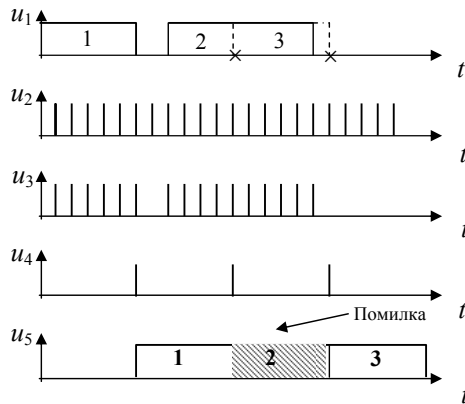


Рисунок 1.50 – Діаграми, що пояснюють принцип реєстрації інтегральним методом

Якщо крайові спотворення δ підкоряються гауссівському закону

$$W(\delta) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(\delta \pm a)/(2\sigma^2)}, \quad (1.93)$$

де a – математичне сподівання δ методом стробування; σ^2 – дисперсія δ , то ймовірність помилки при реєстрації

$$p_{\text{ек}}^{(c)} = 0,75 - 0,5\Phi(z) - 0,25[\Phi(z)]^2, \quad (1.94)$$

де $\Phi(z) = \frac{2}{\sqrt{2\pi}} \int_0^z e^{-x^2/2} dx$ – функція Крампа;

$$z = (\mu - a) / \sigma,$$

де μ – виправляюча здатність приймача; a – математичне очікування зміщення границі елемента; σ – середнє квадратичне відхилення зміщення.

При реєстрації інтегральним методом

$$p_{\text{ек}}^{(i)} = 0,75 - 0,5\Phi(z/\sqrt{2}) - 0,25[\Phi(z/\sqrt{2})]^2. \quad (1.95)$$

При виведенні формул, що наведені вище, передбачається, що елемент сигналу обмежений з обох сторін ЗМ, а

$$W_1(\delta) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(\delta-a)^2/(2\sigma^2)}, \quad W_2(\delta) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(\delta+a)^2/(2\sigma^2)},$$

де $W_1(\delta), W_2(\delta)$ – густина розподілу крайових спотворень для лівого і правого ЗМ елемента сигналу відповідно.

Як приклад наведемо методику виведення (1.94). Елемент сигналу реєструється невірно в тому випадку, якщо ліва або права границі змістяться в середині послілки на величину, що перевищує виправляючу здатність приймача. Ймовірність подій позначимо відповідно p_1 і p_2 . Невірна реєстрація має місце також в тому випадку, якщо обидві границі одночасно змістяться на величину, більшу μ . Ймовірність цієї події в припущенні незалежності зміщення границь елементів визначимо, як $p_1 p_2$. Очевидно, що

$$p_1 = \frac{1}{\sqrt{2\pi\sigma}} \int_{\mu}^{\infty} e^{-(\delta-a)/(2\sigma^2)} d\delta = 0,5[1 - \Phi(z)], \quad (1.96)$$

$$p_2 = \frac{1}{\sqrt{2\pi\sigma}} \int_{-\infty}^{-\mu} e^{-(\delta+a)/(2\sigma^2)} d\delta = 0,5[1 - \Phi(z)]. \quad (1.97)$$

Враховуючи, що $p_{ек}^{(c)} = p_1 + p_2 - p_1 p_2$, одержимо (1.94).

Розглянемо дію дроблень. Будемо вважати, що на одиничний інтервал припадає тільки одне дроблення. Позначимо тривалість дроблення $t_{др}$. Очевидно, що всі дроблення можуть бути розділені на дві групи $t_{др} < \tau_0/2$ і $t_{др} \geq \tau_0/2$. Якщо $t_{др} < \tau_0/2$ при інтегральному методі приймання буде вірним, тому що спотворюється менше половини ППТ. Якщо $t_{др} > \tau_0/2$, і при цьому спотворено більше половини ППТ, то при інтегральному методі реєстрації буде невірне приймання. Але оскільки спотворено більше половини послілки, то буде спотворена і її середина. Отже буде невірним приймання і при реєстрації методом стробування. Таким чином, якщо при реєстрації методом стробування невірне приймання можливе як у випадку, якщо $t_{др} < \tau_0/2$, так і при $t_{др} > \tau_0/2$, то при інтегральному – тільки при $t_{др} \geq \tau_0/2$. Тому $p_{ед}^{(c)} > p_{ед}^{(i)}$, де $p_{ед}^{(c)}, p_{ед}^{(i)}$ – відповідно ймовірності помилки при дії дроблень для випадків реєстрації методом стробування та інтегральним методом. Ймовірність помилки буде тим більшою, чим частіше з'являється дроблення, а також чим більша середня тривалість дроблення і дисперсія тривалості дроблення. При спільній дії крайових спотворень і дроблень ймовірність помилки наближено може бути визначена за формулою

$$p_e \approx p_{ед} + p_{ек} - p_{ед} p_{ек}.$$

В останні роки ведеться пошук простих у реалізації, але досить ефективних (близьких за завадостійкістю до оптимальних) методів реєстрації. Запропоновано низку методів, серед яких багатоінтервальний та інтегрування з ваговою функцією, які розглядаються нижче.

Особливість *багатоінтервального методу* полягає у відмові від обов'язкового оброблення сигналу на одиничному інтервалі τ_0 . Інтервал оброблення, на якому здійснюється реєстрація інтегральним методом, вибираються в залежності від характеру спотворень ПТТ. Алгоритм вибору інтервалу обробки полягає в наступному. Якщо надходить посилка, що містить дві границі (два ЗМ), причому кожна з границь зміщена відносно ідеального положення не більше, ніж на задане граничне значення, то посилка інтегрується в інтервалі часу,

обмеженому цими двома границями. Якщо ж зміщення границі (обох границь) перевищує граничне значення, то границя (границі) замінюються тактовим імпульсом (імпульсами), що виробляються системою поелементної синхронізації. У випадку, коли в елементі сигналу (посилки), що надходить, немає границі (границь), тобто надходять підряд декілька однакових посилок, то як і раніше відсутня границя замінюється тактовим імпульсом. Коли в інтервал часу, обмежений граничними зміщеними границями (інтервал фіксації границь t_{ϕ}), попадає кілька границь (з'являються хибні границі), то інтегрування сигналу починається (закінчується) при появі першої границі, що надходить.

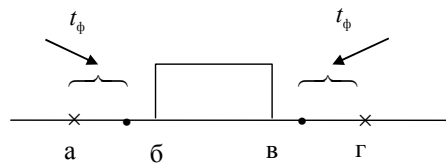


Рисунок 1.51 – До реєстрації посилок багатоінтервальним методом

На рис.1.51 для прикладу показана спотворена посилка. Реєстрація сигналу звичайним інтегральним методом відбувається в інтервалі $a-z$ (що відповідає випадку неспотвореного прийому). При цьому враховуються частини попереднього та наступного елементів. При багатоінтервальному методі інтегрування здійснюється в інтервалі $б-в$, що дозволяє краще використати енергію сигналу.

Ймовірність помилки можна також зменшити, застосовуючи *реєстрацію з ваговою функцією*. Якщо відомо характер спотворень різних ділянок на тривалості одиничного елемента, то відлік необхідно здійснювати з різною вагою: там, де спотворення з'являються рідше, вагу необхідно збільшити і навпаки. Описані раніше методи реєстрації – інтегральний і стробування – можна розглядати як поодинокий випадок методу реєстрації з ваговою функцією. При інтегральному методі вага береться однаковою на всьому інтервалі реєстрації τ_0 , а при стробуванні середня частина береться з вагою 1, а всі останні частини – з вагою 0 (не враховуються).

На рис. 1.52 показано приймання стартової комбінації при реєстрації в середній частині кожного елемента.

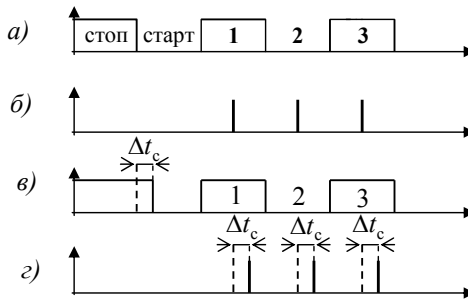


Рисунок 1.52 – Реєстрація посилок стартової комбінації:

- a* – прийнята ідеальна стартова послідовність;
- б* – відповідна їй послідовність стробімпульсів;
- в* – стартова послідовність зі зміщенням в сторону відставання стартової комбінації;
- з* – відповідна їй послідовність стробімпульсів.

1.2.5. Статистика помилок на виході дискретного каналу. 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 $p(\hat{\mathbf{a}}/\mathbf{a})$, де $\mathbf{a} = (a_1, a_2, a_3, \dots, a_i, \dots)$ – довільна послідовність символів вхідного алфавіту і $a_i \in A$ – символ на вході каналу в i -й момент часу $\hat{\mathbf{a}} = (\hat{a}_1, \hat{a}_2, \hat{a}_3, \dots, \hat{a}_i, \dots)$ – відповідна \mathbf{a} послідовність символів із вихідного алфавіту, а $\hat{a}_i \in \hat{A}$ – символ на виході каналу в i -й момент; $p(\hat{\mathbf{a}}/\mathbf{a})$ – умовна ймовірність прийому послідовності $\hat{\mathbf{a}}$ за умови, що передана послідовність \mathbf{a} .

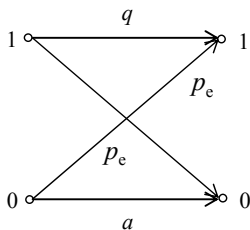


Рисунок 1.53 – Діаграма переходів у бінарному каналі

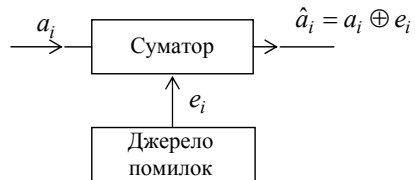


Рисунок 1.54 – Еквівалентна схема дискретного симетричного каналу

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.

Помилки в реальних каналах зв'язку. 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 передавалась, 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 $p_{eп}$, то їхнє число підкоряється біно-

міальному 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 $p_{eп} = p_{eв}$, за якої малоімовірно одержати частість помилок $\xi < \xi_0$. Ця межа шукається із рівняння

$$\sum_{i=0}^r C_n^i p_{eв}^i (1 - p_{eв})^{n-i} = 1 - \beta_0. \quad (1.98)$$

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

$$\sum_{i=r}^n C_n^i p_{eн}^i (1 - p_{eн})^{n-i} = 1 - \beta_0. \quad (1.99)$$

Якщо $r = 0$, то рівняння (1.98) набуде вигляду

$$(1 - p_{eв})^n = 1 - \beta_0.$$

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

$$n_m = l_п = \frac{\lg(1 - \beta_0)}{\lg(1 - p_{eв})}.$$

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

При кореляції помилок з коефіцієнтом ρ_0 ймовірність спотворення символу всередині пакета

$$p'_{eп} = 2p_{eп}(1 - \rho_0),$$

а довжина пакета

$$l_п = \frac{\lg(1 - \beta_0)}{\lg \rho_0}. \quad (1.100)$$

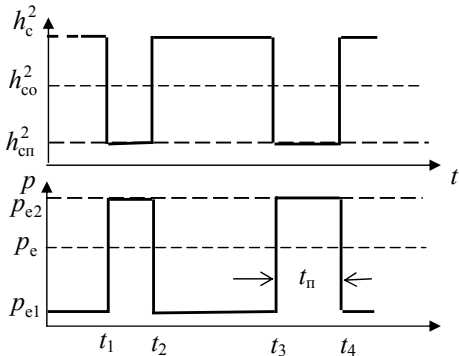


Рисунок 1.55 – Модель каналу з двома станами

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 $p_e = \varphi(t)$.

Нехай функція $h_c^2(t)$ має прямокутну форму (рис.1.55).

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 хорошому 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*.

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_b .

Для повної ймовірності оцінки потоку помилок необхідно знати середню ймовірність спотворення кодового символу p_e , ймовірність спотворення кодограми $P_{ек}$, а також функції розподілу помилок в спотворених кодограмах $F(n_c)$, інтервалів між помилками $F(\tau_c)$ та інтервалів між помилками відносно попередніх інтервалів $F_t(\tau_c)$.

При досить великому числі символів ймовірність

$$p_e = \frac{n_c}{n_0} = \frac{r}{n_0}, \quad (1.101)$$

де n_0 і n_c – відповідно число переданих і спотворених символів. Сам по собі цей параметр не має особливого значення, але він дуже впливає на величину ймовірності

$$P_{ек} = \frac{N_{кc}}{N_{кз}}$$

де $N_{кз}$ – загальне число переданих кодограм; $N_{кc}$ – число спотворених кодограм. Ймовірність $P_{ек}$ залежить від надлишковості коду, типу і інтенсивності завад, способу оброблення сигналів.

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. 1.56, 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.1.56, б інтервал між помилками виражений в двійкових символах).

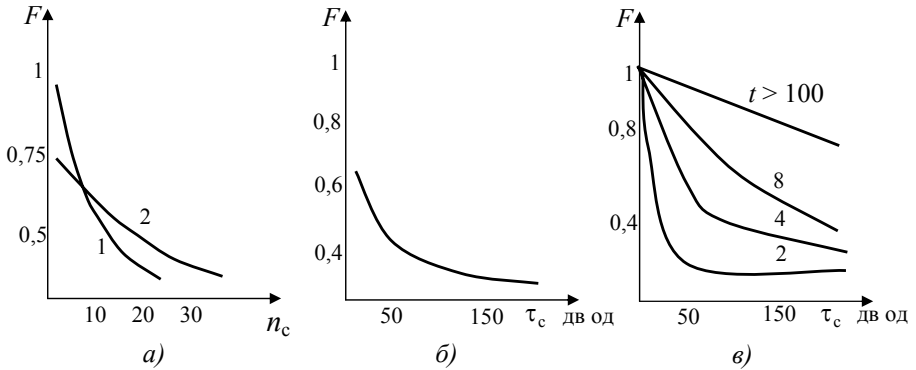


Рисунок 1.56 – Статистичні характеристики кабельних каналів

Функція $F(n_c)$ більш тонко відображає статистичну структуру потоку помилок, оскільки враховує вплив попередніх моментів часу (на рис. 1.56, в за віссю абсцис відкладені поточні часові інтервали між помилками в двійкових символах, а біля кривих – попередні часові інтервали).

Природа кореляції помилок точно не встановлена. Але відзначені інтервали кореляції двох видів – короткі, тривалістю до 5...10 мс, і довгі, вимірювані десятками хвилин. Перші обумовлені в основному дією завод, другі – порушенням умов нормальної експлуатації апаратури.

Наведені приклади показують суттєву відмінність реальних каналів від каналу з гауссівською заводою. Для порівняння на рис. 1.57 наведені залежності ймовірності помилок для каналів з різними типами модуляції та прийому.

Розглянемо деякі моделі потоків помилок в дискретних каналах зв'язку.

Модель потоку помилок у двійковому симетричному каналі. 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.

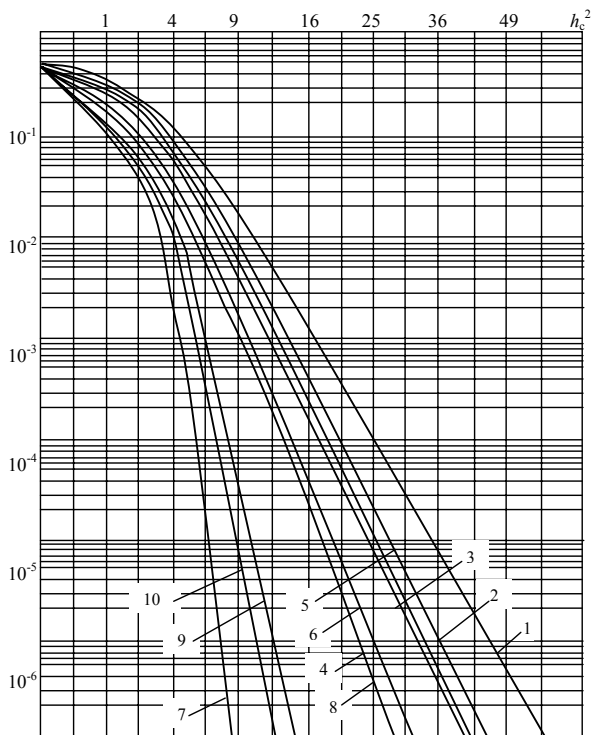


Рисунок 1.57 – Характеристики завадостійкості телеграфних каналів при флуктуаційних завадах:

- 1 – некогерентна АМ; 2 – когерентна АМ; 3 – некогерентна ЧМ;
- 4 – когерентна ЧМ; 5 – некогерентна ДЧМ; 6 – когерентна ДЧМ;
- 7 – ФМ; 8 – ДФМ; 9 – ОФМ₁; 10 – ОФМ₂

Для ДСК раціонально використати коди, що виправляють всі помилки кратності $r \leq r_0$ і не виправляють помилки більш високої кратності.

Модель потоку помилок в каналі з двома станами. Ця модель, запропонована Гільбертом, описує потік помилок у каналі простим однорідним ланцюгом Маркова з двома станами. В одному стані – хорошому – пе-

ревищення сигналу h_c^2 більше порогового значення $h_{cн}^2$ (рис.1.55) 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 $h_c^2 < h_{cн}^2$, і ймовірність спотворення символів $p_{e2} \gg p_e$. Моменти часу t_1 та t_3 відповідають появі пакетів помилок довжиною l_n символів, при цьому помилки всередині пакетів і самі пакети передбачаються некорельованими.

Ймовірність помилки залежить від величини перевищення сигналу над шумами h_c^2 (передбачається, що в каналі зв'язку діють адитивні гауссівські шуми). Завмирання викликають зміну h_c^2 , тому при визначенні залежності $p_e(h_c^2)$ необхідно перейти від функції $w(U_c)$ до функції $w(h_c^2)$. Згідно з теоремою про перетворення розподілу ймовірностей маємо

$$w(h_c^2) = w[f(h_c^2)] \frac{df(h_c^2)}{dh_c^2},$$

де функція

$$f(h_c^2) = U_c^2 = 2h_c^2 \sigma_{ш}^2.$$

У Ланька А.А. ця модель характеризується параметрами: p_n – ймовірність появи пакета помилок (ймовірно переходу каналу від хорошого стану в поганий); $p(l_n)$ – ймовірність утворення пакета помилок довжиною l_n в поганому стані каналу; p_{e1} – ймовірність спотворення символів в хорошому стані каналу (за відсутності пакета помилок); p_{e2} – ймовірність спотворення символів в поганому стані каналу (всередині пакета помилок).

Нехай в пакетах зосереджено $\alpha_0\%$ усіх помилок. Тоді

$$\int_0^{h_{cн}^2} f(h_c^2) w(h_c^2) dh_c^2 = \alpha_0 \int_0^{\infty} f(h_c^2) w(h_c^2) dh_c^2 = \alpha_0 p_e$$

Тому що ймовірність

$$p_{e1} = \frac{\int_{h_{cн}^2}^{\infty} f(h_c^2) w(h_c^2) dh_c^2}{\int_{h_{cн}^2}^{\infty} w(h_c^2) dh_c^2}; \quad p_{e2} = \frac{\int_0^{h_{cн}^2} f(h_c^2) w(h_c^2) dh_c^2}{\int_0^{h_{cн}^2} w(h_c^2) dh_c^2}$$

то при заданому значенні $h_{cн}^2$ одержимо

$$p_{e1} = \frac{1 - \alpha_0}{1 - \Phi_1} p_e; \quad p_{e2} = \frac{\alpha_0 p_e}{\Phi_1},$$

де функція

$$\varphi_1 = \int_0^{h_{c_n}^2} w(h_c^2) dh_c^2.$$

Середнє число викидів за 1 с обвідної випадкового процесу $h_c^2(t)$ вище рівня $h_{c_n}^2$ визначається виразом

$$v_0 = \frac{0,85}{\sqrt{h_{c_0}^2 T_{30}}}.$$

Тоді ймовірність

$$p_n = v_0 T_c e^{-v_0 T_c}.$$

Якщо t_n – тривалість викиду обвідної функції $h_c^2(t)$, то ймовірність

$$p(l_n) = \int_{(l_n-0,5)T_c}^{(l_n+0,5)T_c} w(t_n) dt_n.$$

При завмиранні за законом Релея густина ймовірності

$$w(h_c^2) = \frac{2\sqrt{h_{c_0}^2}}{h_{c_0}^2} e^{-\frac{h_c^2}{h_{c_0}^2}},$$

де $h_{c_0}^2$ – середнє значення h_c^2 . В цьому випадку при некогерентному прийманні ортогональних сигналів ймовірності

$$p_{e1} = \frac{1}{2} e^{-\frac{h_c^2}{2}}, \quad p_{e2} = \frac{1}{2 + h_{c_0}^2}.$$

Тоді при $\alpha_0 = 0,99$ одержимо

$$h_{c_n}^2 \approx 3; \quad \varphi_1 = 1 - e^{-\frac{9}{h_{c_0}^2}} \approx \frac{9}{h_{c_0}^2}$$

При $h_{c_0}^2 \geq 100$, що часто виконується на практиці, ймовірності

$$p_{e1} \approx 10^{-2} p_e; \quad p_{e2} \approx 0,11 p_e h_{c_0}^2,$$

$$p(l_n) = \exp\left[-\frac{\pi(l_n - 0,5)^2}{4l_{no}^2}\right] - \exp\left[-\frac{\pi(l_n + 0,5)^2}{4l_{no}^2}\right],$$

де середня довжина пакету помилок у символах

$$l_{no} = t_{no} v_T \approx 10,6 \frac{T_{30} v_T}{\sqrt{h_{c_0}^2}};$$

T_{30} – середній період завмирань, а ймовірність

$$p_n = 0,99 \frac{p_e}{p_{e2} l_{no}} = \frac{9}{h_{c_0}^2 l_{no}}.$$

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 рознесені прийомі.

В табл. 1.2 наведені основні параметри реальних каналів зв'язку при передаванні дискретних повідомлень.

Таблиця 1.2 – Характеристики реальних каналів

№ каналу	Тип каналу	Вид модуляції	Швидкість модуляції, Бод	Кількість переривів по НЧ або по-ряджність передавача	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

Статистична ймовірність появи спотворених комбінацій визначається як відношення кількості спотворених комбінацій $N_{\text{пом}}(n)$ до загальної кількості комбінацій $N_3(n)$:

$$P(\geq 1, n) = \frac{N_{\text{пом}}(n)}{N_3(n)}$$

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 .

Для гіпотетичного каналу з двома станами, один з яких характеризується ймовірністю появи помилки $p_1 = 1$, а другий $p_2 = 0$ $P(\geq 1, n) = p$. Виходячи з цього, можна визначити границі можливого змінювання величини ймовірності появи спотворених комбінацій: $p < P(\geq 1, n) < np$. У реальних каналах через груповий характер завад величина $P(\geq 1, n)$ менше залежить від довжини комбінації, ніж у випадку незалежних помилок, і тому експериментальні значення $P(\geq 1, n)$ розміщуються приблизно у середній частині між цими границями.

На рис. 1.58 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.

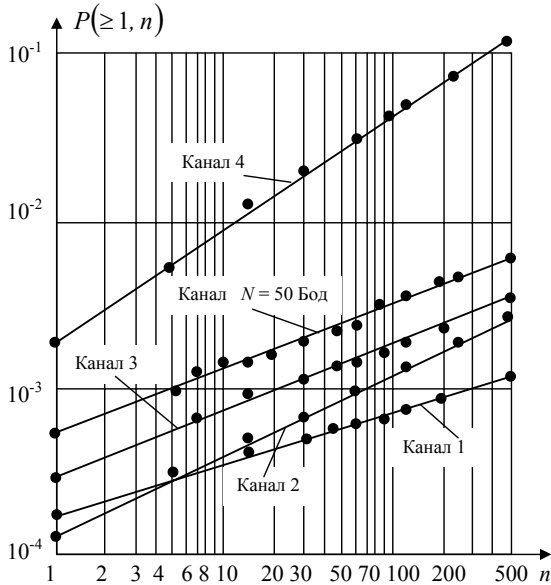


Рисунок 1.58 – Залежність $P(\geq 1, n)$ від n для телефонних кабельних каналів

Установлено, що звичайно для однакових каналів нахил прямих приблизно є однаковим, а зі зміною частоти помилок апроксимуюча пряма зміщується не змінюючи кута нахилу. Для каналів різного виду нахил прямих є різним. На підставі рівняння прямої лінії можна одержати

$$P(\geq 1, n) = n^{1-\alpha} p, \quad 0 < \alpha < 1. \quad (1.102)$$

Коефіцієнт α характеризує міру зростання ймовірності $P(\geq 1, n)$ зі збільшенням n . Із міркувань фізики явищ назвемо його показником групування помилок. Для двох границь величини ймовірності $P(\geq 1, n)$ значення є такими: для каналу з незалежними помилками $\alpha = 0$; для гіпотетичного каналу, коли всі помилки зосереджені в одній групі, $\alpha = 1$. Таким чином, параметр α характеризує міру групування помилок в реальному каналі зв'язку і є другим його параметром. За допомогою двох параметрів p і α можна визначити характеристики каналів зв'язку. Значення показників групування для різних каналів наведені в табл. 1.2.

Найбільше значення α має в телефонних кабельних каналах. Це пояснюється тим, що короточасні переривання у різних проміжних пунктах кабельної магістралі призводять до появи груп з великою густиною помилок. Менше значення α має у радіорелейних каналах, через те, що в них, поруч з ділянками великої густоти, є ділянки з рідкісними помилками, які з'являються через підвищення рівня шумів. У тропосферних телефонних каналах і КХ радіотелеграфних каналах через завмирання сигналу і вплив завад спостерігаються не лише пачки помилок, але і одиничні помилки. Тому показник групування набуває найменше значення ($\alpha \approx 0,32...0,45$). Для каналів тонального телеграфування звичайно параметр α має таке саме значення, що і для кабельних телефонних каналів, через ті ж самі причини виникнення помилок. Про це свідчить приблизно однаковий нахил прямих залежності $P(\geq 1, n) = f(n)$ на рис. 1.58 для кабельних виділених каналів і каналу тонального телеграфування.

Таким чином, величина параметра α певною мірою відображає фізичні причини появи помилок. Тому параметр α є надто важливим параметром послідовності помилок E .

Одним із відомих способів зменшення впливу групування помилок на ефективність систем підвищення достовірності є декореляція помилок рознесенням елементів, що передаються, у часі. На рис. 1.59 наведено залежності $P(\geq 1, n) = f(n)$ для каналів 2, 4 і 11 в табл. 1.2 при інтервалах декореляції $j = 10$ і 1000 елементів (випадок $j = 1$ відповідає відсутності декореляції). Пунктиром на рис. 1.59 нанесено залежності $P(\geq 1, n) = f(n)$ для незалежного розподілу помилок.

При оцінці ефективності блокових коректуючих 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

$$P(\geq 1, n) = P(1, n) + P(2, n) + \dots + P(m, n) + \dots + P(n, n) = \sum_{i=1}^n P(i, n). \quad (1.103)$$

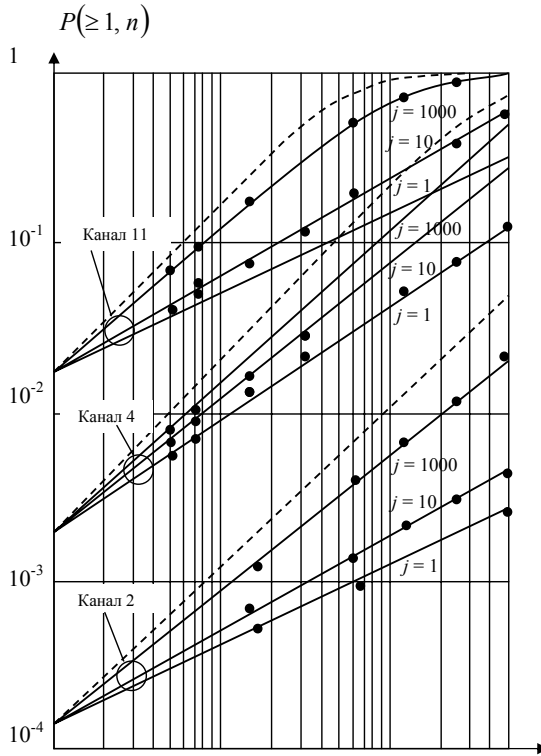


Рисунок 1.59 – Залежність $P(\geq 1, n)$ від n за різних інтервалів декореляції

Для оцінки ефективності деяких коректуючих кодів необхідно також знати сумарну (накопичену) ймовірність появи спотворених комбінацій з m і більше помилками:

$$P(\geq m, n) = P(m, n) + P(m+1, n) + \dots + P(n, n) = \sum_{i=m}^n P(i, n).$$

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:

$$P(\geq m, n) = \frac{\sum_{i=m}^n N(i, n)}{N_3(n)}, \quad (1.104)$$

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 обробленню 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 $N_3 = L/n$.

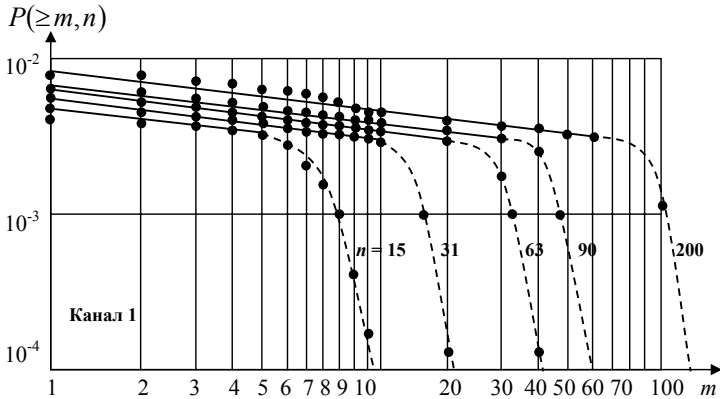


Рисунок 1.60 – Залежність $P(\geq m, n)$ від m для каналу 1

На рис. 1.60 – 1.62 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. 1.2). 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.

Порівнюючи рис. 1.59 – 1.61 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. 1.60) є найменшою. У радіорелейному і тим більше у радіотелеграфному каналі (рис. 1.62) ймовірність $P(\geq m, n)$ зі збільшенням кількості помилок спадає швидше.

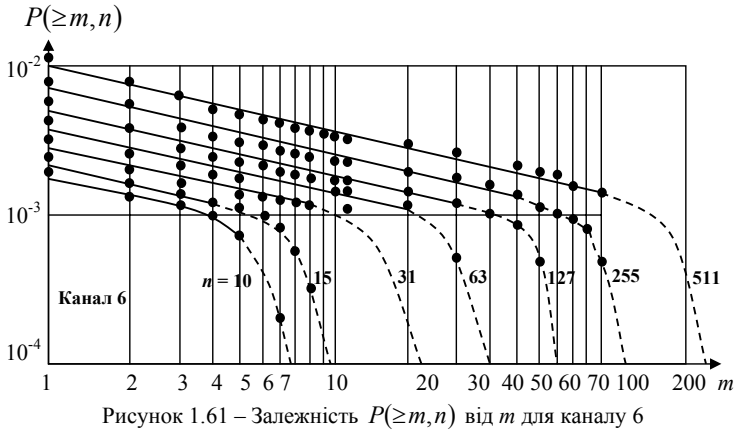


Рисунок 1.61 – Залежність $P(\geq m, n)$ від m для каналу 6

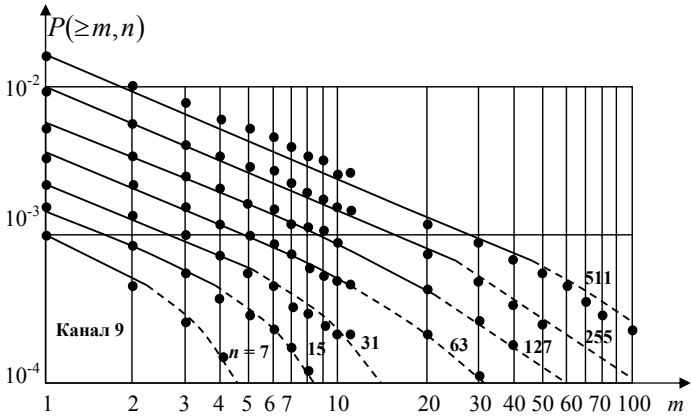


Рисунок 1.62 – Залежність $P(\geq m, n)$ від m для каналу 9

1.2.6. Питання та задачі для самоперевірки

1. Що характеризує критерій фізичної реалізації лінійної системи?
2. Проаналізуйте вираз (1.62) і вкажіть методи зменшення середньоквадратичної похибки відтворення.
3. Якими параметрами характеризується ефективна смуга частот?
4. Що є фіксованими обмеженнями на параметри сигналу у виразі (1.69)?
5. Яке максимальне значення двійкового каналу: а) без завад; б) при наявності завад?

6. Як змінюється пропускна здатність при використанні числа станів інформаційного параметра $a > 2$?

7. При яких значеннях ймовірності p_e у виразі (1.79) величина пропускної здатності буде максимальною?

8. Що характеризує апіорна ймовірність сигналу?

9. Що призводить до різних затримок на виході каналу різних значущих моментів відтворення?

10. В якому випадку змінюється довжина кодових посилок при затримці ЗМВ?

11. Опишіть процес появи характеристичних спотворень.

12. Як впливає параметр τ у виразі (1.84) на величину характеристичних спотворень?

13. Установіть зв'язок між значенням m і середнім значенням тривалості дроблення (вираз 1.90).

14. Установіть залежність між середньоквадратичним відхиленням $\ln \tau_{др}$ і середньоквадратичним для $\tau_{др}$ (вираз 1.90).

15. Чим визначається виправляюча здатність приймального пристрою зі стробуванням у середині посилки за наявності зсувів ЗМВ?

16. Чим відрізняється дискретне інтегрування сигналу посилки від аналогового?

17. Що характеризує коефіцієнт групування помилок α ?

18. Наведіть приклади повідомлень при передаванні яких коефіцієнт групування є позитивним фактором, а для яких негативним?

19. Наведіть послідовність алгоритму декореляції помилок при матричному методі.

20. Порівняйте час затримки повідомлення з декорелятором і без нього за однакової ймовірності помилкового прийому кодового слова за рахунок надлишкового кодування.

ЧАСТИНА 2

ЗАВАДОСТІЙКЕ КОДУВАННЯ

Глава 2.1. Блокові коди

2.1.1. Основні характеристики блокових кодів, їхнє описання та властивості

Класифікація основних коректуючих кодів. На сьогодні відома значна кількість кодів, коректуючих 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. 2.1) розглядаються тільки ті коди, які знаходять застосування у системах передачі дискретних повідомлень (СПДП).

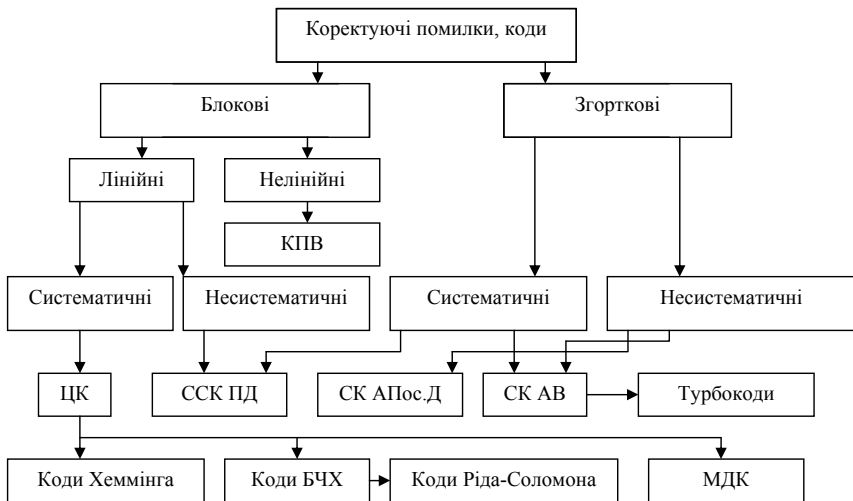


Рисунок 2.1 – Класифікація основних завадостійких кодів

Двійкові коректуючі 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. 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 коректуючі 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 коректуючих кодів, серед яких найбільш відомими є:

- коди Хеммінга, що виправляють однократні і виявляють двократні помилки;

- коди БЧХ, що володіють високою коректуючою 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 коректуючих кодів. Ефективним методом підвищення надійності СПДП є використання коректуючих 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 коректуючого 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:

$$b_j \equiv \left(\sum_{i=0}^m a_i \times \alpha_{ji} \right) \text{mod } 2, \quad (2.1)$$

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 перевірочних 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. Нагадаємо, 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 елементи нульові.

В n -значних кодах з усіх можливих з'єднань кодових комбінацій

$$N_{06} = C_n^0 + C_n^1 + C_n^2 + \dots + C_n^n = 2^n$$

для передавання повідомлень використовується тільки $N_p = 2^m$ КК, які називаються *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 зазначеного можна зробити висновок, що будь-який лінійний код завжди має нульове кодове слово (000...000), утворене в результаті підсумовування декількох дозволених.

Коректуючі 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 – біноміальні коефіцієнти; $p_0 = P(1/0) + P(0/1)$ – повна ймовірність помилки у каналі зв'язку.

Коректуюча здатність двійкових кодів залежить від мінімальної кодової 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, *мінімальна кодова відстань* або *кодова відстань* дорівнює найменшій із усіх можливих відстаней в матриці Хеммінга між усіма можливими парами КС. Для лінійних кодів, з урахуванням того, що в коді 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:

$$W(A_j) = \sum_{i=1}^m a_i + \sum_{i=1}^r b_i.$$

Максимальна кратність виявлення помилок t_b або виправлення помилок $t_{вп}$ пов'язані з кодовою відстанню наступними виразами:

– в режимі виявлення помилок

$$t_b = d_0 - 1; \tag{2.2}$$

– в режимі виправлення помилок

$$t_{вп} = \lceil (d_0 - 1) / 2 \rceil. \tag{2.3}$$

Теорема 1. Якщо d_0 парне, то код може одночасно виправляти $(d_0 - 2)/2$ помилок і виявляти $d_0/2$ помилок.

На рис. 2.2 наведена геометрична модель найпростішого коректуючого 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.

Із рис. 2.2 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.

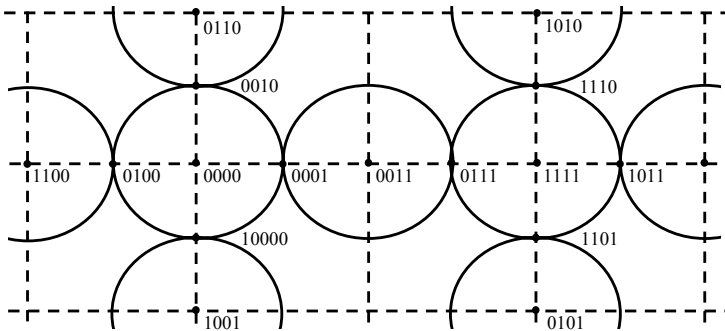


Рисунок 2.2 – Геометрична модель коректуючого коду

Подібно коду $(4, 3)$, на рис. 2.3 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 (2.2), (2.3).

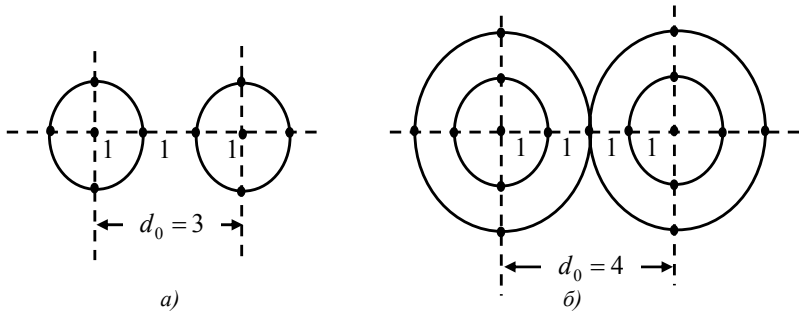


Рисунок 2.3 – Геометричні моделі кодів:
a – що виправляють однократні помилки;
б – що виправляють однократні помилки
та виявляють двократні помилки

Деякі відомості про граничні можливості коректуючої здатності лінійних блокових кодів. Як раніше зазначалося, побудова коректуючого 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 займалися 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, коректуючого 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

$$2^{n-m} \geq \sum_{i=0}^{t_{\text{вн}}} C_n^i. \quad (2.4)$$

Значення цього виразу полягає в наступному. Якщо задані основні параметри лінійного коду n і $t_{\text{вн}} = (d_0 - 1)/2$, то можлива мінімальна кількість надлишкових символів $r = n - m$ може бути визначена за допомогою умови (2.4). Для наочності на рис. 2.4 наведені графіки границь Хеммінга згідно з виразом

$$n - m \geq \left\lceil \log_2 \sum_{i=0}^{t_{\text{вн}}} C_n^i \right\rceil \quad d_0 \in 3; 5; 7. \quad (2.5)$$

Тут $\lfloor x \rfloor$ означає найближче ціле число більше або рівне x . Наприклад, для коду з $t_{\text{вн}} = 1$ 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 коректуючий код з параметрами (n, m, d_0) не існує. В протилежному випадку можливе існування коректуючого коду з такими параметрами.

При цьому слід підкреслити, що рівність (2.5) 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 (2.5).

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

$$2^{n-m} \geq \sum_{i=0}^{d_0-2} C_{n-1}^i, \quad (2.6)$$

то існує (n, m, d_0) код, який реалізується за допомогою не більше $n - m$ перевірок на парність.

Для пояснення співвідношень (2.4) і (2.6) розглянемо конкретний приклад побудови коректуючого коду. Нехай треба реалізувати код з $n = 63$, що виправляє двократні помилки $t_{\text{вп}} = 2$ ($d_0 = 5$). Тоді, згідно з (2.4),

$$2^{n-k} \geq \sum_{i=0}^2 C_{63}^i = 1 + 63 + 1953 = 2017.$$

Із нерівності $2^{n-k} \geq 2017$, що відповідає мінімальному значенню кількості перевірочних 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 (2.6) 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.

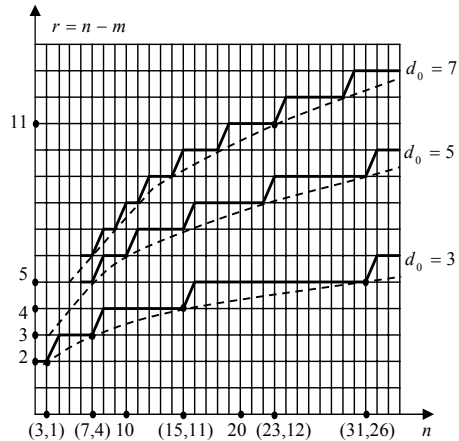


Рисунок 2.4 – Границі Хеммінга для блокових кодів з $d_0 = 3, 5, 7$

Звернемося тепер до умови (2.6), 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 перевірючих символів в (n, m) коді, для якого виконується гранична умова Варшавова-Гільберта, дорівнює 16. Таким чином, умова (2.6) гарантує можливість побудови коду (63, 47, 5).

Тепер, звертаючись до таблиць відомих коректуючих 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 коректуючої 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 Голя (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 (2.4) виконується зі знаком рівності

$$\sum_{i=0}^{t_{\text{вн}}} C_n^i = C_{23}^0 + C_{23}^1 + C_{23}^2 + C_{23}^3 = 1 + 23 + 253 + 1771 = 2048 = 2^{11}.$$

Код Голя займає важливе місце в середовищі досконалих кодів і є джерелом для багатьох досліджень в теорії кодування.

Матричне описання блокових кодів. Умови Варшавова 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 перевірючих елементів $B_{(n-m),m}$

$$G_{n,m} = \|I_{m,m} B_{(n-m),m}\| = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \alpha_{11} & \alpha_{12} & \dots & \alpha_{1(n-m)} \\ 0 & 1 & 0 & \dots & 0 & 0 & \alpha_{21} & \alpha_{22} & \dots & \alpha_{2(n-m)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 & \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{m(n-m)} \end{vmatrix}. \quad (2.7)$$

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:

$$\begin{aligned} A_2 \times G_{3,2} &= \|a_1 \ a_2\| \times \begin{vmatrix} 1 & 0 & \alpha_{11} \\ 0 & 1 & \alpha_{21} \end{vmatrix} = \begin{vmatrix} (a_1 \cdot 1) & (a_1 \cdot 0) & (a_1 \cdot \alpha_{11}) \\ (a_2 \cdot 0) & (a_2 \cdot 1) & (a_2 \cdot \alpha_{21}) \end{vmatrix} = \\ &= \|(a_1 \cdot 1) + (a_2 \cdot 0) \ (a_1 \cdot 0) + (a_2 \cdot 1) \ (a_1 \cdot \alpha_{11} + a_2 \cdot \alpha_{21})\| = \|a_1 \ a_2 \ b_1\|. \end{aligned}$$

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 перевірені символи b_1, b_2, \dots, b_{n-m} визначаються системою двійкових рівностей

$$b_j \equiv \left(\sum_{i=0}^m a_i \times \alpha_{ji} \right) \text{mod } 2, \quad (2.8)$$

а $j = 1, 2, 3, \dots, n - m$.

Система рівностей (2.8) використовується як алгоритм для побудови функціональної схеми кодера систематичного (n, m) коду, коректуюча здатність якого повністю визначається видом перевіреної під матриці

$$B_{(n-m),m} = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1(n-m)} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2(n-m)} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{m(n-m)} \end{vmatrix}. \quad (2.9)$$

Правило обчислення перевіренних символів за допомогою матриці $G_{n,m}$ за відомими інформаційними символами може бути записане у вигляді:

Перевірочна 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

$$H_{n,(n-m)} = \|B_{m,(n-m)} I_{(n-m),(n-m)}\|,$$

де $B_{m,(n-m)}$ – транспонована підматриця перевірочних 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 перевірочна матриця з використанням позначень згідно з (2.7) має вигляд:

$$H_{n,(n-m)} = \left\| \begin{array}{cccc|cccc} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1m} & 1 & 0 & 0 & \dots & 0 \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2m} & 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \alpha_{(n-m)1} & \alpha_{(n-m)2} & \dots & \alpha_{(n-m)m} & 0 & 0 & 0 & \dots & 1 \end{array} \right\|.$$

Розглянемо побудову перевірочної матриці на основі породжуючої матриці коду Хеммінга (7, 4)

$$G_{7,4} = \left\| \begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array} \right\|.$$

Перевірочна матриця при заданій породжуючій матриці має вигляд

$$H_{7,3} = \left\| \begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right\|.$$

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 помилки, що містить одиниці тільки на тих позиціях, які створюють кодові символи в прийнятій КК на транспоновану матрицю $H_{n,(n-m)}^T$, називається *синдромом*

$$D'_n \times H_{n,(n-m)}^T = S_{(n-m)}. \quad (2.10)$$

У розгорнутому вигляді вираз (2.10) можна подати так:

$$a'_1 a'_2 \dots a'_m b'_1 b'_2 \dots b'_{n-m} \times \begin{pmatrix} \alpha_{11} & \alpha_{21} & \dots & \alpha_{(n-m)1} \\ \alpha_{12} & \alpha_{22} & \dots & \alpha_{(n-m)2} \\ \dots & \dots & \dots & \dots \\ \alpha_{1m} & \alpha_{2m} & \dots & \alpha_{(n-m)m} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} = \|s_1 s_2 \dots s_{n-m}\|.$$

Неважко переконатися в тому, що елементи матриці-рядка синдрому визначаються таким чином:

$$s_j \equiv \left(\sum_{i=1}^m a'_i \times \alpha_{ji} + b'_j \right) \text{mod } 2, \quad (2.11)$$

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 встановлюється 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 $t_{\text{ном}} > (d_0 - 1)/2$, 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 відбутися.

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 коректующого коду (5, 3) з $d_0 = 2$, який має породжуючу $G_{5,3}$ і перевіряючу $H_{5,2}$ матриці:

$$G_{5,3} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \text{ и } H_{5,2} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

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 $G_{7,3}$.

2.1.2. Кодування і декодування при блокових кодах

Основу пристрою реалізації кодера вибраного коректуючого 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 кодеків коректуючих 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 Варшавова-Гільберта (2.6):

$$2^{n-m} \geq \sum_{i=0}^{d_0-2} C_{n-1}^i = \sum_{i=0}^1 C_6^i = 1 + 6 = 7.$$

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)

$$G_{7,4} = \left\| I_{4,4} \ B_{3,4} \right\| = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

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*:

$$B_{3,4} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

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 коректуючу здатність.

Використавши співвідношення (2.8) стосовно отриманої раніше матриці $G_{7,4}$, отримуємо 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 сформувати відповідні перевірочні символи КС

коду (7, 4). На рис. 2.5 наведена функціональна схема кодера, принцип роботи якої полягає в наступному.

На вхід кодера надходять інформаційні символи a_1, a_2, a_3, a_4 від джерела повідомлень. Як вхідний пристрій використовується демультимплексор 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 мультимплексором М, призначення якого полягає в комутації семи кодових елементів і видачі їх послідовно на вхід модулятора.

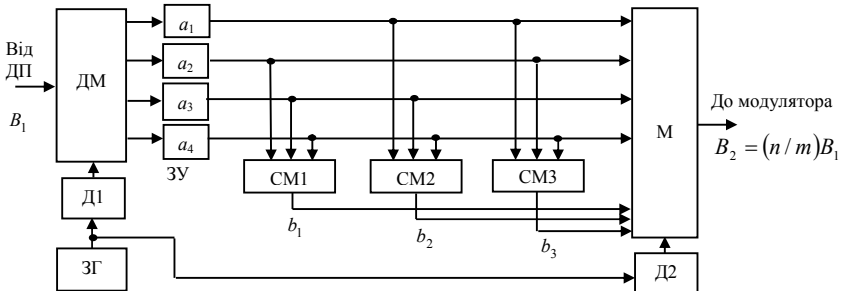


Рисунок 2.5 – Функціональна схема кодера блокового коду (7, 4)

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

$$f_r = \text{НЗК}(f_1, f_2),$$

де НЗК – найменше загальне 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. 2.6 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 демультимплексора і запам'ятовуючого пристрою; v – відображено формування перевірочних символів b_1, b_2, b_3 і на діаграмі c – наведено формат КС коректуючого коду (7, 4), швидкість модуляції якого $B_2 = B_1 n / k$

Побудова схеми декодера (n, k) коду. Найбільш очевидним загальним методом декодування коректуючих кодів є метод зіставлення прийня-

того 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 видалення перевіірочних 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).

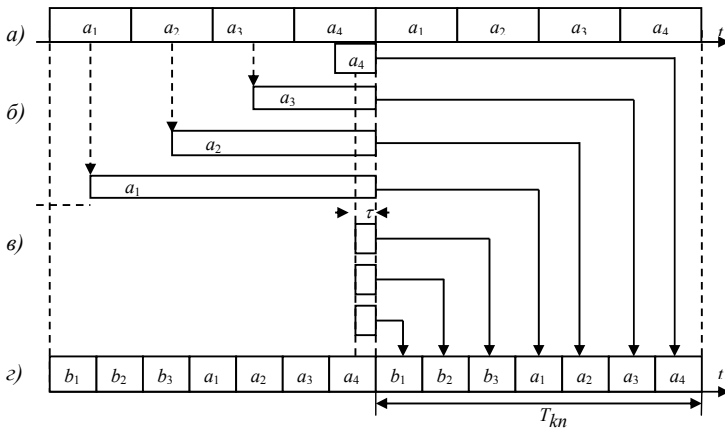


Рисунок 2.6 – Послідовність формування елементів коду (7, 4)

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 декодуванні згорткових кодів за алгоритмом Вітербі. Недоліком його при декодуванні блокових кодів є те, що для навіть не дуже великого значення t 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 (2.11), отримуємо систему двійкових рівностей для обчислення трибітової послідовності, яка є синдромом, або ознакою для корекції помилок:

$$\left. \begin{aligned} s_1 &= a_2 + a_3 + a_4 + b_1 \\ s_2 &= a_1 + a_3 + a_4 + b_2 \\ s_3 &= a_1 + a_2 + a_4 + b_3 \end{aligned} \right\} \text{mod } 2. \quad (2.12)$$

Для полегшення визначення значень синдрому, які відповідають різним однократним помилкам та іншим, будемо вважати, що по каналу передається нульове КС (нагадаємо, 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. Skorиставшись КС з однократними і деякими двократними помилками та системою рівностей (2.12), неважко визначити значення синдромів для деяких варіантів помилок. Результати отриманих значень синдромів при однократних і деяких багатократних помилках наведені в табл. 2.1.

Таблиця 2.1 – Таблиця синдромів коду (7, 4)

Можливі спотворені символи КК		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	1	0	0	1	0	0
	S_2	0	1	0	1	1	0	1	0	1	0	0
	S_3	0	1	1	0	1	0	0	1	1	1	0

Із табл. 2.1 бачимо, що синдром однозначно відповідає символам тільки при однократних помилках. Так, наприклад, при спотворенні двох кодових 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 ви-

явленні і виправленні помилок в межах коректуючої 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. 2.7. 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 mod2 – СМ1, СМ2 і СМ3. Підсумовування кодових символів КС виконується з урахуванням системи рівностей (2.12). 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 mod2 СМ4, СМ5, СМ6 і СМ7, на інші входи яких подаються одиничні сигнали для інвертування спотворених кодових символів у КС.

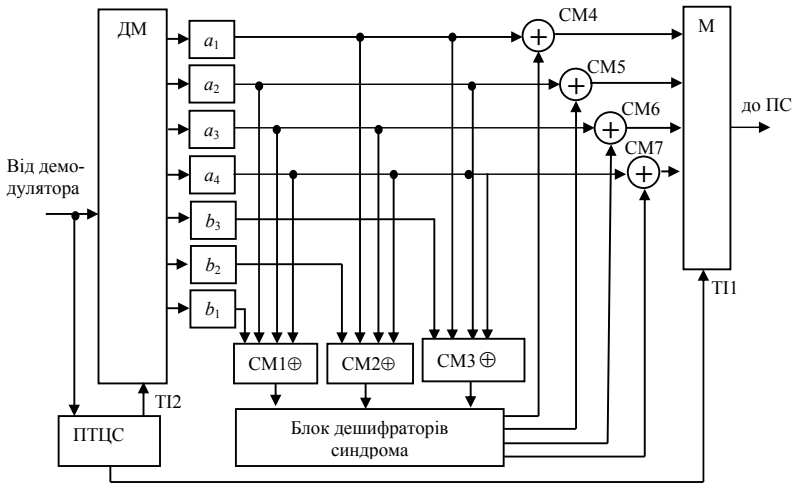


Рисунок 2.7 – Функціональна схема декодера блокового коду (7, 4)

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 дозволеними, що ускладнює схему декодера за великої значності коду.

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 дворові 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, коректуючих 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}	...	a_{1k_2}	$b_{1(k_2+1)}$	} Горизонтальні перевірки на парність
a_{21}	a_{22}	a_{23}	...	a_{2k_2}	$b_{2(k_2+1)}$	
...	
$a_{k_1 1}$	$a_{k_1 2}$	$a_{k_1 3}$...	$a_{k_1 k_2}$	$b_{k_1(k_2+1)}$	
$b_{(k_1+1)1}$ $b_{(k_1+1)2}$ $b_{(k_1+1)3}$... $b_{(k_1+1)k_2}$					$b_{(k_1+1)(k_2+1)}$	} Перевірки вер- тикальних і го- ризон- тальних 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. 2.8), а також інші помилки певної конфігурації, ймовірність утворення яких надто мала.

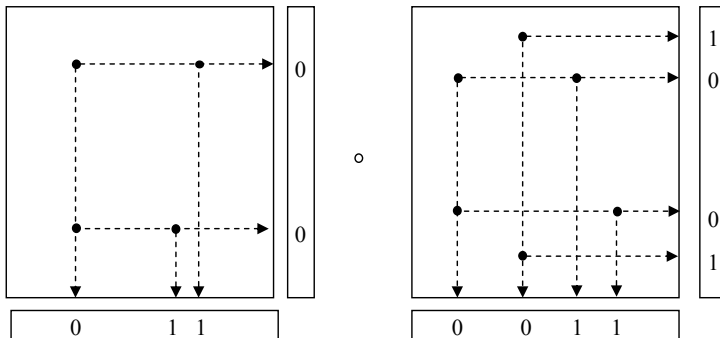


Рисунок 2.8 – Варіанти деяких малоімовірних виявлених, але не виправлених помилок

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

$$G_{3,2}^{(1)} = G_{3,2}^{(2)} = \begin{Bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{Bmatrix} = \begin{Bmatrix} A_1 \\ A_2 \end{Bmatrix},$$

що відповідає найпростішим кодам $(3, 2)$ з перевіркою на парність. 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 порожуючу 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. 2.9. 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.

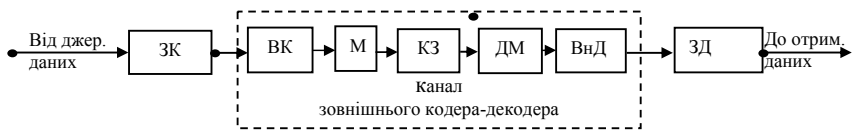


Рисунок 2.9 – Структурна схема кодера послідовного складового каскадного коду

2.1.3. Кореляційне трактування завадостійких кодів

Подання кодограм у вигляді векторів n -вимірного 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

$$\rho_{j\zeta} = \sum_{v=1}^n a_{vj} b_{v\zeta}, \quad (2.13)$$

де a_j , b_ζ – символи сигнальних конструкцій. Добуток

$$a_{vj} b_{v\zeta} = \begin{cases} +1 & \text{за } a_{vj} = b_{v\zeta}, \\ -1 & \text{за } a_{vj} \neq b_{v\zeta}. \end{cases} \quad (2.14)$$

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

$$\Delta\rho = \rho_{jj} - \rho_{j\zeta} \quad (2.15)$$

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

$$\Delta\rho_{\min} = \rho_{jj} - \rho_{j\delta} \quad (2.16)$$

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 $\Delta\rho_{\min} = 2$.

Значимо, 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 (2.16) величина $\Delta\rho_{\min} = 6$. Для корекції r помилок необхідно мати

$$\Delta\rho_{\min} = 4r + 2.$$

Це ілюструється рис. 2.10. 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

$$m \leq n - \log_2 \sum_{v=0}^{\alpha} C_n^v, \quad (2.17)$$

де параметр $\alpha = \frac{\mu - 1}{2}$.

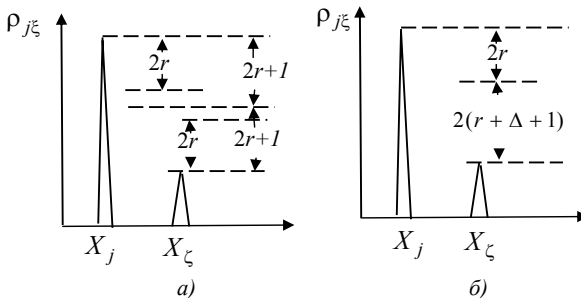


Рисунок 2.10 – Кореляційне трактування виправлення помилок

Якщо $\Delta\rho_{\min} = 2\mu + 2$, то обчислення здійснюються відповідно до виразу (2.17), 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 $\Delta = 1$, $\Delta\rho_{\min} = 12$, $\mu = 5$, $\nu = 2$, $n = 8$. 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 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. 2.11)

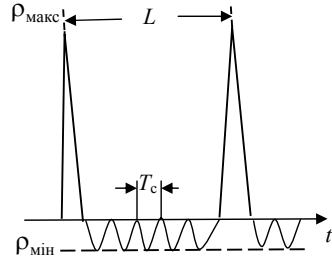


Рисунок 2.11 – До визначення коефіцієнта ρ

$$\rho_{1\max} = 2^l - 1;$$

$$\rho_{2\max} = 2^l - 1;$$

$$\rho_{\min} = -1.$$

Величина ρ_{\max} відповідає часовому зсуву $\tau = 0$, причому значення $\rho_{2\max}$ отримується при незвідних поліномах $g(x)$ і $h(x)$, а значення $\rho_{1\max}$ – при $g(x)$ незвідному й $h(x)$ звідному поліномах. Одиначна помилка зменшує ρ_{\max} на дві одиниці і змінює (зменшує або збільшує при даному τ) ρ_{\min} , тому в найгіршому разі $\Delta\rho_{\min} = 2^l$ 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, $\rho_{\max} = 7$, $\rho_{\min} = -1$, $r = 1$.

Двійкові коди для каналів зі стиранням помилок. У випадку каналу зі стиранням символів коефіцієнт кореляції між кодограмами

$$\rho_{j,\zeta} = \sum_{\nu \neq l \neq i}^n a_{i,j} b_{i,\zeta} + b_{\nu,\zeta} \delta_{\nu,j} + a_{i,j} \delta_{i,\zeta}, \quad (2.18)$$

де символ стирання δ задовольняє умові $\delta a_{i,j} = \delta b_{\nu,\zeta} = 0$. 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

$$\Delta\rho_{\min} = 2(2r + \Delta + \varepsilon + 1).$$

Коди з основою $a > 2$. При $a > 2$ задача 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: $\rho_{1,1} = 27$; $\rho_{2,2} = \rho_{3,3} = \dots = \rho_{7,7} = 19$; $\rho_{8,8} = \rho_{9,9} = \dots = \rho_{19,19} = 11$; $\rho_{20,20} = \rho_{21,21} = \dots = \rho_{27,27} = 3$; $\rho_{1,2} = \rho_{1,3} = \rho_{1,4} = 21$; $\rho_{1,5} = \rho_{1,6} = \dots = \rho_{1,10} = 15$; $\rho_{1,11} = \rho_{1,12} = \rho_{1,13} = \rho_{1,21} = \rho_{1,22} = \rho_{1,23} = 3$; $\rho_{1,14} = \rho_{1,15} = \dots = \rho_{1,20} = 9$; $\rho_{1,24} = \rho_{1,25} = \dots = \rho_{1,26} = -3$; $\rho_{1,27} = -9$.

Величина $\Delta\rho$ завжди парна. Тому для будь-яких m і q отримаємо

$$\Delta\rho_{\min} = 2q(m-1)(2r + \Delta + \varepsilon + 1)$$

2.1.4. Способи побудови двійкових циклічних кодів

У цьому підрозділі розглядається важливий підклас лінійних двійкових блокових кодів, в який входять прості, з точки зору розширення циклічні поліномінальні 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 поліномінальній 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 інформацій-

них символів, яка підлягає кодуванню ЦК, а $F(x) = x^{n-1} + x^{n-2} + \dots + 1$ – є КК в поліноміальній формі ЦК.

Визначення 1. 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 $\rightarrow 1 + x^3 + x^5 + x^6$.

$$x \times (1 + x^3 + x^5 + x^6) = \begin{array}{r|l} x + x^4 + x^6 + x^7 & x^7 + 1 \\ \underline{x^7 + 1} & 1 \\ 1 + x + x^4 + x^6 & \rightarrow 1100101 \end{array}$$

Тепер необхідно з'ясувати умови завдання і побудови циклічного коду. Відповідь на це в першу чергу дає теорема 3.

Теорема 3. 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. 2.2.

Таблиця 2.2 – 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. 2.2 бачимо, що некоректуючий семизначний код (7, 7) є одним випадком ЦК з $\rho = 0$ і $d_0 = 1$, тобто при значенні $G(x) = 1$. Наступний код (7, 6) з породжуючим багаточленом $G(x) = x + 1$ є найпростішим коректуючим 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 коректуючою 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 дозволені КС є 0000000 і 1111111. На закінчення зазначимо, що з підвищенням степеня $G(x)$ при фіксованому n коректуюча здатність ЦК підвищується.

Циклічні коди Хеммінга. Кодами Хеммінга називають лінійні блокові (n, m) коди з $d_0 = 3$, що задовольняють умові (2.4) 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. 2.3 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 2.3 – Параметри деяких ЦК Хеммінга

Вісітковий 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. 2.3, 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 $t > t_{\text{вн}}$, що виходить із формули Бернуллі

$$P_t = C_n^t p_0^t (1 - p_0)^{n-t}$$

На рис. 2.12 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).

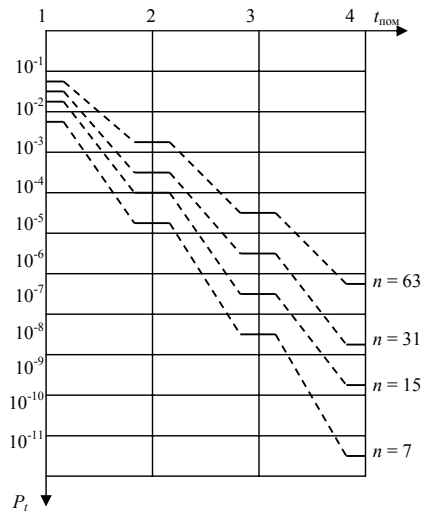


Рисунок 2.12 – Діаграма залежності ймовірності утворення t -кратних помилок при $p_e = 10^{-3}$

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 $G_1(x) = x^3 + x + 1$.

$$\begin{array}{r} x^6 \\ \underline{x^6 + x^4 + x^3} \\ x^4 + x^3 \\ \underline{x^4 + x^2 + x} \\ x^3 + x^2 + x \\ \underline{x^3 + x + 1} \\ x^2 + 1 \end{array} \rightarrow \begin{array}{r} x^3 + x + 1 \\ x^3 + x + 1 \\ 101 \end{array}$$

$$x^5 \bmod G_1(x) = x^2 + x + 1 \rightarrow 111, \quad x^4 \bmod G_1(x) = x^2 + x \rightarrow 110, \\ x^3 \bmod G_1(x) = x + 1 \rightarrow 011.$$

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 перевірочної 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

$$H_{7,3} = \begin{vmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{vmatrix} \text{ або } H_{7,3} = \begin{vmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}.$$

Таким чином, при розгляді ЦК аналогом породжуючої матриці $G_{7,4}$ є породжуючий багаточлен $G_1(x)$, а перевіркою 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 4. Породжуючий багаточлен $G(x)$ кодів БЧХ с параметрами (n, m) і $d_{\text{БЧХ}} = 2t_{\text{вп}} + 1$ визначається виразом

$$G(x) = \text{НЗК} [\mu_1(x), \mu_3(x), \mu_5(x), \dots, \mu_{\text{БЧХ}-2}(x)], \quad (2.19)$$

де НЗК – найменше загальне 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 коректуюча здатність коду. Розглянемо приклад, який дозволяє безпосередньо розв'язати ту або іншу задачу, не використовуючи додаткову літературу.

Приклад 6. 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) вписати 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 (2.19) 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. 2.3.

Із табл. 2.4 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 $\text{GF}(2^5)$ $\beta^0 \rightarrow 00010$. 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 2.4 – 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. 2.4 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 коректуючу 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.

2.1.5. Технічні засоби кодування і декодування циклічних кодів

Лінійні кола з кінцевим числом станів. Основу пристроїв, використовуваних при двійковому кодуванні і декодуванні, складають *лінійні перемикальні* схеми, що імітуються іноді *багатотактними лінійними фільтрами Хаффмена*, або *регістрами зсуву з лінійними зворотними зв'язками*, які виконуються на дискретних елементах з двома станами. Основними компонентами цих схем є: комірки пам'яті (тригери), запам'ятовуючі на необхідне число тактів кодові символи та суматори за модулем 2.

Процес кодування і декодування при схемній реалізації кодеків циклічних кодів базується на застосуванні вище згаданих регістрів зсуву зі зворотним і незворотним зв'язком, які в цьому випадку виконують головну роль. Тому що операція ділення багаточленів з коефіцієнтами в полі $GF(2)$ є основною в кодері ЦК, то треба показати, як вона реалізується на практиці.

Визначення структури перевірочних символів для захисту від помилок. При кодуванні циклічним кодом з метою формування додаткових символів треба виконати ділення добутку багаточлена $A(x)$ і одночлена на x^{n-m} на породжуючий багаточлен $G(x)$ згідно з виразом

$$A(x) \times x^{n-m} / G(x) = Q(x) + R(x) / G(x),$$

де $Q(x)$ – одиничне, а $R(x)$ – багаточлен, що відповідає перевірочним символам. Операцію ділення можна виконати без попереднього множення $A(x)$ на x^{n-m} , застосувавши схему, показану на рис. 2.13. У цій схемі цикл ділення скорочується, тому що інформаційні символи $A(x)$ накопичуються в $(n-m)$ -розрядний регістр з боку виходу старшої комірки пам'яті x^2 . При цьому операція ділення $A(x) \times x^{n-m}$ на $G(x)$ завершується на останньому такті введення $A(x)$.

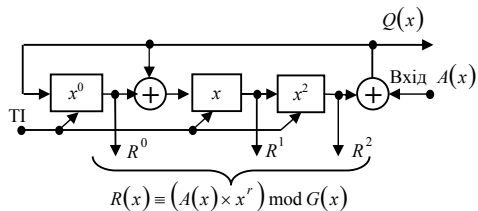


Рисунок 2.13 – Схема ділення для формування перевірочних біт КС ЦК

У цьому легко переконатися на конкретному прикладі інформаційної послідовності біт 1101, тобто $A(x)x^3 = (x^3 + x^2 + 1)x^3 = x^6 + x^5 + x^3$ і $G(x) = x^3 + x + 1$. Виконавши ділення стовпчиком, отримаємо частку $Q(x) = x^3 + x^2 + x + 1$ і остачу $R(x) = 1$, що відповідає перевірочним бітам 001.

Схема ділення реалізується шляхом зсуву праворуч на кожному такті з урахуванням підсумовування кодових біт, введених в регістр x^0, x, x^2 , і фіксованих нових біт, що утворилися згідно з правилом:

$$x^0 \equiv A(x) + \hat{x}^2; \quad x \equiv A(x) + \hat{x}^2 + \hat{x}; \quad x^2 \equiv \hat{x},$$

де \hat{x}^2 і \hat{x} – зміст комірки пам'яті регістру на попередніх тактах. Етапи і результат ділення за допомогою обладнання за схемою рис. 2.13 наведені в табл. 2.5.

Таблиця 2.5 – Ілюстрація роботи схеми згідно з рис. 2.13

№ ТП	Стан регістру			Вхід дільника $A(x)$	Частка $Q(x)$
	x^0	x	x^2		
	0	0	0	0	0
1	1	1	0	1	1
2	1	0	1	1	1
3	1	0	0	0	1
4	1	0	0	1	1

←----- $R(x) = 1$ ----->

У схемі ділення для коду (7, 4) процес обчислення $R(x)$ закінчується на 4-му такті, тому що степінь $A(x)$ не перевищує 3.

Обчислення синдрому для контролю помилок. Розглянемо схему ділення, яка знаходить застосування при декодуванні ЦК. Щоб усвідомити процес ділення багаточленів, розділимо звичайним способом, тобто стовпчиком багаточлен прийнятої із каналу КК $F(x) = x^4 + x^2 + 1$ на породжуючий багаточлен $G(x) = x^3 + x + 1$.

$$\begin{array}{r} x^4 + x^2 + 1 \\ x^4 + x^2 + x \\ \hline 0 + 0 + x + 1 \end{array} \quad \left| \begin{array}{r} x^3 + x + 1 \\ x \end{array} \right.$$

Тут $Q(x) = x$ – частка і $S(x) = x + 1$ – остача, за mod $G(x)$. Схема пристрою $F(x)$ на $G(x)$ зображена на рис. 2.14.

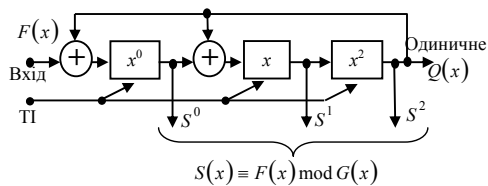


Рисунок 2.14 – Схема ділення для формування синдромних біт прийнятої КК ЦК

Схемою ділення реалізується аналогічно раніше розглянутому дільнику (рис. 2.13) при кодуванні КК циклічним кодом з урахуванням алгоритму обчислення вмісту комірок пам'яті регістру:

$$x^0 \equiv F(x) + \hat{x}^2; \quad x \equiv \hat{x}^0 + \hat{x}^2; \quad x^2 = \hat{x}.$$

Етапи ділення і результат наведені в табл. 2.6.

Вміст комірок пам'яті регістра x^0, x, x^2 після подання 7-го ТІ визначають біти синдрому переданої за каналом зв'язку КК.

Таблиця 2.6 – Ілюстрація роботи схеми згідно з рис. 2.14

№ ТІ	Вхід дільника $F(x)$	Стан регістру			Одиничне $Q(x)$
		x^0	x	x^2	
1	0	0	0	0	0
2	0	0	0	0	0
3	1	1	0	0	0
4	0	0	1	0	0
5	1	1	0	1	1
6	0	1	0	0	0
7	1	1	1	0	0

Особливістю пристрою ділення багаточленів зі зворотним зв'язком є те, що, якщо $F(x)$ або $A(x) \times x^{n-m}$ не ділиться без остачі на $G(x)$, то комірки пам'яті при подачі скільки завгодно великого числа нульових символів не обнулюються. В цьому випадку вміст їх буде періодично повторюватися за законом проходження елементів розширеного поля Галуа $GF(2^3)$, визначеного примітивним багаточленом $G(x)$ степеня 3. Іншими словами, пристрій перетворюється в генератор псевдовипадкової послідовності (ПВП) з періодом, що дорівнює $2^3 - 1$ символів.

Процедура кодування без попереднього обчислення перевірючих символів. Кодування циклічного (n, m) -коду може бути виконане за допомогою регістру зсуву з m комірками пам'яті і суматорами за $\text{mod } 2$, які включені в коло зворотного зв'язку. На рис. 2.15 зображена лінійна перемикаюча схема з кінцевим числом станів, з'єднання в якій відповідає перевірючому багаточлену $H(x)$ циклічного коду. Перші k символів на виході схеми будуть інформаційними, а останні $(n - m)$ символів – перевірючими. Інформаційна послідовність a_0, a_1, \dots, a_{k-1} вводиться в схему паралельним способом.

Пристрій множення без зворотного зв'язку з послідовно ввімкненими суматорами за $\text{mod } 2$ знаходять застосування у виді схемної або програмної реалізації при циклічному кодуванні.

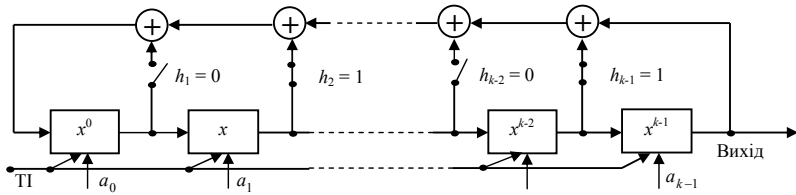


Рисунок 2.15 – Схема формування КС систематичного ЦК

2.1.6. 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 ($l_n = 2$) 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 загальне кратне чисел ξ і $\beta = 2^\alpha - 1$:

$$n = \text{НЗК}(2^\alpha - 1, \xi)$$

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 7. Побудуємо породжуючий поліном коду Файра, що має такі властивості: $l_{\text{п вп}} = 3$, $l_{\text{п в}} = 0$, $p(x) = 1011$. Величини $\mu = 3$; $\beta = 7$, $\alpha = l_{\text{п в}} = 3$; $\xi = 2$; $n = \text{НСК}(7, 2) = 14$; $k = 9$; $l = 5$; 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 кожна кодограма X_j передається μ разів, у результаті чого послідовність символів має вигляд

$$\frac{x_1 x_2 \dots x_n}{1} \quad \frac{x_1 x_2 \dots x_n}{2} \quad \dots \quad \frac{x_1 x_2 \dots x_n}{\mu}.$$

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 перевірконою матрицями

$$G^{(2)} = \|E_n, E_n\|; \quad H^{(2)} = \left\| \begin{matrix} E_n \\ E_n \end{matrix} \right\|,$$

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

$$G^{(3)} = \|E_n E_n E_n\|; \quad H^{(3)} = \begin{Bmatrix} E_{2n} \\ E_n E_n \end{Bmatrix},$$

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

$$N_r(v) = 3^{v-r} C_n^r \sum_{j=0}^{\varepsilon} 3^{-2j} C_r^j C_{n-r}^{v-(2r+j)}, \quad (2.20)$$

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, незбіжних 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 по-

милки, 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

$$N'_r(v) = 3^{v-r} C_n^r \sum_{j=0}^{\alpha} 3^{-2j} C_r^j C_{n-r}^{v-(2r+j)}, \quad (2.21)$$

де $\alpha = \left\lceil \frac{v-r-M_0}{2} \right\rceil$ – найближче більше ціле число.

Формула (2.21) виходить із (2.20): 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 (2.21) 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 Δr_{\min} . Укрупнюючи інформаційні символи, отримуємо

$$k_y \leq n_y - \log_2 \sum_{v=0}^{\alpha} C_{n_y}^v, \quad (2.22)$$

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

$\Delta r_{\min} = 2\mu$ ($\mu = 3, 5, 7, \dots$). При $\Delta r_{\min} = 2\mu + 2$ обчислення здійснюються за

формулою (2.22), а потім значення n_y збільшується на одиницю (якщо $\Delta\rho_{\min} = 4$, то $n_y = k_y + 1$). Остаточно значність кодограми

$$n = (n_y - 1)l_{\Pi} + k_{y_0},$$

де k_{y_0} – значність останнього укрупненого інформаційного символу.

Приклад 8. 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 9. 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 передану 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:

$$\rho_{3',1} = \rho_{3',5} = \rho_{3',6} = \rho_{3',7} = -2; \rho_{3',2} = \rho_{3',4} = -4; \rho_{3',3} = +2, \rho_{3',8} = 0.$$

Величина $\rho_{3',3} > \rho_{3',j}$, що свідчить про передачу кодограми 0011101.

Приклад 10. 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 $k_y = 19$; $n_y = 23$; $n_b = 69$ 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 $n_o > n_b$, 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

$l_{\text{пв}} > l_{\text{пвп}}$. У цьому випадку значність коду n необхідно вибирати з умови виправлення пакета помилок $l_{\text{пвп}}$ і потім з умови виявлення пакета помилок $l_{\text{пв}}$ визначити нову значність коду n' . Якщо

$$n = n' \geq 2l_{\text{пв}} - 1, \quad (2.23)$$

то код значності n буде відповідати поставленим вимогам; якщо ж $n - n' < 2l_{\text{пвп}} - 1$, то значність коду треба збільшити, щоб виконувалася нерівність (2.23). 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 впливає умова (2.23).

Приклад 11. Даний (70, 57)-код, що виправляє пакет помилок $l_{\text{пвп}} = 3$. Визначимо його виявляючі властивості. Відповідно до формули (2.23) $n' = 65$. 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.

2.1.7. Кодування в реальному масштабі часу

На жаль, в літературі, де розглядаються питання завадостійкого кодування, під кодером ЦК часто розглядають тільки пристрої для формування перевірочних символів. Це не розкриває по суті того, як формується закодований сигнал і, як виконується неперервне його передавання каналами зв'язку. Для цілісного уявлення про те, що собою являє кодер коректующого коду, необхідно розглянути ще ряд пристроїв, за допомогою яких виконується запис інформаційних символів під час формування перевірочних, а також пристроїв для узгодження швидкостей передавання вхідних і вихідних символів на виході кодера.

Усі відомі кодуєчі пристрої ЦК виконуються на регістрах зсуву, які можна звести до двох типів схем, а саме до схем, де реалізується процес ділення на породжуючий багаточлен $G(x)$, або де використовується регістр зсуву з зворотним зв'язком, побудованим з урахуванням перевірочного багаточлена $H(x)$.

Побудова схеми кодера на основі породжуючого багаточлена. Процедура формування кодових слів при циклічному кодуванні в систематичному вигляді

$$F(x) = A(x)x^{n-k} + R(x),$$

де $A(x)$ – багаточлен інформаційних символів степеня $m-1$; $R(x)$ – багаточлен, визначаючий послідовність перевірочних символів з урахуванням інформаційних. Інформаційні символи в результаті множення $A(x)$ на x^{n-m} переміщуються в область старших розрядів, звільняючи при цьому місце для перевірочних символів. Переконалися в цьому можна, виконавши операції ділення і множення згідно з останнім виразом на прикладі коду (7, 4) при $A(x) = x^3 + x^2 + 1$ і $G(x) = x^3 + x + 1$.

Структурна схема кодера ЦК наведена на рис. 2.16, яка складається із: ДП – джерела повідомлень, швидкість модуляції якого B_1 ; БУШП – блока узгодження швидкості передавання ДП і закодованого сигналу; УФПС – схеми формування перевірочних символів; ЗГ – задаючий генератор; П – дільника частоти, формуючого когерентні коливання для синхронізації ДП і УФПС, а також БЧУ – блока часового ущільнення інформаційних і перевірочних символів, що забезпечують неперервну передачу закодованого повідомлення з лінійною швидкістю модуляції $B_2 = nB_1/m$.

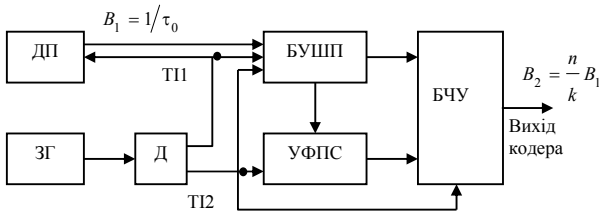


Рисунок 2.16 – Структурна схема кодера циклічного коду

Розглянемо тепер функціональну схему кодера (рис. 2.17) з використанням формувача перевірочних символів, який містить регістр затримки зі зворотним зв'язком. Схема регістра РГ3 у відповідності з $G(x) = x^3 + x + 1$ докладно розглянута у підрозділі 2.1.5 (рис. 2.15). Наведена схема містить буферний регістр РГ1, швидкість заповнення якого визначається П1 з частотою $f_1 = B_1$, і вихідний регістр РГ2. Перезапис вмісту РГ1 в РГ2 здійснюється паралельним способом, а зчитування із РГ2 відбувається послідовно під дією П2 з частотою $f_2 = f_1 n/m$. Керуюче обладнання містить лічильник ЛЧ тактових імпульсів П2 з додатковим входом R для скидання комірок пам'яті в нульовий стан імпульсом перезапису з РГ1 в РГ2. Ємність лічильника для коду (7, 4) дорівнює 4. RS -тригер призначений для формування сигналів управління ключа Кл в колі зворотного зв'язку РГ3 і електронного перемикача ЕП, який знаходиться в положенні 1 під час передачі в канал інформаційних символів, і в положенні 2, коли формуються перевірочні символи.

На рис. 2.18 наведені часові діаграми формування закодованого кодового слова циклічним кодом. Для інших (n, m) -кодів кодер, що забезпечує кодування систематичним кодом в реальному масштабі часу, з іншими значеннями надлишковості ρ і кодів з виправленням багаторазових помилок може бути побудований за таким самим принципом, що і для розглянутого випадку.

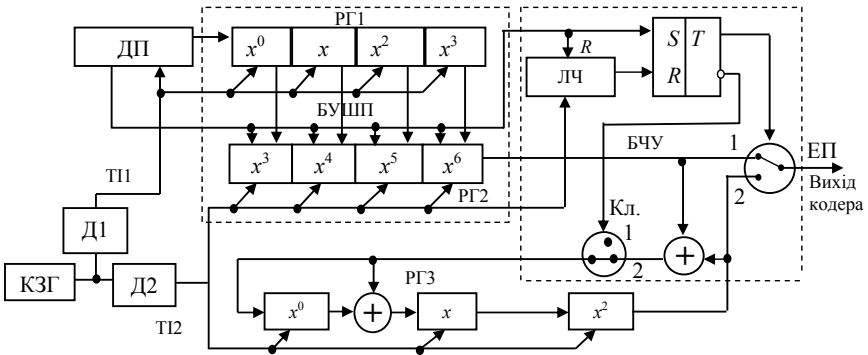


Рисунок 2.17 – Функціональна схема кодера циклічного коду (7, 4)

Побудова кодера на основі перевірного багаточлена. Другий спосіб кодування базується на понятті перевірного багаточлена $H(x) = (x^n + 1)/G(x)$.

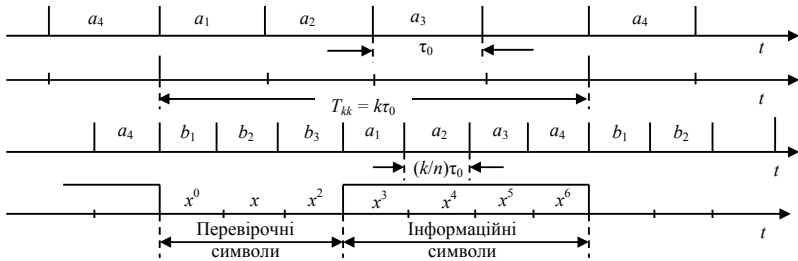


Рисунок 2.18 – Часові діаграми при формуванні КК ЦК (7, 4)

У такому кодері для формування систематичного коду як регістр зсуву зі зворотним зв'язком використовується пристрій (див. рис. 2.24), який складається із m комірок пам'яті і зовнішніх суматорів за $\text{mod } 2$, ввімкнених в коло зворотного зв'язку. Побудова кодера з урахуванням перевірного багаточлена $H(x)$ для коду (7, 4) визначається виразом

$$h(x) = \sum_{i=0}^{m-1} h_i x^i = h_0 + h_1 x + h_2 x^2 + h_3 x^3.$$

Розглянемо конкретну схему кодера на прикладі перевірного багаточлена $H(x) = (x^7 + 1)/(x^3 + x + 1) = x^4 + x^2 + x + 1$. У цьому прикладі коефіцієнти h_i набувають наступні значення: $h_0 = 0$, $h_1 = 1$, $h_2 = 1$, $h_3 = 1$. Функціональна схема кодера наведена на рис. 2.19. У такому кодері комірки пам'яті регістра РГ2 зберігають до початку кодування інформаційні символи, причому старшим розрядам відповідають комірки x^3 і x^2 , а молодшим – x і x^0 , яким відповідають степені багаточлена $F(x)$ x^6, x^5, x^4 і x^3 . В табл. 2.7 наведені стани комірок пам'яті на кожному такті кодування інформаційних символів, які представлені в поліноміальній формі $A(x) = x^3 + x^2 + 1$.

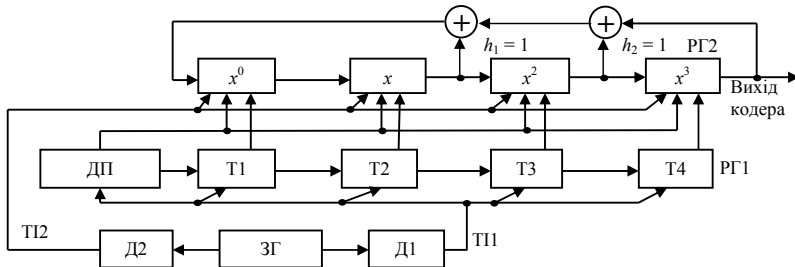


Рисунок 2.19 – Функціональна схема кодера на основі перевірного багаточлена

$$H(x) = x^4 + x^2 + x + 1$$

Таблиця 2.7 – Ілюстрація процесу формування КС кодером на основі $H(x)$

ТІ	$x^0 = \mathcal{E} + \mathcal{E}^2 + \mathcal{E}^3$	x	x^2	x^3	x^i	Інформаційні символи
0	1	0	1	1	x^6	
1	0	1	0	1	x^5	
2	0	0	1	0	x^4	
3	1	0	0	1	x^3	Перевірочні символи
4	1	1	0	0	x^2	
5	1	1	1	0	x	
6	0	1	1	1	x^0	

Робота кодера починається з того, що після завантаження інформаційних символів у буферний регістр РГ1 вміст його імпульсом циклової синхронізації (КС) від джерела повідомлення переноситься паралельним способом в кодувальний регістр РГ2. З цього регістру символи КС зчитуються зі швидкістю $B_2 = nB_1/m$ і надходять на вихід кодера. Першими чотирма тактовими імпульсами виводяться інформаційні символи, а потім трьома – перевірочні. Далі цей процес періодично повторюється для інших КС.

Виконавши перевірку сформованого КС можна перекоонатися, що $(x^6 + x^5 + x^3 + 1) \bmod (x^3 + x + 1) \equiv 0$, тобто в правильності процесу кодування.

Відзначимо, що кодери, побудовані на базі утворюючих або перевірочних багаточленів, рівноцінні за структурою вихідного сигналу. Однак, зіставляючи функціональні схеми розглянутих кодерів ЦК з точки зору їх практичного застосування, перевагу слід надати останній, тому що в ній міститься менше регістрів, не потребують допоміжні пристрої.

Ефективність блокових кодів. Перш ніж вирішити питання щодо ефективності спільного використання блокових кодів і таймерних сигналів, необхідно оцінити ефективність надлишкових блокових кодів, що використовуються у реальних каналах зв'язку при розрядно-цифровому кодуванні.

Ефективність застосування коректуючого коду в режимі виправлення помилок можна визначити через коефіцієнт підвищення достовірності:

$$\eta \approx \frac{P(\geq 1, n)}{P(\geq 1, n) - P_{\text{вп}}(n)}, \quad (2.24)$$

де $P(\geq 1, n)$ – ймовірність прийому n -елементної кодової комбінації з однією й більше помилками; $P_{\text{вп}}(n)$ – ймовірність прийому n -елементної комбінації з помилками, які виправляють деяким (n, m) -кодом.

Вибір величини η для оцінки ефективності застосування коду обумовлено простотою її обчислення, а також тим, що ця величина легко перераховується у відповідне відношення еквівалентних ймовірностей η_e .

Наприклад, при $P(\geq 1, n) \ll 1$ $\eta_e \approx \frac{m}{n} \eta$, тому що без застосування коректую-

чого коду $p_e \approx \frac{P(\geq 1, n)}{n}$, а при використанні коректуючого коду –

$p_e \approx \frac{P(\geq 1, n) - P_{\text{вп}}(n)}{m}$. Крім того, через те, що $\eta > \eta_e$, при малій величині η

можна свідчити про неефективність коду й без визначення величини η_e .

Для кодів, що виправляють помилки кратності $t_{\text{вп}}$ й менше,

$$\eta = \frac{P(\geq 1, n)}{P(\geq t_{\text{вп}} + 1, n)}. \quad (2.24a)$$

На рис. 2.20 наведено графіки залежності $\eta = f(t)$ для різних значень n , отримані на підставі експериментальних даних для телефонного кабельного каналу ($p = 3,07 \cdot 10^{-4}$; $\alpha = 0,613$).

Із графіків видно, що для даних каналів застосування коду в режимі виправлення помилок при $n \leq 511$ не призводить до підвищення достовірності більш ніж у 10 разів.

Для кодів, що виправляють пакети помилок довжиною λ і менше елементів,

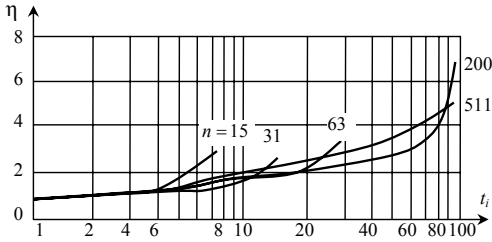


Рисунок 2.20 – Залежність $\eta = f(t_i)$ для телефонного кабельного каналу

елементності коду за різних значень відношення $m/n = 0,2; 0,5; 0,8$.

Отже, коди, що виправляють пакети помилок у цих каналах за $n < 511$, також не забезпечують помітного підвищення достовірності.

Розглянемо вплив на ефективність декореляції помилок. Якщо з послідовності помилок e_1, e_2, e_3, \dots виділити послідовність елементів $e_{\nu j+i}$ ($\nu = 1, 2, 3, \dots$), то отриману послідовність $e_i, e_{j+1}, e_{2j+1}, \dots$ так само, як і первинну, можна характеризувати параметрами p і α . Тут ν – номер елемента в отриманій послідовності, а $\nu j + i$ – номер цього елемента у вихідній послідовності. При збільшенні j параметр p не змінюється, а показник групування α зменшується. Починаючи з деякого значення $j = j_1$, помилки в отриманій послідовності можна вважати практично незалежними. Величини j_1 різні для різних каналів зв'язку.

Якщо передавати кодові комбінації так, щоб помилки, що впливають на окремі їхні елементи, були практично незалежними, то можна отримати значне збільшення досивірності при малих довжинах кодових комбінацій і виправленні помилок малої кратності.

Розмістимо n елементів деякого блока, складеного з j n_1 -елементних ($n = j n_1$) комбінацій (рис. 2.22), у вигляді матриці з j рядків і n_1 стовпців. Індекси елементам припишемо так, щоб вони відповідали порядку передавання елементів у канал зв'язку. Тоді при $j \geq j_1$ можна вважати, що на елементи будь-якого рядка матриці діють практично незалежні помилки. Отже, якщо вибрати як рядки матриці вектори деякого групового (n_1, m_1) -коду, то ймовірність помилкового декодування буде зменшуватися зі збі-

$$\eta_n = \frac{P(\geq 1, n)}{P_n(\geq \lambda, n)}. \quad (2.24б)$$

Через те, що при $\lambda = t = x$

$$P_n(x+1, n) \geq P(x+1, n),$$

то

$$\eta_n \leq \frac{P(\geq 1, n)}{P_n(\geq \lambda + 1, n)}.$$

На рис. 2.21 наведена залежність коефіцієнта η від

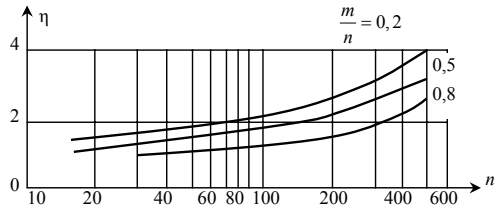


Рисунок 2.21 – Залежність $\eta = f(t_i)$ для телефонного кабельного каналу

льшенням j і при $j \geq j_1$ наближатися до ймовірності помилкового декодування в каналі з незалежними помилками.

Необхідно відзначити, що при збільшенні j відносна швидкість передавання не змінюється, через те що $R = m/n = jm_1/jn_1 = m_1/n_1$, а лише змінюється ємність пам'яті приймача й передавача, яка дорівнює jn_1 двійкових елементів, і зростає час затримки інформації, який дорівнює за будь-яким повідомленням довжині $l \leq jm_1$

$$t(l) = jn_1 t_0 + t_p + t_{ак}.$$

Виграш за достовірністю, який отримується при декореляції й виправленні помилок кратності t ,

$$\eta_d = \frac{P(\geq 1, n_1)}{P_d(\geq t+1, n_1)} = \eta\theta,$$

де $P_d(\geq t+1, n_1)$ – ймовірність появи n -елементної комбінації з помилкою кратності $t+1$ і більше в послідовності помилок, яку отримуємо після їх декореляції; $\eta = P(\geq 1, n_1) / P(\geq t+1, n)$ – виграш за достовірністю, який отримуємо при виправленні помилок кратності t без декореляції; $\theta = P(\geq t+1, n) / P_d(\geq t+1, n_1)$ – виграш за достовірністю, який отримуємо за рахунок декореляції помилок.

$$\begin{vmatrix} a_1 & a_{j+1} & a_{2j+1} & \dots & a_{(n_1-1)j+1} \\ a_2 & a_{j+2} & a_{2j+2} & \dots & a_{(n_1-1)j+2} \\ \dots & \dots & \dots & \dots & \dots \\ a_j & a_{2j} & a_{3j} & \dots & a_{n_1j} \end{vmatrix}$$

Рисунок 2.22 – Матриця елементів при декореляції помилок

Максимальний виграш за достовірністю, який можна отримати при повній декореляції ($j \geq j_1$) і виправленні помилок, дорівнює

$$\eta_{\max} = \frac{P(\geq 1, n_1)}{\sum_{i=t+1}^{n_1} C_{n_1}^i p^i (1-p)^{n_1-i}}, \quad (2.24в)$$

де p – ймовірність помилкового прийому символу.

Максимальний виграш за достовірністю, який одержується за рахунок декореляції помилок при $j \geq j_1$, визначається як

$$\theta_{\max} = \frac{P(t+1, n_1)}{\sum_{i=t+1}^{n_1} C_{n_1}^i p^i (1-p)^{n_1-i}}.$$

На рис. 2.23 показані графіки залежностей η , η_d і θ від j, n і $t_{вп}$ для телефонного каналу.

З наведеного бачимо ефективність декореляції помилок на якість передачі.

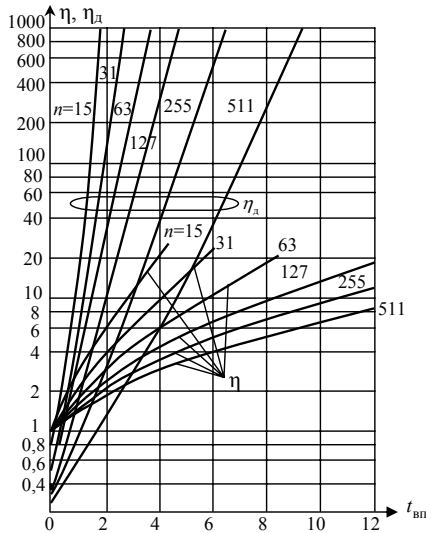


Рисунок 2.23 – Залежність виграшу при декореляції помилок ($j = 300$) від кратності виправляємих помилок $t_{\text{вп}}$ та довжини кодової комбінації n

2.1.8. 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 Рїда-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 Рїда-Соломона з $t = 2$ над $GF(16)$. Може бути обране кожне j_0 ; ми виберемо $j_0 = 1$. Тодї

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + (z^3 + z^2 + 1)x^3 + (z^3 + z^2)x^2 + z^3x + (z^2 + z + 1) = x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10}.$$

Оскільки степїнь $g(x)$ дорївнює 4, $n - k = 4$ і $k = 11$. Інформаційний багаточлен являє собою послїдовнїсть одинадцяти символїв з $GF(16)$, що еквівалентно 44 бїтам.

Як другий приклад знайдемо $g(x)$ для (7, 3)-коду Рїда-Соломона з $t = 2$ над $GF(8)$. Може бути обране кожне j_0 ; ми виберемо $j_0 = 4$. Тодї

$g(x) = (x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^0) = x^4 + (z^2 + 1)x^3 + (z^2 + 1)x^2 + (z + 1)x + z$ (тут використане подання елементїв поля $GF(8)$ у виглядї багаточленїв вїд z). Інформаційний багаточлен являє собою послїдовнїсть трьох вїсіmkових символїв (що еквівалентно дев'яти бїтам). Припустимо, що

$$i(x) = (z^2 + z)x^2 + x + (z + 1).$$

Кодове слово несистематичного коду запишеться у виглядї

$$c(x) = i(x)g(x) = (\alpha^4x^2 + x + \alpha^3)(x^4 + \alpha^6x^3 + \alpha^6x^2 + \alpha^3x + \alpha) = \alpha^4x^6 + \alpha x^5 + \alpha^6x^4 + 0x^3 + 0x^2 + \alpha^5x + \alpha^4,$$

що являє собою послїдовнїсть семи вїсіmkових символїв.

Коди Рїда-Соломона є оптимальними в змїсті границї Сїнглтона.

Теорема 5. Код Рїда-Соломона має мїнїмальну вїдстань $n - k + 1$ і є кодом з максимальною вїдстанню.

Доведення. Нехай $d = 2t + 1$ – конструктивна вїдстань коду. Мїнїмальна вїдстань d^* задовольняє нерївностї

$$d^* \geq d = 2t + 1 = n - k + 1,$$

оскїльки для кодїв Рїда-Соломона $2t = n - k$. Але для будь-якого лїнійного коду має місце границя Сїнглтона

$$d^* \leq n - k + 1$$

Отже, $d^* = n - k + 1$ і $d^* = d$.

Доведена теорема стверджує, що при фїксованих n і k не існує коду, мїнїмальна вїдстань якого бїльше, нїж у коду Рїда-Соломона. Не слїд розумїти це твердження буквально. Часто перевага вїддається кодам з такими параметрами (n', k') , за яких не існує коду Рїда-Соломона. У той же час коди Рїда-Соломона завждї виявляються коротше всїх інших циклїчних кодїв над тим же алфавїтом.

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 продовженням 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 окремий випадок – визначення розширеного коду Ріда-Соломона.

Визначення 2. 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 3. 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*.

Порівнянню 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 6. 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. 2.24 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.

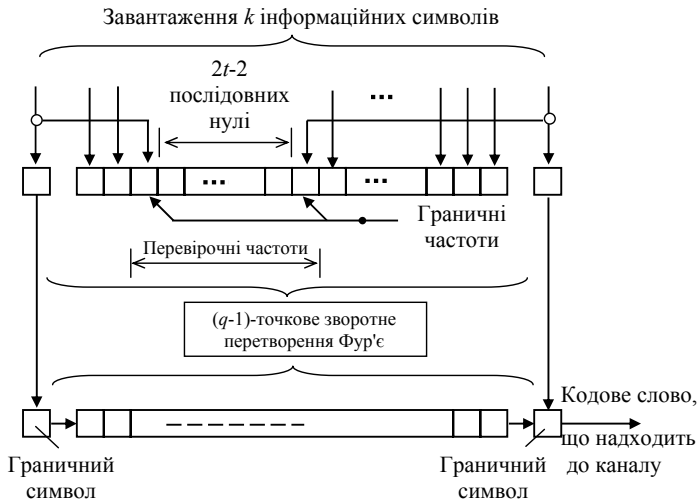


Рисунок 2.24 – Кодер для розширеного коду Ріда-Соломона в частотній області

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 та-

ким самим числом інформаційних символів, як і у вихідного коду, але з мінімальною відстанню $d^* + 2$. Звичайно, ми одержимо той самий розширений 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. 2.25. У цьому випадку розширення розглядається як подовження $(n-2, k)$ -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.

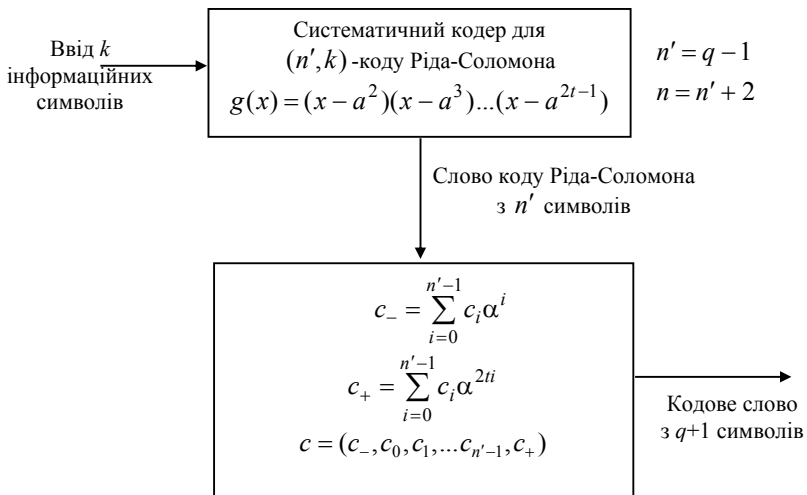


Рисунок 2.25 – Систематичний кодер для розширеного коду Ріда-Соломона

2.1.9. Декодування блокових надлишкових кодів

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 – пер-

ший ступінь декодування – слугує для визначення параметра елементарних символів прийнятого кодового слова і входить як складова частина приймального 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 декодуючим пристроєм, що ототожнює прийняту комбінацію з однією із дозволених кодограм. В оптимальному випадку декодуючий пристрій повинен мати пам'ять, розраховану на збереження всіх $2m$ кодограм. Декодування полягає в обчисленні $2m$ лінійних сум і визначенні максимумальної з них.

Разом з тим тенденція працювати за швидкостей, близьких до пропускової здатності каналу зв'язку, з досить малою ймовірністю помилки викликає необхідність збільшувати значність коду, тому що тільки завдатостійкі 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. Бородіним, 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:

$$Z_j = z_1, \dots, z_n = X_i \oplus \Pi_0, \quad (2.25)$$

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 Байєса, умовна ймовірність:

$$p_{Z_j}(X_i) = \frac{p_{X_i}(Z_j) \cdot p(X_i)}{p(Z_j)}, \quad (2.25a)$$

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 (2.25a) 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 (2.25) 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 :

$$S_0 = Z_j \| H_{n,m} \| = P_{0,j} \| H_{n,m} \|.$$

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 12. 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 $S_{01} = 111$, $S_{02} = 011$, $S_{03} = 101$, $S_{04} = 110$, $S_{05} = 100$, $S_{06} = 010$. Відшукання 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 $h(x)$:

$$f_j(x)h(x) = 0; \quad (2.26)$$

– 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 (2.26) 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 $p_t(x)$ $p_{t+1}(x)$, 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 13. Розглянемо роботу декодуючого циклічного (7, 4)-коду множенням на перевірочний поліном $h(x) = 10111$ (рис. 2.26). 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.

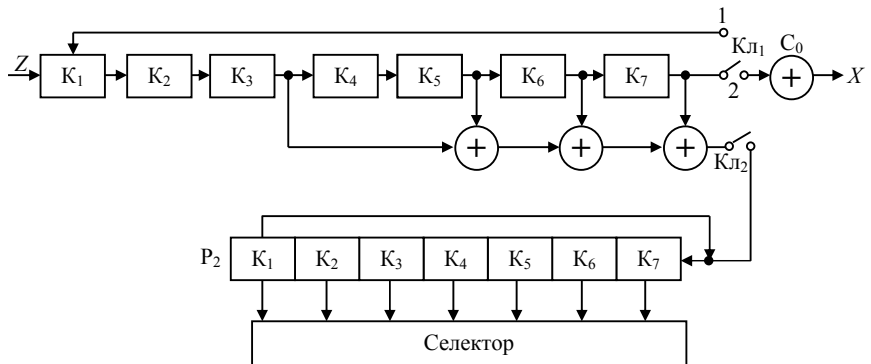


Рисунок 2.26 – Декодуючий пристрій циклічного (7, 4)-коду з множенням на поліном $h(x) = 10111$

Процес роботи схеми ілюструється табл. 2.8, 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 2.8 – Ілюстрація роботи схеми згідно з рис. 2.26

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	1	0	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 14. Розглянемо роботу декодуючого пристрою циклічного (7, 4)-коду діленням на породжуючий поліном $g(x) = 1011$ (рис. 2.27). Спочатку ключі K_1 та K_2 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_1 та K_2 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. 2.9 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 .

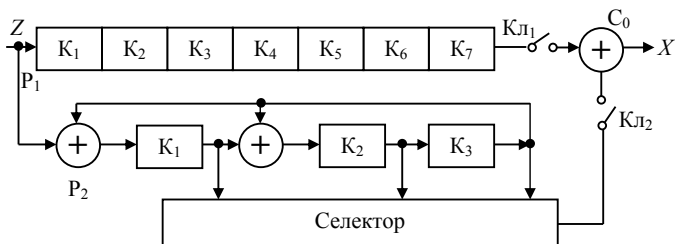


Рисунок 2.27 – Декодуєчий пристрій циклічного (7, 4)-коду з діленням на поліном $g(x) = 1011$

Найбільші ускладнення викликає побудова селектора, складність якого залежить від характеру і числа помилок, що виправляються.

Таблиця 2.9 – Ілюстрація роботи схеми згідно з рис. 2.27

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 виправляється 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 надлишкової. 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:

$$h_{i,n}x_n \oplus h_{i,n-1}x_{n-1} \oplus \dots \oplus h_{i,1}x_1 \oplus, \quad (2.27)$$

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 (2.27).

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* (СПП) щодо символу x_v .

Принцип мажоритарного декодування полягає в наступному. Якщо підставити прийняті символи в рівняння перевірок (2.27) 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 $\theta_{v,1}$, що відповідає збільшенню індексів всіх символів на одиницю.

Мажоритарний декодуючий 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 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 15. Побудуємо мажоритарний приймальний кодоперетворювач циклічного $(7, 3)$ -коду, заданого поліномом $g(x) = 10111$, що використовує розділені перевірки. Перевірочна матриця H_{74} і матриці $\theta_{v,1}$ 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:

$$\begin{aligned} x_1 &= x_1; & x_2 &\oplus x_4; & x_3 &\oplus x_7; & x_5 &\oplus x_6 = 1; & 24; & 37; & 56; \\ x_2 &= x_2; & x_3 &\oplus x_5; & x_4 &\oplus x_1; & x_6 &\oplus x_7 = 2; & 35; & 41; & 67; \\ x_3 &= x_3; & x_4 &\oplus x_6; & x_2 &\oplus x_5; & x_7 &\oplus x_1 = 3; & 46; & 25; & 71. \end{aligned}$$

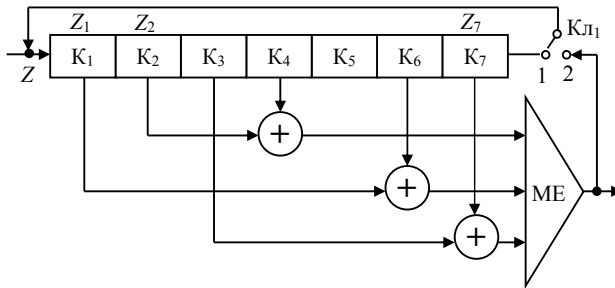


Рисунок 2.28 – Мажоритарний декодуєчий пристрій циклічного (7, 3)- коду з розділеними перевірками

Оскільки число нетривіальних перевірок $\mu = 3$, та кодова відстань $d_p = 4$ і, отже, код виправляє одиничні помилки. Схема кодоперетворювача зображена на рис. 2.28. При положенні «1» ключа $K_{Л1}$ здійснюється циклічний зсув записаних в регістрі символів. Оскільки декодування відбувається послідовно, то в положенні «2» ключа $K_{Л1}$ в регістр 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 $r\lambda_3$ залишених рівнянь перевірок, то символ x_v може бути виправлений.

Зв'язні перевірки. Побудувати схему мажоритарного декодування, що реалізує 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 $\lfloor \cdot \rfloor$ 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 16. 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:

$$x_1 = x_2 \oplus x_3 \oplus x_6; x_3 \oplus x_4 \oplus x_5; x_4 \oplus x_6 \oplus x_7; x_2 \oplus x_5 \oplus x_7 = \quad (2.27a) \\ = 236; 345; 467; 257.$$

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. 2.29, опущена перевірка $x_1 = x_4 \oplus x_6 \oplus x_7$.

Рівняння перевірок (2.27a) 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 коректуючої здатності коду, спрощуючи одночасно схему кодоперетворювача.

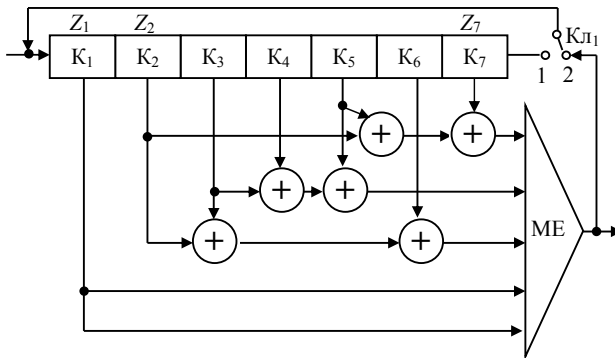


Рисунок 2.29 – Мажоритарний декодуєчий пристрій циклічного (7, 4)-коду з двозв'язними перевірками

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 17. Для циклічного (15,10)-коду з перевірочним поліномом $h(x) = 10100110111$ можна побудувати нетривіальні тривіазні 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 коректуючу 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 $\text{mod } 2$) 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 18. Для циклічного (15, 5)-коду, заданого поліномом $g(x) = 10100110111$, перевірочна матриця (записана в транспонованій формі) має вигляд:

$$H_{15,10}^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

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 $\theta_{2,v}^T$ 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 $\text{mod } 2$ 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 перевірна 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 $x_i \oplus x_j = a_c$ (приклад 18). 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 декодуючий 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 19. Для циклічного $(15, 5)$ -коду, заданого поліномом $g(x) = 10100110111$, матриця:

$$H_d = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ a_1 & a_2 & a_3 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_{14} & a_{15} & \dots \end{pmatrix}$$

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} :

$$\begin{aligned} x_{15} = x_{15}; \quad x_5 \oplus a_2 \oplus a_3; \quad x_6 \oplus a_1 \oplus a_3; \quad x_7 \oplus a_1 \oplus a_2; \quad x_9 \oplus a_3; \\ x_{10} \oplus a_1; \quad x_{13} \oplus a_2 \end{aligned} \quad (2.276)$$

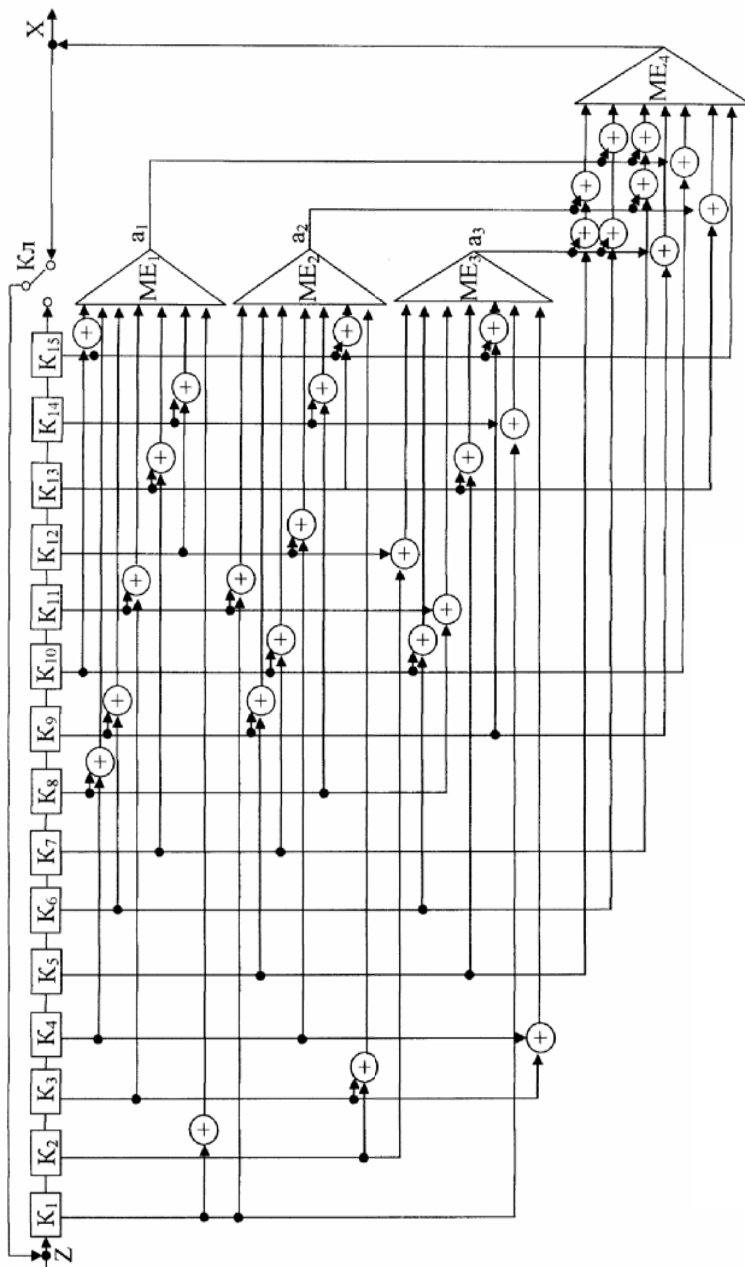


Рисунок 2.30 – Мажоритарний декодувальний пристрій циклічного (15, 5)-коду з ортогоналізацією перевірок у два кроки

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. 2.30. За циркуляції в регістрі зсуваються не тільки символи системи (2.27б), 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:

$$\frac{\mu}{\lambda_3} = \frac{n - v - \alpha}{\max \left\{ d_d - v; \left\lfloor \frac{d_d + 1}{2} \right\rfloor \right\}}, \quad (2.28)$$

де параметр

$$\alpha = \begin{cases} 1 & \text{при } d_d - \text{непарному та } \frac{v}{d_d} < 0,5; \\ \lambda_3 & \\ 0 & \text{в інших випадках;} \end{cases}$$

d_d – кодова відстань дуального коду.

Якщо нехтувати значенням $\lambda < 1$, то вираз (2.28) набуде вигляду:

$$\frac{\mu}{\lambda_3} = \begin{cases} \frac{n - v}{d_d - v} & \text{при } \frac{v}{d_d} < 0,5; \\ \frac{2(n - v)}{d_d(1 + \beta)} & \text{при } \frac{v}{d_d} \geq 0,5; \end{cases} \quad (2.28a)$$

де

$$\beta = \begin{cases} 0 & \text{при } d_d - \text{парному}; \\ \frac{1}{d_d} & \text{при } d_d - \text{непарному}. \end{cases}$$

Приклад 20. Для циклічного (15, 4)-коду, заданого поліномом $g(x) = 11001$, відстань дуального коду $d_d = 3$. Якщо $v = 1$, то $\frac{\mu}{\lambda_3} = 7$ і $d_{p \text{ мин}} = 8$.

Приклад 21. 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 ортогоналізацію 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

$$\mu \leq \frac{n-1}{d_0-1},$$

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 $d_{p\text{мін}} = \mu + 1 < 3$.

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

$$\lambda_L = \frac{L_{X_r^0}(Y)|_{\max}}{L_{X_l^1}(Y)|_{\max}} < 1, \quad (2.29)$$

то повинне виноситися рішення про приймання кодограми X_r^0 .

Припустимо, що в каналі діють адитивні нормальні флукуаційні 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 :

$$\begin{aligned} L_{X_v^0}(Y) &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[(y_1 - 1)^2 + \sum_{j=2}^n (y_j - X_{v_j}^0)^2 \right] \right\} = \\ &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[\sum_{j=1}^n (y_j^2 + n - 2y_1) - 2 \sum_{j=2}^n Y_j X_{v_j}^0 \right] \right\} \end{aligned} \quad (2.30)$$

а для кодограми X_l^1 , яка починається з одиниці:

$$\begin{aligned} L_{X_l^1}(Y) &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[(y_1 + 1)^2 + \sum_{j=2}^n (y_j - X_{l_j}^1)^2 \right] \right\} = \\ &= \frac{1}{(\sqrt{2\pi\sigma_{\text{ш}}})^n} \exp \left\{ -\frac{1}{2\sigma_{\text{ш}}^2} \left[\sum_{j=1}^n (y_j^2 + n + 2y_1) - 2 \sum_{j=2}^n Y_j X_{l_j}^1 \right] \right\} \end{aligned} \quad (2.30a)$$

Підставивши вирази (2.30) і (2.30a) в (2.29), 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 $X_r^0 = 0, x_{r2}, x_{r3}, \dots, x_{rn}$; $X_l^1 = 1, x_{l2}, x_{l3}, \dots, x_{ln}$ – кодограми, що починаються з 0 або 1, для яких сума:

$$S = \sum_{j=2}^n Y_j X_{v_j}$$

– максимальна.

Нехай для кожного інформаційного символу (n, m) -коду можна скласти систему з r розділених перевірок, кожна з яких містить тільки два символи:

$$x_i = x_{21} \oplus x_{22}; x_{31} \oplus x_{32}; \dots; x_{r1} \oplus x_{r2}, \quad (2.31)$$

де перший індекс членів у правій частині рівності (2.31) 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 (2.31), 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 (2.31) дозволяє взяти за символи $x_{21}, x_{31}, \dots, x_{r1}$ у формулі для S^0 інформаційні символи. Тоді

$$S^0_{\max} = |y_{21} + y_{22}| + |y_{31} + y_{32}| + \dots + |y_{r1} + y_{r2}|.$$

Аналогічно для кодограм підмножини $\{X^1\}$ маємо:

$$S^1 = (y_{21} - y_{22}) \cdot x_{21} + (y_{31} - y_{32}) \cdot x_{31} + \dots + (y_{r1} - y_{r2}) \cdot x_{r1};$$

$$S^1_{\max} = |y_{21} - y_{22}| + |y_{31} - y_{32}| + \dots + |y_{r1} - y_{r2}|.$$

Зробивши відповідні підстановки, отримаємо:

$$2y_1 + (|y_{21} + y_{22}| - |y_{21} - y_{22}|) + \dots + (|y_{r1} + y_{r2}| - |y_{r1} - y_{r2}|). \quad (2.32)$$

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 (2.32). 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 рішення $x_l = 1$, а решті символів привласнюються значення, відповідні знакам різниць $y_{i1} - y_{i2}$. Отже, декодуванню піддаються відразу всі інформаційні символи.

Приклад 22. 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 23. 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 (2.32) 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 (2.32) 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 (2.32) слугує лише для визначення інформаційного символу x_1 . Потім з використанням системи перевірок для інформаційного символу x_2 обчислюється сума, аналогічна (2.32), і за нею визначається символ x_2 . Цей процес повторюється послідовно стільки разів, скільки інформаційних символів міститься у кодограмі.

2.1.10. Ефективність декодування при квантуванні інформаційного параметра на виході каналу

За коди з використанням зони стирання (канал зі стиранням) вважаємо такий спосіб передавання інформації, за якого на приймальній стороні наряду із зонами, що відповідають прийому сигнальних ознак, які визначаються основою коду, вводиться додатково деяка зона невизначеності (рис. 2.31) Цю зону називатимемо зоною стирання і позначимо додатковим символом X . На рис. 2.31 зону стирання з символом X наведено стосовно до двійкового коду і є проміжним значенням амплітуди сигналу між значеннями амплітуди сигналу символів 1 і 0. При потраплянні сигналу і завади в зону стирання вирішальна схема на прийомній стороні фіксує додатковий символ стирання X .

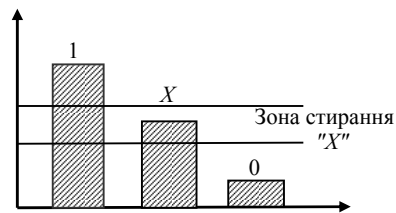


Рисунок 2.31 – Зона стирання X у двійковому коді

З викладеного вище виходить, що введення зони стирання фактично призводить до змінювання основи коду за рахунок збільшення кількості використаних значень амплітудних сигнальних ознак з двох значень до трьох. Замінювання нульової сигнальної ознаки у двійковому коді на всі з'єднання другою струмовою сигнальною ознакою призводить до змінювання кількості кодових переходів з $d = 1$ до $d = 2$.

Таким чином, змінювання основи коду за незмінної кількості кодових комбінацій супроводжується підвищенням надлишковості коду. Звідси виходить, що введення зони стирання за незмінної кількості кодових комбінацій також буде супроводжуватися підвищенням надлишковості коду, що може бути використане або тільки для виявлення помилок стирань, або в кодах, що мають інші види надлишковості для виявлення та виправлення помилок стирання.

Здатність коду виявляти помилки або виявляти та виправляти помилки при використанні зони стирання залежить від надлишковості початкового коду, що застосовується. Задля того, щоб код міг виявляти та виправляти $t_{\text{вп}}$ помилок і виправляти $t_{\text{в}}$ помилок стирання, достатньо виконати умову:

$$d_{\text{мін}} = 2t_{\text{вп}} + t_{\text{в}} + 1.$$

Процес декодування прийнятого повідомлення за наявності помилок стирань та інших помилок є дуже складним завданням, а за кількості помилок $t_{\text{вп}} > 2$ практично складно реалізується через збільшення обсягу об'єднання.

Необхідно на закінчення відзначити, що використання зони стирання можливе лише за рахунок зменшення областей прийому сигнальних ознак, що призводить до перерозподілу ймовірностей проходження, захисної відмови і трансформації. Як правило, застосування зони стирання дає можливість зменшити ймовірність трансформації і відповідно збільшити ймовірність захисної відмови, що є дуже суттєвим для систем передавання цифрової інформації.

Структура оптимального приймача. Розглянемо структуру приймального пристрою, що забезпечує оптимальне оброблення двійкових сигналів з довільним числом рівнів квантування (рис. 2.32). Як бачимо з рисунку, між вирішальною схемою BC_1 , що містить демодулятор сигналів, і схемою BC_2 включено квантизатор KB , що дозволяє квантувати рівень вихідних сигналів демодулятора. Таким чином, квантизатор перетворює вихідний алфавіт демодулятора $\{y\}$ в новий алфавіт символів $\{z\}$. Ймовірнісні 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 подати в матричній формі (рис. 2.33, а) або графічно (рис. 2.33, б).

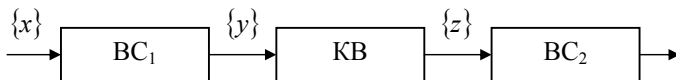


Рисунок 2.32 – Приймач з довільним числом рівнів квантування сигналів

У залежності від числа рівнів квантування S отримуємо різні способи приймання сигналів. Посимвольне приймання реалізується таким чином. Область вихідних значень сигналів демодулятора Y ділиться порогом U_0 на дві зони – позитивну і від’ємну (рис. 2.34, 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 у 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. 2.34, б). Ці пороги разом з нульовим розділяють всю ділянку значень вихідних сигналів демодулятора на чотири попарно симетричні зони, що рівнозначно квантуванню сигналів на два рівні. У цьому випадку обсяг інформації про прийнятий сигнал збільшується за рахунок використання відомостей про знаходження сигналу в тій чи іншій зоні, що підвищує завадостійкість зв’язку.

Продовжуючи збільшувати число рівнів квантування, ми все більше будемо підвищувати завадостійкість зв’язку, наближаючись в межі до завадостійкості оптимального прийому в цілому, що являє собою приймання з нескінченним числом рівнів квантування.

Таким чином можна виділити клас способів прийому, які відрізняються між собою числом рівнів квантування сигналів з виходу демодулятора або, що те ж саме, точністю роботи схеми ВС₁. Прийом в цілому і посимвольний прийом є граничними випадками для цього класу.

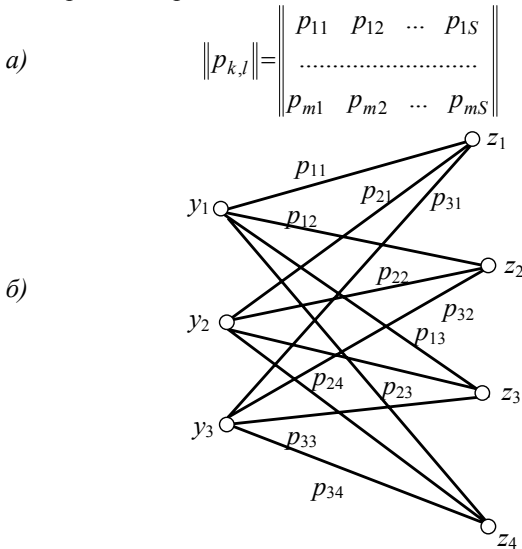


Рисунок 2.33 – Перехідні ймовірності квантизатора

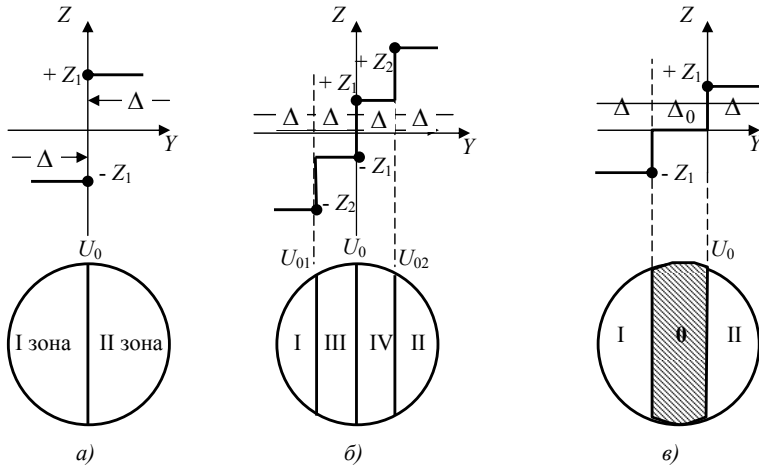


Рисунок 2.34 – Робочі області сигналів за різних способів прийому

Оптимальний алгоритм декодування. Алгоритм декодування при довільному числі рівнів квантування відрізняється тим, що якщо функції правдоподібності $L_{пк}$ і $L_{ок}$ являють собою густину ймовірностей при правильному і помилковому прийомі і для будь-якого кінцевого числа рівнів квантування вони повинні бути замінені перехідними ймовірностями q_j і p_j попадання вихідного сигналу демодулятора в j -ту зону ($j = 1, 2, \dots, S$) відповідно при правильному і помилковому прийомі. Тоді оптимальний алгоритм декодування при довільному числі рівнів квантування S можна подати у вигляді

$$\sum_{j=1}^S \log \frac{q_j}{p_j} \sum_{k_j} x_{r,k} y_k > \sum_{j=1}^S \log \frac{q_j}{p_j} \sum_{k_j} x_{l,k} y_k, \quad (2.33)$$

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 -й зоні квантування, причому

$$\sum_{j=1}^S k_j = n.$$

Неважно бачити, що при $S = 1$ вираз (2.33) переходить в

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k.$$

Поділивши обидві частини нерівності (2.33) на $\log \frac{q_1}{p_1}$, одержимо іншу форму оптимального алгоритму декодування:

$$\sum_{j=1}^S \gamma_j \sum_{k_j} x_{r,k} y_k > \sum_{j=1}^S \gamma_j \sum_{k_j} x_{l,k} y_k, \quad (2.33a)$$

де коефіцієнт

$$\gamma_j = \frac{\log \frac{q_j}{p_j}}{\log \frac{q_1}{p_1}}.$$

Згідно з алгоритмом (2.33a) схема BC_1 формує символи, амплітуда яких залежить від того, в якій зоні знаходився рівень сигналу на даній позиції кодограми. Якщо сигнал попав в першу зону, то амплітуда символу на виході схеми BC_1 умовно дорівнює одиниці; для j -ї зони амплітуда символу дорівнює коефіцієнту γ_j . Величина γ_j залежить від перевищення сигналу і способу прийому. Схема BC_2 підсумовує символи з урахуванням їх знаків у 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 за довільного числа рівнянь 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

$$\sum_{k_j} x_{v,k} y_k = k_j - 2d_{v,y}^{(j)},$$

де $d_{v,y}^{(j)}$ – відстань між кодограмами X_v і Y за тими k_j позиціями, де сигнал знаходився в j -й зоні квантування. Після перетворень отримаємо

$$\sum_{j=1}^S \gamma_j d_{r,y}^{(j)} < \sum_{j=1}^S \gamma_j d_{l,y}^{(j)}.$$

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 $\gamma_j = \gamma = \text{const}$, тоді маємо правило $d_{r,y} < d_{l,y}$ для посимвольного прийому з виправленням помилок.

Ймовірність помилкового прийому неквантованих двійкових сигналів в гауссівському каналі визначається виразом

$$p_0 < 2^{-n(V_{0n} - V_n)}, \quad (2.34)$$

де V_{0n} – граничне значення швидкості передавання інформації в дв. од/мірність (ступінь вільності) сигналу, що визначає експоненційний характер спадання ймовірності помилки; параметр

$$V_n = \frac{V_i}{n_0} \quad \frac{\text{дв од/с}}{\text{мірність/с}};$$

n_0 – швидкість передавання сигналів, виражена числом ступенів вільності сигналу за 1 с.

При квантуванні вихідних сигналів демодулятора обсяг інформації на вході схеми ВС₂ змінюється і формула (2.34) набуде вигляду

$$p_0 < 2^{-n(V_{0k} - V_n)}. \quad (2.34a)$$

Різниця між значеннями V_{0n} і V_{0k} може слугувати мірою зменшення складності приймального пристрою при переході від приймання в цілому до приймання з кінцевим числом рівнянь квантування.

Величина p_{0k} залежить від апіорних ймовірностей передаваних сигналів $\{p_k\}$ і перехідних ймовірностей $\{p_{k,l}\}$ і визначається виразом:

$$V_{0k} = -\log_2 \sum_{l=1}^S \left(\sum_{k=1}^m p_k \sqrt{p_{k,l}} \right). \quad (2.34b)$$

При прийомі в цілому число рівнів квантування $S \rightarrow \infty$ і, отже, крок квантування $\Delta l \rightarrow 0$ (див. рис. 2.34). При малому, але кінцевому Δ_l , перехідна ймовірність

$$p_{k,l} \approx \Delta_l p(z_l / y_k).$$

Тоді граничне значення швидкості передавання інформації при квантуванні сигналів

$$V_{0k} = -\log_2 \sum_{l=1}^S \Delta_l \left(\sum_{k=1}^m p_k \sqrt{p(z_l / y_k)} \right)^2. \quad (2.35)$$

При $\Delta_l \rightarrow 0$ перша сума переходить в інтеграл, і для двійкових гауссових каналів з рівноймовірними сигналами величина V_{0n} (приймання в цілому) складає

$$V_{0k} \rightarrow V_{0n} = 1 - \log_2 \left(1 + e^{-\frac{Q_0^2}{2\sigma_m^2}} \right). \quad (2.35a)$$

де параметр

$$Q_0^2 = \frac{Q_c^2}{n} \quad (2.35b)$$

характеризує енергію, що припадає на одну ступінь вільності сигналу.

Розглянемо декілька одиничних випадків.

Двійковий симетричний канал. ДСК відноситься до числа каналів з двома рівнями квантування, де перехідні ймовірності

$$p_{12} = p_{21} = p_0; \quad p_{11} = p_{22} = q_0 = 1 - p_0.$$

Тоді гранична швидкість передавання інформації згідно з виразом (2.35)

$$V_{0,2} = -\log_2 \sum_{l=1}^2 \left(\sum_{k=1}^2 p_k \sqrt{p_{k,l}} \right)^2 = 1 - \log_2 [1 + 2\sqrt{p_0(1-p_0)}].$$

Ймовірність p_0 визначається перевищенням сигналу, способами маніпуляції і оброблення сигналів, а також характером завмирань.

Двійковий канал зі стиранням. Двійковий канал із стиранням являє собою по суті різновид ДСК. При прийомі зі стиранням символи, рівень яких лежить нижче порога U_0 у межах деякої зони Δ_0 , названою зоною стирання (нульовою зоною), не враховуються при декодуванні у схемі ВС₂ («стираються»). Розбиття ділянки значень вихідних сигналів демодулятора при прийманні зі стиранням показано на рис. 2.34, в, а діаграма перехідних ймовірностей – на рис. 2.35, де

$$p_{12} = p_{21} = p_0; \quad p_{13} = p_{23} = p_{ст}; \quad p_{11} = p_{22} = 1 - p_0 - p_{ст}.$$

При рівноймовірних сигналах величина

$$V_{0,3} = -\log_2 \sum_{l=1}^3 \left(\sum_{k=1}^3 p_k \sqrt{p_{k,l}} \right)^2 = 1 - \log_2 [1 + p_{ст} + 2\sqrt{p_0(1-p_0-p_{ст})}]. \quad (2.36)$$

Ймовірності p_0 і $p_{ст}$ залежать від тих самих факторів, що й в ДСК, і, крім того, від величин U_0 і Δ_0 :

$$p_0 = \frac{1}{\sqrt{2\pi}\sigma_{ш}} \int_{U_0}^{\infty} e^{-\frac{(x+Q_0^2)^2}{2\sigma_{ш}^2}} dx; \quad p_{ст} = \frac{1}{\sqrt{2\pi}\sigma_{ш}} \int_{\Delta_0}^{U_0} e^{-\frac{(x+Q_0^2)^2}{2\sigma_{ш}^2}} dx.$$

Таким чином, величина $V_{0,k} = f(Q_0^2, U_0, \sigma_{ш}^2)$.

У свою чергу, поріг залежить від відношення

$$\mu_0^2 = \frac{Q_0^2}{2\sigma_{ш}^2}.$$

Ця залежність показана на рис. 2.36.

При слабких сигналах оптимальне значення порога

$$U_{0,опт} \approx 0,65\sqrt{2\mu_0^2}.$$

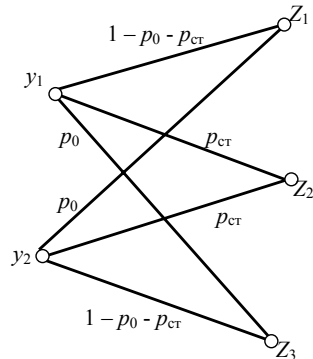


Рисунок 2.35 – Діаграма перехідних ймовірностей каналу зі стиранням символів

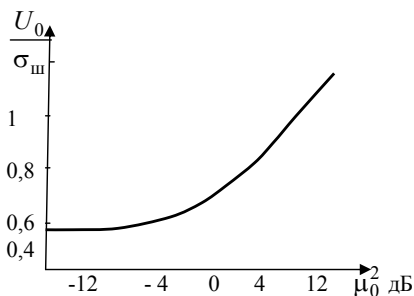


Рисунок 2.36 – Залежність $U_0 = f(\mu_0)$

двома рівнями квантування.

Квантування сигналів з високою основою коду. При використанні кодів з високою основою ($a > 2$) і квантуванні сигналів величина V_{0k} визначається формулою (2.34б). На рис. 2.38 показані залежності для випадку рівномірних повідомлень при числі рівнів квантування $S = m$ і використанні сигналів ФТ при ненадлишковому кодуванні з ймовірністю спотворення кодограм

$$p_{0k} = \frac{2(m-1)}{m} \left[1 - \Phi \left(\frac{1}{m-1} \sqrt{2\mu_0^2} \right) \right] = 10^{-5}.$$

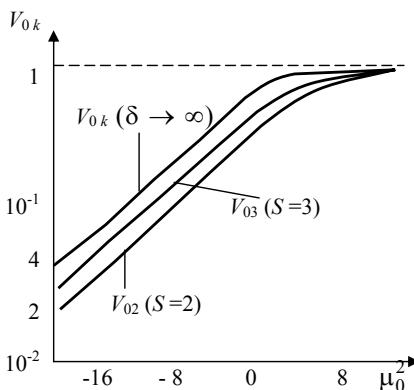


Рисунок 2.37 – Залежність

$$V_{0k} = f(\mu_0^2; S)$$

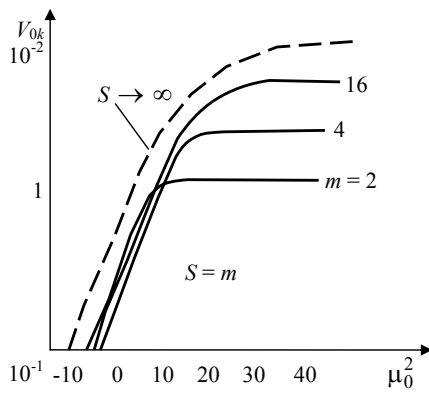


Рисунок 2.38 – Залежність

$$V_{0k} = f(m, \mu_0^2; S)$$

Там же наведена крива для прийому в цілому $S \rightarrow \infty$. Із графіків видно, що при $\mu_0^2 \leq 10$ дБ основа коду мало впливає на величину V_{0k} ; програвш у швидкості передавання інформації при прийомі двійкових сигналів з двома рівнями квантування порівняно з прийомом в цілому не перевищує 2 дБ.

З покращенням якості каналу (зі зростанням параметра μ_{0k}^2) коди з високою основою при $S=m$ забезпечують більшу швидкість передавання інформації, ніж двійкові коди.

Виправляюча здатність групових кодів за довільного числа рівнів квантування. Розглянемо спочатку найпростіші випадки прийому двійкових сигналів з одним рівнем квантування (посимвольний прийом). Будемо думати, 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

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k \text{ отримаємо умову правильного приймання сигналів} \\ - \sum_{d_v} y_k > 0; \quad (2.37)$$

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, у 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

$$- \sum_{d_v} y_k \geq d_v - 2r, \quad (2.37a)$$

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

$$d_0 - 2r > 0, \quad (2.37б)$$

де d_0 – мінімальна відстань коду.

Тому що d_0 і r – цілі числа, то із нерівності (2.37б) отримаємо умову, що пов’язує мінімальну кодову відстань і максимальну кратність виправляємих кодом помилок:

$$r_0 = \begin{cases} \frac{d_0 - 1}{2} & \text{за } d_0 - \text{непарним,} \\ \frac{d_0 - 1}{2} & \text{за } d_0 - \text{парним.} \end{cases} \quad (2.37в)$$

Вирази (2.37в) являють собою нижню оцінку виправляючої здатності коду. Якщо r помилок розподілені всередині кодограми таким чином, що у виразі (2.37а) має місце знак рівності, то можливе виправлення помилок кратності $r > r_0$, але не у всіх з’єднаннях, а тільки в частині з’єднань, визначуваних тонкою структурою коду.

Важливо відзначити, що згідно з формулою (2.37в) виправляюча здатність коду при посимвольному прийомі залежить тільки від його структури.

При прийомі сигналів з довільним числом рівнів квантування із формули (2.33а) отримаємо умову правильного прийому 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:

$$\sum_{j=1}^S \gamma_j (d_{v,j} - 2r_j) > 0. \quad (2.38)$$

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 нерівність (2.38) вироджується в нерівність (2.34б), а виправляюча здатність коду характеризується формулою (2.37в) 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 (2.38), 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 (2.38), 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 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 (2.38) 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

$$r_{j-\xi} < \frac{\gamma_j}{\gamma_j - \gamma_{j-\xi}}(d_0 - 2r_j)$$

помилко. 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 в нижній зоні квантування, причому верхня границя

$$r_0 = d_0 - 1$$

і забезпечується при умові, що

$$\alpha_{j,\xi} > d_0 - 1. \quad (2.38a)$$

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 (2.38а), 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 (2.38а) достатньо, щоб ці помилки були виправлені. Це виходить з того, що у формулі (2.34) 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

$$\gamma(d_{v_2} - 2r_2) + (d_{v_1} - 2r_1) > 0. \quad (2.39)$$

При оцінці нижньої границі виправляючої здатності коду слід брати

$$d_{v_2} + d_{v_1} = d_0.$$

Тоді із нерівності (2.39) отримаємо рівняння зв'язку між мінімальною відстанню коду d_0 , кратністю повністю виправляємих 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 $\gamma \rightarrow \infty$ одержимо

$$2r_2 + d_{v_1} < d_0$$

і тому що величини цілочисельні, то

$$2r_2 + d_{v_1} + 1 = d_0. \quad (2.40)$$

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 (2.40) установлює зв'язок між максимальною кратністю виправляємих кодом помилок 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 (2.39) установлює зв'язок між мінімальною відстанню коду, числом стирань і максимальною кратністю виправляємих кодом не «стертих» помилок.

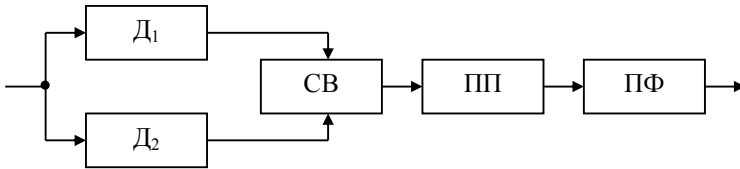


Рисунок 2.39 – Оптимальний приймач сигналів ЧТ з двома рівнями квантування

Підкреслимо, що зв'язок, що установлюється формулою (2.40), залежить тільки від мінімальної відстані коду і справедливий лише при $\gamma \rightarrow \infty$ або, що в даному випадку те ж саме, при $\gamma > d_0 - 1$. В загальному випадку справедлива умова (2.39), яка враховує параметри схеми прийому сигналів. Із цієї умови, зокрема, виходить, що не завжди байдуже, правильно чи помилково прийняті стерті символи. Інакше кажучи, формула (2.40) характеризує, які помилки може виправляти код у відповідності зі своєю структурою, а вираз (2.39) – 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. 2.39, де Д – детектори, СВ – схема віднімання, ПП – порогів пристрій, ПФ – пристрій формування сигналів. Обмежимося випадком некогерентного сигналу ЧТ в каналі з релієвськими завмираннями й адитивними шумами. Густина ймовірності сигналів на вході схеми СВ при цьому визначається виразом

$$w(y) = \frac{a^2 - b^2}{2a} e^{-a|y|+by},$$

де параметри

$$a = \frac{\sigma_{c\text{ш}1}^2 + \sigma_{c\text{ш}2}^2}{4\sigma_{c\text{ш}1}^2\sigma_{c\text{ш}2}^2}; \quad b = \frac{\sigma_{c\text{ш}1}^2 - \sigma_{c\text{ш}2}^2}{4\sigma_{c\text{ш}1}^2\sigma_{c\text{ш}2}^2};$$

$\sigma_{c\text{ш}j}^2 = (\sigma_c^2 + \sigma_{\text{ш}}^2)_j$ – сумарна середня потужність сигналу ($\sigma_c^2 = P_c$) 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

$$w_{x_1}(y) = \frac{1}{2\sigma_{\text{см}}^2(2+h_{\text{с}0}^2)} \exp\left[\frac{h_{\text{с}0}^2(y)}{4\sigma_{\text{см}}^2(1+h_{\text{с}0}^2)} - \frac{(2+h_{\text{с}0}^2)|y|}{4\sigma_{\text{см}}^2(1+h_{\text{с}0}^2)}\right];$$

U_0 – порогова напруга; $h_{\text{с}0}^2$ – середнє статистичнє перевищення сигналу.

При спотворенні позитивного символу ймовірність 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

$$q_1 = q_0 \left(1 - e^{-\frac{q_{\text{нн}}}{1+h_{\text{с}0}^2}}\right); \quad p_1 = p_0 \left(1 - e^{-q_{\text{нн}}}\right). \quad (2.41)$$

де нормований поріг

$$q_{\text{нн}} = \frac{U_0^2}{2\sigma_{\text{см}}^2},$$

а ймовірності помилкового і правильного прийому символів за відсутності порога

$$p_0 = \frac{1}{2+h_{\text{с}0}^2}; \quad q_0 = \frac{1+h_{\text{с}0}^2}{2+h_{\text{с}0}^2}.$$

Ймовірності попадання сигналу в другу зону квантування при правильному і помилковому прийомі відповідно будуть

$$q_2 = q_0 - q_1 = q_0 e^{-\frac{q_{\text{нн}}}{1+h_{\text{с}0}^2}}; \quad p_2 = p_0 - p_1 = p_0 e^{-q_{\text{нн}}}. \quad (2.42)$$

Підставивши ці значення в формулу (2.33а), отримаємо

$$\gamma = \frac{\log\left[(1+h_{\text{с}0}^2)e^{-\frac{h_{\text{с}0}^2}{1+h_{\text{с}0}^2}q_{\text{нн}}}\right]}{\log\left[(1+h_{\text{с}0}^2)\frac{1-\exp\left(-\frac{q_{\text{нн}}}{1+h_{\text{с}0}^2}\right)}{1-\exp(-q_{\text{нн}})}\right]}. \quad (2.43)$$

Криві залежності $\gamma = f(h_{c0}^2; q_{пн})$ показані на рис. 2.40. З рисунка виходить, що нерівність (2.38а) може бути забезпечена не при всіх значеннях 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 становить певний інтерес такі схеми прийому двійкових сигналів, у 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. 2.39, а обчислюється деяка функція їх відношення

$$z = f(y) = f\left(\frac{y_1}{y_2}\right).$$

Однією із можливих функцій є логарифмічна:

$$f(y) = \log_a \left(\frac{y_1}{y_2} \right); \quad f^{-1}(z) = y = a^z. \quad (2.44)$$

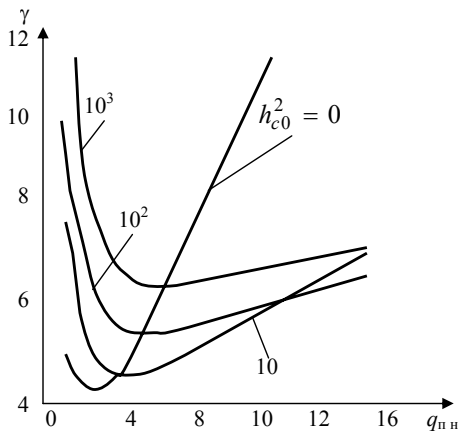


Рисунок 2.40 – Залежність $\gamma = f(h_{c0}^2; q_{пн})$

При цьому схема прийому має вигляд рис. 2.39, але детектори повинні мати логарифмічні характеристики. Можна показати, що коефіцієнт визначається виразом

$$\gamma = \frac{\log_a \left[\left(\frac{1-p_0}{p_0} \right) \frac{p_0 + (1-p_0)f^{-1}(U_0)}{(1-p_0) + p_0 f^{-1}(U_0)} \right]}{\log_a \left[\frac{p_0 + (1+p_0)f^{-1}(U_0)}{(1-p_0) + p_0 f^{-1}(U_0)} \right]}. \quad (2.45)$$

У формулу (2.45) входить тільки абсолютна величина порога U_0 , тому завадостійкість прийому залежить лише від перевищення сигналу.

На рис. 2.41 показані криві залежності $\gamma = f(a^{U_0})$, побудовані за формулою (2.45) з урахуванням (2.44). Така схема прийому також не дозволяє забезпечити нерівність $\gamma = d_0 - 1$ за будь-яких умов у каналі зв'язку.

Потенційна завадостійкість прийому в цілому. Оцінимо завадостійкість прийому в цілому двійкових рівномірних кодограм (n, k) -коду в каналі з постійними параметрами й адитивними білими шумами. При ФМ оптимальний алгоритм оброблення кодограм можна подати у вигляді

$$A_r = \sum_{k=1}^n a_{r,k} > A_l = \sum_{k=1}^n a_{l,k}, \quad (2.46)$$

де коефіцієнт

$$a_{v,k} = x_{v,k} \eta_k = \frac{2}{v_{\text{ш}}^2} \int_{T_{c(k-1)}}^{T_{ck}} y_k(t) x_{v,k}(t) dt, \quad (2.47)$$

$y_k(t)$ – реалізація вхідної напруги приймача в інтервалі часу $(T_{c(k-1)} - T_{ck})$, який відповідає k -му символу кодограми; $x_{v,k}(t)$ – напруга, що відповідає

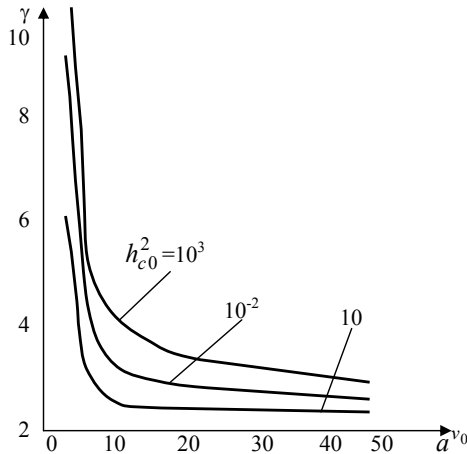


Рисунок 2.41 – Залежність $\gamma = f(a^{U_0})$

значенню k -ї позиції v -ї кодограми. Тому що повідомлення рівноймовірні, то ймовірність правильного прийому визначається ймовірністю спільного виконання $M-1$ нерівностей (2.46) за умови передавання кодограми X_r . Ця ймовірність залежить від математичного очікування, дисперсії та коефіцієнта кореляції між величинами A_r і A_l .

Визначимо ці параметри. Будь-яка пара кодограм X_r і X_l має $n-d_{r,l}$ позицій, що збігаються $x_{r,k}(t)=x_{l,k}(t)$ та $d_{r,l}$ позицій, що не збігаються, $[x_{r,k}(t)=-x_{l,k}(t)]$, де $d_{r,l}$ – кодова відстань між X_r і X_l . Тому на позиціях, що збігаються, значення $a_{r,k}=a_{l,k}$, а на позиціях, що не збігаються, $a_{r,k}=-a_{l,k}$. Випадкові величини розподілені за нормальним законом з параметрами

$$\sigma_{a_{v,k}}^2 = |\bar{a}_{v,k}| \frac{2Q_c^2}{v_{\text{ш}}^2} = 2h_c^2 \quad (v=r,l), \quad (2.48)$$

де Q_c^2 – енергія елементарного надсилання тривалістю T_c . Внаслідок незалежності $a_{l,k}$ випадкова величина A_l також розподілена за нормальним законом з параметрами

$$A_r = A_{01} + A_{02}; \quad A_l = A_{01} - A_{02}. \quad (2.49)$$

Через те, що випадкові величини A_v розрізняються між собою тільки знаками складових $a_{v,k}$ на відповідних позиціях, то A_r і A_l можна подати у вигляді двох величин, кожна з яких є сумою двох незалежних складових.

$$\sigma_{A_l}^2 = 2nh_c^2; \quad \bar{A}_l = 2(n-d_{r,l})h_c^2 - 2(n-2d_{r,l})h_c^2,$$

де A_{01} – центрована випадкова величина, що являє собою суму величин $a_{v,k}$, відповідних позиціям кодограм X_r і X_l , що збігаються, і має дисперсію

$$\sigma_{A_{01}}^2 = 2(n-d_{r,l})h_c^2;$$

A_{02} – центрована випадкова величина, що являє собою суму величин $a_{v,k}$, відповідних позиціям кодограм X_r і X_l , що не збігаються, з дисперсією

$$\sigma_{A_{02}}^2 = 2d_{r,l}h_c^2.$$

Тоді коефіцієнт кореляції між будь-якою парою величин A_r і A_l

$$\rho_{r,l} = \rho(A_r, A_l) = \frac{\overline{A_r A_l}}{\sigma_{A_r} \sigma_{A_l}} = 1 - \frac{2d_{r,l}}{n}. \quad (2.50)$$

Завадостійкість (n,k) -кодів з різною надлишковістю будемо визначати за однакової величини v_i . Це означає, що тривалість кодограм T_k залишається незмінною за будь-якої надлишковості коду. Тому при збільшенні числа перевірочних символів необхідно зменшити тривалість елементар-

них посилок T_c . Звідси виходить, що на сигнал не накладається обмежень по смузі займаних ним частот. Енергія кодограми

$$Q_k^2 = P_c T_k = n Q_c^2 = \text{const}$$

і параметри

$$\sigma_{A_r}^2 \equiv A_r = 2nh_c^2; \quad \sigma_{A_l}^2 = 2nh_c^2; \quad \overline{A_l^2} = 2n\rho_{r,l}h_c^2.$$

Таким чином, завадостійкість двійкових кодів з надлишковістю при заданому перевищенні сигналу

$$h_c^2 = \frac{Q_k^2}{n}$$

залежить тільки від коефіцієнта кореляції $\rho_{r,l}$. Цей коефіцієнт, як відомо, чисельно дорівнює косинусу кута між векторами кодограм. Через те, що $Q_k^2 = \text{const}$, то правильність зв'язку визначається лише взаємним розміщенням векторів кодограм у просторі сигналів, а введення надлишковості переслідує мету оптимального їхнього розміщення для забезпечення максимальної завадостійкості.

Очевидно, що максимальну завадостійкість має система рівновіддалених сигналів, для яких коефіцієнт $\rho_{r,l} = \rho = \text{const}$. Для групових (n, k) -кодів з основою m справедливе співвідношення

$$\frac{1}{n} \sum_{j=1}^m d_j = 2^{k-1},$$

або при рівності всіх відстаней між кодограмами

$$\frac{d_0}{n} = \frac{2^{k-1}}{m-1} = \frac{m}{2(m-1)}. \quad (2.51)$$

З урахуванням формул (2.50) і (2.51) коефіцієнт кореляції

$$\rho = -\frac{1}{m-1}. \quad (2.51a)$$

Вирази (2.51) і (2.51a) являють собою відомі співвідношення для *симплексних сигналів* – найкращої системи рівновіддалених сигналів, яка характеризується найбільшою відстанню між ними. Тому групові двійкові коди з ФМ є найкращими із усіх можливих у каналі з постійними параметрами і забезпечують максимальну завадостійкість, яку можна розглядати як потенційну.

Відзначимо, що згідно з виразом (2.51a) кути між векторами сигналів лежать у межах від π до $\frac{\pi}{2}$, тобто при $m \rightarrow \infty$ система прямує до ортогональної. Інакше кажучи, із двох рівновіддалених систем сигналів, симплексна система завжди краще ортогональної і лише за досить великого m ця відмінність згладжується.

Із співвідношення (2.51) виходить, що при різному числі інформаційних символів m можна одержати різні симплексні коди з однаковим співвідношенням $\frac{d_0}{n}$, але з такими $d_0 = cd_1$ і $n = cn_1$, що відрізняються, де $c=1, 2, 3, \dots$, а d_1 і n_1 – мінімальні значення, за яких дотримується умова (2.51). Код при $c=1$ будемо називати *першим симплексним кодом*. Цей код являє собою M -послідовність, яка має при даному k відстань $d_0 = 2^{m-1}$ і значність $n = 2^m - 1$.

Таким чином, при кодуванні сигналів у каналі з постійними параметрами завжди можна вказати мінімальну надлишковість за будь-якого значення m , що забезпечує максимальну завадостійкість. Подальше збільшення надлишковості не тільки некорисне, але й шкідливе. Дійсно, за даного m симплексні коди зі значністю $n_1 = 2^m - 1$ і $n_2 = 2(2^m - 1)$ мають однакове відношення $\frac{d_0}{n}$ і, отже, однакову завадостійкість. Однак смуга частот сигналів у другому випадку в два рази більша, що не виправдано. За $n < n_1$ і $n_1 < n < n_2$ система стає нерівновіддаленою, і завадостійкість знижується. Тому оптимальним є випадок $n_1 = 2^m - 1$, що відповідає першому симплексному коду.

Сигнали, закодовані двійковим кодом з надлишковістю, можна розглядати як особливий вид широкосмугових сигналів з базою

$$B_c = \frac{\Delta f T_k}{k} \approx \frac{n T_c}{k T_c} = 1 + R_1,$$

де $R_1 = \frac{n-k}{k}$ – коефіцієнт відносної надлишковості коду. База, за якої для різних k завадостійкість виявляється максимальною, буде

$$B_{c \text{ макс}} = \frac{2^k - 1}{k}.$$

Подальше розширення бази недоцільне, тому що при цьому або погіршується завадостійкість, або розширюється смуга займаних частот за тієї ж правильності зв'язку.

2.1.11. 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 Варшавова-Гільберта.
9. Поясніть методику побудови породжуючої і перевірконої матриць групових кодів. Побудуйте матриці H_v і H_n 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 кодуючих 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 $f(x)$ 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 $p_e = 10^{-2}$.

28. Поясніть принцип рекурентного кодування. Закодуйте число 25 рекурентним (2,1)-кодом Фінка-Хагельбаргера. Намалуйте 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 намалуйте кодове дерево сигналів.

30. Закодуйте число 95 згортковим (3/4)-кодом при довжині утворюючої послідовності $n = 16$, складіть схему кодувального пристрою.

Глава 2.2. Неперервні коди

2.2.1. Синтез згорткових кодів

У 1995 р. П. Елайєс запропонував згорткові коди (ЗК), які він розглядав як спосіб неперервного оброблення інформації, а також довів застосовність до них основної теореми Шеннона. Того ж року радянським ученим Л.М. Фінком і В.І. Шляпоберським був уперше запропонований ЗК для виправлення пачок помилок. Пізніше з'явилася більш докладна стаття Хегельбергера, що викликала появу інших робіт, присвячених ЗК для виправлення пачок помилок.

Хегельбергер увів назву «рекурентні коди» для кодів, у яких перевіряючі символи на всій довжині кодової послідовності підпорядковуються тому самому рекурентному співвідношенню.

Одночасно з цим з'явилися статті, що описують виправлення незалежних помилок за допомогою ЗК. Особливо потрібно відзначити роботу Мессі, який запропонував для декодування ЗК простий і ефективний спосіб порогового декодування. У вищевказаних джерелах описуються методи декодування, засновані на використанні алгебраїчної структури кодів. Такі методи прийнято називати *алгебраїчними*.

Паралельно розвивалося ймовірнісне декодування ЗК, засноване на добірці кодової послідовності й перевірці правильності вибору за функцією правдоподібності. Стосовно до цієї групи послідовне декодування й деякі інші ймовірнісні алгоритми декодування ЗК виявилися єдиними способами декодування, що задовольняють умовам теореми Шеннона.

Почнемо вивчення ЗК з опису способів їхнього подання. ЗК складніші для дослідження, ніж блокові коди. Для різних алгоритмів декодування зручно використовувати й різні способи подання ЗК. У зв'язку з тим, що ці способи призначені для опису тих самих кодів, доцільно навести співвідношення, що однозначно зв'язують усі способи подання між собою. Розглянемо приклад.

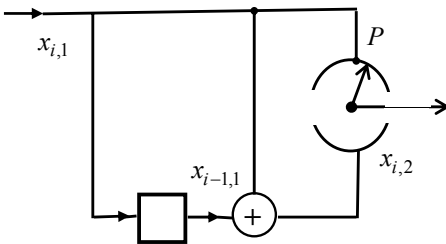


Рисунок 2.42 – Кодер найпростішого ЗК

На рис. 2.42 зображений кодуючий пристрій, або кодер найпростішого ЗК. Символи $x_{i,1}$ і $x_{i,2}$ можуть набувати тільки 2-х значень: 0 і 1. Кодер будемо вважати таким, що складається з таких основних елементів: розряду затримки, позначуваного прямокутником, і суматора за модулем два (\oplus), що виконує операції за

правилом: $0 + 1 = 1$; $1 + 1 = 0$. Послідовність інформаційних символів $x_{i,1}$ надходить на перший «контакт» (розряд) вихідного розподільвача P , а на другий розряд P подається послідовність перевірочних символів $x_{i,2}$. У даному позначенні перший індекс відповідає номеру символу в послідовності, а 2-й індекс – номеру самої послідовності. Вихідний розподільвач здійснює перемежування послідовностей, і в канал вони надходять у наступному вигляді: $x_{i,1}, x_{i,2}, x_{i+1,1}, x_{i+1,2}, x_{i+2,1}, \dots$.

Послідовність символів з однаковим першим номером утворює «маленький» блок ЗК, ми будемо надалі називати його елементарним блоком (ЕБ).

У кодері рис. 2.42 інформаційні символи надходять у канал незмінними; такі коди й кодери за аналогією з блоковими називаються *систематичними*.

У наведеному прикладі перевірочні символи $x_{i,2}$ виражаються через інформаційні за допомогою лінійного перевірочного співвідношення

$$x_{i,2} = x_{i,1} + x_{i-1,1}, \quad (2.52)$$

де самі символи складаються за модулем 2, а знак « $-$ » в індексі має звичайне значення.

Даний код дозволяє виправляти одиничні помилки, під якими ми будемо розуміти зміни значень переданих символів, що відбуваються на відносно великій відстані один від одного. Якщо рівняння (2.52) не виконується 2 рази підряд, то найбільш імовірно, що спотворено інформаційний символ $x_{i,1}$, оскільки рівняння (2.52) не виконується для $x_{i,1}$ та $x_{i+1,1}$, тобто для i -го і $(i + 1)$ -го тактів часу. Якщо ж рівняння не виконується в i -му такті, а в $(i - 1)$ -му та $(i + 1)$ -му тактах виконується, то найімовірніше спотворений перевірочний символ $x_{i,2}$. Якщо ж спотворено два символи в одному ЕБ або двох сусідніх ЕБ, то в наведеному коді неможливо зробити виправлення й потрібно застосовувати більш складні коди.

У лінійному систематичному блоковому коді розмірності (n, k) перевірочні символи блоку зв'язані $n - k$ перевірочними співвідношеннями з k інформаційними символами

$$x_{n-k+j} = \sum_{i=1}^{n-k} a_{i,j} x_i$$

для $j = 1, 2, \dots, n - k$, де x_i – інформаційні символи, коли $1 \leq i \leq k$, і перевірочні, якщо $k + 1 \leq i \leq n$.

Основна ідея використання блокових кодів досить проста. Виберемо множину з k дискретних символів повідомлення, призначених для передачі, до них додамо $n - k$ перевірочних символів, сформованих зазначеним способом, і передамо символи всі разом у вигляді блока з n каналних

символів. Якщо завади в каналі спотворюють малу частину цих n символів, то й $n - k$ перевірочних символів дають на приймальній стороні достатню інформацію, що дозволяє виявити або виправити помилки, які відбулися в каналі. У блокових кодах $n - k$ перевірочних символів будь-якого блока не зв'язані ніякою функціональною залежністю із символами сусідніх блоків.

ЗК також можна розділити на елементарні блоки (ЕБ) довжини b , що складаються з кодових символів $x_{i,j}$ ($1, 2, \dots, b$), де індекси позначають відповідно номер ЕБ у кодовій послідовності та порядковий номер символу всередині ЕБ. ЗК використовується для перетворення інформаційної послідовності Z , що розбивається на ЕБ довжиною $b - k$, тобто $Z = z_{i,1}; z_{i,2}; \dots; z_{i,b-k}; z_{i+1,1}; \dots; z_{i+1,b-k}; z_{i+2,1}; \dots$. Будемо вважати інформаційну послідовність Z , що складається з $b - k$ підпослідовностей Z_j , кожна з яких складається з символів $z_{i,j}$ з однаковим 2-м індексом.

Більша частина матеріалу відноситься до двійкового поля, тобто $x_{i,j} = \{0, 1\}$. Будемо відзначати щоразу окремо результати, що відносяться до поля Галуа $GF(q)$ або до розширеного двійкового поля $GF(2^r)$. Надамо спочатку визначення систематичного ЗК, на початку кожного ЕБ якого є $b - k$ інформаційних символів, а в його кінці k перевірочних символів (рис. 2.43).

У зв'язку з введенням поняття елементарний блок (ЕБ), при аналізі згорткових кодів на відміну від блокових інформаційні елементи позначені символом k , а перевірочні m .

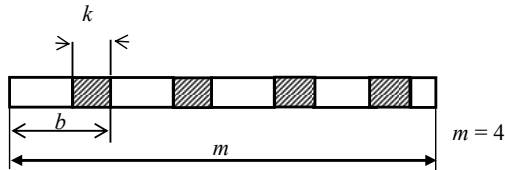


Рисунок 2.43 – Структура ЗК

Визначення 1. Систематичним згортковим $(b, b - k)_K$ -кодом назвемо відображення множини інформаційних послідовностей $Z = \{z_{i,j}\} (j = 1, \dots, b - k)$ на множину кодових послідовностей $X = \{x_{i,j}\}$; послідовність X розділена на ЕБ довжиною b символів ($j = 1, \dots, b$), містить у собі незмінними символи інформаційної послідовності, тобто $x_{i,j^*} = z_{i,j^*}$ для $j^* = (1, \dots, b - k)$, а символи кожного з K сусідніх ЕБ зв'язані між собою за допомогою k лінійних перевірочних співвідношень

$$\sum_{\theta=0}^{K-1} \sum_{j=1}^b a_{\theta,j}^{(\xi)} x_{i-\theta,j} = 0, \quad \xi = 1, \dots, m, \quad (2.53)$$

коефіцієнти $a_{\theta,j}^{(\xi)}$ взяті з того ж поля, що й символи $x_{i,j}$, а знак \sum означає підсумовування в цьому полі.

Число символів у K ЕБ, символи яких зв'язані перевірочними співвідношеннями (2.53), називається *кодовим обмеженням* n_A

$$n_A = Kb.$$

У виразі (2.53) не завжди можна в явному виді виразити перевірочні символи $x_{i,j}$ для $b - m + 1 \leq j \leq b$ через інформаційні. Систематичні коди, в яких це здійснюване, тобто

$$x_{i,b-m+\xi} = \sum_{\theta=0}^{K-1} \sum_{j=1}^{b-m} a_{\theta,j}^{(\xi)} x_{i-\theta,j}, \quad (2.54)$$

будемо називати *модульними*.

Для $(b, b-1)_K - 3K$, в яких є єдине значення $\xi = 1$, будемо опускати індекс ξ у позначенні коефіцієнтів.

Якщо $K = 1$, то 3К переходить у блоковий код, для якого завжди можна подати вираз (2.53) у вигляді (2.54), оскільки друге додавання відсутнє.

Таким чином, у систематичних 3К інформаційні символи залишаються незмінними, а кожний з m перевірочних символів будь-якого ЕБ є лінійною функцією символів K сусіднього ЕБ: даного й $K-1$ раніше переданих. У несистематичному 3К всі b символів ЕБ є лінійними функціями сусідніх $K(b-m)$ символів інформаційної послідовності. Точне визначення несистематичних 3К подається нижче, а тут відзначимо лише, що вираз (2.53) справедливий і для них, але, як буде показано нижче (2.53) однозначно визначає систематичний 3К і не може однозначно визначити несистематичний код.

Приклад 1. Вираз (2.52) є перевірочним співвідношенням типу (2.54) для модульного $(2,1)_2$ -коду.

Приклад 2. $(3,1)_2$ -код, що подається рівняннями

$$x_{i,1} + x_{i,3} + x_{i-1,3} = 0 \quad (\xi = 1);$$

$$x_{i,2} + x_{i-1,1} + x_{i-1,2} + x_{i-1,3} = 0 \quad (\xi = 2),$$

має наступні значення коефіцієнтів $a_{i,j}^{(\xi)}$:

$$a_{0,1}^{(1)} = a_{0,3}^{(1)} = a_{1,3}^{(1)} = a_{0,2}^{(2)} = a_{1,1}^{(2)} = a_{1,2}^{(2)} = a_{1,3}^{(2)} = 1; a_{0,2}^{(1)} = a_{1,1}^{(1)} = a_{1,2}^{(1)} = a_{0,1}^{(2)} = a_{0,3}^{(2)} = 0$$

і не є модульним.

Завдання згорткового коду за допомогою перевірконої матриці.

Розглянемо коди для передачі неперервного потоку інформації, тому природне введення нескінченного вектор-стовпця кодової послідовності X і

Відзначимо, що число стовпців матриці H_N дорівнює кодовому обмеженню, тому

$$n_A = Nb/m; \quad (2.57)$$

$$N = Km. \quad (2.58)$$

У каналі кодова послідовність X складається з послідовності завад E . Аналогічно кодовій послідовності X послідовність завад будемо вважати такою, що складається із символів $e_{i,j}, 1 \leq j \leq b$. Додавання X та E виконується за правилом додавання векторів, тобто відповідні один одному символи X та E підсумовуються в кінцевому полі. При декодуванні одержуємо послідовність ознак помилок – синдром S

$$S = H(X + E) = HX + HE = HE. \quad (2.59)$$

Таким чином, S є напівнескінченим вектор-стовпцем, що являє собою суму за модулем q тих стовпців матриці H , які відповідають спотвореним позиціям кодової послідовності. Синдром неспотвореної кодової послідовності дорівнює нульовому вектору (2.55).

Будемо вважати, що в приймачі декодується блок з b символів одночасно, а для його декодування використовуються перші N позицій синдрому, які позначимо через S_N .

Приклад 3. Розглянемо ЗК, утворений матрицею $B = \begin{bmatrix} 11 \\ 10 \end{bmatrix}$,

$m = 1$. Перевірочна матриця $H_N = \begin{bmatrix} 11 & 00 \\ 10 & 11 \end{bmatrix}$. Нехай вхідна послідовність

інформаційних символів $Z = 110100 \dots$. Їй відповідає кодова послідовність (у транспонованому вигляді) $X^T = 11 \ 10 \ 01 \ 11 \ 01 \ 00 \dots$.

Нехай послідовність помилок має вигляд $E^T = [e_{1,1}, e_{1,2}, e_{2,1}, e_{2,2}, \dots]$,

де $e_{i,j}, j = \begin{cases} 1 \\ 2 \end{cases}$, набувають значення 1 або 0 залежно від того, спотворюються

чи ні символи при передаванні каналом. Тоді синдром має вигляд

$$S_N = \begin{bmatrix} e_{1,1} + e_{1,2} \\ e_{1,1} + e_{2,1} + e_{2,2} \end{bmatrix}.$$

Приклад 4. Для матриці $(3, 1)_2$ -коду

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}; \quad m = 2 \quad H_N = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Розглянуте вище подання ЗК лінійними перевіірочними співвідношеннями є історично «найстарішим». Покажемо, що між цими співвідношеннями й перевіірочною матрицею H_N є взаємно однозначна відповідність.

Нехай $(b, b - m)_k$ -код заданий матрицею B з коефіцієнтами $\{a_{k,j}^{(\xi)}\}$ ($k = 0, 1, \dots, k - 1$, $j = 1, 2, \dots, b$; $\xi = 1, \dots, m$)

$$B = \begin{bmatrix} a_{0,1}^{(1)} & a_{0,2}^{(1)} & \dots & a_{0,b}^{(1)} \\ a_{0,1}^{(2)} & a_{0,2}^{(2)} & \dots & a_{0,b}^{(2)} \\ \dots & \dots & \dots & \dots \\ a_{0,1}^{(m)} & a_{0,2}^{(m)} & \dots & a_{0,b}^{(m)} \\ a_{1,1}^{(1)} & a_{1,2}^{(1)} & \dots & a_{1,b}^{(1)} \\ \dots & \dots & \dots & \dots \\ a_{1,1}^{(m)} & a_{1,2}^{(m)} & \dots & a_{1,b}^{(m)} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{K-1,1}^{(m)} & a_{K-1,2}^{(m)} & \dots & a_{K-1,b}^{(m)} \end{bmatrix}. \quad (2.60)$$

У першому рядку записуються коефіцієнти $a_{0,j}^{(1)}$, потім індекс ξ збільшується до величини m при незмінних нижніх індексах, після чого записується рядок з коефіцієнтами $a_{0,j}^{(1)}$ і так далі. Доцільність запису матриці B у такій формі пояснюється нижче.

Якщо падати коефіцієнти матриці H_N відповідно до рис. 2.44, то нижні m рядків цієї матриці мають вигляд

$$a_{K-1,1}^{(1)}; \dots; a_{K-1,b}^{(1)}; a_{K-2,1}^{(1)}; \dots; a_{K-2,b}^{(1)}; \dots; a_{0,b}^{(1)},$$

.....

$$a_{K-1,1}^{(m)}; \dots; a_{K-1,b}^{(m)}; a_{K-2,1}^{(m)}; \dots; a_{K-2,b}^{(m)}; \dots; a_{0,b}^{(m)}.$$

Вирази для коефіцієнтів різних рядків відрізняються один від одного тільки верхнім індексом $\xi = 1, \dots, m$. При обчисленні матричного добутку кожен з вектор-рядків помножується скалярно на вектор кодової послідовності

$$X^T = x_{i,1}, \dots, x_{i,b}, x_{i+1,1}, \dots, x_{i+1,b}, x_{i+2,1}, \dots.$$

При скалярному множенні останніх двох виразів перші b членів підсумовуємо за другим індексом $\sum_{j=1}^b a_{K-1,j}^{(\xi)} x_{i,j}$, потім так само записуємо

суму других доданків $\sum_{j=1}^b a_{K-2,j}^{(\xi)} x_{i+1,j}$ й т.д., потім всі ці суми ще раз

підсумовуємо за першим індексом (для якого введемо змінну γ) і у відповідності з (2.55) привіряємо суму нулю

$$\sum_{\gamma=0}^{K-1} \sum_{j=1}^b a_{K-\gamma-1,j}^{(\xi)} x_{i+\gamma,j} = 0, \quad \xi = 1, 2, \dots, m.$$

Виконаємо підстановку $i' = i + K - 1$; $i = i' - K + 1$. Отримаємо

$$\sum_{\gamma=0}^{K-1} \sum_{j=1}^b a_{K-\gamma-1,j} x_{i'-(K-\gamma-1),j} = 0, \quad \xi = 1, \dots, m.$$

Величина $K - \gamma - 1$ змінюється при другому підсумовуванні від $K - 1$ до 0. Виконаємо підстановку $K - \gamma - 1 = \theta$; $\gamma = K - \theta - 1$

$$\sum_{\theta=K-1}^0 \sum_{j=1}^b a_{\theta,j}^{(\xi)} x_{i'-\theta,j} = 0, \quad \xi = 1, \dots, m.$$

Змінюючи порядок 2-го підсумовування (у порядку зростання θ) та замінюючи i' на i , одержимо остаточно

$$\sum_{\theta=0}^{K-1} \sum_{j=1}^b a_{\theta,j}^{(\xi)} x_{i-\theta,j} = 0, \quad \xi = 1, \dots, m. \quad (2.61)$$

Пояснимо значення m сум (2.61). Спочатку для простоти розберемо випадок $(b, b - 1)_N$ -коду ($\zeta = m = 1$),

$$\sum_{\theta=0}^{N-1} \sum_{j=1}^b a_{\theta,j} x_{i-\theta,j} = 0, \quad (2.62)$$

що задається матрицею B вигляду

$$B = \begin{bmatrix} a_{0,1} & \dots & a_{0,1} \\ a_{1,1} & \dots & a_{1,b} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ a_{N-1,1} & \dots & a_{N-1,b} \end{bmatrix}.$$

Коефіцієнти $a_{\theta,j}$ матриці й рівняння, зазначених вище, однакові, що дозволяє легко переходити від матриці B до рівняння (2.62) і назад. Кожний рядок матриці B у лівій частині (2.62) скалярно помножується на відповідний їй ЕБ, причому при збільшенні номера рядка на 1 переходимо до раніше переданого ЕБ, в якому індекс зменшується на 1.

Приклад 5. Рівняння (2.62) для коду прикладу 1 має вигляд $x_{i,1} + x_{i,2} + x_{i-1,1} = 0$.

Відмінність рівняння (2.61) від окремого випадку (2.62) полягає в тому, що при переході до раніше переданого ЕБ зі зменшеним на 1 першим індексом перехід у матриці (2.60) здійснюється до рядка коефіцієнтів з тим самим індексом (ξ), що знаходиться на m рядків нижче попереднього. Таким чином, матрицю B можна розбити на m складових підматриць $B^{(\xi)}$, рядки яких вибираються з рядків матриці B з кроком m . Кожний з матриць $B^{(\xi)}$ відповідає своє рівняння (2.61).

Приклад 6. Приклади 2 та 4 відносяться до одного й того ж $(3,1)_2$ -коду. Перевірочним співвідношенням ЗК для $\xi = 1, 2$ відповідають підматриці

$$B^{(1)} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}; \quad B^{(2)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

2.2.2. Породжуючі багаточлени згорткового коду

У більшості літературних джерел ЗК визначаються за допомогою породжуючих багаточленів від оператора затримки D . Кожну затримку на i тактів (вважаємо, що за кожний такт передається один ЕБ) зіставимо з оператором затримки Хаффмена D^i . Дамо підпоследовності j -х символів ЕБ коду у вигляді багаточленів $X_j(D) = \sum_i x_{i,j} D^i$. У цих позначеннях перевірочні символи систематичних ЗК виражаються через інформаційні згідно з виразом:

$$X_{b-m-\xi}(D) = \sum_{j=1}^{b-m} X_j(D) f_j^{(\xi)}(D), \quad \xi = 1, \dots, m, \quad (2.63)$$

де $f_j^{(\xi)}(D)$ – породжуючі багаточлени від аргументу D . Для несистематичного коду всі b підпоследовностей виражаються співвідношеннями типу (2.63).

Приклад 7. Розглянемо код та кодову послідовність прикладу 1. Інформаційній послідовності 1101 відповідає багаточлен $X_1(D) = 1 + D + D^2$, а перевірочній підпоследовності 10111 – багаточлен $X_2(D) = 1 + D^2 + D^3 + D^4$. Очевидно, що $X_2(D) = (1 + D) X_1(D)$ (коефіцієнти при D складаються за модулем 2), тобто $f_1(D) = 1 + D$.

Виведемо співвідношення між породжуючими багаточленами систематичного ЗК і матрицею B , для чого розглянемо спочатку випадок $(b, b-1)_N$ -коду. Змінимо в (2.62) порядок підсумовування

$$\sum_{j=0}^b \sum_{\theta=0}^{N-1} a_{\theta,j} x_{i-\theta,j} = 0.$$

Підпоследовності j -х символів коду $x_{i,j}$ можна зіставити з багаточленом $X_j(D) = \sum_i x_{i,j} D^i$. Позначимо послідовність коефіцієнтів j -го стовпця матриці B через багаточлен $f_j(D)$

$$f_j(D) = \sum_{\theta=0}^{N-1} a_{\theta,j} D^\theta.$$

У цих позначеннях попередня рівність може бути написана у вигляді

$$\sum_{j=1}^b X_j(D) f_j(D) = 0.$$

Тепер (враховуючи, що операції з коефіцієнтами багаточленів виконуються над двійковим полем, в якому віднімання рівнозначне додаванню) можна записати рівняння перевірконої підпоследовності звичайного, немодульного систематичного ЗК через інформаційні символи в явному вигляді

$$X_b(D) = \sum_{j=1}^{b-1} X_j(D) f_j(D) / f_b(D).$$

Якщо правий стовпець матриці B складається з одиниць у верхньому рядку й нулів в інших місцях, тоді $f_b(D) = 0$, і ми приходимо до рівнянь модульного ЗК (2.63) і (2.54) (для $\xi = 1$). Таким чином, багаточлени $f_j(D)$ є породжуючими для $(b, b-1)_N$ -коду ($N = K$).

Вигляд останньої формули пояснює назва «модульні коди»: множини дробів багаточленів f_j / f_b , які є елементами поля, (оскільки дріб має зворотний елемент f_b / f_j), може породжувати векторний простір, а багаточлени $f_j^{(\xi)}$ у виразі (2.63) є елементами ланки й породжують модуль.

Код розмірності $(b, b-m)_K$ можна розглядати як код, що складається з m підкодів розмірності $(b-m+1, b-m)_K$ із загальними інформаційними символами, а кожний з m перевірочних символів блока належить своєму підкоду.

Для цього матрицю B (2.60) складемо так, щоб у кожному рядку з індексом ξ серед правих m коефіцієнтів, що відповідають перевірочним символам ЗК, тільки $a_{\theta, b-m+\xi}^{(\xi)}$ (для $\theta = 0, 1, \dots, K-1$) міг бути нерівним нулю. Цю вимогу назвемо *умовою обчислення*.

При виконанні умови обчислення матриця $B^{(\xi)}$ має єдиний ненульовий стовпчик, що відповідає последовності $x_{i, b-m+\xi}$ перевірочних символів коду. Позначимо

$$f_j^{(\xi)}(D) = \sum_{\theta=0}^{K-1} a_{\theta, j}^{(\xi)} D^\theta. \quad (2.64)$$

З матриць $B^{(\xi)}$ і рівнянь (2.61) отримаємо

$$\sum_{j=1}^b X_j(D) f_j^{(\theta)}(D) = 0, \quad \xi = 1, 2, \dots, m. \quad (2.65)$$

Умова обчислення для матриці B дозволяє виразити перевірочні символи через інформаційні

$$X_{b-m+\xi}(D) = \left[\sum_{j=1}^b X_j(D) f_j^{(\theta)}(D) = 0 \right] / f_{b-m+\xi}(D). \quad (2.66)$$

Приклад 8. Розглянемо код прикладів 4 і 6 ($b = 3, m = 2, N = 4$). Підматриці $B^{(1)}$ та $B^{(2)}$ не задовольняють умові обчислення, тому що в

першій з них третій стовпчик ненульовий, а повинен бути ненульовим стовпчик із номером $b - m + \xi = 2$, а в другій ненульовим є 2-й стовпчик. Перепозначимо індекси матриць і отримаємо

$$B^{(2)} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \text{ звідки } f_1^{(2)}(D) = 1; f_3^{(2)}(D) = 1 + D$$

$$X_3(D) = X_1(D)/(1 + D). \quad (2.67)$$

З матриці $B^{(1)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ як для $(b, b - 1)$ -коду (для $b = 3$) отримаємо $X_1(D)D + X_2(D)(1 + D) + X_3(D)D = 0$. Підставляючи (2.67) у це рівняння, виразимо перевірочну послідовність $X_2(D)$ через інформаційну $X_1(D)$. $X_1(D)D + X_2(D)(1 + D) + X_1(D)/(1 + D) = 0$, звідки

$$X_2(D) = D^2 / (1 + D)^2 = D^2 / (1 + D^2). \quad (2.68)$$

Відповідно до (2.68) отримаємо $B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ та

$$B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \quad (2.69)$$

Матриця B (2.69) задовольняє умові обчислення й описує в точності той самий код, що й матриця B у прикладі 4. Відзначимо, що матриця (2.69) має більше значущих рядків, ніж матриця прикладу 4. Таким чином, дійсна величина кодового обмеження визначається числом рядків матриці B , яка задовольняє умові обчислення.

Узагальнимо порядок дій у прикладі при переході від матриці B $(b, b - m)_K$ -коду до породжуючих багаточленів. З вихідної матриці B^* , що не задовольняє умові обчислення, складаються m підматриць $B^{(\xi)*}$. Позначаючи їхні коефіцієнти через $a_{i,j}^{(\xi)*}$ і представляючи стовпці підматриць у вигляді багаточленів $f_{i,j}^{(\xi)*}(D)$ аналогічно (2.60), (2.64), отримаємо систему з m рівнянь вигляду

$$\sum_{j=1}^b X_j(D) f_j^{(\xi)*}(D) = 0, \quad \xi = 1, \dots, m$$

щодо перевірочних підпослідовностей $X_j(D)$, $j = b - m + 1, \dots, b$; при цьому підпослідовності $X_j(D)$ для $j = 1, 2, \dots, b - m$ вважаються відомими. Розв'язавши цю систему методом підстановок (як у прикладі

8) або, наприклад, за методом Гаусса (звичайно, якщо рівняння системи лінійно незалежні й сумісні), отримаємо рівняння у вигляді (2.66).

Відзначимо також, що в монографії Пітерсона $(b, b - 1)_K$ -ЗК задаються у вигляді

$$X_b(D) = \sum_{j=1}^{b-1} \frac{f_j(D)}{g_j(D)} X_j(D). \quad (2.70)$$

Легко побачити, що, приводячи всі дроби у правій частині (2.70) до загального знаменника, одержимо подання коду у вигляді (2.66). Позначаючи багаточлени інформаційних підпоследовностей через $Z_K(D)$ $k = 1, \dots, b - m$, подамо несистематичний ЗК у вигляді

$$X_j(D) = \sum_{k=1}^{b-m} Z_K(D) f_k^{(j)}(D), \quad k = 1, \dots, b - m; \\ j = 1, \dots, b,$$

де $\{f_k^{(j)}(D)\}$ суть $b(b - m)$ багаточленів від аргументу D . При декодуванні несистематичних кодів у загальному випадку потрібно здійснити інверсію ЗК для отримання вихідної інформації й видачі її споживачеві. Відзначимо тільки, що в технічному виконанні такої інверсії зазвичай потреби немає, тому що при виконанні ЗК для ймовірнісних алгоритмів – послідовного декодування та алгоритму Вітербі – декодування здійснюється підбором інформаційної послідовності так, щоб кодова послідовність задовольняла критеріям алгоритму. Таким чином, у декодері потрібне лише повторне кодування інформаційної послідовності, що підбирається, але не її інверсія.

Тепер можна дати формальне визначення несистематичного ЗК.

Визначення 2. Несистематичним $(b, b - m)_K$ -ЗК називається відображення $b - m$ множини інформаційних підпоследовностей на b множин кодових послідовностей за допомогою співвідношень типу (2.66)

$$X_j(D) = \frac{\sum_{k=1}^{b-m} Z_k^*(D) f_k^{(j)}(D)}{g_j(D)}, \quad k = 1, \dots, b - m; \\ j = 1, \dots, b, \quad (2.71)$$

З формули (2.71) випливає, що кожній інформаційній послідовності $\bar{Z} = \{Z_k^*(D), k = 1, \dots, b - m\}$ відповідає своя послідовність $\bar{X} = \{X_j(D), j = 1, \dots, b\}$, але на відміну від систематичного коду в загальному випадку послідовності $Z_k(D)$ і $X_k(D)$ нерівні. Щоб з'ясувати, яке співвідношення існує між систематичними й несистематичними кодами введемо поняття еквівалентності кодів.

Визначення 3. Еквівалентними згортковими кодами називаються ЗК, що мають однакові сукупності кодових послідовностей \bar{X} .

При цьому, звичайно, у різних кодах одній й тій самій послідовності $\{X_i(D)\}$ будуть відповідати різні інформаційні послідовності $\{Z_i(D)\}$. Такі коди еквівалентні в тому розумінні, що потрібні ті самі завади в каналі зв'язку, щоб перевести одну кодову послідовність в іншу й викликати помилку декодування. Якщо символи інформаційних послідовностей випадкові й рівномірнісні, то ймовірності помилки декодування еквівалентних кодів однакові.

Теорема 1. Будь-який несистематичний код має еквівалентний йому систематичний код і несистематичний модульний код.

Для доведення теореми використовуються дві прості леми про послідовності довжини M , розглянутих від моменту часу, що відповідає D^0 , тобто за модулем D^M .

Лема 1. Якщо повна множина всіх можливих послідовностей $\{\Pi(D)\} \bmod D^M$ помножити або поділити на багаточлен $f(D)$, що не має множника D , то отримана множина послідовностей також повна.

Доведення леми 1. Припустимо, що при помноженні на багаточлен множина послідовностей виходить неповною. Тоді для двох послідовностей $\Pi_1(D)$ і $\Pi_2(D)$ маємо

$$\Pi_1(D)f(D) = \Pi_2(D)f(D) \bmod D^M,$$

звідки випливає $[\Pi_1(D) - \Pi_2(D)]f(D) = 0 \bmod D^M$, що можливо тільки за $\Pi_1 = \Pi_2$.

Аналогічно останній формулі для випадку ділення на багаточлен отримаємо $\Pi_1(D)/f(D) = \Pi_2(D)/f(D) \bmod D^M$.

Помножуючи цю рівність на $f(D)$, отримаємо останнє співвідношення, що й доводить повністю лему.

Відзначимо, що якщо $f(D)$ не має члена з D^0 , то рівність можлива й за різних Π_1 і Π_2 . Наприклад, для $M=4$ $f(D)=2$, $\Pi_1 = 1 + D + D^3$, $\Pi_2 = 1 + D$ маємо $\Pi_1(D)D = \Pi_2(D)D = D + D^2 \bmod D^4$.

Лема 2. Сума двох множин послідовностей за модулем D^M , одна з яких є повною, є також повна множина послідовностей.

Лема очевидна, тому що сума повної множини послідовностей з будь-якою послідовністю є також їхньою повною множиною.

Докладне доведення теореми можна знайти у відповідній літературі.

2.2.3. Побудова кодерів та декодерів згорткових кодів

Кодером називається пристрій, що перетворює послідовність Z інформаційних символів у кодову послідовність X відповідно до виразів (2.65) для систематичних кодерів або (2.71) для несистематичних.

Кодер будемо вважати таким, що складається з наступних основних елементів: розряду затримки регістру і суматора за модулем 2.



Рисунок 2.45 – Регістр зсуву

Як розряд затримки, так і суматори у загальному випадку можуть бути недвійковими, а зберігати й підсумувати числа за модулем $g \geq 2$. Послідовне з'єднання розрядів затримки утворює регістр зсуву (рис. 2.45), в якому зберігаються двійкові (або g -ічні) символи. В момент надходження нового символу символ, що зберігається в правому розряді, виводиться з регістру. Кожний з інших символів, що містяться в регістрі, переміщається на 1 розряд вправо, звільняючи крайній лівий розряд, куди й надходить новий символ.

З регістру зсуву й суматора будуються основні вузли кодера: схеми множення й ділення на породжуючі багаточлени. Розкриваючи в добутку багаточленів праві дужки,

$$Z_j(D)f_j(D) = (z_{0,j} + z_{1,j}D + z_{2,j}D^2 + \dots + z_{\theta,j}D^{\theta} + \dots) \times (a_{0,j} + a_{1,j} + \dots + a_{k,j}D^k + \dots),$$

можна подати процес множення як затримку помножуваної інформаційної послідовності $Z_j(D)$ на k тактів, множення всіх символів послідовності на елемент поля $- 0$ або 1 для двійкового поля або на елемент із $GF(q)$ для g -ічного поля $- i$ підсумовування всіх послідовностей, які отримані у результаті зазначених операцій. Два типи пристроїв, що виконують множення на фіксований багаточлен у модульному ЗК, показані на рис. 2.46 і 2.47.

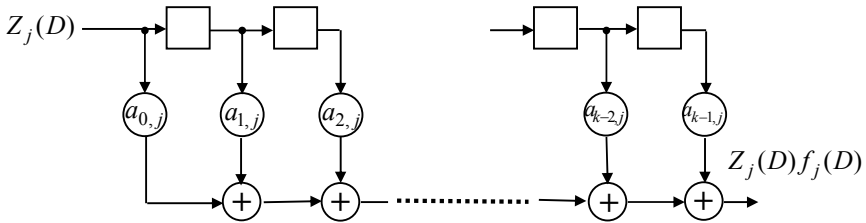


Рисунок 2.46 – Вузол помноження на багаточлен I типу

Вузол множення I типу зручний для побудови схеми множення однієї кодової послідовності на декілька фіксованих багаточленів $f_j(D)$ без збільшення числа елементів пам'яті, а вузол множення II типу зручний для множення різних послідовностей на багаточлени й наступного підсумовування, тобто для операції виду $\sum_{(j)} Z_j(D)f_j(D)$.

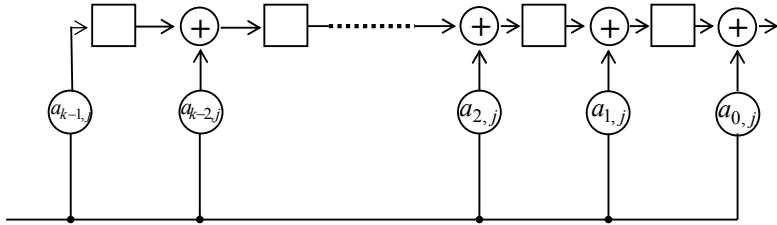


Рисунок 2.47 – Вузол помноження на багаточлен II типу

Множення на коефіцієнти у двійковому полі $a_{k,j} = \begin{cases} 0 \\ 1 \end{cases}$ реалізується

просто наявністю або відсутністю з'єднання.

Принцип побудови вузла поділу на багаточлен розберемо на конкретному прикладі. Процес поділу зручно подати таким чином, що старшим членам відповідають коефіцієнти з малими степенями D .

Приклад 9. Операцію ділення багаточлена $1 + D + D^2 + D^3 + D^4 + D^5 + D^6$ на багаточлен $1 + D + D^3$ у двійковому полі зручно подати у вигляді

$$\begin{array}{l}
 t = 0: \frac{1 + D + D^2 + D^3 + D^4 + D^5 + D^6}{1 + D + D^3} \left| \frac{1 + D + D^3}{1 + D^2 + D^3} \right. \\
 t = 2: \frac{D^2 + D^4 + D^5 + D^6}{D^2 + D^3 + D^5} \\
 t = 3: \frac{D^3 + D^4 + D^6}{D^3 + D^4 + D^6} \\
 \quad \quad \quad 0
 \end{array}$$

Із прикладу наочно видно, що щоразу, коли в послідовності діленого з'являється ненульовий символ, до неї потрібно додавати дільник і записувати ненульовий символ у частку: у прикладі це виконується в моменти часу $t = 0, 2, 3$. Потім ті ж операції виконуються із залишком.

На рис. 2.48 і 2.49 показані два варіанти схем ділення послідовності на багаточлен $1 + D + D^3$. Вузли множення й ділення відповідно I і II типів зручно комбінувати один з одним з використанням тих самих елементів пам'яті для одержання схем множення послідовності на один багаточлен і ділення на інший.

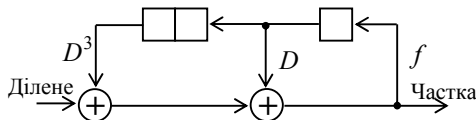


Рисунок 2.48 – Вузол ділення на багаточлен I типу

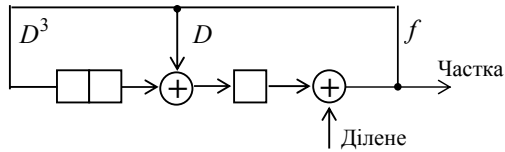


Рисунок 2.49 – Вузол ділення на багаточлен II типу

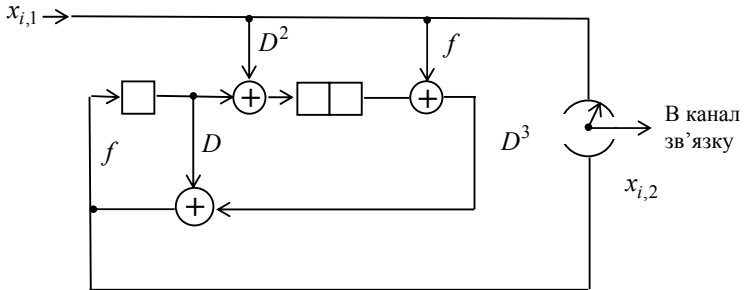


Рисунок 2.50 – Кодер систематичного (2,1)-3К

За принципом побудови згорткові кодери з операцією ділення також можуть бути розбиті на два типи. У кодері I типу чисельник (2.66) отримується шляхом затримки й накопичення інформаційних розрядів у $b - m$ регістрах і наступного підсумовування розрядів відповідно до коефіцієнтів багаточленів $f_j^{(\xi)}(D)$. Кодер I типу зручний також для реалізації несистематичних кодів, тому що в цьому випадку потрібно не більше $b - m$ регістрів пам'яті. Кодер II типу містить m схем Хаффмена, кожна з яких виконує множення на $b - m$ багаточленів. Кодери обох типів містять m схем ділення на багаточлени $f_{b-m+\xi}^{(\xi)}(D)$. Принцип побудови кодерів зручніше за все пояснити на прикладах.

Приклад 10. Кодер систематичного $(2,1)_3$ -ЗК, в якому $X_2(D) = [(1 + D^2)/(1 + D + D^3)]X_1(D)$, можна скласти, комбінуючи вузли множення I типу на багаточлен $1 + D^2$ і ділення на багаточлен $1 + D + D^3$ (рис. 2.50). Розподільувач P на 2 розряди надсилає в канал зв'язку символи: інформаційної $x_{i,1}$ та перевірконої $x_{i,2}$ кодових послідовностей у канал зв'язку.

Приклад 11. Нехай вирази (2.66) для $(5, 3)_5$ -ЗК мають вигляд

$$X_4(D) = [X_1(D)f_1^{(1)}(D) + X_2(D)f_2^{(1)}(D) + X_3(D)f_3^{(1)}(D)] / f_4^{(1)}(D);$$

$$X_5(D) = [X_1(D)f_1^{(2)}(D) + X_2(D)f_2^{(2)}(D) + X_3(D)f_3^{(2)}(D)] / f_5^{(2)}(D);$$

(тут $b = 5$, $m = 2$, $\xi = 1, 2$), де $f_1^{(1)}(D) = 1 + D + D^4$;

$$\begin{aligned}
 f_2^{(1)}(D) &= 1 + D^3 + D^4; & f_3^{(1)}(D) &= D + D^2 + D^4; \\
 f_1^{(2)}(D) &= D + D^2 + D^4; & f_2^{(2)}(D) &= D + D^3 + D^4; \\
 f_3^{(2)}(D) &= D^2 + D^3 + D^4; & f_4^{(1)}(D) &= 1 + D^2 + D^5; \\
 f_5(D) &= 1 + D^2.
 \end{aligned}$$

У кодері I типу (рис. 2.51) інформаційні символи Z за допомогою «перемикача» розподіляються на три послідовності, які в буфері вирівнюються в часі одна відносно іншої. Кожна з послідовностей надходить на вихідний розподілвач і одночасно затримується на необхідне число розрядів. Спосіб отримання добутоків багаточленів $X_{j_1}(D) \cdot f_{j_2}^{(\xi)}(D) (1 \leq j_1, j_2 \leq 3)$ зрозумілий з рис. 2.51. Потім отримані добутоків підсумовуються на двійкових суматорах і відбувається ділення на багаточлени $f_4^{(1)}(D)$ і $f_5^{(2)}(D)$ за допомогою схем розподілу I типу. Символами D^i на цих схемах позначені з'єднання, що відповідають ненульовим коефіцієнтам багаточленів $f_4^{(1)}(D)$ та $f_5^{(2)}(D)$. Перевірочні підпослідовності $X_4(D)$ і $X_5(D)$ подаються на 4 і 5 розряди розподілвача. У цьому кодері на відміну від прикладу 10 не надається можливим використовувати ті самі розряди пам'яті для множення й ділення.

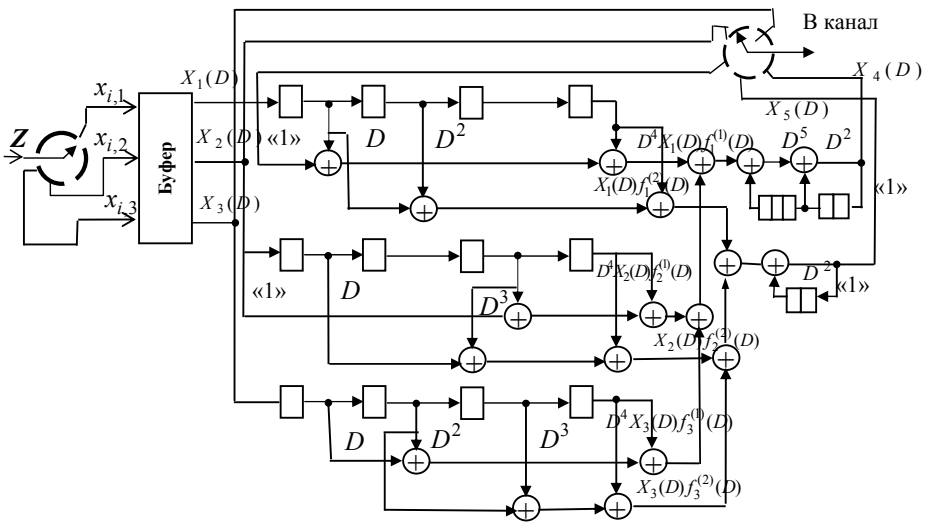


Рисунок 2.51 – Кодер $(5,3)_5$ -3K I типу

У кодері II типу (рис. 2.52) верхній регістр виконує множення інформаційних підпоследовностей $X_j(D)$ ($j=1...3$) на багаточлени $f_1^{(1)}(D)$, $f_2^{(1)}(D)$ і $f_3^{(1)}(D)$ відповідно й складання добутків, а також ділення отриманої суми на багаточлен $f_4^{(1)}(D)$. Входи підпоследовностей $X_j(D)$ на регістр мають на рис. 2.52 позначення ненульових коефіцієнтів багаточленів $f_j^{(1)}(D)$. У результаті верхній регістр формує перевіірочну підпоследовність $X_4(D)$. Аналогічно нижній регістр формує перевіірочну підпоследовність $X_5(D)$.

Найбільша довжина регістру для множення або ділення в кодерах обох типів дорівнює $K-1$.

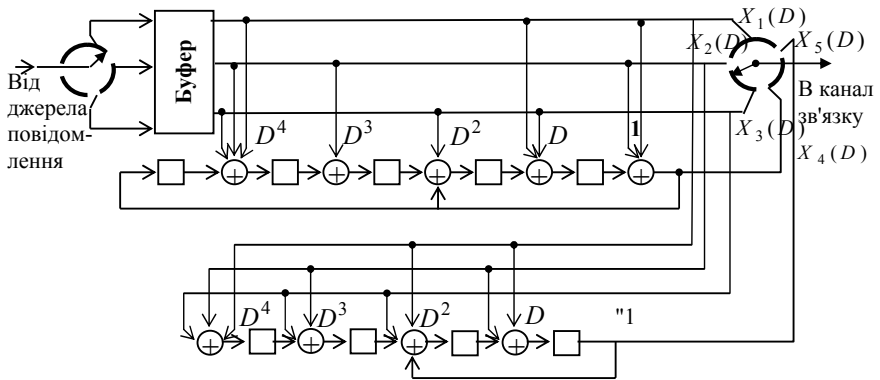


Рисунок 2.52 – Кодер II типу

Очевидно, що кодер I типу доцільно використовувати для кодів з великою інформаційною надлишковістю $m > b - m$, а також для несистематичних кодів, у той час як кодери II типу вигідніше для кодів з малою надлишковістю: $b - m > m$.

Способи отримання синдрому. Отримання синдрому S , що задовольняє формулі (2.54), є першою операцією, яка здійснюється при алгебраїчному декодуванні ЗК. Алгебраїчне декодування застосовується звичайно для систематичних кодів. Тому розглянемо спочатку способи отримання синдрому для цих кодів.

У декодері запам'ятовується N компонент синдрому, що породжуються відрізком кодової послідовності довжиною n_A символів. Тому формула (2.59) для кінцевої перевіірочної матриці H_N набуде вигляду

$$S_N = H_N Y_{n_A}, \quad (2.72)$$

де $Y = X + E$. Кінцеві послідовності S_N , Y_{n_A} можна розглядати як вектори.

Для $(b, b - m)_K$ -ЗК отримаємо m символів синдрому на кожний ЕБ; таким чином, синдром S можна подати як такий, що складається з m підпоследовностей $S^{(\xi)}$ ($\xi = 1, \dots, m$), причому в декодері запам'ятовується m підпоследовностей $S_K^{(\xi)}$ (векторів з K елементів). Кожний елемент підпоследовності S_N (2.72) являє собою скалярний добуток вектора прийманої кодової последовності Y_{nA} .

$$Y_{nA}^T = y_{i,1}, \dots, y_{i,b}, y_{i+1,1}, \dots, y_{i+1,b}, y_{i+2,1}, \dots, y_{i+K-1,b}. \quad (2.73)$$

На деякий $(km + \xi)$ -й рядок матриці $H_N = [B, T_m, B, \dots, T_m^{K-1}B]$, де $k = 0, 1, \dots, K - 1$, загальний вид матриць B та T_m поданий відповідно виразами (2.60) і (2.56). Цей рядок має вигляд

$$a_{k,1}^{(\xi)}, a_{k,2}^{(\xi)}, \dots, a_{k,b}^{(\xi)}, a_{k-1,1}^{(\xi)}, \dots, a_{0,b}^{(\xi)}, 0, 0, \dots, 0. \quad (2.74)$$

Таким чином, k -та компонента вектора $S_k^{(\xi)}$ ($k = 0, 1, \dots, K - 1$), яка дорівнює скалярному добутку (2.73) на (2.74), має вигляд

$$s_k^{(\xi)} = \sum_{\theta=0}^k \sum_{j=1}^b a_{k-\theta,j}^{(\xi)} y_{i+\theta,j} \quad \xi = 1, \dots, m. \quad (2.75)$$

Вираз (2.68) назвемо перевіркою. Оскільки $y_{i,j} = x_{i,j} + e_{i,j}$, де $e_{i,j}$ — елементи адитивного шуму, а для $y_{i,j} = x_{i,j}$ всі $s_0^{(\xi)} = 0$ відповідно до виразу (2.55), та рівність (2.75) може бути записана у вигляді

$$s_k^{(\xi)} = \sum_{\theta=0}^k \sum_{j=1}^b a_{k-\theta,j}^{(\xi)} e_{i+\theta,j}, \quad \xi = 1, \dots, m.$$

Перейдемо до багаточленної форми последовностей перевірок.

Помножимо праву частину рівності (2.64) на вираз шумової последовності $E_j(D) = \sum_{k=0}^{K-1} e_{i+k,j} D^k$. Коефіцієнт при D^k добутку багаточленів

$E_j(D) f_j^{(\xi)}(D)$ має вигляд $\sum_{\theta=0}^k a_{\theta,j} e_{i+k-\theta,j}$. Таким чином, права частина зазначеного вище рівності являє собою коефіцієнт при D^k у сумі добутків багаточленів

$$\sum_{j=1}^b f_j^{(\xi)}(D) E_j(D) = \sum_k s_k^{(\xi)} D^k = S^{(\xi)}(D). \quad (2.76)$$

Слід зазначити, що коефіцієнт при D^{K-1} має вигляд

$$s_{K-1}^{(\xi)} = \sum_{j=1}^b \sum_{\theta=0}^{K-1} a_{\theta,j}^{(\xi)} e_{(i+K-1)-\theta,j} = \sum_{j=1}^b \sum_{\theta=0}^{K-1} a_{\theta,j}^{(\xi)} y_{(i+K-1)-\theta,j},$$

що (з урахуванням можливості заміни $i + K - 1 = i'$ і потім $i' = i$) є перевірочним співвідношенням (2.61) для прийнятих символів.

Вираз (2.76) може бути реалізований шляхом затримки кодових послідовностей і підсумовування відповідних розрядів в m багатогодових суматорах (для $\xi = 1, \dots, m$). Це відповідає також і реалізації останнього виразу. Дійсно, якщо відраховувати синдром починаючи з ненульових символів, тобто $e_{i^*,j} = 0$ для $i^* < i$, то справедлива рівність

$$\sum_{j=1}^b \sum_{\theta=0}^k a_{\theta,j}^{(\xi)} e_{i+k-\theta,j} = \sum_{j=1}^b \sum_{\theta=0}^{K-1} a_{\theta,j}^{(\xi)} e_{i+k-\theta,j}.$$

Таким чином, виконавши заміну $i + k = i'$; $i' = i$, отримаємо властивості синдромів.

Властивість 1. Синдром S складається з m послідовностей $s^{(\xi)}$, визначуваних таким чином через послідовності прийнятих символів $y_{i,j}$

$$s^{(\xi)} = \sum_{j=1}^b \sum_{\theta=0}^{K-1} a_{\theta,j}^{(\xi)} y_{i-\theta,j}.$$

Приклад 12. З рівняння $(3,1)_2$ -ЗК прикладу 4 отримаємо вираз для перевірок: $s^{(1)} = y_{i,2} + y_{i,3} + y_{i-1,3}$; $s^{(2)} = y_{i,2} + y_{i-1,2} + y_{i-1,3}$, які можуть бути реалізовані у формувачі синдрому за схемою рис. 2.53. Пристрої такого типу назвемо формувачем синдрому I типу. Число запам'ятовувальних розрядів регістру для нього в точності таке саме, як і для кодера I типу; тому воно особливо зручне для ЗК із малою інформаційною швидкістю.

Для модульних систематичних кодів формувач синдрому може бути побудований за іншим принципом, перед розглядом якого доведемо наступне твердження.

Властивість 2. Перевірки $S_k^{(\xi)}$ для модульних систематичних ЗК можуть бути отримані складанням прийнятих перевірочних символів: y_{i,j^*} , де $b - m + 1 \leq j^* \leq b$ перевірочними символами y_{i,j^*}^0 , отриманими при кодуванні прийнятих інформаційних символів $y_{i,j'} (1 \leq j' \leq b - m)$.

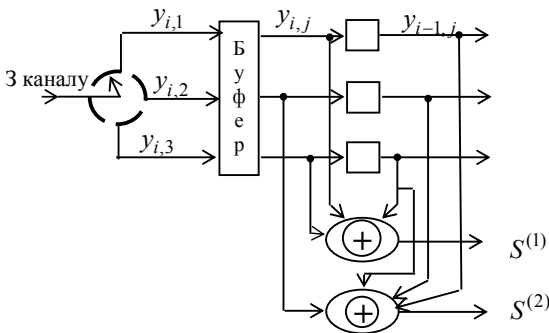


Рисунок 2.53 – Формувач синдрому I типу

Доведення. Для модульного ЗК, рівняння (2.61) аналогічне (2.52) і прикладу 5 може бути записане у вигляді

$$x_{i,b-m+\xi} + \sum_{\theta=0}^{K-1} \sum_{j=1}^{b-m} a_{\theta,j}^{(\xi)} x_{i-\theta,j} = 0$$

звідки отримаємо вираз (2.54).

Підставляючи в ліву частину останнього виразу прийняті символи $y_{i,j}$ замість $x_{i,j}$, отримаємо вираз для послідовностей символів типу

$$s^{(\xi)} = \sum_{\theta=0}^{K-1} \sum_{j=1}^{b-m} a_{\theta,j}^{(\xi)} y_{i-\theta,j} + y_{i,b-m+\xi}.$$

Відповідно до (2.54) сума в правій частині останнього виразу являє собою вираз для перевірочних символів $y_{i,j}^0$, вважаючи $y_{i,j}$ інформаційними. Звідси виходить, що

$$s^{(\xi)} = y_{i,b-m+\xi}^0 + y_{i,b-m+\xi},$$

що й доводить властивість 2.

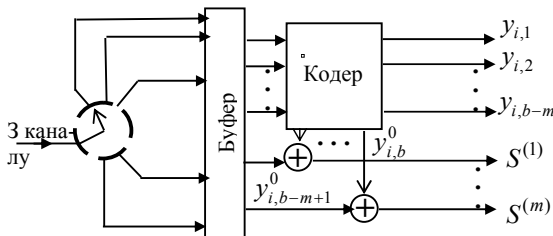


Рисунок 2.54 – Формувач синдрому II типу

Тому схема рис. 2.54 може бути використана для обчислення синдрому модульних систематичних ЗК з великою швидкістю ($b - m > m$) з використанням кодера II типу.

Таким чином, незалежно від того, є ЗК модульним чи ні, не обов'язковим є операції ділення на багаточлен при формуванні синдрому. Цей факт цілком узгоджується з тим, що одна і та сама матриця $H(D)$ є перевірконою для всього сімейства еквівалентних кодів. Виходить, у відповідності з вищенаведеними міркуваннями можна узагальнити поняття синдрому на несистематичні коди.

Визначення 4. Синдромом несистематичного ЗК (так само як і систематичного) розмірності $(b, b - m)$ називається послідовність, що являє собою вектор з m підпослідовностей, отримуваних обчисленням матричного виразу

$$\overline{Y(D)} \cdot H^T(D),$$

де $\overline{Y(D)}$ – послідовності коду $\overline{X(D)}$ на приймальній стороні, а $H(D)$ – R -матриця, зворотна матриці $G(D)$ еквівалентного базового мінімального коду.

Реалізація останнього виразу може бути виконана аналогічно схемам кодера I і II типів (без ділення), відповідно до чого можна ввести також і формувачі синдрому II типу (додатково до I типу). Проте не слід робити висновок, що формувач синдрому II типу, який аналогічно рис. 2.52 складається з m регістрів, забезпечує вираш у числі елементів пам'яті. Справа в тому, що при алгебраїчному декодуванні потрібно затримувати $b - m$ послідовностей на K тактів перед виправленням; тому загальне число елементів пам'яті, необхідних для формування синдрому ЗК, дорівнює сумі числа елементів пам'яті власне формувача синдрому $(b - m) K$ і числа елементів регістрів затримки $b - m$ послідовностей – $(b - m) K$ елементів пам'яті, тобто дорівнює числу елементів пам'яті формувача синдрому I типу, в якому здійснюється затримка послідовностей на K тактів, як впливає із прикладу на рис. 2.53.

Приклад 13. Для $(5,3)_5$ -ЗК прикладу 11 породжуюча матриця багаточленів

$$G(D) = \begin{bmatrix} 1 & 0 & 0 & (1+D+D^4)/(D+D^2+D^5)/(D+D^2+D^4)/(1+D^2) \\ 0 & 1 & 0 & (1+D^3+D^4)/(1+D^2+D^5)/(D+D^3+D^4)/(1+D^2) \\ 0 & 0 & 1 & (D+D^2+D^4)/(D+D^2+D^5)/(D^2+D^3+D^4)/(1+D^2) \end{bmatrix}.$$

Транспонована перевірюча матриця

$$H^T(D) = \begin{bmatrix} \frac{1+D+D^4}{1+D^2+D^5} & \frac{D+D^2+D^4}{1+D^2} \\ \frac{1+D^3+D^4}{D+D^3+D^4} & \frac{D+D^3+D^4}{D^2+D^3+D^4} \\ \frac{1+D^2+D^5}{D+D^2+D^4} & \frac{1+D^2}{D^2+D^3+D^4} \\ \frac{1+D^2+D^5}{1} & \frac{1+D^2}{0} \\ 0 & 1 \end{bmatrix}.$$

Транспонуємо її позбуваючись від дроблення, отримуємо

$$H^T(D) = \begin{bmatrix} 1+D+D^4 & 1+D^3+D^4 & D+D^2+D^4 & 1+D^2+D^5 & 0 \\ D+D^2+D^4 & D+D^3+D^4 & D^2+D^3+D^4 & 0 & 1+D^2 \end{bmatrix}.$$

Формувач синдрому II типу, що реалізує вираз разом з регістрами затримки інформаційних послідовностей, показаний на рис. 2.55.

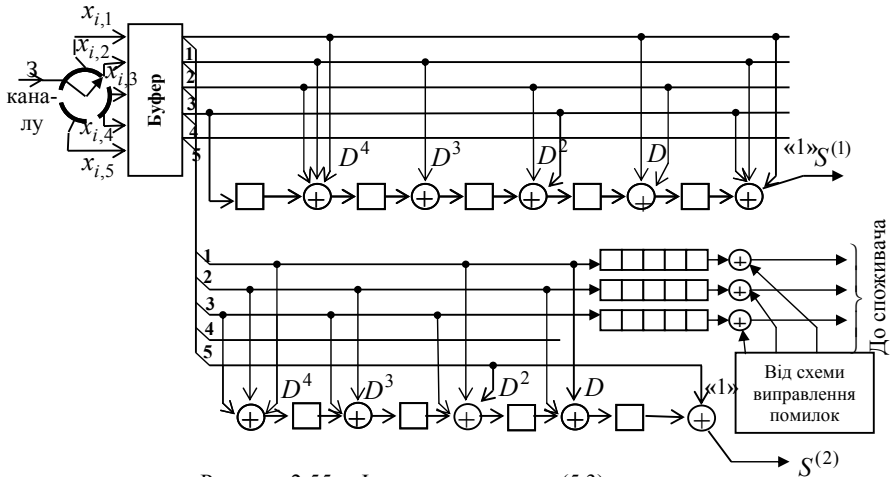


Рисунок 2.55 – Формувач синдрому $(5,3)_5$ – коду

Кодери для виправлення пачок помилок. Перший відносно простий декодер ЗК, запропонований Фінком і Шляпоберським, був призначений для виправлення пачок помилок.

Для характеристики пачки помилок треба задатися величиною проміжку між пачками $\alpha_{\text{П}}$.

Визначення 5. Пачкою помилок називається частина послідовності помилок, що починається й закінчується 1, між якими число послідовних нулів завжди менше $\alpha_{\text{П}}$, а перед першою й за останньою її одиницею розташовано не менш $\alpha_{\text{П}}$ нулів підряд.

Реалізація декодерів, призначених для виправлення пачок помилок, значно простіше, ніж для незалежних помилок, тому що легше виправити помилки, локалізовані в пачці, ніж незалежні помилки, розподілені випадковим чином у кодовій послідовності.

При корекції пачок великої довжини символи коду, що входять у перевірочні співвідношення, розносяться з кроком r з метою зменшення числа спотворених символів, що входять в одну перевірку. Це відповідає введенню $r - 1$ нульових рядків між кожними сусідніми рядками матриці B . Характеристиками ЗК, що виправляє пачки помилок, є довжина пачки l , що виправляється, і захисний проміжок α , відсутність помилок в якому гарантує виправлення пачки помилок довжиною не більше l . Для будь-якого коду можна одержати необхідну величину l шляхом вибору відповідного значення r , у той час як її α визначається структурою коду.

В «хороших» кодах прагнуть отримати величину α можливо меншою, що вступає в протиріччя з бажанням збільшення l . Чим більше

надлишковість коду, тим менша величина α може бути отримана при тому самому r . Зазначена суперечливість розв'язується шляхом компромісного вибору R , r і вибором «найкращого» для даних умов коду.

ЗК, що виправляють будь-які пачки помилок довжиною не більше l при захисному проміжку α , названі B_l -кодами (від англійського слова burst – пачка).

Опис ряду блокових і згорткових кодів, що виправляють пачки помилок, є в книзі Пітерсона. У статті Хегельбергера запропоновані $(b, b-1)_N$ -ЗК з малою надлишковістю, що виправляють пачки помилок довжиною $l = rb$ при захисному проміжку

$$\alpha = lbL(b) - 1,$$

де $L(b) = \log_2 b + 1$.

Відзначимо, що підстановка $b = 2$ в останній вираз дає $\alpha = 4l + 1$, що перевищує реалізовану величину й вказує на можливість кращого узагальнення (2,1)-ЗК.

Одним із узагальнень (2,1)-ЗК є так звані фазозалежні ЗК для виправлення пачок помилок.

Визначення 6. Фазозалежними ЗК називаються коди, що виправляють пачки помилок, які містяться повністю всередині r сусідніх ЕБ.

Ці коди будемо називати B_2 -кодами.

Таким чином B_2 -код може гарантовано виправляти пачки, що починаються з останнього символу ЕБ, довжиною

$$l = rb - (b - 1) = r(b - 1) + 1.$$

Крім того, може бути виправлена частина пачок довжиною l^* ;

$$r(b - 1) + 1 < l^* \leq rb.$$

Визначення 7. Оптимальними $(b, b - 1)_N$ -ЗК називаються B_2 -коди, що виправляють пачки помилок довжиною l при захисному проміжку α

$$\alpha = Nb - 1, \text{ де } N = r(rb - 1) + 1.$$

На перший погляд створюється враження, що фазозалежний код принципово повинен бути «гірше» B_1 -коду, тому що вводяться додаткові обмеження. Однак коди Хегельбергера значно поступаються своїми параметрами оптимальним B_2 -кодам.

Приклад 14. Порівняємо код Хегельбергера з параметрами $b = 3$, $r = 4$, $l = 12$ з оптимальним B_2 -кодом, для якого $B = 3$ і $r = 5$. Для коду Хегельбергера $\alpha = 107$. Для B_2 -коду $l = 13$, $\alpha = 77$; при цьому виправляється частина пачок довжини 14 і 15. Таким чином, параметри оптимальних B_2 -кодів істотно кращі, ніж для кодів Хегельбергера.

Розглянемо елементи аналізу ЗК, що виправляють пачки помилок.

Теорема 2. ЗК виправляє комбінації помилок типу Γ (узятих з множини Γ), якщо ніяка комбінація помилок $E = E_1 + E_2$ на довжині n_A символів, де $E_1 \in \Gamma$ та $E_2 \in \Gamma$, не призводить до нульового синдрому.

Доведення. Необхідність доводиться від протилежного. Якщо E дає нульовий синдром, то з лінійності коду випливає, що E_1 і E_2 дають однакові синдроми. Тоді комбінації помилок E_1 і E_2 не можна відрізнити один від одного, а отже, і декодувати.

Достатність випливає з того, що при виконанні умови теореми як E_1 , так і $E_2 \in \Gamma$ можна зіставити свій синдром, а це робить можливим декодування за таблицею синдромів.

Аналізувати $B2$ -коди будемо при $r = 1$. Пачки помилок, що можна виправити, для $r = 1$ повинні розміщатися тільки в одному ЕБ. За теоремою ніякі спотворення в двох різних ЕБ, що знаходяться поряд або віддалених один від одного не більше ніж на $K - 2$ ЕБ, не повинні давати нульовий синдром S_N . Кожному спотвореному символу коду відповідає стовпець матриці A_N . Сума стовпців A_N , що відповідають ненульовим символам пачки помилок $E \in \Gamma$, являє собою синдром S_N . Звідси очевидна наступна теорема.

Теорема 3. Фазозалежний ЗК виправляє пачки помилок довжиною $r(b - 1) + 1$, якщо матриця A_N коду для $r = 1$ не містить ніякої нульової лінійної комбінації стовпців, що входять у підматриці B та $T_m^i B (1 \leq i \leq K - 1)$ і включають у себе хоча би один стовпець із підматриці B .

Над стовпцями матриці B можуть вироблятися елементарні операції. Оскільки елементарні операції над стовпцями, що входять у лінійні комбінації теореми 3, змінюють одні лінійні комбінації на інші, то із цієї теореми випливає наслідок.

Наслідок. Елементарні операції над стовпцями матриці B $B2$ -коду призводять знову до матриці $B2$ -коду.

Матриці B оптимальних $B2$ -кодів розмірності $(b, b - 1)_N$ мають $N = 2b$. Наведемо достатню умову їхнього існування.

Теорема 4. Матриця B розмірності $(2b \times b)$ є матрицею оптимального $B2$ -коду, якщо всі визначники виду $|B, T_1^k B| \neq 0$ для $k = 1, 2, \dots, b$.

Доведення. Якщо визначники $|B, T_1^i B| \neq 0$ для $i = 1, 2, \dots, b - 1$, то в них не міститься нульових лінійних комбінацій стовпців. Розглянемо визначник $|B, T_1^b B|$. Він має вигляд $\begin{vmatrix} M_1 & 0_b \\ M_2 & M_1 \end{vmatrix}$, де $M_1, M_2, 0_b$ – квадратні матриці розмірності b . Матриця 0_b складається з нулів. За властивістю діагонального визначника й з урахуванням таблиці множення в полі модуля 2 маємо

$$|B, T_1^b B| = \begin{vmatrix} M_1 & 0_b \\ M_2 & M_1 \end{vmatrix} = |M_1| \cdot |M_2| = |M_1| = 1$$

для оптимального коду. Отже, стовпці матриці M_1 лінійно незалежні.

Нижня частина останньої матриці для $b = 7$ має вигляд

$$B = \begin{bmatrix} & & & & & & 1 \\ & & & & & 1 & 1 \\ & & & & 1 & 1 & 1 \\ & & & 1 & 1 & 0 & 1 \\ & & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Коди для $b < 7$ отримуються простим відкиданням нижніх $7 - b$ рядків матриці. Легко перевірити, що коди задовольняють теоремі 4.

Для фазонезалежних або $B1$ -кодів також можна сформулювати умову, аналогічну теоремі 2, для чого, на відміну від теореми 3, у якості першої потрібно брати або пачку $[x_{i,1}, x_{i,2}, \dots, x_{i,b}]$, або одну з $b - 1$ пачок

$$[x_{i,2}, x_{i,3}, \dots, x_{i,b}, x_{i+1,1}] \dots [x_{i,b}, x_{i+1,1}, \dots, x_{i+1,b-1}],$$

а в якості 2-ї пачки – всі інші $(N - 2)b + 1$ пачок, які можуть бути розміщені в захисному проміжку – замість $N - 1$ пачок помилок теореми 3.

2.2.4. Зображення згорткових кодів та оцінка їхньої кодової відстані

Перш ніж перейти до оцінок кодової відстані ЗК розглянемо приклад найпростішого згорткового кодера, призначеного для використання у двійковому каналі. Інформаційна послідовність

$$u = u_1, u_2, \dots, u_t, \dots, \quad t = 1, 2, \dots$$

находить у регістр зсуву довжини $N = 3$, деякі з розрядів якого пов'язані з двома суматорами за модулем 2. Суматори здійснюють додавання після кожного надходження нового інформаційного символу в кодер і передають результат додавання на відповідний контакт комутатора. У комутатор, поряд з вихідними символами суматорів, які іноді називаються *перевірочними*, надходить (на контакт K_1) безпосередньо із входу кодера інформаційний символ. Комутатор здійснює зчитування цих символів (перевірочних і інформаційного) після кожного їхнього надходження й передає їх у канал; символи на виході комутатора утворюють *кодovu послідовність*.

Тому що на кожний інформаційний символ припадає три символи кодової послідовності, швидкість передавання по каналу дорівнює $R = \frac{1}{3}$.

Зображений на рис. 2.56 кодер є *систематичним* кодером, оскільки по каналу, поряд з перевірочними символами, передаються й інформаційні

символи. Якщо забрати відвід, що з'єднує вхід кодера з контактом K_1 , і сам контакт, отримаємо несистематичний згортковий кодер зі швидкістю передавання $R = \frac{1}{2}$.

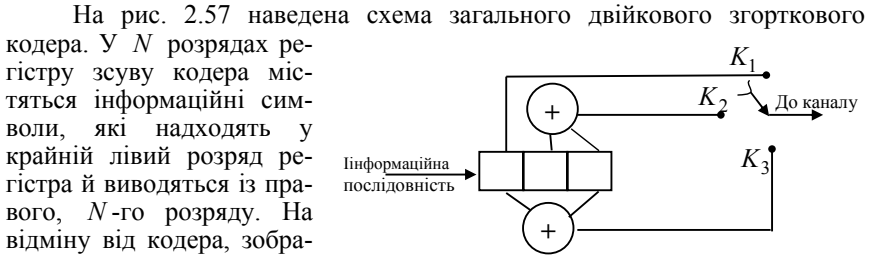


Рисунок 2.56 – Найпростіший двійковий згортковий кодер

На рис. 2.57 наведена схема загального двійкового згорткового кодера. У N розрядах регістру зсуву кодера містяться інформаційні символи, які надходять у крайній лівий розряд регістра й виводяться із правого, N -го розряду. На відміну від кодера, зображеного на рис. 2.56, комутатор робить зчитування вихідних символів суматорів, число яких дорівнює m , $m = 2, 3, \dots$, не після кожного надходження інформаційного символу, а після кожних l , $l = 1, 2, \dots$ символів (відповідно після кожних l зсувів регістру). З міркувань зручності надалі будемо вважати, що N завжди вибирається кратним l . Позначимо відношення $\frac{N}{l} = n$.

Легко бачити, що швидкість передавання розглянутого кодера $R = \frac{l}{m}$.

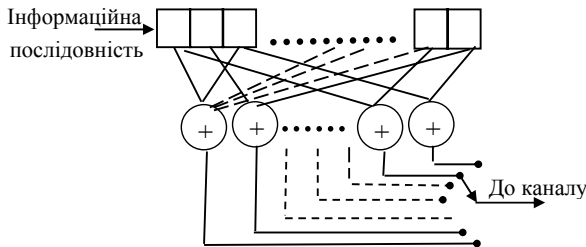


Рисунок 2.57 – Загальний двійковий згортковий кодер

Для того щоб задати двійковий згортковий кодер, необхідно зазначити, які розряди регістру зсуву пов'язані з кожним із суматорів за модулем 2. Зв'язки i -го суматора за модулем 2 описуються шляхом завдання i -х породжуючих послідовностей.

Вихідний сигнал i -го суматора (після надходження t -го символу u_t) дорівнює

$$s_i(t) = g_{i1}u_t \oplus g_{i2}u_{t-1} \oplus \dots \oplus g_{iN}u_{t-N+1}, \quad (2.77)$$

де $u_t = 0$ при $t \leq 0$.

Породжуючі послідовності повністю визначають структуру двійкового кодера.

Доречно відзначити тут наступну просту, але важливу властивість згорткових кодерів.

Лема 3. Для будь-якого згорткового кодера сума $\xi \oplus \xi'$ кодових послідовностей ξ і ξ' відповідних інформаційним послідовностям u і u' , є кодова послідовність, яка відповідає інформаційній послідовності $u \oplus u'$.

Лема безпосередньо випливає з (2.77) і визначення суми ξ і ξ' за модулем 2. Коди, що мають властивість, сформульовану в лемі 3, називаються *лінійними*.

Кодер на рис. 2.57 є несистематичним згортковим кодером. Його можна перетворити в систематичний згортковий кодер, якщо перший суматор зв'язати лише з першим розрядом регістру, другий – із другим розрядом, l -й – лише з l -м розрядом (передбачається, що число суматорів m завжди більше l).

Важливою характеристикою кодера є довжина кодового обмеження $v = nt$, що лінійно залежить від довжини регістру N . *Довжиною кодового обмеження* називається число кодових символів, породжуваних кодером у проміжку часу між надходженням у нього даного інформаційного символу й виведенням його з регістру. Довжина кодового обмеження відіграє в теорії згорткових кодів роль, аналогічну довжині блока в теорії блокових кодів. Для спрощення формулювань надалі будемо використовувати термін (R, v) -кодер. Він означає згортковий кодер зі швидкістю передавання R й довжиною кодового обмеження v .

Розглянутий вище згортковий кодер – це кінцевий автомат, стан якого U_T в момент після надходження інформаційного підблока $u_T^{(l)}$ визначається n підблоками, що зберігаються в регістрі зсуву

$$U_T = \{u_{T-n+1}^{(l)}, \dots, u_{T-1}^{(l)}, u_T^{(l)}\}. \quad (2.78)$$

Роботу кінцевого автомата зручно описувати за допомогою *діаграми станів*. Діаграма станів згорткового кодера, зображеного на рис. 2.56, показана на рис. 2.58. Стрілками показані можливі переходи між станами; уздовж стрілок записані кодові символи, які генеруються кодером при цих переходах.

Стан кодера $U_T = \{0, 0, \dots, 0\}$ будемо називати *нульовим*, інші стани називаються *ненульовими*.

Розглянемо дві інформаційні послідовності

$$u = u_1^{(l)}, u_2^{(l)}, \dots, u_T^{(l)} \quad (2.79)$$

i

$$u' = u_1^{(l')}, u_2^{(l')}, \dots, u_T^{(l')}, \quad (2.80)$$

які можуть надходити у згортковий кодер, довжина регістру якого розрахована на зберігання n підблоків. Ці послідовності й стани кодерів, у які надходять ці послідовності, називаються *суцільними* в T -му підблоці, якщо

$$u_{T-n+1}^{(l)} = u_{T-n+1}^{(l')}, \dots, u_{T-1}^{(l)} = u_{T-1}^{(l')}, u_T^{(l)} = u_T^{(l')}, \quad T = 0, 1, 2, \dots \quad (2.81)$$

(за визначенням будемо вважати $u_T^{(l)} = u_T^{(l')}, T < 0$).

Розглянемо два можливих стани довільного згорткового кодера в момент після надходження T -го блока:

$$U_T = (u_{T-n+1}^{(l)}, \dots, u_{T-1}^{(l)}, u_T^{(l)}), \quad (2.82)$$

$$U_T' = (u_{T-n+1}^{(l')}, \dots, u_{T-1}^{(l')}, u_T^{(l')}). \quad (2.83)$$

Нехай виконується $u_{T-i}^{(l)} \neq u_{T-i}^{(l')}, u_{T-i+1}^{(l)} = u_{T-i+1}^{(l')}, \dots, u_T^{(l)} = u_T^{(l')}$.

Величина it називається *ступенем злиття* між станами U_T й U_T' ; тут t – число кодових символів у підблоці. Якщо $U_T = U_T'$, тобто стан суцільний, за визначенням вважаємо ступінь злиття рівним v .

Поряд з діаграмою станів зручним апаратом для дослідження декодування є *кодове дерево*. На рис. 2.59 показано кодове дерево для згорткового кодера, зображеного на рис. 2.56. Точками виділені *вузли* кодового дерева. Крайній ліворуч вузол називається *початковим*. Відрізки між сусідніми вузлами називаються *ребрами*. Сукупність декількох послідовних ребер називається *гілкою*.

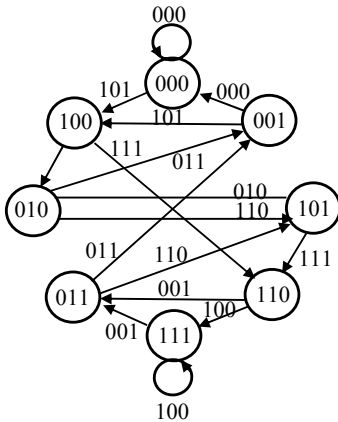


Рисунок 2.58 – Діаграма станів згорткового кодера, зображеного на рис. 2.56

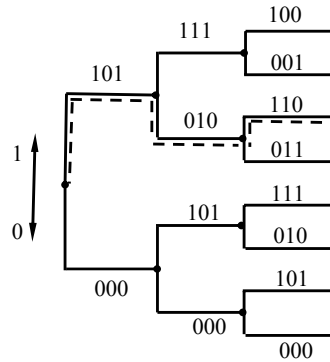


Рисунок 2.59 – Кодове дерево для згорткового кодера, зображеного на рис. 2.56

Кожний вузол відповідає певній інформаційній послідовності на вході кодера. Початковий вузол відповідає моменту, коли в кодер ще не надходила інформаційна послідовність. Щоб визначити, який вузол відповідає даній інформаційній послідовності, необхідно рухатися з початкового вузла по кодовому дереву, роблячи з вузла крок вниз, якщо інформаційний символ, що надходить, дорівнює 0, і крок вгору, якщо він дорівнює 1. Записані уздовж прохідного шляху нулі й одиниці являють собою кодові символи, що відповідають даній інформаційній послідовності. На рис. 2.59 пунктиром показано шлях, що відповідає інформаційній послідовності 101.

Надалі в тих випадках, коли це не викликає непорозуміння, будемо ототожнювати ребра й гілки з відповідними їм кодовими символами, а вузли – з кодовими інформаційними символами, записаними уздовж гілок, що з'єднують цей вузол з початковим. *Довжиною* гілки будемо називати число кодових символів у ній, *глибиною* вузла будемо називати число кодових символів у гілці, що з'єднує цей вузол з початковим. Сукупність вузлів, що належать одній гілці, глибина яких не перевищує t , називається *t -зрізаною гілкою*. Два вузли, відділені одним ребром, називаються *сусідніми*. Вузол, відділений від даного одним ребром і лежить на більшій глибині, називається *безпосередньо наступним* за ним. Вузол, відділений від даного одним ребром і лежить на меншій глибині, називається *безпосередньо попереднім* даному. Вузли, що мають загальний безпосередньо попередній вузол, називаються *суміжними*.

На рис. 2.59 з кожного вузла виходить два ребра, а кожне ребро складається із трьох двійкових символів, що відповідає швидкості передавання $\frac{1}{3}$. У випадку загального згорткового кодера з кожного ребра виходять $L = 2^l$ ребер і кожне ребро складається із t двійкових символів.

Розглянемо довільне ребро S кодового дерева, зумовлене вузлом, з якого воно виходить, і вузлом, яким воно закінчується. Назвемо *S -піддеревом* сукупність вузлів кодового дерева, в яких гілка, що з'єднує його з початковим вузлом, містить ребро S ; t -зрізаним *S -піддеревом* назвемо сукупність тих вузлів S -піддерева, глибина яких не більше t .

Уведемо також додаткові визначення, пов'язані з передачею конкретної інформаційної послідовності. *Правильною* гілкою кодового дерева назвемо гілку, що відповідає переданій інформаційній послідовності. *Першим неправильним піддеревом* називається сукупність вузлів кодового дерева, у яких гілка, що з'єднує його з початковим вузлом, не містить ніяких вузлів правильної гілки, крім першого, початкового вузла. Аналогічно *i -м неправильним піддеревом* називається сукупність вузлів кодового дерева, у яких гілка, що з'єднує його з початковим вузлом, містить у собі 1-, 2-, ..., i -й вузол правильної гілки, і не містить $(i+1)$ -й вузол.

Перш ніж переходити до аналізу процесів кодування й декодування, сформулюємо вимоги до кодера й побудованого на його основі декодера. Першою основною властивістю кодера повинне бути його практичне здійснення, що залежить від *складності* кодера. Складність згорткового кодера визначається числом його найпростіших елементів, якими є розряди в регістрі зсуву, суматори за модулем 2 і зв'язки суматорів з розрядами регістру зсуву. Відзначимо, що практично число суматорів рідко перевищує 5, довжина регістру зсуву має порядок декількох десятків одиниць, а кожний суматор зв'язаний приблизно з половиною розрядів регістру. Тому можна вважати, що складність згорткового кодера лінійно залежить від довжини регістру або від довжини кодового обмеження.

Друга вимога, що ставиться до кодера – *надійність* виробленого ним кодування, зумовлена ймовірністю правильного декодування. Очевидно, що не кожний вибір зв'язків у згортковому кодері призведе до задовільної побудови кодера. Наприклад, свідомо погано зв'язувати кожний із суматорів з тими самими розрядами регістру. Тому, насамперед, необхідно переконатися в існуванні кодера, в якого надійність виробленого ним кодування задовольняла б проектувальника.

Значною мірою надійність кодування визначається сукупністю кодових відстаней між послідовностями, породжуваними кодером.

Нехай $\xi^{(\tau)}$ – довільна кодова послідовність довжини τ на виході згорткового кодера. *Вагою* d цієї послідовності називається число одиниць у цій послідовності $d = d(\xi^{(\tau)})$. *Відстанню Хеммінга* між двома послідовностями на виході згорткового кодера $\xi^{(\tau)}$ й $\xi^{(\tau)'}$ називається вага їхньої суми за модулем 2

$$d = d(\xi^{(\tau)} \oplus \xi^{(\tau)'}) ,$$

де додавання за модулем 2 між двома векторами визначено вище. Надалі ми будемо вивчати відстань Хеммінга між різними гілками кодового дерева.

Таким чином, відстань Хеммінга між двома кодовими послідовностями визначається числом символів, в яких вони відрізняються. Аналогічно блоковому випадку умовимося говорити, що декодування правильне, якщо всі символи на виході декодера збігаються з переданими, і неправильним – у протилежному випадку. Зрозуміло, що якщо відстань Хеммінга переданої кодової послідовності від будь-якої іншої можливої послідовності не менше, ніж $d_{\text{мін}}$, декодер може правильно декодувати її в усіх випадках, коли при передаванні було спотворено не

більш ніж $\left\lfloor \frac{d_{\text{мін}} - 1}{2} \right\rfloor$ символів, де $\lfloor x \rfloor$ означає цілу частину числа x . Тому

однією з характеристик надійності кодування (правда, не завжди достатньою) є мінімальна відстань між кодовими послідовностями.

При теоретичному розгляді звичайно обмежуються знаходженням відстаней між кодovими послідовностями, які відповідають інформаційним послідовностям з відмінними першими підблоками (інші підблоки можуть бути довільні).

Розглянемо довільний згортковий (R, v) -кодер. Зафіксуємо довільну кодову послідовність $\xi^{(\tau)}$. Нехай для початку $\tau \leq v$. За визначенням, будемо вважати цю гілку правильною. Розглянемо безліч гілок її першого неправильного τ -зрізаного піддерева. Позначимо через $\upsilon(d, v, \tau)$ число кодovих послідовностей цього піддерева, відстань яких до послідовності $\xi^{(\tau)}$ дорівнює d .

Відповідно до значення d відстань між двома кодovими послідовностями дорівнює вазі їхньої суми за модулем 2. Додамо послідовність $\xi^{(\tau)}$ за модулем 2 до всіх гілок кодового дерева. При цьому відповідно до леми 3 послідовність $\xi^{(\tau)}$ перейде в кодову послідовність, що відповідає нульовій (тобто цілком складається з нулів) інформаційній, а кодovі послідовності її першого неправильного піддерева перейдуть у кодovі послідовності першого неправильного піддерева для нульової інформаційної послідовності.

Таким чином функція $\upsilon(d, v, \tau)$ не залежить від вибору послідовності $\xi^{(\tau)}$ й знаходиться шляхом підрахунку ваг кодovих гілок у першому неправильному τ -зрізаному піддереві. Величина $\upsilon(d, v, \tau)$, розглянута як функція d , називається τ -спектром коду. Максимально можливе значення d , рівне d_{\min} , таке, що при $d < d_{\min}$ функція $\upsilon(d, v, \tau)$ перетворюється на нуль, називається мінімальною кодовою відстанню.

Тепер розглянемо випадок $\tau > v$. Нехай нас цікавить мінімальна відстань кодової послідовності $\xi^{(\tau)}$ до кодovих послідовностей її першого неправильного піддерева. Без обмеження спільності можна вважати, що $\xi^{(\tau)}$ відповідає нульовій інформаційній послідовності. Якщо, у першому неправильному піддереві є вузли, в яких ступінь злиття з правильною гілкою дорівнює v . З кожного такого вузла виходить одна гілка, в якій всі наступні символи збігаються із символами правильної гілки. Отже, при знаходженні мінімальної відстані не обов'язково розглядати всю гілку, можна обмежитися розглядом відстані між гілками лише до моменту їхнього злиття.

Дамо визначення τ -спектра у випадку $\tau > v$.

Вузол розглянутого піддерева називається (τ, v) -істотним, якщо:

- а) його глибина дорівнює τ , або
- б) його ступінь злиття з правильною гілкою дорівнює v .

У більшості випадків (τ, v) -істотні вузли будемо називати просто істотними.

У даних позначеннях функція $\upsilon(d, \nu, \tau)$ визначається як *число істотних вузлів першого неправильного піддерева, вага яких дорівнює d* .

Спектр характеризує згортковий код безвідносно до каналу, по якому виконується передавання. Надійність методу кодування – декодування при передачі по конкретному каналу характеризує ймовірність правильного декодування.

Однією з найважливіших характеристик згорткового коду є його *вільна відстань* – d_f . Воно визначається, як мінімальна вага шляху по модифікованій діаграмі коду з вузла S_0 , що ліворуч, до вузла S_0 , що праворуч. Значення d_f легко визначити з вигляду породжуючої функції, оскільки воно дорівнює показнику степеня біля змінної D у першому члені ряду. Так, наприклад, для розглянутого коду (5,7) $d_f = 5$. Вільна відстань для лінійного згорткового коду збігається зі значенням мінімальної кодової відстані і значною мірою визначає завадостійкість системи зв'язку. Якщо код нелінійний, то пошук мінімальної кодової відстані вимагає набагато більше ресурсів, тому що в цьому випадку мінімальну кодову відстань необхідно вираховувати порівнюючи всі можливі кодові комбінації між собою, а не тільки з нульовою кодовою комбінацією.

При розрахунку завадостійкості лінійних згорткових кодів важливе значення має *ваговий спектр* коду. Його можна отримати із породжуючої функції, якщо привласнити змінній $L = 1$. В такому випадку породжуюча функція для коду (5,7) набуває вигляду

$$T(D, N) = D^5 N + 2D^6 N^2 + \dots + 2^m D^{5+m} N^{1+m} + \dots, \quad (2.84)$$

потім слід знайти похідну від функції за змінною N і привіняти $N = 1$, тоді отримаємо вираз

$$\left. \frac{dT(D, N)}{dN} \right|_{N=1} = D^5 + 4D^6 + 12D^7 + \dots + (1+m)2^m D^{5+m} + \dots. \quad (2.85)$$

Згідно з цим виразом, код має одну напівнескінченну послідовність вагою 5 одиниць, чотири послідовності вагою 6, дванадцять послідовностей вагою 7 і так далі.

У загальному вигляді цей вираз можна записати у вигляді

$$\left. \frac{dT(D, N)}{dN} \right|_{N=1} = \sum_k w_k D^k, \quad (2.86)$$

де $k \geq d_f$ – ціле число. Набір коефіцієнтів w_k називається ваговим спектром згорткового коду. Спектр коду називає загальну кількість помилок на виході декодера, якщо замість правильної кодової комбінації при декодуванні буде обрано помилкову. Таким чином, ймовірність помилки на біт на виході декодера $p < w_k P_k$, де P_k – ймовірність обрання при декодуванні помилкової комбінації ваги $d = k$.

$$P_k = \begin{cases} \sum_{i=\frac{k+1}{2}}^k C_k^i P_0^i (1-P_0)^{k-i}, & \text{при непарному } k \\ \frac{1}{2} C_k^{k/2} P_0^{k/2} (1-P_0)^{k/2} + \sum_{i=\frac{k}{2}+1}^k C_k^i P_0^i (1-P_0)^{k-i}, & \text{при парному } k \end{cases}, \quad (2.87)$$

де P_0 – середня ймовірність помилки символу в каналі.

Наприклад, для каналів із ФМ-2 або ФМ-4

$$P_0 = \operatorname{erf} \left(\sqrt{\frac{2E_b}{N_0}} \right),$$

де $\operatorname{erf}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$ – інтеграл помилок.

Тоді, для коду з відносною швидкістю кодування R

$$P_k = \operatorname{erf} \left(\sqrt{\frac{2kE_b R}{N_0}} \right),$$

а ймовірність помилки біта на виході декодера не перевищує значення

$$P \leq \sum_{k=d_f}^{\infty} w_k P_k.$$

Таким чином, знаючи спектр коду можливо обчислити його характеристики завадостійкості. Найпоширенішою характеристикою вимірювання завадостійкості є енергетичний виграш кодування (ЕВК). ЕВК визначає на скільки, порівняно з некодованим передаванням сигналу, можна зменшити енергію сигналу в каналі залишивши незмінною ймовірність помилки.

Якщо для коду відома тільки вільна відстань d_f , то можна розрахувати асимптотичний енергетичний виграш кодування (АЕВК), тобто приблизну величину завадостійкості. Так, якщо в каналі застосовано модуляцію ФМ-4 або ФМ-2, то АЕВК легко розрахувати за виразом

$$\text{АЕВК} = 10 \log \frac{2d_f}{4}, \quad [\text{дБ}], \quad (2.88)$$

а якщо відомо спектр коду, то ймовірність помилки можна обчислити з більшою точністю.

На жаль не всі згорткові коди можна використовувати для боротьби з помилками. Такі коди дістали назву *катастрофічних кодів*. У них кожен кодову послідовність породжує більше, ніж одна інформаційна послідовність. Наприклад, розглянемо двійковий згортковий код (3,3). Інформаційна послідовність $B_1 = \{\dots, 0, 0, 0, \dots\}$ породжує кодову послідовність $S_1 = \{\dots, 00, 00, 00, \dots\}$, інформаційна послідовність $B_2 = \{\dots, 1, 1, 1, \dots\}$ породжує кодову послідовність $S_2 = \{\dots, 00, 00, 00, \dots\}$, яка

нічим не відрізняється від послідовності S_1 . Таким чином, декодер за кодовою послідовністю не може винести рішення про те, яка інформація передавалась за будь-який інтервал часу. Тобто виникає «катастрофа», пов'язана з неможливістю прийому.

Універсальною ознакою катастрофічного коду є те, що визначальник його матриці переходів дорівнює 0. Стосовно лінійних двійкових згорткових кодів є більш очевидна ознака, а саме, якщо кожний породжуючий поліном згорткового коду має парну кількість зв'язків, то цей згортковий код катастрофічний. Такі коди неможливо використовувати в каналах зв'язку.

2.2.5. Методи декодування згорткових кодів

Процес декодування будь-якого коду полягає у виборі такої можливої переданої кодограми X_j , яка віддалена від прийнятого сигналу Z_j на мінімальну відстань, в результаті чого ймовірність $P_{X_j}(Z_j)$ є максимальною. Оцінка ймовірності $P_{X_j}(Z_j)$ при послідовному декодуванні згорткових кодів відбувається не при повній довжині n сигналу Z_j , а послідовно при довжині груп символів, що приймаються, $v, 2v, \xi v, \dots, n$. Якщо при v символах ймовірність $P_{X_j}(Z_j)$ більше деякого порогового значення P_0 , то аналіз продовжується при значенні $2v$ і т. п. Якщо ж при ξv виявляється, що $P_{X_j}(Z_j) < P_0$, то кодограма X_j вважається малоімовірною і відкидається (оцінка ймовірності передачі X_j при довжинах груп символів $gv < \xi v$ не робиться). Деревовидна структура кодового дерева дозволяє виключити із розгляду всі n -значні кодограми, які співпадають з відкинутою імпульсною послідовністю у перших ξv розрядах. Дуже правдоподібно, що невірні послідовності будуть відкинуті в процесі розв'язання при малому ξv . Це дозволяє виключити із розгляду значну кількість помилкових послідовностей символів за невеликого обсягу обчислень.

Процес декодування являє собою рух по кодовому дереву, коли кодоперетворювач намагається побудувати m -гілчастий шлях до однієї з 2^T його вершин, при цьому він формує гіпотетичну послідовність X_j і порівнює її з Z_j .

Нехай в процесі декодування символу x , проходиться шлях із l_v гілок ($0 < l_v < m$); при цьому створюється функція розузгодження.

$$\theta_p(l_v) = Z_j(l_v) \oplus X_{r_j}(l_v) = (X_j(l_v) \oplus X_{r_j}(l_v)) \oplus U_{ш}(l_v), \quad (2.89)$$

де $U_{ш}(l_v)$ – реалізація завади.

Для аналізу шлях по кодовому дереву зручно уявити в координатах (θ_p, l_v) . Якщо при кожному кроці декодування розв'язання правильне, то

$X_{rj}(l_v) = X_j(l_v)$ і $\theta_p(l_v) = U_{ш}(l_v)$. Цей випадок відповідає руху за вірними гілками дерева і для (1/3)-коду і однієї із реалізацій $U_{ш}(l_v)$ показаний на рис. 2.60.

За помилкового розв'язання $X_{rj}(l_v) \neq X_j(l_v)$ і функція $\theta_p(l_v)$ визначається виразом (2.89). Цей випадок показаний на рис. 2.60, б. Пунктирні лінії відображають збільшення кодової відстані (1/3)-коду зі зростанням l_v при різній кількості помилок. Декодууючий пристрій буде рухатись по одній з цих ліній; при появі додаткових помилок пристрій переходить на іншу лінію. Таким чином, величина $\theta_p(l_v) = f(l_v, U_{ш})$.

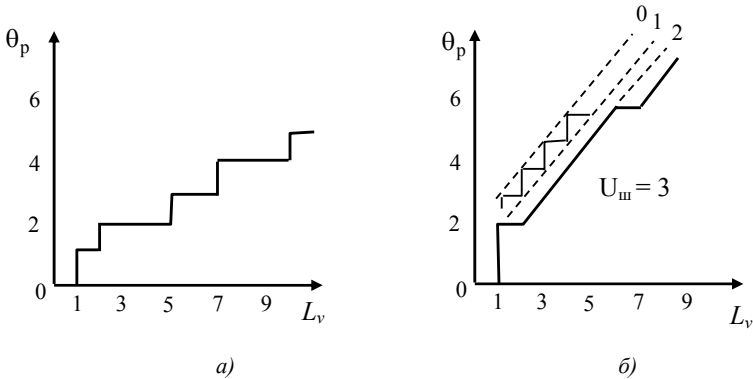


Рисунок 2.60 – Функція розузгодження $\theta_p(L_v)$

Функція $\theta_p(l_v)$ являє собою вектори помилок змінної довжини. На кожному кроці пошуку визначається її вага:

$$w_p(l_v) = ((X_j(l_v) \oplus X_{rj}(l_v)) \oplus U_{ш}(l_v)) = d(l_v)$$

Якщо для деякого кроку величина $d(l_v)$ не перевищує деякого допустимого значення $D_{п}$, відповідна гілка кодового дерева вважається прийнятною і аналізуються наступні гілки. Якщо ж $d(l_v) > D_{п}$, то обраний шлях вважається малоймовірним і кодоперетворювач повертається назад до найближчої недослідженої гілки дерева, для якої $d(l_v) < D_{п}$, і знову починає рухатися вперед по шляху, де ця умова виконується. Відкидання малоймовірної гілки кодового дерева і всіх наступних з нею зв'язаних гілок суттєво зменшує множину досліджуваних комбінацій символів. Якщо ж знову $d(l_v) > D_{п}$, то робиться ще один крок назад і т.п. до того часу, поки не буде знайдена послідовність X_{rj} , яка відрізняється від Z_j на допустимому кількості символів на повній довжині пошуку. Тоді перший інформаційний символ вважається остаточно декодованим, початок відліку в послідовності символів, що приймається, переноситься до сусіднього вузла дерева і починає аналізуватися його чергове ребро. Оскільки малоймовірні

послідовності символів вилучаються у процесі розв'язання, то величину D_{Π} будемо називати *порогом розузгодження*.

Приклад 16. Повідомлення $S = 1001$, закодоване (1/5)-кодом в канонічній формі, утворює кодограму $X_j = 11111 \ 01010 \ 00111 \ 11100$, показану на рис. 2.61 жирною лінією. Нехай вектор завади $U_{\text{ш}} = 0$, тоді декодувальний пристрій вибере в першому вузлі кодового дерева те ребро, яке співпадає з першою $v = 5$ -значною групою символів прийнятої послідовності Z_j . Тим самим задається напрямок на другий вузол, де буде обрано ребро, співпадаюче з 5-значною групою символів Z_j і т.д. Очевидно, що в розглядуваному випадку процедура декодування не викликає ускладнень.

У каналі з шумами повного співпадання ребер гілок кодового дерева не може бути. Тому в кожному вузлі обирається те ребро, яке відстоїть від Z_j на мінімальній відстані. Нехай, наприклад, $U_{\text{ш}} = 10100 \ 10101 \ 00000 \ 01000$, тоді $Z_j = 01011 \ 11111 \ 00111 \ 10100$. В цьому випадку декодування відбувається вірно до вузла a , а потім буде обраний помилковий шлях до вузла b . Проте в подальшому помилка буде виявлена, оскільки жодна гілка, що лежить за вузлом b , не розташована так близько до Z_j , як вірна гілка, і код перетворювач повернеться до вузла a і далі піде вірним шляхом.

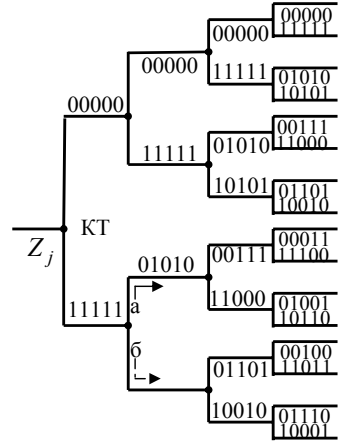


Рисунок 2.61 – Пошук шляху при послідовному декодуванні

Вибір величини порога розузгодження суттєво впливає на ймовірність помилки декодування й обсяг обчислень. Розглянемо деякі алгоритми вибору D_{Π} .

Алгоритм Возенкрафта. Цей алгоритм заснований на ймовірнісному тлумаченні величини D_{Π} . Задамося деяким додатним числом a_k , яке називається *ймовірнісним критерієм*, таким що ймовірність появи на шляху із l_v ребер D_{Π} або більше помилок не перевищувала величини 2^{-a_k} . За такого завдання a_k є функція l_v , яка задовольняє умові:

$$p(d(l_v) > D_{\Pi}) < 2^{-a_k}. \quad (2.90)$$

При декодуванні може використовуватися один канал або декілька ймовірнісних критеріїв і відповідні їм пороги розузгодження D_{Π} .

З точки зору простоти декодуєчого пристрою доцільно задати лінійний закон зміни $\theta_p(l_v)$ зі зміною довжини пошуку (пряма I на рис. 2.62, a , тангенс куту нахилу якої дорівнює νp_0). Величина $d(l_v)$

вздовж вірного шляху декодування буде відображатися кривою II. Пунктирні криві III та IV відповідають зміні величини $d(l_v)$ вздовж неправильного шляху декодування із початкового ($l_v=0$) і проміжного $l_v = j$ вузлів кодового дерева.

Являє інтерес гранична оцінка обсягу обчислень N_0 , який повинен проробити декодуючий пристрій для виявлення правильного шляху на кодовому дереві. При цьому в одне обчислення входять визначення ваги $d(l_v + 1)$ за вагою $d(l_v)$ та символах $x_{v(l_v+1)}$ і $z_{v(l_v+1)}$ послідовностей X_{rj} та Z_{rj} і порівняння $d(l_v+1)$ з $D_{\Pi}(l_v + 1)$:

$$d(l_v + 1) = d(l_v) + (x_{v(l_v+1)} \oplus z_{v(l_v+1)}) \geq D_{\Pi}(l_v + 1)$$

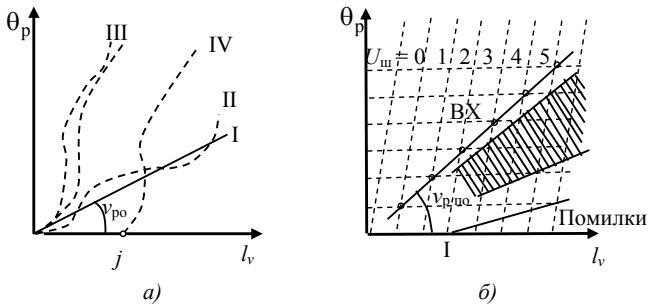


Рисунок 2.62 – Характеристики однопорогового декодуючого пристрою

Звідси виходить, що за заданого a_k величина N_0 зростає лінійно зі збільшенням n . Звідси можна зробити висновок щодо доцільності однопорогового декодувального пристрою, який використовує один критерій a_k . Проте такий алгоритм не дає достатньо хороших результатів. Дійсно, помилка при декодуванні символу x_j може відбутися у двох випадках:

- якщо відкинута вірна підмножина гілок кодового дерева, а в невірній підмножині є хоча б одна послідовність, яка задовольняє обраному значенню $a_k(D_{\Pi})$;

- якщо вибір вірної гілки кодового дерева ускладнений, то обидві підмножини гілок відкидаються і формується *сигнал захисної відмови*.

При вдалому виборі виробляючої послідовності відстань між кодограмами обох підмножин досить велика і перший випадок малоімовірний – він може наступити тільки в каналах з високим рівнем шумів. Другий випадок може мати місце при виборі завищеного значення D_{Π} . Практично ймовірність помилки декодування (ймовірність відкидання вірної послідовності при заданому a_k) при використанні єдиного порога D_{Π} визначається можливістю такої ситуації, і можна вважати, що верхня границя цієї ймовірності:

$$p(d(l_v) > D_{\Pi}) \approx 2^{-a_k}. \quad (2.91)$$

Для експоненціального спадання ймовірність помилки декодування зі зростанням n необхідно, щоб величина a_k лінійно залежала від n . Проте при цьому обсяг обчислень, а отже, складність декодуючого пристрою буде зростати за експоненціальним законом. Це є основним недоліком однопорогових декодуючих пристроїв.

Здатність коду виправляти задане число помилок на заданій довжині пошуку характеризується *пороговою характеристикою* (ПХ). Вона будується накладанням кривих рис. 2.62, *a* та 2.62, *b* за заданої кількості помилок у каналі. На окремих ділянках функція розузгодження лежить нижче ПХ, що відповідає критерію максимуму правдоподібності. Тому декодуючий пристрій шукає таку функцію $\theta_p(l_v)$, вага якої нижче рівня ПХ. Перевищення цього рівня свідчить про невірний вибір за кодовим деревом або про різке зростання рівня завад у каналі зв'язку.

Однопороговий декодуючий пристрій доцільний тільки тоді, коли кількість помилок не перевищує деякого допустимого значення, а самі помилки розподілені в кодограмі рівномірно. Зміна закону розподілу помилок призводить до зростання обсягу обчислень на ділянці з низьким рівнем завад, оскільки, якщо помилки з'явилися в кінці ділянки шляху, що аналізується, то для декодуючого пристрою існує багато варіантів вибрати на ділянці I неправильний шлях (область помилкових шляхів на рис. 2.62, *b* заштрихована).

Для того, щоб запобігти експоненціального зростання обсягу обчислень, слід використовувати зростаючу послідовність критеріїв $a_{k1}, \dots, a_{kj}, \dots$ і відповідну множину порогів $D_{\Pi(1)}, \dots, D_{\Pi(j)}, \dots$. При цьому декодуючий пристрій повинен зберігати в пам'яті (або повинен бути здатний обчислювати) матрицю порогів розузгодження

$$M_D = \begin{pmatrix} D_{\Pi(1)} & D_{\Pi(2)} & \dots & D_{\Pi(n)} \\ D_{\Pi(2)} & D_{\Pi(2)} & \dots & D_{\Pi(2)} \\ \dots & \dots & \dots & \dots \\ D_{\Pi(j)} & D_{\Pi(2)} & \dots & D_{\Pi(j)} \end{pmatrix}, \quad (2.92)$$

i -ий рядок якої відповідає критерію a_{ki} .

Алгоритм декодування символу x_j в цьому випадку має наступний вигляд:

– обирається найменший критерій a_{k1} і відкидаються всі n -значні послідовності символів, які відрізняються від прийнятої в $D_{\Pi(1)}$ або більшої кількості символів; при цьому, звісно, перевірка кожної послідовності починається з $k = 1$;

– після виявлення деякої послідовності символів, яка задовольняє критерію a_{k1} на довжині n , символ x_1 вважається декодованим;

– якщо всі послідовності символів множини $\{x\}$ не задовольняють критерію a_{k1} на довжині n , то береться критерій a_{k2} і т.п. до того часу, поки не буде знайдена послідовність, яка задовольняє критерію a_{kj} .

Отже, багатопороговий алгоритм оброблення сигналів зводиться до автоматичного підстроювання декодуючого пристрою до рівня завад у каналі зв'язку методом послідовного наближення.

Алгоритм Возенкрафта заснований на лінійному законі зміни порога D_{Π} , оскільки оцінка ймовірності декодування шляхом прийняття рішення на повній довжині пошуку автоматично переносяться окремі ділянки кодограм. Це передбачає в свою чергу рівномірний закон розподілу помилок у каналі зв'язку, що звужує область застосовності алгоритму.

Алгоритм Фано. Цей алгоритм був запропонований для ДСК і полягає в наступному. Введемо замість кодової відстані $d(l_v)$ *нормовану функцію розузгодження*:

$$\theta_{p.n.}(l_v) = d(l_v) - \nu p_{\text{ОП}} l_{\Pi}, \quad (2.93)$$

де $\nu p_{\text{ОП}}$ – тангенс нахилу порогової характеристики. При цьому сімейство порогів буде являти собою множину горизонтальних ліній з кроком квантування Δ_{Π} . Очевидно, що для вірного шляху декодування функція $\theta_{p.n.}(l_v)$ – від'ємна, а для помилкового шляху – додатна.

Кожний вузол і вершина кодового дерева характеризується своїм значенням $\theta_{p.n.}(l_v)$, що дозволяє подати кодове дерево в координатах $\theta_{p.n.}(l_v)$. Це показано на рис. 2.63 для випадку кодування тризначного повідомлення. Будемо вважати, що вузол кодового дерева не порушує порогові рівняння, які лежать не нижче нього; всі рівні, розміщені вище даного вузла, порушуються. Вузли, які відстоять від даного вузла на мінімальну і максимальну відстань $\theta_{p.n.}(l_v)$, будемо називати відповідно *найближчим* та *віддаленим вузлами* (вузли B_2 і B_3 на рис. 2.63).

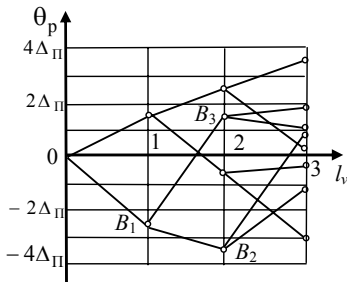


Рисунок 2.63 – Подання кодового дерева нормованою функцією розузгодження

У процесі декодування поріг у заданому інтервалі може набувати будь-яких значень $D_{\Pi} = \beta \Delta_{\Pi}$, де $\beta = 0, \pm 1, \pm 2, \dots$, тобто є «плаваючим». Якщо припустити, що декодуючий пристрій містить вказівник руху (ВР) і індикатор вузлів (ІВ), то процес декодування можна уявити як зворотно-поступовий

рух ІВ. При цьому кожного разу перевіряється умова непорушення порога й при виконанні встановлюється найближче для даного вузла непорушуване значення порога. Цей процес ілюструється рис. 2.64.

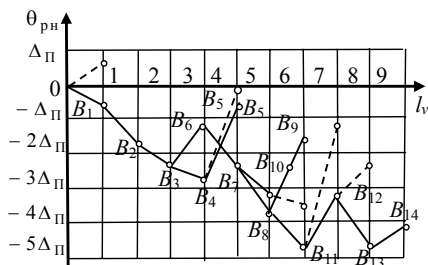


Рисунок 2.64 – Динаміка багатопорогового послідовного декодування

У стартовій точці ($l_v = 0$) поріг $D_{\Pi} = 0$, і ВР показує напрямок руху на вузол B_1 , оскільки для нього цей поріг не порушується, при цьому виносяться гіпотетичне рішення 0 або 1 відносно інформаційного символу x_1 ; у вузлі B_1 встановлюється поріг $D_{\Pi 1} = 0$. Після цього ВР показує шлях на вузол B_2 , і виносяться рішення про символ x_2 ; у вузлі B_2 встановлюється поріг $D_{\Pi 2} = -\Delta_{\Pi}$. Ця процедура продовжується до вузла B_4 , де встановлюється поріг $D_{\Pi 4} = -2\Delta_{\Pi}$, і ВР показує шлях на вузол B_5 . Проте при цьому буде виявлений факт порушення порога $D_{\Pi 4}$ і ІВ у вузол B_3 , при цьому рішення про символ x_4 стирається. Звідси ІВ вирушить до вузла B_6 і буде винесена нова гіпотеза відносно x_4 . Оскільки при цьому поріг $D_{\Pi 3} = -2\Delta_{\Pi}$ порушується, то ВР задає зворотний напрям руху, причому буде встановлений поріг $D_{\Pi 3} = -\Delta_{\Pi}$, а попереднє рішення відносно x_4 стирається. За нового порогу $D_{\Pi 3} = -\Delta_{\Pi}$ ВР знову перейде до вузла B_4 з порогом $D_{\Pi 4} = -\Delta_{\Pi}$ і далі зміститься до вузла B_5 . Оскільки при цьому поріг виявиться порушеним, то ВР повернеться до вузла B_3 і потім перейде до вузла B_6 для якого поріг $D_{\Pi 6} = -\Delta_{\Pi}$ задовольняється, при цьому буде винесено рішення про символ x_4 . Після цього ІВ переміститься до вузла B_7 , буде встановлений поріг $D_{\Pi 7} = -2\Delta_{\Pi}$, прийнято рішення про символ x_5 і т.п. Процес декодування символів x_1, \dots, x_{10} ілюструється табл. 2.9, де знак «+» й «-» означають відповідно наявність і відсутність порушень встановленого порога.

Відзначимо, що вірний шлях декодування характеризується зменшенням величини $\theta_{p,n}(l_v)$ зі зростанням l_v . При цьому декодувальний пристрій повинен мати великий об'єм пам'яті, оскільки перед тим, як збільшити поріг $D_{\Pi i}$ на Δ_{Π} , необхідно перевірити всі вузли кодового дерева, які лежать нижче даного порога. Фано запропонував спосіб спрощення алгоритму, проте й в цьому випадку його реалізація складна.

Таблиця 2.9 – Процес декодування символів x_1, \dots, x_{10}

Номер вузла, Y_i	Поріг, $D_{\Pi i}$	Направлення ВР на вузол, Y_{i+j}	Перевірка $D_{\Pi i}$ для вузла Y_{i+j}	Направлення ВР на вузол Y_{i+j}	Перевірка $D_{\Pi i}$ для вузла Y_{i+j}	Рішення про x_i		Встановлювальний поріг
						фіксується	стирається	
0	0	y_1	–			x_1		0
y_1	0	y_2	–			x_2		$-\Delta_{\Pi}$
y_2	$-\Delta_{\Pi}$	y_3	–			x_3		$-2\Delta_{\Pi}$
y_3	$-2\Delta_{\Pi}$	y_4	–			x_4		$-2\Delta_{\Pi}$
y_4	$-2\Delta_{\Pi}$	y_5	+	y_3	–		x_4	$-2\Delta_{\Pi}$
y_3	$-2\Delta_{\Pi}$	y_6	+	y_2	+			$-\Delta_{\Pi}$
y_3	$-\Delta_{\Pi}$	y_4	–			x_4		$-\Delta_{\Pi}$
y_4	$-\Delta_{\Pi}$	y_5	+	y_3	–		x_4	$-\Delta_{\Pi}$
y_3	$-\Delta_{\Pi}$	y_6	–					$-\Delta_{\Pi}$
y_6	$-\Delta_{\Pi}$	y_7	–			x_3		$-2\Delta_{\Pi}$
y_7	$-2\Delta_{\Pi}$	y_8	–			x_6		$-3\Delta_{\Pi}$
y_8	$-3\Delta_{\Pi}$	y_9	+	y_7	+			$-2\Delta_{\Pi}$
y_8	$-2\Delta_{\Pi}$	y_9	+	y_7	–		x_6	$-2\Delta_{\Pi}$
y_7	$-2\Delta_{\Pi}$	y_{10}	–			x_6		$-3\Delta_{\Pi}$
y_{10}	$-3\Delta_{\Pi}$	y_{11}	–			x_7		$-4\Delta_{\Pi}$
y_{11}	$-4\Delta_{\Pi}$	y_{12}	+	y_{10}	+			$-3\Delta_{\Pi}$
y_{11}	$-3\Delta_{\Pi}$	y_{12}	–			x_8		$-3\Delta_{\Pi}$
y_{12}	$-3\Delta_{\Pi}$	y_{13}	–			x_9		$-4\Delta_{\Pi}$
y_{13}	$-4\Delta_{\Pi}$	y_{14}	–			x_{10}		$-4\Delta_{\Pi}$

Модифікація алгоритму Возенкрафта-Фано. Для розширення можливостей послідовного декодування слід відмовитися від лінійного закону наростання порога D_{Π} і здійснити статистичне узгодження швидкості зміни D_{Π} з потоком помилок у каналі. За відсутності помилок величина D_{Π} повинна бути постійною: при зростанні рівня завад поріг може змінюватися ступінчасто. Це дозволяє вибирати шлях за кодовим

деревом з різними швидкостями зміни функції $\theta_p(l_v, U_{ш})$ й локалізувати ділянки з інтенсивними завадами. Такий принцип уперше був запропонований В.В. Деєвим та В.П. Черновим.

Алгоритм роботи декодуючого пристрою повинен передбачати можливість появи рівномірно розподілених одиничних помилок і пакетів помилок. З цією метою розіб'ємо всю довжину пошуку L_0 , вимірювану кількістю ребер, на відрізки довжиною l_0 ; замість пошуку шляху на всій ділянці $(0, L_0)$ будемо здійснювати пошук на ділянках $(0, l_0)$, $(l_0, 2l_0)$, ..., (jl_0, L_0) . Декодуючий пристрій послідовно аналізує гілки кодового дерева й відкидає як малоймовірні ті з них, для яких $d(l_v) > D_{\Pi}$. При появі одиничних помилок поріг D_{Π} збільшується на одиницю через певну кількість кроків l_0 . При отриманні відмови декодуючий пристрій повертається назад і при довжині $D_{\Pi} = \text{const}$ перевіряються попередні рішення на довжині проміжного пошуку $L_{\Pi} = j\gamma_{\Pi}$ ($j = 1, 2, \dots$), де параметр

$$\gamma_{\Pi} = \frac{l_0 L_0}{r_0 l_0 - L_0} \quad (2.94)$$

тут r_0 – повна кількість помилок, що виправляються, на довжині пошуку L_0 . Якщо на довжині L_{Π} не буде знайдена кодова послідовність, задовольняюча значенню D_{Π} , то фіксується проміжна відмова, вважається, що відбулася певна помилка, поріг D_{Π} зростає на одиницю ($j + 1$) інтервал L_{Π} для перевірки гіпотези про трикратну помилку і т.п. При пошуку кодової послідовності з функцією $\theta_p(l_v) < D_{\Pi}$ інформаційний символ x_1 вважається декодованим, початок відліку переноситься в наступний вузол кодового дерева, й аналіз продовжується. Якщо на довжині пошуку L_0 жодна гілка дерева не задовольняє значенню $D_{\Pi} = D_{\Pi \text{макс}}$, то фіксується захисна відмова, декодування припиняється, а прийняті символи стираються.

Реалізація алгоритму Фано характеризується низкою особливостей. Для їх з'ясування розглянемо в загальному вигляді принцип роботи декодуючого пристрою (2.51). Символи $\{z\}$, що приймаються, послідовно по одному вводяться в лінійки буферного регістру P_1 . Кількість лінійок дорівнює v . Тому за цикл роботи комутатора K в однойменних комірках лінійок буде записане v -значне ребро кодового дерева. При надходженні нових v -значних послідовностей записані символи зсуваються праворуч. Керуючий

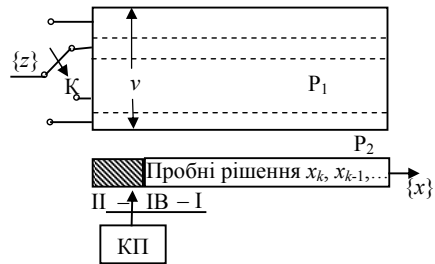


Рисунок 2.65 – Принцип роботи декодуючого пристрою

пристрій КП містить копію передавального кодоперетворювача, обчислювальний й логічний пристрій. В результаті формуються гіпотетичні ребра кодового дерева, обчислюється функція $\theta_{p,n}(l_v)$ і гіпотетичне значення інформаційних символів записуються в реєстр пробних рішень P_2 . У відповідності з алгоритмом і значенням $\theta_{p,n}(l_v)$ індикатор вузла ІВ переміщується вздовж дистанції пошуку L_0 , при цьому переміщення праворуч відповідає зменшенню номера l_v , а рух ліворуч – збільшенню l_v . Таким чином, комірки P_2 , розміщені праворуч від ІВ, заповнені символами рішень, а ті, що знаходяться ліворуч від нього – порожні. Кожного разу, коли в реєстр P_1 вводиться нове ребро кодового дерева, реєстр P_2 й індикатор вузла зміщується на один розряд праворуч.

Декодовані символи $\{x\}$ виводяться з останньої правої комірки реєстру P_2 . Переміщення індикатора вузла, а отже, заповнення реєстру P_2 й формування декодованих символів $\{x\}$ залежать від швидкості надходження символів $\{z\}$ з лінії зв'язку, швидкості обчислень декодуючого пристрою й характеру потоку помилок. Якщо помилок мало (ділянка I на рис. 2.66), то обсяг обчислень при побудові гіпотези X_{rj} невеликий й індикатор вузла знаходиться біля лівого вхідного кінця реєстру P_2 .

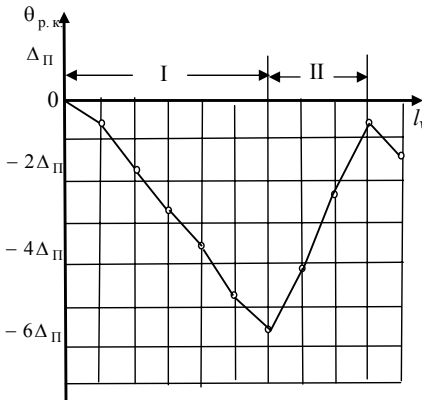


Рисунок 2.66 – Нормована функція розузгодження алгоритму Фано декодування

Пакети помилок (ділянка II на рис. 2.66) будуть збільшувати кількість кроків вздовж досліджуваного шляху на кодовому дереві. При цьому декодуючий пристрій повинен мати можливість переміщуватися далеко назад. Це означає, що ІВ зміщується праворуч, в результаті чого пристрій може виявитися перевантаженим й припинити нормально функціонувати.

Аналіз таких найважливіших характеристик, як середня ймовірність помилки p_0 й середня кількість обчислень N_0 для згорткових кодів ускладнюється двома причинами. По-перше, реєстри P_1 й P_2

мають кінцеву довжину L_0 ; в той самий час при інтенсивному потоці помилок може бути потрібний зворотний (до вершини) рух по кодовому дереву на кількість ребер l_v , що перевищує кількість комірок реєстрів. По-друге, індикатор ІВ в процесі декодування може переміщуватися в двох напрямках – вперед і назад, які в статистичному відношенні нерівноцінні: якщо i -й вузол не порушує поріг D_{Pi} , то з певною вірогідністю можна передбачити, що всі попередні вузли лежать на правильному шляху

декодування; що стосується наступних вузлів, то відносно них ніяких висновків зробити неможливо.

Тому представляють інтерес граничні оцінки величин p_0 й N_0 , отримані в роботі для ДСК. Хоча згорткові коди можна розглядати як особливий тип блочних кодів, це не означає, що для них справедливо граничне значення середньої ймовірності помилки декодування символу:

$$p_n < 2^{-n(v_{i0} - v_{in})}, \quad (2.95)$$

де $v_{in} = \frac{v_i}{2F_c}$ – швидкість передавання інформації, виражена в дв.од/мірність сигналу; v_{i0} – граничне значення швидкості передавання інформації. Це пояснюється тим, що в блокових кодах кожний символ може впливати на будь-який символ блоку, в той час, коли в згорткових кодах інтервал обмеження зв'язків дорівнює μ символів.

Для згорткових кодів верхня границя ймовірності помилки декодування визначається виразом:

$$p_0 < A_0 2^{-\frac{\mu}{2}(\alpha_v - 1)}, \quad \alpha_v > 1, \quad (2.95, a)$$

де параметри

$$\alpha_v = \frac{v_{i0}}{v_{in}}, \quad A_0 = \frac{2}{1 - \sqrt{2^{\alpha_v + 1}}}.$$

У залежності від типу каналу величина v_{i0} може змінюватися в границях від:

$$v_{i0} = 1 - \log_2(1 + 2\sqrt{p_0(1 - p_0)})$$

до

$$v_{i0} = 1 - \log_2(1 + e^{-h_c^2}).$$

Ці вирази справедливі відповідно для симетричних й несиметричних двійкових каналів.

Вказані граничні умови визначають важливі властивості згорткових кодів:

– при $\alpha_v > 1$ інтервал обмежень зв'язків (параметр μ) може бути збільшений без розширення обсягу обчислень, при цьому ймовірність невиявленої помилки зменшується експоненційно зі зростанням μ ;

– при $\alpha_v < 1$ граничні помилки p_0 й N_0 порушуються;

– згорткові коди з послідовним декодуванням придатні для широкого класу каналів.

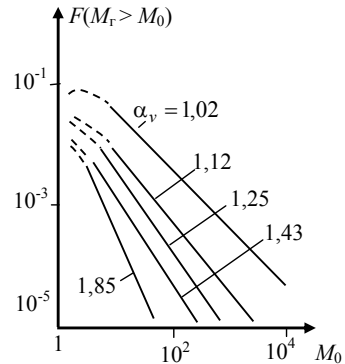


Рисунок 2.67 – Інтегральна функція розподілу $F(M_T > M_0)$

Випробування реальної системи показали, що величина N_0 визначається емпірично в основному параметром α_v і слабо залежить від абсолютних значень v_0 і v_{in} . Для (1/2...1/6)-кодів при $\alpha_v > 1,1$ величина $N_0 \leq 6...10$ швидко збільшується зі зменшенням α_v . Проте кількість гілок кодового дерева M_Γ , досліджуваних в процесі руху від одного вузла до іншого, змінюється в широких границях. Інтегральна функція розподілення $F(M_\Gamma > M_0)$, де M_0 – задана величина, показана на рис. 2.67.

Таким чином, необхідно забезпечити малу ймовірність помилки декодування й одночасно малу ймовірність перевантаження декодуючого пристрою. Друга задача більш складна, оскільки ймовірність виникнення перевантаження тим вище, чим повільніше спадає функція $F(M_\Gamma > M_0)$ зі зростанням M_0 ; вона залежить від обсягу пам'яті кодоперетворювача, його швидкодії й параметра α_v .

Нехай об'єм пам'яті кодоперетворювача допускає розміщення L_0 гілок. Позначимо через η_Γ кількість гілок кодового дерева, які повинні бути проаналізовані для визначення переданого сигналу (гілки). Якщо досліджується більше ніж $\eta_\Gamma L_0$ гілок, то настає перевантаження. Згідно з виразом для $F(M_\Gamma > M_0)$ ймовірність цієї події:

$$p_{\text{пер}} = F(M_\Gamma > \eta_\Gamma L_0) \approx 3^{-\frac{(1-\frac{1}{\alpha_v})}{\alpha_v} (\eta_\Gamma L_0)^{-\frac{(2,9-\frac{2}{\alpha_v})}{\alpha_v}}} \quad (2.96)$$

Наведені вирази дозволяють оцінювати потрібний об'єм пам'яті I_0 декодуючого пристрою.

Приклад 17. Нехай параметри каналу зв'язку складають $v_m = 1200$ Бод, $v_{in} = 0,25$, $p_0 = 10^{-1}$, $p_{\text{пер}} = 10^{-6}$, припустимий час аналізу $T_{\text{ан}} = 10$ мкс. Тоді для ДСК величина $v_{i0} \approx 0,318$, $\alpha_v \approx 1,27$ й згідно з виразом (2.96) величина $\eta_\Gamma L_0$ задовольняє співвідношенню:

$$10^{-6} = 3^{-0,222} (\eta_\Gamma L_0)^{-1,344}$$

звідки $\eta_\Gamma L_0 = 8,7 \cdot 10^4$. Оскільки

$$\eta_\Gamma = \frac{1}{v_m T_{\text{ан}}} \approx 83,3$$

то $L_0 = 1,05 \cdot 10^3$. У випадку, що розглядається, $v = \frac{1}{v_{in}} = 4$, тому кожний

символ, що приймається, потребує для обробки пам'яті об'ємом 4 дв. од. в регістрі P_1 і 1 дв.од. в регістрі P_2 . Отже, повний об'єм пам'яті кодоперетворювача $I_0 = 5L_0 = 5250$ дв.од.

Таку пам'ять реалізувати технічно нескладно. Необхідно, проте, мати на увазі, що ймовірність $p_{\text{пер}}$ не спадає експоненціально зі зростанням I_0 . Так, якщо в прикладі 17 $\eta_\Gamma L_0$ збільшити в 100 разів, то ймовірність $p_{\text{пер}}$ зменшиться лише до $5 \cdot 10^{-7}$. Тому зниження ймовірності перевантаження за інших рівних умов, можна досягти тільки ціною зниження швидкості передавання інформації.

Згідно з формулою (2.95а) ймовірність помилки декодування зменшується експоненціально зі зростанням μ . Тому значення μ для забезпечення заданої величини p_0 виходять значно меншими, ніж значення L_0 , які потрібні для забезпечення $p_{\text{пер}}$. Це означає, що за досить малої ймовірності перевантаження, ймовірність появи невиявлених символів буде незначною.

На закінчення відзначимо, що використання послідовного декодування в адаптивних системах зв'язку уявляється досить перспективним, але потребує додаткового аналізу, який враховує специфіку роботи зворотного каналу.

Алгоритм Вітербі. Алгоритм декодування Вітербі призначений для декодування згорткових кодів і є оптимальним з погляду зменшення ймовірності помилки в кодовій послідовності. При декодуванні за Вітербі, код необхідно подати у вигляді решітки, де вузлам відповідають стани кодера, а гілкам – можливі переходи кодера зі стану в стан. Рис. 2.68 містить один такт решітки для коду (5, 7). Довжина

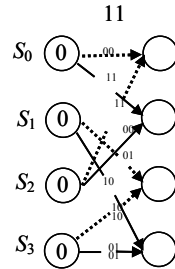


Рисунок 2.68 – Один такт решітки для коду (5, 7)

кодового обмеження цього коду $v = 2$, тому кількість станів на решітці $2^v = 2^2 = 4$. На вхід кодера може надходити лише по одному символу за такт або 0, або 1. Тому з кожного вузла решітки виходять тільки дві гілки, які входять до вузлів наступного такту. Ці вузли відповідають новому стану кодера, в який він перейшов. Біля кожної гілки вказано два символи кодової послідовності, які виникають на виході кодера в процесі кодування чергового символу інформаційної послідовності. Будь-яка дозволена кодова комбінація відповідає конкретному шляху на кодовій решітці.

Процес декодування згорткового коду алгоритмом Вітербі – це пошук такого шляху по кодовій решітці згорткового коду, кодова комбінація для якої найбільш схожа на кодову комбінацію, що надійшла з каналу. Розглянемо наступний приклад.

Приклад 18. Нехай інформація в каналі кодована згортковим кодом (5,7). Приймачем отримано з каналу таку кодову комбінацію $X = \{11, 01, 10, 10, 10, 11, 00, 00, 00, \dots\}$, яка, можливо, містить помилки. Виконаємо декодування в матриці Хеммінга. Перед початком процедури декодування, тому що нам апіорі невідомо, якій інформаційній послідовності відповідає отримана кодова вага всіх можливих шляхів по кодових решітках дорівнює «0» (метрики шляхів записані в колах, які відповідають вузлам решітки).

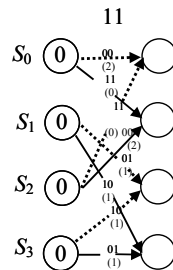


Рисунок 2.69,1 – Декодування за Вітербі. Такт 1

Перший такт (рис. 2.69,1). На вхід надійшли кодові символи «11». Розрахуємо метрики всіх гілок на кодовій решітці. Якщо гілка відповідає кодовим символам «00», то обидва символи не збігаються з отриманою кодовою комбінацією і метрика гілки дорівнює двом (метрики гілок відображені в дужках біля кожної гілки). Якщо гілка відповідає кодовим символам «10», або «01», то метрика гілки дорівнює одиниці, а якщо «00», то метрика гілки дорівнює нулю.

Розрахуємо метрики шляхів по решітці коду. У вузол решітки, що відповідає стану кодера «00», заходять два шляхи: від вузла «00» попереднього такту і від вузла «10» попереднього такту. Додамо до метрик цих шляхів метрики гілок поточного такту. Із двох цих шляхів «живим» залишається лише один шлях, а саме той, вага якого менше. Аналогічно поступимо з іншими трьома вузлами. Які шляхи залишилися і їх метрики можна подивитися на рис. 2.69,2. Після цього декодер проходить решіткою у зворотному напрямку, щоб відкинути ті шляхи, які «померли» на поточному такті. Оскільки залишилось більше одного шляху, то декодер ще не може видати рішення про те, яка інформація була передана.

Потім аналогічно виконується розрахунок метрик гілок для другого такту рис. 2.69,2, аналогічно обчислюються метрики шляхів рис. 2.69,3, відкидаються шляхи, які мають більшу вагу на поточному й на всіх попередніх тактах, для яких декодер ще не виніс рішення. Таким чином, кодер проводить розрахунки далі, такт за тактом, як це показано на рисунках з рис. 2.69,3 по рис. 2.69,11.

На одинадцятому такті декодера нарешті вдається вибрати один шлях на інтервалі від першого до восьмого такту включно і він виносить рішення, яке визначає, які саме символи найбільш ймовірно передавалися. Декодовані символи вказано в рядку нижче решітки (рис. 2.69,11), а в останньому рядку наведені інформаційні символи, які відповідають вибраному декодером відрізку кодової комбінації (вибраному шляху). Декодер визначив, що на третьому такті в каналі ймовірно була помилка і її було виправлено.

Після того, як декодер виніс рішення про прийняту інформацію на перших восьми тактах, він може звільнити свою пам'ять від цієї інформації й при зворотній рекурсії (це рух по решітці коду у зворотному напрямку з метою відкидання «померлих» шляхів) більше не рухатись далі восьмого такту.

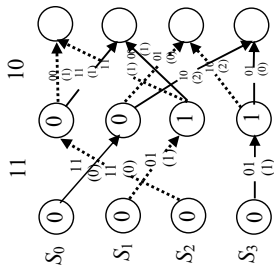


Рисунок 2.69,2 – Декодування за Вітербі. Такт 2

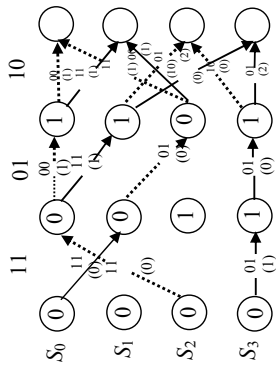


Рисунок 2.69,3 – Декодування за Вітербі. Такт 3

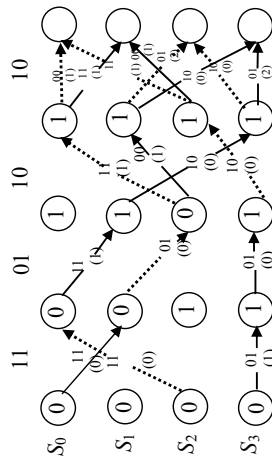


Рисунок 2.69,4 – Декодування за Вітербі. Такт 4

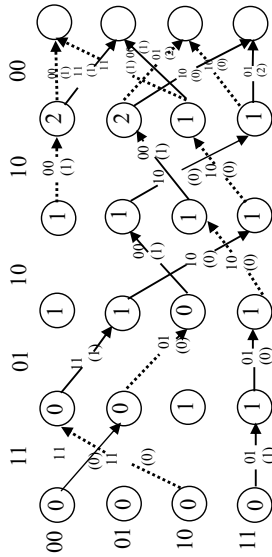


Рисунок 2.69,5 – Декодування за Вітербі. Такт 5

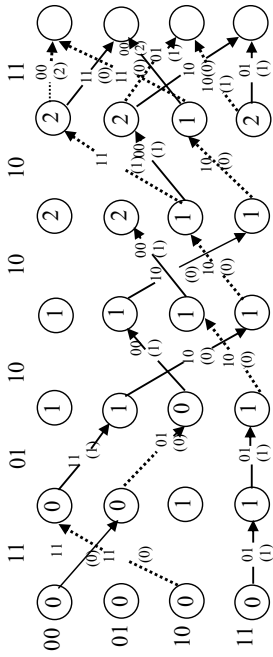


Рисунок 2.69,6 – Декодування за Вітербі. Такт 6

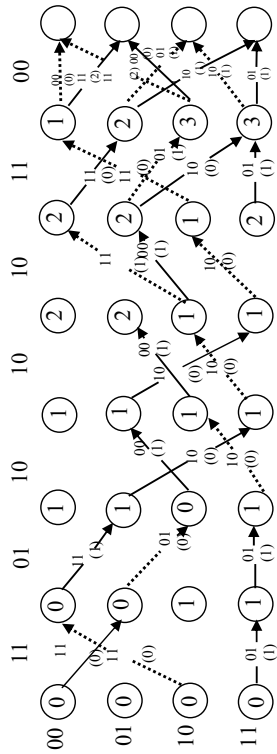


Рисунок 2.69,7 – Декодування за Вітербі. Такт 7

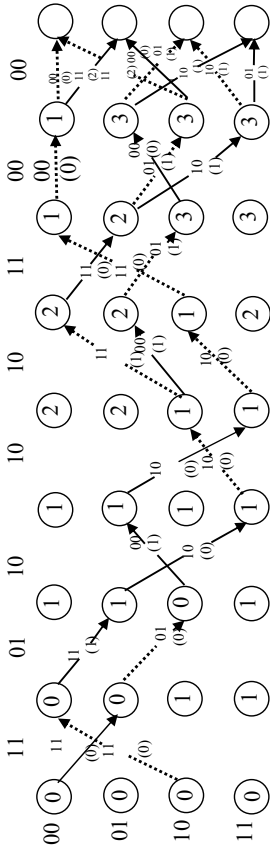


Рисунок 2.69,8 – Декодування за Вітербі. Такт 8

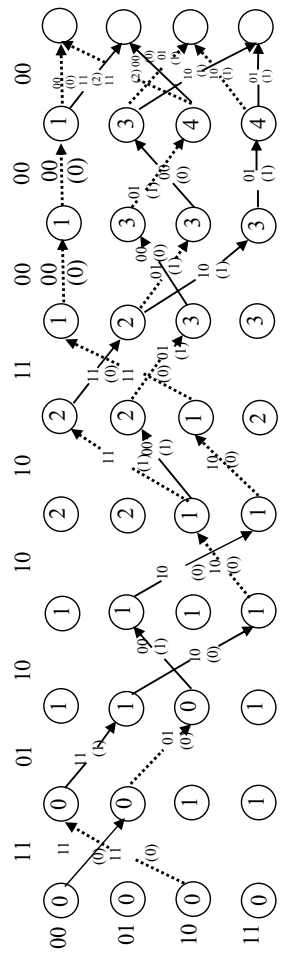


Рисунок 2.69,9 – Декодування за Вітербі. Такт 9

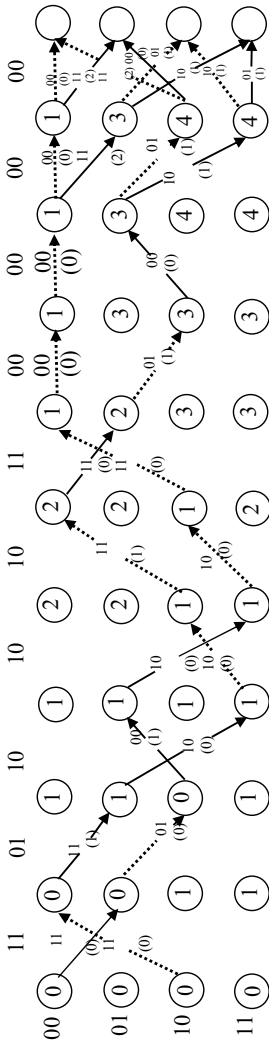


Рисунок 2.69,10 – Декодування за Вітербі. Такт 10

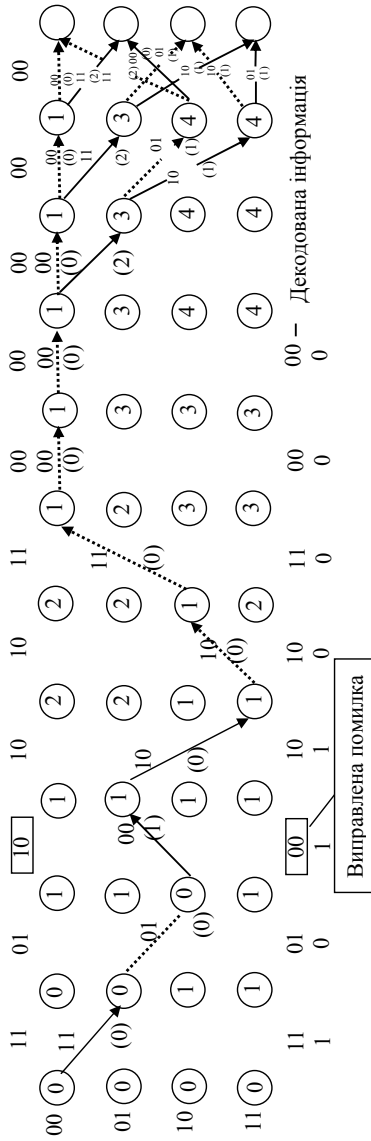


Рисунок 2.69,11 – Декодування за Вітербі. Такт 11

Грунтуючись на розглянутому принципі можна записати алгоритм роботи декодера Вітербі:

1. Визначити метрики всіх шляхів рівними нулю.
2. Розрахувати метрики всіх гілок на поточному такті.
3. Розрахувати метрики всіх шляхів на поточному такті.
4. Відкинути всі «померлі» шляхи за допомогою зворотної рекурсії.
5. Якщо на деякому інтервалі при зворотній рекурсії визначився єдиний шлях, що «вижив», то на цьому інтервалі винести рішення.
6. Перейти до оброблення наступного такту.

На рис. 2.70 залежності 2, 3 показують ефективність використання двох згорткових кодів в каналі з ФМ-2.

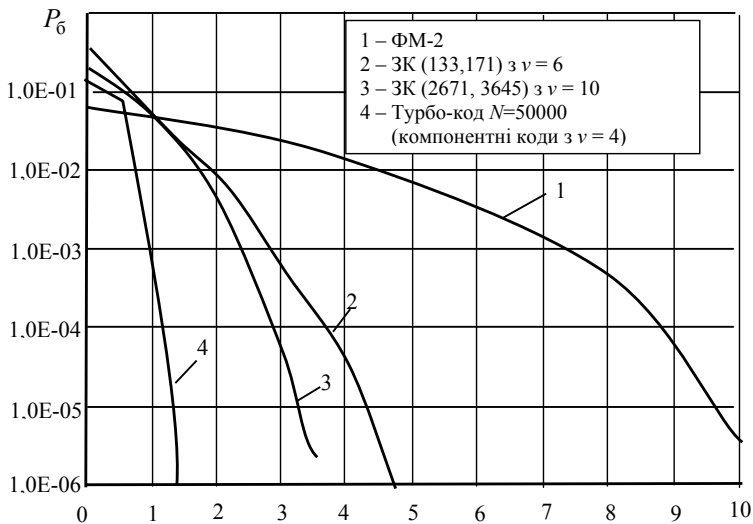


Рисунок 2.70 – Порівняння характеристик згорткових кодів і турбо-кодів з $R = \frac{1}{2}$

2.2.6. Характеристики турбо-кодів

Турбо-код утворюється при паралельному каскадуванні двох і більше згорткових кодів, названих компонентними, розділених перемежувачем. У зв'язку з цим турбо-коди інколи називають *паралельними каскадними згортковими кодами*. Якщо в ролі компонентних кодів використовуються стандартні згорткові коди – коди Хеммінга, БЧХ або Ріда-Соломона, то такі коди називають *паралельними каскадними блоковими кодами або кодами добутку (product codes)*.

Структурна схема кодера узагальненого турбо-коду наведена на рис. 2.71. В процесі кодування інформаційна послідовність u розбивається на блоки довжини N символів. Після цього сформована послідовність надходить на систематичний вихід кодера $y^{(1)}$, а також паралельно на z гілок, що складаються із послідовного з'єднання пристрою перемежування і компонентного кодера.

Найбільшого розповсюдження на практиці отримала схема з двома ідентичними компонентними згортковими кодерами і одним перемежувачем. Розглянемо структуру і роль компонентних кодів у складі турбо-кодів.

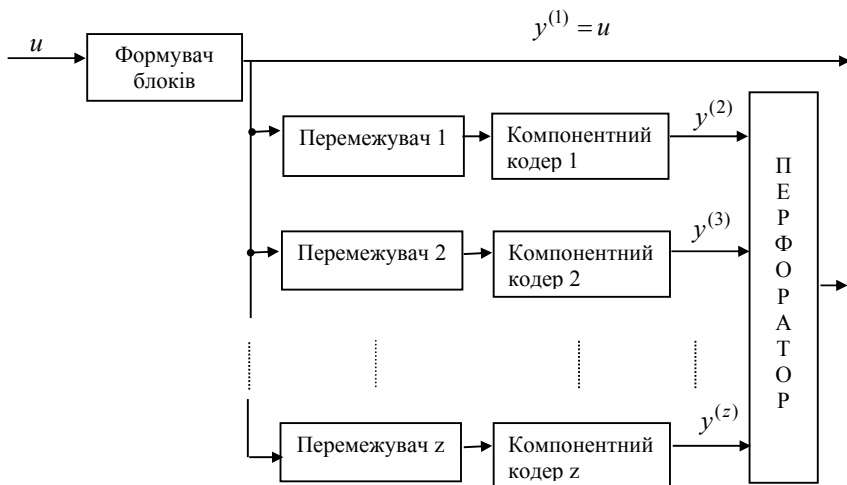


Рисунок 2.71 – Структурна схема кодера узагальненого турбо-коду

В оригінальній роботі К. Берроу як компонентні запропоновано використовувати рекурсивні систематичні згорткові коди (РСЗК). Доведено, що використання РСЗК за інших рівних умов гарантує турбо-коду найкращі характеристики. Для цього показано, що ймовірність помилкового декодування турбо-кодів пропорційна виразу

$$\frac{N}{C_N^{i_{\min}}} \approx N^{1-i_{\min}} \cdot i_{\min} \quad \text{при } N \gg i_{\min}. \quad (2.97)$$

Тут i_{\min} – мінімальна вага інформаційної послідовності породжуючого шляху, що співпадає на решітковій діаграмі компонентного згорткового кодера; N – розмір інформаційного блока турбо-коду.

Аналізуючи вираз (2.97) бачимо, що зі зростанням i_{\min} ймовірність помилкового декодування зменшується. Таким чином, параметр i_{\min} є ключовим при виборі компонентних кодів. У стандартних згорткових

кодів без зворотного зв'язку $i_{\min} = 1$. При цьому із (2.97) випливає, що зі збільшенням довжини перемежувача характеристики турбо-кодів не змінюються – так називаний «виграш перемежувача» відсутній. Якщо ж у ролі компонентних використати рекурсивні згорткові коди, в яких i_{\min} завжди більше 1 (зокрема, для кодів зі швидкістю $\frac{1}{n}$ $i_{\min} = 2$), то ймовірність помилкового декодування турбо-кодів зменшується зворотно пропорційно N – з'являється «виграш перемежувача».

Декодування турбо-кодів. Турбо-коди відносяться до класу так званих паралельних каскадних кодів. Принцип побудови кодера турбо-коду досить простий (рис. 2.72). Зі структури кодера видно, що турбо-код являє собою систематичний код, у якому перевірна група утвориться з перевірочних бітів, генерованих двома кодерами складових рекурсивних систематичних згорткових кодів (РСЗК), причому інформаційна послідовність подається в кодер першого РСЗК (РСЗК1) безпосередньо, а в кодер другого РСЗК (РСЗК2) через пристрій псевдовипадкового перемежування. Схема виколування перевірочних біт застосовується для регулювання загальної швидкості турбо-коду. Причина феноменальної завадостійкості турбо-кодів лежить у поєднанні наступних властивостей:

1. Сильна залежність ваги вихідної послідовності РСЗК від виду вхідної інформаційної послідовності, тобто від порядку розміщення нулів і одиниць у ній.

2. Застосування перемежувача для зміни виду вхідної послідовності, що подається на входи кодерів складових РСЗК.

Поєднання цих властивостей призводить до того, що якщо при подаванні певної інформаційної послідовності на вхід кодера РСЗК1 вага його перевірочної послідовності виявляється малою, то перемежена версія цієї інформаційної послідовності, яка подається на вхід кодера РСЗК2, з високою ймовірністю призведе до генерації перевірочної послідовності великої ваги через зазначену вище властивість РСЗК. Таким чином, якщо будь-яка комбінація помилок не може бути виправлена одним РСЗК, то це майже напевно, буде зроблено за допомогою перевірочної групи іншого РСЗК і навпаки. Необхідно пам'ятати, що при використанні в складі турбо-коду нерекурсивної форми згорткових кодів з тією самою коректуючою здатністю виграш від кодування виявляється набагато менше. Це відбувається саме тому, що вага вихідної послідовності згорткових кодів у нерекурсивній формі слабо залежить від вхідної інформаційної послідовності

Існує чотири алгоритми з м'яким рішенням, придатні для декодування турбо-кодів: алгоритм максимуму апостеріорної імовірності (MAI), максимуму логарифму апостеріорної імовірності (log MAI), максимізації логарифму апостеріорної імовірності (max-log MAI),

алгоритм Вітербі з м'яким рішенням АВМР. Алгоритм МАІ – в обчислювальному відношенні набагато більш складний, ніж алгоритм АВМР. Операції в алгоритмі МАІ – множення й піднесення до ступеня, у той час як в алгоритмі Вітербі це просто додавання, порівняння та вибір.

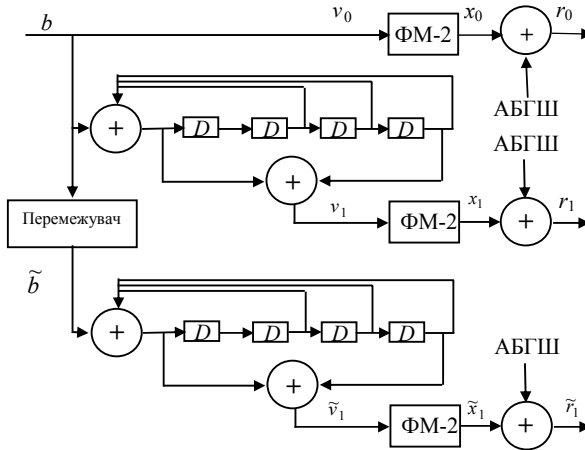


Рисунок 2.72 – Схема побудови турбо-кодера з компонентним РСЗК(1,21/35)

Ітераційний декодер для складових кодів складається із двох «м'яких декодерів», виходи яких розділені перемежувачами. Складові декодери основані або на алгоритмі МАІ, або алгоритмі Вітербі, що генерує зважену м'яку оцінку вхідної послідовності. Ітераційний алгоритм виконує обмін інформацією між двома складовими декодерами.

Алгоритм МАІ зменшує імовірність помилкового прийому символу (або біта), тоді як алгоритм Вітербі мінімізує імовірність помилки в ланцюжку символів. При передаванні по каналу з низьким рівнем шуму характеристики обох алгоритмів практично ідентичні. При великому рівні шуму алгоритм МАІ забезпечує кращі характеристики передавання в порівняно з алгоритмом Вітербі для ітераційного декодування.

В обчислювальному відношенні алгоритм МАІ більш складний, ніж Вітербі. Основні операції для алгоритму МАІ – це множення й піднесення до ступеня, тоді як для алгоритму Вітербі це просто додавання, порівняння й вибір.

Алгоритм декодування МАІ. Алгоритм МАІ виносить жорстке рішення та дійсне число, що називається апостеріорною імовірністю (АПІ). АПІ є імовірністю того, що тверде рішення правильне.

Ітераційне декодування за МАІ. Турбо-кодер, який засновано на двійковому РСЗК (1, 21/35) кодї зі зворотними зв'язками зображений на

рис. 2.72. На перший кодер надходить інформаційна послідовність b довжини N

$$b = (b_1, b_2, \dots, b_N).$$

Він створює на своєму виході дві кодовані послідовності позначені v_0 і v_1 . На другий кодер надходить та сама інформаційна послідовність, яка пройшла через перемержувач і позначена \tilde{b} . Відповідно на виході другого кодера виникають послідовності \tilde{v}_0 й \tilde{v}_1 . Однак, вихідна послідовність \tilde{v}_0 не передається. Вона відновлюється на приймальній стороні шляхом деперемержування послідовності v_0 .

Перше призначення перемержувача – побудова довгого коду. Друге призначення – декореляція вхідних послідовностей двох кодерів для створення можливості субоптимального ітераційного алгоритму декодування, заснованого на обміні інформацією між двома декодерами. Якщо вхідні послідовності двох декодерів практично некорельовані, то, з великою ймовірністю, помилки не виправлені одним можуть бути виправлені іншим. І так багаторазово.

Псевдовипадково перемержувач приймає блок довжиною в N символів, після чого видає його символи в псевдовипадковому порядку. Порядок перемерження повинен співпадати з перемержувачем декодера.

Турбо-кодер генерує $(n(N+m), N)$, блоків коду, де n – кількість вихідних кодованих послідовностей. Наприклад в даному випадку $n = 3$.

Два компоненти коду можна замінити й змінювати їх відносно швидкості. Різні швидкості коду, такі як $1/2$, $2/3$, $3/4$ і т.п. можна отримати з коду з відносною швидкістю $1/3$ шляхом перфорації.

Для інших відносних швидкостей конструкція кодера може мати більше двох кодуючих компонентів.

Алгоритми декодування повинні бути з м'яким виходом. Це алгоритми МАІ або алгоритм Вітербі з м'яким рішенням (АВМР). Ітераційний турбо-декодер зображений на рис. 2.73.

В ітераційній схемі, заснованій на МАІ, перший декодер МАІ приймає вхідну нековдану послідовність r_0 і кодовану послідовність r_1 . Він обробляє її й видає м'яке рішення, яке через перемержувач надходить на другий декодер разом з прийнятою інформаційною послідовністю, що пройшла через такий самий перемержувач r_0 , а також з кодованою послідовністю із другого кодера r_1 . Другий декодер теж виносить м'яке рішення, яке може бути використане першим декодером для подальшого виправлення помилок у декодувальному блоці й так багаторазово.

Після декількох ітерацій декодування блока, м'який вихід обох декодерів більше не використовується для подальшого виправлення помилок. На останній стадії виноситься жорстке рішення.

Нехай, наприклад, перший декодер МАІ перебуває на першій ітерації. Логарифм імовірності на виході першого МАІ має додаткову інформацію за рахунок ітерації $\Lambda_1(b_i)$

$$\Lambda_1(b_i) = \log \frac{\sum_{l=0}^{M-1} \alpha_l(l) p_l^1(1) \exp\left(-\frac{\sum_{j=0}^{n-1} (r_{l,j} - x_{b,j}^1(l))^2}{2\sigma^2}\right) * \beta_l(S_f^1(l))}{\sum_{l=0}^{M-1} \alpha_l(l) p_l^1(0) \exp\left(-\frac{\sum_{j=0}^{n-1} (r_{l,j} - x_{b,j}^0(l))^2}{2\sigma^2}\right) * \beta_l(S_f^0(l))}, \quad (2.98)$$

де позначені $p_l^1(1)$ й $p_l^1(0)$ апіорні ймовірності надходження 0 і 1 на вхід першого декодера. Аналогічно для входу другого декодера апіорні ймовірності позначені $p_l^2(1)$ й $p_l^2(0)$.

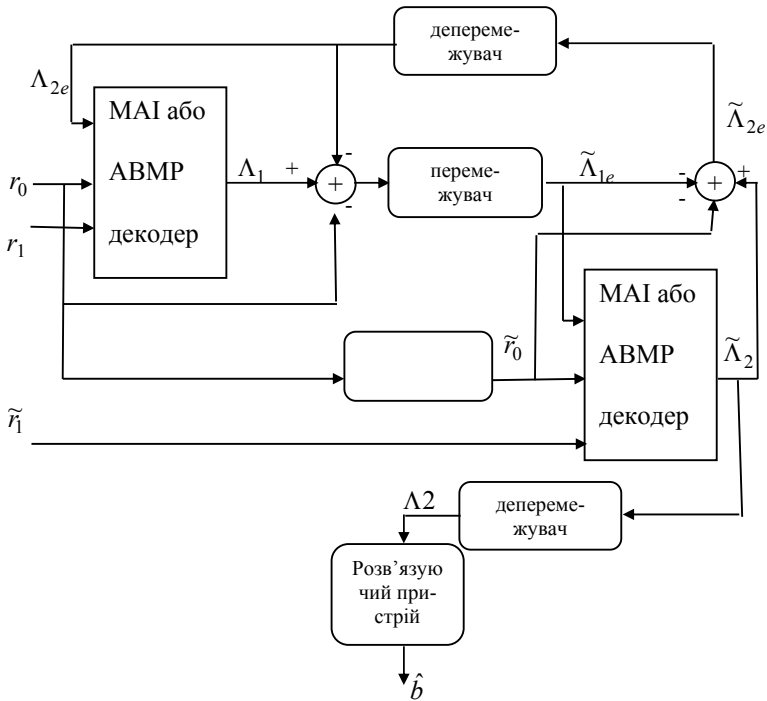


Рисунок 2.73 – Ітераційний декодер турбо-коду

Вплив кількості ітерацій на ймовірність помилки ілюструє рис. 2.74.

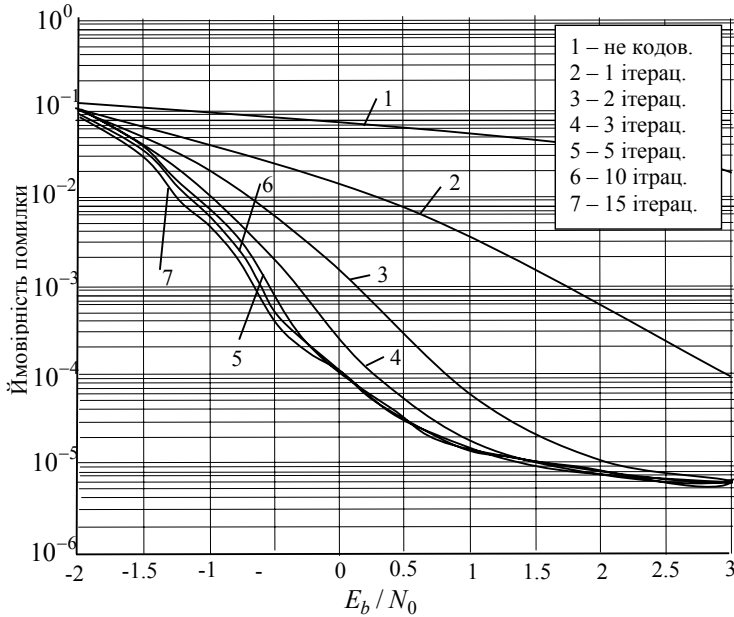


Рисунок 2.74 – Код (1, 5/7), $R = 1/2$, модуляція ФМ-2, алгоритм декодування SOVA

Характеристики завадостійкості турбо-кодів. У зв'язку з тим, що як компонентні коди в турбо-кодах використовуються згорткові коди, то зупинимося на визначенні їхніх характеристик завадостійкості через породжуючі функції згорткових кодів. Однією з таких характеристик є поняття вільної відстані згорткового коду d_{free} , визначувану як мінімальна кодова відстань між нульовим кодовим словом й усіма іншими кодовими словами. У випадку якщо код лінійний, то величина вільної відстані коду й мінімальної кодової відстані збігаються, а обчислити вільну відстань коду значно легше, ніж мінімальну відстань коду. Справа в тому, що в першому випадку треба порівняти нульове кодове слово з усіма іншими й вибрати найменший результат порівняння, а в другому випадку треба кожне кодове слово порівняти з усіма іншими й вибрати найменший результат порівняння. Вільна відстань використовується для попереднього вибору згорткового коду для аналізу систем зв'язку.

У загальному виді породжуюча функція $T(D, N, L)$ описує повну множину шляхів, які починаються й закінчуються в нульовому стані коду

$$T(D, N, L) = \sum_{w=d_{free}}^{\infty} \sum_{i_w} \sum_{l_w} c_{w, i_w, l_w} D^w N^{i_w} L^{l_w}, \quad (2.99)$$

де ступінь w за формальної змінної D дорівнює вазі Хеммінга цього шляху; ступінь i_w за формальної змінної N дорівнює вазі інформаційної послідовності, що породила цей шлях; ступінь l_w за формальної змінної L відповідає довжині цього шляху в тактових інтервалах, а коефіцієнт c_{w,i_w,l_w} – відповідає кількості існуючих шляхів із зазначеними параметрами, які починаються й закінчуються в нульовому стані.

Породжуюча функція дозволяє розрахувати верхню границю ймовірності помилкового декодування біта за критерієм максимуму правдоподібності. Оскільки при розрахунках характеристик завадостійкості згорткового коду довжина помилкового шляху не враховується, то разом з функцією $T(D, N, L)$ застосовується функція

$$T(D, N) = T(D, N, L)|_{L=1} = \sum_{w=d_{free}}^{\infty} \sum_{i_w} c_{w,i_w} D^w N^{i_w}, \quad (2.99a)$$

де c_{w,i_w} – число шляхів із загальною вагою w й інформаційною вагою i_w . набір коефіцієнтів $c_w = \sum_w c_{w,i_w}$, де $w \geq d_{free}$ називається спектром відстаней згорткового коду.

Важливою характеристикою так само є спектр інформаційних ваг $a_w = \sum_w c_{w,i_w} \times i_w$, де $w \in [d_{free}, \infty)$. Він показує сумарну кількість помилок на виході декодера максимальної правдоподібності, коли замість переданого шляху вибирається помилковий, що знаходиться від нього на відстані $w = d$.

Розрахунок імовірності помилки відбувається на підставі припущення, що помилкові події відбуваються рідко, що дозволяє скористатися верхньою границею. Оскільки верхня границя визначається виразом

$$P = \sum_{w=d_{free}}^{\infty} a_w P(d_{err} > \frac{w-1}{2}) \text{ для жорсткого рішення,}$$

$$P = \sum_{w=d_{free}}^{\infty} a_w P(d_{err} > \frac{w}{2}) \text{ для м'якого рішення}$$

Ймовірність помилки біта для каналу з модуляцією ФМ-2 або ФМ-4 визначається виразом

$$P_b = \left(erf \left(\sqrt{\frac{E_b}{N_0}} \right) \right),$$

де $erf(x) = \frac{1}{\pi} \int_x^{\infty} \exp\left(-\frac{t^2}{2}\right) dt$ – інтеграл помилок.

Крім власне компонентних кодів, у якості яких у складі турбо-коду використовуються рекурсивні систематичні згорткові коди, у складі турбо-коду також використовується перемежувач. Через це корисним для аналізу є поняття рівномірного перемежувача, уведеного С. Бенедетто й Г. Монторсі. Рівномірний перемежувач – це абстрактний пристрій, який з імовірністю $1/C_N^i$ відбиває вхідну послідовність довжини N символів ваги i у вихідну послідовність тієї ж ваги. Тут у знаменнику дробу число сполучення із N по i

$$C_N^i = \frac{N!}{i!(N-i)!}.$$

Дистанційні властивості й характеристики декодування турбо-коду з використанням рівномірного перемежувача є математичним сподіванням характеристик повного ансамблю турбо-кодів з довжиною блоку N (повне число кодів з довжиною блоку N дорівнює $N!$). При цьому характеристики турбо-коду з детермінованим перемежувачем можуть бути, як краще, так і значно гірше характеристик коду з рівномірним перемежувачем.

У цьому випадку адитивна верхня границя ймовірності помилки біта в ТЗК, що захищена завадостійким кодом, виражається в такий спосіб

$$P_b \leq \frac{2}{N} \operatorname{erf} \left(\sqrt{\frac{2d_{free_eff} R \Delta^2}{4\sigma^2}} \right) B_{free_eff}, \quad (2.100)$$

де N – глибина перемежування (для псевдовипадкового перемежувача – це довжина блоку перемежувача у символах); B_{free_eff} – ефективна кількість помилкових бітів, що виникають на виході турбо-декодера в результаті дії завади (у найкращому разі 1 біт); d_{free_eff} – ефективна вільна відстань турбо-кода.

Ефективна вільна відстань турбо-коду визначається як мінімальна вага кодованої послідовності на виході турбо-коду з рівномірним перемежувачем, генерованим інформаційною послідовністю ваги $w = 2$. Повну вагу Хеммінга d будь-якої послідовності на виході турбо-коду можна подати у вигляді трьох компонентів

$$d = w + z_1 + z_2,$$

де w – вага послідовності на систематичному виході, а z_1 і z_2 ваги послідовностей на виході перших і другого компонентних кодів відповідно. Мінімальна вага на виході кожного компонентного коду не перевищує величину

$$z_{\min} \leq 2^{v-1} + 2.$$

Отже, ефективна вільна відстань коду обчислюється наступним чином:

$$d_{free_eff} = 2z_{\min} + 2 = 2^v + 6.$$

Якщо в складі ТК використовуються перфоровані компонентні коди, то й перфорації піддаються тільки відповідні виходи компонентних кодів, що викликає зменшення d_{free_eff} внаслідок зменшення величини z_{min} .

У табл. 2.10 нижче зазначені граничні величини d_{free_eff} у залежності від відносної швидкості турбо-коду й довжини кодового обмеження його компонентних кодів.

Таблиця 2.10 – Залежність ефективної вільної відстані турбо-коду від його відносної швидкості й довжини компонентних кодів

Відн. швидкість коду R_{TK}	1/3	1/2	2/3	3/4
$v = 2, d_{free_eff}$	10	6	5	4
$v = 3, d_{free_eff}$	14	8	6	5
$v = 4, d_{free_eff}$	22	12	9	7
$v = 5, d_{free_eff}$	38	20	14	11

За наведеними у табл. 2.10 даними можна побудувати верхні границі ймовірності помилок для ЗК у складі ТК і каналу з ФМ у залежності від величини E_b / N_0 , що зроблено для турбо-кодів з довжиною кодового обмеження $v = 2$ і показаних на графіках рис. 2.75, рис. 2.76.

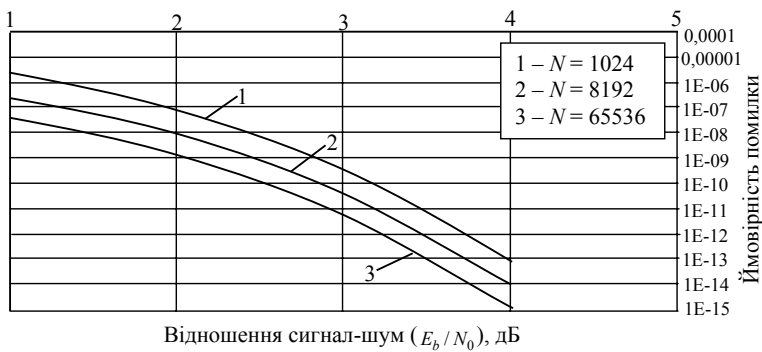


Рисунок 2.75 – Ймовірність помилки турбо-коду при $R = 1/3$ та кодовим обмеженням 2

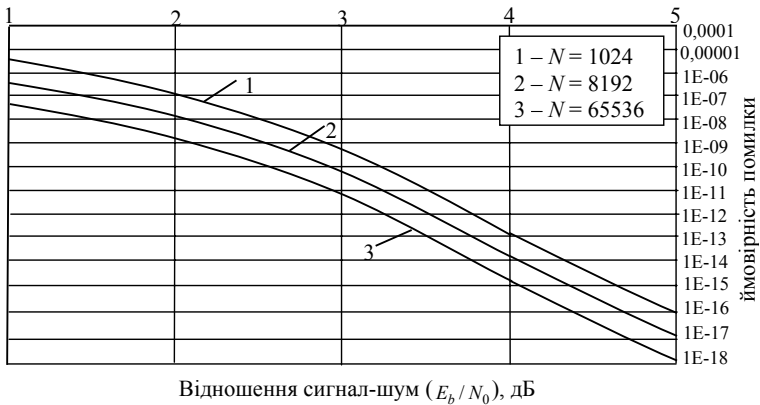


Рисунок 2.76 – Ймовірність помилки турбо-коду при $R = 1/2$ та кодним обмеженням 2

2.2.7. Питання та задачі для самоперевірки

1. Що входить до складу елементарного блока згорткового коду?
2. Які умови не виконання рівняння (2.52) призводять до спотворення інформаційного символу?
3. Дайте визначення структури систематичного згорткового коду.
4. Які параметри ЗК впливають на кодове обмеження.
5. Який зв'язок параметрів кінцевої перевірконої матриці (2.56) і кодним обмеженням?
6. Для параметрів матриці H_N і B та послідовності помилок, наведених в прикладі 3, знайдіть синдроми для послідовності символів $Z \rightarrow 111000110011\dots$
7. Сформулюйте необхідні співвідношення між породжуючою матрицею B та породжуючими багаточленами систематичного ЗК.
8. Які згорткові коди називаються еквівалентними?
9. Сформулюйте відмінність кодерів на рис. 2.51 та 2.52.
10. Яка структура синдрому на кожний елементарний блок, отриманого згідно з виразом 2.72.
11. Які відмінності формувачів синдрому, зображених на рис. 2.53 і 2.40, дозволяють другий використовувати за великої швидкості $b - m > m$?
12. Побудуйте діаграму станів згорткового коду, в якому на відміну від зображеного на рис. 2.61 на верхній суматор подаються сигнали 1, 2, 3 комірках.

13. Які параметри характеризують зрізану гілку кодового дерева?
14. Як визначити ваговий спектр ЗК, знаючи його породжуючу функцію?
15. Побудуйте кодове дерево для ЗК (5,7).
16. Поясніть принцип рекурентного кодування. Закодуйте число 25 рекурентним (2,1) кодом Фінка-Хагельбаргерая.
17. Поясніть принцип послідовного декодування. Нарисуйте кодове дерево для повідомлення $S \rightarrow 1101$, закодоване (1/3) кодом.
18. Дайте характеристику послідовного алгоритму Фано і виділіть його відмінності від алгоритму Возенкрафта.
19. Сформулюйте алгоритми визначення порогів D_{Π} для функції розузгодження (2.89).
20. Визначте вплив коефіцієнта групування помилок на можливість локалізування ділянок з інтенсивними завадами в алгоритмі Возенкрафта-Фано (рис. 2.65).
21. Побудуйте багатократний кодовий фільтр для множення на поліном $g(x) = 110101000101$.
22. Порівняйте час затримки повідомлення при передаванні згортковим кодом з заданою ємністю перемежувача з турбо-кодом, в якому використано два компонентних коди з характеристиками згорткового.
23. Опишіть процес обміну інформацією між декодерами компонентних кодів за нерівних швидкостей передавання їх 1/2, 2/3, 3/4.
24. Чому в схемі турбо-кодера (рис. 2.72) перемежувач ввімкнений на вході тільки одного компонентного коду?
25. Проведіть порівняльний аналіз часу затримки повідомлення за рахунок ітерацій і перемежування.
26. Опишіть процес зменшення помилки прийому елемента кодового слова при збільшенні числа ітерацій.
27. Що характеризує вільна відстань для окремих компонентних згорткових кодів?
28. Які характеристики породжуючої функції компонентних ЗК визначають верхню границю ймовірності помилкового декодування біта?
29. Як змінюються дистанційні властивості декодування турбо-кодів при використанні рівномірного перемежувача?
30. За даними табл. 2.10 проаналізуйте вплив швидкості компонентних кодів на ефективну вільну відстань.

ЧАСТИНА 3

ПОБУДОВА НАДЛИШКОВИХ БЛОКОВИХ КОДІВ ПРИ БАГАТОПОЗИЦІЙНИХ СИГНАЛАХ

Глава 3.1. Ймовірнісні характеристики якості приймання надлишкових блокових кодів

3.1.1. Пропускна здатність каналу з алфавітом $a > 2$

Пропускною здатністю інформаційного каналу (C) називають максимальне значення (точніше, верхню межу) швидкості передавання інформації при заданих фіксованих обмеженнях, тобто

$$C = \sup_{\substack{a_1 \in B_1 \\ \dots \\ a_i \in B_i \\ \dots}} \left\{ \bar{I}(W, X) \right\} \frac{\text{ДВ.ОД}}{c} . \quad (3.1)$$

У цій рівності позначка \sup вказує на те, що обчислюється верхня межа, а запис $a_i \in B_i$ говорить про те, що параметр a_i задовольняє заданому фіксованому обмеженню, тобто лежить в деякій області B_i .

Спосіб відшукування верхньої межі залежить від того, яка сукупність фіксованих обмежень задана.

Якщо інформаційний канал визначений повністю, то верхня межа повинна відшукуватись за статистичними характеристиками джерела повідомлень, тобто відшукуються розподіл імовірностей повідомлень (x) та корелятивні зв'язки між ними, за яких швидкість передавання інформації буде найбільша.

Таким чином, пропускна здатність є характеристика каналу і не залежить від фактичної швидкості передавання інформації від даного джерела.

Можна показати, що

$$C = \sup \left\{ \lim_{T \rightarrow \infty} \frac{H(X_T)}{T} \right\} , \quad (3.2)$$

де T – довжина одиничного сигналу; $H(X_T)$ – ентропія.

Позначимо через $N(T)$ число всіх можливих послідовностей повідомлень тривалістю T . З властивостей ентропії, розглянутих у першій частині, випливає, що $H(X_T)$ буде максимальною, якщо всі послідовності повідомлень рівноймовірні. Це максимальне значення дорівнює $\log N(T)$. Тоді з (3.2) бачимо, що для заданого інформаційного каналу

$$C = \lim_{T \rightarrow \infty} \frac{H(X_T)}{T} . \quad (3.3)$$

Розглядаючи лише один канал зв'язку, аналогічно отримаємо

$$C_c = \lim_{T \rightarrow \infty} \frac{N_c(T)}{T} \quad (3.3a)$$

де $N_c(T)$ – число всіх можливих послідовностей кодових сигналів довжиною T .

Співвідношення (3.3) і (3.3a) звичайно використовують як визначення пропускної здатності дискретного каналу без шумів.

Знайдемо пропускну здатність дискретних каналів, використовуючих код з основою a (тобто з a різними символами), тривалість усіх символів коду однакова і дорівнює найквістовому елементу t_0 . Інші фіксовані обмеження відсутні.

Для обчислення C_c розглянемо послідовність з M символів. Тривалість такої послідовності дорівнює $T_k = Mt_0$. При $T \rightarrow \infty$ число символів в одній послідовності $M \rightarrow \infty$. Очевидно, що всього можна утворити a^M послідовностей довжиною M символів, отже, $N_c(Mt_0) = a^M$. З (3.3a) отримаємо

$$C_c = \lim_{T \rightarrow \infty} \frac{a^M}{Mt_0}$$

або

$$C_c = \frac{1}{t_0} \log a. \quad (3.4)$$

Потрібно зазначити, що якщо розглядати вихід кодуєчого пристрою як джерело повідомлень, то $\log a$ є ентропія цього джерела, тобто $\log a = H(Y)$, у якого корелятивні зв'язки між символами відсутні і ймовірності передавання різних символів однакові. Звідси слідує надто важливе зворотне твердження: для того щоб у даному каналі швидкість передавання була максимальною, необхідно, щоб імовірності передавання різних символів були однаковими.

При використанні двійкового коду $a = 2$ із (3.4) отримаємо, що

$$C_c = \frac{1}{t_0} \frac{\text{дв.од}}{\text{с}}. \quad (3.5)$$

Для дискретних каналів прийнято позначати $\frac{1}{t_0} = B$, де B називають швидкістю модуляції, яка виражається в бодах, якщо t_0 вимірюється в секундах. Таким чином, $C_c = B$, тобто пропускну здатність двійкового каналу a , виражена у двійкових одиницях за секунду, дорівнює швидкості передавання в бодах.

Розглянемо випадок, коли символи коду (або окремі повідомлення) мають однакову тривалість, що дорівнює t_0 . На припустиму послідовність символу накладаються деякі фіксовані обмеження.

Розглянемо сигнал y_T тривалістю $T = Mt$. Ентропія цього сигналу

$$H(Y_T) = MH(Y),$$

де $H(Y)$ – ентропія джерела, обчислена з урахуванням накладених фіксованих обмежень.

Очевидно, що швидкість передавання інформації у такому каналі

$$\bar{I} = \frac{H(Y_T)}{T} = \frac{H(Y)}{t_0}, \quad (3.6)$$

а пропускна здатність

$$C_c = \frac{H(Y)_{\text{макс}}}{t_0}, \quad (3.6a)$$

де $H(Y)_{\text{макс}}$ – максимально можливе значення ентропії кодованого сигналу з урахуванням накладених обмежень.

Для передавання повідомлень використовується код з основою a , тривалості символів коду різні і дорівнюють $\tau_1, \tau_2, \dots, \tau_a$. Фіксовані обмеження на припустиму послідовність передавання різних символів не накладаються.

Аналіз цього випадку показує, що на достатньо великому інтервалі часу T число можливих послідовностей дорівнює

$$N_c(T) = Ar_1^{\frac{T}{\tau_0}}, \quad (3.7)$$

де A – деяка стала; τ_0 – довільний відрізок часу, який звичайно зручно вибрати рівним мінімальній тривалості символу.

Значення r_1 знаходиться як найбільший, дійсний, позитивний корінь рівняння

$$1 - r^{\frac{\tau_1}{\tau_0}} - r^{\frac{\tau_2}{\tau_0}} - \dots - r^{\frac{\tau_a}{\tau_0}} = 0.$$

Підставляючи значення для $N_c(T)$ в (3.3a) і переходячи до границі, отримуємо

$$C_c = \frac{1}{\tau_0} \log r_1. \quad (3.8)$$

Можна показати, що для отримання максимальної швидкості передавання по каналу, в якого тривалості символів не рівні, ймовірності передавання рівних символів також повинні бути нерівними. Так, зокрема, для

розглядуваного випадку ймовірність передавання символу y_j повинна дорівнювати

$$p(y_j) = r_1^{\frac{\tau_j}{\tau_0}}.$$

Корелятивні зв'язки між символами повинні при цьому бути відсутніми.

3.1.2. Побудова недвійкових надлишкових кодів

Оцінка границь елементності q -ічних кодів. Для оцінки розмірів нероздільних q -ічних кодів побудуємо для них аналог границі Варшавова-Гільберта. У двійковому випадку ця границя дається числом K перевірочних символів у коді (N, L) , достатнього для виправлення всіх помилок до кратності t включно (з метою виділення параметрів надлишкових кодів при $q > 2$ від конструкції з $q = 2$ введено нові позначення N, k)

$$K > \log_2 \sum_{i=0}^{2t-1} C_{N-1}^i, \quad (3.9)$$

або

$$2^k > \sum_{i=0}^{2t-1} C_{N-1}^i. \quad (3.9a)$$

Тому що $k = N - L$, то $2^k = 2^N 2^{-L}$. Але 2^N – число можливих N -розрядних двійкових слів, а 2^L – число дозволених L -розрядних (інформаційних) двійкових слів. Отже, величина $2^N 2^{-L}$ аналогічна введеному вище для кодів виду $mBrq$ відношенню $\rho = q^r 2^{-m}$. Значенню N у формулі (3.9a) у коді $mBrq$ відповідає величина $\lceil r \log_2 q \rceil$, де знак $\lceil \rceil$ позначає найближче більше ціле число. Таким чином, отримуємо q -ічний аналог оцінки Варшавова-Гільберта (при $h = 1$)

$$q^r 2^{-m} > \sum_{i=0}^{2t-1} C_{\lceil r \log_2 q \rceil}^i \quad (3.10)$$

де $\lceil \rceil$ – ціле більше число.

Зважаючи на те, що

$$q^r 2^{-m} = q^r 2^{-\rho r} = 2^{r \log_2 q} 2^{-\rho r},$$

то

$$q^r 2^{-m} > 2^{r(\log_2 q - \rho)},$$

і вираз (3.10) можна подати у вигляді

$$2^{r(\log_2 q - \rho)} > \sum_{i=0}^{2r-1} C_{\lceil r \log_2 q - 1 \rceil}^i,$$

де $\rho = \frac{m}{r}$.

У табл. 3.1 наведені результати розрахунків за формулою (3.10).

Отже, при $q = 3$, $\rho = 1,33$ одиничні помилки першого порядку виправляє код 28В21Т ($l = 7$); помилки кратності 2 виправляє код 96В72Т ($l = 24$).

Таблиця 3.1 – Оцінка розмірів кодів $mBrq$, $h = 1$ *

$q = 3, \rho = 1,33$		$q = 5, \rho = 2$	
r		r	
$t = 1$	$t = 2$	$t = 1$	$t = 2$
21	72	20	59

* h – порядок помилки – число дискретних рівнів, на яке змінюється сигнал $1 \leq h \leq q - 1$

виправляє код 28В21Т ($l = 7$); помилки кратності 2 виправляє код 96В72Т ($l = 24$).
Коректуючі п'ятіркові і коди ($q = 5$, $\rho = 2$) мають вигляд – для $t = 1$ 40В20Q1 ($l = 20$) і для $t = 2$ 118В59Q1 ($l = 59$).

Коди $mBrq$ можуть бути побудовані методом модифікованої композиції.

Поняття базового коду. Число дозволених q -ічних слів у кодї $mBrq$ (тобто потужність коду) $M = 2^m$; число можливих q -ічних слів $Q = q^r$. При

$\rho < \log_2 q$ відношення $\mu = \frac{q^r}{2^m} > 1$. За досить великих μ можна будувати коди, що об'єднують корекцію помилок зі збільшенням питомої швидкості передавання ($\rho > 1$).

Назвемо базовим код, для якого при заданому ρ і q значення M мінімальне, тобто код з мінімальним значенням довжини блока. Введемо для базового коду позначення ($\min r, p, q$).

Наприклад, широко застосовуваний у лінійних трактах цифрових систем передачі трійковий код 4В3Т є базовим для $q = 3$, $\rho = 1,33$. Збільшуючи довжину кодових слів (наприклад код 4/В3Т, $l = 2, 3, 4 \dots$, за досить великого l), отримаємо трійковий коректуючий код, що забезпечує збільшення питомої швидкості передавання в $\rho = 1,33$ разів ($l = 7$, код 28В21Т виправляє одиничні помилки; $l = 24$, код 96В72Т виправляє помилки кратності два).

П'ятірковий код 2В/Q1 є базовим для $q = 5$, $\rho = 2$. При $l = 20$ маємо код 40В20Q1, що виправляє одиничні помилки першого порядку, $l = 59$ маємо код 118В59Q1, що виправляє помилки кратності 2 першого порядку.

Метод композиції побудови q -ічних коректуючих кодів. Нехай $X = [x_1, x_2, \dots, x_r]$, $Y = [y_1, y_2, \dots, y_r]$. Слова в q -ічному кодї ($0 \leq x_k, y_k \leq q - 1$; x_k, y_k – цілі числа). Відстань між словами X і Y визначимо формулою:

$$\rho_{\varphi}(X, Y) = \sum_{k=1}^r \varphi(|x_k - y_k|), \quad (3.11)$$

де $\varphi(0) = 0$; $\varphi(p) \geq 1$ при $0 \leq p \leq q-1$.

Окремими випадками (3.11) є відстані Хеммінга ($\varphi(p) = 1$ при $1 \leq p \leq q-1$, Мінковського ($\varphi(p) = p$ при $1 \leq p \leq q-1$), або ($\varphi(p) = \min\{p, q-p\}$ при $1 \leq p \leq q-1$).

Будемо вважати, що множини слів H мають структуру (M, r, ω, d_1, d_2) , якщо виконуються такі умови:

1. Множина H складається з M слів довжини r .
2. Множину H розбито на ω підмножин $H_l (1 \leq l \leq \omega)$.
3. Відстань між словами з тієї ж самої підмножини H_l не менше d_2 .
4. Відстань між словами з різних підмножин не менше d_1 .

Нехай дано дві множини слів F і G , що містять відповідно M_1 і M_2 слів довжини r_1 й r_2 . Композицію F і G будемо називати множиною слів H , складену зі слів виду

$$X = [X_F, X_G], \quad X_F \in F, \quad X_G \in G.$$

Тоді H складається з M_1 і M_2 слів довжини $r_1 + r_2$. Символічно будемо записувати $H = F \cdot G$. Якщо $F = G$, то $H = F^2$. Наприклад, якщо множина F складається зі слів /00/ і /22/, то символічно можна записати:

$$F = \left\{ \begin{array}{cc} 0 & 0 \\ 2 & 2 \end{array} \right\}.$$

Візьмемо множину $G = F$, тоді композиція $H = F \cdot G = F^2$ буде складена з чотирьох наступних слів довжини 4

$$H = \left\{ \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 2 & 2 & 2 & 2 \end{array} \right\}.$$

Для такої композиції можливо сформулювати теорему.

Теорема 1. Нехай є дві множини слів F і G структури $(M_1, r_1, \omega, d_1, d_2)$ і $(M_2, r_2, \omega, d_1, d_2)$, причому у випадку вибору метрики ρ_{φ} вірна нерівність

$$d_2 \geq 2d_1.$$

Тоді композиція $H = F \cdot G$ має структуру $(M_1 \cdot M_2, r_1 + r_2, \omega, d_1, d_2)$.

Доведення. Розіб'ємо множину H на r підмножин за таким правилом:

$$H_l = F_1 G_l + F_2 G_{l+1} + \dots + F_{\omega-l+1} G_{\omega} + F_{\omega-l+2} G_1 + \dots + F_{\omega} G_{l-1}, \quad (3.12)$$

де $1 \leq l \leq \omega$.

Усередині кожного з доданків, що стоять у правій частині (3.12) відстань між словами не менше d_2 . Відстань між словами, що належать різним доданкам, не менше, ніж $2d_1$. Враховуючи відношення $d_2 \geq 2d_1$ ця відстань не менше d_2 . Відстань між словами з H_i і H_j ($i \neq j$) не менше d_1 . Виходить, H має структуру $(M_1 \cdot M_2, r_1 + r_2, \omega, d_1, d_2)$. Теорема доведена.

Наслідок 1. Нехай H має структуру (M, r, ω, d_1, d_2) . Далі у випадку ρ_ϕ вірна нерівність $d_2 \geq 2d_1$. Тоді H^k має структуру $(M^k, k \cdot r, \omega, d_1, d_2)$.

Таким чином, H^k припускає подання

$$H^k = H_1 + H_2 + \dots + H_\omega,$$

де усередині H_l ($1 \leq l \leq \omega$) відстань між словами не менше d_2 , а між словами, що належать двом різним групам H_i і H_j ($i \neq j$), не менше d_1 .

Наслідок 2. Нехай виконуються вимоги наслідку 1 і задано ω слів y_l ($1 \leq l \leq \omega$) довжини r_0 таких, де відстань між будь-якою парою цих слів не менше d_0 . Тоді множина \tilde{H} , утворена словами виду

$$[X_l, Y_l], x_l \in H_l, 1 \leq l \leq \omega,$$

складається із M^k слів довжини $kr + r_0$, причому відстань між будь-якою парою слів з \tilde{H} у випадку метрики ρ_ϕ не менше

$$\min\{d_2, d_1 + d_0\}.$$

Приклад 1. Нехай множини H_1, H_2, H_3 складаються відповідно зі слів

$$\begin{Bmatrix} 0 & 0 \\ 2 & 2 \end{Bmatrix}; \begin{Bmatrix} 2 & 0 \\ 0 & 2 \end{Bmatrix}; \{1 \ 1\}.$$

Тут $q=3$, $\omega=3$, $M=5$, $r=2$. Якщо вибираємо метрику Мінковського, то $d_1=2$, $d_2=4$, тоді виконується й вимога $d_2 \geq 2d_1$. Відповідно до наслідку 1 група H^k має структуру $(5^k, 2k, 3, 2, 4)$. Візьмемо тепер три слова 0, 1, 2, тобто $n_0=1$, $d_0=1$. Через наслідок 2 одержуємо 5^k слів довжини $2k+1$ з мінімальною відстанню між словами, що дорівнює 3. При $k=3$ отримуємо 125 слів довжиною 7 елементів з мінімальною відстанню за Мінковським, що дорівнює 3.

3.1.3. Композиційний метод побудови q -ічних коректуючих кодів

Будемо говорити, що множина слів H має структуру $(M, r, \omega_1 \omega_2, d_1, d_2, d_3)$, якщо виконуються наступні умови:

1. Множина H складається з M слів довжини r .

2. Множина H розбита на ω_1 підмножин H_i ; $0 \leq i \leq \omega_1 - 1$.
3. Кожна множина H_i розбита на ω_2 підмножини H_{ij} ; $0 \leq j \leq \omega_2 - 1$.
4. Відстань між словами в межах однієї підмножини H_{ij} не менше d_3 .
5. Відстань між словами в межах однієї підмножини H_i не менше d_2 ($d_3 > d_2$).
6. Відстань між словами з різних підмножин H_i не менше d_1 ($d_2 > d_1$).

Введемо поняття модифікованої композиції множин кодових слів F і G , що мають структури $(M_F, r_F, \omega_1, \omega_2, d_1, d_2, d_3)$ і $(M_G, r_G, \omega_1, \omega_2, d_1, d_2, d_3)$ відповідно.

Модифікованою композицією цих множин будемо називати множини слів H , побудованих за таким правилом:

1. Складемо композиції

$$\begin{aligned}
 H_{i,k\omega_2+j} = & F_{k,0}G_{(i+k)\bmod\omega_1,j} + F_{k,1}G_{(i+k)\bmod\omega_1,(j+1)\bmod\omega_2} + \dots \\
 & \dots + F_{k,\omega_2-1}G_{(i+k)\bmod\omega_1,(j+\omega_2-1)\bmod\omega_2}, \quad (3.13) \\
 & (0 \leq k, i \leq \omega_1 - 1; 0 \leq j \leq \omega_2 - 1).
 \end{aligned}$$

2. Підмножини H_i визначаються виразом

$$H_i = \sum_{l=0}^{\omega_1\omega_2-1} H_{i,l}. \quad (3.13a)$$

3. Моделювання множини слів H визначається виразом

$$H = \sum_{i=0}^{\omega_1-1} H_i. \quad (3.13б)$$

Приклад 2. Нехай множина F чотвіркових дворозрядних слів має наступні підмножини

$$\begin{aligned}
 F_{0,0} = \begin{Bmatrix} 00 \\ 22 \end{Bmatrix}; F_{0,1} = \begin{Bmatrix} 02 \\ 20 \end{Bmatrix}; F_{0,2} = \begin{Bmatrix} 11 \\ 33 \end{Bmatrix}; F_{0,3} = \begin{Bmatrix} 31 \\ 13 \end{Bmatrix}; \\
 F_{1,0} = \begin{Bmatrix} 01 \\ 23 \end{Bmatrix}; F_{1,1} = \begin{Bmatrix} 30 \\ 12 \end{Bmatrix}; F_{1,2} = \begin{Bmatrix} 10 \\ 32 \end{Bmatrix}; F_{1,3} = \begin{Bmatrix} 21 \\ 03 \end{Bmatrix}.
 \end{aligned}$$

Тут $M_F = 16$; $r_F = 2$; $\omega_1 = 2$; $\omega_2 = 4$; $d_1 = 1$; $d_2 = 2$; $d_3 = 4$. Значить F має структуру (16, 2, 2, 4, 1, 2, 4).

Візьмемо множину $G = F$, тоді $H = F^2$, з урахуванням виразу (3.13) можемо розрахувати всі підмножини $H_{i,l}$. Як приклад розрахуємо для випадку, коли $i = 0, k = 1, j = 0$:

$$H_{0,4} = F_{1,0}F_{1,0} + F_{1,1}F_{1,1} + F_{1,2}F_{1,2} + F_{1,3}F_{1,3}.$$

З урахуванням визначення композиції маємо

$$F_{1,0}F_{1,0} = \left\{ \begin{array}{l} 0101 \\ 0123 \\ 2301 \\ 2323 \end{array} \right\}; \quad F_{1,1}F_{1,1} = \left\{ \begin{array}{l} 3030 \\ 3012 \\ 1230 \\ 1212 \end{array} \right\};$$

$$F_{1,2}F_{1,2} = \left\{ \begin{array}{l} 1010 \\ 1032 \\ 3210 \\ 3232 \end{array} \right\}; \quad F_{1,3}F_{1,3} = \left\{ \begin{array}{l} 2121 \\ 2103 \\ 0321 \\ 0303 \end{array} \right\}.$$

Із наведеного підмножина $H_{0,4}$ буде складатися з 16 наступних слів:

0101	1010	2103	3012
0123	1032	2121	3030
0303	1212	2301	3210
0321	1230	2323	3232

Відстань між цими словами не менше 4. Із цих слів можна побудувати код 4B4Q, що виправляє одиничні помилки, тому що маємо 16 підмножин $H_{i,l}$, що мають однакове число слів, тобто маємо 16 варіантів цього коду.

За виразом (3.13a) можемо розрахувати всі підмножини H_i , а за (3.13б) множину H .

Теорема 2. Нехай є дві множини слів F і G структури $(M_F, r_F, \omega_1, \omega_2, d_1, d_2, d_3)$ і $(M_G, r_G, \omega_1, \omega_2, d_1, d_2, d_3)$. Причому у випадку вибору метрики ρ_ϕ вірними нерівностями будуть:

$$2d_1 \geq d_2;$$

$$2d_2 \geq d_3.$$

Тоді модифікована композиція $H = FG$ має структуру

$$(M_F \cdot M_G; r_F + r_G; \omega_1, \omega_1\omega_2, d_1, d_2, d_3). \quad (3.13в)$$

Доведення. З виразу (3.13) видно, що відстань між словами усередині кожного зі складових, що стоять у правій частині (3.13) не менше d_3 . Відстань між словами, що належать різним складовим, не менше, ніж $2d_2$, внаслідок відношень d_1 і d_2 , ця відстань не менше d_3 . Відстань між словами з $H_{i, k\omega_2+a}$ і $H_{i, k\omega_2+b}$ ($a \neq b$) не менше d_2 . Відстань між словами з $H_{i, c\omega_2+j}$ і $H_{i, d\omega_2+j}$ ($c \neq d$) не менше, ніж $2d_1$, тобто ця відстань не менше d_2 . Виходить, що H_i містить $\omega_1\omega_2$ підмножин, відстань між якими не менше d_2 . Відстань між словами з H_g і H_h ($g \neq h$) не менше d_1 . Значить H має структуру $(M_F M_G, r_F + r_G, \omega_1, \omega_1\omega_2, d_1, d_2, d_3)$. Теорема доведена.

Зауваження. При $\omega_1 = 1, \omega_2 > 1$; або $\omega_1 > 1, \omega_2 = 1$ теорема 2 перетворюється в теорему 1. Дійсно, наприклад $\omega_1 > 1, \omega_2 = 1, F$ має структуру $(M_F, r_F, \omega_1, d_1, d_2)$, G має структуру $(M_G, r_G, \omega_1, d_1, d_2)$ і тоді H має структуру $(M_F \cdot M_G, r_F + r_G, \omega_1, d_1, d_2)$.

Наслідок 3. Якщо $\omega_1 > 1, d_3$ непарне, тобто

$$d_3 \geq 2t + 1; t = 1, 2, \dots \quad (3.14)$$

і

$$d_1 + d_2 \geq d_3, \quad (3.14a)$$

тоді модифікована композиція $L = HF$ має структуру $(M_F \cdot M_G \cdot M_F, r_F + r_G + r_F, \omega_1 \cdot \omega_1, \omega_2, d_1, d_2, d_3)$, де $H = FG$ відповідає структурі (3.13в).

Дійсно, якщо складемо композиції

$$\begin{aligned} L_{(i\omega_1+k),j} = & (H_{i,0}F_{k,j} + H_{i,1}F_{k,(j+k)\bmod\omega_2} + \dots + H_{i,\omega_1-1}F_{k,(j-1k)\bmod\omega_2}) + \\ & + H_{i,\omega_2}F_{(k+1)\bmod\omega_1,j} + H_{i,\omega_2+1}F_{(k+1)\bmod\omega_1,(j+1)\bmod\omega_2} + \dots \\ & \dots + H_{i,2\omega_2-1}F_{(k+1)\bmod\omega_1,(j-1)\bmod\omega_2} + \dots + (H_{i,(\omega_1-1)\omega_2}F_{(k-1)\bmod\omega_1,j} + \\ & + H_{i,(\omega_1-1)\omega_2+1}F_{(k-1)\bmod\omega_1,(j+1)\bmod\omega_2} + \dots + H_{i,(\omega_1\omega_2-1)}F_{(k-1)\bmod\omega_1,(j-1)\bmod\omega_2}) \} \\ & (0 \leq k \leq \omega_1 - 1; 0 \leq i \leq \omega_1 - 1; 0 \leq j \leq \omega_2 - 1); \end{aligned} \quad (3.15)$$

$$L_l = \sum_{j=0}^{\omega_2-1} L_{l,j}; \quad (3.15a)$$

$$L = \sum_{l=0}^{\omega_1\omega_2-1} L_l, \quad (3.15b)$$

то побачимо, що відстань між словами усередині кожного зі складових, що стоять у правій частині (3.15) не менше d_3 . Відстань між словами, що належать різним складовим не менше, ніж $d_1 + d_2$. Враховуючи відношення між d_1, d_2, d_3 , внаслідок (3.14a), ця відстань не менше d_3 . Відстань між словами із $L(i\omega_1 + k)$, а $L(i\omega_1 + k), b$; ($a \neq b$) не менше d_2 . Відстань між словами із $L(g\omega_1 + k), j$ і $L(h\omega_1 + k), j$; ($g \neq h$) не менше d_1 . Відстань між словами із $L(i\omega_1 + c), j$ і $L(i\omega_1 + d), j$; ($c \neq d$) не менше d_1 .

Значить L має структуру $(M_F \cdot M_G \cdot M_F, r_F + r_G + r_F, \omega_1 \cdot \omega_1, \omega_2, d_1, d_2, d_3)$.

Приклад 3. Нехай множина F трійкового дворозрядного коду має наступні множини:

$$\begin{aligned} F_{0,0} = \left\{ \begin{array}{l} 00 \\ 22 \end{array} \right\}; & \quad F_{0,1} = \left\{ \begin{array}{l} 02 \\ 20 \end{array} \right\}; & \quad F_{0,2} = \{11\}; \\ F_{1,0} = \{01\}; & \quad F_{1,1} = \{10\}; & \quad F_{1,2} = \{21\}. \end{aligned}$$

Тут $M_F = 8, r_F = 2; \omega_1 = 2; \omega_2 = 3; d_1 = 1; d_2 = 2; d_3 = 4$ (відстань у метриці Мінковського). Відношення між d_1 і d_2 виконується. Якщо візьмемо $d_3 = 3$, то виконуються ще умови (3.14) і (3.14а). Отже F має структуру (8, 2, 2, 3, 1, 2, 3). Візьмемо множину $G = F$, тоді за наслідком 3 композиція $L = FH$ або $L = F^3$ має структуру $(8^3, 6, 4, 3, 1, 2, 3)$. За (3.15) можна розрахувати всі значення $L_{h,j}$, де $H_{i,l}$ розраховуються за (3.13). Як приклад наведемо три наступних розрахованих підмножин:

$$1) k = 0, i = 0, j = 0$$

$$L_{0,0} = H_{0,0}F_{0,0} + H_{0,1}F_{0,1} + H_{0,2}F_{0,2} + H_{0,3}F_{0,1} + H_{0,4}F_{1,1} + H_{0,5}F_{1,2}.$$

$$2) k = 0, i = 0, j = 0$$

$$L_{0,1} = H_{0,0}F_{0,1} + H_{0,1}F_{0,2} + H_{0,2}F_{0,0} + H_{0,3}F_{1,1} + H_{0,4}F_{1,2} + H_{0,5}F_{1,0}.$$

$$3) k = 0, i = 0, j = 2$$

$$L_{0,2} = H_{0,0}F_{0,2} + H_{0,1}F_{0,0} + H_{0,2}F_{0,1} + H_{0,3}F_{1,2} + H_{0,4}F_{1,0} + H_{0,5}F_{1,1},$$

де за (3.13)

$$H_{0,0} = F_{0,0}F_{0,0} + F_{0,1}F_{0,1} + F_{0,2}F_{0,2};$$

$$H_{0,1} = F_{0,0}F_{0,1} + F_{0,1}F_{0,2} + F_{0,2}F_{0,0};$$

$$H_{0,2} = F_{0,0}F_{0,2} + F_{0,1}F_{0,0} + F_{0,2}F_{0,1};$$

$$H_{0,3} = F_{1,0}F_{1,0} + F_{1,1}F_{1,1} + F_{1,2}F_{1,2};$$

$$H_{0,4} = F_{1,0}F_{1,1} + F_{1,1}F_{1,2} + F_{1,2}F_{1,0};$$

$$H_{0,5} = F_{1,0}F_{1,2} + F_{1,1}F_{1,0} + F_{1,2}F_{1,1}.$$

За визначенням композиції, можемо записати всі слова в кожній підмножині. Для спрощення не будемо записувати всі слова, а тільки їх суму, яку позначимо через $N(H_{i,l})$ або $N(L_{h,j})$. Таким чином:

$$N(H_{0,0}) = 4 + 4 + 1 = 9;$$

$$N(H_{0,1}) = 4 + 2 + 2 = 8;$$

$$N(H_{0,2}) = 2 + 4 + 2 = 8;$$

$$N(H_{0,3}) = 1 + 1 + 1 = 3;$$

$$N(H_{0,4}) = 1 + 1 + 1 = 3;$$

$$N(H_{0,5}) = 1 + 1 + 1 = 3;$$

$$N(L_{0,0}) = 18 + 16 + 8 + 3 + 3 + 3 = 51;$$

$$N(L_{0,1}) = 18 + 8 + 16 + 3 + 3 + 3 = 51;$$

$$N(L_{0,2}) = 9 + 16 + 16 + 3 + 3 + 3 = 50.$$

Відстань між словами в кожній підмножині $L_{0,j}$ не менше 3. Відстань між словами з різних підмножин $H_{0,l}$ або $L_{0,j}$ теж не менше 3. Відстань між словами з різних підмножин $H_{0,l}$ або $L_{0,j}$ не менше 2. Додаючи 0, 1, 2 до кожного $L_{0,j}$, наприклад $[0][L_{0,0}]; [1][L_{0,1}]; [2][L_{0,2}]$, отримуємо 152 трійкових семирозрядних слова, що мають відстань не менше 3. (Методом композиції при цьому виходить тільки 125 слів). Із цих слів можемо побудувати код 7В7Г, що виправляє одиничні помилки, не змінюючи питомої швидкості передавання.

Наслідок 4. Якщо ω_1 непарне, тобто

$$\omega_1 = 2t + 1, \quad t = 1, 2, \dots,$$

і виконуються умови (3.14), (3.14а), то модифікована композиція $L = HF$ буде мати структуру

$$(M_F \cdot M_G \cdot M_F, r_F + r_G + r_F, \omega_1, \omega_1 \omega_2, d_1, d_2, d_3), \quad (3.15в)$$

де $H = FG$ має структуру (3.13в). Модифікована композиція $Q = LF$ в цьому випадку має структуру

$$(M_F \cdot M_G \cdot M_F \cdot M_F, r_F + r_G + r_F + r_F, \omega_1 \omega_2, \omega_2, d_1, d_2, d_3). \quad (3.15г)$$

Доведення. Якщо виконується умова для ω_1 , то з (3.13) видно, що відстань між словами з підмножин $H_{i, k\omega_2 + j}; H_{(i+1) \bmod \omega_1, ((k+1) \bmod \omega_1) \omega_2 + j}; \dots; H_{(i-1) \bmod \omega_1, ((k-1) \bmod \omega_1) \omega_2 + j}$ не менше d_2 , хоча вони належать різним підмножинам H_i . Із цього зауваження можемо скласти такі композиції:

$$\begin{aligned} L_{i, ((i+h) \bmod \omega_1) \omega_2 + j} &= \sum_{k=0}^{\omega_1 - 1} (H_{(i+h) \bmod \omega_1, k\omega_2} F_{(k-h) \bmod \omega_1, j} + \\ &+ H_{(i+h) \bmod \omega_1, k\omega_2 + 1} F_{(k-h) \bmod \omega_1, (j+1) \bmod \omega_2} + \dots \\ &\dots + H_{(i+h) \bmod \omega_1, k\omega_2 + \omega_2 - 1} F_{(k-h) \bmod \omega_1, (j + \omega_2 - 1) \bmod \omega_2}), \\ (0 \leq h \leq \omega_1 - 1; \quad 0 \leq i \leq \omega_1 - 1; \quad 0 \leq j \leq \omega_2 - 1); \end{aligned}$$

$$L_i = \sum_{l=0}^{\omega_1 \omega_2 - 1} L_{i,l};$$

$$L = \sum_{i=0}^{\omega_1 - 1} L_i.$$

Зі значень для h, i, j видно, що відстань між словами усередині кожного зі складових, що стоять у правій частині не менше d_3 . Відстань між словами, що належать різним складовим не менше, ніж $d_1 + d_2$. Внаслідок (3.14а) ця відстань не менше d_3 . Відстань між словами з підмножин $L_{i, ((i+h) \bmod \omega_1) \omega_1 + a}$ і $L_{i, ((i+h) \bmod \omega_1) \omega_2 + b}; (a \neq b)$ не менше d_2 . Відстань між словами з $L_{i, c\omega_2 - j}$ і $L_{i, d\omega_2 + j}; (c \neq d)$ теж не менше d_2 . Відстань між словами з

підмножин $L_{g,((i+h) \bmod \omega_1)\omega_2+j}$ і $L_{f,((i+h) \bmod \omega_1)\omega_2+j}$; ($g \neq f$) не менше d_1 . Зна-
 чить L має структуру $(M_F \cdot M_G \cdot M_F, r_F + r_G + r_F, \omega_1, \omega_1\omega_2, d_1, d_2, d_3)$.

Модифіковану композицію $Q = LF$ будемо будувати за (3.15),
 (3.15а), (3.15б), при цьому замість H вводимо L , а замість L значення Q .
 Тоді отримаємо структуру (3.15г).

Приклад 4. Нехай множина трійкових трирозрядних слів (B) склада-
 ється з таких підмножин

$$\begin{aligned} B_{0,0} &= \begin{Bmatrix} 000 \\ 111 \\ 222 \end{Bmatrix}; & B_{0,1} &= \begin{Bmatrix} 012 \\ 120 \\ 201 \end{Bmatrix}; & B_{0,2} &= \begin{Bmatrix} 021 \\ 102 \\ 012 \end{Bmatrix}; \\ B_{1,0} &= \begin{Bmatrix} 001 \\ 112 \\ 220 \end{Bmatrix}; & B_{1,1} &= \begin{Bmatrix} 010 \\ 121 \\ 202 \end{Bmatrix}; & B_{1,2} &= \begin{Bmatrix} 022 \\ 100 \\ 211 \end{Bmatrix}; & (3.15д) \\ B_{2,0} &= \begin{Bmatrix} 002 \\ 110 \\ 221 \end{Bmatrix}; & B_{2,1} &= \begin{Bmatrix} 011 \\ 122 \\ 200 \end{Bmatrix}; & B_{2,2} &= \begin{Bmatrix} 020 \\ 101 \\ 212 \end{Bmatrix}. \end{aligned}$$

Тут $M_B = 3^3$; $r_B = 3$; $\omega_1 = \omega_2 = 3$; $d_1 = 1$; $d_2 = 2$; $d_3 = 3$, тобто множина
 B має структуру $(3^3, 3, 3, 3, 1, 2, 3)$ (відстані в метриці Хеммінга). Умови
 (3.14), (3.14а), (3.15в) виконуються. Тоді модифікована композиція
 $E = B \cdot B = B^2$, за теоремою 3.2 має структуру $(3^6, 6, 3, 9, 1, 2, 3)$. Модифі-
 кована композиція $G = E \cdot B = B^3$ за наслідком 4 має структуру $(3^9, 9, 3, 9,$
 $1, 2, 3)$. Модифікована композиція $K = G \cdot B = B^4$ за наслідком 4 має струк-
 туру $(3^{12}, 12, 9, 3, 1, 2, 3)$.

Тому що числа слів у кожній підмножині $B_{i,j}$ однакові, то числа слів
 у підмножинах $E_{i,j}$ ($0 \leq i \leq 0, 0 \leq j \leq 8$); $G_{i,j}$ ($0 \leq i \leq 2, 0 \leq j \leq 8$) і
 $K_{i,j}$ ($0 \leq i \leq 8, 0 \leq j \leq 2$) теж однакові, і вони легко розраховуються і дорі-
 внюють загальній кількості слів, що поділена на загальну кількість під-
 множин, таким чином

$$N(E_{i,j}) = \frac{M_F}{3 \cdot 9} = 3^3; \quad (3.16)$$

$$N(G_{i,j}) = \frac{M_G}{3 \cdot 9} = 3^6; \quad (3.16а)$$

$$N(K_{i,j}) = \frac{M_K}{9 \cdot 3} = 3^9. \quad (3.16б)$$

Теорема 3. Повна множина q -ічних трирозрядних кодових слів
 $M = q^3$ має структуру $(q^3, 3, 3, 3, 1, 2, 3)$.

Доведення. Однорозрядні q -ічні кодові слова при $q > 3$ завжди можна поділити на три групи, відстань між словами з однієї і тієї самої групи дорівнює 3, а відстань між словами із різних груп дорівнює 1. Так, наприклад, для $q = 4$ маємо

$$I_0 = \left\{ \begin{matrix} 0 \\ 3 \end{matrix} \right\}, \quad I_1 = \{1\}, \quad I_2 = \{2\}. \quad (3.17)$$

Для $q = 5$ отримаємо

$$I_0 = \left\{ \begin{matrix} 0 \\ 0 \end{matrix} \right\}, \quad I_1 = \left\{ \begin{matrix} 1 \\ 4 \end{matrix} \right\}, \quad I_2 = \{2\}. \quad (3.17a)$$

Для $q = 6$

$$I_0 = \left\{ \begin{matrix} 0 \\ 3 \end{matrix} \right\}, \quad I_1 = \left\{ \begin{matrix} 1 \\ 4 \end{matrix} \right\}, \quad I_2 = \left\{ \begin{matrix} 2 \\ 5 \end{matrix} \right\} \quad (3.17б)$$

і т.д.

Множина трійкових трирозрядних кодових слів, як показано в прикладі 4, має структуру $(3^3, 3, 3, 3, 1, 2, 3)$ (відстані в метриці Хеммінга). Якщо замість $[0]$, $[1]$, $[2]$ підставимо I_0, I_1, I_2 відповідно, то в результаті композиції множин I_i ($i = 0, 1, 2$) отримаємо множину трирозрядних q -ічних кодів, що мають структуру $(q^3, 3, 3, 3, 1, 2, 3)$.

Приклад 5. Розглянемо приклад для $q = 5$. Запишемо I_0, I_1, I_2 замість 0, 1, 2 відповідно, тоді $B_{0,0}$ (3.15д) буде мати вигляд

$$B_{0,0} = \left\{ \begin{matrix} I_0 & I_0 & I_0 \\ I_1 & I_1 & I_1 \\ I_2 & I_2 & I_2 \end{matrix} \right\}. \quad (3.17в)$$

В результаті для композицій I_0, I_1, I_2 за (3.17в) отримаємо 17 слів трирозрядного п'ятіркового коректуючого коду:

$$B_{0,0} = \left\{ \begin{matrix} 000 & 111 \\ 003 & 114 \\ 030 & 141 \\ 033 & 144 \\ 300 & 411 \\ 303 & 414 \\ 330 & 441 \\ 333 & 444 \end{matrix} \right\}.$$

Відстань між цими словами не менше 3. Код 222 виправляє одиничні помилки першого порядку. З цих слів можна будувати код 4В3Q1.

Аналогічним чином згідно з (3.15г) можна отримати всі останні слова $B_{i,j}$ (3.15д).

Для множини п'ятіркових трирозрядних слів маємо структуру ($5^3, 3, 3, 3, 1, 2, 3$).

Застосовуючи наслідки 3, 4 і теорему 3 можемо розрахувати всі дозволені слова п'ятіркових коректуючих кодів ($d_M \geq 3$) з будь-якою довжиною не менше трьох. Із таких слів можемо побудувати відповідні коди $mBrQ1$. Деякі результати для різних r наведені в табл. 3.2.

Аналогічно прикладу 4, розрахунки можна виконувати для всіх $q \geq 3$, тобто можна розрахувати всі дозволені слова q -ічних коректуючих кодів ($d_M \geq 3$).

Таблиця 3.2 – Деякі коректуючі коди $mBrQ1$, отримані методом модифікованої композиції

r	3	4	10	15	20
N_p	17	70	5^8	$5^{13} \cdot 13 / 27$	$5^{20} / 81$
Коди	4B3Q1	6B4Q1	19B10Q1	29B15Q1	40B20Q1
ρ	1,33	1,5	1,8	1,93	2,0

Для порівняння в табл. 3.3 наведені деякі результати розрахунків за двома методами. З табл. 3.3 видно, що метод модифікованої композиції дає більш щільне упакування при збільшенні r і q .

Таблиця 3.3 – Порівняння методів композиції і модифікованої композиції

r	$q = 3 \ N_p(r)$		$q = 4 \ N_p(r)$		$q = 5 \ N_p(r)$	
	методом композиц.	модифік. композиц.	методом композиц.	модифік. композиц.	методом композиц.	модифік. композиц.
3	5	5	8	10	14	17
4	9	9	16	32	51	70
5	25	25	64	64	205	210
6	46	51	256	256	663	765
7	125	152	1024	1024	3061	3125
8	261	264	2048	3244	8619	
9	629	787	8192	9766	33813	

Оцінки коректуючої здатності q -ічних кодів. Проведемо порівняння трійкових і п'ятіркових коректуючих кодів з відповідними базовими кодами, тобто за фіксованих значень ρ і q .

Ймовірність помилки на символ базових кодів розраховується за наближеною формулою:

$$P_{\text{пом с}} = \frac{q-1}{q} \left[1 - 2\Phi\left(\frac{1}{q-1} \frac{U_c}{\sigma}\right) \right], \quad (3.18)$$

Формула (3.18) отримана в припущенні, що

$$\Phi\left(\frac{3}{q-1} \frac{U_c}{\sigma}\right) \approx 1.$$

Будемо вважати, що в тракці передачі відсутні міжсимвольні спотворення і не враховуються девіації моментів відхилення тактових імпульсів на приймальній стороні.

Ймовірність помилки в слові коректуючого коду з мінімальною кодовою відстанню d_M (у метриці Мінковського) можна оцінити за формулою

$$P_{\text{помдек}} = \sum_{h=\frac{d_M+1}{2}}^{q-1} P_{\text{пом}}(h, t=1) + \sum_{t=\frac{d_M+1}{2}}^r P_{\text{пом}}(t, h=1). \quad (3.18a)$$

де $P_{\text{пом}}(h, t=1)$ – ймовірність помилки порядку h і кратності $t=1$; $P_{\text{пом}}(t, h=1)$ – ймовірність помилки порядку кратності t і $h=1$.

Для $q=3$, $d=3$ (код 28B21T) отримуємо

$$P_{\text{помдек}} = P_{\text{пом}}(h=2, t=1) + \sum_{t=2}^r P_{\text{пом}}(t, h=1). \quad (3.18б)$$

Ймовірність помилки другого порядку при кратності $t \geq 3$ (за існуючих захищеностей A_3 , характерних для лінійних трактів цифрових систем передачі) мала порівняно $P_{\text{пом}}(t=2, h=1)$. Зневажаючи ними у формулі (3.18б), отримуємо

$$P_{\text{помдек}}(q=3, d_M=3) \approx P_{\text{пом}}(t=2, h=1) = \frac{r!}{2!(r-2)!} P_{\text{помс}}^2. \quad (3.18в)$$

Аналогічно, для коду 96B72T ($q=5$, $d=3$), отримуємо

$$P_{\text{помдек}}(q=3, d_M=5) \approx \frac{r!}{3!(r-3)!} P_{\text{помс}}^3. \quad (3.18г)$$

Для п'ятіркових коректуючих кодів отримуємо з формули (3.18а) – при $q=5$, $d=3$

$$P_{\text{помдек}} = \sum_{h=2}^4 P_{\text{пом}}(h, t=1) + \sum_{t=2}^r P_{\text{пом}}(t, h=1). \quad (3.18д)$$

Зневажаючи у формулі (3.18д) ймовірностями помилок високого порядку й кратності, отримуємо для коду 40B20Q1

$$P_{\text{помдек}}(q=5, d_M=3) \approx \frac{r!}{2!(r-2)!} P_{\text{помс}}^2. \quad (3.19)$$

Аналогічно для коду 118B53Q1 ($d=2$), маємо

$$P_{\text{помдек}}(q=2, d_M=5) \approx \frac{r!}{3!(r-3)!} P_{\text{помс}}^3. \quad (3.20)$$

Результати розрахунків за формулами (3.18a ... 3.20) наведені на рис. 3.1. На рис. 3.2 показані залежності, що характеризують енергетичний вигравш, що дається коректуючим кодами 96B72T і 118B59Q1 порівняно з базовими кодами 4B3T і 2B1Q1 відповідно.

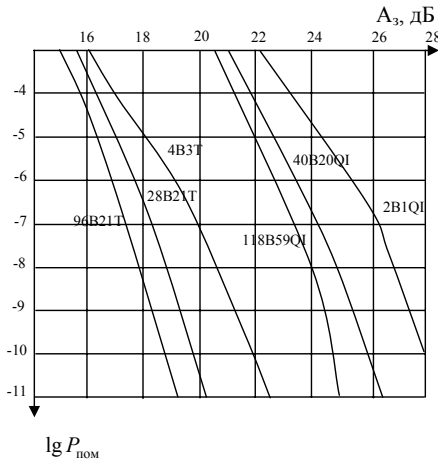


Рисунок 3.1 – Розрахунки за формулами (3.18a ... 3.20)

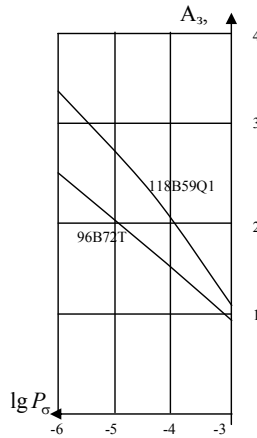


Рисунок 3.2 – Енергетичний вигравш кодів 96B72T і 118B59Q

3.1.4. Ефективність використання алфавіту каналу при $q > 2$

При розгляді інформаційних характеристик каналів зв'язку було показано, що пропускна здатність неперервного каналу при гауссівському шумі визначається смугою ΔF й відношенням потужностей сигналів P_c і завади P_3

$$\frac{P_c}{P_3} = h_c^2,$$

$$C = 2\Delta F \log_2(1 + h_c^2). \quad (3.21)$$

У бінарних дискретних системах пропускна здатність обмежена смугою пропускання ΔF , тому що межа Найквіста для швидкості модуляції B при лінійних амплітудно-частотній і фазо-частотній характеристиках $B = \Delta F$ забезпечує можливість роботи за відсутності міжсимвольних спотворень. Отже, для стандартного телефонного каналу зі смугою $\Delta F = 3100$ при передаванні двійкових сигналів $C \leq 6200$ біт/с.

У той самий час реальне значення h^2 існуючих провідних телефонних каналів дозволяє отримати при $h^2 \geq 25$ $C > 15000$ біт/с. Отримання пропускної здатності, що перевищує швидкість модуляції, можливо тільки

у випадку, коли кожний елементарний сигнал тривалістю $t_0 = 1/\Delta F$ (найквістовий елемент) переносить більше одного біта інформації. У цьому випадку основа коду більше двох і сигнали називають багатопозиційними. Нехай алфавіт джерела містить M повідомлень. Тоді, порівнюючи сигнали з основами a_1 і a_2 з умови

$$M = a_1^{n_1} = a_2^{n_2},$$

можна отримати співвідношення для значності кодових комбінацій

$$\frac{n_1}{n_2} = \frac{\log_2 a_1}{\log_2 a_2}. \quad (3.22)$$

Отже, при заданій швидкості модуляції час передавання повідомлень при використанні багатопозиційних сигналів можна зменшити в $\log_2 n_2$ разів. Якщо тривалість сигнальної конструкції залишити постійною, то за цей рахунок можна збільшити значення h^2 на інтервалі кодового слова.

Розрахунок імовірності помилкового приймання P_e , одного із можливих з ансамблю «а» сигналів, на одиничному інтервалі досить складний, тому що не всі сигнали ортогональні, рівноймовірні й мають однакову енергію. Якщо вважати, що зазначені властивості є, то можна визначити верхню межу P_e .

На рис. 3.3 сигнали (позиції) представлені в тривимірному просторі. При передаванні сигналу U_{c1} вектор прийнятого сигналу $U_p = (U_{c1} + U_{s1}) + U_{s2} + U_{s3}$, де U_s – напруга завади; U_{s1} , U_{s2} , U_{s3} – складові флукутаційної завади на осях φ_1 , φ_2 і φ_3 ; вектор $U_{c1} = \Psi_1 \sqrt{Q_c}$; Ψ_1 – одиничний вектор координатної осі φ_1 (Q_c – енергія сигналу).

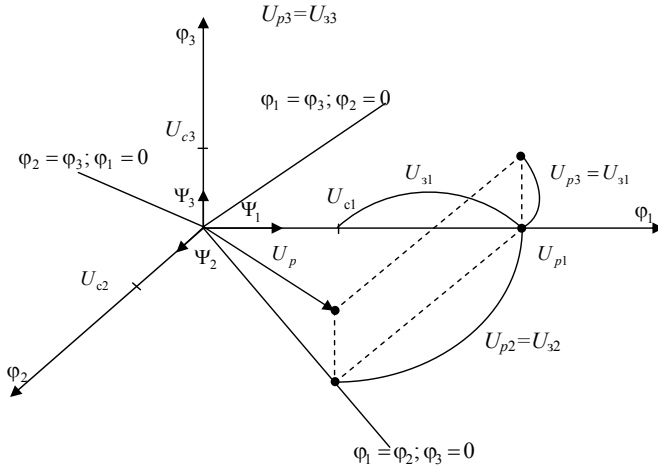


Рисунок 3.3 – Сигнали у тривимірному просторі

На приймальній стороні може бути помилка, якщо $U_{32} > U_{c1} + U_{32}$ або $U_{32} > U_{c1} + U_{31}$. У цьому випадку буде зареєстровано сигнал U_{c3} . Відповідно до критерію максимуму правдоподібності, оптимальний приймач повинен вибрати з ансамблю «а» випадкових величин

$$\alpha(l) = \left\{ \frac{1}{\sigma_3^2} \cdot \int_{-T/2}^{T/2} U_{cl} U_3 dt + h_{cl}^2 \Delta_{lr} \right\}, \quad (3.23)$$

де $l = 1; 2; \dots a$, найбільша величина, що відповідає передаванню сигналу U_{cr} . Тут h_{cl}^2 – перевищення l -го сигналу; Δ_{lr} – символ Кронекера.

Знайдемо закон розподілу величин α_l , де $l \neq r$. Розкладаючи заваду й сигнал у ряд Котельникова

$$U_c(t) = \sum_{k=1}^n A_{ck} \Phi_k(t), \quad U_3(t) = \sum_{k=1}^n A_{3k} \Phi_k(t),$$

отримаємо

$$\alpha_l = \frac{1}{\sigma_3^2} \sum_{k=1}^n A_{3k}; \quad A_{ck} = \sum_{k=1}^n A_{3k} \frac{A_{ck}}{\sigma_3^2}. \quad (3.24)$$

Вагові коефіцієнти A_{ck} – не випадкові, а A_{3k} – статистичні випадкові величини з нормальним законом розподілу й дисперсією σ_3^2 . Тому доданки A_{3k} також мають нормальний закон розподілу:

$$W(\alpha_l) = \frac{1}{\sqrt{2\pi}\sigma_\alpha} e^{-\frac{\alpha_l^2}{2\sigma_\alpha^2}}. \quad (3.25)$$

Величина α_r має густину розподілу ймовірностей

$$\omega(\alpha_r) = \frac{1}{\sqrt{2\pi}\sigma_\alpha} e^{-\frac{(\alpha_r - 2h_c^2)^2}{2\sigma_\alpha^2}}.$$

Для вірного виявлення сигналу U_{cr} необхідно, щоб $\alpha_r \geq U_0$, а для $(a-1)$ інших величин $\alpha_l < U_0$. Тоді ймовірність помилкового розв'язання

$$\begin{aligned} p(U_{cr}) &= 1 - \int_{-\infty}^{\infty} [p(\alpha_l < U_0)]^{a-1} \omega(\alpha_r) dU_0 = \\ &= \int_{-\infty}^{\infty} \left[\frac{1}{\sqrt{2\pi}\sigma_\alpha} \int_{-\infty}^{U_0} e^{-\frac{z^2}{2\sigma_\alpha^2}} dz \right]^{a-1} \times \frac{1}{\sqrt{2\pi}\sigma_\alpha} \exp\left[-\frac{(U_0 - 2h_c^2)^2}{2\sigma_\alpha^2}\right] dU_0. \end{aligned}$$

Після перетворень отримаємо

$$p_0 = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} V^{(a-1)} \left(\sqrt{2h_c^2} + U_0 \right) e^{-\frac{z^2}{2}} dz, \quad (3.26)$$

де $V(z)$ – функція Лапласа.

Враховуючи припущення, що всі «а» сигналів рівноймовірні й мають однакову енергію, то вираз (3.26) справедливий для будь-якого сигналу «а» алфавіту.

Якщо сигнали рівноймовірні, але мають різну питому енергію

$$P_{0a} = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^a \prod_{k=1}^a \left[V \left(\frac{Q_{cr}^2 + Q_{ck}^2}{\sqrt{2V_3^2 Q_{ck}^2}} + U_0 \sqrt{\frac{Q_{cr}^2}{Q_{ck}^2}} \right) \right] e^{-\frac{z^2}{2}} dz. \quad (3.27)$$

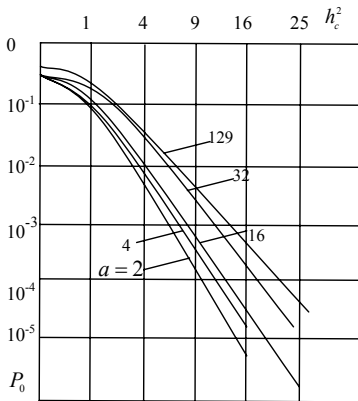


Рисунок 3.4 – Залежності ймовірності помилкового приймання елемента за різних а та h_c^2

сигнал при $a_1 = 16$, двохелементний при $a_2 = 4$, чотирихелементний при $a_3 = 2$.

Для розрахунку завадостійкості скористаємося виразом (3.26) і розкладанням інтеграла ймовірностей в ряд

$$\Phi(Z) = \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} \left(\frac{1}{z} - \frac{1}{z^3} + \frac{3}{z^5} - \frac{15}{z^7} \right).$$

Тоді ймовірність помилки за двійкових сигналів з однаковою енергією

$$P_{0(a=2)} = \Phi\left(\sqrt{h_{c(a=2)}^2}\right) = \frac{1}{\sqrt{2\pi h_{c(a=2)}^2}} e^{-\frac{h_{c(a=2)}^2}{2}}.$$

В зв'язку з тим, що перевищення чотиризначного двійкового сигналу

$$h_{c(n=4)}^2 = 4h_{c(a=2)}^2,$$

то ймовірність помилкового приймання кодового слова довжиною $n = 4$

Легко показати, що при $Q_c^2 = \text{const}$ вираз (3.27) переходить у вираз (3.26).

На рис. 3.4 наведені залежності ймовірності помилкового приймання елемента за різних а і h_c^2 . Із цих залежностей слідує, що зміна числа позиції сигналу від 2 до 128 при «хороших» каналах ($h^2 > 9$) збільшує ймовірність помилкового приймання елемента більш ніж на два порядки.

Порівняння багатопозиційних і багатозначних двійкових сигналів.

Як приклад розглянемо випадок, коли алфавіт джерела містить 16 рівноймовірних символів. Для передачі такого алфавіту можна використовувати однозначний (одноеlementний) кодовий

$$P_{a=2}^{(n=4)} = (1 - p_{0(a=2)})^4 \approx 4p_{0(a=2)}.$$

З огляду на те, що при розкладанні $\Phi(z)$ для $z \geq 3$ похибка становить не більше 10 %, для p_{0a} отримаємо

$$p_{0a} \approx \frac{a-1}{\sqrt{2\pi h_c^2}} e^{-\frac{h_c^2}{2}}. \quad (3.28)$$

З огляду на вираз (3.28), отримаємо

$$P_{(a=2)}^{(n=4)} = \frac{8}{\sqrt{2\pi h_{c(n=4)}^2}} e^{-\frac{h_{c(n=4)}^2}{2}}. \quad (3.29)$$

Ймовірність спотворення двозначного чотирипозиційного сигналу

$$P_{(a=4)}^{(n=2)} = 1 - (1 - p_{0(a=4)})^2 = 2p_{0(a=4)},$$

де

$$p_{0(a=4)} = \frac{1}{\sqrt{2\pi h_{c(a=4)}^2}} e^{-\frac{h_{c(a=4)}^2}{2}}. \quad (3.30)$$

Тому що перевищення чотирипозиційного сигналу (імпульсу) $h_{c(a=4)}^2$ однозначно пов'язане з перевищенням двозначного чотирипозиційного сигналу $h_{c(n=2)}^2$ відношенням

$$h_{c(n=2)}^2 = 2h_{c(a=4)}^2, \quad (3.31)$$

то остаточно отримаємо

$$P_{(a=2)}^{(n=4)} = \frac{2}{\sqrt{2\pi h_{c(n=2)}^2}} e^{-\frac{h_{c(n=2)}^2}{4}}. \quad (3.32)$$

За отриманими виразами побудовані залежності $p_0 = f(h_c^2)$ для $n = 2$ і $a = 4(1)$; $n = 4$; $a = 2(2)$; $n = 1$, $a = 16(3)$ (рис. 3.5).

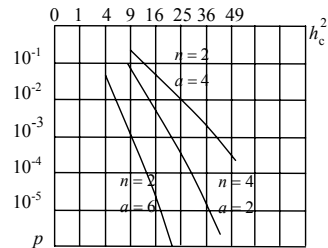


Рисунок 3.5 – Залежність $p_0 = f(h_c^2)$

З рис. 3.5. слідує, що потенційна завадостійкість при $a > 2$ вище завадостійкості багатоеlementних конструкцій двійкового сигналу.

Вплив швидкості передавання інформації на вірність зв'язку. Якщо швидкість модуляції становить B дв. од/с (Бод), то за час T можна передати $M = 2^{BT}$ різних рівноймовірних повідомлень. При використанні простого (безнадлишкового коду) число інформаційних символів $m \geq \log_2 M$.

При введенні надлишкових елементів отримаємо n -елементні кодові слова ($n = m + k$), що зменшує швидкість передавання до величини

$$R = \frac{n-m}{n}.$$

Якщо час передачі T задано, то збільшення елементності кодових слів вимагає збільшення швидкості передавання (за умови $B < \frac{1}{\Delta F}$), що пов'язано зі зменшенням питомої енергії. У результаті n_2^c зменшується, що приводить до збільшення ймовірності помилки.

Таким чином, збільшення надлишковості і збільшення швидкості модуляції впливають на вірність зв'язку.

Установимо залежність імовірності помилкового прийому багатозначних (n -елементних) символів від параметра

$$Q_c^2 = \frac{P_c}{B},$$

що характеризує витрату питомої енергії на одну двійкову одиницю інформації. Роль параметра Q_c^2 особливо важлива в системах зв'язку, де обсяг інформації великий, а енергія мала. Це характерно для систем передачі параметрів космічних систем. Для ілюстрації впливу параметра Q_c^2 на вірність зв'язку розглянемо два способи передачі повідомлень.

При першому способі, який називається *посимвольним* (поелементним), сигнальні конструкції представляють m -значні двійкові кодові слова з енергією $mQ_c^2 = BT_m Q_c^2$ й передаються елемент за елементом. При другому способі, який називається передачею укрупненими сигналами, алфавіт сигналів має 2^m ортогональних векторів з питомою енергією $Q_y^2 = mQ_c^2$.

У цьому випадку передача j -го символу повідомлення оцінюються в момент закінчення формування цього повідомлення.

Для конкретності виберемо повідомлення, що відповідає кодовому слову 1011. Представивши ортогональні сигнали виразом

$$U_c(t) = \sum_{j=1}^k \sqrt{Q_c^2} \phi_j(t - jt_0) \quad (j = 1, 2, m),$$

де $\phi_j(t)$ – нормована за енергією координатна функція, що являє собою імпульс тривалістю T_0 з одиничною енергією; $m = BT_k$ – число двійкових символів у кодовім слові тривалістю T_k .

Розмістимо всі $M = 2^m$ символів у вершинах 2^m гіперкуба.

Тоді ймовірність хоча б однієї помилки

$$p_{0k} = 1 - (1 - P_c)^k = 1 - (1 - P_c)^{BT_k},$$

де

$$P_c = \Phi(\sqrt{h_c^2}) = \Phi\left(\sqrt{\frac{P_c}{v_s^2 B}}\right); \Phi(k) - \text{інтеграл імовірності.}$$

Як впливає з наведеного виразу, ймовірність помилки зростає зі збільшенням тривалості повідомлення: за фіксованого T_k , ймовірність P_e може бути зроблена малою тільки шляхом збільшення питомої енергії елементарного символу, тобто середньої потужності сигналу або за рахунок зниження швидкості передавання інформації B .

3.1.5. Статистичні параметри БЧМ

Більшість існуючих систем з ЧМ використовують двійковий код. Поряд із цим знаходять застосування багатопозиційна частотна модуляція (БЧМ) з основою частотного коду $a > 2$.

Канали БЧМ за деяких технічних показників кращі за двійкові канали з ЧМ, наприклад, спотворення тривалості посилок через багатопроменеве поширення радіохвиль є серйозною завадою для підвищення швидкості передавання по КВ каналах: у тих випадках, коли абсолютна величина цих спотворень перевищує виправляючу здатність приймального пристрою – настає невірне приймання. Для боротьби з цим явищем необхідно збільшувати тривалість посилки, однак за двійкової ЧМ це пов'язане зі зниженням швидкості передавання інформації v_i .

Наприклад, перехід від двійкової ЧМ до БЧМ із $a = 32$ дозволить збільшити тривалість посилок у 5 разів при збереженні тієї самої швидкості B_i . Якщо ж, навпаки, зберегти колишню величину t_0 , то в 5 разів необхідно збільшити B .

Подовження посилок за постійної швидкості передавання інформації $v_i = \text{const}$ призводить до більш надійної їхньої реєстрації. Дійсно, якщо припустити, що спотворення тривалості посилок підкоряються нормальному закону розподілу, то ймовірність помилкової реєстрації посилок при виправляючій здатності $\mu_n = \delta t_{0\text{макс}}$ характеризується виразом

$$P_0 = \int_{\mu_n t_0}^{\infty} \omega(T) dT = 1 - V\left(\frac{\mu_n t_0}{\sigma_T}\right),$$

де $V(z)$ – функція Лапласа; σ_T – середньоквадратичне значення зміни тривалості посилки.

Нехай, наприклад, умови в каналі такі, що ймовірність $P_0 = 0,1$; це відповідає значенню $\frac{\mu_n t_0}{\sigma_T} = 1,64$. Якщо тепер посилку t_0 подовжити в 3 рази, то ймовірність $P_e = 1 - V(4,92) < 10^{-6}$, що свідчить про підвищення вірності приймання.

Смуга частот при БЧМ. Відстань сусідніх частот F_b при БЧМ у загальному вигляді визначається виразом

$$F_B = \frac{\zeta}{T_{ca}} = 2\zeta F_M, \quad (3.33)$$

де ζ – деякий коефіцієнт, що залежить від стабільності частоти; F_M – частота маніпуляції; T_{ca} – тривалість елементарної послідовності a -позиційного коду.

Відстань між максимальною й мінімальною частотами при БЧМ буде

$$F_{B \text{ макс}} = F_B (a - 1).$$

Це відповідає максимальній девіації частоти

$$F_{D \text{ макс}} = \zeta(a - 1)F_M$$

і сумарному індексу частотної маніпуляції

$$m_{ч \text{ макс}} = \frac{F_{D \text{ макс}}}{F_M} = \zeta(a - 1).$$

Тоді смуга частот при БЧМ визначається

$$\Delta f_a = \frac{1}{T_{ca}} \left[1 + \zeta(a - 1) + \sqrt{\zeta(a - 1)} \right]. \quad (3.34)$$

Порівняємо величину Δf_a зі смугою частот

$$\Delta f_2 = \frac{1}{T_{c2}} (1 + \zeta + \sqrt{\zeta}). \quad (3.35)$$

У зв'язку з тим, що

$$T_{ca} = T_{c2} \log_2 a.$$

Коефіцієнт розширення смуги

$$k_a = \frac{\Delta f_a}{\Delta f_2} = \frac{1 + \zeta(a - 1) + \sqrt{\zeta(a - 1)}}{(1 + \zeta + \sqrt{\zeta}) \log_2 a}. \quad (3.36)$$

Вираз подано графічно на рис. 3.6, на якому бачимо, що розширення смуги при переході від ЧМ до БЧМ порівняно невелике. Так, наприклад, при $\zeta = 2$ й $a = 32$ коефіцієнт $k_{32} \approx 3,2$.

Таке значне розширення смуги має місце тільки за високої стабільності частоти, коли смуга частот приймача визначається тривалістю елементарного імпульсу, у результаті чого звуження його спектра деякою мірою компенсує вплив збільшення числа частот.

За низької стабільності частоти смуга пропускання приймача меншою мірою залежить від величини T_c і приблизно можна вважати, що $T_{ca} \approx T_{c2}$. При цьому коефіцієнт

$$k_a \approx \frac{1 + \zeta(a - 1) + \sqrt{\zeta(a - 1)}}{1 + \zeta + \sqrt{\zeta}} \quad (3.37)$$

і для розглянутого прикладу $k_8 \approx 4,2$ й $k_{32} \approx 16$.

Таким чином, БЧМ доцільно застосовувати в каналах з високою стабільністю частоти або з метою зменшення впливу крайових спотворень імпульсів. Найбільшу економію смуги частот при $\zeta = 1$ забезпечують трійкові системи БЧМ з $a = 3$, еквівалентні двійковим системам з ЧМ.

Структура сигналів БЧМ. За принципом побудови частотного коду методи формування сигналів БЧМ можна поділити на дві групи: з *послідовним* і *паралельним кодуванням*. У першому випадку кодова комбінація утвориться послідовним у часі набором посилок різних частот, і по лінії зв'язку в кожний момент часу передаються коливання тільки однієї частоти (мелодія). У другому випадку кодові комбінації утворюються набором посилок різних частот, переданих по лінії зв'язку одночасно. Можливі два типи такої системи. На рис. 3.7 подано принцип побудови сигналу, який характеризується тим, що в кожний даний момент часу може передаватись $r - 1, 2, \dots, a$ коливань різних частот системи типу «Акорд». Характеристики такої системи подібні характеристикам звичайної системи з амплітудною модуляцією. У системі «Акорд-ЧМ» (рис. 3.7, б) кількість випромінюваних частот для кожного знака (літери або цифри) постійна. Це досягається тим, що весь алфавіт m частот можна поділити на n груп по k частот у групі ($m = kn$) і передавати щоразу по одній частоті з кожної групи. Очевидно, що в межах будь-якої групи частот приймання може здійснюватися аналогічно k -позиційній системі. Тому система БЧМ є окремим випадком системи «Акорд-ЧМ» при $k = 1$.

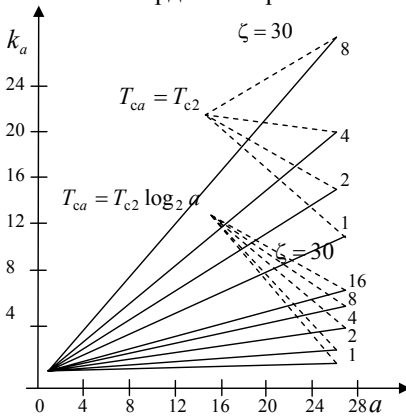


Рисунок 3.6 – Смуга частот при БЧМ

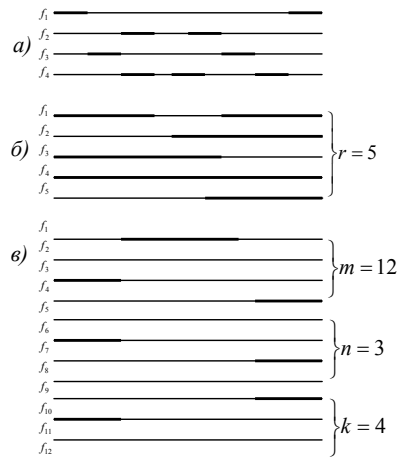


Рисунок 3.7 – Структура сигналів БЧМ:
 а – «Мелодія», б – «Акорд-АМ»,
 в – «Акорд-ЧМ»

Для такої системи смуга частот, займана сигналом при передаванні інформації із заданою швидкістю, буде різною для кожної системи, тому що

$$B_T = \frac{H(X)}{T_c} = B_T H(X),$$

де $H(X)$ – ентропія алфавіту, переданого за одиницю часу. Ємність алфавіту джерела

$$M = 2^{H(X)} = 2^{\nu_d T_c},$$

а смуга вибраних частот

$$\Delta f = \frac{M}{T_c} = \nu_T 2^{\nu_d T_c}. \quad (3.38)$$

Для системи «Акорд-АМ» ентропія й смуга частот будуть

$$H(X) = \log_2 2^m = m; \quad \Delta f = H(X). \quad (3.39)$$

Нарешті, для системи «Акорд-ЧМ» ентропія $H(X) = n \log_2 k$, звідки алфавіт джерела

$$M = 2^{\frac{\nu_d T_c}{n}},$$

а смуга частот

$$\Delta f = \frac{m n}{T_c} = \nu_T 2^{\frac{\nu_d T_c}{n}}. \quad (3.40)$$

Розширення смуги частот при зростанні B супроводжується зростанням потужності адаптивних флуктуаційних завод у смузі пропускання приймача. При заводах з однорідним енергетичним спектром це може бути скомпенсоване підвищенням потужності передавача, пропорційним розширенню смуги частот. Потрібно визначити параметри каналу, в якому для передавання інформації зі швидкістю $B_{i2} > B_{i1}$ потрібне найменше збільшення потужності передавача. У такій постановці зазначена проблема вперше була вирішена Л.М. Фінком, який довів, що в однопроменевих радіоканалах, характерних для систем «Мелодія» з основою коду $a=3$ за тривалості елементарної посилки

$$T_c = \frac{1}{\nu_d \ln 2} = \frac{1,443}{\nu_d}.$$

3.1.6. Ймовірнісні параметри БЧМ

Загальний метод аналізу заводостійкості каналів БЧМ ґрунтується на поданні їх розгалуженим ланцюгом (рис. 3.8), де кожний частотний тракт на передавальному й на приймальному кінцях відповідає одному сигналу m -позиційного коду. Підкреслимо, що таке графічне подання справедливе для будь-якого способу модуляції ортогональних сигналів – ДЧМ, БЧМ тощо.

Загальною умовою правильної реєстрації сигналів при завадах довільного типу є перевищення амплітуди сумарного коливання сигналу й завади в робочому тракті над амплітудою завади в будь-який з $m - 1$ вільних трактів. Тоді вираз для ймовірності помилки буде



Рисунок 3.8 – Геометрична модель каналу БЧМ

$$P_{nm} = 1 - \sum_{k=1}^m P_k (1 - P_{nk}), \quad (3.41)$$

де P_k – апіорна ймовірність k -го сигналу; P_{nk} – ймовірність помилкового приймання сигналів у кожному із трактів, що залежить від перевищення сигналу h_c^2 , статистичної структури завади й числа трактів m . Ймовірність

$$P_{nk} = 1 - \int_{-\infty}^{\infty} \omega(U_{pk}) \left[\prod_{j=1}^{m-1} P(U_{zj} < U_{pk}) \right] dU_{pk}, \quad (3.42)$$

де $\omega(U_{pk})$ – густина розподілу ймовірності амплітуди результуючого (сумарного) коливання в k -му робочому тракті; $P(U_{zj} < U_{pk})$ – ймовірність того, що амплітуда завади U_{zj} в j -му холостому тракті менше амплітуди сумарного коливання в k -му робочому тракті.

Надалі будемо вважати, що всі сигнали рівноймовірні й мають однакову енергію, всі тракти ідентичні, а статистична структура завод у них однакова. В цих умовах ймовірність помилки

$$P_{nm} = P_{nk}, \quad (3.43)$$

тобто заводостійкість БЧМ кількісно характеризується ймовірністю помилкового визначення сигналу в кожному із трактів системи.

При некогерентному прийманні густина ймовірності амплітуди завади $\omega(U_3)$ в кожному тракті описується законом Релея. Тоді ймовірність

$$P(U_{zj} < U_{pk}) = \int_{-\infty}^{U_{pk}} \omega(U_3) dU_3 = 1 - e^{-\frac{U_{pk}^2}{2\sigma_3^2}} \quad (3.44)$$

Враховуючи, що розподіл ймовірності сумарного коливання $\omega(U_p)$ в кожному тракті описується узагальненим законом розподілу Релея, ймовірність помилки буде

$$P_{0m} = 1 - \int_{-\infty}^{\infty} \frac{U_p^2}{\sigma_3^2} e^{-\frac{U_p^2 + U_3^2}{2\sigma_3^2}} I_0 \left(\frac{U_p U_{c \text{ макс}}}{\sigma_3} \right) \left(1 - e^{-\frac{U_p^2}{2\sigma_3^2}} \right)^{m-1} dU_p.$$

Представивши модифіковану функцію Бесселя виразом

$$I_0(q_p q_c) = \sum_{l=0}^{\infty} \frac{(\sqrt{2h_c^2} q_p)^{2l}}{2^{2l} (l!)^2} \quad (3.45)$$

і застосувавши біноміальне розкладання

$$\left(1 - e^{-\frac{q_p^2}{2}}\right)^{m-1} = \sum_{l=0}^{m-1} (-1)^l \frac{(m-1)!}{l!(m-l-1)!} e^{-\frac{q_p^2}{2} l},$$

після перетворень отримаємо вираз для ймовірності помилки у системі БЧМ

$$P_{nm} = (m-1)! e^{-h_c^2} \sum_{k=1}^{m-1} \frac{(-1)^{k+1}}{(k+1)!(m-k-1)!} e^{-\frac{kh_c^2}{k+1}}. \quad (3.46)$$

Для випадку використання двох трактів отримаємо ймовірність

$$P_{02} = \frac{1}{2} e^{-\frac{h_c^2}{2}}, \quad (3.47)$$

що збігається з виразом для простих двійкових каналів ЧМ.

За великих значень h_c^2 можливо обмежитися тільки першими двома членами ряду (3.46), при цьому ймовірність

$$P_{0m} \approx \frac{m-1}{2} e^{-\frac{h_c^2}{2}}. \quad (3.48)$$

Завадостійкість когерентного БЧМ. Метод аналізу когерентного приймання сигналів БЧМ залишається колишнім з тією лише різницею, що необхідно враховувати тільки синфазну складову завади, розподілену за нормальним законом. Тому, опускаючи проміжні викладення, наведемо остаточний вираз для ймовірності помилки:

$$P_{nm} = 1 - \frac{1}{\sqrt{2\pi}\sigma_3} \int_{-\infty}^{\infty} e^{-\frac{q_3^2}{2}} \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{q_c + q_3} e^{-\frac{z^2}{2}} dz \right)^{m-1} dU_3. \quad (3.49)$$

В окремому випадку при $m = 2$ ймовірність

$$P_{02} = \Phi\left(\sqrt{h_c^2}\right),$$

що збігається з формулою для простих двійкових каналів ЧМ.

За великих значень h_c^2 формула (3.49) може бути замінена наближеним виразом

$$P_{nm} \approx \frac{m-1}{2} \Phi\left(\sqrt{h_c^2}\right). \quad (3.50)$$

Завадостійкість БЧМ при імпульсних і зосереджених завадах. Якщо ідеальна густина імпульсної завади однакова в усіх трактах БЧМ, то ймовірність помилки тотожно дорівнює (принаймні теоретично) ймовірності

помилки у двійкових каналах ЧМ. Практично завадостійкість БЧМ трохи менше внаслідок відхилення параметрів трактів (коефіцієнтів підсилення, ефективних смуг пропускання, форми частотних характеристик).

Завадостійкість до зосереджених завад залежить від закону розподілу ймовірності попадання завади в тракт системи БЧМ від типу уражених трактів (холості й діючі). Тому точний аналіз тут стає важким, а погіршення завадостійкості порівняно з двійковими каналами ЧМ більш помітним.

Вплив стабільності частоти на завадостійкість БЧМ. Оцінімо, як впливає стабільність частоти генератора на вірність зв'язку при некогерентному прийманні сигналів БЧМ і дії в каналі флуктуаційних завад. Позначимо через n_2 і n_m значності кодових комбінацій, а через P_{n_2} і P_{nm} – ймовірності спотворення елементарних символів при ЧМ і БЧМ.

Ймовірність спотворення n -значної кодової комбінації

$$P_n = 1 - (1 - P_e)^n \approx nP_e.$$

Тоді для ЧМ і БЧМ відповідно отримаємо

$$P_{n_2} \approx nP_{n_2}; \quad P_{nm} \approx n_m P_{nm}. \quad (3.51)$$

Враховуючи, що

$$n_m = \frac{n_2}{\log_2 m},$$

для величини відношення вірності зв'язку при БЧМ відносно ЧМ маємо

$$\varepsilon_{m2} = \frac{P_{nm}}{P_{n_2}} = \frac{P_{nm}}{P_{02} \log_2 m}. \quad (3.52)$$

Підставивши в (3.52) вирази (3.46) і (3.47), отримаємо

$$\varepsilon_{m2} = \frac{2e^{h_{c2}^2} (m-1)!}{\log_2 m} \sum_{k=1}^{m-1} \frac{(-1)^{k+1}}{(k+1)!(m-k+1)!} e^{-\frac{kh_{cm}^2}{k+1}}, \quad (3.53)$$

де h_{c2}^2, h_{cm}^2 – перевищення сигналів ЧМ і БЧМ над флуктуаційними завадами.

За низької стабільності частоти, коли $T_{c2} \approx T_{cm}$, можна вважати, що $h_{c2}^2 \approx h_{cm}^2$ й

$$\varepsilon_{m2} = \frac{2(m-1)!}{\log_2 m} \sum_{k=1}^{m-1} \frac{(-1)^{k+1}}{(k+1)!(m-k+1)!} e^{\frac{h_{c2}^2(1-k)}{2(1+k)}}. \quad (3.54)$$

За високої (ідеальної) стабільності частоти тривалості посилок при ЧМ і БЧМ пов'язані, тому смуга пропускання розділювальних фільтрів при БЧМ може бути звужена в $\log_2 m$ разів. У цьому випадку для h_{cm}^2 отримаємо

$$h_{cm}^2 = h_{c2}^2 \log_2 m. \quad (3.55)$$

При цьому

$$\varepsilon_{m2} = \frac{2(m-1)! \sum_{k=1}^{m-1} \frac{(-1)^{k+1}}{(k+1)!(m-k+1)!} \exp\left\{\frac{h_{c2}^2}{2} \left[\frac{1+k(1-\log_2 m)}{2(k+1)} \right]\right\}}{\log_2 m} \quad (3.56)$$

Формули (3.54) і (3.56) справедливі при виконанні рівностей (3.51), тобто за мінімальних імовірностей P_{n2} і P_{nm} або, інакше кажучи, за великих значень h_{c2}^2 . Вважаючи, що $h_{c2}^2 \gg 1$, у формулах (3.54) і (3.56) можна обмежитися числами з індексами $k=1$ і $k=2$. Тоді отримаємо:

– за низької стабільності частоти

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m} - \frac{(m-1)(m-2)}{3 \log_2 m} e^{-\frac{h_{c2}^2}{6}}; \quad (3.57)$$

– за високої (ідеальної) стабільності частоти генераторів

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m} \exp\left[\frac{h_{c2}^2}{2}(1-\log_2 m)\right] - \frac{(m-1)(m-2)}{3 \log_2 m} \exp\left[\frac{h_{c2}^2}{2}(1-1,33 \log_2 m)\right]. \quad (3.58)$$

Для орієнтовної оцінки величини ε_{m2} можна користуватися наближеними співвідношеннями:

– для низької стабільності частоти

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m}; \quad (3.59)$$

– для високої стабільності частоти

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m} \exp\left[\frac{h_{c2}^2}{2}(1-\log_2 m)\right]. \quad (3.60)$$

Вираз (3.59) подано графічно на рис. 3.9, а, з чого бачимо, що підвищення основи коду за низької стабільності частоти несуттєво погіршує вірність зв'язку при БЧМ порівняно з ЧМ. Так, наприклад, перехід до БЧМ з основою частотного коду $m=4$ і $m=8$ при перевищенні $h_{c2}^2=25$ призводить до зменшення ймовірності спотворення кодової комбінації відповідно в $5 \cdot 10^{-3}$ і $5 \cdot 10^{-5}$ разів.

Результати розрахунку за формулою (3.60) наведені на рис. 3.9, б.

Зменшення ймовірності помилки при підвищенні m еквівалентно до виграшу в необхідній середній потужності сигналу. Однак за кількісної оцінки величини виграшу необхідно враховувати вплив на ймовірність помилки двох протилежних факторів: з одного боку, вона зменшується зі зростанням перевищення сигналу відповідно до виразу (3.55), з іншого – вона зростає за рахунок збільшення числа частот пропорційного множника $\frac{m-1}{\log_2 m}$ у формулі (3.60). Вважаючи в цій формулі $P_{n2} = P_{nm}$, отримаємо

$$\frac{m-1}{\log_2 m} \exp\left(\frac{h_{c2}^2 - h_{cm}^2}{2}\right) = 1.$$

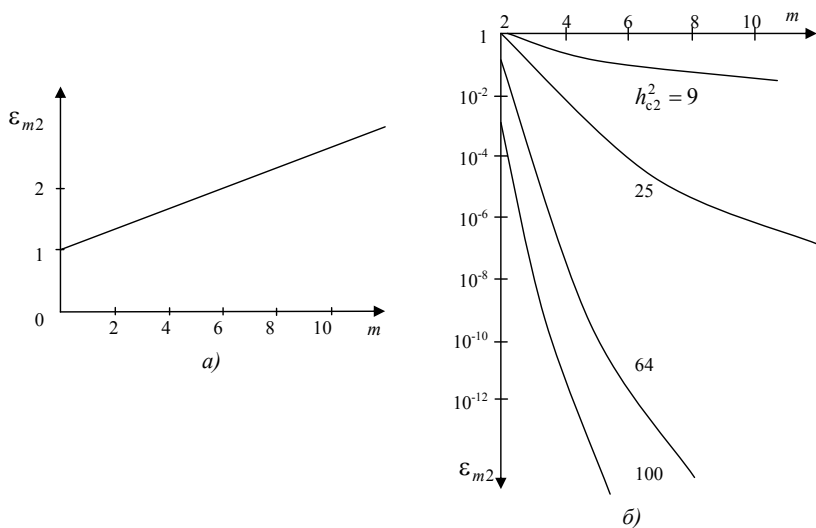


Рисунок 3.9 – Вплив основи коду БЧМ на відносну ймовірність помилки: *a* – низька стабільність частоти; *б* – висока стабільність частоти

Цей вираз визначає величину перевищення $h_{cm}^2 = h_{0m}^2$ при БЧМ, що компенсує вплив множника $\frac{m-1}{\log_2 m}$ на ймовірність помилки. У результаті виграш у середній потужності сигналу складе

$$\beta_P = \frac{h_{c2}^2}{h_{0m}^2} \log_2 m. \quad (3.61)$$

Результати розрахунку за формулою (3.61) наведені на рис. 3.10.

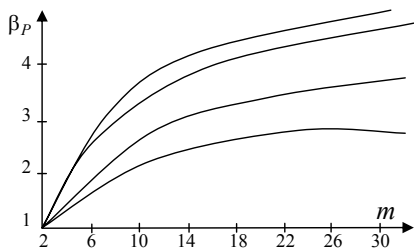


Рисунок 3.10 – Енергетичний виграш за БЧМ

Аналіз кривих показує, що за практичних прийнятних значень m і h_{c2}^2 величина $\beta_P \geq 2 \dots 3$.

Розглянемо тепер проміжний випадок, коли стабільність частоти така, що при подовженні посилок у $\log_2 m$ разів смуга пропускання може бути звужена в $\eta < \log_2 m$ ра-

зів. Тоді перевищення сигналу при БЧМ

$$h_{cm}^2 = \eta h_{c2}^2, \quad (3.62)$$

і вираз (3.53) набуде вигляду

$$\varepsilon_{m2} = \frac{2(m-1)! e^{\frac{h_{c2}^2}{2}}}{\log_2 m} \sum_{k=1}^{m-1} \frac{(-1)^{k+1}}{(k+1)!(m-k-1)!} \exp\left\{\frac{h_{c2}^2 [1+k(1-2\eta)]}{2(k+1)}\right\}. \quad (3.63)$$

Вважаючи $h_{c2}^2 \gg 1$ і можна обмежитися тільки числами з індексами $k=1$ і $k=2$. Тоді отримаємо

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m} \exp\left[\frac{h_{c2}^2(1-\eta)}{2}\right] - \frac{(m-1)(m-2)}{3 \log_2 m} \exp\left[\frac{h_{c2}^2(1-1,33\eta)}{2}\right]. \quad (3.64)$$

Для орієнтовної оцінки можна користуватися наближеним виразом

$$\varepsilon_{m2} \approx \frac{m-1}{\log_2 m} \exp\left[\frac{h_{c2}^2(1-\eta)}{2}\right]. \quad (3.65)$$

Неважко побачити, що формули (3.59) і (3.60) є окремими випадками виразу (3.65), з якого вони одержані за значень $\eta=1$ (низька стабільність частоти) і $\eta=\log_2 m$ (висока стабільність частоти).

Припустимо, що смуга пропускання розподіляючого фільтра

$$\Delta f_{\Phi} = \frac{1}{T_c} + f_n, \quad (3.66)$$

де величина Δf_n визначається нестабільністю частоти. Тоді будемо мати:

– для ЧМ

$$\Delta f_{\Phi 2} = \frac{1}{T_{c2}} + \Delta f_n = \frac{1}{T_{c2}} (1 + T_{c2} \Delta f_n); \quad (3.67)$$

– для БЧМ

$$\Delta f_{\Phi m} = \frac{1}{T_{cm}} + \Delta f_n = \frac{1}{T_{cm}} \left(\frac{1}{\log_2 m} + T_{c2} \Delta f_n \right). \quad (3.68)$$

Позначимо через

$$\alpha_0 = T_{c2} \Delta f_n = \Delta f_n T_{c2}. \quad (3.69)$$

Величина α_0 показує, у скільки разів абсолютна нестабільність частоти перевищує ширину спектра елементарної послідовності. Тоді

$$\eta = \frac{\Delta f_{\Phi 2}}{\Delta f_{\Phi m}} = \frac{(1 + \alpha_0) \log_2 m}{1 + \alpha_0 \log_2 m}, \quad (3.70)$$

а вираз (3.65) буде

$$\varepsilon_{m2} = \frac{m-1}{\log_2 m} \exp\left[\frac{h_{c2}^2}{2} \frac{1 - \log_2 m}{1 + \alpha_0 \log_2 m}\right]. \quad (3.71)$$

Результати розрахунку за формулою (3.71) для БЧМ з підставленням частотного коду $m = 4$ і $m = 8$ при $h_{c2}^2 = 25$ й $h_{c2}^2 = 100$ наведені на рис. 3.11.

Аналіз залежностей показує, що за високої стабільності частоти (параметр α_0 малий) збільшення m підвищує завадостійкість БЧМ порівняно з ЧМ, причому виграш у завадостійкості тим більше, чим значення m і h_{c2}^2 .

Зі зниженням стабільності частоти коливань вплив доданка Δf_n у формулах (3.67) і (3.68) зростає й, починаючи з деяких значень α_0 , виграш БЧМ у завадостійкості зі зростанням m зменшується. За деякого граничного значення α_0 величина $\epsilon_{m2} = 1$, що відповідає однаковій завадостійкості каналів ЧМ і БЧМ. За більшого значення α_0 ймовірність зв'язку за БЧМ стає гірше, ніж за ЧМ.

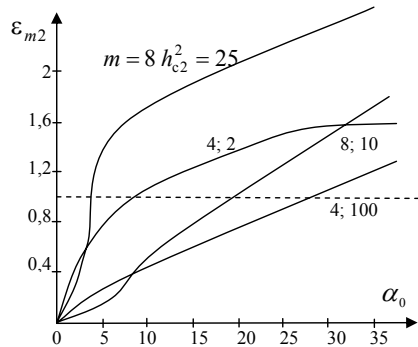


Рисунок 3.11 – Вплив стабільності частоти на вірність зв'язку за БЧМ

3.1.7. Параметричне кодування як метод збільшення алфавіту каналу

Висока вірність передавання та часові вимоги до затримки повідомлення є суперечними. Тому коди доцільно оцінювати узагальненими параметрами, наприклад, коефіцієнтом ефективності K_E

$$K_E = \xi_V \cdot \epsilon_{PB}, \quad (3.72)$$

де параметр ξ_V характеризує відносну швидкість передавання

$$\xi_V = \frac{m}{n}.$$

Параметр ϵ_{PB} характеризує вірність передавання і визначається через ймовірність помилкового приймання кодового слова P_{pk}

$$\xi_{PB} = -\log P_{pk}.$$

При використанні критерію еквівалентної ймовірності помилки P_e умова використання коректуючих кодів має вигляд:

$$P_{pk} \leq mP_e.$$

Для каналів з незалежними помилками при виправленні r -кратних помилок

$$P_{nk} = \sum_{r=l_0+1}^n C_n^r p_0^r (1-p_0)^{n-r}. \quad (3.72a)$$

Зрозуміло, що зі збільшенням кратності виправлених помилок зростає число надлишкових елементів k , що зменшує ϵ_v .

У каналах з урахуванням пакетів помилок для кодів, виправляючих пакети довжиною l_n – символів, нижня межа надлишкових елементів

$$k \geq l_n - 1 + \lceil \log_2(n+2-l_n) \rceil.$$

При визначенні ймовірності появи в кодовому слові помилок кратності t необхідно врахувати стан каналу

$$P_{nk}(t) = P_{k1}(t) + P_{k2}(t),$$

де $P_{k1}(t)$, $P_{k2}(t)$ – ймовірності появи помилок кратності $t_i \geq r_i + 1$ за наявності і відсутності пакетів помилок.

Розглянемо два приклади, які виникають на практиці.

Приклад 6. Параметри надлишкового коду узгоджені з параметрами каналу.

Якщо в каналі помилки не групуються (канал з незалежними помилками), то ймовірність помилкового приймання визначається виразом (3.72).

Якщо використовується канал з групуванням помилок ($\alpha \neq 0$), то ймовірність помилок в кодовім слові визначається

$$P_{k1}(l_n, r) = \frac{2p_{\text{пн}}}{(2+l_{\text{пн}})^2} \sum_{l_n=r+1}^n (n-l_n+1) \left(1 - \frac{2p_{\text{пн}}}{2+l_{\text{пн}}}\right)^{n-l_n} \left(1 - \frac{1}{2+l_{\text{пн}}}\right)^{l_n-1}, \quad (3.73)$$

де $l_{\text{пн}}$ – середня довжина пакета, $p_{\text{пн}}$ – ймовірність помилкового приймання елемента в «поганому» стані каналу.

Приклад 7. Параметри коду не узгоджені з характеристиками потоку помилок.

Якщо в каналі з незалежними помилками використовується код, виправляючий помилки довжиною l_n , вагою r , то ймовірність помилкового кодового слова

$$P_{nk}(l_n, r) = 1 - (1-p_0)^n - \sum_{r=1}^n C_{l_n}^r p_{\text{пн}}^r (1-p_{\text{пн}})^{n-r}. \quad (3.74)$$

Якщо в каналі з групуванням використовується код, який виправляє незалежні помилки, то

$$P_{nk}(l_n, r) = P_{k1}(l_n, r) \sum_{r=r_0+1}^{l_n} C_{l_n-2}^{r-2}. \quad (3.75)$$

Якщо в каналі з групуванням помилок використовується код, випра-вляючий незалежні помилки кратності r_0 і відомий коефіцієнт кореляції помилок ρ на інтервалі пакета, то

$$P_{nk}(l_n, r) = P_{k1}(l_n, r) \sum_{r=r_0+1}^n C_{l_n-2}^{r-2} \rho_0^{l_n-r} (1-\rho_0)^n. \quad (3.76)$$

При параметричному кодуванні використовується більша кількість різних каналних сигналів за фіксованої довжини n -елементного коду.

На рис. 3.12 показані залежності $P_{nk} = f(p_0)$ і $K_E = f(\xi_v)$ для узгоджених і неузгоджених кодів з відповідними параметрами каналу і побудовані згідно з виразами (3.73), (3.75) та (3.72).

Із побудованих залежностей можна зробити висновки:

- для узгоджених з потоком помилок кодів вплив ξ_v на ймовірність вірного приймання більше ніж для неузгоджених кодів;
- кращими властивостями володіють коди більшої довжини (n);
- узгоджені коди для параметра $K_{ck} = f(P_0, \xi_v)$ мають екстремум.

Таким чином ефективність коду залежить від його узгодженості з характеристиками потоку помилок. У каналах зі змінними параметрами потоку помилок доцільно вести контроль їх і проводити адаптацію методу передачі. Одним із методів адаптації – є *параметричне кодування*.

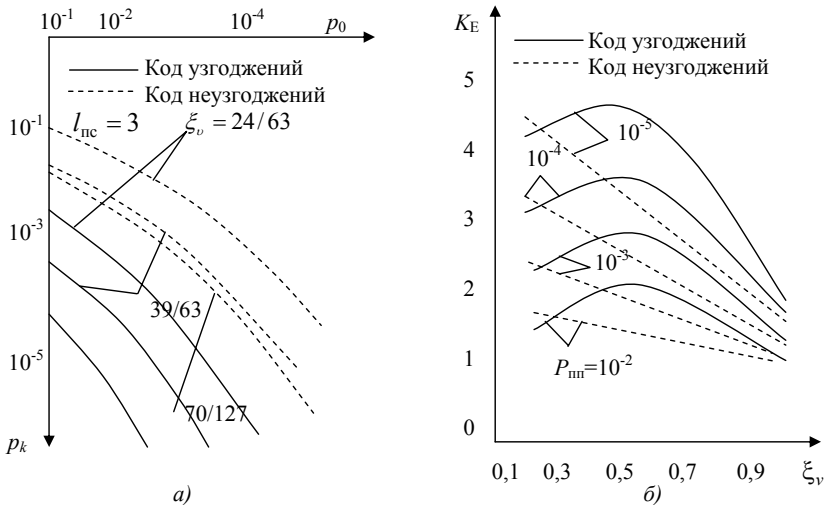


Рисунок 3.12 – Характеристики завадостійкості (а) та ефективності (б) кодів у каналах з групуванням помилок при $\xi_0 = \varnothing ar$

Приклад 8. Нехай при передаванні двійкових повідомлень використовується $a = 3$. Тоді при первинному кодуванні «1» відповідає a_1 , а символу «0» сигнал a_2 або a_3 . Домовимось, що сигналом a_2 нуль кодується в тому випадку, коли сигналом S_2 (тобто нулем) починається повідомлення, або якщо перед даним S_2 передавалось парне число одиниць. Тоді, якщо $S \rightarrow 0101011011001$ – то в канал передається $x \rightarrow a_2 a_1 a_3 a_1 a_3 a_1 a_2 a_1 a_2$. Введені таким чином кореляційні зв'язки дозволяють виявляти помилки за меншої надлишковості. Для збільшення алфавіту каналу доцільне збільшення числа координат n -вимірного вектора.

Перетворення сигналів за рахунок зміни системи координат є одним зі способів завадостійкого кодування і забезпечує зменшення впливу імпульсних завад у каналах зв'язку без погіршення їх стійкості до зосереджених і флукуаційних завад.

Перерозподіл енергії зосереджених завад. Двійкові n -значні сигнали утворюють безліч 2^n векторів, кінці яких знаходяться на вершинах n -вимірного гіперкуба. Области розв'язання (відповідно області сигналів) визначаються розбиттям усього простору $(n-1)$ -вимірними поверхнями, паралельними координатним осям n -вимірного простору.

Одиночну адитивну заваду можна подати вектором U_3 , який виходить з вершини гіперкуба, що відповідає сигналу X_{cv} паралельно одній з ортогональних осей простору. За двійкових сигналів, що мають значення ± 1 , відстань між сусідніми вершинами гіперкуба $d = 2$. Тому помилка станеться лише при довжині вектора завади $\|U_3\| = \sqrt{Q^2} > 1$, коли кінець сумарного вектора $X_{cv} + U_3$ виявиться у власній області сигналу X_{cv} (рис. 3.13).

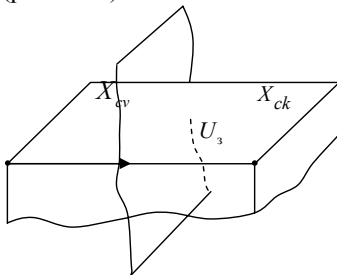


Рисунок 3.13 – Принцип обертального перетворення сигналів

Очевидно, що енергія імпульсної завади може бути невеликою. Ймовірність помилки можна знизити, збільшуючи енергію сигналу Q^2 , тобто кодову відстань d_{cv} між кодограмами X_{cv} і X_{ck} . Проте така міра у ряді випадків може виявитися недостатньо ефективною через велику інтенсивність завад або за обмеженої потужності переданих сигналів.

Повернемо всю координатну систему відносно її центра. Оскільки вектор U_3 паралельний одній з осей, то він також повернеться відносно точки X_{cv} . Зро-

зуміло, що при розміщенні U_3 і радіуса гіперсфери довжина вектора U_3 може збільшитися, не виключаючи помилки. Таке розміщення координат називатимемо *оптимальним*. Помилка при цьому станеться лише тоді, коли

$$\|U_3\| = \sqrt{Q_3^2} > \sqrt{Q_c^2} = \sqrt{n}, \quad (3.77)$$

тобто при перевищенні енергії завади над енергією сигналу.

Одиночну імпульсну заваду до перетворення можна подати n -рядним вектором вигляду $U_n = 00u_{n3}0\dots 0$. Після оптимального повороту вектор завади буде $U_{zn} = u_{zn1}, u_{zn2}, \dots, u_{znn}$. Аналітично таке перетворення можна виконати, помноживши первинний сигнал X_c на квадратну ортогональну матрицю

$$A_A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}. \quad (3.78)$$

Дійсно, норма вектора $\|U_3\|$ при обертанні не змінюється, тому

$$\|U_{zn}\| = \sqrt{\sum_{i=1}^n u_{zni}^2} = \|U_3\|.$$

Звідки

$$u_{zni} = \frac{u_{3i}}{\sqrt{n}}.$$

Такі матриці виходять з матриць Адамара – квадратних матриць з елементами ± 1 і ортогональними рядками – шляхом множення їх на $\frac{1}{\sqrt{n}}$.

Матриці Адамара існують для $n \geq 2$, при чому $n = 2^z$ повинна виконуватися умова $z = 2\xi$, де $\xi = 1, 2, 3, \dots$. Наприклад, при $z = 4$ матриці Адамара і обертальна мають вигляд

$$A_A = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{vmatrix}; \quad A_o = \begin{vmatrix} 0,5 & 0,5 & 0,5 & 0,5 \\ 0,5 & -0,5 & 0,5 & -0,5 \\ 0,5 & -0,5 & -0,5 & 0,5 \\ 0,5 & 0,5 & -0,5 & -0,5 \end{vmatrix}. \quad (3.79)$$

Приклад 9. Для оптимального повороту системи координат розмір матриці має бути $n = 4\xi$, $\xi = 1, 2, 3, \dots$. Якщо значність первинного сигналу $n \neq 4\xi$, то слід використовувати ортогональні матриці, елементи яких якомога менше відрізнялися б від оптимального значення $\frac{1}{\sqrt{n}}$.

$$A_0 = \begin{vmatrix} \frac{2-n}{n} & \frac{2}{n} & \frac{2}{n} & \dots & \frac{2}{n} \\ \frac{2}{n} & \frac{2-n}{n} & \frac{2}{n} & \dots & \frac{2}{n} \\ \frac{2}{n} & \frac{2}{n} & \frac{2}{n} & \dots & \frac{2-n}{n} \end{vmatrix}. \quad (3.79a)$$

Поворот системи координат – є збільшення надлишковості кодового простору. Завадостійкість коду може зростати при збільшенні його значності n і збільшенні основи m . За обертального перетворення значення n і Q_c^2 не змінюються, і збільшення завадостійкості досягається за рахунок підвищення a . Дійсно, помноживши первинний сигнал X на обертальну матрицю A_0 , отримаємо закодований сигнал

$$X_n = XA_n = x_{n1}, x_{n2}, \dots, x_{nm},$$

де символ

$$x_{ni} = \sum_{j=1}^n x_j a_{ij}.$$

Таким чином, новий алфавіт коду a_n визначається безліччю значень $\{x_n\}$ і в загальному випадку $a_n = f(a, n)$.

За двійкових символів ± 1 значення $x_{nj \text{ макс}}$ можливо отримати, коли символи сигналу X збігаються або протилежні за знаком до елементів стовпців матриці A_m , і складає

$$x_{mj \text{ макс}} = \pm \sqrt{n}.$$

При незбігу знаків одного або $n-1$ елементів матриці

$$x_{nj} = \pm \frac{n-2}{\sqrt{n}}.$$

Таким чином, символи алфавіту мають значення

$$0; \pm \frac{2}{\sqrt{n}}; \pm \frac{4}{\sqrt{n}}; \dots; \pm \frac{n-2}{\sqrt{n}}; \pm \sqrt{n} \quad (3.80)$$

і об'єм алфавіту $m_b = n + 1$.

Коефіцієнт надлишковості за обертального кодування

$$R_n = 1 - \frac{\log_2 2^n}{\log_2 (n+1)^n} = 1 - \frac{1}{\log_2 (n+1)}.$$

Таким чином, зі збільшенням n надлишковість обертального кодування зростає.

Надлишковість повинна вводитися у сигнали раціональним способом для боротьби з найбільш імовірними завадами. Тому для каналів з адитив-

ними флуктуаційними й імпульсними завадами доцільне двоступінчатє кодування – шляхом обертального перетворення кодів з надлишковістю. У цьому випадку коефіцієнт

$$R_n = 1 - \frac{\log_2 2^m}{\log_2 (n_n + 1)^{n_n}} = 1 - \frac{m}{n_n \log_2 (n_n + 1)},$$

де m – значність первинного сигналу; n_n – значність коду з надлишковістю. Очевидно, що для оптимального обертального перетворення необхідно, щоб $n_n = 4\xi$, де $\xi = 1, 2, 3, \dots$

Декодування за обертального перетворення. Для формування вихідного сигналу X прийняте коливання $Z = X \oplus U$ необхідно піддати додатковому обертальному перетворенню шляхом множення Z на зворотну матрицю A_0^{-1} . Через ортогональність матриць та їхньої структури $A_0^{-1} = A_0$. Таким чином, послідовність операцій в каналі зв'язку має вигляд

$$X \rightarrow XA_0 \rightarrow X_0 \rightarrow X_0 \oplus U_3 \rightarrow Z \rightarrow ZA_0^{-1} \rightarrow XA_0 A_0 + U_0 A_0 \rightarrow X + U_3 A_0.$$

У результаті отримуємо початковий сигнал X і перетворену імпульсну заваду $U_{30} = U_3 A_0$. Вектор цієї завади спроектований на всі координатні осі, тобто завада рівномірно «розтягується» по всьому інтервалу сигналу з амплітудою в \sqrt{n} разів меншою, ніж до перетворення.

Алфавіт сигналів (3.80) визначає раціональні способи модуляції у системах зв'язку з обертальним перетворенням – АМ з біполярними сигналами або різні вектори за фазової модуляції.

Завадостійкість обертального кодування. Імпульсні завади є випадковим процесом з законом розподілу, відмінним від нормального. Труднощі аналізу завадостійкості посилюються тим, що при обертальному перетворенні спотворення кодових символів за числа помилок $r > 1$ – події завжди залежні і необхідно шукати багатовимірну функцію розподілу не гауссівських випадкових функцій. Таке завдання в загальному вигляді не вирішується. Відомі наближені аналітичні вирази для оцінки вірності зв'язку за обертального перетворення у разі дії адитивних флуктуаційних й імпульсних завад.

Усі імпульсні завади можна об'єднати в дві групи:

- амплітуда і тривалість імпульсів завади постійні або розподілені рівномірно (цей випадок відповідає завадам малої потужності);
- амплітуда і тривалість імпульсів завади розподілені за експоненціальним законом $w(y) = \alpha e^{-\alpha y}$ (цей випадок відповідає на практиці завадам великої потужності).

В обох випадках розподіл числа імпульсів завад N_3 підлягає закону Пуассона:

$$p(N_3) = \frac{N_{30}^{N_3}}{N_3!} e^{-N_{30}},$$

де N_{30} – середнє число імпульсів завад в одиницю часу.

Аналіз показує, що відмінність імовірнісних характеристик параметрів імпульсної завади чинить незначний вплив на вірність зв'язку. Проте завади другого типу все ж таки небезпечніші, й оцінку ймовірності помилки при їх дії можна вважати граничною.

Для ймовірності спотворення кодових слів з ФМ за одночасної дії адитивних флуктуаційних й імпульсних завад для випадку, коли їхня сума описується нормальним випадковим процесом, мають такий вигляд.

1. Прості коди

$$P_{\text{кп}} = P_{\text{п}} = 1 - (1 - P_{\Sigma})(1 - P_3)^n, \quad (3.81)$$

де P_{Σ} – ймовірність спотворення одиничного символу за одночасної дії шумів та імпульсних завад і одних тільки шумів описується

$$P_{\Sigma} = \frac{1}{2} \left[1 - F(\sqrt{2h_{\text{cp}}^2}) \right]^n; \quad P_3 = \frac{1}{2} \left[1 - F(\sqrt{2h_c^2}) \right], \quad (3.81a)$$

а перевищення сигналу над шумами і над сумою шумів та імпульсних завад характеризується.

$$h_c^2 = \frac{Q_c^2}{v_3^2}; \quad h_{\text{cp}}^2 = \frac{Q_c^2}{v_i^2 + v_3^2}. \quad (3.82)$$

2. Надлишкові (n, m) -коди, що виправляють одиничні помилки:

$$P_{n,m}^{(1)} = 1 - \left[\begin{aligned} &(1 - P_{\Sigma})(1 - P_3) + P_{\Sigma}(1 - P_3) + \\ &+ (k - 1)P_{\Sigma}(1 - P_{\Sigma})(1 - P_3)^{k-2} \end{aligned} \right], \quad (3.82a)$$

де значення P_{Σ} і P_3 визначаються формулою (3.81a) відповідно, а перевищення сигналу

$$h_c^2 = \frac{n Q_c^2}{k v_3^2}; \quad h_{\text{cp}}^2 = \frac{n}{k} \left(\frac{Q_c^2}{v_i^2 + v_3^2} \right). \quad (3.82б)$$

3. Обертальне перетворення простого коду:

$$P_{\text{пк}}^0 = 1 - (1 - P_{\Sigma})^n, \quad (3.82в)$$

де значення P_{Σ} і h_{cp}^2 визначаються за формулами (3.81a) і (3.82).

4. Обертальне перетворення (n, m) -кодів, що виправляють одиничні помилки:

$$P_{n,m}^0 = 1 - \left[(1 - P_{\Sigma})^m + mP_{\Sigma}(1 - P_3)^{m-1} \right], \quad (3.82г)$$

де ймовірність

$$P_{\Sigma} = \frac{1}{2} \left[1 - F(\sqrt{2h_{cp}^2}) \right],$$

а перевищення сигналу

$$h_{cp}^2 = \frac{n}{m} \cdot \frac{Q_c^2}{v_3^2 + \frac{v_i^2}{m}}$$

Приклад 10. За аналітичними виразами (3.81...3.82г) побудувати залежності $P_{n,m}$, $P_{пк}$ як функції $f(h^2, n)$.

На рис. 3.14 зображені криві залежності

$$P_{пк} = f\left(h_c^2, n, \frac{v_i^2}{v_3^2}\right)$$

для різних способів кодування. З рисунка видно, що імпульсні завади сильно знижують вірність зв'язку, а обертальне перетворення підвищує стійкість сигналів до імпульсних завад. Найбільша завадостійкість забезпечується за обертального перетворення для кодів з надлишковістю.

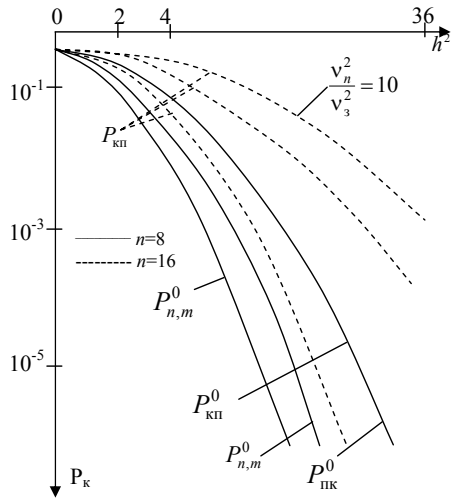


Рисунок 3.14 – Характеристики завадостійкості за обертального перетворення сигналів для $n_1 = 8, n_2 = 16$

3.1.8. Порівняння посимвольного приймання кодівих слів та приймання сигналів у цілому

Приймання сигналів у цілому. Розглянемо детальніше алгоритм кодування на прийомі за умови, коли як параметр η_k може безпосередньо використовуватися вихідна напруга демодулятора. Як показано в п. 3.1.1, коли ця напруга підлягає закону розподілу експоненціального типу, наприклад, нормальному, то функції правдоподібності мають вигляд

$$L_{nk} = \frac{1}{\sqrt{2\pi\sigma_3}} e^{-\frac{(y_k - \bar{y})^2}{2\sigma_3^2}}; \quad L_{ok} = \frac{1}{\sqrt{2\pi\sigma_3}} e^{-\frac{(y_k - \bar{y})^2}{2\sigma_3^2}} \quad (3.83a)$$

і параметр

$$|\eta_k| = \frac{2y_k \bar{y}}{\sigma_3^2} \log e,$$

де \bar{y} – середнє значення сигналу символу. Опустивши незалежні від номера позиції кодового слова величини, отримаємо правило розв'язання

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k. \quad (3.836)$$

У приймальному пристрої завжди існує дві вирішальні схеми: ВС1 – виносить рішення про приймання конкретного елемента коду (посилки) і вирішальна схема ВС2, включена після схеми ВС1 і є власне декодуючим пристроєм. Ця схема помножує параметр η_k (або y_k) на значення k -го символу кодограми і підсумовує добутки за всіма її позиціями. Подібні операції виконуються для кожного з M кодових слів, після чого виноситься рішення про реєстрацію тієї з них, для якої обчислена сума є найбільшою.

Вихідна напруга демодулятора передбачається тут у межах тривалості символу неперервною функцією часу, що приймає будь-які значення в діапазоні свого вимірювання. При цьому використовується вся наявна інформація про переданий сигнал, що забезпечує максимальну завадостійкість. У літературі подібний спосіб приймання дискретних сигналів дістав назву *приймання в цілому*. Технічне використання цього методу обмежене, що пояснюється двома причинами. По-перше, декодуючий пристрій повинен містити в своїй пам'яті $M = 2^m$ кодових слів, тобто об'єм пам'яті і число операцій за декодуванням різко зростають з довжиною повідомлення.

Приклад 11. Якщо швидкість передавання інформації $C = 5 \cdot 10^{-3}$ дв. од/с, швидкість телеграфування $B = 50$ Бод, довжина кодового блока $n = 100$, то обсяг обчислень у розв'язувальній схемі складе

$$n 2^{\frac{C}{B}} = 10^2 \cdot 2^{100} \approx 10^{32}$$

операцій, що вимагає навіть за низької швидкості величезної швидкодії елементів. По-друге, декодуючий пристрій повинен оперувати з аналоговими величинами, що ускладнює його схемне розв'язання.

Посимвольне приймання сигналів. Складність реалізації приймання в цілому призвела до того, що в даний час переважного розповсюдження набув *посимвольний метод приймання* дискретних сигналів. За цим методом на кожній позиції кодового слова формується еталонний символ, знак якого відповідає знаку вихідної напруги демодулятора. Потім кодограма, складена з таких еталонних символів, піддається обробленню у декодуючому пристрої з метою виправлення можливих помилок.

У літературі зустрічаються різні пояснення відмінності між вказаними методами приймання сигналів. Найбільш поширене трактування, за-

пропоноване Л.М.Фінком. Згідно з цим трактуванням приймальний пристрій у разі приймання сигналів у цілому містить лише одну розв'язувальну схему, яка відразу, без проміжних етапів, ототожнює прийнятий сигнал з однією із можливих кодограм. При посимвольному прийманні приймальний пристрій містить дві розв'язувальні схеми.

У зв'язку з цим зупинимось детальніше на кожному методі. При посимвольному прийманні символи на кожній позиції кодограми можуть мати два значення: $y_k = \pm 1$. За відсутності помилок символи $x_{v,k}$ і y_k збігаються, а функція правдоподібності для k -ї позиції кодограми буде

$$\left[L_{X_v}(y_k) \right]_{\text{пр}} = q_0, \quad (3.83\text{в})$$

де q_0 – ймовірність правильного приймання символу ($q_0 = 1 - P_0$). У разі спотворень символи $x_{v,k}$ і y_k мають протилежні знаки, а функція правдоподібності

$$\left[L_{X_v}(y_k) \right]_{\text{пом}} = p_0 = 1 - q_0, \quad (3.84)$$

де p_0 – ймовірність спотворення символу. Тоді в загальному вигляді можна записати

$$L_{X_v}(y_k) = p_0 \frac{(x_{v,k} - y_k)^2}{4} + q_0 \frac{(x_{v,k} + y_k)^2}{4}. \quad (3.85)$$

Після відповідних перетворень з урахуванням формул (3.83в ... 3.85) отримаємо оптимальний алгоритм декодування за посимвольного приймання

$$\sum_{k=1}^n x_{r,k} y_k > \sum_{k=1}^n x_{l,k} y_k. \quad (3.86)$$

Порівняння виразів (3.82б) і (3.86) показує, що оптимальні алгоритми декодування для обох способів приймання зовні повністю збігаються. Відмінність між ними полягає лише в характері величини y_k . При прийманні в цілому y_k – неперервна функція часу і несе інформацію як про знак, так і про амплітуду сигналу на виході демодулятора. За символьного приймання y_k – дискретна величина, інформація про амплітуду сигналу втрачається і використовуються відомості лише про його знак. Звідси випливає, що посимвольне приймання не оптимальне і поступається за завданістю приймання в цілому.

Таким чином, приймальний пристрій дискретних сигналів у будь-якому випадку містить дві розв'язувальні схеми: РС1 визначає значення символу на кожній позиції кодового слова, а РС2 ототожнює прийнятий

сигнал з однією із можливих кодових конструкцій. Вся відмінність приймання в цілому від посимвольного приймання полягає в точності роботи схеми РС1. У першому випадку значення сигналу визначається з нескінченно високою точністю, в другому – з точністю тільки до знаку.

Оптимальний алгоритм декодування за посимвольного приймання (3.86) можливо подати в іншому вигляді. Дійсно, якщо при передаванні кодограми X_v не відбулося спотворень, то сума

$$\sum_{k=1}^n x_{r,k} y_k = n, \quad (3.87)$$

якщо ж спотворилося $d_{v,y}$ символів, то

$$\sum_{k=1}^n x_{r,k} y_k = n - 2d_{v,y}, \quad (3.88)$$

де $d_{v,y}$ – відстань між кодограмами X_v і Y . Підставивши суму (3.88) в (3.86), отримаємо відоме правило ототожнення прийнятої кодограми з найближчою до неї за Хеммінгом:

$$d_{r,y} < d_{l,y}. \quad (3.89)$$

Це правило досить просто реалізується в декодуючих пристроях, що діють за принципом виправлення помилок, що і зумовило переважне розповсюдження методу посимвольного приймання.

3.1.9. Питання та задачі для самоперевірки

1. Для табл. 3.1 визначте елементність бінарного коду (m), знаючи значення r .

2. Для табл. 3.1 порівняйте потужність простору бінарних сигнальних конструкцій з потужностями просторів з $\rho = 1,33$ і $\rho = 2$.

3. Для табл. 3.1 визначте надлишковість q -ічного коду (число забонених кодових слів на одне дозволене кодове слово).

4. Визначте за яких значень ρ по відношенню до q надлишковість q -ічного коду $M > 1$.

5. Яка виправляюча можливість коду 40B20Q1 при $q = 5$, $\rho = 2$, $l = 20$?

6. Доведіть, що підмножина $H_{0,4}$ множини F чотвіркових (0; 1; 2; 3) дворозрядних слів забезпечує виправлення одиничних помилок.

7. Для множини F трійкового (0; 1; 2) дворозрядного числа визначте відстань в метриці Мінковського.

8. Наведіть доведення для аналітичних виразів для ймовірності помилкового приймання кодового слова коректуючого коду з відстанню d_M (метрика Мінковського) для коду 28B21T (аналітичні вирази 3.18а, 3.18б).

9. Джерело інформації з алфавітом з 32 символів підключене до лінії зв'язку через накопичувальний пристрій, що містить 1000 двійкових елементів пам'яті. Продуктивність джерела дорівнює 10 симв/с. Скільки часу необхідно для заповнення накопичувача інформацією?

10. Вартість двійкової комірки накопичувального пристрою складає s_1 . Як зміниться вартість накопичувача, що містить 1000 комірок, якщо застосувати 16-позиційні елементи вартістю s_2 за штуку?

11. Чому інформативність системи зв'язку підвищується зі збільшенням алфавіту каналу?

12. Користуючись формулою (3.37), визначте коефіцієнт M , розширення смуги для $m_1 = 64$; $m_2 = 32$.

13. Множина сигналів

$$\{V_c\} = \sqrt{Q_c^2} \sum_{j=1}^n \psi_{kj}(t + jT_c)$$

утворена за допомогою ортогональних функцій, що відрізняються за фазою

$$\psi_k(t) = \sqrt{\frac{2}{T_c}} \sin 2\pi \left(\frac{r}{T_c} t + \frac{k}{m} \right) \text{ за } 0 \leq t \leq T_c,$$

де $k = 1, 2, \dots, m$; $r > 0$ – ціле число. Будь-який сигнал U_{cj} можна представити вектором (U_{c1}, \dots, U_{cn}) з цілочисельними компонентами $0 \leq U_{ck} \leq m$. Доведіть, що за рівномірних сигналів

$$v_{om} = \frac{1}{2} \log_2 \frac{1}{m} \sum_{k=1}^m \exp\left(-h_c^2 \sin^2 \frac{k\pi}{m}\right).$$

14. Визначте в умовах задачі 13 величину v_{om} за значень $m = 2$ і $m = 4$.

15. Визначте в умовах завдання 13 величину v_0 за двійкових антиподальних сигналів. Порівняйте відповідь з результатом завдання 14.

16. Використовуючи співвідношення

$$\sum_{k=1}^{m-1} \sin^2 \frac{k\pi}{m} = \frac{m}{2} \text{ при } m \geq 2,$$

доведіть, що

$$\lim_{h_0^2 \rightarrow \infty} v_{om}^2 = 1,443 h_0^2.$$

17. Назвіть коди, які використовують в каналах зв'язку з групуванням помилок. Побудуйте код Файра, що виправляє пакети помилок завдовжки $l_{\text{пн}} = 5$ і виявляє пакети помилок завдовжки $l_{\text{по}} = 2$. Для яких інших помилок цей код зберігає свою ефективність?

18. Порівняйте вірність зв'язку за використання коду Хеммінга в режимі одноразового і триразового передавання з мажоритарним оброб-

ленням прийнятих сигналів, якщо ймовірність спотворення символу $\rho_0 = 10^{-2}$.

19. Закодуйте число 95 згортковим $(\frac{3}{4})$ -кодом за довжиною породжуючої послідовності $n = 16$. Синтезуйте схему кодуючого пристрою.

20. Як впливають статистичні властивості потоку помилок на ефективність коду. Назвіть основні проблеми побудови адаптивних систем зв'язку.

21. Поясніть принцип кодування сигналів методом обертого перетворення. Назвіть області застосування цього способу кодування.

22. Поясніть принцип кореляційного трактування завадостійких кодів. Побудуйте код з параметрами $k = 4$, $r \leq 3$, $s = 4$.

23. Використовуючи кореляційний метод, визначте, які помилки виправляють і виявляють циклічний код, заданий породжуючим поліномом $g(x) = 101111$ при елементності $n = 31$.

24. Використовуючи кореляційний метод, побудуйте код для передавання 16 повідомлень, який виправляє пакети помилок завдовжки $l_{\text{пк}} = 2$.

25. Дайте характеристику коду Баркера. Закодуйте числа 15 і 31 кодом Баркера. Складіть схеми кодоперетворювачів.

Глава 3.2. Ефективність таймерних сигнальних конструкцій при роботі в реальних каналах зв'язку

3.2.1. Принцип формування таймерних сигнальних конструкцій

У першій і другій частинах підручника розглядалися системи кодування, в яких інформаційний параметр елементарних сигналів (складових кодових слів) на інтервалах, визначених ефективною смугою каналу (найквістових інтервалах $- t_0$), залишався незмінним, а змінювався лише в моменти кратні значенню t_0 .

У зв'язку з цим граничне значення пропускної здатності двійкового каналу не перевищує значення $C = \log_2 2 = 1$.

Як показано в главі 1 частини 3 для отримання пропускної здатності $C > 1$ використовуються канали з алфавітом (числом розпізнавальних значень інформаційного параметра) на виході каналу $a > 2$.

Збільшення значення пропускної здатності (C) проходить на інтервалах значень a , на яких приріст $\log_2 a$ більше втрат за рахунок збільшення ймовірності помилки. Слід зазначити, що такий метод формування сигнальних конструкцій властивий поелементному кодуванню-декодуванню.

Результатом такого методу є визначеність енергетичної відстані між КС цілим числом відмінних за інформаційним параметром посліжок. Наприклад, для простого двійкового коду існує відмінність мінімум в одному елементі на найквістовому інтервалі t_0 . Для коду з парним числом одиниць відмінність у двох елементах. Таку аналогію можна знайти і для систем з алфавітом $a > 2$.

У цій главі розглядаються сигнальні конструкції, в яких кодова відстань визначається не цілим числом найквістових елементів. Назвемо такі сигнальні конструкції *таймерними*.

На відміну від розрядно-цифрового способу кодування, коли інформація про передаваний розряд визначається видом сигналу на одиничному (найквістовому) інтервалі, в таймерних сигнальних конструкціях (ТСК) інформацію закладено у тривалостях декількох окремих часових відрізків сигналу τ_c на інтервалі конструкції T_c і їхньому взаємному положенні. З метою зменшення міжсимвольних спотворень тривалість відрізків не менше найквістового інтервалу $t_c = t_0 + k\Delta$ ($k \in 0, 1, \dots, I$). Часовий відрізок Δ показує частину одиничного елемента $t_0 > \Delta = \frac{t_0}{s}$ і визначається завадами у каналі та припустимою ймовірністю помилкового приймання сигнальної конструкції ($s \in 2, 4 \dots 5$).

Із вищесказаного можна зробити висновок, що таймерні сигнали являють собою розрядно-цифрові коди, в яких дозволені для передавання сигнальні конструкції мають підряд передаваних не менше s одиниць (Δ) або нулів.

Оцінимо ефективність використання таймерних сигнальних конструкцій при передаванні двійковим симетричним каналом.

На рис. 3.15 наведено декілька реалізацій таймерних сигнальних конструкцій.

Для такого способу формування сигнальних конструкцій число $N_{\text{пр}}$ на інтервалі $T_c = mt_0$ при $\Delta = \frac{1}{S}$ дорівнює

$$N_{\text{пр}} = C_{ms-i(s-1)}^i \quad \tau_c \geq \Delta(s+i), \quad i = 1; 2; \dots \quad (3.90)$$

При використанні конструкцій з різним числом ЗММ (i)

$$N_{\text{пр}} = \sum_{i=1}^m C_{ms-i(s-1)}^i \quad (3.91)$$

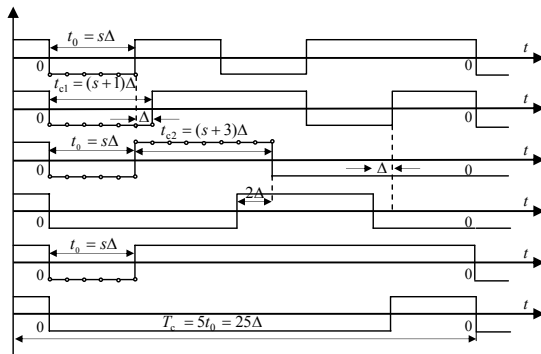


Рисунок 3.15 – Реалізація ТСК

Приклад 1. 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 $\Delta = \frac{t_0}{s}$ ($s \in 2 \dots 10$).

Розрахунки проводяться згідно з формулою 3.90 для різних значень параметрів m ; s ; i . Результати розрахунку наведені в табл. 3.4.

Таблиця 3.4 – Число реалізацій ТСК при зміні i та Δ_c $i = 1$

$m \backslash s$	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

 $i = 2$

$m \backslash s$	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

 $i = 3$

$m \backslash s$	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

$i = 4$

$\begin{matrix} s \\ m \end{matrix}$	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

$i = 5$

$\begin{matrix} s \\ m \end{matrix}$	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

$i = 6$

$\begin{matrix} s \\ m \end{matrix}$	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

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 $N_p(4)$;

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:

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} < 2 \text{ при } i < 3;$$

$$\frac{N_p[(m+1)t_0]}{N_p(mt_0)} > 2 \text{ при } i \geq 3; \quad (3.92)$$

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 $N_p = f(S)$

$$i = 2 \quad \sqrt[2]{N_p(i, m, S)} = 1,416S + 1,045;$$

$$N_p(i, m, S) = (1,416S + 1,045)^2; \quad (3.92)$$

$$i = 3 \quad \sqrt[3]{N_p(i, m, S)} = 0,554S + 1,053;$$

$$N_p(i, m, S) = (0,554S + 1,053)^3; \quad (3.93)$$

для $N_p = f(m)$.

$$i = 2 \quad \sqrt[2]{N_p(i, m, S)} = 3,536m - 6,02;$$

$$N_p(i, m, S) = (3,536m - 6,02)^2; \quad (3.94)$$

$$i = 3 \quad \sqrt[3]{N_p(i, m, S)} = 2,759m - 7,23;$$

$$N_p(i, m, S) = (2,759m - 7,23)^3. \quad (3.95)$$

З метою оцінки ефективності таймерного кодування порівняємо результати передавання інформації для двох методів кодування:

- а) розрядно-цифровий з реєстрацією в середині посилки (РЦК);
- б) використання таймерних сигналів (ТСК).

Приклад 2. В табл. 3.5 наведені число змін (γ) сигналу на виході двійкового каналу міської комутованої мережі при постійному передаванні однієї двійкової цифри та ймовірнісні характеристики «поганого» стану: середня довжина завади (пропадання сигналу) \bar{l} , середньо-квадратичне значення завади σ_0 та дисперсія D_0 , а в табл. 3.5,а результат передавання кодових слів у режимі ТСК і РЦК при смузі $\Delta F = 700$ Гц та швидкості $B = 600$ Бод.

Таблиця 3.5 – Статистичні параметри завод в каналі МТМ

$\Delta F, \text{Гц}$	$\gamma, \text{1/год}$	$L_0, \text{мс}$	\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

Таблиця 3.5,а – 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 в сім разів меншою відносно РЦК ($\Delta = t_0/7$), імовірності помилкового приймання КС різняться не суттєво, а в тих випадках, коли $T_c(\text{ТСК}) < T_c(\text{РЦК})$, імовірність помилкового приймання при ТСК може бути меншою порівняно з РЦК.

Аналіз причин спотворення сигнальних конструкцій при ТСК буде проведено далі. Відносно даних табл. 3.5,а звернемо увагу тільки на те що, практично, за рівних імовірностей 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. 3.4), 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 $T_c = 10t_0$ можлива реалізація 658008 КС (табл. 3.5), тобто коефіцієнт збільшення відносно РЦК буде дорівнювати 642, 585.

Таке збільшення числа реалізацій суттєво збільшує пропускну здатність каналу (навіть при алфавіті каналу, який дорівнює $a = 2$).

При чому граничне значення пропускну здатності буде визначатися виразом

$$C_{\text{макс}} = \frac{\log_2 N_{\text{р}\Sigma}}{T_{\text{ск}}}, \quad (3.96)$$

де $T_{\text{ск}}$ – часовий інтервал сигнальної конструкції в числі найквістових елементів; $N_{\text{р}\Sigma}$ – загальна кількість реалізацій, які використовуються з урахуванням кількості ЗММ – i .

Зважаючи на те, що ймовірності помилкового приймання КС при РЦК і ЗМВ при ТСК майже рівні (при роботі в реальних каналах), а середнє число ЗМВ та довжина кодової конструкції менше – слід очікувати зменшення ймовірності помилкового приймання кодового слова. Оскільки $N_{\text{пр}} > 2^m$, то пропускна здатність каналу при таймерних сигналах більша ніж при РЦК навіть для гауссівського каналу.

Розглянемо дроблення сигналу за рахунок впливу шуму в каналі.

Відомо, що функція кореляції для вузькосмугового процесу симетричного відносно середньої частоти f_0 має вигляд

$$R(t) = r(t) \cos 2\pi f_0 t. \quad (3.97)$$

Для такого процесу середнє число сплесків шуму відносно рівня C визначається виразом

$$N = \left(\frac{\rho_0^\alpha}{2\pi} \right)^{1/2} \frac{C}{\sigma_m} \exp \left[-\frac{1}{2\sigma^2} (A^2 + C^2) \right] \times I_0 \left(\frac{A_m C}{\sigma_m^2} \right),$$

де $I_0(\alpha)$ – функція Бесселя нульового порядку.

Для аналізу зручніше припустити, що амплітуда сигналу $A_m = 1$. Тоді середнє число сплесків такого квазігармонічного процесу (шуму) складе

$$N_1 = \left(\frac{P_0''}{2\pi} \right)^{1/2} \frac{C}{\sigma} \exp \left[-\frac{1}{2} \left(\frac{C}{\sigma} \right)^2 \right],$$

де $P_0'' = \frac{d^2 \rho(t)}{(dt)^2}$.

Можна показати, що число сплесків (викидів) за одиницю часу визначається

$$N_1 = K_\rho \Delta F \exp p \left[-1/2(C/\sigma)^2 \right],$$

де ΔF – смуга каналу; K_ρ – коефіцієнт, що визначається функцією кореляції $R(t)$ і задовольняючий умові $K < 1$.

Зокрема, при

$$\left. \begin{aligned} R_1(t) &= (1 + \alpha/t) e^{-\alpha/t}; & K_\rho &= 0,136 \\ R_2(t) &= e^{-\alpha t^2}; & K_\rho &= 0,388 \\ R_3(t) &= \frac{\sin(1/2 \Delta \omega t)}{1/2 \Delta \omega t}; & K_\rho &= 0,288 \end{aligned} \right\}. \quad (3.97a)$$

Приклад 3. Зважаючи, що $C/\sigma = h$, можна показати, що число сплесків на смугу 1 Гц при $h \geq 3$ становить

$$N_0 \leq 0,001 \cdot K_p.$$

Середня тривалість дії всплеску шуму над рівнем h визначається

$$\bar{\tau} = \sqrt{\pi/2} \frac{1}{\Delta F} V(h) \exp(h^2/2),$$

$$V(h) = 1 - \Phi(h),$$

де $\Phi(h)$ – інтеграл імовірностей.

Із останнього виразу випливає, що середня тривалість дії набагато менша тривалості одиночного елемента кодового слова $t_0 \geq 1/\Delta F$.

Розподіл ймовірностей нормованої тривалості дроблень визначається аналітичними виразами :

$$P_{д1}(l) = \delta(l)(1 - P_{д}) + 1,6 \frac{l(T_{пв} - l)}{t_0^3} V \frac{h}{\sqrt{n}} l^{-0,8l^2/t_0^2}; \quad (3.976)$$

$$0 \leq l \leq 1,5t_0, \quad l < T_{пв}$$

$$P_{д2}(l) = \frac{42(T_{пв} - l)}{t_0^2} V \left(\frac{h}{\sqrt{n}} \right) l^{-2,93l/t_0};$$

$$l > 1,5t_0; \quad l < T_{пв}$$

$$P_{д3}(l) = 0; \quad l > T_{пв}; \quad l < 0,$$

де $T_{пв}$ – відносна тривалість плоскої вершини; $n = t_0 \Delta F$; $\delta(1)$ – функція Дірака.

Приклад 4. Визначити ймовірності появи дроблень відповідної довжини при $h=3$.

У табл. 3.6 подані ймовірності появи дроблень заданої тривалості (l/t_0) для $n=1$ і $n=2$ при $h=3$, розраховані за виразами (3.976).

Таблиця 3.6 – Ймовірність появи дроблень

$n \backslash l/t_0$	0,1	0,2	0,3	0,4	0,5	h
1	$2 \cdot 10^{-2}$	10^{-2}	$2 \cdot 10^{-3}$	$6 \cdot 10^{-5}$	10^{-7}	3
2	$7 \cdot 10^{-1}$	$2 \cdot 10^{-1}$	$8 \cdot 10^{-3}$	$8 \cdot 10^{-4}$	$2 \cdot 10^{-5}$	
1	$9 \cdot 10^{-4}$	$2 \cdot 10^{-4}$	$9 \cdot 10^{-6}$	10^{-7}	10^{-9}	4
2	$2 \cdot 10^{-1}$	$5 \cdot 10^{-3}$	10^{-4}	10^{-6}	10^{-7}	

З наведеного аналізу отримуємо:

1. Оскільки ймовірність зсуву ЗМВ на величину $\Theta \geq t_0/2$ на декілька порядків менше за ймовірність помилкового приймання елемента кодового слова, яка визначається сплеском шуму, то доцільно використати сигнальні конструкції, в яких запас надійності (ймовірності помилки) обмінюється на швидкість передавання інформації.

2. Оскільки ймовірність помилкового приймання елементу визначається, в основному, дробленнями сигналу, а ймовірність появи дроблень тривалістю $l \geq l_0/2$ часто набагато менше заданої ймовірності невиявленої помилки в сигнальній конструкції, то є доцільним будувати такі сигнальні конструкції, в яких є параметрична можливість вилучити дроблення тривалістю $l \leq 0,5t_0$.

Закон зміщення ЗМВ залежить від виду обвідної сигналу, яка частіше описується узагальненим законом – m -розподілом:

$$m(U_c) = \frac{2m^m U_c^{2m-1}}{\Gamma(m) (\bar{U}_c^2)^m} e^{-\frac{mU_c^2}{\bar{U}_c^2}} = f(m, U_c, \bar{U}_c^2), \quad (3.98)$$

де \bar{U}_c^2 – середній квадрат обвідної сигналу;

$$m = \frac{(\bar{U}_c^2)^2}{(U_c^2 - \bar{U}_c^2)^2} = \frac{(\bar{U}_c^2)^2}{\bar{U}_c^4 - (\bar{U}_c^2)^2} \geq 0,5$$

– параметр розподілу; $\Gamma(m)$ – гама-функція, яка пов'язана з m і \bar{U}_c^2 співвідношенням

$$\bar{U}_c^v = \frac{\Gamma(m+0,5v)}{\Gamma(m)} \sqrt{\left(\frac{\bar{U}_c^2}{m}\right)^v}.$$

Узагальнений закон m -розподілу використовується для будь-яких каналів. Так, при $m = 1$ обвідна сигналу U_c підпорядковується простому закону Релея

$$\omega(U_c) = \frac{2U_c}{\bar{U}_c^2} e^{-\frac{U_c^2}{\bar{U}_c^2}}.$$

При завмираннях за законом Релея густина ймовірності $\omega(h^2)$ має вигляд

$$\omega(h_c^2) = \frac{2\sqrt{h_c^2}}{h_{c0}^2} e^{-\frac{h_c^2}{h_{c0}^2}},$$

де h_{c0}^2 – середнє значення h_c^2 . У цьому випадку за некогерентного приймання ортогональних сигналів ймовірності

$$p_{01} = \frac{1}{2} e^{-\frac{h_c^2}{2}}; \quad p_{02} = \frac{1}{2 + h_{c0}^2}.$$

Тоді, при $\alpha_0 = 0,99$ дістанемо

$$h_{\text{сн}}^2 \approx 3; \quad \varphi_1 = 1 - e^{-\frac{9}{h_{\text{сн}}^2}} \approx \frac{9}{h_{\text{сн}}^2}.$$

При $h_{\text{сн}}^2 \geq 100$, що часто виконується на практиці, ймовірності $p_{01} \approx 10^{-2} p_0$; $p_{02} \approx 0,11 p_0 h_{\text{сн}}^2$.

Для таких умов ймовірності появи пакета визначаються

$$p(l_{\text{п}}) = \exp\left[-\frac{\pi(l_{\text{п}} - 0,5)^2}{4l_{\text{п0}}^2}\right] - \exp\left[-\frac{\pi(l_{\text{п}} - 0,5)^2}{4l_{\text{п0}}^2}\right], \quad (3.99)$$

де середня довжина пакета помилок у символах

$$l_{\text{п0}} = t_{\text{п0}} v_T \approx 10,6 \frac{T_{30} v_T}{\sqrt{h_{\text{сн}}^2}};$$

T_{30} – середній період завмирань, а ймовірність

$$p_{\text{п}} = 0,99 \frac{p_0}{p_{02} l_{\text{п0}}} = \frac{9}{h_{\text{сн}}^2 l_{\text{п0}}}.$$

Для кабельних каналів можна прийняти $p_{02} \approx 0,3 \dots 0,4$ і $p_{\text{п}} \approx 3 \cdot 10^{-5} \dots 3 \cdot 10^{-6}$.

3.2.2. Параметри зміщень нуль-переходів на виході бінарного каналу

Координатні функції подання сигналів (див. частину 1) $\varphi_k(z) = \frac{\sin z}{z}$ не є найкращими. Достойнство їх полягає у простоті визначення вагових коефіцієнтів A_k . Проте їхній спектр недостатньо швидко спадає зі зростанням z . Функція $\frac{\sin z}{\text{sh}z}$ 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.

Вказане 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:

$$s(t_k) = 0, \quad k = 1, 2, \dots, m^8.$$

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

$$S(\omega) = \int_0^{\tau} s(t) e^{-i\omega t} dt, \quad (3.100)$$

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

$$S(t) = \frac{1}{2} \sum_{k=-n}^n c_k e^{ik\Omega t}, \quad 0 < t < \tau, \quad \Omega = \frac{2\pi}{\tau}, \quad (3.100a)$$

де $e^{ik\Omega t}$ – так звані тригонометричні багаточлени, що мають безпосереднє відношення до багатоканальних УПС.

Незважаючи на те, що вираз (3.100a) 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 $-c_{-k} = a_{-k} - ib_{-k}$, 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 $c_0 = a_0 - ib_0$, $b_0 = 0$.

⁸ Сигнал може в загальному випадку володіти також і комплексними нулями вигляду. Проте комплексні нулі не зручні для спостереження, тому що вони не можуть бути визначені як моменти перетинів сигналом деякого фіксованого рівня. У зв'язку з цим частіше увага приділяється дійсним нулям.

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 УПС 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 (3.100а), 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 (3.100а)

$$t_1, t_2, \dots, t_{2n}. \quad (3.100б)$$

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 (2.100б) 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 (3.100a) 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 (3.100a) з його дійсними коренями. Незважаючи на те, що отримувачу 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 (3.100a) можна представити у вигляді

$$s(t) = \frac{1}{2} e^{-in\Omega t} (1 - \alpha_1 e^{i\Omega t}) (1 - \alpha_2 e^{i\Omega t}) \dots (1 - \alpha_{2n} e^{i\Omega t}), \quad (3.101)$$

де

$$\alpha_k = e^{-i\Omega t_k}, \quad k = 0, 1, 2, \dots, 2n.$$

Справедливість формули (3.101) випливає з того факту, що числа t_1, t_2, \dots, t_{2n} , які є коренями багаточлена, перетворюють в нуль і праву частину рівності (3.101). 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 (3.100a), дорівнювати відповідно $-n\Omega t$ і $n\Omega t$. Отже, праві частини у (3.100a) і (3.101), 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 в «своєму» інтервалі завдовжки $\frac{\tau}{2n}$. Пригадавши, що найвища частота в сигналі $s(t)$ є $n\Omega$, 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. 3.16). Маючи на увазі двійкове кодування в цифровому процесорі УПС номера цього короткого підінтервалу комбінаціями R -значного коду, вважаємо, 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

$$\Delta = \tilde{\tau}/2^R.$$

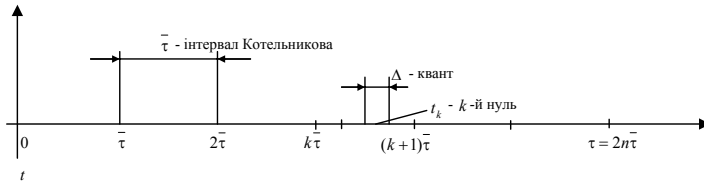


Рисунок 3.16 – Положення нуля t_k на інтервалі Котельникова

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 вигляд

$$S_1(t) = \frac{1}{2} \sum_{k=-n+1}^{n-1} c_k e^{ik\Omega t} + \xi(t) + \cos n\Omega t.$$

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 вигляді

$$\xi(t) = \frac{1}{2} \sum_{k=-n}^n \xi_k e^{i\Omega k t}, \quad \xi_k = \bar{\xi}_{-k}, \quad k = 0, 1, 2, \dots, n, \quad (3.101a)$$

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 (3.101a), 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 (3.101a), 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

$$g_k = c_k + \xi_k, \quad k = 0, \pm 1, \dots, \pm(n-1),$$

$$g_{-n} = \bar{\xi}_{-n}, \quad g_n = \xi_n.$$

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 у реальних бінарних каналах зв'язку. Нехай напруга на виході ФНЧ впливає на пороговий пристрій з характеристикою

$$u_n(i) = \begin{cases} 1 & \text{за } u(t) > U_n \\ -1 & \text{за } u(t) < U_n \end{cases},$$

де $u_n(i)$ і $u(t)$ – відповідно вихідна і вхідна напруга порогового пристрою; U_n – 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

$$U_n = \frac{u_1 + u_0}{2},$$

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 дроблення цих вихідних відеоімпульсів.

Як ми побачимо 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 за дуже малих значень $q_{\text{вих}}$.

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 ($t_1 < \tau_n/2$), збігається з ймовірністю того, що у момент часу t_1 реалізація шумів лежить нижче кривої – $u(t)$ (рис. 3.17).

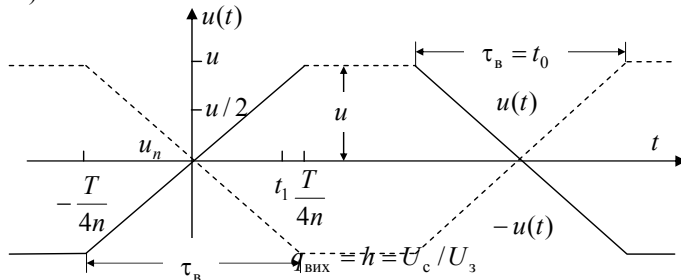


Рисунок 3.17 – Пояснення механізму виникнення зсувів фронтів відеоімпульсів

Отже функція розподілу ймовірностей зсувів фронтів для $t_1 < \frac{\tau_n}{2}$ є нормальною і має вигляд:

$$p_c(l) = \frac{4q_{\text{вих}}n}{\sqrt{2\pi}} e^{-8q_{\text{вих}}^2 n^2 l^2} \quad \text{при } |l| < \tau_{\text{но}}, \quad (3.102)$$

де l – відносне значення зсуву фронту імпульсу $\left(l = \frac{t_1}{t_0}\right)$; $\tau_{\text{но}} = \frac{\tau_n}{2t_0}$ – відносна тривалість цього фронту.

На рис. 3.18 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 відеоімпульсів необмежено зменшуються. Це пояснюється тим, що зі зростанням n пропорційно зростає крутість фронту відеоімпульсу і зменшується час становлення сигналу на виході τ_B .

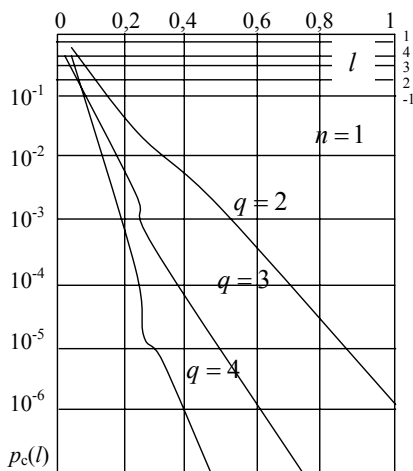


Рисунок 3.18 – Графік функції $p_c(l)$

імпульсу (нагадаємо, що переважна більшість дроблень лежить усередині плоскої вершини).

Для обчислення розподілу ймовірностей довжин дроблень при $|l| > \tau_{нв}$ розглянемо рівень напруги – u та сплеск шумів під цей рівень.

Ймовірність попадання точки⁹ $t = \frac{\tau_{н}}{2}$ усередину такого сплеску збігається з ймовірністю того, що напруга шумів у цей момент буде перевищувати u та дорівнювати:

$$\rho_v(q_{вих}) = \text{erf}(q_{вих}),$$

($\text{erf}(x)$ – функція помилок).

Нехай тепер точка $t = \frac{\tau_{н}}{2}$ попала усередину сплеску шуму, що має тривалість τ_v . Враховуючи, що ця точка може рівноймовірно займати будь-яке положення усередині сплеску, для умовної густини розподілу інтервалу τ_1 між точкою і кінцем викиду можна записати:

$$p_{\tau_1}(\tau/\tau_v) = \begin{cases} \frac{1}{\tau_v} & \text{при } \tau_v > \tau, \\ 0 & \text{при } \tau_v < \tau. \end{cases}$$

Тому

Проте при цьому зменшується $q_{вих}$ і дія перших двох факторів виявляється все-таки переважною.

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 $q_{вих}$. Ці сплески (викиди) стимулюють появу дроблень, якщо вони закінчуються усередині плоскої вершини відео-

⁹ Під точкою t мається на увазі значення напруги в момент t .

$$p_{\tau_1}(\tau) = \int_{\tau}^{\infty} \frac{1}{\tau_{\text{в}}} p_{\text{в}}(\tau_{\text{в}}) d\tau_{\text{в}},$$

де $p_{\text{в}}(\tau)$ – розподіл тривалості сплесків шуму, причому, оскільки ми прийняли $\sigma = 1$, слід вважати $h = q_{\text{вих}}$.

Можна показати, що

$$P_c(l) = \begin{cases} F(4q_1\sqrt{nl}) & \text{при } 0 < l < \tau_{\text{нв}}, \\ F\left(\frac{q_1}{\sqrt{n}}\right) Q(l_1) & \text{при } l > \tau_{\text{нв}}, \end{cases}$$

де позначено $l_1 = \frac{l - \tau_{\text{нв}}}{t_0}$; $t_0 = \frac{\tau_{\text{в}}}{T}$;

$$Q(l_1) = \begin{cases} 0,98e^{-0,81l_1^2} - 3,16l_1F(1,27l_1) + 0,02 & \text{при } 0 < l_1 < 1,5, \\ 42\left[0,34e^{-2,93l_1} + l_1Ei(-2,93l_1)\right] & \text{при } l_1 > 1,5; \end{cases} \quad (3.102a)$$

$Ei(x)$ – інтегральна показова функція і $q_1 = q_{\text{вих}}\sqrt{n}$.

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. 3.19 наведена залежність $Q(l_1)$, розрахована згідно з виразом 3.102а.

Враховуючи вираз 3.102а ймовірність появи дроблень різної тривалості визначається:

$$\rho_d = \begin{cases} F\left(\frac{q_1}{\sqrt{n}}\right) [\tau_{\text{нв}} - \Phi(1,27\tau_{\text{нв}})] & \text{при } \tau_{\text{нв}} < 1,5, \\ F\left(\frac{q_1}{\sqrt{n}}\right) [\tau_{\text{нв}} - 1 + 4,87e^{-2,93\tau_{\text{нв}}}] & \text{при } \tau_{\text{нв}} > 1,5, \end{cases} \quad (3.103)$$

де $\tau_{\text{нв}} = \frac{T_{\text{пл}}}{t_0}$.

Розподіл імовірностей нормованої тривалості дроблень складас:

$$p_d(l) = \begin{cases} \delta(l)(1 - \rho_d) + 1,6 \frac{l(\tau_{\text{нв}} - l)}{t_0^3} F\left(\frac{q_1}{\sqrt{n}}\right) e^{-0,8 \frac{l^2}{t_0^2}} & \text{при } 0 \leq l < 1,5t_0 \text{ і } l < \tau_{\text{нв}}, \\ \frac{42(\tau_{\text{нв}} - l)}{t_0^2} F\left(\frac{q_1}{\sqrt{n}}\right) e^{-2,93 \frac{l}{t_0}} & \text{при } l > 1,5t_0 \text{ і } l < \tau_{\text{нв}}, \\ 0 & \text{при } l > \tau_{\text{нв}} \text{ і } l < 0. \end{cases} \quad (3.103a)$$

Розподіл $p_d(l)$ для $n = 1$ і деяких h наведено на рис. 3.20 (враховується відносна величина l).

Аналіз виразів 3.103 і залежностей $p_d(l)$ свідчить, що зі зростанням n за постійного значення q_1 ймовірність дроблень збільшується. Це пояснюється зменшенням середньої тривалості сплеску і співвідношення сигнал/завада зі зростанням n .

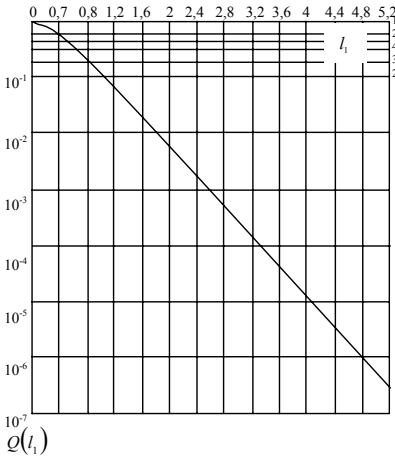


Рисунок 3.19 – Графік функції $Q(l_1)$

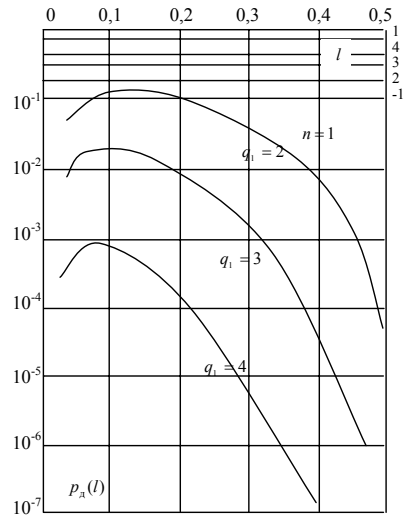


Рисунок 3.20 – Графік функції $p_d(l)$

На закінчення відзначимо, що наведені вище дані про зсув фронтів і дроблення відеоімпульсів під дією шумів добре узгоджуються з результатами експериментальних досліджень.

Знаючи дисперсію зміщення ЗМВ на виході гауссівського каналу і розподіл дроблень різної довжини можна провести порівняння ймовірності прийому елементів не тільки з урахуванням зміщень ЗМВ за середину послілки, а й за рахунок сплесків шуму (тобто дроблень).

Приклад 5. Провести порівняння ймовірності помилки для когерентного приймання при протилежних сигналах з ймовірністю зміщення ЗМВ за середину елементарної послілки.

Із частини 1 відомо, що для протилежних сигналів

$$P_{01} = P_{10} = 1 - \Phi\left(\sqrt{\frac{\lambda E}{N_0}}\right),$$

де E , N_0 – енергія сигналу та спектральна густина шуму; λ – коефіцієнт відмінності сигналів для різних видів модуляції. Для нашого випадку він дорівнює 1; $\Phi(x)$ – інтеграл ймовірностей.

Враховуючи дані співвідношення

$$P_{01} = P_{02} = 1 - \Phi(h),$$

а для зміщення ЗМВ за середину посилки, враховуючи середньоквадратичне значення $\sigma_c = \frac{1}{4h}$ (вираз 2.102 при $n = 1$)

$$P_{013M} = P_{023M} = 1 - \Phi\left(\frac{4h}{2}\right) = 1 - \Phi(2h).$$

Порівнюючи P_{01} , P_{02} і P_{013M} , P_{023M} бачимо, що при оцінці сигналу за нуль-перетинами ймовірність помилки для $h \geq 3$ на 4-5 порядків менша порівняно з когерентним прийманням.

3.2.3. Пропускна здатність каналу при ТСК

Пропускна здатність двійкового каналу, представляючи максимальне значення швидкості передавання інформації за заданих фіксованих меж W_c , визначається

$$C = \sup \left[I(n, W_c) \right] \frac{\text{ДВ.ОД}}{c};$$

$$L_1 \in W_{1\dots}; L_i \in W_i, \quad (3.104)$$

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

$$I = [1 + P_c \log_2 P_c + (1 - P_c) \log_2 (1 - P_c)]. \quad (3.104a)$$

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 (3.90).

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

$$\left. \begin{aligned} \bar{i} &= \sum_{i=1}^m P[N_p(i)] i \\ P[N_p(i)] &= \frac{N_p(i)}{N_{p\Sigma}} \end{aligned} \right\} \quad (3.105)$$

Кожна з таймерних сигнальних конструкцій за рівномірних 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

$$H_r = -\sum_{i=1}^m P[N_p(i)] \log_2 P[N_p(i)] = \sum \frac{N_p(i)}{N_p} \log_2 \left[\frac{N_p(i)}{N_p} \right]. \quad (3.105a)$$

Якщо приймач отримав сигнал з i -переходами, то невизначеність у достовірності передавання кожного з них на k -му місці знаходиться умовною ентропією

$$H\left(\frac{Z_i}{K_i}\right) = -\sum_{i=1}^{Z_0} P\left(\frac{Z_i}{K_i}\right) \log_2 P\left(\frac{Z_i}{K_i}\right), \quad (3.105б)$$

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)

$$I = H_i - H_{\Sigma i} = \log_2 N_p - \sum_{i=1}^m P(i) H\left(\frac{Z_i}{K_i}\right). \quad (3.105в)$$

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 (3.105в), 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

$$I_0 = \frac{\log_2 N_p - \sum_{i=1}^m iP(i)H\left(\frac{Z_i}{K_i}\right)}{m}. \quad (3.106)$$

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

$$H\left(\frac{Z_i}{K_i}\right) = -2\Phi\left(\frac{2h}{S}\right) \log_2 \left[2\Phi\left(\frac{2h}{S}\right) \right] + 2 \sum_{i=1}^{Z_{0i}} \left\{ \Phi(2i+1) \left[\frac{2h}{S} \right] - \Phi\left[(2i-1) \frac{2h}{S} \right] \right\} \log_2 \left\{ \Phi\left[(2i+1) \frac{2h}{S} \right] - \Phi\left[(2i-1) \frac{2h}{S} \right] \right\}. \quad (3.106a)$$

Через те що вираз (2.106а) 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

$$H_{\Sigma i} = +H\left(\frac{Z_i}{K_i}\right) \sum_{i=1}^m P(i) = -H\left(\frac{Z_i}{K_i}\right) \bar{i}. \quad (3.106б)$$

Враховуючи (2.106), (2.106а), (2.106б), пропускна здатність каналу без завад дорівнює

$$I_0 = \frac{\log_2 N_p - \bar{i}H\left(\frac{Z_i}{K_i}\right)}{m}. \quad (3.107)$$

Таким чином, з виразів (2.106), (2.106а) виходить, що пропускна здатність каналу без завад визначається числом реалізацій сигналів за заданого значення s або Δ і потужністю міжсимвольних завад.

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. 3.21 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 .

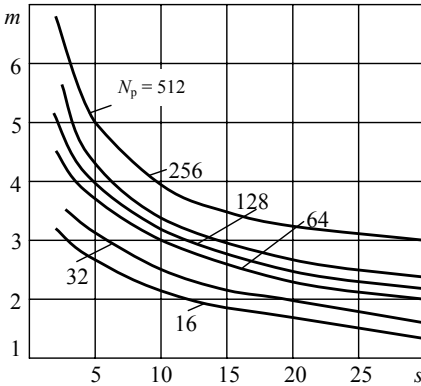


Рисунок 3.21 – Залежності $m = f(s)$ при $N = \text{const}$

При роботі по каналах з гауссівським шумом слід враховувати, що ймовірність помилкового приймання кодової конструкції ТСК (P_n) визначається величиною зони Δ , середньоквадратичним відхиленням ЗМВ (σ), що в свою чергу, залежить від співвідношення сигнал/завада, а також числом переходів у слові (i)

$$P_n = 1 - [\Phi(\Delta/2\sigma)]^{\bar{i}}, \quad (3.108)$$

де \bar{i} – середнє число ЗММ у кодовому слові,

$$\Phi(x) = \frac{1}{\sqrt{2\sigma}} \int_0^x e^{-\frac{t^2}{2\sigma}} dt. \quad (3.109)$$

$\Phi(x)$ – інтеграл імовірностей.

Виходячи з виразів (3.106), (3.107), середнє число переходів у сигнальній конструкції при $i \in (1 \dots m)$

$$\bar{i} = \sum_{i=1}^m \frac{iC_{ms-i}^2(s-1)}{C_{ms-i}^i(s-1)}. \quad (3.110)$$

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

$$C_m = \frac{1}{m} (\log_2 N_{pz} - H_{вт}). \quad (3.111)$$

Тут $H_{вт}$ визначає втрати в каналі через невизначеність у прийманні кодової сигнальної конструкції

$$H_{вт} = - \left[p_v \log_2 p_v + (1 - p_v) \log_2 \frac{1 - p_v}{N - 1} \right], \quad (3.112)$$

$$P_i = [2\Phi(\Delta / 2\sigma)]^i, \quad (3.113)$$

де P_i – ймовірність вірного приймання сигнальної конструкції з i -переходами.

На рис. 3.22 наведено залежності пропускної здатності каналів з різним рівнем флукуаційних шумів (задано $h = u_c / u_{\text{ш}}$) 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

$$\left. \begin{aligned} \sigma_3 &= 1/4h \\ h &= u_c / u_{\text{ш}} \end{aligned} \right\}.$$

З принципу формування ТСК зрозуміло, що множина дозволених для передавання КС не є лінійною, тобто серед дозволених сигналів можна знайти пару таких, сума яких може утворити сигнал,

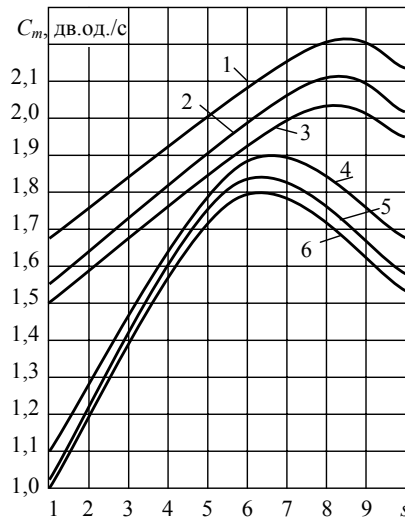


Рисунок 3.22 – Залежності пропускної здатності каналу $C_i = f(s)$ при $h = \text{const}$, $m = \text{const}$

в якого відстань між суміжними моментами модуляції менша за $t_0 = s\Delta$. Наприклад, сума двох кодових слів (для $s = 5$):

$$\begin{array}{r} 1111100000111111 \\ \oplus \\ 1111100000111111 \end{array}$$

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 6. 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. 3.23 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 $(i-1)$.

Визначимо число комбінацій в групі. Для цього розглянемо випадок, коли комбінації групи містять лише один нуль. Ненульові члени комбінації можуть набувати $(a-1)$ значень.

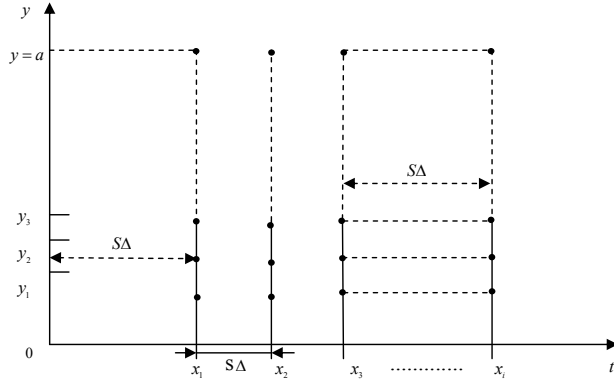


Рисунок 3.23 – Принцип формування недвійкових ТСК

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

$$B_{i-1} = (a-1)^{i-1} C_i^{i-1}. \quad (3.114)$$

Подібні міркування можна навести і для груп, які вмщують 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:

$$N_p(a > 2) = \sum_{i=1}^m (a-1)^i \cdot C_{ms-i(s-1)}^i. \quad (3.115)$$

Рівність (3.115) 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 пропускної здатності

$$C_{\text{макс}} = \frac{i \log_2(\alpha-1) + \log_2 C_{ms-i(s-1)}^i}{m} = \frac{i \log_2(a-1)}{m} + \frac{\log_2 C_{ms-i(s-1)}^i}{m}. \quad (3.116)$$

Із останнього виразу видно, що введення багатопозиційного сигналу суттєво доповнює складову, яка забезпечується за рахунок розміщення моментів модуляції в точках некратних найквістовому інтервалу.

Приклад 7. 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 3.116 дорівнює $\frac{3 \cdot 4}{5} \approx 2,4$. По відношенню до C_{\max} для бінарного каналу цей приріст збільшує максимальне значення пропускнуої здатності майже вдвічі (див. рис. 3.22).

3.2.4. Зв'язок коефіцієнтів A_i з кодовою відстанню

Через те що кодові сигнальні конструкції, в яких число ЗМВ відрізняється від заданого, легко виявляються на прийомі, то при виборі метрики будемо виходити з необхідності оцінювати відстані при відомих місцях знаходження ЗМВ, тобто будемо враховувати тільки зміщення значущих моментів відтворення.

З принципу формування сигналів видно, що прийнята метрика повинна враховувати не тільки сам факт відмінності кодових слів, а й величину відмінності в окремих позиціях. Припустимо, що є канал, в якому сигнал на виході залежить тільки від виду сигналу на вході (дискретний канал без пам'яті),

$$\left. \begin{aligned} P(Z/0) &= P_i; i = 0, 1, 2, \dots, S_0; S < \frac{A_0}{2}, \\ P(-Z/0) &= P_i; i = 0, 1, 2, \dots, S_0; \\ P(i/i') &= P(k/0); k = i - i' \pmod{A_0} \end{aligned} \right\} \quad (3.117)$$

де $P(Z/0)$ – ймовірність зміщення будь-якого ЗММ на Z поділів Δ під дією завад.

Рівність правих частин першого та другого рівнів (3.117) говорить про те, що поява позитивних і негативних зсувів ЗМ рівноймовірна. З цього випливає, що при передаванні n -елементного кодового слова x_1, x_2, \dots, x_n на прийомі отримуємо слово $(y_1, \dots, y_{n-1}, y_n)$ з імовірністю

$$P(x_1 - y_1, x_2 - y_2, x_n - y_n) / 0_1, \dots, 0_n = \prod_{i=1}^n P\left(\frac{x_i}{y_i}\right). \quad (3.117a)$$

Будемо вважати, що метрика d_L в даному дискретному каналі забезпечує мінімальну помилку декодування в тому випадку, коли для двох векторів помилок забезпечується умова

$$\left. \begin{aligned} E &= (e_1, e_2, e_3, \dots, e_n); \\ E &= (e'_1, e'_2, e'_3, \dots, e'_n); \\ d - (0, E) &< d(0, E^+); \\ P\left(\frac{E}{0}\right) &> P\left(\frac{E'}{0}\right). \end{aligned} \right\} \quad (3.118)$$

Нерівності (3.118) говорять про те, що ймовірність появи зміщення ЗМ на більшу величину менше ймовірності зміщення на меншу величину. Для умов помилкового декодування кодових слів з постійним числом ЗМ, що задовольняє умовам (ТСК), можна довести теорему.

Теорема 4. Модульна і Лі метрики в дискретному каналі з крайовими спотвореннями, розподіленими за нормальним законом, забезпечують мінімум імовірності помилкового декодування сигналів ТСК.

Припустимо, що передається n -елементний вектор з числом значущих моментів модуляції $-n$.

$$x_1 = A_1 x_1 + A_2 x_2 + \dots + A_n x_n = 0 \pmod{A_0}, \quad (2.118a)$$

де A_i – деякі коефіцієнти, що забезпечують необхідні відстані між дозволеними ТСК (буде розглянуто нижче).

Під впливом завади $E'_1 = (e'_1, e'_2, e'_3, \dots, e'_n)$ переданий вектор КС може бути прийнятий як вектор $\bar{X}_2 \in A$, віддалений на відстані d_2 , або як вектор \bar{X}_3 віддалений на відстань d_3 .

$$\left. \begin{aligned} -z_2 - z_4 &\leq \frac{d-3}{2}; z_3 - z_4 \leq \frac{d+1}{2}; \\ -z_2 - z_3 &\leq \frac{d-3}{2}; z_2 \leq 0; \\ z_3 &\leq -1; z_4 \leq -1; z_1 > 0; \end{aligned} \right\}$$

Доведемо, що якщо $d_3 > d_2$, то

$$P\left(\frac{E_3}{E_1}\right) < P\left(\frac{E_2}{E_1}\right). \quad (3.118b)$$

Позначимо через $W(E'_1)$ – вагу вектора помилки \bar{E}'_1 . Відповідно до визначення вага вектора $W(E'_1)$

$$\left. \begin{aligned} W(E_1) &= \sum_{i=1}^{m_i} i_i h_i = d_2; \\ W(E_2) &= \sum_{i=1}^{m_i} i_i h'_i = d_3, \end{aligned} \right\}$$

i_i – число ЗМВ, яке змістилося на величину h_i .

Ймовірність появи такого вектора завади для випадку нормально-розподілених зсувів ЗМВ з нульовим середнім значенням дорівнює

$$\begin{aligned}
 P\left(\frac{E_1}{0}\right) &= \left[P\left(\frac{1}{0}\right)\right]^{h_1} \left[P\left(\frac{2}{0}\right)\right]^{h_2} \dots \left[P\left(\frac{S}{0}\right)\right]^{h_s} \left[P\left(\frac{0}{0}\right)\right]^{h-\sum_{i=1}^m h_i} = P_0^{n-\sum_{i=1}^m h_i} P_1^{h_1} P_2^{h_2} P_m^{h_m} = \\
 &= \frac{P_0^{n-\sum_{i=1}^m h_i} P_1^{h_1} [P_0^{(i-1)}]^{h_1} P_2^{h_2} [P_0^{(2-1)}]^{h_2} P_m^{h_m} [P_0^{(m-1)}]^{h_m}}{P_0^{\sum_{i=1}^m i h_i - \sum_{i=1}^m h_i}} = P_0^{n-W(E_1)} \prod_{i=1}^m P_i (P_0^{i-1})^{h_i}.
 \end{aligned} \tag{3.119}$$

В останньому перетворенні враховано, що

$$\frac{P_0^{n-\sum_{i=1}^m h_i}}{P_0^{\sum_{i=1}^m i h_i - \sum_{i=1}^m h_i}} = P_0^{n-\sum_{i=1}^m h_i - \sum_{i=1}^m i h_i + \sum_{i=1}^m h_i} = P_0^{n-\sum_{i=1}^m h_i} = P_0^{h-W(E_1)}. \tag{3.119a}$$

Приклад 8. Нехай задана ТСК з трьома переходами $i = 3$. Для ймовірності появи завади, що трансформує одне кодове слово в інше, віддалене на $W(E) = d$, $n = 3$ добуток $\prod_{i=1}^m P_i (P_0^{i-1})^{h_i}$ у вираз (3.119) буде мати два співмножники: $i = 1, i = d - 1$, отже

$$P\left(\frac{E_1}{0}\right) = P(0)P(1)P(d-1),$$

тобто помилка буде не виявлена, коли один перехід буде прийнятий вірно $P(0)$, другий зміститься на величину 1Δ , а третій на величину $(d-1)\Delta$.

В основному значення $P\left(\frac{E_1}{0}\right)$ визначається $P(d-1)$.

З іншого боку, закон розподілу ймовірностей появи відповідної величини зміщення ЗММ описується нормальним законом, отже

$$P(d-1) = P[\theta > (d-1)\Delta] = 0,5 \left[1 - \Phi\left(\frac{(d-1)\Delta}{\sqrt{\sigma}}\right) \right] = 0,1 \exp\left\{-\left(\frac{d-\Delta}{\sigma}\right)^2\right\}.$$

Після перетворень отримаємо

$$\left. \begin{aligned}
 P\left(\frac{E_2}{0}\right) / P\left(\frac{E_1}{0}\right) &> 1, d_1 > d_2, \\
 P\left(\frac{E_2}{0}\right) / P\left(\frac{E_1}{0}\right) &< 1, d_1 < d_2.
 \end{aligned} \right\} \tag{3.120}$$

Отже, застосування метрики Лі або модульної при передаванні інформації на реальних каналах сигналами ТСК забезпечує мінімум ймовірності помилкового декодування.

Зв'язок коефіцієнтів A_i з кодовою відстанню ТСК. Запишемо рівняння (3.118а) у вигляді

$$A_1x_1 + A_2x_2 + \dots + A_{n-1}x_{n-1} + A_nx_n = \sum_{i=1}^n A_ix_i = 0 \pmod{A_0}.$$

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 5. Якщо координати і модуль порівняння A_0 визначені за формулами

$$\left. \begin{aligned} A_n &= 1; \\ A_{n-1} &= d - 1; \\ A_{n-k} &= E^{-}\left(\frac{d-1}{2}\right)A_{n-k+1} + E^{-}\left(\frac{d}{2}\right), k = 1, 2, \dots, n; \\ A_0 &= E^{-}\left(\frac{d+1}{2}\right)A_1 + E^{-}\left(\frac{d}{2}\right), \end{aligned} \right\} \quad (3.121)$$

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 (3.121) за парного та непарного d мають вигляд:

$$\left. \begin{aligned} A_n &= 1, \\ A_{n-1} &= d - 1, \\ A_{n-k} &= A_{n-k+1}\left(\frac{d}{2} - 1\right) + \frac{d}{2}, \\ A_0 &= A_1\frac{d}{2} + \frac{d}{2}, \end{aligned} \right\}, d - \text{парне} \quad (3.121a)$$

$$\left. \begin{aligned} A_n &= 1, \\ A_{n-1} &= d - 1, \\ A_{n-k} &= A_{n-k+1}\left(\frac{d-1}{2}\right) + \frac{d-1}{2}, \\ A_0 &= A_1\frac{d+1}{2} + \frac{d-1}{2}, \end{aligned} \right\}, d - \text{непарне} \quad (3.121b)$$

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 (3.121a) легко перевірити, що за непарного d вектори

$$\left. \begin{aligned} \bar{Y}_1 & \left(1, \frac{d-1}{2}, 0, 0, 0, \dots, \frac{d-1}{2} \right); \\ \bar{Y}_2 & \left(0, -1, \frac{d-1}{2}, 0, 0, \dots, \frac{d-1}{2} \right); \\ \bar{Y}_{n-2} & \left(0, \dots, 0, -1, \frac{d-1}{2}, 0, \frac{d-1}{2} \right); \\ \bar{Y}_{n-1} & \left(0, \dots, 0, 0, -1, \frac{d-1}{2}, \frac{d-1}{2} \right); \\ \bar{Y}_n & \left(0, \dots, 0, 0, 0, -1, \frac{d-1}{2} \right) \end{aligned} \right\} \quad (3.121\text{в})$$

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}' :

$$\left. \begin{array}{l} \bar{Y}_1 \quad (-1, \quad \frac{d}{2}, \quad 0, \quad 0, \quad \dots, \quad 0, \quad \frac{d}{2}); \\ \bar{Y}_2 \quad (0, \quad 1, \quad \frac{d}{2}, \quad 0, \quad \dots, \quad 0, \quad \frac{d}{2}); \\ \bar{Y}_{n-2} \quad (0, \quad 0, \quad -1, \quad \frac{d}{2}-1, \quad \dots, \quad 0, \quad \frac{d}{2}); \\ \bar{Y}_{n-1} \quad (0, \quad 0, \quad 0, \quad 1, \quad \dots, \quad \frac{d-1}{2}, \quad \frac{d}{2}); \\ \bar{Y}_{n-2} \quad (0, \quad 0, \quad 0, \quad 0, \quad \dots, \quad -1, \quad \frac{d}{2}). \end{array} \right\}$$

Розглянемо послідовність доведення для модуля порівняння A_0 при $n = 4$. Рівняння (3.118а) 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 (3.121а)

$$\left. \begin{array}{l} A_4 = 1; A_3 = d - 1; \\ A_2 = E^-\left(\frac{d-1}{2}\right) + E^-\left(\frac{d}{2}\right); \\ A_1 = \begin{cases} A_2 \frac{d-1}{2} - A \frac{d-3}{2} + 1; d - \text{нечетне}; \\ A_2 \left(\frac{d}{2} - 1\right) + \frac{d}{2}; d - \text{парне}. \end{cases} \end{array} \right\} \quad (3.122)$$

Базисом у цьому випадку будуть вектори

$$\left. \begin{array}{l} \bar{Y}_1(0, \quad 0, \quad -1, \quad d-1); \\ \bar{Y}_2(0, \quad -1, \quad E^-\left(\frac{d-1}{2}\right), \quad E^-\left(\frac{d}{2}\right)); \\ \bar{Y}_3(-1, \quad \frac{d-1}{2}, \quad \frac{d-3}{2}, \quad 1), \quad d - \text{нечетне}; \\ \bar{Y}_4(-1, \quad \frac{d}{2}-1, \quad 0, \quad \frac{d}{2}), \quad d - \text{парне}. \end{array} \right\} \quad (3.122a)$$

Кожен із векторів (3.122) має вагу $W(\bar{Y})$ і задовольняє умові ТСК. Однак серед векторів, що мають вагу d можна знайти і такі, лінійна форма яких

$$L(\bar{X}) = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 \neq 0.$$

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 6. Існує такий вектор $Z(z_1, z_2, z_3, z_4) \in M$, координати якого задовольняють будь-якому з таких обмежень:

$$\left. \begin{aligned} -z_2 - z_4 &\leq \frac{d-1}{2}; z_3 - z_4 \leq \frac{d-1}{2}; \\ z_3 - z_2 &\leq \frac{d-5}{2}; \\ z_4 &\leq -1; z_3 \geq 0; z_2 \leq -1; z_1 > 0. \end{aligned} \right\}, \quad (3.123a)$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-5}{2}; z_2 + z_3 \leq \frac{d+1}{2}; \\ z_3 - z_4 &\leq \frac{d+1}{2}; z_2 \geq 0; z_3 \geq 1; \\ z_4 &\leq 0; z_1 \geq 0. \end{aligned} \right\}, \quad (3.123б)$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-7}{2}; -z_3 + z_4 \leq \frac{d+1}{2}; \\ -z_3 - z_2 &\leq \frac{d-1}{2}; z_4 \geq 0; z_3 \leq 1; \\ z_2 &\leq 0; z_1 > 0. \end{aligned} \right\}, \quad (3.123в)$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d-1}{2}; z_3 + z_4 \leq \frac{d-1}{2}; \\ z_2 - z_3 &\leq \frac{d+1}{2}; z_3 \geq -1; z_2 \geq 0; \\ z_4 &\leq 1; z_1 > 0. \end{aligned} \right\}, \quad (3.123г)$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d-3}{2}; z_3 + z_4 \leq \frac{d-3}{2}; \\ z_3 - z_2 &\leq \frac{d-3}{2}; z_2 \leq -1; z_3 \geq 0; \\ z_4 &\geq 0; z_1 > 0. \end{aligned} \right\} \quad (3.123д)$$

$$\left. \begin{aligned} z_2 + z_4 &\leq \frac{d+1}{2}; -z_3 + z_4 \leq \frac{d-1}{2}; \\ z_3 + z_2 &\leq \frac{d-3}{2}; z_3 \leq -1; \\ z_2 &\geq 1; z_4 \geq 1; z_1 > 0. \end{aligned} \right\} \quad (3.123ж)$$

$$\left. \begin{aligned} -z_2 - z_4 &\leq \frac{d-3}{2}; z_3 - z_4 \leq \frac{d+1}{2}; \\ -z_2 - z_3 &\leq \frac{d-3}{2}; z_2 \leq 0; \\ z_3 &\leq -1; z_4 \leq -1; z_1 > 0. \end{aligned} \right\} \quad (3.123з)$$

$$\left. \begin{aligned} z_2 - z_4 &\leq \frac{d-1}{2}; -z_3 - z_4 \leq \frac{d-3}{2}; \\ z_2 - z_3 &\leq \frac{d-1}{2}; z_2 \geq 1; \\ z_3 &\leq 0; z_4 \leq 0; z_1 > 0. \end{aligned} \right\} \quad (3.123к)$$

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 (3.123б)

$$\left. \begin{aligned} \bar{Y}_5 &= \bar{Y}_2 - \bar{Y}_1; \bar{Y}_5(0; -1; \frac{d+1}{2}; \frac{-d+1}{2}); \\ \bar{Y}_3 + 2\bar{Y}_7 - \bar{Y}_1 &= \bar{Y}_7(-1; \frac{d-5}{2}; \frac{d+3}{2}; 1); \\ L(Y_i) &= 0; i = 5, 6, 7. \end{aligned} \right\} \quad (3.124)$$

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 (3.124)

$$\left. \begin{aligned} z_1 > 0; 0 \leq z_2 \leq \frac{d-5}{2}; \\ 1 \leq z_3 \leq \frac{d+3}{2}; z_4 \leq 0; \\ d \geq 7. \end{aligned} \right\} \quad (3.124a)$$

Віднімемо з нерівності (3.124) рівність (3.123б)

$$|z_1 + 1| - |z| + \frac{d-5}{2} - 2z_2 + \frac{d+3}{2} - 2z_3 + |z_4 - 1| - |z_4| \geq 0. \quad (3.124б)$$

Враховуючи обмеження (3.124a) і зауваживши

$$|z_1 + 1| - |z| = 1; \quad |z_4 - 1| - |z_4| = 1,$$

після підставлення зазначених різниць у вираз (3.124б) та простих перетворень, отримаємо третю з нерівностей (3.121в)

$$z_3 - z_4 \leq \frac{d+1}{2}.$$

Другу та першу з нерівностей (3.121в) можна вивести, використовуючи замість (3.124)

$$W(\bar{Z} - \varphi_6) \geq d, \quad W(\bar{Z} - \varphi_5) \geq d.$$

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:

$$\left. \begin{aligned} A_0 = L(\bar{Z}_1) &= A_1 \frac{d-1}{2} + \frac{5d-1}{2}; d \geq 5; \\ A_0 = L(\bar{Z}_2) &= A_1 \frac{d-1}{2} - A_3 \frac{d-1}{2} + 1; d \geq 7; \\ L(\bar{Z}_1) &> L(\bar{Z}_2). \end{aligned} \right\} \quad (3.124в)$$

З виразів (3.124в) 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 9. Визначити кількість кодових конструкцій, які задовольняють умові (3.118а) при $i = 3$, $d = 4$, $s = 7$, $m = 5$.

Користуючись табл. 3.5 для заданих параметрів m, i, s визначимо загальну кількість таймерних сигналів $N_p = 680$.

Згідно з виразом (3.121) значення коефіцієнтів A_i в рівнянні (3.118а) $A_3 = 1$ $A_2 = 3$ $A_1 = 5$ $A_0 = 12$. Число реалізацій, які відповідають умові (3.118а), буде $N_p(\sum A_i x_i = 0) = \frac{680}{12} \approx 56$.

3.2.5. Теорема 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

$$\begin{aligned} Q_1 : x_j &\geq 0; \quad j = 1, \dots, i; \\ Q_2 : \sum_{j=1}^i x_j &\leq n - is - 1, \end{aligned} \quad (3.125)$$

де $n = ms$.

Зазначені умови повинні використовуватись таким чином, щоб декодер міг за прийнятою послідовністю чисел однозначно відновити початкову інформацію. Розв'язання задачі синтезу кодуємого алгоритму подано в наступній лемі.

Теорема 7. Нерівності

$$\frac{1}{(i-1)!} \sum_{r=0}^{x_i} \prod_{t=0}^{i-2} (n - is - r + t + 1) - N(x) \leq 0 \quad (3.126)$$

та

$$\begin{aligned} &\frac{1}{(k-1)!} \sum_{r=0}^{x_k} \prod_{t=0}^{k-2} (n - is - r + t + 1) + \\ &+ \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-2} \left(n - is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right) - N(x) \leq 0, \end{aligned} \quad (3.127)$$

де $k = 1, \dots, i-1$ дають змогу однозначно надати всім членам $0 \leq N(x) < \binom{n-i(s-1)}{i}$ множину чисел (x_1, x_2, \dots, x_i) , які задовольняють обмеженням Q_1 й Q_2 .

Схема перетворення числа $N(x)$ у множину 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 коду-

вання, як множину чисел (x_1, x_2, \dots, x_i) . З урахуванням обмежень (3.125) складемо схему перетворення (див. послідовність) й визначення a_k , $k \in [1; i]$:

$$a_1 = n - is; \quad a_2 = \frac{1}{2!}(n - is + 1)(n - is); \quad (3.127a)$$

$$a_3 = \frac{1}{3!}(n - is + 2)(n - is + 1)(n - is); \quad (3.127б)$$

$$a_i = \frac{1}{i!}(n - is + (i - 1))(n - is + (i - 2)) \dots (n - is); \quad (3.127в)$$

$$a_k = \frac{1}{k!} \prod_{t=0}^{k-1} (n - is + t) = \frac{1}{(k-1)!} \sum_{r=0}^{n-is-1} \prod_{t=0}^{k-2} (n - is - r + t + 1). \quad (3.127г)$$

$N(x)$	$x(i)$	x_{i-1}	\dots	x_2	x_1	
0	0	0	\dots	0	0	} a_1
1	0	0	\dots	0	1	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
$n - is - 1$	0	0	\dots	0	$n - is - 1$	} a_2
$n - is$	0	0	\dots	1	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
$2(n - is) - 2$	0	0	\dots	1	$n - is - 2$	
$2(n - is) - 1$	0	0	\dots	2	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	} a_{i-1}
\vdots	0	0	\dots	$n - is - 1$	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	} a_i
\vdots	0	1	\dots	0	0	
\vdots	0	1	\dots	0	1	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
\vdots	0	1	\dots	0	$n - is - 2$	
\vdots	0	1	\dots	1	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
\vdots	0	$n - is - 1$	\dots	1	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
\vdots	1	0	\dots	0	0	
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	
$\binom{n-i(s-1)}{i} - 1$	$n - is - 1$	0	\dots	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 (3.127) верхня межа суми буде змінною величиною $x_i \in [0, n-is-1]$, то можна буде перейти до нерівності (3.126) і знайти елемент x_i множини чисел (x_1, x_2, \dots, x_i) . Вираз (3.127) складається з трьох членів. Перший, як і у виразі (3.126) – 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 8. Інформація, подана у вигляді десяткового числа $N(x)$, однозначно відновлюється за значеннями множини чисел (x_1, x_2, \dots, x_i)

$$N(x) = \sum_{\mu=1}^i \frac{1}{(\mu-1)!} \sum_{r=0}^{x_\mu} \prod_{t=0}^{\mu-1} \left(n-is - \sum_{v=\mu+1}^i x_v - r + t + 1 \right). \quad (3.128)$$

Доведення. Оскільки (x_1, x_2, \dots, x_i) відомі, то вираз (3.127) 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 9. 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 (3.125).

Теорема 10. 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 (3.127а ... 3.127г) в наступні рівності:

$$\begin{aligned} a_1 &= n - is; \\ a_2 &= \frac{1}{2!} (a_1^2 + 3a_1 + 2); \\ a_3 &= \frac{1}{3!} (a_1^3 + 6a_1^2 + 11a_1 + 6); \end{aligned}$$

$$\dots\dots\dots$$

$$a_i = \frac{1}{i!} \left(\sum_{k=0}^i S(i, k) a_1^k \right),$$

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 11. 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

$$\max \|L\| > \binom{ms - (i-1)(s-1)}{i-1}, \quad (3.129)$$

$$\max \|L\| > \binom{ms - (i+1)(s-1)}{i+1}. \quad (3.129a)$$

Доведення. Теорему буде доведено, якщо доведемо вирази (3.129), (3.129a).

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:

$$\left(\frac{m}{m+1+s}\right) \prod_{k=1}^{s-1} \left(1 + \frac{1}{1+(s-k)\frac{s+1}{ms}}\right) < 1. \quad (3.130)$$

Дослідимо (3.130) 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 (3.129).

Аналогічно для виразу (3.129а) 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 (3.129а) доведене. Для випадку, коли $(ms, s+1) = 1$, вірність виразів (3.129) і (3.129а) 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.

3.2.6. Теорема синтезу надлишкових ТСК

Основна задача при синтезі асиметричних таймерних кодів, які вправляють та виявляють помилки, полягає в тому, що необхідно знайти залежності вагових коефіцієнтів A_k ($k = 1, \dots, i$) та модуля A_0 для виразу $\sum A_i x_i = 0 \pmod{A_0}$ 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 12. Якщо коефіцієнти рівняння $\sum A_i x_i = 0 \pmod{A_0}$ визначені так, що

$$\begin{aligned} A_k &= (e_0 + 1)^{k-1}; & k \in \{1 \dots i\} \\ A_0 &= (e_0 + 1)^i \end{aligned} \quad (3.131)$$

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

$$\sum_{k=1}^i A_k \widehat{x}_k \equiv \sum_{k=1}^i A_k (x_k + e_k) \equiv \sum_{k=1}^i A_k e_k \pmod{A_0}, \quad (3.131a)$$

де $e_k \in [-e_0; e_0]$.

Припустимо $e_k = e_0$. Тоді з урахуванням (3.131) можна записати

$$\sum_{k=1}^i A_k e_0 \equiv e_0 \sum_{k=1}^i (e_0 + 1)^{k-1} \equiv (e_0 + 1)^i - 1 \pmod{A_0}. \quad (3.131б)$$

Аналогічно для $e_k = -e_0$ отримуємо

$$-\sum_{k=1}^i A_k e_0 \equiv -[(e_0 + 1)^i + 1] \equiv -A_0 + 1 \pmod{A_0}. \quad (3.41)$$

Беручи до уваги вирази, 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 викладень, 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:

$$\begin{aligned}
 e_1 \leq \left\lfloor \pm \frac{e_0}{2} \right\rfloor &\Rightarrow C_s \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right]; \\
 e_2 \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right], e_k = 0 (k = 3, \dots, i); \\
 e_2 = \mp 1 &\Rightarrow C_s \in \left[-\frac{3e_0}{2} - 1, -\frac{e_0}{2} - 1 \right] \cup \left[\frac{e_0}{2} + 1, \frac{3e_0}{2} + 1 \right] \\
 \dots\dots\dots &\dots\dots\dots \\
 e_2 = \mp \frac{e_0}{2} &\Rightarrow C_s \in \left[-\frac{e_0^2}{2} - e_0, -\frac{e_0^2}{2} \right] \cup \left[\frac{e_0^2}{2}, \frac{e_0^2}{2} + e_0 \right]; \\
 \dots\dots\dots &\dots\dots\dots \\
 e_k \in \left[-\frac{e_0}{2}, \frac{e_0}{2} \right] &; \\
 e_k = \mp 1 &\Rightarrow C_s \in \left[-\frac{3(e_0+1)^{i-1} - 1}{2}, -\frac{(e_0+1)^{i-1} + 1}{2} \right] \cup \left[\frac{(e_0+1)^{i-1} - 1}{2}, \frac{3(e_0+1)^{i-1} + 1}{2} \right] \\
 \dots\dots\dots &\dots\dots\dots \\
 e_k = \mp \frac{e_0}{2} &\Rightarrow \\
 \Rightarrow C_s \in \left[-(e_0+1)^i + 1, -\frac{(e_0-1)(e_0+1)^{i-1} + 1}{2} \right] \cup \left[\frac{(e_0-1)(e_0+1)^{i-1} + 1}{2}, (e_0+1)^i - 1 \right].
 \end{aligned}$$

Отже, показано, що $C_s \in [-(e_0 + 1)^i, (e_0 + 1)^i - 1]$ 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 остач $A_0 - 1$, і код виправляє помилки величини $[-(e_0 - 1), (e_0 - 1)]$ вагою $W(\vec{E}) \leq e_0 - 1$. Висновок доведено.

Теорема 13. Якщо коефіцієнти A_k рівняння $\sum A_i x_i = 0 \pmod{A_0}$ визначено таким чином, що

$$\begin{aligned} A_k &= (2e_0 + 1)^{k-1}; & k \in \{1 \dots i\}, \\ A_0 &= (2e_0 + 1)^i, \end{aligned} \quad (3.132)$$

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 $\vec{\hat{X}}(\hat{x}_1, \hat{x}_2, \dots, \hat{x}_i)$, за умови $\sum A_i x_i = 0 \pmod{A_0}$ та виразу (3.131а) 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 :

$$\frac{\sum A_k e_k}{A_0} = Z + C_s, \quad (3.133)$$

де Z — ціле число, C_s — остача від ділення.

Визначимо потрібне число різних остач за модулем A_0 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, тобто ЗМВ за-

лишився в «своїй» зоні Δ). Таким чином, число різних синдромів, що відповідають різним виправленим помилкам, буде дорівнювати

$$N_c = (2e_0 + 1)^i.$$

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 дорівнювати 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

$$A_2 = 2e_0 + 1.$$

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

$$A_3 = 2C_{1+2} + 1 = 4e_0(e_0 + 1) + 1.$$

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 для A_4 отримаємо

$$A_4 = 8e_0^3 + 12e_0^2 + 6e_0 + 1 = (2e_0 + 1)^3. \quad (3.133a)$$

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 правилом (3.132).

На основі сказаного можливо установити взаємозв'язок між коефіцієнтами A_k та потрібною кодовою відстанню d_x у матриці Хеммінга.

У табл. 3.7 подано значення параметрів таймерного коду з трьома ЗММ за різних величин виправлених помилок e_0 : коефіцієнти A_k та мінімальна кодова відстань d_{\min} . Значення d_{\min} визначені, виходячи із коефіцієнтів A_k , у відповідності з виразами (3.122) та (3.133). Для порівняння в правій колонці табл. 3.7 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 відстань d_0 будуть такими:

$$\left. \begin{aligned} t_{\kappa} &= i \cdot e_0 \\ d_0 &= 2t_{\kappa} + 1 = 2i \cdot e_0 + 1 \end{aligned} \right\} \quad (2.134)$$

Порівнюючи d_{\min} та d_0 , бачимо, що за умови розподілу помилок рівномірно в сигнальній конструкції за одного й тому ж самого значення виправленої помилки можна зменшити кодову відстань більш ніж у два рази.

Таблиця 3.7 – 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:

$$A_0 = 2 \sum_{k=1}^i A_k + 1. \quad (3.135)$$

Аналіз наведених міркувань може привести до питання про доцільність використання таймерних кодів, які виправляють помилки зміщення замість кодів, що виявляють ці зміщення за більшого значення Δ . Для відповіді на це питання розглянемо табл. 3.8, в якій наведено значення числа реалізацій сигнальних конструкцій на різних інтервалах часу i за різних значень s для таких кодів:

1. Число сигнальних конструкцій, які реалізовані на інтервалі $T = mt_0$ при $s = 3$ та відповідають умові $\sum A_i x_i = 0 \pmod{A_0}$ при $d = 3$, $A_1 = 1$, $A_2 = 2$, $A_3 = 3$, $A_0 = 7$.

2. Число реалізацій сигнальних конструкцій на інтервалі $T = mt_0$ при $s = 9$, у відповідності з умовою $\sum A_i x_i = 0 \pmod{A_0}$ та виправленні помилок кратності $i = 3$ величини $e_0 = 1$. 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 $T = mt_0$ при $s = 9$, у відповідності з умовою $\sum A_i x_i = 0 \pmod{A_0}$ та виправленні 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 $T = mt_0$ при $s = 15$, у відповідності з умовою $\sum A_i x_i = 0 \pmod{A_0}$ та виправленні поми-

лок 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 $T = mt_0$ при $s = 15$, у відповідності з умовою $\sum A_i x_i = 0 \pmod{A_0}$ та виправленні 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 3.8 – 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	55	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 взяте 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 будуть рівними.

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. Використовувати виправлення i -кратних помилок величиною $e_0 = 2$ за нерівномірного їх розподілу у межах сигнальної конструкції недоцільно, тому що потужність множини дозволених сигналів зменшується (код № 4). У той самий час за рівномірного розподілу помилок у межах сигнальної конструкції потужність множини на заданому інтервалі можливо суттєво збільшити (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 $\forall e_0 > 0$

$$2e_0 (2e_0 + 1)^{i-1} < \frac{1}{2} \left((2e_0 + 1)^i + 1 \right) \quad (3.136)$$

і при $A_i \geq \sum_{k=1}^{i-1} A_k$ нерівність виконується в усіх інших випадках. Тим самим висновок доведено.

Висновок 2. Синдром помилки C_s кратності меншої або рівної i величиною $[-e_0, e_0]$ визначається як

$$\begin{aligned}
C_{i-1} &= \left\lfloor \frac{C_i}{2e_0 + 1} \right\rfloor, & e_i' &= R_{(2e_0+1)}(C_i); \\
C_{i-2} &= \left\lfloor \frac{C_{i-1}}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^2} \right\rfloor, & e_{i-1}' &= R_{(2e_0+1)}\left(\frac{C_i}{2e_0 + 1}\right); \\
&\dots\dots\dots & & \dots\dots\dots \\
C_2 &= \left\lfloor \frac{C_3}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^{i-1}} \right\rfloor, & e_2' &= R_{(2e_0+1)}\left(\frac{C_i}{(2e_0 + 1)^{i-2}}\right); \\
C_1 &= \left\lfloor \frac{C_1}{2e_0 + 1} \right\rfloor = \left\lfloor \frac{C_i}{(2e_0 + 1)^i} \right\rfloor, & e_1' &= R_{(2e_0+1)}\left(\frac{C_i}{(2e_0 + 1)^{i-1}}\right)
\end{aligned}$$

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 $\bar{e}_k = e_0 - e_k'$, то висновок доведено.

3.2.7. Ефективність наднайквістової швидкості модуляції

Оцінимо ефективність використання ТСК на прикладах використання їх для різних систем передачі.

Приклад 10. Оцінимо ефективність перетворення якості передавання в бінарному каналі 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

$$h_{\Omega}(t) = \frac{1}{2\pi} \int_{-\Omega}^{\Omega} H_{\Omega}(\omega) e^{i\omega t} d\omega. \quad (3.137)$$

Якщо на вхід такого каналу подати сигнал, що являє собою δ -імпульсну послідовність, то на його виході дістанемо напругу

$$z(k) = \sum_{l=-\infty}^{\infty} x_l h_{\Omega}(k-l), \quad k = 0; \pm 1; \dots, \quad H(\omega) = \begin{cases} 1 & |\omega| \leq \pi \\ 0 & |\omega| > \pi \end{cases}. \quad (3.138)$$

Отже, сигнал помилки при передаванні корисного сигналу визначається виразом

$$z(k) = \sum_{l=-\infty}^{\infty} x_l u(k-l) - \sum_{l=-\infty}^{\infty} x_l h_{\Omega}(k-l) = \sum_{l=-\infty}^{\infty} x_l [u(k-l) - h_{\Omega}(k-l)], \quad (3.139)$$

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

$$h_{\Omega}(0) = 1, \quad (3.140)$$

$$\frac{1}{2\pi} \int_{-\Omega}^{\Omega} H_{\Omega}(\omega) d\omega = 1. \quad (3.141)$$

Останнє співвідношення очевидно виходить із виразів (3.140) та (3.137).

Припустимо, що випадкова інформаційна послідовність $x(K)$ є стандартною в широкому розумінні і має автокореляційну функцію, чи, точніше, автокореляційну послідовність

$$B(m) = M \{x_n, x_{n+m}\}, \quad m = 0, \pm 1, \dots, \quad (3.142)$$

де M - операція усереднення за множиною реалізацій та нульовим математичним сподіванням. Енергетичний спектр (спектр густини потужності) розглядуваної випадкової залежності дорівнює

$$P(e^{i\omega}) = \sum_{m=-\infty}^{\infty} B(m) e^{-i\omega m}, \quad -\pi \leq \omega < \pi. \quad (3.143)$$

Відповідно до відомих співвідношень для перетворення енергетичного спектра лінійною системою та формулою (1.139), спектр густини потужності випадкової послідовності

$$Q(e^{i\omega}) = P(e^{i\omega}) |\sigma(e^{i\omega})|^2, \quad (3.144)$$

де

$$\sigma(e^{i\omega}) = \sum_{k=-\infty}^{\infty} [u(k) - h_{\Omega}(k)] e^{-i\omega k} = 1 - \sum_{k=-\infty}^{\infty} h_{\Omega}(k) e^{-i\omega k} = 1 - H_{\Omega}(e^{i\omega}), \quad (3.145)$$

$$-\Omega \leq \omega \leq \Omega$$

Причому, як відомо, спектр відліків імпульсної реакції

$$H_{\Omega}(e^{i\omega}) = \sum_{p=-\infty}^{\infty} H_{\Omega}(\omega - p2\pi). \quad (3.146)$$

Оскільки дисперсію випадкової послідовності можна знайти діленням на 2π її енергетичного спектра, дисперсія міжсимвольної завади, що нас цікавить, обчислюється за допомогою наступного співвідношення, що впливає з рівностей (3.143) та (3.145):

$$\sigma_z^2 = \frac{1}{\pi} \int_{-\pi}^{\pi} Q(e^{i\omega}) d\omega = \frac{1}{2\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) \left[1 - \sum_{p=-\infty}^{\infty} H_{\Omega}(\omega - p2\pi) \right]^2 d\omega. \quad (3.147)$$

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 (3.147) можна перетворити до вигляду

$$\sigma_z^2 = \frac{1}{2\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) [1 - H_{\Omega}(\omega)]^2 d\omega \quad (3.148)$$

З урахуванням парності підінтегрального виразу з формули (3.148) та смугової обмеженості $H_{\Omega}(\omega)$, можемо записати остаточно

$$\sigma_z^2 = \frac{1}{\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) [1 - H_{\Omega}(\omega)]^2 d\omega + \frac{1}{\pi} \int_{-\pi}^{\pi} P(e^{i\omega}) d\omega. \quad (3.149)$$

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

$$B(\tau) = e^{-2\lambda|\tau|}, \quad -\infty < \tau < \infty, \quad (3.150)$$

де λ_0 – середнє число перетинів нульового рівня за одиницю часу.

Енергетичний спектр

$$P(\omega) = \int_{-\infty}^{\infty} B(\tau) e^{-i\omega\tau} d\tau = \frac{4\lambda_0}{4\lambda_0 + \omega^2}; \quad -\infty < \omega < \infty. \quad (3.151)$$

Оскільки кореляційна послідовність відліків випадкового телеграфного сигналу має вигляд $B(m) = e^{-2\lambda|m|}$, $m = 0, \pm 1, \dots$, а її дискретне перетворення Фур'є (спектр густини потужності)

$$P(e^{i\omega}) = \sum_{p=-\infty}^{\infty} P(\omega - p2\pi) = \frac{4\lambda_0}{4\lambda_0 + (\omega - p2\pi)^2} \sum_{p=-\infty}^{\infty}, \quad -\pi \leq \omega < \pi, \quad (3.152)$$

то можна показати, що

$$\sigma_{z_1}^2 = \frac{(1 - \pi/\Omega)^2}{\pi\lambda_0} \int_0^{\Omega} \sum_{p=-\infty}^{\infty} \frac{1}{1 + \left[\frac{\omega - p2\pi}{2\lambda_0} \right]^2} d\omega + \frac{1}{\pi\lambda_0} \int_{\Omega}^{\infty} \sum_{p=-\infty}^{\infty} \frac{1}{1 + \left[\frac{\omega - p2\pi}{2\lambda_0} \right]^2} d\omega. \quad (3.153)$$

При розрахунках за формулою (3.153) з'являється похибка через скінченні значення членів суми, яку визначають за виразом

$$\xi^2(n) = \frac{(1-\pi/\Omega)^2}{\pi\lambda_0} \int_0^\Omega \frac{2\lambda_0^2}{\pi^2} \left(\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right) d\omega + \frac{1}{\pi\lambda_0} \int_\Omega^\pi \frac{2\lambda_0}{\pi^2} \left(\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right) d\omega =$$

$$= \frac{2\lambda_0(\pi-\Omega)}{\pi^2\Omega} \left[\frac{\pi^2}{6} - \sum_{p=1}^n \frac{1}{p^2} \right]. \quad (3.154)$$

Амплітуда міжсимвольної завади визначається

$$u_{мз} = \sqrt{\sigma_z^2}. \quad (3.155)$$

Величина $\frac{\pi}{\Omega} = \mu$ показує, у скільки разів швидкість передавання посилає більша за найквістову граничну швидкість для даного каналу.

Абсолютне значення похибки для дисперсії, яку визначають за виразом (3.155), становить 5 ... 10%.

Результати розрахунків σ^2 та $u_{мз}$ при $\lambda = 0,4$ за формулами (3.139) та (3.141) 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, викликаной позанайквістовою швидкістю передавання, зменшенням сигналу в $\sqrt{\mu}$ разів, відношення сигнал/завада

$$h^* = \frac{u_c}{\sqrt{\mu(u_3^2 + u_{мз}^2)}}. \quad (3.156)$$

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. 3.24).

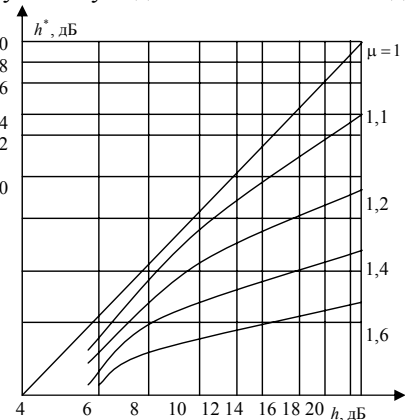


Рисунок 3.24 – Вплив флукуційного шуму на момент спрацьовування безінерційного реле

Наслідком зниження величини відношення сигнал/шум є зменшення завадостійкості переданої інформації. На графіках рис. 3.25 показано залежність ймовірності помилкового приймання елемента p_e , визначену для двійкової системи передавання з ЧМ за когерентного приймання відповідно до виразу

$$p_e = \lfloor 1 - \Phi(h^*) \rfloor, \quad (3.157)$$

де $\Phi(h^*)$ – функція Крампа. На рис. 3.25 показана залежність ймовірності помилки елемента за рахунок його скорочення в μ разів, а на рис. 3.26 – з урахуванням міжсимвольних спотворень при зростанні μ [12].

Передаванню зі швидкістю, яка дорівнює граничній швидкості Найквіста, відповідає лінія $p_n = f(p_n(\mu = 1))$.

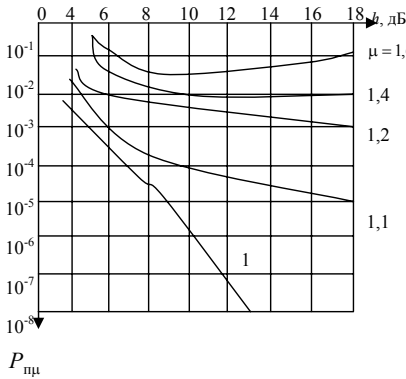


Рисунок 3.25 – Графік залежності ймовірності помилкового приймання елемента

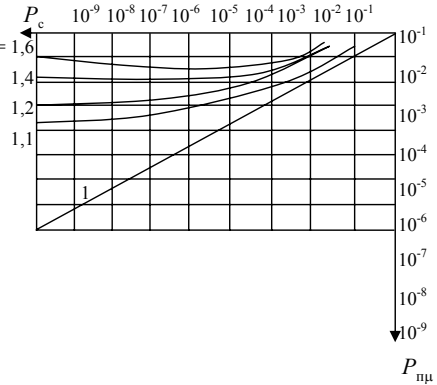


Рисунок 3.26 – Графік залежності ймовірності помилки елемента

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 сформувати на тому самому часовому інтервалі, що й раніше, більшу кількість реалізацій, тобто утворити можливості для збільшення пропускнуої здатності каналу:

$$C = \mu \left[1 + p_n \log_2 p_n + (1 - p_n) \log_2 (1 - p_n) \right]. \quad (3.158)$$

На рис. 3.27 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 пропускнуої 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 завадостійкос-

ті. 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 коректуючі здатності коду.

У табл. 3.9 подано значення параметрів $n(\mu)$, r , d_{\min} та t_v надлишкових кодів для різних значень μ [37].

Таблиця 3.9 – 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_v	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,

$$p_{\text{пц}} = \sum_{i=d_{\min}}^{n(\mu)} C_{n(\mu)}^i p_{\text{пц}}^i (1-p_{\text{пц}})^{n(\mu)-i}, \quad (3.159)$$

а для кодів, що виправляють помилки кратності $t_{\text{вп}}$,

$$p_{\text{пц}} = \sum_{i=t_{\text{вп}}+1}^{n(\mu)} C_{n(\mu)}^i p_{\text{пц}}^i (1-p_{\text{пц}})^{n(\mu)-i}. \quad (3.160)$$

На рис. 3.28 показана залежність швидкості передавання R^k від μ з урахуванням числа надлишкових елементів згідно з табл. 3.9.

Як бачимо, застосування кодів, що виправляють помилки за рахунок найквістової швидкості модуляції, зменшує ймовірність помилкового приймання елемента, але не компенсує втрату завадостійкості повністю.

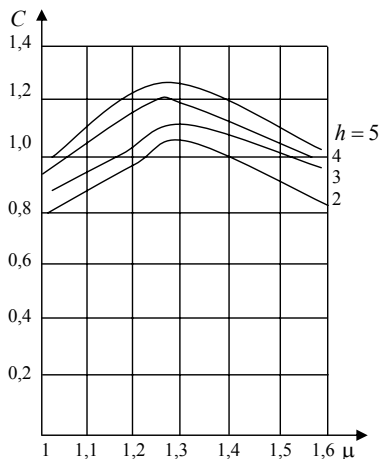


Рисунок 3.27 – Залежності $C = f(\mu)$

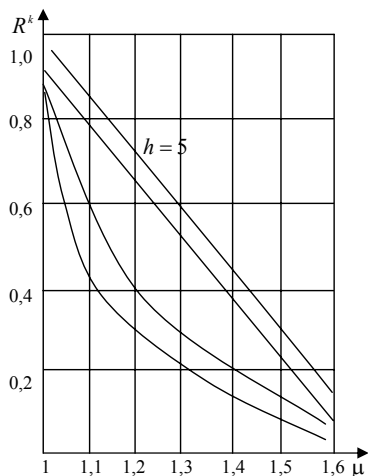


Рисунок 3.28 – Графіки залежностей $R^k = f(\mu)$

Таким чином, застосування понаднайквістової швидкості модуляції з метою збільшення швидкості передавання не дає бажаного ефекту завдяки виникненню додаткової завади у вигляді міжсимвольної інтерференції.

3.2.8. Ефективність використання ТСК для трансформації якості у швидкість передавання

Для оцінки ефективності використання таймерних сигналів для трансформації якості приймання у швидкість передавання інформації знайдемо зону Δ , яку необхідно забезпечити при синтезі ТСК для отримання ймовірності помилкового приймання $P_{пт}$ більше ніж при використанні надлишкової швидкості модуляції P_n ($P_t < P_n$).

Приклад 11. Вважаючи, що в каналі зв'язку з ЧМ, як і в попередньому прикладі, існує гауссівський шум із параметром $h = \frac{u_c}{u_3} = 8$. При збіль-

шенні швидкості модуляції на 25 % (при базі сигналу $B = \Delta F t_0 = 1$) за рахунок додаткових міжсимвольних завад нове співвідношення значення $h^* = 3$ (див. рис. 3.24). Оцінімо величину втрат якості передавання.

Зважаючи на те, що інтеграл імовірності апроксимують з похибкою $\delta < 0,02$ виразом

$$\Phi(z) = 0,5 - 0,65 \exp[-0,44(z + 0,75)^2] \quad (3.161)$$

для ймовірності помилкового приймання одного елемента при РЦК маємо

$$P_e = 0,65 \exp \left[-0,44(z + 0,75)^2 \right]. \quad (3.162)$$

Для $h=7$ отримаємо $P_e = 10^{-12}$, а для $h^* = 3$ за наднайквістової швидкості $P_{ен} = 1,4 \cdot 10^{-3}$ (де P_e і $P_{ен}$ – ймовірності помилки при найквістової і наднайквістової швидкості відповідно).

Зважаючи на те, що за нормального закону зміщення ЗМВ ймовірність помилкового приймання одного внаслідок відхилення його за величину $\Delta/2$ ($\Theta > \Delta/2$) не повинна перевищувати $P_{ен}$ отримаємо

$$P(\Theta) > \Delta/2 = 0,5 - \Phi(\Delta/2) \leq P_{ен},$$

$$\Phi(\Delta/2) = \frac{1}{\sqrt{2\pi}\sigma_3} \int_0^{\Delta/2} e^{-z^2/2\sigma_3^2} dz. \quad (3.163)$$

У зв'язку з тим, що в каналі з ЧМ $\sigma_3 = 1/4h$, то є можливість оцінити величину зони Δ . Враховуючи вирази (3.163) легко показати, що для каналу з $h=8$ $\sigma_3 = \frac{1}{4 \cdot 8} = 3,125\%$ для отримання нерівності $P(\Delta/2) \leq P_{ен} \approx 1,4 \cdot 10^{-3}$ достатньо вибрати зону $\Delta = 0,2t_0$ ($s=5$), яка забезпечить ймовірність помилкового приймання одного ЗМВ – $P_{зм}^{(1)} = 1,45 \cdot 10^{-3}$.

У табл. 3.10 наведено число реалізацій таймерних сигнальних конструкцій та середнє значення числа ЗМВ за різних значень $s \in (1...30)$ для двох значень довжини конструкції $T_c = 8t_c$; $T_c = 10t_0$.

Таблиця 3.10 – Кількість реалізацій ТСК для $m \in 8, 10$ при $s \in (1...30)$

$\begin{matrix} s \\ m \end{matrix}$	1	2	3	4	5	10	15	20	25	30
8	255	1596	5895	16492	38739	735450	4952841	20628612	64825462	$1,69 \cdot 10^8$
	4,02	4,3	4,5	4,67	4,76	5,11	5,3	5,49	5,52	5,596
10	1023	10945	58424	217224	644760	27042520	$3,02 \cdot 10^8$	$1,83 \cdot 10^9$	$7,787 \cdot 10^9$	$2,6 \cdot 10^{10}$
	5	5,4	5,67	5,85	6	6,44	6,68	6,83	6,96	7,05

Із таблиці видно, що при передаванні байта ($m=8$) при $s=5$ можна реалізувати 38739 сигнальних конструкцій, які відповідають 15-елементним бінарним кодовим словам $E^-(\log_2 38739) = 15$.

У зв'язку з тим, що за наднайквістової швидкості з коефіцієнтом 1,25 на інтервалі ($T_c = 8t_0$) можна сформулювати всього $(8 \times 1,25) = 12$ -елементні кодові слова, а при ТСК – 15-елементні, тоді формування ТСК більш ефективно за критерієм швидкості передавання.

Приклад 12. Для розрахування параметрів таймерного коду порівняємо ймовірності вірного приймання кодових слів за наднайквістової швидкості передавання і ТСК.

Вважаючи, що суми гауссівської завади та міжсимвольних спотворень описується нормальним законом, ймовірність вірного приймання при передаванні з наднайквістовою швидкістю буде

$$P_{\text{вн}} = (1 - P_{\text{ен}})^{n^*} = (0,9985)^{12} = 0,982,$$

де n^* – число елементів у кодовім слові на інтервалі байта за наднайквістової швидкості.

При ТСК інформація міститься в числі ЗММ кодової конструкції та місцях їх розміщення. Тому що середнє число ЗММ на інтервалі $T_c = 8 t_c$ при $s = 5$ дорівнює $\bar{i} = 4,76$, то

$$P_{\text{вт}} = (1 - P_{\text{зм}})^{4,76} = 1 - 1,45 \cdot 10^{-3} = 0,993.$$

Порівнюючи $P_{\text{вн}}$ і $P_{\text{вт}}$ бачимо, що при ТСК не тільки швидкість передавання більше в 1,25 разів $\left(\frac{15}{12}\right)$, а й ймовірність вірного приймання.

Приклад 13. Порівняємо характеристики передавання для цього ж каналу за наднайквістової швидкості передавання сигналів ТСК для $\Delta = 0,25t_0$ ($s = 4$).

Згідно з табл. 3.10 видно, що число реалізацій при $s = 4$ і $m = 8$, $N_p = 16492$, що відповідає 14-елементному кодовому слову ($\log_2 16492 = 14$).

Ймовірність зміщення одного ЗМВ ($P_{\text{зм}}^{(1)}$) за величину зони $\Theta > 0,25 t_0$

$$P_{\text{зм}}^{(1)} = 2 \left(0,5 - \Phi \left(\frac{25}{2 \cdot 34} \right) \right) = 2 [0,5 - \Phi(3,787)] = 1,6 \cdot 10^{-4}.$$

Ймовірність вірного приймання ТСК буде дорівнювати

$$P_{\text{вт}} = (0,99984)^{\tau} = (0,99984)^{4,67} = 0,9992.$$

Із результатів розрахунків видно, що зменшення швидкості передавання при ТСК $\left(\frac{15}{14}\right)$ на 7% на передавання суттєво збільшує функцію правдоподібності приймання конструкцій.

Розглянемо ефективність використання ТСК в реальних каналах. З метою оцінки параметрів реальних нестационарних каналів зв'язку оцінимо результати експерименту, наведені в прикладі 14.

Приклад 14. Як реальний канал при експерименті використовувався канал комутованої телефонної мережі загального користування. На прийомі фіксувалася кількість переданих конструкцій, кількість вірно прийнятих конструкцій, кількість конструкцій зі зміною числа ЗМВ, кількість кодових слів зі зміщенням окремих ЗМВ і величиною змін, номери помилкових кодових слів і довжини окремих відрізків сигналу, якість приймання десяти кодових слів після помилкового слова, інтервал між спотвореними ТСК.

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 перевірки ефективності виправлення частини помилок синдромним методом для ТСК і надлишковим РЦК, була реалізована система з базовим елементом $\Delta = 0,14t_0$ ($s = 7$) на інтервалі одного байта $T_c = 8t_0$. При синтезі сигнальних конструкцій як вагові коефіцієнти вибрані:

$$A_1 = 1; A_2 = 3; A_3 = 9; A_0 = 27.$$

Статистичні дані одного фрагмента передавання такі:

- 1) число переданих кодових слів ТСК – 73676;
- 2) число помилкових кодових слів ТСК при прийманні 834;
- 3) число вірно виправлених помилкових ТСК синдромним методом – 731 (всі зі зміщенням одного ЗМВ);
- 4) число невірно виправлених кодових слів ТСК синдромним методом – 103.

Слід зауважити, що при реєстрації були зафіксовані сигнали всіх 834 кодових конструкцій з частотою аналізу – 7 строб на один елемент Δ .

Для можливості використання рівняння якості $\sum A_i x_i = 0 \pmod{A_0}$ з наведеними коефіцієнтами (за умови передавання одного байта $m = 8$) необхідно було реалізувати $2^m \cdot 27 = 6912$ сигнальних конструкцій. В зв'язку з тим, що на інтервалі $T_c = 8t_0$ при $s = 7$, $i = 3$ можливо отримати 8436 кодових слів, що на 1529 більше необхідного, то для отримання $2^8 \cdot 27$ конструкцій достатньо було взяти $T_c = 7,7$ елементів.

Структура помилкових ТСК наведена нижче.

Кодові слова з помилкою в прийманні одного ЗМВ:

$$\begin{aligned} |x|0|0| &= \Delta|1|2|3| = |38|4|4| \\ |0|x|0| &= \Delta|1|2|3| = |28|1|0| \\ |0|0|x| &= \Delta|1|2|3| = |218|7|2|. \end{aligned}$$

Кодові слова з помилкою в прийманні двох ЗМВ:

$$\begin{aligned}
 |x|x|0| &= \Delta|1|2|3| * |1|2|3| = |92|6|7| * |93|5|7| \\
 |0|x|0| &= \Delta|1|2|3| * |1|2|3| = |20|1|2| * |2|2|0| \\
 |0|0|x| &= \Delta|1|2|3| * |1|2|3| = |107|6|1| * |105|7|2|.
 \end{aligned}$$

Кодові слова з помилкою в прийманні трьох ЗМВ:

$$|x|x|x| = \Delta|1|2|3| * |1|2|3| * |1|2|3| = |44|8|5| * |42|7|8| * |49|2|6|,$$

де $|x|$ – означає місце помилки; Δ – число ЗМВ, які змістились на відповідну величину; z – кількість помилок.

Вважаючи, що отримані помилкові кодові слова зі зміщенням одного ЗМВ на величину 1Δ (кількістю 731) отримані за «хорошого» стану каналу, то легко визначити середнє значення квадратичного відхилення σ змішень ЗМВ

$$\begin{aligned}
 2 \left(0,5 - \Phi \left(\frac{\Delta}{2\sigma_3} \right) \right) &= \frac{731}{4 \cdot 73676} = 2,4 \cdot 10^{-3}, \quad \Phi \left(\frac{14}{2\sigma_3} \right) = 0,4976, \\
 \frac{0,14}{2\sigma_3} &= 2,95, \quad \sigma_3 = 0,0237.
 \end{aligned}$$

Враховуючи, що ресстрація з кожної зони Δ проводилась методом відрахунку по відношенню до початку ТСК, то

$$\sigma_0 = \frac{\sigma_3}{\sqrt{2}} = 0,017.$$

Зважаючи на те, що для каналу з ЧМ $\sigma_3 = 1/4h$, то співвідношення сигнал/завада (h) в «хорошому» стані буде дорівнювати

$$h = \frac{1}{4 \cdot 0,017} = 14,7, \quad \text{тобто } h^2 > 100,$$

що відповідає моделі Гільберта каналу з двома станами.

За такого значення σ_0 ймовірність зміщення ЗМВ на величину $\Theta \geq 2\Delta$ повинна бути

$$P(\Theta \geq 1,5\Delta) = 2 \left[0,5 - \Phi \left(\frac{1,5\Delta}{\sigma} \right) \right] < 10^{-8}.$$

Проведена ресстрація всіх спотворених ТСК дала можливість виявити розміщення помилкових кодових слів у блоці з 10 ТСК: помилкове одне кодове слово із 10 – 83%; помилкових кодових слів два підряд – 13%; помилкових два кодових слова із 10, але через одне – 4%. Аналіз отриманої статистики дозволяє розрахувати середню тривалість інтервалу між помилковими кодовими словами $\bar{T} = 1700$ мс. Виходячи з інтервалу між помилковими словами було визначено алгоритм повторення одного і того ж самого слова. Мінімальну ймовірність помилки можливо отримати при повторенні через два слова. У цьому випадку вимагається тільки виявляти помилки ТСК, що дозволяє збільшити швидкість передавання.

Аналіз 103 невірно виправлених кодових слів показав, що після синдромного виправлення всі кодові слова задовольняли рівнянню якості, але не відповідали переданим кодовим словам. Для прикладу, наведемо одне з кодових слів, в якому моменти модуляції передавання знаходились на відстанях – 12Δ , 23Δ , 21Δ , а на прийманні отримана конструкція з моментами модуляції 12Δ , 8Δ , 14Δ . Пов'язане це з тим, що два вектори помилок, один з яких E_1 табличний і має координати не більше одиниці, а другий E_2 , який в сумі з E_1 дає нульовий вектор E_0 , мають одне і те ж саме числове надання синдромів:

$$\begin{aligned} E_1 + E_2 = E_0, \quad E_{01} = 0; \pm 3; \mp 1, \\ E_0 - E_1 = E_2, \quad E_{02} = \pm 3; \mp 1; 0. \end{aligned}$$

Оцінимо ефективність використання ТСК для компенсації надлишковості в блокових кодах.

Приклад 15. Оцінимо структуру таймерної сигнальної конструкції при використанні коду Слепяна (9,5) в каналі Гільберта.

Нагадаємо, що код Слепяна (9,5) синтезовано на інтервалі $n = 9$ для $m = 5$ при $d = 3$. Код дозволяє виправляти одноразові помилки. На жаль на один інформаційний елемент припадає 0,8 елементів перевірючих, що суттєво знижує кодову швидкість передавання.

Для оцінки ефективності компенсації надлишковості коду при передаванні ТСК, будемо вважати що $\Delta = 0,2t_0$ ($s = 5$). Вважатимемо, що величина середньоквадратичного відхилення ЗМВ розрахована раніше $\sigma_0 = 0,017 < 0,02$. Тому що для виправлення двократних помилок кодова відстань повинна дорівнювати $d = 5$, а число перевірючих елементів 8, то для синтезу 2^{13} реалізацій ТСК можна взяти всі сигнальні конструкції на інтервалі $T_c = 6,7 t_0$ при $i \in \overline{1...6}$ ($N_{p\Sigma} = 9494$) (див. табл. 3.5).

Знаючи значення σ_0 і Δ розрахуємо ймовірність помилкового приймання одного ЗМВ $P_{\text{пн}}$ для «хорошого» стану каналу

$$P_{\text{пн}}^{(1)} = 2 \cdot \left[0,5 - \Phi \left(\frac{20}{2 \cdot 0,02} \right) \right] = 5,8 \cdot 10^{-7}.$$

Отже ймовірність вірного приймання одного $P_{\text{вп}}^{(1)}$ ЗМВ у сигнальній конструкції ТСК при «хорошому» стані $P_{\text{вп}}^{(1)} = 1 - P_{\text{пн}} = 0,99999942$.

Оскільки використовуються сигнальні конструкції з різним числом ЗММ $i \in (1...6)$, то середнє значення $\bar{i} = \frac{\sum_{i=1}^m i \cdot C_{mS-i}^{i(S-1)}}{\sum_{i=1}^m C_{mS-i}^{i(S-1)}}$ і становить

4 ($8 \bar{i} = 4$), тоді ймовірність вірного приймання конструкції:
 $P_{\text{вп}} = (0,99999942)^4 = 0,9999976$.

Зважаючи на те, що сигнальна конструкція ТСК несе інформацію про 13-елементні комбінації РЦК, то ймовірність вірного приймання одного елемента після перекодування ТСК в РЦК (у «хорошому» стані каналу) буде

$$P_{\text{е вп}} = \sqrt[13]{P_{\text{вп}}} = 0,999999875.$$

Ймовірність помилкового приймання елемента в «хорошому» стані після перекодування ТСК в РЦК буде $P_{\text{е}}^* = 2 \cdot 10^{-7}$.

Враховуючи те, що ця ймовірність більш ніж на чотири порядки менше ймовірності помилкового приймання елемента за розрядно-цифрового кодування ($P_{\text{е р}} \approx (1,8 \dots 2,3) \cdot 10^{-3}$), слід припустити, що сумарна ймовірність після перетворення ТСК в РЦК буде менша. Викликано це тим, що конструкції ТСК формуються на інтервалі $T_{\text{с}} = 6,7 t_0$ замість 13-елементних при РЦК $\left(k = \frac{6,7}{13} = 0,515\right)$. Отже, ймовірність «поганого» стану каналу на інтервалі одного ТСК в 2 рази менше порівняно з РЦК. За наявності кодового перемежувача помилки на виході будуть практично незалежними.

Враховуючи те, що 13-елементний код виправляє помилки кратності 2 – загальна ймовірність правильного приймання комбінації дорівнює сумі ймовірностей того, що всі тринадцять елементів прийнято вірно або що з тринадцяти елементів невірно прийнято не більше двох елементів:

$$P_{\text{пр}} = (0,999999875)^{13} + 13 \cdot (0,999999875)^{12} \cdot 0,001 + \\ + 78 \cdot (0,999999875)^{11} \cdot 10^{-6} = 0,9999996.$$

Для порівняння з ймовірністю вірного приймання первинного коду розрахуємо значення еквівалентної ймовірності $P_{\text{е р}}$ вірного приймання, при РЦК враховуючи, що інформаційних елементів в початковому кодовому слові $m = 5$:

$$P_{\text{е р}} = \sqrt[5]{0,9999996} = 0,9999999, \\ P_{\text{е в}} = 1 - P_{\text{е п}} = 10^{-7}.$$

Таким чином, результати розрахунку підтверджують, що за рахунок використання ТСК можна проводити компенсацію надлишковості 13-елементного коду з $d = 5$, побудованої на базі коду Слепяна (9,5), знизити ймовірність помилкового приймання на чотири порядки і підвищити кодову швидкість майже вдвічі (з 5/13 до 5/6,7).

Приклад 16. Отримані в прикладі 14 параметри спотворень таймерних сигналів дають можливість оцінити доцільність перетворення якості передавання в швидкість у каналі моделі Гільберта. Зрозуміло, що коли мова йде тільки про швидкість передавання в нестационарному каналі, то мається на увазі, що середня ймовірність помилкового приймання кодового слова буде не більше ніж при РЦК. Тому що швидкість передавання визначається кількістю реалізацій на інтервалі T_c , задовольняючих умовам якості, то доцільно використовувати КС без виправлення зміщень ЗМВ, тому що вибір виправляючих зміщення ЗМВ суттєво впливає на їх кількість на заданому інтервалі реалізацій.

Слід зауважити, що при проведенні експерименту до початку передавання ТСК по даному каналу з метою оцінки появи помилок відповідної кратності при РЦК, була організована передача 8-елементних кодових слів з розрядно-цифровим кодуванням.

Результати вимірювання наведені в табл. 3.11.

Таблиця 3.11 – Розподілення помилок кратності t_k

$P_{\text{пр}} (\geq 1, n)$	Питома вага помилок кратності							
	1	2	3	4	5	6	7	8
$2,3 \cdot 10^{-3}$	0,58	0,32	0,06	0,02	0,015	0,002	0,0015	0,0005

Ймовірність помилки при ТСК (при вилученні виправлених кодових слів) дорівнює $P_{\text{пт}} = \frac{103}{73676} = 1,49 \cdot 10^{-3}$. Як бачимо, $P_{\text{пр}}$ незначно відрізняються від $P_{\text{пт}}$. Важливо відзначити, що ця ймовірність не може бути більшою по відношенню до $P_{\text{пр}}$, тому що частина зосереджених завад (переривань сигналу) не привела до помилок при ресстрації в середині помилки.

Зрозуміло, що при використанні алгоритму приймання без виправлення число помилкових КС буде (731+103) дорівнювати 834 при тому ж самому числі переданих.

Загальна ймовірність помилкового приймання стану таймерних конструкцій $P_{\text{пт}} = \frac{834}{73676} = 1,1 \cdot 10^{-2}$ (див. приклад 14).

Для зменшення значення $P_{\text{пт}}$ збільшимо зону Δ до значення $\Delta = 0,2t_0$ ($s = 5$).

За такого значення s на інтервалі $T_c = 8t_0$ можна реалізувати $N_p = 38739$ кодових слів. Тому що $\lfloor \log_2 38739 \rfloor = 15$, то швидкість передавання збільшується в $K = \frac{15}{8} = 1,875$ разів.

Порівняємо ймовірність вірного приймання $P_{\text{вт}}$ на інтервалі «хорошого» стану каналу для одного ЗМВ при $s = 7$ і трьох ЗМВ в кодовім слові, як було в експерименті і $s = 5$ при використанні ТСК з $i \in \overline{1 \dots 8}$:

$$- s = 7 (\Delta = 0,142t_0)$$

$$P_{\text{вт}}^{(1)} = 2\Phi\left(\frac{14}{2 \cdot 2}\right) = 2\Phi(3,5) = 0,999534,$$

а для трьох інформаційних ЗМВ

$$P_{\text{вт}}(s = 7) = (0,999534)^3 = 0,9996,$$

$$- s = 5 (\Delta = 0,2t_0); \bar{i} = 4, 1$$

$$P_{\text{вт}}^{(1)} = 2\Phi\left(\frac{20}{2 \cdot 2}\right) = 2\Phi(5) = 0,9999994 \quad (s = 5),$$

а для \bar{i} ЗМВ

$$(0,9999994)^{\bar{i}} = 0,9999976.$$

Така суттєва зміна ймовірності вірного приймання на інтервалі «хорошого» стану каналу при переході від ТСК ($s = 7$) до ТСК ($s = 5$) практично не впливає на середню ймовірність помилкового приймання сигнальної конструкції (тому що ймовірність появи зосередженої завади $2,3 \cdot 10^{-3}$, табл. 3.11).

Пояснюється це тим, що середнє значення інтервалу між «поганими» станами каналу залишається незмінними і середня ймовірність помилкового приймання може збільшитись тільки в K_0 число разів, яке визначається відношенням довжин ТСК і РЦК.

Враховуючи наведене при переході від РЦК до ТСК в реальних каналах не можливо суттєво зменшити ймовірність помилкового приймання сигнальної конструкції, а можливо збільшити тільки швидкість передавання.

Враховуючи, що при проведенні експерименту з визначення якості передавання сигнальних конструкцій ТСК (приклад 14) були зареєстровані всі помилкові кодові слова, то є можливість провести аналіз інших алгоритмів використання ТСК, що забезпечують підвищення якості приймання.

Приклад 17. Розглянемо ефективність використання ТСК при матричному декореляторі помилок.

У зв'язку з тим, що при проведенні експерименту після кожного помилкового КС ТСК записували 10 наступних кодових слів, це дозволяє зробити аналіз ефективності блокового декорелятора ємністю 10 слів. Структура зафіксованих спотворених блоків із 10 кодових слів наступна:

- одне спотворене кодове слово ТСК на 10 КС в блоці – 83%;
- два кодових слова спотворених підряд – 13%;
- два кодових слова спотворених через одне вірно прийняте – 3,5%;
- три спотворених кодових слова в блоці з 10 кодових слів 0,5%.

Середня тривалість інтервалу між помилковими кодовими словами 1700 мс (183 кодових слова).

Аналіз 103 кодових слів, які були невірно прийняті, після синдрому виправлення показав, що всі виправлення задовольняли умові якості, але були декодовані в друге дозволене кодове слово РЦК.

Невірно декодовані кодові слова можна поділити на п'ять груп.

I. Кодові слова зі зміною тривалості одного інформаційного відрізка сигналів за рахунок іншого на величину $\Theta \geq 2\Delta$.

II. Кодові слова, в яких було одне дроблення на інтервалі T_c .

III. Кодові слова з наявністю дроблень, або декількох дроблень на інтервалах двох інформаційних відрізків.

IV. Кодові слова з дробленням і зсуванням мінімум одного ЗМВ на величину $\Theta > \frac{1}{2}\Delta$.

V. Пари підряд переданих кодових слів, в яких спотворені останні інформаційні відрізки однієї кодової конструкції і перші відрізки наступної.

У табл. 3.12 наведені приклади переданих і прийнятих кодових слів ТСК, що відносяться до окремих груп і їх відповідності після декодера ТСК-РЦК.

Таблиця 3.12 – Приклади переданих до помилково прийнятих ТСК, таких, що відносяться до окремих груп

№	Слова	Кодові слова ТСК		Кодові конструкції РЦК		
		передавання	приймання*	передавання	приймання	n_p
1	14892	12; 23; 21; 8	121; 229; 227; 63	01101010	01111110	3
2	59810	12; 29; 13; 10	118; 147; 75; 67; 130; 101	01101011	01011000	4
3	96440	12; 20; 19; 13	119; 103; 80; 20; 97; 46; 77; 128	01100001	00010010	5
4	15250	9; 18; 17; 20	123; 51; 16; 77; 178; 199	00100000	01010101	4
5	68798	15; 7; 8; 34	149; 70; 79; 55; 187	01100001	01100011	1
5	68 7 94	9; 18; 17; 20	82; 40; 181; 179; 202	00100000	10111001	4

* на прийманні кожний елемент Δ стробувався в 10 точках.

З аналізу спотворених кодових слів можна зробити наступні висновки:

– при дії імпульсних завад або переривань сигналу на інтервалі кодової конструкції спотворюються відповідні інформаційні відрізки при незначному відхиленні тривалості $[(0,5 \dots 1,5)\%]$ інших сигнальних відрізків кодового слова;

– з метою зменшення ймовірності спотворення відрізків на величину $\Theta > 0,5\Delta$ відлік їх тривалості слід проводити по відношенню до початку сигнальної конструкції, а не вимірювати абсолютні значення тривалості окремих відрізків (оскільки зсув першого переходу вліво на певну величину зменшує довжину першого і збільшує довжину наступного другого відрізу);

– внаслідок невідповідності числа інформаційних відрізків ТСК і елементності РЦК відбувається множення (групування) помилок при декодуванні ТСК → РЦК.

Відомо, що для боротьби з групуванням помилок, яке зменшує ефективність використання надлишковості коду, використовують декорелятори помилок, які реалізують рознесення в часі суміжних елементів з відновленням їх місця після приймання. Через те що ефективність використання блокового коду оцінюється відношенням імовірності помилкового приймання кодового слова без виправлення до ймовірності помилкового приймання після виправлення

$$h = \frac{P(\geq 1, n)}{\sum e_n^i P_c^i (1 - P_c)^{n-i}},$$

рис. 2.23 можна оцінити вплив декореляції на ефективність коду в телефонному каналі.

З урахуванням викладеної характеристики спотворень таймерних сигнальних конструкцій в реальному каналі і впливу декореляції на ефективність блокових кодів можна сформулювати вимоги до таймерної сигнальної конструкції й алгоритму передавання в канал, послідовності перетворення отриманої ТСК в РЦК на прийомі:

1. Сигнальна конструкція ТСК повинна забезпечувати виявлення помилок на прийомі не всього n -елементного надлишкового коду, а нести інформацію відносно частини елементів кодового слова, що зменшить множення помилок. Наприклад, для 9-елементного коду Слепяна можливо однією конструкцією ТСК передавати одну із 512 комбінацій, а можливо на інтервалі $T_c = 9 t_0$ реалізувати трьома послідовно розміщеними конструкціями ТСК, які дозволять передати ті ж 512 символів (в кожній конструкції по 3 біти, загальне число кодових N_3 слів $N_3 = 2^3 \cdot 2^3 \cdot 2^3 = 2^9 = 512$).

Надалі сигнальні конструкції, що несуть інформацію про частину двійкових одиниць, називатимемо «малими» (ТСК_м), а складену загальну сигнальну конструкцію назвемо «великими» (ТСК_в).

2. Поставимо умову до ТСК_м, а саме, що вона повинна передавати інформацію не тільки про три двійкові одиниці, але і створювати умови оцінки якості їх приймання. Цю процедуру можна забезпечити за рахунок збільшення мірності простору розв'язань (квантування прийманого сигналу) при декодуванні малої сигнальної конструкції ТСК_м.

3. З метою зменшення впливу множення помилок за рахунок кодоперетворення на прийомі ТСК_м–РЦК доцільно ввести матричне перемежування символів кодових слів.

На рис. 3.29, а наведена «велика» таймерна конструкція, синтезована з трьома ЗММ на інтервалі $T_c = 7,5 t_0$ при $s = 10$, а на рис. 3.29, б, в у збільшеному вигляді подано «малу» сигнальну конструкцію ТСК_м-1.

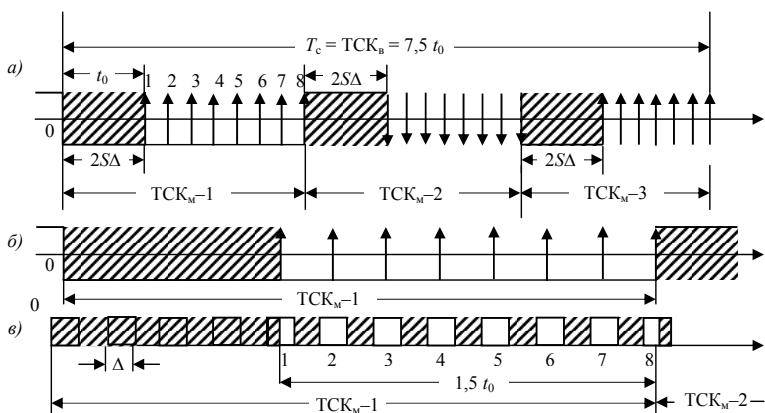


Рисунок 3.29 – Таймерна конструкція, синтезована з трьома ЗММ на інтервалі $T_c = 7,5 t_0$ при $S = 10$

На рис. 3.29, в незаштрихованими показані зони, в яких можуть розміщуватись ЗМВ за синхронного приймання і відсутності спотворень.

З рисунка виходить, що при прийманні ТСК_м повинні виконуватися умови:

- а) наявність тільки одного ЗММ відповідного вигляду (або 0→1 або 1→0);
- б) ЗМВ не можуть знаходитись в заштрихованих зонах.

Розрахунки показують, що за умови реєстрації тільки в заштригованих зонах при $s = 10$ ймовірність помилкового приймання буде не більшою, ніж при $S = 7$ з реєстрацією в кожній зоні. Поява ЗМВ в заштригованих зонах дає можливість зафіксувати ненадійне приймання інформаційного ЗМВ. Реєстрація ЗМВ в незаштригованій зоні «не своїй» призводить до невиявленої помилки.

З метою зменшення множення помилок при переході від ТСК_м до РЦК, що складається з трьох бітів, доцільно використати код Грея. В табл. 3.13 наведені номери кодових слів і їх подання в розрядно-цифровому вигляді та кодї Грея.

Таблиця 3.13 – Код Грея

N_0	0	1	2	3	4	5	6	7
Код РЦК	000	001	010	011	100	101	110	111
Код Грея	000	001	011	010	10	111	101	100

Відзначимо, що поява двох помилок в одному початковому кодовому слові (із записаних по горизонталі в матриці), можлива, коли дві конструкції ТСК, передані підряд (вертикалі), були спотворені (ТСК_{вi} і ТСК_{в(i+1)}) за рахунок неввірного приймання однойменних блоків ТСК_м. Результати обро-

бки даних статичних вимірювань, наведених вище, показують, що ймовірність появи двох підряд спотворених ТСК дорівнює $(12:73676) p(\text{ТСК}_i / \text{ТСК}_{i+1}) = 1,6 \cdot 10^{-4}$. При цьому спотворюється кінець однієї ТСК_{vi}, і початок іншої ТСК_{v(i+1)}, що зменшує групування помилок в горизонталях. Спотворення однойменних двійкових цифр в трибітових словах після перетворення ТСК_М-РЦК за умови збігу номерів ТСК_М більш ніж на два порядки менше ймовірностей спотворення однойменних ТСК_М.

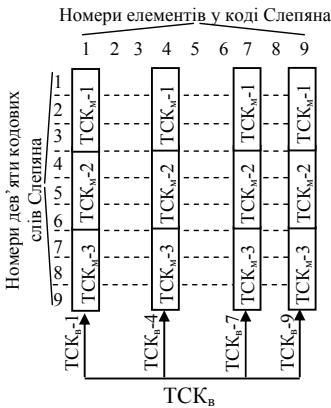


Рисунок 3.30 – Структура матричного перемежувача з використанням кодоперетворювача РЦК-ТСК

Структура матричного перемежувача з використанням кодоперетворювача РЦК-ТСК показана на рис. 3.30.

Припустимо, що передаються дозволені 9-елементні комбінації коду Слепяна (9, 5). Кожен рядок матриці представляє 9 елементів надлишкового коду з $d=3$ при п'яти інформаційних елементах.

Дев'ять однойменних елементів дозволених кодових слів (вертикалі матриці рис. 3.31) представляють 9-розрядне двійкове число, яке передається трьома ТСК_М: 1, 2, 3 елементи відповідають ТСК_М-1; 4, 5, 6 – ТСК_М-2; 7, 8, 9 – ТСК_М-3.

У табл. 3.14,а подані вектори помилок на виході кодоперетворювача ТСК_в-РЦК. Номери кодових слів ТСК і їх параметри прийому взяті із зафіксованого фрагмента вимірювань при проведенні експерименту.

Таблиця 3.14,а – Вектори помилок при декодуванні

Номери елементів		Спотворені елементи РЦК після кодоперетворювача ТСК-РЦК								
		1	2	3	4	5	6	7	8	9
ТСК _в -РЦК	№ 71199(1)	1	0	0	0	0	1	1	1	0
	№ 71201(3)	0	0	0	0	0	0	0	1	0
	№ 71203(5)	0	0	1	1	1	0	0	0	0

У таблиці наведені слова для однієї з реалізацій коду на інтервалі 9-таймерних сигнальних конструкцій, передаваних підряд після спотворення (у десятиці аналізованих виявилися три спотворені № 71199; 71201; 71203).

З таблиці виходить, що після перетворення ТСК_в в РЦК у векторах помилок є від однієї до чотирьох одиниць.

У табл. 3.14,а для вказаних спотворених кодових слів РЦК (після коперетворювача ТСК–РЦК) вказані реальні в експерименті місця знаходження моментів модуляції з ТСК на приймальній та передавальній сторонах і відповідні двійкові кодові слова.

Таблиця 3.14,б – Значення місць знаходження ЗММ і ЗМВ

№ зп	Передавання		Приймання	
	РЦК	ТСК	ТСК	РЦК
71199	011100100	12; 29; 13; 10	25; 16; 12; 10	111101010
711201	011010110	12; 23; 21; 8	12; 24; 19; 9	011010100
71203	001000000	10; 18; 17; 20	10; 16; 18; 20	000110000

Із табл. 3.14,б випливає, що в наведених кодових словах ТСК зосереджена завада знаходилась в різних зонах «великої» таймерної конструкції:

- 71199 – у першій зоні (збільшення першого відрізка τ_{c1} з 12Δ до 25Δ) за рахунок чого зменшився другий;
- 711209 – у третій зоні (зміщення на 2Δ);
- 711209 – у другій зоні.

За такого розміщення спотворених ТСК_м можливі спотворені слова коду Слепяна тільки з одним помилково прийнятим елементом, який буде виправлений кодом з $d = 3$ (передавання ТСК проходить по вертикальних бігах записаних в горизонталях 9-елементних кодових словах).

Для появи двократної помилки необхідно:

- щоб при передаванні різних ТСК_в одного блоку були спотворені однойменні (за номером) ТСК_м;
- щоб у векторах помилок трибітових конструкцій ТСК_м були «1» на одних і тих самих позиціях.

Як зазначалося вище ймовірність такої події на багато менше ймовірності появи двократної помилки при РЦК.

Враховуючи той факт, що площа заштрихованих зон (рис. 3.30, в) набагато більше ніж заштрихованих, з'являється можливість за появами ЗМВ в заштрихованих зонах прогнозувати ненадійні символи на прийомі та використовувати для підвищення якості приймання.

Оцінимо ефективність використання ТСК у системах із зворотним зв'язком.

Приклад 18. При виборі методу захисту у системах з ВЗЗ необхідно виходити з таких принципів:

- у системах такого типу недоцільно використовувати декорелятор помилок (перемежування), оскільки повторення всього спотвореного блоку на інтервалі перемежування суттєво впливає на швидкість передавання;
- в зв'язку з тим, що доцільність зворотного зв'язку визначається можливістю дістати більшу швидкість передавання в нестационарних кана-

лах порівняно з однобічними системами (при заданій якості), то порівняння необхідно проводити за цим критерієм;

– при виборі параметрів ТСК слід пам'ятати, що ймовірність помилкового приймання кодового слова ТСК не може бути меншою ніж при РЦК ($P_{пр} \leq P_{пр}$) для T_c (ТСК) = T_c (РЦК).

Для виявлення спотворених ТСК на виході каналу необхідно формувати КС, які задовольняють умові якості

$$A_1 x_1 + A_2 x_2 + A_3 x_3 = 0 \pmod{A_0}. \quad (3.164)$$

Коефіцієнти A_i визначаються вимогою до якості приймання. Значення місць знаходження окремих ЗММ відраховуються у величинах Δ відносно вихідної (стартової) відлікової точки початку ТСК.

Оскільки величина s визначається значенням, що забезпечує максимум швидкості передавання $\Delta_0 = (4,5 \dots 5)\sigma$ для заданого каналу.

Виникає питання вибору довжини кодового слова. Для цього розглянемо табл. 3.15.

Таблиця 3.15 – До розрахунку максимальної швидкості передавання

N	i	$\begin{matrix} m \\ s \end{matrix}$	5	6	7	8	9	10
1	3	5	286 1,631	816 1,61	177 11,54	3276 1,45	5436 1,37	8436 1,3
2	3	7	680 1,88	2020 1,83	4495 1,73	8436 1,63	14190 1,53	22100 1,44
3	4	5	126 1,39	1001 1,66	3876 1,7	10620 1,67	23751 1,61	46376 1,55
4	4	7	330 1,67	3060 1,675	12650 1,94	35960 1,89	72251 1,81	168185 1,73

У кожній клітинці таблиці наведене число реалізацій ТСК із заданими параметрами і максимальна кількість інформації, яку можна «упакувати» в середньому на один найквістовий елемент кодової конструкції

$$I_{\max} = \frac{\log_2 N_p}{m}.$$

Із таблиці слідує, що для кожної довжини кодового слова існує значення i_{\max} за якого число реалізацій максимальне.

Наведені дані показують, що при $s = 7$ краще використати ТСК з чотирма ЗММ при довжині ТСК $T_k = 7 t_0$. Взагалі значення S необхідно вибирати в залежності від значення середньоквадратичного відхилення в «хорошому» стані.

Нагадаємо, що у системах з вирішальним зворотним зв'язком ефективна швидкість передавання R_B визначається двома коефіцієнтами

$$R_B = \gamma_k \cdot \gamma_n,$$

де γ_k – кодова швидкість, яка дорівнює відношенню числа інформаційних елементів в кодовім слові (m) до загального числа елементів (n), ($n = m + r$); γ_n – коефіцієнт затрат на повторення кожного спотвореного кодового слова, який визначається числом кодових слів, які необхідно повторно передати згідно з алгоритмом роботи системи.

$$\gamma_n = \frac{1 - P_n}{1 - P_n + MP_n} \quad (3.165)$$

де P_n – імовірність повторення кодового слова, яка визначається як імовірність виявлення помилки в кодовім слові.

Розглянемо ймовірнісні характеристики роботи системи з ВЗЗ.

У табл. 3.16 наведені результати передавання інформації в системі з ВЗЗ для трирозрядно-цифрових кодів ($n = 15; 31; 63$) для каналів:

1. Телефонного з $P_e = 7 \cdot 10^{-4}$; $\alpha = 0,545$.
2. Радіотелеграфного з $P_e = 2,85 \cdot 10^{-4}$; $\alpha = 0,372$.
3. Радіотелефонного УКК з $P_e = 4 \cdot 10^{-4}$; $\alpha = 0,266$.

Таблиця 3.16 – Результати експериментальних оцінок швидкості передавання для трьох каналів: телефонного каналу, радіотелеграфного та радіотелефонного УКК

n	1-й канал			ΔR -канал	2-й канал		3-й канал	
	$r = n - m$	$\frac{m}{n}$	$R_{\text{екс}}$	$-\Delta R$	$R_{\text{екс}}$	$-\Delta R$	$R_{\text{екс}}$	$-\Delta R$
15	5	0,6666	0,66	0,0066	0,663	0,003	0,661	0,005
15	7	0,53333	0,527	0,0033	0,530	0,0033	0,462	0,0713
31	5	0,83870	0,825	0,0137	0,835	0,0037	0,825	0,0137
31	7	0,77419	0,763	0,011	0,771	0,0031	0,730	0,044
63	7	0,8888	0,874	0,014	0,84	0,04	0,848	0,040

Символ α позначає коефіцієнт групування помилок, а ΔR – втрати на повторення. З табл. 3.16 виходить, що втрати на повторення мінімум в десятки разів менше втрат на надлишкові елементи. З іншого боку, надлишковість спільно з параметрами потоку помилок в каналі визначає залишкову ймовірність помилки.

Для оцінки ймовірнісних характеристик, що виявляють помилки ТСК, розглянемо вектори завад, за яких помилки будуть невиявленими.

Із аналізу окремих векторів зміщень ЗМВ слідує, що максимальна ймовірність невивраченої помилки при ТСК визначається вектором $E \rightarrow \pm 1; \mp (d - 1); 0$

$$P_{\text{нв}} = P_{\text{ТТ}}(1)P_{\text{Т}}(d - 1)P_{\text{Т}}(0), \quad (3.166)$$

де $P_T(1)$, $P_T(d-1)$, $P_T(0)$ – ймовірність зміщень відповідних ЗМВ під час ресстрації в середній точці на (1), $(d-1)$, (0) значень Δ .

Легко показати, що для нормального закону зміщень ЗМВ

$$\begin{aligned} P(1) &= \Phi(1,5\Delta/\sigma) - \Phi(0,5\Delta/\sigma), \\ P(0) &= 2\Phi(\Delta/2\sigma); \end{aligned} \quad (3.167)$$

$$P(d-1) = \Phi\left(\frac{(d-0,5)\Delta}{\sigma}\right) - \Phi\left(\frac{(d-1,5)\Delta}{\sigma}\right).$$

Із наведених виразів випливає, що ймовірність невиявленої помилки визначається кодовою відстанню d для таймерних сигналів та величиною Δ : чим більше d і менше Δ , тим більше ймовірність невиявленої помилки. Фізика процесу тут зрозуміла: чим менше Δ , тим менше ймовірність забезпечення рівняння (3.166).

Таким чином, з точки зору значення $P_{\text{нв}}$ зону Δ необхідно вибирати меншою. У той самий час, величина зони Δ не повинна забезпечувати ймовірність помилкового приймання ТСК на інтервалі «хорошого» стану більше ніж ймовірність помилкового приймання за рахунок зосереджених завад при передаванні по даному каналу кодових слів РЦК.

Для зменшення ймовірності повторення при зменшенні $P_{\text{нв}}$ можна скористатися властивістю кодів ТСК, які виправляють i -кратні помилки зміщень величиною $e = \pm e_0$. В цьому випадку величину реальної зони можна зменшити відносно Δ_0 у $(e_0 + 1)$ разів і значення ймовірностей зміщень окремих ЗМВ будуть визначатися:

$$\left. \begin{aligned} P(0) &= \Phi\left(\frac{\Delta_0}{2\sigma(2e_0 + 1)}\right); \\ P(1) &= \Phi\left(\frac{3\Delta_0}{2\sigma(2e_0 + 1)}\right) - \Phi\left(\frac{\Delta_0}{2\sigma(2e_0 + 1)}\right); \\ P(d-1) &= \Phi\left(\frac{(2d-1)\Delta_0}{2\sigma(2e_0 + 1)}\right) - \Phi\left(\frac{(2d+3)\Delta_0}{2\sigma(2e_0 + 1)}\right). \end{aligned} \right\} \quad (3.168)$$

Тут Δ_0 відповідає величині зони, яка максимізує швидкість передавання у системі з вирішальним зворотним зв'язком (ВЗЗ) при виправленні помилок зміщень.

Із виразів (3.167) і (3.168) слідує, що $P_{\text{нв}}$ визначається здебільшого значенням $p(1) \cdot p(d-1)$, які при виправленні помилок зміщень визначаються значенням $p(1)$, тому що $p(d-1)$ на декілька порядків менше $p(1)$.

Аналіз статистичних даних результатів експерименту з використання ТСК на реальних каналах (приклад 14) приводить до висновку, що невірні виправлені помилки в спотворених кодових словах ТСК відповідають таким подіям:

– зміщенню одного або більшого числа ЗМВ на величину більше одного Δ ;

- зміні числа ЗМВ в кодовім слові;
- наявності перших двох спотворень.

Зважаючи на те, що всі спотворені кодові слова при проведенні експерименту були виявлені або за числом ЗМВ в прийнятій кодовій конструкції, або невиконанням умови якості (3.164) можливо зробити висновок про недоцільність виправлення спотворених КС у системі з ВЗЗ.

Доцільно реалізувати такі структури надлишкових ТСК, в яких на меншому інтервалі часу можна синтезувати більше КК, здатних виявляти спотворені кодові слова за ймовірності помилкового приймання близькій до ймовірності помилкового приймання кодових слів РЦК кодів, для яких $T_{\text{СК}}(\text{РЦК}) \approx T_{\text{СК}}(\text{ТСК})$.

Розглянемо приклад.

Приклад 19. Побудуємо таймерний надлишковий код, який виправляє помилки зміщення в «хорошому» стані каналу тільки одного ЗМВ і має $P_{\text{T}}(1) < 10^{-8}$.

Зважаючи на те, що в вірно виправлених ТСК був зміщений тільки один ЗМВ (приклад 14) в якості коефіцієнтів A_i рівняння $\sum A_i x_i = 0 \pmod{A_0}$, візьмемо прості числа 2; 3; 7 при $A_0 = 19$.

Легко показати, що нульовими векторами в цьому випадку будуть

$$E_0(0) \rightarrow \pm 3; \pm 2; 0 \quad w = 5,$$

$$E_0(0) \rightarrow \pm 2; \pm 1; \mp 1 \quad w = 4,$$

$$E_0(A_0) \rightarrow \mp 1; 0; \pm 3 \quad w = 4,$$

де w – вага вектора.

Із наведених векторів E_0 видно, що мінімальна вага вектора E_0 більше ніж за коефіцієнтів (1; 3; 9, $A_0 = 27$), що забезпечує меншу ймовірність невиявлених спотворень таймерної конструкції.

Менше значення A_0 дозволяє отримати більше число реалізацій на заданому інтервалі. Так, для одержання 256 дозволених реалізацій при $s = 7$ з наведеними коефіцієнтами A_i необхідно мати всього ($256 \times 19 = 4864$) таймерних конструкцій при $i = 3$.

Згідно з табл. 3.4 таку кількість реалізацій можливо отримати для $i = 3$, $s = 7$, $m = 7$.

Ймовірність помилкового приймання ТСК при «хорошому» стані каналу буде:

$$P_{\text{пт}} = 1 - \left[2\Phi\left(\frac{\Delta}{2l}\right)^i \right] = 1 - \left[2\Phi(3,35)^3 \right] = 1 - 0,9988 = 1,2 \cdot 10^{-3}.$$

Тобто $P_{\text{пт}}$ майже в 2 рази менше $P_{\text{пр}}$ (табл. 3.11).

З урахуванням помилок в «поганому» стані каналу сумарна ймовірність виявлених помилок $P_{\text{пт}\Sigma} = P_{\text{пт}} + P_{\text{пр}} (\geq 1, n)$.

Проведені експерименти в реальному каналі МТМ (приклад 14) при заданих коефіцієнтах A_i показали, що ймовірність невиявлених спотворень ТСК $P_{\text{нв}} < 10^{-8}$.

Порівняємо залишкову ймовірність для надлишкового коду РЦК при виправленні помилок кратності $t_b = 2$ (див. табл. 3.11).

Враховуючи, що при $t_b = 2$ кодова відстань $d = 5$ і число надлишкових елементів для інформаційних $m = 8$ відповідає 10 ($n = 18$). Набагато менше «хорошого» стану середня ймовірність помилкового приймання кодового слова при збільшенні елементності з $n = 8$ до $n = 18$ збільшується в 1,1...1,2 рази, при практично незмінних імовірностях помилок відповідної кратності i , враховуючи, що залишкова ймовірність помилкового приймання

$$P_{\text{зр}} = P(\geq 1, n) - \sum P_u \approx \frac{1}{2^{n-m}} P(\geq t_i, n),$$

де u – множина векторів помилок, які виправляються даним кодом. Остаточне значення $P_{\text{з}} \approx 2,8 \cdot 10^{-6}$.

Таким чином, залишкова ймовірність помилки при виправленні двократних помилок РЦК більш ніж на 2 порядки більше по відношенню до невиявлених спотворень надлишковими ТСК, реалізованих на інтервалі $T_c = 7 t_0$. Кодова швидкість при ТСК складає $(\frac{8}{7})$, а при РЦК $(\frac{8}{15})$ відповідно 0,53, що більше ніж в 2 рази менше кодової швидкості ТСК.

Із наведеного прикладу зрозуміло, що кодова швидкість при використанні ТСК в системах з ВЗЗ визначається числом реалізацій надлишкових сигнальних конструкцій на заданому інтервалі часу. В зв'язку з цим постає питання: яка потужність дозволених ТСК може бути реалізована додатково на заданому інтервалі T_c при нових коефіцієнтах A_i і заданій кодовій відстані для ТСК. Для прикладу розглянемо структуру множини ТСК на інтервалі $T_c = 7 t_0$ ($m = 7$) при $s = 5, i = 3$ задовольняючих умові

$$\sum_{i=0}^k A_i x_i = zA_0 = 0(\text{mod } A_0)$$

при коефіцієнтах $A_1 = 2, A_2 = 3, A_3 = 7$ і $A_0 = 19$. Можна показати, що їх кількість дорівнює 94.

Структура множини ТСК для заданих параметрів A_i показана на рис. 3.31.

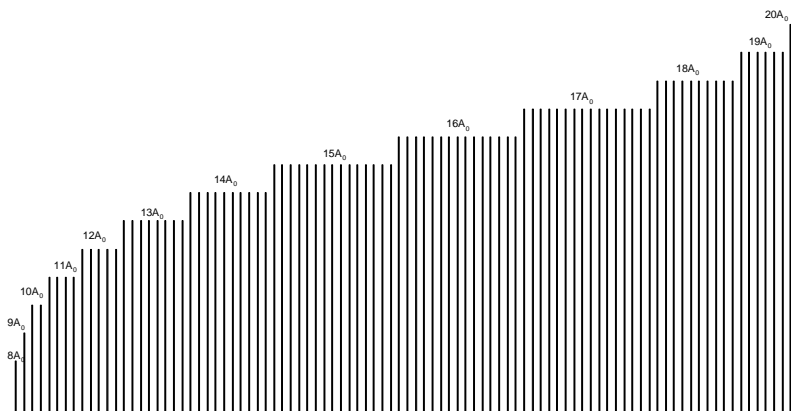


Рисунок 3.31 – Структура дозволених ТСК, задовольняючих умові

$$\sum_{i=0}^k A_i x_i = zA_0 = 0 \pmod{A_0}$$

У табл. 3.17 наведені координати всіх 94 дозволених кодових слів, які задовольняють умові та обчисленню суми $\sum_{i=1}^3 A_i x_i = 0 \pmod{19}$.

Із рис. 3.31 та табл. 3.17 видно, що при заданих коефіцієнтах A_i і A_0 всі ТСК належать інтервалу зміни по $\sum_{i=1}^3 A_i x_i$ від $\overline{8A_0, 20A_0}$. Різним значенням kA_0 ($k \in 8 \dots 20$) відповідає різна кількість кодових слів, що мають одну і ту ж саму $\sum_{i=1}^3 A_i x_i$.

Враховуючи, що при заданих коефіцієнтах A_i для x_i повинні виконуватися умови

$$s \leq x_k \leq (m - i + 1)s, \quad 5 \leq x_1 \leq 25,$$

$$\sum_{k=1}^n x_k \leq (m - i + n)s, n \leq i, \quad \text{тобто для заданих параметрів ТСК } 10 \leq x_2 \leq 30,$$

$$15 \leq x_3 \leq 35.$$

Таблиця 3.17 – ДКК для $A_1 = 2, A_2 = 3, A_3 = 7, A_0 = 19$

№	x_1	x_2	x_3	$\sum_{i=0}^3 A_i x_i$	kA_0	№	x_1	x_2	x_3	$\sum_{i=0}^3 A_i x_i$	kA_0	№	x_1	x_2	x_3	$\sum_{i=0}^3 A_i x_i$	kA_0
1	5	10	16	152	8A ₀	33	5	17	32	285	15A ₀	65	8	23	34	323	17A ₀
2	6	11	18	171	9A ₀	34	5	24	29	285	15A ₀	66	9	20	35	323	17A ₀
3	5	11	21	190	10A ₀	35	6	14	33	285	15A ₀	67	9	27	32	323	17A ₀
4	7	12	20	190	10A ₀	36	6	21	30	285	15A ₀	68	10	24	33	323	17A ₀
5	5	15	22	209	11A ₀	37	7	18	31	285	15A ₀	69	11	21	34	323	17A ₀
6	6	12	23	209	11A ₀	38	8	15	32	285	15A ₀	70	12	18	35	323	17A ₀
7	7	16	21	209	11A ₀	39	8	22	29	285	15A ₀	71	12	25	32	323	17A ₀
8	8	13	22	209	11A ₀	40	9	19	30	285	15A ₀	72	13	22	33	323	17A ₀
9	5	12	26	228	12A ₀	41	10	16	31	285	15A ₀	73	14	19	34	323	17A ₀
10	6	16	24	228	12A ₀	42	10	23	28	285	15A ₀	74	14	26	31	323	17A ₀
11	7	13	25	228	12A ₀	43	11	20	29	285	15A ₀	75	15	23	32	323	17A ₀
12	8	17	23	228	12A ₀	44	12	17	30	285	15A ₀	76	17	24	31	323	17A ₀
13	9	14	24	228	12A ₀	45	13	21	28	285	15A ₀	77	19	25	30	323	17A ₀
14	5	16	27	247	13A ₀	46	15	22	27	285	15A ₀	78	5	29	35	342	18A ₀
15	6	13	28	247	13A ₀	47	5	21	33	304	16A ₀	79	8	27	35	342	18A ₀
16	6	20	25	247	13A ₀	48	6	18	34	304	16A ₀	80	10	28	34	342	18A ₀
17	7	17	26	247	13A ₀	49	6	25	31	304	16A ₀	81	11	25	35	342	18A ₀
18	8	14	27	247	13A ₀	50	7	15	35	304	16A ₀	82	13	26	34	342	18A ₀
19	9	18	25	247	13A ₀	51	7	22	32	304	16A ₀	83	14	23	35	342	18A ₀
20	10	15	26	247	13A ₀	52	8	19	33	304	16A ₀	84	15	27	33	342	18A ₀
21	11	19	24	247	13A ₀	53	9	16	34	304	16A ₀	85	16	24	34	342	18A ₀
22	5	13	31	266	14A ₀	54	9	23	31	304	16A ₀	86	18	25	33	342	18A ₀
23	5	20	28	266	14A ₀	55	10	20	32	304	16A ₀	87	20	26	32	342	18A ₀
24	6	17	29	266	14A ₀	56	11	17	33	304	16A ₀	88	13	30	35	361	19A ₀
25	7	14	30	266	14A ₀	57	11	24	30	304	16A ₀	89	16	28	35	361	19A ₀
26	7	21	27	266	14A ₀	58	12	21	31	304	16A ₀	90	18	29	34	361	19A ₀
27	8	18	28	266	14A ₀	59	13	18	32	304	16A ₀	91	19	26	35	361	19A ₀
28	9	15	29	266	14A ₀	60	14	22	30	304	16A ₀	92	21	27	34	361	19A ₀
29	10	19	27	266	14A ₀	61	16	23	29	304	16A ₀	93	23	28	33	361	19A ₀
30	11	16	28	266	14A ₀	62	5	25	34	323	17A ₀	94	24	29	35	380	20A ₀
31	12	20	26	266	14A ₀	63	6	22	35	323	17A ₀						
32	5	10	35	285	15A ₀	64	7	26	33	323	17A ₀						

Подано значення всіх ТСК (рис. 3.32), задовольняючих умові

$$\sum_{i=0}^k A_i x_i = 0 \pmod{A_0}.$$

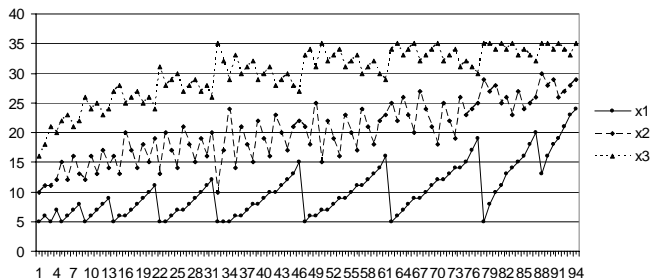


Рисунок 3.32 – Зміни координат дозволених ТСК

Вісь координат з нумерацією 1...94 відповідає номеру РКК з табл. 3.17.

На рис. 3.33 зображені дозволені ТСК у вигляді куль, а недозволені у вигляді точок. Осі координат x_i , ($i=1...3$) – відповідають часовим моментам змін інформаційних параметрів на інтервалі T_k . Для наочності кожна ТСК розміщена у сфері радіуса 1,5, оскільки мінімальна відстань між комбінаціями повинна складати $d \geq 3$, а КК, для яких умова по відстані між моментами модуляції не виконана, наведені у вигляді точок.

З рис. 3.33 слідує, що всі дозволені кодові комбінації (ДКК) у сферах згруповані в одному місці та займають майже половину всього об'єму куба, поверхня якого обмежена параметрами ТСК. Друга частина об'єму куба (заповнена точками) відповідає (КК), для яких умова за відстанню між моментами модуляції не виконується. Як було показано вище, неможливо збільшити потужність множини ДКК за тих самих параметрів ТСК й іншому A_0 .

З наведеного можна зробити висновок, що кількість додаткових ТСК з тією ж кодовою відстанню між множинами і в середині нової підмножини не більше 1.

Суттєво можливо збільшити потужність дозволених надлишкових ТСК на заданому інтервалі, якщо використовувати сигнальні конструкції з різним числом ЗММ. Наприклад, якщо в наведеному вище прикладі передбачались кодові слова, які мають три ЗММ ($i=3$), то додатково можна

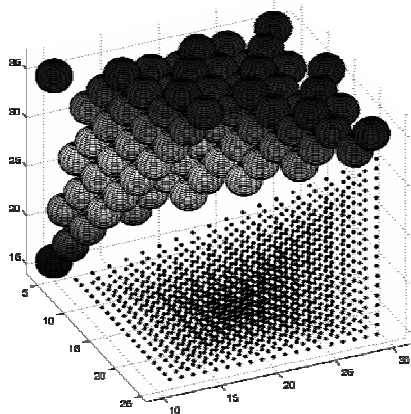


Рисунок 3.33 – ДКК і КК в просторі для заданих параметрів ТСК

взяти кодові слова з $i = 4$ за тих самих значень $m = 7$ і $s = 5$. Згідно з табл. 3.5 таких реалізацій буде 3876.

$$N_d = \lfloor 3876 : 3 \rfloor = 125.$$

Як коефіцієнти A_i можливо взяти $A_1 = 2; A_2 = 3; A_3 = 7; A_4 = 13$ і $A_0 = 31$ – це забезпечить потужність додаткової множини дозволених ТСК.

Приклад 20. Оцінимо ефективність турбокодів при передаванні збиткової кодової послідовності таймерними сигналами при параметрах сигналу, який аналізувався в прикладах 12 ... 19. Зважаючи на те, що в турбокодах використовуються мінімум два компонентних згорткових коди і перемешувач (декорелятор) будемо вважати, що після перетворення ТСК в РЦК і оберненої перестановки символів на приймальній стороні помилки елементів коду будуть незалежними. При перетворенні РЦК в ТСК на виході турбо-кодера будемо формувати сигнальні конструкції на інтервалі $T_c = 8 t_0$ з числом ЗММ $i \in 1 \dots 8$, що дозволяє реалізувати $2^{16} = 65536$ КС.

Зважаючи, що математичне сподівання числа помилкових таймерних конструкцій буде дорівнювати 110 (статистика прикладу 3.14) в середньому 8 помилкових елементів із 16. Визначимо ймовірність помилкового приймання анкет елемента P_e після кодоперетворювача ТСК в РЦК

$$P_e = \frac{110 \cdot 8}{73676 \cdot 16} = 7 \cdot 10^{-4}, \text{ що відповідає відношенню } h = 3,2.$$

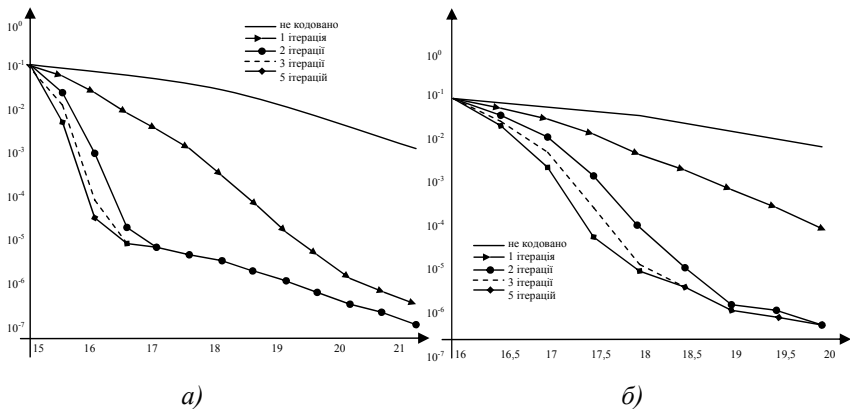


Рисунок 3.34 – Турбо-код з РЗСК (1,35/23) і $R_1 = \frac{1}{3}$ в каналі з ТСК (а);

Турбо-код з РЗСК (1,17/15) і $R_2 = \frac{1}{2}$ в каналі з ТСК (б)

Проведене моделювання роботи систем різних турбокодів з використанням ТСК за різних компонентних згорткових кодів і різних значень s

показує ефективність використання ТСК для передавання кодових послідовностей після турбокодера.

На рис. 3.34 наведено результати моделювання двох турбокодів з $R_1 = 1/3$ і $R_2 = 1/2$.

З цих рисунків можна зробити висновки:

- при одному і тому ж каналі згортковий код з меншим значенням R при першій ітерації дає більший приріст якості приймання;
- друга ітерація при обробленні сигналів більш ефективна для кодера з більшим R .

Через те що кожна ітерація використовує результати м'яких рішень при декодуванні, то розглянемо їхню ефективність на виході демодулятора.

М'яке рішення на виході перетворювача ТСК в кодові слова РЦК. Нехай ансамбль сигналів містить $M = 2^m$ реалізацій, які позначимо $\{S_0, S_1, \dots, S_{M-1}\}$, і кожен сигнал з'являється на виході модулятора з однаковою ймовірністю. Модулятор перетворює блоки двійкового РЦК довжиною m символів у таймерні сигнали. Тоді апіорні ймовірності сигналів $P(S_i) = 1/M \forall i \in \{0, 1, \dots, (M-1)\}$. Якщо з каналу було прийнято сигнал X , то апостеріорні густини ймовірності можна подати у вигляді

$$p(S_i | X) = \prod_{j=1}^k \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(x_j - s_j)^2}{2\sigma}\right) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{\sum_{j=1}^k (x_j - s_j)^2}{2\sigma}\right), \quad (3.171)$$

де k – кількість значущих моментів модуляції у сигналі; x_j – значущі моменти модуляції у прийнятому сигналі X ; s_j – значущі моменти модуляції у сигналі S_i . Таким чином, у чисельнику показника степеня знаходиться сума квадратів Евклідових відстаней між значущими моментами модуляції. По-

значимо $d^2 = \sum_{j=1}^k (x_j - s_j)^2$, тоді (3.171) для густини ймовірності можна записати у вигляді

$$p(S_i | X) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{d_i^2}{2\sigma}\right) = p(S_i). \quad (3.172)$$

Обчисливши густину ймовірності для кожного з можливих сигналів, можна отримати ймовірність для кожного біта з блока РЦК.

Визначимо ймовірність появи біта за номером n . Для цього поділимо всю множину сигналів на дві підмножини. У першій підмножині зберемо ті сигнали, в яких біт $n = 0$, а в другій підмножині зберемо ті сигнали, в яких біт $n = 1$. Обчислимо суму густини ймовірності кожної з підмножини

$$p(b_n = 0) = \sum p(S_i | b_n = 0), \quad (3.173)$$

$$p(b_n = 1) = \sum p(S_i | b_n = 1) \quad (3.174)$$

оскільки переданий біт набуває значення або 0, або 1, то ці дві події утворюють повну групу і, отже, можна обчислити ймовірність для кожного значення біта

$$P(b_n = 0) = \frac{p(b_n = 0)}{p(b_n = 0) + p(b_n = 1)}; \quad (3.175)$$

$$P(b_n = 1) = \frac{p(b_n = 1)}{p(b_n = 0) + p(b_n = 1)}. \quad (3.176)$$

Ця ймовірність є м'якою оцінкою значення прийнятого біта і може бути використана надалі при декодуванні за ітераційним алгоритмом максимуму апостеріорної ймовірності сигнальної кодової конструкції з турбокодом і ТСК.

3.2.9. Питання та задачі для самоперевірки

1. Чому при числі інформаційних відрізків i в ТСК, синтезованих на інтервалі m елементарних посилок, $N_p = 1$ для випадку $m = i$?

2. На якому інтервалі $T_c = mt_0$ при $s = 7$, $i = 4$ можливо синтезувати 2^{16} сигнальних конструкцій?

3. За якого мінімального значення s можна синтезувати 2^{12} сигнальних конструкцій, які мають число інформаційних відрізків $i = 3$ або $i = 4$ за умови, що $m = \text{const} = 6$?

4. Яким методом можливо фільтрувати (відділяти) дроблення сигналів з тривалістю $I_{\text{др}} \leq 0,5t_0$?

5. Розрахуйте величину середньоквадратичного відхилення ЗМВ (σ_2) для каналу з базою $B = \Delta F \cdot t_0 = 2$, якщо при $B = 1$ $\sigma_1 = 0,02t_0$.

6. Визначте середнє значення плоскої вершини сигналу (рис. 3.17) при передаванні всіх реалізацій ТСК на інтервалі $m = 4$, $s = 4$, $i = 3$ для $B = \Delta F \cdot t_0 = 1$.

7. Як зміниться середнє значення плоскої вершини для умов задачі 6, взявши $i = 2$?

8. Побудуйте залежність $\log_2 N_{\text{рз}}$ при зміні $s \in 2 \dots 10$ для $T_c = 5t_0$.

9. Для умов задачі 8 розрахуйте втрати пропускної здатності при зміні $s \in 2 \dots 10$ для $h = 3$.

10. Визначте, яким способом можливо реалізувати ТСК в каналі з БЧМ $a = 5$ для отримання пропускної здатності згідно з виразом (3.115).

11. Визначте відношення мінімальних енергетичних відстаней для простого коду, реалізованого на інтервалі $T_c = 5t_0$ і надлишкового коду при використанні ТСК при $T_c = 5t_0$; $s = 4$; $i = 3$; $d = 3$.

12. Як зміниться число реалізацій для умов прикладу 9, коли значення коефіцієнтів A_i буде: $A_1 = 2; A_2 = 3; A_3 = 7; A_0 = 17$.

13. Які вектори помилок з мінімальною вагою призводять до невиявлених помилок згідно з умовою якості (2.118а) при параметрах ТСК задачі 12?

14. Які коефіцієнти A_i є достатніми для виправлення помилкового приймання ТСК при $i=3$, якщо допустити, що зміщення на величину $\Theta > \Delta/2$ має тільки один ЗМВ (формула 3.131)?

15. Яка мінімальна кодова відстань між множиною ТСК, задовольняючих умові якості $\sum A_i x_i = 0 \pmod{A_0}$ при $i=3$, якщо коефіцієнти A_i, A_0 вибрані згідно з виразом (3.131), а $l_0 = 1$?

16. Чи можна побудувати код, виправляючий зміщення двох ЗМВ на величину $e_0 = 1$ і одного на $e_0 = 2$ за умовами задачі 15, збільшивши тільки значення A_0 ?

17. Підберіть коефіцієнти для множини ТСК, задовольняючих умові якості при $i=3$ для умови задачі 16.

18. Дайте пояснення на скільки чисельно відрізняється кодова відстань для надлишкових ТСК з $i=3$, задовольняючих умові якості при виборі коефіцієнтів A_i згідно з виразом (3.131) по відношенню до РЦК, виправляючих помилки тієї ж кратності.

19. Дайте своє тлумачення відмінностей кодових відмінностей для РЦК і ТСК для умов задачі 18.

20. Яку кількість реалізацій надлишкових ТСК можна отримати для коду 2 табл. 3.8, якщо $A_1 = 2; A_2 = 3; A_3 = 7; A_0 = 17$. Оцініть еквівалентну зону Δ_e для коду 2 і порівняйте з кодом 1 цієї ж таблиці.

21. Визначте співвідношення $h = \frac{u_c}{u_3}$ для перевищення найквістової швидкості модуляції $M_1 = 1,2; M_2 = 1,4$ за умови, що при $M = 1$ $h = 4$ (рис. 3.24).

22. Визначте залишкову ймовірність приймання кодового слова на виході гауссівського каналу за умови $h_k = 4$, коефіцієнт перевищення найквістової швидкості модуляції $M = 1,6$, число елементів простого коду дорівнює 4, а як надлишкові використовуються елементи, що отримані за рахунок перевищення швидкості модуляції в каналі з базою $B = t_0 \Delta F$.

23. Як зміниться загальна ймовірність помилкового приймання ТСК за умов прикладу 14 (розд. 3.2.8) для $s = 10$?

24. Знаючи середньоквадратичне значення зміщень ЗМВ на виході каналу $\sigma_3 = 0,02t_0$, визначте величину зони, за якої ймовірність помилко-

вого приймання одного ЗМВ ($P_T(1)$) буде більше $P_T(1) \leq 10^{-3}$. Кількість реалізацій ТСК з числом інформаційних ЗМВ при $i=4$ та еквівалентне значення ймовірності помилки одного елемента при перекодуванні ТСК в РЦК.

25. Використовуючи дані табл. 3.11 визначте коефіцієнт групування помилок на виході каналу.

26. Визначте залишкову ймовірність помилки в прийманні сигнальної конструкції коду Хеммінга (9, 5), якщо ймовірності помилок t_k кратних помилок для $t_k \in 1 \dots 7$ відповідає табл. 3.11, а поява 8-кратних і 9-кратних помилок відповідно дорівнюють 0,0003 і 0,0002.

27. Для умов задачі 26 визначте за якого мінімального значення s можна реалізувати 2^9 сигнальних конструкцій на інтервалах $T_c = 5 t_0$.

28. Для умов задач 26 і 27 при знайденому значенні Δ визначте на якому інтервалі $T_c = z t_0$ можливо реалізувати 2^{13} сигнальних конструкцій, що забезпечить виправлення двократних помилок.

29. При знайденому значенні числа найквістового елемента в сигнальній конструкції z (задача 28) визначте середнє значення \bar{i} та ймовірність правильного приймання ТСК в «хорошому» стані каналу при $\sigma_c = 0,002 t_0$.

30. Для знайденого значення $P_{вт}$ (задача 29) таймерної конструкції, яка перетворюється в 13-елементну комбінацію після перекодування ТСК \rightarrow РЦК, знайти еквівалентне значення вірного приймання одного елемента.

Література

1. Аксенов Б.Е. Об одном методе исследования потоков ошибок в каналах связи / Б.Е. Аксенов, А.М. Александров // Проблемы передачи информации. – 1968. – Т. IV, вып. 4. – С. 79-86.
2. Аксенов Б.Е. Применение обобщенного пауссоновского потока к исследованию методов повышения достоверности / Б.Е. Аксенов, А.М. Александров, А.И. Баканов // Проблемы передачи информации. – 1973. – Т. IX, вып. 3. – С. 80-86.
3. Аксенов Б.Е. Повышение эффективности передачи информации в автоматизированных системах управления / Б.Е. Аксенов, А.М. Александров, В.И. Ключко. – Л., 1983. – С. 332.
4. Аршинов М.Н. Коды и математика / М.Н. Аршинов, Л.Е. Садовский. – (Библиотека “Квант”, вып. 30). – М.: Наука, 1983. – 143 с.
5. Басов В.Е. Эффективность совместного использования многопозиционных сигналов и свёрточных кодов: дис... канд. техн. наук: 05.12.02 / Басов В.Е. – Одесса, 2006. – 208 с.
6. Берликэмп Э. Алгебраическая теория кодирования / Берликэмп Э.; пер. с англ.; под ред. С.Д. Бирмана. – М.: Мир, 1971. – 477 с.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р.; пер с англ. – М.: Мир, 1986. – 576 с.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Мир, 1986. – 576 с.
9. 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.
10. 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.
11. Борисов Ю.П., Основы многоканальной передачи информации / Борисов Ю.П., Пенин П.И. – М.: Связь, 1967. – 436 с.
12. Бородин Л.Ф. Введение в теорию корректирующих кодов / Бородин Л.Ф. – М.: Сов. радио, 1968. – 408 с.
13. Буга Н.Н. Основы теории связи и передачи данных / Буга Н.Н. – Ч. 4. – Л.: ЛВИКА им. А.Ф. Можайского, 1970. – 704 с.
14. Буга Н.Н. Основы теории связи и передачи данных / Буга Н.Н. – Ч. I. – Л.: ВИКА им. А.Ф. Можайского, 1968. – 542 с.
15. Варакин Л.Е. Теория систем сигналов / Варакин Л.Е. – М.: Сов. радио, 1978. – 304 с.
16. Витерби А.Д. Принципы цифровой связи и кодирования / А.Д. Витерби, Д.К. Омура. – М., Радио и связь, 1982. – 320 с.
17. Ворон А.А. О спектрах псевдослучайных двоичных последовательностей / Ворон А.А. // Труды ЛВИКА А.Ф. Можайского. – Вып. 472, 1964.
18. 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.
19. Галлагер Р. Теория информации и надежная связь : Галлагер Р.; ПЕР. с англ.; под ред. М.С. Пинскера и Б.С. Цыбакова. – М.: Сов. Радио, 1974. – 304 с.
20. Гитлиц М.В. Теоретические основы многоканальной связи / Гитлиц М.В., Лев А.Ю. – М.: Радио и связь, 1985. – 248 с.
21. Гойхман Э.Ш. Передача информации в автоматизированных системах управления / Гойхман Э.Ш., Лосев Ю.И. – М., 1971. – 160 с.
22. Захарченко В.М. Синтез багатопозиційних часових кодів / Захарченко В.М. – К.: Техніка, 1999. – 281 с.

23. Методи підвищення ефективності використання каналів зв'язку / [Захарченко В.М., Гайдар В.П., Улеєв О.П., Липчпнський О.І.]. – К.: Техніка, 1998. – 248 с.
24. 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.
25. 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. : Техника, 1996. – С. 161-165.
26. 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.
27. 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.
- 28.; 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.
29. Захарченко Н.В. О возможности уменьшения избыточности блочных кодов для каналов с группированием ошибок / Захарченко Н.В. // Тр. УНИИРТ. – 1997. – №3. – С. 73-77.
30. Захарченко Н.В. Эффективность использования многопозиционных кодов в низовых системах ПДИ. МС СССР / Захарченко Н.В. – Одесса: ОЭСИ, 1984. – 92 с.
31. 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.
32. 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.
33. Системы передачи документальной электросвязи : учеб. пособие / Н.В. Захарченко, Б.С. Владишевский, И.А. Киреев, А.П. Улеєв и др.; под ред. Н.В. Захарченко. – Одесса: УГАС им. А.С. Попова, 2000. – 327 с.
34. 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.
35. Методы повышения эффективности использования каналов связи / Захарченко Н.В., Гайдар В.П., Улеєв А.П., Липчанский А.И.. – К.: Техніка, 1998. – 248 с.
36. Захарченко Н.В. Пораметры 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.
37. 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.
38. 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.
39. 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.

40. Захарченко Н.В. Односторонние системы передачи: метод. пособие / Н.В. Захарченко, А.С. Крысько. – Одесса: ОНАС им.А.С. Попова, 2007. – 88 с.
41. 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.
42. 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.
43. 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.
44. Захарченко Н.В. Выбор узлов аппаратуры передачи данных ч.1. учебное пособие / Захарченко Н.В., Нудельман П.Я. // Одесский электротехнический институт связи им. А.С. Попова. – Одесса, 1980. – 92 с.
45. Захарченко Н.В. Основы передачи дискретных сообщений / Захарченко Н.В., Нудельман П.Я., Кононович В.Г. – М.: Радио и связь, 1990. – 240 с.
46. / Эффективные системы передачи информации / Н.В. Захарченко, Е.М. Рудый, А.А. Вараксин, М.А. Мамедов, М.М.Гаджиев; под ред. Н.В. Захарченко. – Баку: ЭЛМ. – 2007. – 568 с.
47. Злотник Б.М. Помехоустойчивые коды в системах связи / Злотник Б.М. – М.: Радио и связь, 1989. – 232 с.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. Игнатов В.А. Теория информации и передачи сигналов / Игнатов В.А. – М.: Сов. радио, 1979. – 280 с.
54. 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.
55. 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.
56. Коган И.М. Прикладная теория информации / Коган И.М. – М.: Радио и связь, 1981.
57. Колесник В.Д. Декодирование циклических кодов / В.Д. Колесник, Е.Т. Мирончиков. – М.: Связь, 1968. – 251 с.
58. Коричнев Л.П. Статистический контроль каналов связи / Л.П. Коричнев, В.Д. Королев. – М.: Радио связь, 1989. – 240 с.
59. Котельников В.А. Теория потенциальной помехоустойчивости / Котельников В.А. – М.: Госэнергоиздат, 1956. – 152 с.

60. Котов П.А. Повышение достоверности передачи цифровой информации / Котов П.А. – М.: Связь, 1966, – 185 с.
61. Коханов О.Б. Оптимальное синхронное линейное детектирование РАМ сигналов с компенсацией фазового сдвига / Коханов О.Б., Захарченко Н.В., Перекрестов И.С. // 36. наукових праць ОНАЗ ім. О.С. Попова. – 2006. – № 1. – С. 18 – 22.
62. Кошевой А.А. Телеметрические комплексы / Кошевой А.А. – М.: Машиностроительные, 1975.
63. Курицин С.А. Теоретические основы построения адаптивных систем: учеб. пособие. / Курицин С.А. – Л.: ЛЭИС, 1983. – 64 с.
64. 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.
65. Мазин И.А. Передача информации в сетях с коммутацией сообщений / Мазин И.А., Уринсон Л.С., Хромешен Г.К. – М.: Связь, 1977. – 326 с.
66. Мазурков М.И. Цифровые методы в радиосистемах передачи информации. – Одесса: ОПИ, 1984. – 101 с.
67. Мазурков М.И. Рекуррентный алгоритм скользящего корреляционного декодирования циклических кодов / Мазурков М.И. // Радиоэлектроника. – 2000. – № 1. – С. 53-59. (Изв. высш. учеб. заведений).
68. 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).
69. 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).
70. Методы и коды сжатия информации / [Мазурков М.И., Ямпольский Ю.С., Бондарь В.И., Чечельницкий В.Я.]. – Одесса: ЛИТО ОНПУ, 1999. – 68 с.
71. Мазурков М.И. Основы теорії передавання інформації / Мазурков М.И. – Одеса. Наука і техніка 2004. – 168 с.
72. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь 1979. – 732 с.
73. Мандзій Б.А., Желяк Р.І. Основы 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.
74. Мановиев А.П. Основы теории радиотелеметрии / Мановиев А.П. – М.: Энергия, 1973. – 592 с.
75. Мешковский К.А. Кодирование в технике связи / К.А. Мешковский, Н.Е. Кириллов. – М.: Связь, 1966. – 340 с.
76. Митряев Е.В. Контроль верности информации в морской радиосвязи / Митряев Е.В., Ростовцев Ю.Г., Рышков Ю.П. – Л.: Судостроение, 1979. – 164 с.
77. Мсеновуев А.П. Введение в цифровую телеметрию / Мсеновуев А.П.. – М.: Энергия, 1967. – 344 с.
78. Основы теории электросвязи. Телекоммуникационные системы коммутации и передачи информации : [учебник] ; под ред. Н.В. Захарченко. – Том 1: Системы электросвязи. – К.: Техніка, 1998. – 303 с.
79. 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.
80. Пухов Г.Е. Вычислительные устройства на таймерных скаляторах / Пухов Г.Е., Бордаченко В.П., Королев Ю.П. – К.: Техніка, 1991. – 215 с.

81. Системы подвижной радиосвязи / [Пышкин И.М., Дежурный И.И., Талызин В.Н., Чвилев Г.Д.]. – М.: Радио и связь, 1986. – 328 с.
82. Системы радио-, телевизионного вещания и документальной электросвязи; под ред. Н.В.Захарченко. – Том 2: Системы электросвязи. – К.: Техніка, 1998 р. – 240 с.
83. Системы частотного мультиплексирования: учеб. пособ.; под ред. Н.В. Захарченко. – К.: Техніка, 2006 р. – 264 с.
84. Финк Л.М. Теория передачи дискретных сообщений / Финк Л.М. – М.: Сов. радио, 1970. – 726 с.
85. Харкевич А.А. Очерки общей теории связи / Харкевич А.А. – М.: Гостехиздат, 1955. – 268 с.
86. Цымбал В.П. Теория информации и кодирования / Цымбал В.П. – К.: Вища школа, 1977. – 288 с.
87. Шеннон К. Математическая теория связи. Работы по теории информации и кибернетике / Шеннон К.; пер с англ.; под ред. Р.Л. Добрушина и О.В. Лупанова. – М.: ИЛ, 1963. – 830 с.
88. 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.
89. 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.

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	0.48422392608909	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	0.417735561323231	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	0.4525450318197053	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	0.499949877899004
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	0.499999999962424
4.520	0.499996908018431	5.520	0.499999983050017	6.520	0.499999999964846
4.530	0.499997050815677	5.530	0.499999983988461	6.530	0.499999999967115
4.540	0.499997187288588	5.540	0.499999984876418	6.540	0.499999999969240
4.550	0.499997317704220	5.550	0.499999985716520	6.550	0.499999999971231
4.560	0.499997442318961	5.560	0.499999986511268	6.560	0.499999999973096
4.570	0.499997561378926	5.570	0.499999987263033	6.570	0.499999999974842
4.580	0.499997675120350	5.580	0.499999987974071	6.580	0.499999999976477
4.590	0.499997783769952	5.590	0.499999988646519	6.590	0.499999999978008
4.600	0.499997887545298	5.600	0.499999989282410	6.600	0.499999999979442
4.610	0.499997986655145	5.610	0.499999989883669	6.610	0.499999999980784
4.620	0.499998081299780	5.620	0.499999990452127	6.620	0.499999999982040
4.630	0.499998171671336	5.630	0.499999990989519	6.630	0.499999999983215
4.640	0.499998257954110	5.640	0.499999991497492	6.640	0.499999999984316
4.650	0.499998340324856	5.650	0.499999991977608	6.650	0.499999999985345
4.660	0.499998418953081	5.660	0.499999992431350	6.660	0.499999999986308
4.670	0.499998494001322	5.670	0.499999992860124	6.670	0.499999999987210
4.680	0.49999856625416	5.680	0.499999993265263	6.680	0.499999999988053
4.690	0.499998633974755	5.690	0.499999993648031	6.690	0.499999999988841
4.700	0.499998699192546	5.700	0.499999994009629	6.700	0.499999999989579
4.710	0.499998761416043	5.710	0.499999994351191	6.710	0.499999999990269
4.720	0.499998820776784	5.720	0.499999994673797	6.720	0.499999999990914
4.730	0.499998877400815	5.730	0.499999994978468	6.730	0.499999999991517
4.740	0.499998931408906	5.740	0.499999995266172	6.740	0.499999999992081
4.750	0.499998982916758	5.750	0.499999995537828	6.750	0.499999999992608
4.760	0.499999032035204	5.760	0.499999995794303	6.760	0.499999999993101
4.770	0.499999078870404	5.770	0.499999996036423	6.770	0.499999999993561
4.780	0.499999123524027	5.780	0.499999996264969	6.780	0.499999999993992
4.790	0.499999166093434	5.790	0.499999996480679	6.790	0.499999999994394
4.800	0.499999206671848	5.800	0.499999996684254	6.800	0.499999999994770
4.810	0.499999245348521	5.810	0.499999996876358	6.810	0.499999999995120
4.820	0.499999282208893	5.820	0.499999997057619	6.820	0.499999999995448
4.830	0.499999317334747	5.830	0.499999997228631	6.830	0.499999999995755
4.840	0.499999350804357	5.840	0.499999997389959	6.840	0.499999999996041
4.850	0.499999382692628	5.850	0.499999997542135	6.850	0.499999999996308
4.860	0.499999413071236	5.860	0.499999997685664	6.860	0.499999999996558
4.870	0.499999442008757	5.870	0.499999997821024	6.870	0.499999999996791
4.880	0.499999469570797	5.880	0.499999997948668	6.880	0.499999999997008
4.890	0.499999495820112	5.890	0.499999998069022	6.890	0.499999999997211
4.900	0.499999520816723	5.900	0.499999998182492	6.900	0.499999999997401
4.910	0.499999544618035	5.910	0.499999998289461	6.910	0.499999999997578
4.920	0.499999567278938	5.920	0.499999998390292	6.920	0.499999999997743
4.930	0.499999588851916	5.930	0.499999998485327	6.930	0.499999999997897
4.940	0.499999609387146	5.940	0.499999998574890	6.940	0.499999999998041
4.950	0.499999628932592	5.950	0.499999998665928	6.950	0.499999999998175
4.960	0.499999647534102	5.960	0.499999998738810	6.960	0.499999999998300
4.970	0.499999665235492	5.970	0.499999998813732	6.970	0.499999999998417
4.980	0.499999682078634	5.980	0.499999998884312	6.980	0.499999999998526
4.990	0.499999698103538	5.990	0.499999998950795	6.990	0.499999999998628
5.000	0.499999713348428	6.000	0.499999999013412	7.000	0.499999999998722

x	$\Phi(x)$	x	$\Phi(x)$	x	$\Phi(x)$
7.000	0.499999999998722	8.000	0.500000000000051	9.000	0.499999999999237
7.010	0.499999999998811	8.010	0.500000000000051	9.010	0.499999999999212
7.020	0.499999999998893	8.020	0.500000000000052	9.020	0.499999999999188
7.030	0.499999999998970	8.030	0.500000000000052	9.030	0.499999999999163
7.040	0.499999999999042	8.040	0.500000000000052	9.040	0.499999999999137
7.050	0.499999999999108	8.050	0.500000000000052	9.050	0.499999999999111
7.060	0.499999999999171	8.060	0.500000000000052	9.060	0.499999999999085
7.070	0.499999999999229	8.070	0.500000000000052	9.070	0.499999999999058
7.080	0.499999999999283	8.080	0.500000000000052	9.080	0.499999999999031
7.090	0.499999999999333	8.090	0.500000000000051	9.090	0.499999999999003
7.100	0.499999999999380	8.100	0.500000000000051	9.100	0.499999999998975
7.110	0.499999999999424	8.110	0.500000000000051	9.110	0.499999999998946
7.120	0.499999999999465	8.120	0.500000000000051	9.120	0.499999999998917
7.130	0.499999999999503	8.130	0.500000000000050	9.130	0.499999999998888
7.140	0.499999999999538	8.140	0.500000000000049	9.140	0.499999999998858
7.150	0.499999999999571	8.150	0.500000000000049	9.150	0.499999999998827
7.160	0.499999999999602	8.160	0.500000000000048	9.160	0.499999999998797
7.170	0.499999999999631	8.170	0.500000000000047	9.170	0.499999999998766
7.180	0.499999999999658	8.180	0.500000000000046	9.180	0.499999999998734
7.190	0.499999999999682	8.190	0.500000000000045	9.190	0.499999999998702
7.200	0.499999999999706	8.200	0.500000000000044	9.200	0.499999999998670
7.210	0.499999999999727	8.210	0.500000000000043	9.210	0.499999999998637
7.220	0.499999999999747	8.220	0.500000000000041	9.220	0.499999999998604
7.230	0.499999999999766	8.230	0.500000000000040	9.230	0.499999999998570
7.240	0.499999999999784	8.240	0.500000000000039	9.240	0.499999999998536
7.250	0.499999999999800	8.250	0.500000000000037	9.250	0.499999999998502
7.260	0.499999999999815	8.260	0.500000000000035	9.260	0.499999999998467
7.270	0.499999999999829	8.270	0.500000000000033	9.270	0.499999999998432
7.280	0.499999999999843	8.280	0.500000000000031	9.280	0.499999999998397
7.290	0.499999999999855	8.290	0.500000000000029	9.290	0.499999999998361
7.300	0.499999999999866	8.300	0.500000000000027	9.300	0.499999999998325
7.310	0.499999999999877	8.310	0.500000000000024	9.310	0.499999999998289
7.320	0.499999999999887	8.320	0.500000000000022	9.320	0.499999999998252
7.330	0.499999999999896	8.330	0.500000000000019	9.330	0.499999999998215
7.340	0.499999999999905	8.340	0.500000000000016	9.340	0.499999999998178
7.350	0.499999999999913	8.350	0.500000000000013	9.350	0.499999999998141
7.360	0.499999999999921	8.360	0.500000000000010	9.360	0.499999999998103
7.370	0.499999999999928	8.370	0.500000000000006	9.370	0.499999999998065
7.380	0.499999999999935	8.380	0.500000000000003	9.380	0.499999999998027
7.390	0.499999999999941	8.390	0.499999999999999	9.390	0.499999999997988
7.400	0.499999999999947	8.400	0.499999999999995	9.400	0.499999999997950
7.410	0.499999999999952	8.410	0.499999999999991	9.410	0.499999999997911
7.420	0.499999999999957	8.420	0.499999999999987	9.420	0.499999999997872
7.430	0.499999999999962	8.430	0.499999999999982	9.430	0.499999999997833
7.440	0.499999999999966	8.440	0.499999999999977	9.440	0.499999999997794
7.450	0.499999999999971	8.450	0.499999999999972	9.450	0.499999999997755
7.460	0.499999999999975	8.460	0.499999999999967	9.460	0.499999999997715
7.470	0.499999999999978	8.470	0.499999999999962	9.470	0.499999999997676
7.480	0.499999999999982	8.480	0.499999999999956	9.480	0.499999999997636
7.490	0.499999999999985	8.490	0.499999999999950	9.490	0.499999999997597
7.500	0.499999999999988	8.500	0.499999999999944	9.500	0.499999999997557
7.510	0.499999999999991	8.510	0.499999999999938	9.510	0.499999999997517
7.520	0.499999999999994	8.520	0.499999999999932	9.520	0.499999999997478

7.530	0.499999999999997	8.530	0.499999999999925	9.530	0.499999999997439
7.540	0.499999999999999	8.540	0.499999999999911	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	10.000	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. Значимо, 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 кожному 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, будемо 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} , 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 вписаний 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 будемо 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, названий 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	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	0	3	2	1	0	1	2	3
2	2	3	0	1	2	0	2	3	1
3	3	2	1	0	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

$$u = a_1v_1 + a_1v_2 + \dots + a_kv_k,$$

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

$$a_1v_1 + a_1v_2 + \dots + a_kv_k = \mathbf{0}.$$

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'яже 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 *повненням* 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 $v_1, \dots, v_k \in$ 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 кінцевовимірною 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 $w = c_1w_1 + \dots + c_nw_n \dots$ Тоді

$$w \cdot u = (c_1w_1 + \dots + c_nw_n) \cdot u = c_1w_1 \cdot u + \dots + c_nw_n \cdot u \dots$$

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

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

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

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \quad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

і $C = AB$, то за умови коректного вибору розмірів блоків (коректного в тому розумінні, що всі добутки й суми матриць визначені)

$$C = \begin{bmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{bmatrix}.$$

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 противному 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 $n \in \mathbb{N}$ є 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 випливають 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 и 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 підібрану так звану *елементарну $(n \times n)$ -матрицю F* . Елементарні матриці визначаються як одна з наступних модифікацій одиничної матриці:

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & 1 & & \\ & & & \ddots & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \ddots & & & \\ & & & a & & \\ & & & & \ddots & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix} \text{ або } \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & a & 1 \\ & & & & & \\ & & & & & & 1 \end{bmatrix}$$

Елементарні операції над рядками використовуються для надання матриці стандартного вигляду, названого *канонічним ступінчастим виглядом* і визначає 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

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Значимо, 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 – невідроджена 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 невивроженої 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_i 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 $\{g_i, \dots, g_k\}$ – 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

$$G(a_1 f_1^T + \dots + a_{n-r} f_{n-r}^T) = 0,$$

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

$n = 3$	L	$n = 8$	L	$n = 9$	L
1101	7	100101011	255	1001101111	511
$n = 4$	L	100101101	255	1001110111	511
10011	15	100111001	17	1001111101	511
11001	15	100111111	85	1010000111	511
11111	5	101001101	255	1010010101	511
$n = 5$	L	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
$n = 6$	L	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
$n = 7$	L	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	$n = 9$	L	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
11111011	127	1001011001	511	1111010101	511
11111101	127	1001011111	511	1111011001	511
$n = 8$	L	1001100101	73	1111100011	511
100011011	51	1001100101	511	1111101001	511
100111011	255	1001101001	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 Слєпяна

(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 Слєпяна

(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										

Навчальне видання

Захарченко Микола Васильович

**СИСТЕМИ ПЕРЕДАВАННЯ ДАНИХ
Том 1. Завадостійке кодування**

Підручник

Видано в авторській редакції

Редактор Л. А. Кодрул, В. В. Терземан

Верстка О. М. Мартинова

Обкладинка Ж. А. Гардиман

Видавник ПП "Фенікс"

(Свідоцтво ДК № 1044 від 17.09.02)

м. Одеса, вул. Зоопаркова, 25. Тел. 7777-591.

Підписано до друку 7.01.09. Формат 60x90/16.

Зам. № 40/09. Наклад 400 прим. Обл.-др. арк. 28,0.

Ціна договірна.

Віддруковано з готового оригінал-макету

у принт-студії "Абрикос" СПД Бровкін О.В.

м. Одеса, вул. Зоопаркова, 25; тел. 357-343.