12 ВИБІР ЗАВАДОСТІЙКОГО КОДУ

12.1 Кодова відстань коригувальних кодів і обгрунтування вибору кодів.
12.2 Код з перевіркою на парність.
12.3 Ітеративний код.
12.4 Код Хеммінга.
12.5 Циклічні коди.

Завадостійкими (коригувальними) називаються коди, що дозволяють виявляти й виправляти помилки в прийнятих кодових послідовностях. *Коригувальна здатність* коду залежить від кодової відстані d, чисельно рівної *мінімальному числу елементів, якими відрізняється будь-яка кодова комбінація від іншої.* У загальному випадку

$$d = t_o + t_u + 1, \qquad (1)$$

де t_o й t_u – число виявлених і виправлених помилок відповідно, причому обов'язково $t_o \geq t_u$.

Якщо код тільки виявляє помилки, то $d = t_o + 1$, а у випадку тільки виправлення $d = 2t_o + 1$. Кількість перевірочних елементів r коригувального коду залежить від виду коду, а число інформаційних елементів $k = n - r$, де n – довжина двійкової послідовності, що кодується завадостійким кодом. Відношення r/n називають коефіцієнтом надмірності коду.

Код з перевіркою на парність – один із простих кодів, що дозволяють виявляти одиночні помилки. Він утворюється шляхом додавання до переданої комбінації, що складає з k інформаційних символів ненадлишкового коду, одного контрольного біта так, щоб загальна кількість одиниць у переданій комбінації була парною. У результаті загальна кількість елементів у переданій комбінації $n = k + 1$. На прийомній стороні роблять перевірку на парність. При парному числі одиниць передбачається, що помилок немає, і споживачеві видається k біт, а контрольний елемент відкидається. Аналогічно може бути побудований код з перевіркою на непарність.

Імовірність невиявлених помилок для коду з перевіркою на парність залежить від довжини блоку n й імовірності P_o помилкового прийому одиничного елемента:

$$P_{кк} \approx C_n^2 P_o^2 (1-P_o)^{n-2}. \qquad (2)$$

Як показують розрахунки по (2), для забезпечення ймовірності помилки по символах менш $1 \cdot 10^{-6}$ припустима довжина кодової комбінації n становить декілька байт.

Ітеративний код характеризується наявністю 2 або більше систем перевірок усередині кожної кодової комбінації. Він будується в такий спосіб: до 7-елементного коду КОИ-7 додають перевірочний біт, що розташовується у восьмій позиції. Елементи переданого блоку й перевірочні біти утворять матрицю:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} & r_1 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} & r_2 \\ . & . & . & . & . & . \\ a_{71} & a_{72} & a_{73} & \dots & a_{7n} & r_7 \\ q_1 & q_2 & q_3 & \dots & q_n & q_{n+1} \end{vmatrix},$$

де a_{ij} – інформаційні біти, $i = 1,2,...,7;\ j = 1,2,...,n$;

$q_1,\ q_2,\dots,q_n$ – перевірочні біти знаків, що утворять першу сукупність перевірок.

Наприкінці матриці стоять біти перевірки на парність r_i, $i = 1,2,...,7$, які є сумою по модулю 2 всіх елементів рядка; $r_1 - r_7$ включається в знак перевірки – це друга сукупність перевірок. До семи елементів знаку додається восьмий перевірочний біт q_{n+1}. Перевірочні біти $q_1,\ q_2,\dots,q_n,q_{n+1}$ формуються таким чином, щоб число одиниць у стовпці було парним для асинхронних систем і непарним – для синхронних. Кожний знак потрібно передавати послідовно, починаючи з першого біта a_{ij} й кінчаючи восьмим перевірочним.

Початковий знак блоку ПТ (початок тексту) і символ СИН (синхронізація) не слід включати в підсумовування. При використанні ітеративного коду в блок обов'язково включається

комбінація КБ (кінець блоку), що вказує, що далі слідує знак перевірки матриці.

Наведений ітеративний код є найпростішим кодом цього класу. Кодова відстань для нього $d = 4$. Він виявляє всі помилки кратності до трьох і непарної кратності, а також будь-який пакет помилок довжиною $l+1$, де l довжина рядка матриці коду. Основним недоліком ітеративних кодів, що використають перевірки на парність по стовпцях і рядкам, є їх відносно висока надмірність $(\approx 15\%)$. Однак кодування й декодування таких кодів дуже просто реалізуються програмними методами, тому найпростіші ітеративні коди доцільно використати в АПД із мікропроцесорними ПЗП. При більше жорстких вимогах по вірогідності передачі даних застосовують ітеративний код із трьома перевірками.

Код Хеммінга – один з найбільш ефективних кодів, що дозволяють виправляти одиночні помилки. Кодова відстань $d = 3$**.** Код утворюється шляхом доповнення інформаційної частини переданого блоку, що складається з k біт, r перевірочними елементами, причому в інформаційну частину при кодуванні можна включати й службові символи (номер, початок і кінець блоку), за винятком маркерних комбінацій, які доцільно розташовувати на початку блоку. При виборі довжини переданого блоку n й кількості перевірочних елементів r варто керуватися нерівністю $2^r \geq n+1$. З огляду на те, що $r = n-k$, нерівність запишеться у вигляді

$$2^k \leq \frac{2^n}{n+1}, \qquad (3)$$

де n й k – цілі числа. Нерівність є вихідною для визначення довжини кодової комбінації по заданому числу k.

Перший перевірочний елемент $П_1$ коду Хеммінга утвориться підсумовуванням по модулю 2 всіх непарних біт блоку, починаючи з першого:

$$П_1 = a_1 + a_3 + a_5 + a_7 + \ldots . \qquad (4)$$

Результат перевірки $П_2$ визначає другий розряд перевірочної комбінації (синдрому помилки). Він обчислюється підсумовуванням тих біт блоку, номера яких відповідають n-розрядним двійковим числам, що мають одиницю в другому розряді, тобто

$$П_2 = a_2 + a_3 + a_6 + a_7 + a_{10} + a_{11} + \ldots \ . \qquad (5)$$

Третя перевірка $П_3$ охоплює розряди, номери яких відповідають n-розрядним числам, що мають одиницю в третьому розряді. Аналогічно перебувають розряди, охоплювані четвертою, п'ятою і т.д. перевірками:

$$П_3 = a_4 + a_5 + a_6 + a_7 + a_{12} + a_{13} + a_{14} + a_{15} + \ldots,$$
$$П_4 = a_8 + a_9 + a_{10} + a_{11} + a_{12} + a_{13} + a_{14} + a_{15} + \ldots, \qquad (6)$$
$$П_5 = a_{16} + a_{17} + a_{18} + a_{19} + a_{20} + \ldots .$$

Місце розташування перевірочних елементів не має значення, їх можна розміщати перед, після й чергуючи з інформаційними символами. Якщо їх розташувати на місцях кратні ступені 2, тобто на позиціях 1, 2, 4, 8 і т.д., то код двійкового числа, утвореного перевірочними елементами, на прийомній стороні буде вказувати номер розряду, у якому відбулася помилка.

Циклічні коди знаходять найбільше поширення в системах передачі даних з вирішальним зворотним зв'язком, що обумовлено їх високими коригувальними властивостями, порівняно простою реалізацією, невисокою надмірністю. Особливо вони ефективні при виявленні пакетів помилок. Циклічні коди відносяться до блокових систематичних кодів, у яких кожна комбінація кодується самостійно у вигляді блоку таким чином, що інформаційні k й перевірочні r елементи завжди перебувають на певних місцях. Для спрощення процедури кодування й декодування перевірочні біти розміщають наприкінці блоку. *Кодування переданого повідомлення здійснюється множенням двійкової послідовності* $G(x)$ *на одночлен* x^r*, що має ту же ступінь, що й утворюючий*

поліном $P(x)$*, з додаванням до цього добутку залишку* $R(x)$*, отриманого після ділення добутку* $G(x)x^r$ *на утворюючий поліном, тобто передане в канал зв'язку повідомлення* $F(x)$ *має вигляд*

$$F(x)=G(x)x^r+R(x). \qquad (7)$$

При декодуванні прийнята послідовність $F(x)$ знову ділиться на утворюючий поліном $P(x)$. Отриманий нульовий залишок $R(x)=0$ свідчить про відсутність помилок у прийнятому блоці, а відмінність від нуля – про наявність помилок. Аналізуючи залишок, можна визначити номера перекручених розрядів і скорегувати їх.

Для побудови циклічних кодів в якості утворюючих поліномів використовуються неприводимі багаточлени. Вони діляться без залишку тільки на себе й на одиницю. $P(x)$ може бути представлений в алгебраїчній формі або у вигляді двійкового або восьмеричного числа. В останньому випадку кожна восьмерична цифра відображає три двійкових розряди. Наприклад, для полінома $P(x)=x^5+x^3+1$ двійковий запис має вигляд 101001, а відповідна йому восьмерична – 51. У таблиці 1 наведені вибірково багаточлени, що не приводяться, до 12-го ступеню включно. Поліноми записані в алгебраїчній формі й у вигляді восьмеричних чисел (для ступенів $r\geq 6$ – тільки восьмеричними числами).

При виборі утворюючого полінома $P(x)$ варто мати на увазі, що показник ступеня утворюючого полінома не може бути менше числа перевірочних елементів r. Для спрощення технічної реалізації кодерів і декодерів необхідно вибирати ступінь полінома, рівний r. Якщо в таблиці є кілька багаточленів, які не приводяться, з даним ступенем, то доцільно вибрати найкоротший, причому число ненульових членів $P(x)$ не повинно бути менше необхідної кодової відстані (1).

Таблиця 1 – Вибіркові неприводимі багаточлени до 12-го ступеня включно

r	$P(x)$		r	$P(x)$
2	x^2+x+1	7	7	211, 217, 235,
3	x^3+x+1	13	8	747, 435, 543
4	x^4+x^2+1	23	9	1055, 1751
5	x^5+x^2+1	45	10	2033, 3177
6	$x^5+x^4+x^3+x^2+1$	75	11	7413, 4505
		103, 147	12	15647, 11015

Існує безліч різновидів циклічних кодів, при наявності пакетів помилок, розглянемо коди, найбільш широко використовувані для виправлення й виявлення таких пакетів.

Циклічні коди з кодовою відстанню $d \geq 5$ розроблені Боузом, Чоудхурі й Хоквінгемом (БЧХ-коди), виявляють і виправляють будь-яке число помилок. При кодуванні заданим є число t_u помилок, які потрібно виправити, і довжина блоку n. Необхідно визначити число інформаційних k і перевірочних r елементів, а також вид утворюючого полінома.

Довжина кодової комбінації визначається по формулі

$$n = 2^m - 1, \qquad (8)$$

де m – ціле число. Наприклад, при $m=6$ $n=63$; при $m=7$ $n=127$; при $m=8$ $n=255$ й т.д.

Утворюючий поліном знаходиться як найменше спільне кратне (НЗК) мінімальних непарних поліномів $m_i(x)$ до порядку $2t_u - 1$ включно:

$$P(x) = \text{НОК}\{m_1(x)m_3(x)...m_{2t_u-1}(x)\}. \qquad (9)$$

Мінімальний багаточлен являє собою простий неприводимий поліном. Існують багаточлени того самого порядку різних стукенів. Показник ступеня мінімальних багаточленів, що входять в (9), повинен бути рівний m, для якого справедливо (8). Так як порядок (номер) самого старшого мінімального багаточлена $2t_u - 1$, то кількість багаточленів, що входять в (9), дорівнює числу помилок t_u які можна виправити.

Наприклад, якщо $t_u = 5$, те $2t_u - 1 = 9$ й в (9) будуть входити багаточлени $m_1(x)$, $m_3(x)$, $m_5(x)$, $m_7(x)$, $m_9(x)$.

Мінімальні багаточлени циклічних кодів різних ступенів представлені в таблиці 2, де значення $m_i(x)$ дані у восьмеричній системі числення. Так, поліном 13-го порядку 9-й ступеня, представлений числом 453, у двійковій формі має вигляд 100101011, а багаточлен записується як $x^8 + x^5 + x^3 + x + 1$. Для знаходження $P(x)$ необхідно виписати з таблиці 2 всі значення мінімальних поліномів, що відповідають показнику ступеня m, до порядку $2t_u - 1$ включно.

Приклад. Розрахувати параметри коду для симплексного ПЗП, що дозволяє виправляти чотириразові помилки. Ефективна швидкість видачі інформації споживачеві повинна становити не менш 90% технічної швидкості передачі по каналі зв'язку.

Таблиця 2 – Мінімальні багаточлени циклічних кодів

Порядок полінома	Мінімальні поліноми при значенні степеня *m*								
	2	3	4	5	6	7	8	9	10
1	7	13	23	45	103	211	435	1021	2011
3	–	–	37	75	127	217	567	1131	2017
5	–	–	07	67	147	235	763	1461	2415
7	–	–	–	–	111	367	551	1231	3771
9	–	–	–	–	015	277	675	1423	2257
11	–	–	–	–	155	326	747	1055	2065
13	–	–	–	–	–	203	453	1167	2157
15	–	–	–	–	–	–	727	1541	2653

Визначимо необхідну кодову відстань, що дозволяє виправляти чотирикратні помилки. Відповідно до (1) $d = 2t_u + 1 = 2 \cdot 4 + 1 = 9$. Тому що $d > 5$, то для виправлення помилок варто застосувати БЧХ код с $d = 9$. Для виконання умови (8) довжину блоку інформації будемо вибирати з ряду: 127, 255, 511, 1023 і т.д. Нехай $n = 127$, тоді по (8) $m = 7$. Кількість контрольних розрядів у блоці буде $r \le m \cdot t_u \le 7 \cdot 4 = 28$. Отже, число інформаційних елементів у блоці $k = n - r = 127 - 28 = 99$. Ефективна швидкість видачі інформації

(при відсутності в блоці службових біт) складе $V_{еф} = V(127-28)/127 \approx 0{,}78 \cdot V$, що не задовольняє технічним вимогам.

Проведемо аналогічні розрахунки при $n = 255$, одержимо $V_{еф} = 0{,}87 \cdot V$. Приймемо $n = 511$, тоді з (8) $m = 9$, а $r \le 9 \cdot 4 = 36$. Кількість інформаційних біт у блоці $k = 475$. Так як довжина інформаційної частини блоку повинна бути кратна байту, то число знаків у блоці $k_{зн} = 475/8 = 59$. Тоді довжина інформаційної частини $k = 59 \cdot 8 = 472$. Вільні три біта можуть бути використані для передачі, наприклад, номера блоку. Ефективна швидкість видачі інформації споживачеві складе $V_{еф} = 0{,}92 \cdot V$. Якщо $V_{еф}$ виявиться менше припустимої або в переданий блок потрібно ввести додаткові службові символи, то n варто взяти 1023 або наступне число з ряду.

Вид утворюючого полінома визначимо по (9). Кількість мінімальних багаточленів дорівнює $t_u = 4$, причому порядок останнього $2t_u - 1 = 7$, а старший показник ступеня $m = 9$. Виписуємо з таблиці 2 мінімальні багаточлени необхідного ступеня й з врахуванням (26) одержуємо

$$P(x) = \left(x^9 + x^4 + 1\right) \cdot \left(x^9 + x^6 + x^4 + x^3 + 1\right) \times$$
$$\times \left(x^9 + x^8 + x^5 + x^4 + 1\right) \cdot \left(x^9 + x^7 + x^4 + x^3 + 1\right).$$

Число контрольних елементів отриманого БЧХ коду визначається показником ступеня отриманого утворюючого полінома й дорівнює 36.

Із циклічних кодів, що виявляють і виправляють пакети помилок, найбільш ефективним є циклічний код Файра, утворюючий поліном якого $P_ф(x)$ визначається виразом:

$$P_ф(x) = P(x) \cdot \left(x^c + 1\right), \qquad (10)$$

де $P(x)$ – багаточлен, що неприводиться, степеня m.

Коди Файра можуть виправляти одиночний пакет помилок довжиною b_u й одночасно виявляти пакет довжиною b_o за умови

$$c \geq b_u + b_o - 1,\ m \geq b_u, \tag{11}$$

c не повинне ділитися на число e без залишку ($e = 2^m - 1$). Якщо застосовувати ці коди тільки для виявлення помилок, то можна виявити будь-який одиночний пакет помилок, довжина якого менше або дорівнює числу перевірочних елементів:

$$r = c + w. \tag{11}$$

Неприводимий багаточлен $P(x)$ вибирають із таблиці 1 згідно (11) , але так, щоб задовольнялася умова (12). Довжина блоку n дорівнює найменшому спільному кратному чисел e і c: $n = \text{НСК}\{e,c\}$, а число перевірочних елементів $r = c + m$.

Приклад. Визначити параметри коду Файра, використовуваного в ПЗП для виявлення одиночних пакетів помилок довжиною 16 біт.

Рішення. Для виявлення пакета помилок довжиною 16 біт утворюючий поліном $P_\phi(x)$ повинен мати показник ступеня $r \geq 16$. Кількість помилок, що $b_u = 0$ виправляють, отже, згідно (28) $m \geq 0$. Для зменшення надмірності коду збільшимо довжину блоку n переданого повідомлення, приймемо $m = 5$. Тоді $e = 2^5 - 1 = 31$. Так як c не повинне ділитися цілком на e, то c з урахуванням (29) одержимо $c = 11$. Довжина блоку $n = \text{НСК}\{e,c\} = 31 \cdot 11 = 341$ біт. З таблиці 1 вибираємо полином, що неприводиться, з показником ступеня $m = 5$: $P(x) = x^5 + x^2 + 1$. Тоді утворюючий поліном коду Файра має вигляд

$$P_\phi(x) = \left(x^5 + x^2 + 1\right) \cdot \left(x^{11} + 1\right) = x^{16} + x^{13} + x^{11} + x^5 + x^2 + 1.$$

Кількість інформаційних елементів у блоці $k = n - r = 341 - 16 = 325$. Надмірність переданого повідомлення $R = r/n = 16/341 = 0{,}047$, тобто менш 5%.

Як ми вже відзначали вище, при виборі довжини блоку переданого повідомлення необхідно враховувати властивості кодів, які накладають обмеження на n. З іншого боку, n повинне бути кратним довжині застосовуваних символів: 8 (байту) або 7 (код КОІ-7). Для виконання цих вимог роблять скорочення довжини блоку до значення, кратного переданим символам при збереженні кількості перевірочних елементів, необхідних для виявлення або виправлення помилок. Коригувальні здатності вкороченого циклічного коду й вихідного повністю збігаються. Такий укорочений код часто називають псевдоциклічним.