Текст лекції

Циклічні коди

Циклічні коди є різновидом систематичних кодів і мають усі їх властивості. Спочатку вони були створені з метою спрощення схем кодування і декодування. Згодом виявилися їх високі коригувальні властивості, що і забезпечило їм широке поширення на практиці.

При побудові циклічних кодів кодові комбінації подають у вигляді поліномів

$$G(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0 \qquad (10.15)$$

де $a_0, a_1,...,a_{n-1}$ - коефіцієнти, що набувають значень 0 або 1. Наприклад, комбінацію 1100101 можна записати як $G(x) = x^6 + x^5 + x^2 + 1$.

Основна властивість розглянутих кодів в тому, що циклічний зсув дозволеної кодової комбінації також є дозволеною кодовою комбінацією. Отже, якщо комбінація 1000111 є дозволеною, то комбінації 0001111, 0011110 і т. д. теж дозволені. Нульова комбінація є дозволеною, оскільки циклічний код належить до класу систематичних. Зазначимо, що циклічний зсув нульової комбінації є також нульовою комбінацією.

Можна показати, що циклічний зсув є еквівалентним множенню на x - кодової комбінації, записаної у вигляді полінома [8]. Дійсно,

$$xG(x) = a_{n-1}x^n + a_{n-2}x^{n-1} + ... + a_1x^2 + a_0x.$$

Оскільки в кодовій комбінації, що має довжину n, ступінь полінома не може перевищувати n-1 (у противному випадку довжина кодової комбінації перевищить n), то x^n замінюють на 1. При цьому

$$xG(x) = a_{n-2}x^{n-1} + ... + a_1x^2 + a_0x + a_{n-1}.$$

Отже, $xG(x)$ є циклічним зсувом комбінації $G(x)$.

Циклічні коди прийнято визначати за допомогою так званих твірних поліномів $P(x)$ ступеня n. Твірну матрицю циклічного коду можна утворити з твірного полінома циклічним зсувом останнього (або, що те саме, множенням його на $x, x^2,..., x^{n-1}$):

$$G=\begin{vmatrix} P(x) \\ xP(x) \\ x^2P(x) \\ x^{k-1}P(x) \end{vmatrix} \qquad (10.16)$$

Безпосередньо з твірної матриці (10.16) випливає, що всі дозволені кодові комбінації циклічного коду без остачі діляться на вироблюваний поліном. Нагадаємо, що тут і далі мається на увазі ділення за модулем 2. Останнє виконується майже так само, як звичайне ділення, з тією різницею, що в процесі ділення операція віднімання замінюється додаванням за модулем 2. Поліном $x^6+x^5+x^3+1$ на поліном x^2+x+1 (відповідні двійкові форми 1101001 і 111) ділиться так:

```
⊕1101001 | 111
 111     | 10101
 ⊕110
  111
  ⊕101
   111
    10
```

Двочлен 10 є остачею від ділення полінома 1101001 на поліном 111.

Оскільки кожна дозволена комбінація без остачі ділиться на твірний поліном, то ця обставина стає основою дуже зручного способу визначення приналежності прийнятої кодової комбінації до дозволених.

Розглянемо принцип побудови циклічних кодів. Кожну кодову комбінацію $G(x)$ простого k - елементного коду помножимо на x^r, а потім поділимо на твірний поліном степеня r. Внаслідок множення степінь кожного члена x_i, що входить у поліном $G(x)$, підвищується на r. При діленні добутку $x^rG(x)$ на $P(x)$ виходить частка $Q(x)$ такого самого степеня, що $G(x)$. Крім того, якщо добуток $x^rG(x)$ не ділиться на $P(x)$ без остачі. То остачею є $R(x)$:

$$\frac{x^rG(x)}{P(x)} = Q(x) \oplus \frac{R(x)}{P(x)} \qquad (10.17)$$

Оскільки частка $Q(x)$ має той самий степінь, що $G(x)$, то вона також є комбінацією простого k-елементного коду.

Помноживши обидві частини рівності (10.17) на $P(x)$, маємо

$$F(x) = Q(x)P(x) = x^r G(x) \oplus R(x) \qquad (10.18)$$

Отже, кодову комбінацію циклічного коду можна отримати двома способами:

• множенням *k*-елементної комбінації простог о коду на твірний поліном $P(x)$;

• множенням кодової комбінації простого коду на одночлен x^r і додаванням до цього добутку остачі від ділення добутку $x^r G(x)$ на $P(x)$.

Зазначимо, що перший спосіб спричинює утворення нероздільного коду. Нероздільність значно ускладнює процес декодування, тому на практиці використовується інший спосіб побудови кодових комбінацій. Дуже важливо, що цей спосіб дає можливість одержати твірну матрицю відразу в канонічній формі:

$$G=\left|E_k, C_{r;k}\right|$$

де $C_{r,k}$ - матриця, що складається з *r* стовпців і *k* рядків, причому кожен рядок є остачею від ділення рядка одиничної матриці, доповненої *r*-нулями, на твірний поліном.

Кодують і декодують циклічні коди не на основі обчислення перевірок на парність, а на основі ділення на твірний поліном. Проте за необхідності перевірну матрицю можна побудувати обчисленням перевірного полінома:

$$h(x) = \frac{x^n + 1}{P^{-1}(x)} \qquad (10.19)$$

де $P^{-1}(x)$ - поліном, обєднаний зтвірним поліномом $P(x)$. Нагадаємо, що в обєднаних поліномах члени розташовані в зворотному порядку. Так, наприклад, поліноми 100111 і 111001 є об'єднаними. Перший рядок перевірної матриці циклічного коду є перевірним поліномом $h(x)$, помноженим на x^{r-1} (тобто доповнений праворуч (r-1)-нулями). Наступні рядки перевірної матриці є циклічним зсувом першої.

Перевірна матриця може бути також побудована звичайним способом, виходячи з твірної матриці. Побудована таким способом перевірна матриця

зовні може відрізнятися від побудованої за допомогою перевірного полінома, однак обидві матриці завжди можуть бути зведені до одного виду.

Наведемо приклад побудови семирозрядного циклічного коду з d_0 = 3. Для цього потрібні три перевірних розряди (d_0 =3) і утворювальний поліном має бути третього степеня. Нехай твірний поліном $P(x) = x^3 + x + 1$=1011. (Принципи вибору твірного полінома розглянемо пізніше.) Твірна матриця має вигляд

$$G=\begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{vmatrix}$$

Нагадаємо, що перевірні розряди 101 маємо внаслідок ділення комбінації 1000000 на твірній поліном 1011, а 111 - внаслідок ділення 100000 на той самий твірній поліном і т. д.

Перевірний поліном

$$h(x)=\frac{x^7+1}{(x^3+x+1)^{-1}}=\frac{10000001}{1101}=11101,$$

отже, перевірна матриця

$$H=\begin{vmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{vmatrix}$$

Якщо будувати твірну матрицю з породжувальної, то одержимо матрицю

$$H'=\begin{vmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}$$

яка відрізняється останнім рядком від раніше отриманої матриці *H*. Однак цю відмінність можна ліквідувати, якщо до останнього рядка матриці H' додати перший рядок; при цьому матриця H' збігається з матрицею *H*.

Коригувальна здатність циклічного коду цілком визначається виглядом твірного полінома. Для деяких циклічних кодів можна сформулювати досить прості принципи вибору вигляду твірного полінома.

Циклічний код з d_0 = 2. Твірний поліном має вигляд x + 1. Цей поліном дає змогу будувати код будь-якої довжини. Циклічний код з d_0= *2* виявляє будь-яку непарну кількість помилок і повністю тотожний коду з парним числом одиниць.

Твірним поліномом для циклічного коду з d_0 =2 може бути також поліном $x^2 + x + 1$. Код при цьому має підвищену завадостійкість - виявляються не тільки будь-які помилки непарної кратності, але й будь-які парні суміжні помилки (тобто пакети помилок завдовжки 2), а також усі парні помилки, поділені одним неспотвореним розрядом.

Циклічний код з d_0 = 3 є різновидом кодів Хемінга. Довжину кодової комбінації вибирають з умови $n = 2^r-1$. Твірним поліномом може бути будь-який *незвідніші поліном* степеня *r*. (Поліном називається незвідним. якщо він ділиться без остачі тільки на одиницю і на самого себе.) Незвідні поліноми до п'ятого степеня включно наведені на стор. 393. Відомості про незвідні поліноми більш високих степенів є в літературі [1,3].

Циклічний код з d_0 = 4 є також різновидом кодів Хемінга і будується на основі твірних поліномів для кодів з d_0 =3. Твірний поліном циклічного коду з d_0 = 4 є добутком двочлена $x+1$ на незвідний поліном, що придатний як твірний для коду з d_0 =3. Довжину кодової комбінації вибирають з умови $n = 2^m - 1$; число перевірних розрядів $r= m+1$. Так, наприклад, при n =1 твірний поліном має вигляд $(x+ 1)(x^3 + x +1)= x^4 + x^3 + x^2 +1$.

Степінь полінома Вигляд полінома

1	$1+x$
2	x^2+x+1
3	x^3+x+1
	x^3+x^2+1
4	x^4+x+1
	x^4+x^3+1
	$x^4+x^3+x^2+x+1$
5	x^5+x^2+1
	x^5+x^3+1
	$x^5+x^3+x^2+x+1$
	$x^5+x^4+x^2+x+1$
	$x^5+x^4+x^3+x+1$
	$x^5+x^4+x^3+x^2+1$