УДК 512:681

КОРИГУВАЛЬНІ КОДИ, МНОГОЧЛЕНИ І МАТРИЦІ

Студ. М.Ю. Білич, гр.БЕК 1-15
Наук. керівник доц. О.Л. Блохін
Київський національний університет технологій та дизайну

Циклічні коди застосовуються в основному при передачі даних між комп'ютерами і дисководами. В свою чергу, циклічні коди являються підкласом в класі *лінійних кодів*, які задовольняють структурним вимогам. Прикладом класичного лінійного коду є код Хеммінга, для якого виконується умова: $n=2^m - 1$.

Важливість циклічних кодів обумовлена ще тим, що вони приводять до ефективних процедур шифрування і дешифрування, легко реалізованим з допомогою логічних схем. Розглянемо коротко принцип цього кодування:

Інформаційне повідомлення $a=a_0a_1 \dots a_{k-1}x^{k-1}$, можна записати за допомогою многочлена: $a(x)=a_0+a_1x+a_2x \dots a_{k-1}x^{k-1}$. Якщо многочлен a(x) помножити на x^m, то символи, які зіставляють повідомлення, будуть коефіцієнтами при більш високих степенях. Далі $a(x)x^m$ розділимо на примітивний многочлен g(x), тим самим знайшовши частку від ділення p(x) і залишок r(x).

Нехай *a=1001, k=4, m=3, n=7, g(x)=1+x+x³* – примітивний многочлен. Знайдемо многочлен, який відповідає коду a: $a(x)= 1+x^3$;

$x^3a(x) = g(x)p(x)+r(x) = (1- x+x^3)(x+x^1)+(x+x^2)$; $F(x) = x+x^2+x^3+x^6$; f=011 1001.

При шифруванні кодовий многочлен f(x) множиться на перевірочний h(x), в результаті отримаємо: $A(x)=f(x)h(x)=a(x)g(x)h(x)=a(x)g(x)h(x)=a(x)(x^n+1)=a(x)s(x)a(x)$, де s(x) – синдром помилки, виконуючий роль коду помилки: s=r.

Замість многочленів можна використовувати матриці. Щоб отримати кодове слово f,

потрібно інформаційне слово *a* помножити на матрицю *G*. Отримуємо формулу f=a*G. Так, якщо a=011- інформаційне слово з k=3 символів і задана матриця G розміром 3x5, то кодове слово буде зіставлятись з n=5 символів, з яких два останніх (m=2) є перевірочним

$$f = a * G = (011)\begin{pmatrix} 1\,0\,0\,1\,0 \\ 0\,1\,0\,0\,1 \\ 0\,0\,1\,1\,1 \end{pmatrix} = 01110$$

Код Хеммінга може бути перетворений в циклічний код з стрічковою матрицею G, утвореною від генеруючого многочлена $g(x) = 1+x^2+x^3$. Для кодування інформації та утворення і виправлення одразу декількох помилок Боуз, Чоудкурі і Хідквінгем (скорочено код БЧХ) запропонували використовувати одразу декілька генеруючих многочленів $g_1(x)$. Генеруючий многочлен БЧХ – кода можна представити у вигляді:

$$g(x) = \text{НСК}[g_1(x), g_2(x), g_3(x), \dots g_{2t}(x)]$$

де $g_1(x)$ – многочлени, t- число помилок. Так для виправлення двох помилок з довжиною слова $n-2^4 -1 = 15$ отримуємо генеруючий многочлен:

$$\begin{aligned} \boldsymbol{g(x)} &= \text{НСК}[\boldsymbol{g_1(x), g_2(x), g_3(x), g_4(x)}] \\ &= \text{НСК}[\boldsymbol{x^4 + x + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x} \\ &\boldsymbol{+ 1}] = \boldsymbol{(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)} \\ &= \boldsymbol{x^8 + x^7 + x^6 + x^4 + 1} \end{aligned}$$

ми отримали корегувальний БЧХ-код.