УДК 004.627

**Д.т.н., професор Дичка І. А., студент Кучмій О. Е.,
асистент Дрозденко Л. В.**

**Національний технічний університету України
«Київський політехнічний інститут імені Ігоря Сікорського»**

ВИЗНАЧЕННЯ ТВІРНИХ МНОГОЧЛЕНІВ ДВІЙКОВИХ КОРЕКТУВАЛЬНИХ КОДІВ БЧХ

Abstract

Ivan Dychka, prof., DSc; Oleksandr Kuchmii, student; Lyubov Drozdenko, assistant
Determination of generation polynomials of binary correction BCH codes

The article deals with the construction of binary BCH codes based on generating polynomials. To determine the generating polynomial of the corresponding BCH code, a Galois field is used, each of whose elements corresponds to a minimal polynomial. To find minimal polynomials, a sequence of integers is divided into (2, n)-cycles. The generating polynomial is defined as the least common multiple of the minimal polynomials of the first 2t elements of the Galois field, where t is the desired correction capability of the designed BCH code

Вступ

У технічних системах, пов’язаних з передачею або зберіганням інформації необхідно вживати заходів щодо забезпечення цілісності даних [1]. Під час передачі (зберігання) інформації можуть виникати спотворення окремих бітів в інформаційних словах. Тому, для гарантування правильності даних при їх передачі або зберіганні застосовують завадостійке кодування інформації [2].

Відома низка завадостійких коректувальних кодів, одним з яких є код БЧХ (код Р. Боуза, Д. Чоудхурі, А. Хоквінгема).

Постановка задачі

Коректувальний код БЧХ може використовуватись для виправлення багатократних помилок у словах даних. Для його ефективного застосування необхідно розробити методику побудови кодів БЧХ з регульованою коректувальною здатністю – залежно від ймовірності появи тієї чи іншої кількості помилок в словах даних.

Визначення мінімальних многочленів елементів поля *GF(2⁴)*

З теорії завадостійкого кодування відомо, що твірний многочлен *g(x)* коректувального коду БЧХ з коректувальною здатністю t визначають як найменше спільне кратне (НСК) мінімальних многочленів $M_1(x), M_2(x), \dots, M_{2t}(x)$, що відповідають елементам α, α^2, $\alpha^3, \dots$, α^{2t} скінченного поля *GF(2^m)*, де $2t < 2^m - 1$.

Отже, для визначення твірного многочлена необхідно спочатку побудувати поле *GF(2^m)*.

Як приклад, розглянемо побудову поля *GF(2⁴)*.

Візьмемо незвідний многочлен четвертого степеня, наприклад,

$$x^4 + x + 1.$$

Нехай α-примітивний елемент поля *GF(2⁴)*. Примітивним є елемент, довільні степені якого дають усі без винятку ненульові елементи поля. Тоді, елементами поля *GF(2⁴)* є:

$$0, \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^7,\ \alpha^8,\ \alpha^9,\ \alpha^{10},\ \alpha^{11},\ \alpha^{12},\ \alpha^{13},\ \alpha^{14}.$$

У полі *GF(2⁴)* виконуються співвідношення:

$$\alpha^i = \alpha^{i-15},\ \alpha^{-i} = \alpha^{15-i},\ \alpha^{15} = \alpha^{-15} = \alpha^0 = 1.$$

Будь-який ненульовий елемент поля α^i, *i=0,1,2,…,14* має п’ять подань: степеневе (з невід’ємним та від’ємним показником степеня примітивного елемента), поліноміальне подання, двійкове та десяткове (табл. 1). Кожному елементу $\alpha^1,\ \alpha^2, \dots,\ \alpha^{14}$ поля відповідає мінімальний многочлен.

Таблиця 1

Подання елементів поля *GF(2⁴)* за модулем незвідного многочлена $x^4 + x + 1$ та мінімальні многочлени елементів

Степеневе подання		Поліноміальне подання (у вигляді многочлена від α)	Двійкове подання	Десяткове подання	Мінімальний многочлен $M_i(x)$, $i=0,1,2,\dots,14$
З невід’ємним показником степеня примітивного елемента α поля	З від’ємним показником степеня примітивного елемента α поля				
0	0	0	0 0 0 0	0	–
α^0	α^{-15}	1	0 0 0 1	1	–
α^1	α^{-14}	α	0 0 1 0	2	$M_1(x) = x^4 + x + 1$
α^2	α^{-13}	α^2	0 1 0 0	4	$M_2(x) = x^4 + x + 1$
α^3	α^{-12}	α^3	1 0 0 0	8	$M_3(x) = x^4 + x^3 + x^2 + x + 1$
α^4	α^{-11}	$\alpha + 1$	0 0 1 1	3	$M_4(x) = x^4 + x + 1$
α^5	α^{-10}	$\alpha^2 + \alpha$	0 1 1 0	6	$M_5(x) = x^2 + x + 1$
α^6	α^{-9}	$\alpha^3 + \alpha^2$	1 1 0 0	12	$M_6(x) = x^4 + x^3 + x^2 + x + 1$
α^7	α^{-8}	$\alpha^3 + \alpha + 1$	1 0 1 1	11	$M_7(x) = x^4 + x^3 + 1$
α^8	α^{-7}	$\alpha^2 + 1$	0 1 0 1	5	$M_8(x) = x^4 + x + 1$
α^9	α^{-6}	$\alpha^3 + \alpha$	1 0 1 0	10	$M_9(x) = x^4 + x^3 + x^2 + x + 1$

α^{10}	α^{-5}	$\alpha^2+\alpha+1$	0	1	1	1	7	$M_{10}(x)=x^2+x+1$
α^{11}	α^{-4}	$\alpha^3+\alpha^2+\alpha$	1	1	1	0	14	$M_{11}(x)=x^4+x^3+1$
α^{12}	α^{-3}	$\alpha^3+\alpha^2+\alpha+1$	1	1	1	1	15	$M_{12}(x)=x^4+x^3+x^2+x+1$
α^{13}	α^{-2}	$\alpha^3+\alpha^2+1$	1	1	0	1	13	$M_{13}(x)=x^4+x^3+1$
α^{14}	α^{-1}	α^3+1	1	0	0	1	9	$M_{14}(x)=x^4+x^3+1$

Мінімальні многочлени елементів поля *GF(2⁴)* визначають на основі *(2,15)*-циклів. Якщо числа: $i, i\cdot 2, i\cdot 2^2, i\cdot 2^3, \dots, i\cdot 2^{14}$, де *i=0,1,2,…,14,* замінити на їх остачі від ділення на 15, то отриману в такий спосіб сукупність чисел називають *(2,15)*-циклом, який містить число *i.*

Сукупність цілих чисел *1,2,…,14* можна розбити на чотири (2,15)-цикли як показано на рис. 1.

Циклу, який містить число 1, ставимо у відповідність обраний нами незвідний многочлен x^4+x+1, на основі якого побудовано поле GF(24) (табл. 1). Тобто $M_1(x)=x^4+x+1$.

Але мінімальні многочлени, що відповідають числам, які належать до одного циклу, збігаються. Тому $M_1(x)=M_2(x)=M_4(x)=M_8(x)=x^4+x+1$.

Для знаходження $M_3(x)$, а, отже, й $M_6(x)$, $M_9(x)$ та $M_{12}(x)$, необхідно взяти цикл, що містить число 3, та обчислити:

$$M_3(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})=x^4+x^3+x^2+x+1.$$

За аналогією знаходять мінімальні многочлени $M_5(x)$ (а, отже й $M_{10}(x)$) та $M_7(x)$(а, отже й $M_{11}(x)$, $M_{13}(x)$ та $M_{14}(x)$).

1, 2, 4, 8	$M_1(x)=M_2(x)=M_4(x)=M_8(x)$ $M_1(x)=x^4+x+1$
3, 6, 9, 12	$M_3(x)=M_6(x)=M_9(x)=M_{12}(x)$ $M_3(x)=x^4+x^3+x^2+x+1$
5, 10	$M_5(x)=M_{10}(x)$ $M_5(x)=x^4+x^3+x^2+x+1$
7, 11, 13, 14	$M_7(x)=M_{11}(x)=M_{13}(x)=M_{14}(x)$ $M_{14}(x)=x^4+x^3+1$

Рис. 1. Розбиття послідовності цілих чисел *1,2,…,14* на чотири (2,15)-цикли та відповідні їм мінімальні многочлени

Формування твірних многочленів *(15,k)*-кодів БЧХ

Визначимо твірні многочлени можливих кодів БЧХ з довжиною кодових слів *n*=15, задаючи різні *t* – коректувальну здатність коду.

При t=1 твірний многочлен визначимо так: $g(x) =$ НСК $(M_1(x), M_2(x))$. Оскільки $M_1(x) = M_2(x)$, то $g(x) = M_1(x) = x^4 + x + 1$. Такий твірний многочлен четвертого степеня відповідає *(n,k)=(15,11)*-коду БЧХ, кодові слова якого мають структуру: *n=15* – довжина кодових слів, *k=11* – кількість інформаційних розрядів у кодових словах, *r=4* – кількість контрольних розрядів (степінь твірного многочлена).

При *t*=2 твірний многочлен визначимо так:

$$g(x) = \text{НСК}\ (M_1(x), M_2(x), M_3(x), M_4(x))$$

Оскільки $M_1(x) = M_2(x) = M_4(x)$, то $g(x) = M_1(x) \cdot M_3(x) =$

$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1.$

За аналогією визначимо твірні многочлени кодів БЧХ з довжиною кодових слів *n=15* при *t*=3 та *t*=4 (табл. 2).

Виконані дослідження показали, що для випадків *t*=4,5,6,7 твірні многочлени є однаковими: $g(x) = M_1(x) \cdot M_3(x) \cdot M_5(x) \cdot M_7(x)$.

Таблиця 2

Двійкові коди БЧХ з довжиною кодових слів *n=15*

Коректувальна здатність коду БЧХ, *t*	Степінь твірного многочлена	*(n,k)*-код БЧХ	Твірний многочлен
1	4	*(15,11)*-код	$g(x) = M_1(x) = x^4 + x + 1$
2	8	*(15,7)*-код	$g(x) = M_1(x) \cdot M_3(x) = = x^8 + x^7 + x^6 + x^4 + 1$
3	10	*(15,5)*-код	$g(x) = M_1(x) \cdot M_3(x) \cdot M_5(x) = = x^{10} + x^8 + x^5 + x^4 + x^2 + x + +1$
4-7	14	*(15,1)*-код	$g(x) = = M_1(x) \cdot M_3(x) \cdot M_5(x) \cdot M_7(x) = = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + +x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + +x^3 + x^2 + x + 1$

Отже, двійкові *(n_i-k)*-коди БЧХ будують за заданими параметрами *n*-довжини кодових слів та *t* – коректувальна здатність коду. Значення *k* невідоме, поки не визначено степінь *r* твірного многочлена $g(x)$; після цього визначають *k=n-r*.

Твірний многочлен $g(x)$, визначений як

$$g(x) = \text{НСК}\ (M_1(x), M_2(x), \dots, M_{26}(x))$$

задає двійковий *(n,k)*- код БЧХ з коректувальною здатністю *t*.

Кодування даних кодом БЧХ

Нехай $A = (a_{k-1}a_{k-2} \dots a_1\, a_0)$ – *k*-розрядне інформаційне слово, яке необхідно закодувати *(n,k)*- кодом БЧХ.

Кодовим словом $C = (c_{n-1}c_{n-2} \dots c_1 c_0)$ коду БЧХ є коефіцієнти многочлена $c(x) = \sum_{i=0}^{n-1} c_i x^i$ степеня *n-1*, отриманого як $c(x) = a(x)g(x)$, де $a(x) = \sum_{i=0}^{k-1} a_i x^i$ - многочлен степеня *k-1*, що відповідає інформаційному слову *A*, а $g(x) = \sum_{i=0}^{r} g_i x^i$ – твірний многочлен *(n,k)*- коду БЧХ.

Нехай інформаційне слово $A = (a_6a_5a_4a_3a_2a_1\, a_0) = (1010011)$ необхідно закодувати кодом БЧХ так, щоб у кодовому слові забезпечувалось виправлення двократних помилок. Інформаційному слову $A = (1010011)$ відповідає многочлен $a(x) = x^6 + x^4 + x + 1$. Оскільки слово *A* – семирозрядне, тобто *k*=7 (кількість інформаційних розрядів), то з табл.2 визначаємо, що для забезпечення заданої коректувальної здатності *t*=2 (кількість помилок, що мають виправитися), слід обрати *(15,7)*-код БЧХ, якому відповідає твірний многочлен $g(x)$ восьмого степеня. Отже, *n*=15, *k*=7, *r*=8.

Кодове слово *C* (15,7)-коду БЧХ знайдемо так:

$$c(x) = a(x)g(x) = (x^6 + x^4 + x + 1)(x^8 + x^7 + x^6 + x^4 + 1) =$$
$$= x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x + 1;$$

	c_{14}	c_{13}	c_{12}	c_{11}	c_{10}	c_9	c_8	c_7	c_6	c_5	c_4	c_3	c_2	c_1	c_0
C = (	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1)

Кодове слово *C* подане в несистематичній формі, тобто неможливо вказати, які розряди слова є інформаційними, а які – контрольними.

Висновки

Запропонована методика визначення твірних многочленів двійкових кодів БЧХ дозволяє на основі двох заданих параметрів: *n* – бажана довжина кодових слів, *t* – бажана коректувальна здатність коду,– визначити *(n,k)*-код БЧХ, де *k* – кількість інформаційних розрядів, *k=n-r* (*r* – степінь твірного многочлена), у кодових словах якого забезпечуватиметься виправлення *t* – помилок.

Твірний многочлен формують на основі мінімальних многочленів елементів поля $GF(2^m)$, для якого $m =]\log_2 n[$.

Подальші дослідження слід зосередити на розробленні ефективних алгоритмів декодування *(n,k)*- кодів БЧХ.

Література

1. Жураковський Б. Ю. Порівняльний аналіз формування та застосування двомірних штрихкодів для передачі даних. Системи управління, навігації та зв'язку, 2015. № 2 (34), С.68–70.
2. ISO/IEC 18004:2015 Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification. https://www.iso.org/standard/62021.html