Теорія інформації та кодування

Лекція 7. Коди Боуза–Чоудхурі–Хоквінгема (БЧХ коди)

БЧХ коди є різновидом циклічних кодів з кодовою відстанню $d_{\min} \geq 3$.

Вони дають змогу виявляти та виправляти будь-яку кількість помилок.

Визначальними параметрами для побудови кодів Боуза–Чоудхурі–Хоквінгема (БЧХ) є:

кількість помилок, яку треба виправити;

мінімальна кодова відстань та загальна кількість елементів n у кодовій комбінації.

Кількість інформаційних k і перевірних r елементів визначають у ході побудови коду (БЧХ).

Правила побудови БЧХ кодів:

1. Довжину кодових комбінацій кодів БЧХ n визначають так:

$$n = 2^h - 1; n = (2^h - 1) / g,$$

де h – ціле додатне число, а g – додатне непарне число, при діленні на яке, n стає цілим непарним числом.

Легко бачити, що довжина кодових комбінацій n може бути тільки непарною.

Розкладемо $2^h - 1$ на множники:

$$7 = 2^3 - 1; 15 = 2^4 - 1 = 5 \cdot 3; 31 = 2^4 - 1; 63 = 2^6 - 1 = 7 \cdot 3 \cdot 3; 127 = 2^7 - 1;$$

$$255 = 2^8 - 1 = 17 \cdot 5 \cdot 3; 511 = 2^9 - 1 = 73 \cdot 7; 1023 = 2^{10} - 1 = 31 \cdot 11 \cdot 3; 2047 = 2^{11} - 1 = 89 \cdot 23;$$

$$4095 = 2^{12} - 1 = 13 \cdot 7 \cdot 5 \cdot 3 \cdot 3\ldots$$

2. Кількість перевірних елементів коду визначають з виразу

$$r \leq \frac{h(d_{\min}-1)}{2} = \left[\log_2(n+1)\right]\frac{d_{\min}-1}{2}$$

Кількість інформаційних елементів – з виразу

$$k \geq \left(2^h - 1\right) - \frac{h(d_{\min}-1)}{2}$$

Означення. Примітивним кодом БЧХ, який виправляє помилки кратності l_2, називають код довжиною $n = 2^h - 1$ над полем $GF(2)$ для якого елементи α, α^2, α^3, …, α^{2l_2} є коренями твірного полінома. Тут α – примітивний елемент поля $GF(2^h)$.

Отже, твірний поліном коду БЧХ є добутком мінімальних поліномів $M_i(x)$, i=1, 3, 5,… $2l_2 - 1$

$$g(x) = M_1(x)\, M_3(x)\, M_5(x) \cdot \ldots \cdot M_{2l_2-1}(x)$$

За заданою довжиною коду n та кратністю помилок, які потрібно виправити, визначають:

– з виразу $s = 2l_2 - 1$ – максимальний номер мінімального полінома, який входить до співмножників у виразі для твірного полінома $g(x)$. Отже, кількість L мінімальних поліномів визначена кратністю помилок l_2, які виправляють кодом $L = l_2$;

– з виразу $n = 2^v - 1$ або $ng = 2^v - 1$ значення параметра v, який буде максимальним степенем мінімального полінома у виразі для твірного полінома $g(x)$. Звідси випливає, що $v = h$;

– користуючись таблицею мінімальних поліномів, визначають твірний поліном залежно від параметрів v та s. Для цього зі стовпця, який відповідає параметру v вибирають поліноми з номерами від 1 до s, які унаслідок множення дають твірний поліном $g(x)$. Степінь q твірного полінома не перевищує добутку vl_2.

Номер мінімального полінома	Мінімальні поліноми степеня ν							
	2	3	4	5	6	7	8	9
$M_1(x)$	7	64	62	51	604	442	561	4204
$M_3(x)$		54	76	57	724	742	735	4644
$M_5(x)$			7	73	714	562	637	4314
$M_7(x)$			46	75	444	736	455	4624
$M_9(x)$				67	54	772	573	6214
$M_{11}(x)$					554	526	717	5504
$M_{13}(x)$						602	651	7344
$M_{15}(x)$							727	4154

Приклад. Визначимо твірний поліном для побудови примітивного коду БЧХ над $GF(2)$ завдовжки n = 15, що виправляє помилки кратності l_2 = 2.

Визначаємо значення параметрів v та s

$$\nu = \log_2(n+1) = \log_2 2^4 = 4\,;$$

$$s = 2 \cdot l_2 - 1 = 2 \cdot 2 - 1 = 3\,.$$

Твірний поліном визначаємо:

$$g^8(x) = M_1^4(x) M_3^4(x)$$

або

$$g^8(x) = 62 \cdot 76 = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) =$$

$$= 1 + x^4 + x^6 + x^7 + x^8 \;\rightarrow\; 100010111.$$

У разі потреби твірну матрицю коду БЧХ можна побудувати за правилами побудови такої матриці для циклічного коду:

$$G_{БЧХ(7,15)}=\begin{pmatrix} 1&0&0&0&1&0&1&1&&1&0&0&0&0&0&0\\ 1&1&0&0&1&1&1&0&&0&1&0&0&0&0&0\\ 0&1&1&0&0&1&1&1&&0&0&1&0&0&0&0\\ 1&0&1&1&1&0&0&0&&0&0&0&1&0&0&0\\ 0&1&0&1&1&1&0&0&&0&0&0&0&1&0&0\\ 0&0&1&0&1&1&1&0&&0&0&0&0&0&1&0\\ 0&0&0&1&0&1&1&1&&0&0&0&0&0&0&1 \end{pmatrix}$$

Оскільки степінь твірного полінома дорівнює 8, то ми отримали (7, 15)-код, що виправляє помилки кратності $l_2 = 2$.

У разі потреби твірну матрицю коду БЧХ можна побудувати за правилами побудови такої матриці для циклічного коду:

$$G_{БЧХ(7,15)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Оскільки степінь твірного полінома дорівнює 8, то ми отримали (7, 15)-код, що виправляє помилки кратності $l_2 = 2$.

n	k	r	$d_{\min}$	Твірний поліном $g^r(x)$
7	4	3	3	64
15	11	4	3	62
	7	8	5	427
	5	10	7	7312
31	26	5	3	51
	21	10	5	4556
	16	15	7	753704
	11	20	9	5266215
	6	25	11	710536646
63	57	6	3	604
	51	12	5	47124
	45	18	7	7464074
	39	24	9	735623334
	36	27	11	6210056604
	30	33	13	7153534131754
	24	39	15	41110103262674
	18	45	17	5274562453206364
127	120	7	3	442
	113	14	5	73541
	106	21	7	61715544
	99	28	9	4726207116
	92	35	11	726220067123
	85	42	13	672226371107064
	78	49	15	54406433420006232
	71	56	17	6577246526470405523
	64	63	19	5100046770755201653024
255	247	8	3	561
	239	16	5	615732
	231	24	7	533027354
	223	32	9	57641332357
	215	40	11	42132713575462
	207	48	13	72236373503537434
	199	56	15	4162270210724606637
	191	64	17	7351476665443740716332
	187	68	19	4563622264000156465572 5

Закономірності для кодів БЧХ:

– співвідношення між мінімальною кодовою відстанню та числом h можна записати як

$$d_{\min} = 2^{h-1} - 1$$

і кількість інформаційних розрядів, яку можна використати за цих значень дорівнює $h + 1$;

– кількість кодів, що відрізняються коригувальною здатністю і мають однакову довжину кодової комбінації на дві одиниці менша від кількості всіх незвідних поліномів, на які розкладається двочлен $x^{2^h - 1} + 1$

Приклад. Знайдемо параметри коду, який виправляє помилки кратності $l_2 = 2$, якщо довжина інформаційної частини коду $k = 40$.

Оскільки $k = 40$, то найближча (але більша) довжина коду дорівнює 63, звідки отримуємо, $h = 6$.

Тому матимемо:

$$r = hl_2 = 12,\ k = 63 - r = 51.$$

Означення. Непримітивним кодом БЧХ, який виправляє помилки кратності l_2, називають код довжиною n над полем $GF(2)$ для якого елементи

$$(\beta^i)^1, (\beta^i)^2, (\beta^i)^3, \ldots, (\beta^i)^{2 \cdot l_2}$$

є коренями твірного полінома. Тут β^i – непримітивний елемент поля $GF(2)$, а довжина коду дорівнює порядку елемента β^i.

Нагадування. Порядком елемента β називають найменше n для якого $\beta^n = 1$.

Твірний поліном непримітивного коду БЧХ, за аналогією з примітивним кодом, визначають виразом

$$g(x) = M_{1\cdot i}(x) M_{3\cdot i}(x) M_{5\cdot i}(x) \ldots M_{(2l_2 - 1)\cdot i}(x)$$

де $M_{ji}(x)$ – мінімальні поліноми елементів

$$(\beta^i)^1, (\beta^i)^3, \ldots, (\beta^i)^j$$

поля $GF(2^h)$, які є коренями $g(x)$, i – степінь непримітивного елемента β.

h	Непримітивні елементи поля		
	$GF(2^h)$	β^i	Порядок елемента (n)
4	$GF(2^4)$	β^3	5
		β^5	3
6	$GF(2^6)$	β^3	21
		β^7	9
		β^9	7
8	$GF(2^8)$	β^3	85
		β^5	51
		β^{15}	17
		β^{17}	15
9	$GF(2^9)$	β^7	73
10	$GF(2^{10})$	β^3	341
		β^{11}	93
		β^{31}	33
		β^{33}	31

Приклад. Побудуємо твірний поліном непримітивного коду БЧХ над полем $GF(2)$ довжини $n = 40$, який виправляє помилки кратності $l_2 = 3$.

З попередньої таблиці вибираємо поле, непримітивний елемент β якого має порядок більший (найближчий) ніж задана довжина $n = 40$. Таким полем є поле $GF(2^8)$ та елемент β^5, порядок якого дорівнює 51.

Маємо:

$$h = 8,\ s = 2l_2 - 1 = 5,\ i = 5$$

Тому

$$g(x) = M_5^8(x) M_{15}^8(x) M_{25}^8(x) = 637 \cdot 727 \cdot 661 = 110011111 \cdot 111010111 \cdot 110110001 =$$
$$(1 + x + x^4 + x^5 + x^6 + x^7 + x^8)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x + x^3 + x^4 + x^8) =$$
$$\ldots$$

Приклад. Побудуємо твірний поліном непримітивного коду БЧХ над полем $GF(2)$ довжини $k = 40$, який виправляє помилки кратності $l_2 = 4$.

З попередньої таблиці вибираємо поле, непримітивний елемент β якого має порядок більший (найближчий) ніж задана довжина інформаційної послідовності $k = 40$. Таким полем є поле $GF(2^8)$ та елемент β^5, порядок якого дорівнює 51.

Маємо:

$$h = 8,\ s = 2l_2 - 1 = 7,\ i = 5$$

Проте, у цьому випадку кількість перевірних елементів дорівнює

$$r = 32$$

Звідки отримуємо $n = r + k = 32 + 40 = 72 > 51$.

Отже, не підходить.

На наступному кроці, з попередньої таблиці вибираємо поле, непримітивний елемент β якого має порядок більший (найближчий) ніж 51. Таким полем є поле $GF(2^9)$ та елемент β^7, порядок якого дорівнює 73.

Маємо:

$$h = 9,\ s = 2l_2 - 1 = 7,\ i = 7$$

Проте, у цьому випадку кількість перевірних елементів дорівнює

$$r = 36$$

Звідки отримуємо $n = r + k = 36 + 40 = 76 > 73$.

Отже, не підходить.

На наступному кроці, з попередньої таблиці вибираємо поле, непримітивний елемент β якого має порядок більший (найближчий) ніж 73. Таким полем є поле $GF(2^8)$ та елемент β^3, порядок якого дорівнює 85.

Маємо:

$$h = 8,\ s = 2l_2 - 1 = 7,\ i = 3$$

У цьому випадку кількість перевірних елементів дорівнює

$$r = 32$$

Звідки отримуємо $n = r + k = 32 + 40 = 72 < 85$. Отже,

$$g(x) = M_3^8(x)M_9^8(x)M_{15}^8(x)M_{21}^8(x) = 735 \cdot 573 \cdot 727 \cdot 643 =$$
$$= 111011101 \cdot 101111011 \cdot 111010111 \cdot 110010011 =$$
$$= (1 + x + x^2 + x^4 + x^5 + x^6 + x^8)(1 + x^2 + x^3 + x^4 + x^5 + x^7 + x^8) \cdot$$
$$\cdot (1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x + x^4 + x^7 + x^8) = \ldots$$