БЧХ

Постановка задачи

- Корректирующий циклический (n, k) код

$$\mathbf{c} = (c_{n-1}, c_{n-2}, \ldots, c_0) \in (F_2)^n$$

- представляется в полиномиальном виде как

$$C(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_0 \in F_2[x]$$

- где $F_2[x]$ - кольцо многочленов над полем F_2 .

Корневой подход

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

$$y(x) = c(x) + e(x)$$

$$e(x) = e_0 + e_1 \cdot x + e_2 \cdot x^2 + \ldots + e_{n-1} \cdot x^{n-1}$$

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,

$$s_j = \sum_{i=0}^{n-1} e_i \cdot \beta_j^i$$

- где $s_i - j$-я компонента синдрома ошибок **s**

Пример

- Обозначим примитивный элемент конечного поля GF(2^m) как α.
- Определим проверочную матрицу **H** кода C , столбцы которой равны α^{n-1}, α^{n-2}, …, $\alpha\ \alpha^0$, где $n = 2^m - 1$.
- Произведению **(cH^T)** соответствует полином

$$C(\alpha) = c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + \ldots + c_2\alpha^2 + c_1\alpha + c_0$$

- Если $c(\alpha) = 0$, то получим циклический код Хэмминга

Пример

$$H' = \begin{array}{c} \begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Корневой подход

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

$$(\beta_1,\ldots,\beta_{2t}) = (\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{2t})$$

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

Алгоритм формирования кода

- 1. Строится поле
  - $\mathrm{GF}(p^m)$,
- для которого α - примитивный элемент поля.
- 2. Определяются минимальные полиномы

$$m_i(x) = m_{\alpha^i}(x) \qquad \alpha^i, \quad i = 1,\ldots,2t$$

- 3. Порождающий полином $g(x)$ вычисляется как

$$g(x) = НОК\left(m_1(x), m_2(x), \ldots, m_{2t}(x)\right)$$

Теорема

- Пусть циклический код **C** длины n задан порождающим полиномом $g(x)$ над полем $GF(p)$ и пусть имеется наименьшее целое m такое, что $n|p^m - 1$, а $\alpha \in GF(p^m)$ – примитивный корень из единицы n-й степени.

- Тогда, если элементы поля $GF(p^m)$ определяют нули кода для целых $b \geq 0$ и $\delta \geq 2$, то код имеет $d_{\min} \geq \delta$.

Определение БЧХ

- Зададим циклический код **C** длины n над полем $GF(p)$, определив наименьшее целое m такое, что $n \mid p^m - 1$ и $\alpha \in GF(p^m)$ – примитивный корень из единицы n-й степени.

- Тогда можно определить БЧХ код **C** с заданным значением кодового расстояния δ и порождающим полиномом

$$g(x) = \text{НОК}\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\}$$

- где $m_b(x)$ минимальный многочлен элемента
- $\alpha^b \in GF(p^m)$, b – целое положительное число.

БЧХ

- Если $b = 1$ то говорят, что код БЧХ определен в *узком* смысле.
- Если же $n = p^m - 1$ (α – примитивный элемент $GF(p^m)$), то БЧХ код называют *примитивным*.

- *Теорема.* БЧХ код длины n с заданным значением кодового расстояния δ, построенный над полем $GF(p)$, имеет $d_{\min} \geq \delta$ и размерность $k \geq n - m(\delta - 1)$
- Для $p = 2$, $b = 1$ и $\delta = 2t + 1$, $k \geq n - mt$.

Соотношение между параметрами кода

- Для $p = 2$, $b = 1$, $n = 2^m - 1$ и $\delta = 2t + 1$ код БЧХ
- имеет $d_{\min} = 2t + 1$, если
- .

$$\sum_{i=0}^{t+1} C_n^i > 2^{mt}$$

- Если $b = 1$, $n = \delta v$, тогда $d_{\min} = \delta$.
- Если $b = 1$, $n = p^m - 1$ и $\delta = p^v - 1$, тогда $d_{\min} = \delta$.
- Если $n = p^m - 1$, тогда $d_{\min} \le p\delta - 1$.

Проверочная матрица БЧХ

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha^{b} & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}$$

Матрица Вандермонда $= \begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{bmatrix}$

a_j – элементы поля. Определитель $\neq 0$, если a_j – различны.

$$\det = \prod_{j=1}^{n-1} \prod_{i=j+1}^{n} (a_i - a_j)$$

Galois Field

- *$GF(2^3)$ с неприводимым полиномом: $x^3 + x + 1$*
- *$\alpha = x$ примитивный элемент*

α	x	010	**2**
α^2	x^2	100	**3**
α^3	$x + 1$	011	**4**
α^4	$x^2 + x$	110	**5**
α^5	$x^2 + x + 1$	111	**6**
α^6	$x^2 + 1$	101	**7**
α^7	1	001	**1**

GF Discrete Fourier Transform (DFT)
GF-DFT

- *Интерполяция полинома в n точках через умножение на матрицу:*
- *α – примитивный n-й корень из единицы ($\alpha^n = 1$) – генератор*

$$T = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{pmatrix}$$

$$\begin{pmatrix} c_0 \\ \cdots \\ c_{k-1} \\ c_k \\ \cdots \\ c_{n-1} \end{pmatrix} = T \cdot \begin{pmatrix} m_0 \\ \cdots \\ m_{k-1} \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

Оценка полинома $m_{k-1}x^{k-1} + \cdots + m_1 x + m_0$ в n различных корнях из 1, 1, α, α^2, α^3, …, α^{n-1}

Обратное ДПФ $m = T^{-1} \cdot c$

Вычисление минимальных полиномов через циклотомические классы

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где s_j – j-я компонента синдрома ошибок **s**

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8$$

$$(\alpha^8)^2 = \alpha$$

Сопряженные элементы

- Так для поля *GF*(16)=*GF*(2^*m*) минимальным многочленом элементов

$$\alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^4)^2 = \alpha^8$$

$$(\alpha^8)^2 = \alpha$$

- является один и тот же многочлен

Сопряженные элементы

- Пусть необходимо исправить t ошибок. $\alpha^{3}, \alpha^{6}, \alpha^{12}, \alpha^{24} = \alpha^{9}$
- Принимаемый сигнал можно записать как

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

Циклотомические классы

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

Циклотомические классы

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

Циклотомический класс

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

$$K_s = \{s, ps, p^2 s, p^3 s, \ldots, p^{t_s - 1} s\} = \{k_{s,0}, k_{s,1}, \ldots, k_{s,t_s}\}$$

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

$$p^{t_s} s \equiv s \bmod (p^m - 1)$$

Пример

- Пусть необходимо исправить t ошибок.
- Принимаемый сигнал можно записать как

- где $e(x)$- полином ошибки
- Если примем, что β_j - корни генераторного полинома $g(x)$, тогда
- $y(\beta_j) = e(\beta_j) = s_j$,
- где $s_j - j$-я компонента синдрома ошибок **s**

Минимальные полиномы

- Циклотомические классы позволяют вычислить минимальные полиномы с помощью выражения

$$m_s(x) = \prod_{i \in K_s} (x - \alpha^i)$$

Пример : исправление 1 ошибки

Построим порождающий полином $g(z)$ БЧХ-кода длины $n = 2^3 - 1 = 7$, исправляющего любую однократную ошибку.

1. Для этого необходимо расширенное поле $GF(2^3)$.

2. Поскольку $\delta = 2t + 1 = 3 = d_{min}$, корнями порождающего полинома должны быть элементы α и α^2 т. к.

$$g(x) = \text{НОК}(m_1(x), m_2(x)), .$$

$GF(2^3)$

$$f(x) = x^3 + x + 1 \qquad f(\alpha) = 0$$

Мл.разряд

Вектор	Полином	Степень α
000 =	0	= 0
001 =	1	= 1
010 =	α	= α
100 =	α^2	= α^2
011 =	$1 + \alpha$	= α^3
110 =	$\alpha + \alpha^2$	= α^4
111 =	$1 + \alpha + \alpha^2$	= α^5
101 =	$1 + \alpha^2$	= α^6
$\alpha^7 = 1$		

Пример: исправление 1 ошибки

3. Минимальный полином элемента α имеет вид

$m_1(x) = (x + \alpha)\,(x + \alpha^2)\,(x + \alpha^4) =$

$= x^3 + (\alpha + \alpha^2 + \alpha^4)\,x^2 + (\alpha\,\alpha^2 + \alpha\,\alpha^4 + \alpha^2\,\alpha^4)\,x + \alpha\,\alpha^2\,\alpha^4.$

Но $\alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \alpha + \alpha^2 = 0,$

$\alpha\,\alpha^2 + \alpha\,\alpha^4 + \alpha^2\,\alpha^4 = \alpha^3 + \alpha^5 + \alpha^6 = \alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + 1 = 1,$ $\alpha\,\alpha^2\,\alpha^4 = \alpha^7 = 1,$

так что

$$m_1(x) = x^3 + x + 1.$$

5. Элемент α^2 сопряжен с α и уже учтен в $m_1(x)$, поэтому

$g(x) = m_1(x) = x^3 + x + 1.$

6. Поскольку $\deg\{g(x)\} = 3$, число информационных символов кода $k = 4$, и, таким образом, построенный код оказался циклической версией (7,4) кода Хэмминга.

Пример: исправление 2 ошибок

Изменим условия примера, потребовав исправления до двух ошибок

$$(t = 2 \Rightarrow s = 2t = 4),$$

множество обязательных корней полинома $g(x)$ пришлось бы расширить до $\alpha, \alpha^2, \alpha^3, \alpha^4$.

Элементы α, α^2 and α^4 входят в один и тот же сопряженный цикл, т.е. уже охвачены минимальным полиномом $g_1(x) = x^3 + x + 1$.

Остается найти лишь минимальный полином для α^3 (корнями которого будут и сопряженные с ним элементы α^6 и $\alpha^{12} = \alpha^5$).

$K_{s=3} = \{s = 3, 2s = 6, 2^2 s = 12 \equiv 5 \bmod 7\} \rightarrow m_3(x) = x^3 + x^2 + 1$

Пример: исправление 2 ошибок

- Степень последнего равна трем, так что степень $g(x)$ окажется равной шести, и полученный код есть тривиальный (7,1) код с повторением, передающий лишь один бит информации.

- $g(x) = (x^3 + x + 1)\,(x^3 + x^2 + 1) =$
- $= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Построение БЧХ кода, корректирующего три ошибки

- Определим конечное поле $GF(2^4)$, для которого существует четыре циклотомических класса
- $K_1 = \{1, 2, 4, 8\}$; $K_3 = \{3, 6, 12, 9\}$; $K_5 = \{5, 10\}$;
- $K_7 = \{7, 14, 13, 11\}$.

- Возьмем элемент поля α^3 , которому соответствует минимальный неприводимый в $Z_2[x]$ полином .

$$m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$GF(2^4)$

Мл. разряд

vector	polynomial	power of α	logarithm
0000	0	?	$-\infty$
0001	1	$\alpha^0=1$	0
0010	x	α	1
0100	x^2	α^2	2
1000	x^3	α^3	3
0011	x+1	α^4	4
0110	x^2+x	α^5	5
1100	x^3+x^2	α^6	6
1011	x^3+x+1	α^7	7
0101	x^2+1	α^8	8
1010	x^3+x	α^9	9
0111	x^2+x+1	α^{10}	10
1110	x^3+x^2+x	α^{11}	11
1111	x^3+x^2+x+1	α^{12}	12
1101	x^3+x^2+1	α^{13}	13
1001	x^3+1	α^{14}	14

$x^4=x+1 \bmod f(x)$

$\alpha^5=\alpha^4\alpha=(\alpha+1)\alpha=\alpha^2+\alpha$

$\alpha^{15}=1$: $x(x^3+1)=x^4+x=(x+1)+x=1$

Построение БЧХ кода, корректирующего три ошибки

- Элемент α^3 является корнем полинома $(x^5 - 1)$. Элементы α и α^3 являются корнями полинома

$$m_{13}(x) = m_1(x)m_3(x) = (x^4 + x + 1)m_3(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

- Степень примитивного элемента поля $(\alpha^5)^3 = \alpha^{15} = 1$
- и, следовательно, α^5 - является корнем многочлена
- $x^3 - 1 = x^3 + 1 = (x + 1)(x^2 + x + 1)$

- кодовые слова должны быть кратны полиному
- $g(x) = m_{135}(x) = m_{13}(x)\, m_5(x) = m_{13}(x)\,(x^2 + x + 1) =$
- $= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$

Вопросы

- ?