Лекция №9
БЧХ -код

I Код БЧХ (BCH) Bose-Ray-Chaudri-Hocquenghem

Важно св-во: скорость $\left(\frac{k}{n}\right)$ лучше, чем у кода RS

В RS: большой алфавит ($n = |\mathbb{F}_q| - 1$).

В BCH: бинарный

Опр. 1 Для длины $n = 2^m - 1$ и min. расстояния d и примитивного эл-та $\alpha \in \mathbb{F}^*_{2^m}$, бинарный BCH код

$$BCH(n,d) = \{ (c_0 \dots c_{n-1}) \in \mathbb{F}_2^n \mid c = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} :$$
$$c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{d-1}) = 0 \}$$

В отличие от кода RS, коэфф-ты c_i лежат в $\mathbb{F}_2$.

Лемма 1 $BCH(n,d)$ - лин. над $\mathbb{F}_2$.

Δ Составим из опр-ия "проверочную" матрицу H:

$$\underset{\in \mathbb{F}^{n-k \times n}}{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{bmatrix}$$

$$H \cdot c = 0 \Leftrightarrow c \in BCH(n,d)$$

$$H \cdot c_1 + H c_2 = 0 \Leftrightarrow H(c_1 + c_2) = 0 \text{ над } \underline{\underline{\mathbb{F}_{2^m}}} \ (!)$$

H задаёт лин. отображение над $\mathbb{F}_{2^m}$. Докажем, что эта линейность сохраняется над $\mathbb{F}_2$.

Для этого ∃ отображение

$$Mul_\alpha : x \mapsto \alpha \cdot x$$

Mul_α — $\mathbb{F}_2$-линейно, т.е. $\alpha(x+y) = \alpha x + \alpha y$ $\quad (\alpha \cdot (\gamma \cdot x) = (\alpha \cdot \gamma) x)$

Т.к. $\mathbb{F}_{2^m}$ - векторное пр-во над $\mathbb{F}_2$ разм-ти m, то $\exists$ $\{\beta_1 \dots \beta_m\} \subset \mathbb{F}_{2^m}$, т.ч. $\forall x \in \mathbb{F}_{2^m} : x = \sum\limits_{i=0}^{m-1} x_i \beta_i$, $x_i \in \mathbb{F}_2$

Тогда $\mathbb{F}_2$-линейность Mul_α продолжается на X действием матрица $M_\alpha \in \mathbb{F}_2^{m \times m}$ на вектор-коэфф-в x_i:

$$\begin{bmatrix} | & | & & | \\ \alpha\beta_1 & \alpha\beta_2 & \dots & \alpha\beta_m \\ | & | & & | \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ \vdots \\ x_{m-1} \end{bmatrix} = x_0 \alpha\beta_1 + \dots x_{m-1}\alpha\beta_m = \alpha(\underbrace{x_0\beta_1 + \dots x_{m-1}\beta_m}_{X})$$

Тогда, условие $C(\alpha) = c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} = 0$ можно переписать

$$\begin{bmatrix} c_0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + M_\alpha \cdot \begin{bmatrix} c_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + M_\alpha^2 \begin{bmatrix} c_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + M_\alpha^{n-1} \begin{bmatrix} c_{n-1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$$

$BCH(n,d)$ – линейный $\Longleftrightarrow$ $c, c' \in BCH(n,d)$, то $c + c' \in BCH(n,d)$

$$\begin{bmatrix} c_0 + c_0' \\ 0 \\ \vdots \\ 0 \end{bmatrix} + M_\alpha \begin{bmatrix} c_1 + c_1' \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \dots + M_\alpha^{n-1} \begin{bmatrix} c_{n-1} + c_{n-1}' \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$$

$$\begin{bmatrix} c_0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad \begin{bmatrix} c_0' \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

II Параметры БЧХ

Лемма №2 Для $n = 2^m - 1$, min. расст-ия d, размерность БЧХ(n, d) удовлетворяет

$$k \geqslant n - \left\lceil \frac{d-1}{2} \right\rceil \cdot \lg(n+1)$$

(сравн., для RS: $k = n-d+1$)

◁ Покажем, что некоторые условия $c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{d-1}) = 0$ из опр-ия БЧХ кода избыточны.

А именно, покажем, что $\forall c \in \mathbb{F}_2[x]$, если $c(\gamma) = 0$, то $c(\gamma^2) = 0$ $(\forall \gamma \in \mathbb{F}_{2^m})$

$$c(\gamma) = 0 \iff (c(\gamma))^2 = 0 \iff$$

$(a+b)^2 = a^2 + b^2$ над $\mathbb{F}_2$

$$(c_0 + c_1\gamma + \ldots + c_{n-1}\gamma^{n-1})^2 = 0 \iff$$

$$c_0^2 + c_1^2\gamma^2 + \ldots c_{n-1}^2 \gamma^{2(n-1)} = 0 \iff$$

$c_i^2 = c_i$

$$c_0 + c_1\gamma^2 + \ldots + c_{n-1}\gamma^{2(n-1)} = 0 \iff$$

$$c(\gamma^2) = 0.$$

$\Rightarrow$ условия $c(\alpha^{2j}) = 0$ $j = 1 \ldots \left\lceil \frac{d-1}{2} \right\rceil$ избыточны $\Rightarrow$

$\Rightarrow$ мы их можем убрать из опр-ия, не меняя мн-во кодовых слов

$\Rightarrow$ получаем $\left\lceil \frac{d-1}{2} \right\rceil \cdot m$ условий над $\mathbb{F}_2$ для лин. векторов длины n

\# уравнений над $\mathbb{F}_{2^m}$

выполнения равенства 0 над $\mathbb{F}_2$ системы над $\mathbb{F}_{2^m}$

$$\Rightarrow \text{р-ть кода над } \mathbb{F}_2 \geqslant n - \left\lceil \frac{d-1}{2} \right\rceil \cdot m = n - \left\lceil \frac{d-1}{2} \right\rceil \cdot \lg(n+1)$$

▶

Следствие BCH-код – "подкод подполя" (subfield subcode) кода Рида-Соломона, а именно

$$BCH(n,d) = RS_{\mathbb{F}, \mathbb{F}^*}[n, n-d+1] \cap \mathbb{F}_2^n$$

$\Rightarrow$ алг-мы декодирования кода RS подходят для декодирования BCH.

III Построение BCH

1. Зафиксируем n
2. Факторизуем $x^n + 1 = \prod\limits_{g_i \in \mathbb{F}_2[x]} g_i(x)$

$\exists \alpha$ – корень x^n+1 (α – корень n-степени из 1)

Для того, чтобы построить $\mathbb{F}_{2^m}$ $(n = 2^m - 1)$, выбираем $g_i(x)$ – неприводим. над $\mathbb{F}_2$ степени m.

Пример $n = 15$ $x^{15} - 1 = \underbrace{(x+1)}_{g_0}\underbrace{(x^2+x+1)}_{g_1}\underbrace{(x^4+x+1)}_{g_2}\underbrace{(x^4+x^3+1)}_{g_3}\underbrace{(x^4+x^3+x^2+x+1)}_{g_4}$

Построим код с min. расстоянием $d=5$ (2 ошибки), $m=4$

$\exists \alpha$ - корень $x^{15}-1$ $(\alpha^{15}=1)$

мн-н g_i	корни
$g_1 = x^2+x+1$	$\{\alpha^5, \alpha^{10}\}$
$g_2 = x^4+x+1$	$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$
$g_3 = x^4+x^3+1$	$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$
$g_4 = x^4+x^3+x^2+x+1$	$\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$

$\Rightarrow$ объединяя корни g_2 и g_4, получим последовательность $\{\underline{\alpha, \alpha^2, \alpha^3, \alpha^4}, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}\}$

$$\Rightarrow \underline{g(x)} = g_2(x) \cdot g_4(x) = x^8 + x^7 + x^6 + x^4 + 1$$

$$BCH(15,5) = \{ m(x) \cdot \underline{g(x)} \mid \forall m \in \mathbb{F}_2[x],\ \deg m(x) \le 6 \}$$

Декодирования

$y = c + e$ – полученное слово, $wt(e) \le t$

$c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{d-1}) = 0 \Rightarrow$

$y(\alpha) = c(\alpha) + e(\alpha) = e(\alpha)$ (аналог. $y(\alpha^{d-1}) = e(\alpha^{d-1})$)

$T = \{i,\ e_i = 1\}$ – позиции ошибок

$E(x) = \prod_{j \in T} (1 - \alpha^j x)$, $E(x) \in \mathbb{F}_2[x]$, $\deg E(x) \le t$

$S(x)$ – синдром $\in \mathbb{F}_{2^m}[x]$, $S_e = y(\alpha^e)$ (или $S = H \cdot y$)

В лекции №7 мы показали, что для некоторого $\Gamma(x) \in \mathbb{F}_{2^m}[x]$, $\deg \Gamma(x) \le t-1$,

выполняется:

$$E(x) \cdot S(x) \equiv \Gamma(x) \mod x^{n-k} \quad (1)$$

Альтернативный метод нахождения $E(x)$ – расширенный алг-м Евклида

$$(1): \quad E(x) \cdot \underbrace{S(x)}_{\deg S(x) \le n-k-1} + x^{n-k} \cdot A(x) = \Gamma(x)$$

Запускаем расширенный алг-м Евклида для $S(x)$, x^{n-k}.

i-ый шаг алгоритма возвращает E_{i-1}, A_{i-1}, Γ_i, т.ч.

$$E_{i-1}(x) \cdot S(x) + x^{n-k} \cdot A_{i-1}(x) = \Gamma_i(x)$$

Как только степень $\Gamma_i(x)$ станет меньше степени $E_{i-1}(x)$, терминируем расш. алг-м Евклида.

Как получить A_i, E_i?

Положим $\Gamma_0 = x^{n-k}$

$\Gamma_1 = S(x)$

На шаге $i \geq 0$ $\exists$ q_i - частное от деления $r_i(x)$ на $r_{i+1}(x)$, т.е.

$$\underbrace{r_i(x)}_{\text{делимое}} = q_i(x) \cdot \underbrace{r_{i+1}(x)}_{\text{делит.}} + \underbrace{r_{i+2}(x)}_{\text{остаток}}$$

$$\begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix} = \underbrace{\left[\prod_{j=0}^{i} \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \right]}_{= \begin{pmatrix} A_i & E_i \\ A_{i+1} & E_{i+1} \end{pmatrix}} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$