Лекция №8

Алгоритм Петерсона декодирования кода Рида-Соломона

Напоминание (см. Лекцию №6): для $1 \le k \le n$, $|\mathbb{F}| = n+1$

$S = \{1, \alpha, .., \alpha^{n-1}\}$, где α - примитивный эл-т $\mathbb{F}_q^*$

$$RS = \{ \underbrace{(c_0, \dots, c_{n-1})}_{c = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}} \in \mathbb{F}_q^n : \ c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{n-k}) = 0 \}$$

Рассмотрим алгоритм Петерсона.

$y = c + e$ - полученное слово

для $\ell \in \{1, .., n-k\}$, определим

$$S_\ell = \sum_{j=0}^{n-1} y_j \alpha^{\ell \cdot j} = \underbrace{\sum_{j=0}^{n-1} c_j \alpha^{\ell \cdot j}}_{\substack{c(\alpha^\ell) \\ \shortparallel \\ 0}} + \sum e_j \cdot \alpha^{\ell \cdot j} \in \mathbb{F}$$

определим $S(x) := \sum_{\ell=1}^{n-k} S_\ell \cdot x^{\ell-1}$, и

$E(x) = \prod_{j \in T} (1 - \alpha^j \cdot x)$, $T = \{i \mid e_i \neq 0\}$ - индексы ошибок

$\deg E(x) = |T| \le \tau$

$E(\alpha^{-j}) = 0 \quad \forall j \in T$

Лемма $$S(x) = \sum_{j \in T} e_j \alpha^j \left(\frac{1 - (\alpha^j x)^{n-k}}{1 - \alpha^j x} \right)$$

$\triangleleft$ $$S(x) = \sum_{\ell=1}^{n-k} S_\ell x^{\ell-1} = \sum_{\ell=1}^{n-k} x^{\ell-1} \sum_{j \in T} e_j \alpha^{j \cdot \ell} =$$

$$= \sum_{j \in T} e_j \alpha^j \sum_{\ell=1}^{n-k} \underbrace{x^{\ell-1} \cdot \alpha^{j(\ell-1)}}_{(x \cdot \alpha^j)^{\ell-1}} = \sum_{j \in T} e_j \alpha^j \cdot \frac{(1 - (\alpha^j x)^{n-k})}{1 - \alpha^j x} \ \blacktriangleright$$

Рассмотрим $E(x) \cdot S(x)$:

$$E(x) \cdot S(x) = \sum_{j \in T} e_j \alpha^j \left(\frac{1 - (\alpha^j x)^{n-k}}{1 - \alpha^j x} \right) \cdot \prod_{i \in T} (1 - \alpha^i x) =$$

$$= \sum_{j \in T} e_j \alpha^j (1 - (\alpha^j x)^{n-k}) \prod_{\substack{i \in T \\ i \neq j}} (1 - \alpha^i x) =$$

$$= \underbrace{\sum_{j \in T} e_j \alpha^j \prod_{\substack{i \in T \\ i \neq j}} (1 - \alpha^i x)}_{\Gamma(x)} - \sum_{j \in T} e_j \alpha^j (\alpha^j \boxed{x)^{n-k}} \cdot \prod_{\substack{i \in T \\ i \neq j}} (1 - \alpha^i x)$$

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

Key Equation

Алгоритм Петерсона использует ур-ие (1) для нахождения $E(x)$:

- В (1) мы знаем $S(x)$
- $\deg \Gamma(x) \le \tau - 1 \Rightarrow$ коэфф-ты левой части $(E(x) \cdot S(x))$ при x^j для $\tau \le j \le n-k-1$ $= 0$

$\Rightarrow$ $n - k - \tau$ уравнений для τ неизвестных коэфф-тов $E(x)$ ($e_0 = 1$ - св. член в $E(x)$).

- Зная $E(x)$, найдём его корни $\Rightarrow$ найдём позиции ошибок
- Т.к. система, полученная из (1), может иметь несколько решений, соответствующий $E_1(x)$ (решение системы) будет кратен $E(x)$.

Алгоритм

Шаг 1. Вычислить $S(x)$ // $O(n^{\omega})$

Шаг 2. Составить из (1) систему ур-ий для неизвестных e_i' $\left(E_1(x)=1+\sum e_i' x^i\right)$ // $O(n^3)$

Шаг 3 Найти корни $E_1(x)$. // $O(n^3)$

Положим корни $\alpha^{-i_1}, \dots, \alpha^{-i_\ell}$, $\ell \le \tau$

Шаг 4. Удалить позиции $i_1, \dots, i_\ell$ из полученного слова, восстановить сообщение по нестёртым символам с помощью интерполяции. // $O(n^3)$

Корректность

Лемма Многочлен $E_1(x)$, найденный на шаге 2, кратен $E(x)$
$\{\text{корни } E(x)\} \subseteq \{\text{корни } E_1(x)\}$

$\triangleleft$ $E(x) = \prod_{j\in T}(1-\alpha^j x)$

$$E^{-1}(x) \bmod x^{n-k} = \prod_{j\in T}\left(1+\alpha^j x + \dots + (\alpha^j x)^{n-k-1}\right)$$

$$\left\{ \text{В самом деле, } E^{-1}(x)\cdot E(x) = \prod_{j\in T}\sum_{i=0}^{n-k-1}(\alpha^j x)^i \cdot \prod_{j\in T}(1-\alpha^j x) = \prod_{j\in T}\left(\frac{1-(\alpha^j x)^{n-k}}{1-\alpha^j x}\right)\cdot\prod_{j\in T}(1-\alpha^j x) = \prod_{j\in T}\left(1-(\alpha^j x)^{n-k}\right) \equiv 1 \bmod x^{n-k} \right\}$$

$\Leftrightarrow$ из (1): $S(x) = \Gamma(x)\cdot E^{-1}(x) \bmod x^{n-k}$ (2)

$\exists$ $\Gamma_1(x)$ - это м-н степени $\le \tau-1$, т.ч.

$$E_1(x)\cdot S(x) = \Gamma_1(x) \bmod x^{n-k} \qquad (3)$$

$\tau = \left\lfloor \frac{d-1}{2} \right\rfloor$

из (2) и (3) $\quad E_1(x)\cdot\Gamma(x)\cdot E^{-1}(x) \equiv \Gamma_1(x) \mod x^{n-k} \Leftrightarrow$

$$\underbrace{E_1(x)\cdot\Gamma(x)}_{\deg E_1(x)\cdot\Gamma(x) \leq \tau+\tau-1=2\tau-1} \equiv \underbrace{E(x)\cdot\Gamma_1(x)}_{\deg:\ \tau+\tau-1 \leq 2\tau-1 \leq d-2 \leq n-k-1} \mod x^{n-k}$$

$\Leftrightarrow$ mod редукция не имеет смысла, сравнение есть р-во многочленов.

$$\Leftrightarrow \quad E_1(x)\cdot\Gamma(x) = E(x)\cdot\Gamma_1(x) \Rightarrow E(x) \mid E_1(x)\cdot\Gamma(x)$$

НОД $(E(x), \Gamma(x)) = 1$ (т.к. $\{\alpha^{-j} \mid j\in T\}$ - все корни $E(x)$

$$\Gamma(\alpha^{-j}) = e_j \prod_{\substack{i\in T\\ i\neq j}} (\alpha^j - \alpha^i) \neq 0 \}$$

$$\Rightarrow E(x) \mid E_1(x)$$

▶

Лемма

$$e_\ell = -\frac{\Gamma(\alpha^{-\ell})}{E'(\alpha^{-\ell})} \quad \forall \ell\in T, \text{ где } E'(x) = \frac{\partial E(x)}{\partial x}$$

◁ из (1):

$$E(x)\cdot S(x) = \Gamma(x) - \sum_{j\in T} e_j \alpha^j (\alpha^j x)^{n-k} \prod_{i\neq j} (1-\alpha^i x) \qquad (1^*)$$

$$E(x) = \prod_{i\in T} (1-\alpha^i x)$$

$$E'(x) = \sum_{j\in T} -\alpha^j \prod_{\substack{i\in T\\ i\neq j}} (1-\alpha^i x)$$

$$E'(\alpha^{-\ell}) = \sum_{j\in T} -\alpha^j \prod_{\substack{i\in T\\ i\neq j}} (1-\alpha^{i-\ell}) \underset{j=\ell}{=} -\alpha^\ell \prod_{\substack{i\neq\ell\\ i\in T}} (1-\alpha^{i-\ell})$$

Подставим $x=\alpha^{-\ell}$ в (1^*):

$$0 = E(\underbrace{\alpha^{-\ell}}_{\text{корень}})\cdot S(\alpha^{-\ell}) = \Gamma(\alpha^{-\ell}) - \underbrace{\sum_{j\in T} e_j \alpha^j (\alpha^{j-\ell})^{n-k} \underbrace{\prod_{i\neq j} (1-\alpha^{i-\ell})}_{=0 \text{ для } i=\ell}}$$

$\neq 0$ только для $j = l$

$$= \Gamma(\alpha^{-l}) - e_l \cdot \alpha^{l} \cdot 1 \cdot \prod_{i \neq l} (1-\alpha^{i-l}) = \Gamma(\alpha^{-l}) + e_l \cdot E'(\alpha^{-l})$$

В итоге, $0 = \Gamma(\alpha^{-l}) + e_l E'(\alpha^{-l})$

$$e_l = -\frac{\Gamma(\alpha^{-l})}{E'(\alpha^{-l})}$$

Пример

$\alpha^0 \ \alpha^1 \ \alpha^2 \ \alpha^3 \quad \alpha = 2$

$\mathbb{F}_5$, $S = \{1, 2, 4, 3\}$, $n = 4$
$k = 2$
$d = n - k + 1 = 3$, $\tau = 1$

$$y = [2, 4, 1, 0]$$

$$H = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{bmatrix}$$

$$s = Hy = \begin{bmatrix} 4 \\ 4 \end{bmatrix} \qquad s(x) = 4 + 4x$$

$$E(x) = 1 - e_1 x \qquad \deg E(x) = \tau = 1$$

$$\Gamma(x) = \gamma_0 \qquad \deg \Gamma(x) = 1$$

ур-ие (1): $E(x) \cdot s(x) = \Gamma(x) \mod x^2$

$$(1 - e_1 x) \cdot (4 + 4x) \equiv \gamma_0 \mod x^2$$

$$4 + 4x - 4e_1 x \equiv \gamma_0 \mod x^2$$

$$4 + (4 - 4e_1)x \equiv \gamma_0 \mod x^2$$

$$\Longleftrightarrow$$

$$\begin{cases} 4 = \gamma_0 \\ 4 - 4e_1 = 0 \end{cases} \Longleftrightarrow \begin{cases} \gamma_0 = 4 \\ e_1 = 1 \end{cases} \text{ в } \mathbb{F}_5$$

$$\Rightarrow E(x) = 1 - \underset{\alpha^0}{\underset{\shortparallel}{1}} \cdot x$$

$\Rightarrow$ ошибка в нулевой позиции (первой, если считать с 1)

$$e_0 = -\frac{\Gamma(\overset{1}{\overset{\shortparallel}{d^0}})}{E'(\underset{1}{\underset{\shortparallel}{d^0}})} = -\frac{4}{-1} = 4$$

$$y = c + e$$

$$c = y - e = [2,4,1,0] - [4,0,0,0] = [3,4,1,0].$$