Лекция № 7

Декодирование кода Рида-Соломона: алгоритм Welch-Berlekamp

0. Код Рида-Соломона

$RS_{\mathbb{F},S}(n,k) = \{ (f(\alpha_1) \ldots f(\alpha_n)) \in \mathbb{F}^n \mid f \in \mathbb{F}[x], \deg f(x) \le k-1 \}$

$S = \{\alpha_1 \ldots \alpha_n\} \subseteq \mathbb{F}$

Encode $(m \in \mathbb{F}^k)$: 1) $f(x) = m_0 + m_1 x + \ldots + m_{k-1} x^{k-1}$
2) Return $(f(\alpha_1) \ldots f(\alpha_n)) \in \mathbb{F}^n$

$d(RS_{\mathbb{F},S}) = n-k+1$

$RS_{\mathbb{F},S}(n,k)$ декодирует $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$ ошибок

$\tau := \left\lfloor \frac{n-k}{2} \right\rfloor$

I. Алгоритм Welch-Berlekamp

$\exists y = (y_1 \ldots y_n)$ – полученное слово $(\notin RS)$, $y_i \ne f(\alpha_i)$ для максимум τ индексов.

Из предыдущей лекции: Если позиции ошибок известны, т.е. известно мн-во индексов $E = \{ i : y_i \ne f(\alpha_i) \}$, то мы можем восстановить $f(x)$ интерполяцией по точкам $y_i = f(\alpha_i)$

Определим многочлен $E(x) = \prod\limits_{f(\alpha_i) \ne y_i} (x - \alpha_i)$ – полином-локатор

$$\deg E(x) \le \tau$$

Для всех $1 \le i \le n$ и $E(x)$ выполняется: $E(\alpha_i) \cdot y_i = E(\alpha_i) \cdot f(\alpha_i)$

(Если i-поз-ия ошибки, то обе части равенства $= 0$, иначе $y_i = f(\alpha_i)$)

Положим, $N(x) := E(x)\cdot f(x)$, $\deg N(x) \le \tau + k - 1$

$P(x,Y) = E(x)\cdot Y - N(x)$.

Заметим, что $P(d_i, y_i) = E(d_i)\cdot y_i - E(d_i)\cdot f(d_i) = 0 \quad \forall i$.

Алгоритм декодирования

Шаг 1 Найти ненулевой многочлен $Q(X,Y)$, т.ч

- $Q(x,Y) = E_1(X)\cdot Y - N_1(X)$
- $\deg E_1(x) \le \tau$, $\deg N_1(x) \le \tau + k - 1$
- $Q(d_i, y_i) = 0 \quad \forall i$

Шаг 2 Вернуть $\frac{N_1(x)}{E_1(x)}$.

Корректность 1) мн-н $Q(x,Y)$ существует (достаточно найти $E_1(x) = E(x) = \prod\limits_{f(d_i)\neq y_i} (x - d_i)$, $N_1 = E(x)\cdot f(x)$)

2) $\forall$ решение E_1, N_1 удовлетворяет $\frac{N_1}{E_1} = f$

Δ Положим, $R(x) = E_1\cdot f - N_1$

- $\deg R(x) \le \tau + k - 1$
- $R(x)$ имеет как min. $n-\tau$ корней, т.к $\forall$ позиции i без ошибки имеем $f(d_i) = y_i$ и $R(d_i) = Q(d_i, y_i) = 0$
- при $n - \tau > \tau + k - 1$ $(*)$ $\Rightarrow R \equiv 0 \Leftrightarrow E_1\cdot f = N_1 \Rightarrow f = \frac{N_1}{E_1}$

$$\left.\begin{aligned} &\tau = \left\lfloor \frac{n-k}{2} \right\rfloor \\ &2\tau < n - k + 1 \\ &\tau < \frac{n-k+1}{2} \end{aligned}\right\} \Rightarrow (*) \text{ всегда выполняется.}$$

$\blacktriangleright$

Сложность Для нахождения мн-ов $E_1 = \sum_{i=0}^{\tau} e_i x^i$, $N_1 = \sum_{i=0}^{\tau+k-1} n_i x^i$

используем $Q(\alpha_i, y_i) = 0$ $\Rightarrow$ получаем систему из $\{(e_0.., e_\tau), (n_0, .., n_{\tau+k-1})\}$

неизвестных (их всего $2\tau+k-1 \leq n$) и n уравнений.

Решаем систему методом Гаусса: $O(n^3)$

Деление мн-ов: $O(n \cdot \lg^{O(1)} n)$ операций в $\mathbb{F}$

$\Bigg\}$ $O(n^3)$.

II Пример

$GF(5) = \langle 2 \rangle$

$S = \{1, 2, 4, 3\}$

$n = 4$, $k = 2$ $\Rightarrow$ $d = n - k + 1 = 3$ $\Rightarrow$ $\tau = 1$

$m = (4, 3) \rightarrow f(x) = 4 + 3x$

$c = Enc(m) = (f(1), f(2), f(4), f(3)) = (2, 0, 1, 3) \overset{+e}{\rightsquigarrow} (2, 1, 1, 3) = y$

$\deg E_1(x) = \tau = 1$ $\qquad E_1(x) = e_0 + \underset{1}{\underset{\parallel}{e_1}} x = e_0 + x$

$\deg N_1(x) = \tau + k - 1 = 2$ $\quad N_1(x) = n_0 + n_1 x + n_2 x^2$

$Q(\alpha_i, y_i) = 0 \ \forall i$ $\qquad Q(x, y) = E_1(x) \cdot y - N_1(x)$

$$Q(\alpha_1, y_1) = Q(1, 2) = E_1(1) \cdot 2 - N_1(1) = (e_0 + 1) \cdot 2 - (n_0 + n_1 \cdot 1 + n_2 \cdot 1^2) = 0$$
$$Q(\alpha_2, y_2) = Q(2, 1) = E_1(2) \cdot 1 - N_1(2) = (e_0 + 2) \cdot 1 - (n_0 + n_1 \cdot 2 + n_2 \cdot 4) = 0$$
$$Q(\alpha_3, y_3) = Q(4, 1) = E_1(4) \cdot 1 - N_1(4) = (e_0 + 4) \cdot 1 - (n_0 + n_1 \cdot 4 + n_2 \cdot 1) = 0$$
$$Q(\alpha_4, y_4) = Q(3, 3) = E_1(3) \cdot 3 - N_1(3) = (e_0 + 3) \cdot 3 - (n_0 + n_1 \cdot 3 + n_2 \cdot 4) = 0$$

$\Leftrightarrow$

$$\begin{cases} 2e_0 + 2 - n_0 - n_1 - n_2 = 0 \\ e_0 + 2 - n_0 - 2n_1 - 4n_2 = 0 \\ e_0 + 4 - n_0 - 4n_1 - n_2 = 0 \\ 3e_0 + 4 - n_0 - 3n_1 - 4n_2 = 0 \end{cases} \Leftrightarrow \begin{cases} e_0 = 3 \\ n_0 = 2 \\ n_1 = 3 \\ n_2 = 3 \end{cases} \Leftrightarrow \begin{matrix} E_1 = 3 + x = (x - 2) \\ N_1 = 2 + 3x + 3x^2 \end{matrix}$$

второй эл-т в мн-ве S
$\Rightarrow$ ошибка во втором символе

$$\begin{array}{r|l} 3x^2 + 3x + 2 & x + 3 \\ \cline{2-2} -\ 3x^2 + 4x & 3x + 4 \\ \hline 4x + 2 & \\ -\ 4x + 2 & \\ \hline 0 & \end{array}$$