Лекция 11

Ilya Yaroshevskiy

10 ноября

Содержание

1 Циклические коды

1.1 Коды Рида-Соломона

Определение. Код Рида-Соломона – код БЧХ длины $q-1$ над $GF(q)$. Минимальный многочлен $\beta \in GF(q)$ над $GF(q)$: $M_\beta(x) = x - \beta$. Порождающий многочлен кода Рида-Соломона $g(x) = \prod_{i=0}^{\delta-2}(x-\alpha^{b+i})$. Размерность кода $k = n-\delta+1$. Минимальное расстояние $d \geq \delta$. Граница Синглтона: $d \leq n-k+1 = \delta \implies d = n-k+1$. Код с максимальным достижимым расстоянием

1.2 Декодирование кодов БЧХ

Замечание. Рассмотрии исправление ошибок в векторе $y = c + e$.

- $y(x) = a(x)g(x) + e(x)$
- Синдром: $S_i = y(\alpha^{b+i}) = a(\alpha^{b+i})g(\alpha^{b+i}) + e(\alpha^{b+i}) = e(\alpha^{b+i}), 0 \leq i < \delta - 1$
- Пусть ошибки произошли в позициях $j_1, \ldots, j_t, t \leq \lfloor(\delta-1)/2\rfloor$

$$S_i = \sum_{r=0}^{n-1} e_r \alpha^{(b+i)r} = \sum_{l=1}^{t} c_{j_l} \alpha^{(b+i)j_l}$$

- Значение ошибок $E_l = e_{j_l}$
- Локаторы ошибок $X_l = \alpha^{j_l}$

$$S_i = \sum_{l=1}^{t} E_l X_l^{b+i}, 0 \leq i < \delta - 1$$

1.2.1 Поиск локаторов ошибок

Многочлен локаторов ошибок $\Lambda(x) = \prod_{l=1}^{t}(1 - X_l x) = \sum_{l=0}^{t} \Lambda_l x^l$

$$0 = \Lambda(X_i^{-1}) = \sum_{l=0}^{t} \Lambda_l X_i^{-l}, 1 \leq i \leq t$$

$$0 = E_i X_i^{b+j+1} \overbrace{\sum}^{\sum_{l=0}^{t} \Lambda_l X_i^{-l} = \sum_{l=0}^{t} \Lambda_l E_i X_i^{b+j+t-l} =}$$
$$= E_i X_i^{bcj+t} + \Lambda_1 E_i X_i^{b+j+t-l} + \cdots + \Lambda_t E_i X_i^{b+j}, 0 \le j < t$$

$$0 = \sum_{i=1}^{t} E_i X_i^{b+j+t} + \Lambda_1 \sum_{i=1}^{t} E_i X_i^{b+j+t-1} + \cdots + \Lambda_t \sum_{i=1}^{t} E_i X_i^{b+j}$$
$$0 = S_{j+t} + \Lambda_1 S_{j+t-1} + \cdots + \Lambda_t S_j$$

$$\Lambda_1 S_{j+t-1} + \cdots + \Lambda_t S_j = -S_{j+t}$$
$$\underbrace{\begin{pmatrix} S_0 & S_1 & \dots & S_{t-1} \\ S_1 & S_2 & \dots & S_t \\ \vdots & \vdots & \ddots & \vdots \\ S_{t-1} & S_t & \dots & S_{2t-2} \end{pmatrix}}_{\mathbb{S}_t} \begin{pmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_t \\ -S_{t+1} \\ \vdots \\ -S_{2t-1} \end{pmatrix}$$

Теорема 1.1. $\mathbb{S}_z$ обратима, если z равно числу произошедших ошибок t, и вырождена, если $z > t$

Доказательство. $S_i = \sum_{l=1}^{t} E_l X_l^{b+1}., E_z = X_z = 0$ при $z > t$

$$\mathbb{S}_z = \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_z \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{z-1} & X_2^{z-1} & \dots & X_z^{z-1} \end{pmatrix}}_{W} \underbrace{\begin{pmatrix} E_1 X_1^b & 0 & \dots & 0 \\ 0 & E_2 X_2^b & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & E_z X_z^b \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} 1 & X_1 & \dots & X_1^{z-1} \\ 1 & X_2 & \dots & X_2^{z-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_z & \dots & X_z^{z-1} \end{pmatrix}}_{W^T}$$

D вырождена, если $z > t$ и обратима при $z \le t$. W – матрица Вандермонда, обратима при $z = t$. $\square$

1.2.2 Алгоритм Питерсона-Горенстайна-Цирлера

$$\Lambda_1 S_{j+t-1} + \cdots + \Lambda_t S_j = -S_{j+t}$$
$$\underbrace{\begin{pmatrix} S_0 & S_1 & \dots & S_{t-1} \\ S_1 & S_2 & \dots & S_t \\ \vdots & \vdots & \ddots & \vdots \\ S_{t-1} & S_t & \dots & S_{2t-2} \end{pmatrix}}_{\mathbb{S}_t} \begin{pmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_t \\ -S_{t+1} \\ \vdots \\ -S_{2t-1} \end{pmatrix}$$

- Вычисление синдрома $S_i = y(\alpha^{b+i}), 0 \le i < \delta - 1$. Сложность при использовании схемы Горнера $O((\delta - 1)n)$
- Будем уменьшать предполагаемое число ошибок $t \le \tau = \lfloor (\delta - 1)/2) \rfloor$, пока матрица $\mathbb{S}_t$ не станет обратимой. Проверка обратимости матрицы требует $O(t^3)$ операций
- Решение СЛАУ задает коэффициенты $\Lambda_i, 1 \le i \le t$, многочлена локаторов ошибок $\Lambda(x) = 1 + \sum_{i=1}^{t} \Lambda_i x^i$
- Сложность непосредственного подбора t и решения СЛАУ $O(\tau^4)$
- Локаторы ошибок $X_i = \alpha^{j_i} : \Lambda(X_i^{-1}) = 0, 1 \le i \le t$. Процедура Ченя поиска корней: подставим в $\Lambda(x)$ все элементы $\alpha^i, 0 \le i < n$. Сложность $O(nt)$
- Значения ошибок $E_l : S_i \sum_{l=1}^{t} E_l X_l^i, 0 \le i < t$. Сложность непосредственного решения $O(t^3)$

$$S_i = \sum_{l_1}^{t} E_l X_l^{b+i}, 0 \le i < \delta - 1 \quad S(x) = \sum_{i=0}^{\delta-2} S_i x^i = \sum_{l=1}^{t} E_l X_l^b \sum_{i=0}^{\delta-2} (X_l x)^i$$

$$1 - (\mathrm{X}_l x)^{\delta-1} d(1 - X_l x) \left(\sum_{i=0}^{\delta-2} (X_l x)^i \right) = 1 \mod x^{\delta-1}$$
$$\sum_{i=0}^{\delta-2} (X_l x)^i = \frac{1}{1 - X_l x} \mod x^{\delta-1}$$
$$\mathrm{S(x)} = \sum_{l=1}^{t} \frac{E_l X_l^b}{1 - X_l x} \mod x^{\delta-1}$$

Многочлен значений ошибок $\Gamma(x) = \sum_{l=1}^{t} E_l X_l^b \prod_{j \ne l} (1 - X_j x) \equiv \Lambda(x) \sum_{l=1}^{t} \frac{E_l X_l^b}{1 - X_l x} \mod x^{b-1}$.

$$\Gamma(x) \equiv \Lambda(x) S(x) \mod x^{\delta-1}, \deg \Lambda(x) \le \lfloor (\delta - 1)/2 \rfloor, \deg \Gamma(x) < \lfloor (\delta - 1)/2 \rfloor$$

Теорема 1.2 (Алгоритм Форни быстрого поиска значений ошибок)**.** $E_i = \frac{X_i^{-b} \Gamma(X_i^{-1})}{\prod_{j \ne i} (1 - X_j X_i^{-1})}, 0 \le i < t$

Доказательство.

$$\frac{X_i^{-b}(X_i^{-1})}{\prod_{j \ne i}(1 - X_j X_i^{-1})} = \frac{X_i^{-b} \sum_{l=1}^{t} E_l X_l^b \prod_{j \ne i}(1 - X_j X_i^{-1})}{\prod_{j \ne i}(1 - X_j X_i^{-1})} = \frac{E_i \prod_{j \ne i}(1 - X_j X_i^{-1})}{\prod_{j \ne i}(1 - X_j X_i^{-1})} = E_i$$

□

Сложность $O(t^2)$

1.3 Расширенный алгоритм Евклида

Поиск наибольшего общего делителя $r_{-1}(x) = a(x), r_0(x) = b(x)$

$$r_{i-1}(x) = q_i(x) r_i(x) + r_{i+1}(x), \deg r_{i+1}(x) < \deg r_i(x)$$

НОД равен последнему ненулевому остатку $r_i(x)$

$$\begin{pmatrix} r_i(x) & r_{i-1}(x) \end{pmatrix} \begin{pmatrix} -q_i(x) & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} r_{i+1}(x) & r_i(x) \end{pmatrix}$$

$$\begin{pmatrix} b(x) & a(x) \end{pmatrix} \underbrace{\prod_i \begin{pmatrix} -q_i(x) & 1 \\ 1 & 0 \end{pmatrix}}_{U(x)} = \begin{pmatrix} 0 & \gcd(a(x), b(x)) \end{pmatrix}$$

Теорема 1.3 (Безу)**.** Существуют многочлены $u(x), v(x) : b(x)u(x) + a(x)v(x) = \gcd(a(x), b(x))$

Пусть $U_j(x) = \prod_{i=0}^{j} \begin{pmatrix} -q_i(x) & 1 \\ 1 & 0 \end{pmatrix} = U_{j-1} \underbrace{\begin{pmatrix} -q_j(x) & 1 \\ 1 & 0 \end{pmatrix}}_{Q_j(x)} = \begin{pmatrix} u_{j,0}(x) & u_{j-1,0}(x) \\ u_{j,1}(x) & u_{j-1,1}(x) \end{pmatrix}$, $U_{-1}(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} r_0(x) & r_{-1}(x) \end{pmatrix} \begin{pmatrix} u_{j,0}(x) & u_{j-1,0}(x) \\ u_{j,1}(x) & u_{j-1,1}(x) \end{pmatrix} = \begin{pmatrix} r_{j+1}(x) & r_j(x) \end{pmatrix}$$

1. $\deg u_{j,0}(x) = \deg u_{j-1,0}(x) + \deg q_j(x) = \sum_{i=0}^{j} \deg q_i(x) = \sum_{i=0}^{j} (\deg r_{i-1}(x) - \deg r_i(x)) = \deg r_{-1}(x) - \deg r_j(x)$
2. $u_{j,0}(x) u_{j-1,1}(x) - u_{j-1,0}(x) u_{j,1}(x) = \det U_j(x) = \prod_{i=0}^{j} \det Q_j(x) = (-1)^{j+1}$
3. $\gcd(u_{j,0}(x), u_{j,1}(x))$1. Если $f(x) | u_{j,0}(x), f(x) | u_{j,1}(x)$, то $f(x) | (u_{j,0}(x) u_{j-1,1}(x) - u_{j-1,0}(x) u_{j,1}(x))$
4. $r_{j+1}(x) = r_0(x) u_{j,0}(x) + r_{-1}(x) u_{j,1}(x)$
   $r_{j+1}(x) \equiv r_0(x) u_{j,0}(x) \mod r_{-1}(x)$ – похоже на ключевое уравнение
5. $\gcd(r_{j+1}(x), u_{j,0}(x)) = \gcd(r_{-1}(x), u_{j,0}(x))$
   $f(x) | r_{j+1}(x) \wedge f(x) | usj, 0(x) \implies f(x) | r_{-1}(x)$ $f(x) | r_{-1}(x) \wedge f(xj | u_{j,0}(x) \implies f(x) | r_{j+1}(x)$

1.4 Алгоритм Сугиямы

Пусть $\delta = 2\tau + 1$

1. Пусть $r_{-1}(x) = x^{2\tau}, r_0(x) = S(x)$
2. Выполнять $r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x)$, пока не получится $\deg r_i(x) \geq \tau, \deg r_{i+1}(x) < \tau$
3. $\Gamma(x) = r_{i+1}(x), \Lambda(x) = u_{i,0}(x)$

Корректность алгоритма

1. Степени $r_i(x)$ монотонно убывают, т.е. условие останова достижимо
2. $\Gamma(x) = r_{i+1}(x) = r_0(x)u_{i,0}(x) + r_{-1}(x)u_{i,1}(x) = S(x)\Lambda(x) + x^{2\tau}u_{i,1}(x) \equiv S(x)\Lambda(x) \mod x^{2\tau}$
3. $\deg u_{i,0}(x) = \deg r_{-1}(x) - \deg r_i(x) \leq 2\tau - \tau \leq \tau$
4. Пусть $\Gamma'(x) \equiv S(x)\Lambda'(x) \mod x^{2\tau}, \deg \Lambda'(x) \leq \tau, \deg \Gamma'(x) < \tau$. Если $\Lambda'(x), \Gamma'(x)$ – истинные многочлены локаторов и значений ошибок, то $\gcd(\Lambda'(x), \Gamma'(x)) = 1$

$$\Gamma'(x)\Lambda(x) \equiv \Lambda(x)S(x)\Lambda'(x) \equiv \Gamma(x)\Lambda'(x) \mod x^{2\tau}$$

$\deg \Gamma'(x) + \deg \Lambda(x) < 2\tau, \deg \Gamma(x) + \deg \Lambda'(x) < 2\tau \implies \Gamma'(x)\Lambda(x) = \Gamma(x)\Lambda'(x)$ Из взаимной простоты $\Lambda'(x), \Gamma'(x)$ следует, что $\mu(x) = \frac{\Lambda(x)}{\Lambda'(x)} = \frac{\Gamma(x)}{\Gamma'(x)}$ – многочленю

$$\Gamma'(x)\mu(x) = \Gamma(x) = S(x)\Lambda(x) + x^{2\tau}u_{i,1}(x) = S(x)\Lambda'(x)\mu(x) + x^{2\tau}u_{i,1}(x)$$

$\implies \mu(x)|u_{i,1}(x)$. Но $\Lambda(x) = \mu(x)\Lambda'(x) = u_{i,0}(x)$ и $u_{i,1}(x)$ взаимно просты $\implies \mu(x) = const$

1.5 Сложность декодирования кодов БЧХ и Рида-Соломона

- Вычисление синдрома
  - Схема Горнера: $S_i = y(\alpha^{b+i}) = y_0 + \alpha^{b+i}(y_1 + \alpha^{b+i}(y_3 + \dots))), 0 \leq i < \delta$. Сложность $O(n\delta)$ операций
  - Метод Герцеля: $r_i(x) \equiv y(x) \mod M_{\alpha^{b+i}}(x); \quad S_i = r_i(\alpha_{b+i}), \alpha \in GF(p^m)$. $M_{\alpha^{b+i}} \in GF(p)[x]$ – минимальный многочлен α^{b+i}. Деление на него тербует только сложений. Минимальные многочлены многих α^{b+i} совпадают
- Решение ключевого уравнения $\Gamma(x) \equiv S(x)\Lambda(x) \mod x^{\delta-1}$. Расширенный алгоритм Евклида: $O(\delta^2)$ операций
- Поиск корней X_i^{-1} многочлена локаторов ошибок $\Lambda(x)$. Процедура Ченя (перебор $\alpha^i, 0 \leq i < n$ и проверка $\Lambda(\alpha^i) = 0$) со сложностью $O(n\delta/2)$
- Поиск значений ошибок. Метод Форни со сложностью $O(\delta^2)$