Списочное декодирование

Tuesday 24 November 2020 11:46

Линейный $[n,k,d]$-код может исправить $\lfloor \frac{d-1}{2} \rfloor$ ошибок
$\exists$ алг-мы декодирования по данному $y = \underline{c} + e$ с $wt(e) < \lfloor \frac{d-1}{2} \rfloor$ возвращающ уникальный вектор.
Мы можем увеличить кол-во возможных ошибок, позволяя алг-мам вернуть список векторов L т.ч. $\Delta(L, y)$ - мало

I. Списочное декодирование кода RS

$$RS_{F, S=\{d_1..d_n\}} = \{ p(d_1), \dots, p(d_n) \in F^n \mid p \in F[x], \deg(p) \le k-1 \}$$

$$d = n-k+1$$

Задача поиска двух многочленов Положим $p_1(x), p_2(x) \in F[x]$, $\deg p_1(x) = \deg p_2(x) \le k-1$
Положим, $n \geq \underline{4k}$ - чётное (для упрощения); $d_1, \dots, d_n \in F$ - различны, $T \subset \{1, .., n\}$, $|T| = \frac{n}{2}$.
Пусть нам даны

$$y_i = \begin{cases} \underline{p_1}(d_i), & i \in T \\ \underline{p_2}(d_i), & i \in \{1, .., n\} \setminus T \end{cases} \qquad \forall i \in \{1, .., n\}$$

Задача состоит в вычислении $p_1(x), p_2(x)$ по данным парам $\{(d_i, y_i)\}_{i \le n}$

Связь с декодированием RS: мы могли бы считать $\{y_i\}_{i \le n}$ - полученным вектором (кодовое слово + "шум"), полагая, например $p_1(x)$ - исх. сообщение, однако, оба мн-на $p_1(x), p_2(x)$ не совпадают с $\vec{y}$ на $\frac{n}{2}$ значениях d_i
$\frac{n}{2} > \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{n-k}{2} \rfloor$. Поэтому "стандартные" алг-мы декодирования RS не подходят. Решение: списочный алг-м.

Из задачи поиска двух мн-в составим ур-ие:

$$(y_i - p_1(d_i)) \cdot (y_i - p_2(d_i)) = 0$$

— запись утверждения "либо $p_1(d_i) = y_i$, либо $p_2(d_i) = y_i$"

Положим

$$Q(x,y) = \underline{(y - p_1(x))(y - p_2(x))} = y^2 - \underbrace{(p_1(x) + p_2(x))}_{B(x)} y + \underbrace{p_1(x) \cdot p_2(x)}_{C(x)}$$

$\deg B(x) = k-1$ $\qquad B(x) = b_0 + b_1 x + .. + b_{k-1} x^{k-1}$
$\deg C(x) = 2(k-1)$ $\qquad C(x) = c_0 + c_1 x + \dots + c_{2(k-1)} x^{2(k-1)}$

$$Q(d_i, y_i) = 0 \quad \forall i = \overline{1, n}$$

Алгоритм

I. Составляем систему $Q(d_i, y_i) = 0$ из $\{b_0, \dots, b_{k-1}, c_0, \dots, c_{2(k-1)}\}$ неизвестных и n ур-ий. сложность: $O(n^3)$ / $O(n^\omega)$
получаем мн-ны $B(x), C(x)$ в явном виде

II. Факторизуем $Q(x,y) = (y - f_1(x))(y - f_2(x))$ сложность: $\deg_x Q \le 2k$, $\deg_y Q = 2$
вывод: $f_1(x), f_2(x)$
Факторизация мн-в общей степ. d над $\mathbb{F}_q$: $O(d^5 \log q)$ $\Rightarrow O(k^5 \log q)$

Корректность: на шаге I мы всегда отыщем какие-либо $B(x), C(x)$, т.к. $\exists$ решение $p_1(x), p_2(x)$ и $B(x) = p_1(x) + p_2(x)$, $C(x) = p_1(x) \cdot p_2(x)$
док-м, что на шаге II, мы получим корректные $p_1(x), p_2(x)$

Лемма $\forall\, Q(x,y)$, полученного на шаге I, $y - p_1(x) \mid Q(x,y)$ и $y - p_2(x) \mid Q(x,y)$

◀ док-м утверждение для $p_1(x)$ (аналог. для $p_2(x)$).

$\exists\, Q(x,y) = Q(y)$ — унитарный мн-н. Для того, чтобы док-ть, что $(y-\beta)$ — делит $Q(y)$, достаточно пок-ть, что $Q(\beta)=0$ $\Rightarrow$ чтобы пок-ть, что $(y - p_1(x))$ делит $Q(x,y)$, достаточно пок-ть, что $Q(x, p_1(x)) \equiv 0$ (тождеств. 0)

$R(x) := Q(x, p_1(x))$, $\underline{\deg(R(x)) \le 2(k-1)}$

$$R(x) = \underbrace{(p_1(x))^2}_{2(k-1)} - \underbrace{(p_1(x)+p_2(x))\cdot p_1(x)}_{2(k-1)} + \underbrace{p_1(x)\cdot p_2(x)}_{2(k-1)}$$

deg:

Заметим, что $\exists\ \frac{n}{2}$ различных α_i, т.ч. $p_1(\alpha_i) = y_i$

Для таких α_i : $R(\alpha_i) = Q(\alpha_i, \underbrace{p(\alpha_i)}_{=y_i}) = 0$

$\frac{n}{2} \geq 2k$ (по условию задачи)

$\Rightarrow$ мы нашли $2k$ различных корней в мн-не степени $2(k-1)$

$\Rightarrow R(x) \equiv 0$ ▶

Пример $GF(3^2) = \mathbb{F}_3[x]/(x^2+x+1)$

$n = 8$, $k = 2$

$d = n-k+1 = 7$ $S = \{1, \alpha, 2\alpha+1, 2\alpha+2, \underbrace{2}_{=\alpha^4}, 2\alpha, \alpha+2, \alpha+1\}$

$t = 3$

$\frac{n}{2} = 4$

$\exists\, m = [2\alpha+1, 2] \Rightarrow f(x) = 2x + 2\alpha + 1$

$c = \text{Encode}(m) = f(S) = (2\alpha, \alpha+1, 0, 2, 2\alpha+2, 1, \alpha+2, \alpha)$

$\exists\, y = c + e = (\underline{\alpha+2}, \alpha+1, \underline{\alpha}, 2, 2\alpha+2, \underline{2\alpha}, \alpha+2, \underline{0})$

$wt(e) = 4$

$B(x) = b_0 + b_1 \cdot x$

$C(x) = c_0 + c_1 x + c_2 x^2$

Шаг I $Q(x,y) = y^2 - B(x)\cdot y + C(x)$

$Q(x,y) = y^2 - (b_0 + b_1 x)\cdot y + (c_0 + c_1 x + c_2 x^2)$

$Q(\alpha_i, y_i) = 0$ $\Rightarrow$ 5 неизвестных $\{b_0, b_1, c_0, c_1, c_2\}$
8 уравнений

$$Q(1, \alpha+2) = (\alpha+2)^2 - (b_0 + b_1\cdot 1)\cdot(\alpha+2) + c_0 + c_1\cdot 1 + c_2 \cdot 1 = 0$$

$$Q(\alpha, \alpha+1) = (\alpha+1)^2 - (b_0 + b_1 \alpha)(\alpha+1) + c_0 + c_1\alpha + c_2\alpha^2 = 0$$

$$Q(2\alpha+1, \alpha) = \alpha^2 - (b_0 + b_1(2\alpha+1))\alpha + c_0 + c_1(2\alpha+1) + c_2(2\alpha+1)^2 = 0$$

$$Q(2\alpha+2, 2) = 2^2 - (b_0 + b_1(2\alpha+2))2 + c_0 + c_1(2\alpha+2) + c_2(2\alpha+2)^2 = 0$$

$$Q(2, 2\alpha+2) = (2\alpha+2)^2 + (b_0 + b_1\cdot 2)\cdot(2\alpha+2) + c_0 + c_1\cdot 2 + c_2\cdot(2)^2 = 0$$

$$\text{ур-ия 5}\quad \begin{array}{c} \begin{array}{ccccc} b_0 & b_1 & c_0 & c_1 & c_2 \end{array} \\ \begin{bmatrix} | & | & | & | & | \\ - & - & - & - & - \\ | & | & | & | & | \end{bmatrix} \end{array} \begin{array}{c} X \\ \begin{bmatrix} \\ \\ \\ \end{bmatrix} \end{array} = \begin{bmatrix} -(\alpha+2)^2 \\ -(\alpha+1)^2 \\ -\alpha^2 \\ -2^2 \\ -(2\alpha+2)^2 \end{bmatrix} \longrightarrow \text{sage} \rightarrow$$

$b_0 = \alpha + 1$

$b_1 = 2\alpha+1$

$c_0 = \alpha+1$

$c_1 = 0$

$c_2 = \alpha+1$

II $\quad Q(x,y) = y^2 - \underbrace{\big((\alpha+1)+(2\alpha+1)x\big)}\, y + \underbrace{(\alpha+1)+(\alpha+1)x^2}$

$$D = \big((\alpha+1)+(2\alpha+1)x\big)^2 - \underset{\substack{\shortparallel \\ +2}}{4}\big((\alpha+1)+(\alpha+1)x^2\big) =$$

$$= (1+\alpha x)^2$$

$$p_1(x) = \frac{(\alpha+1)+(2\alpha+1)x + 1+\alpha x}{2} = 2\cdot(2+\alpha+x) = \underbrace{1+2\alpha+2x}$$

$$p_2(x) = 2\cdot\big((\alpha+1)+(2\alpha+1)x-(1+\alpha x)\big) = 2\big(\alpha+(\alpha+1)x\big) = 2\alpha+(2\alpha+2)x$$

Возвращаем $\{\underset{m_1}{p_1(x)},\ \underset{m_2}{p_2(x)}\}$.