Лекция № 6
Код Рида-Соломона

0. Предварительные сведения. Конечные поля

$\mathbb{F}$ - кон. поле

1. $\forall$ ненулевой многочлен степени d с коэфф. из $\mathbb{F}$ имеет не более d корней в $\mathbb{F}$

2. $\forall p$ - простое $\exists!$ конечное поле мощности p. Это $\mathbb{F}_p$ - мн-во классов вычетов по модулю p.

3. p - простое
   $m \geqslant 1$, $g(x) \in \mathbb{F}_p[x]$ - неприводим. над $\mathbb{F}_p$, $\deg g(x) = m$.
   $\mathbb{F}_p[x]/g(x)$ - кон. поле = мн-во многочленов с коэфф. из $\mathbb{F}_p$ степени $\leq m$
   $|\mathbb{F}_p[x]/g(x)| = p^m$

4. $\forall$ конечное поле изоморфно такому полю

5. $\forall p$ - простое, $m \geqslant 1$ $\exists$ неприводимый мн-н $g(x) \in \mathbb{F}_p[x]$, $\deg g(x) = m$ $\Rightarrow$ $\exists$ кон. поле из p^m элементов

6. $\mathbb{F}_p[x]/g(x)$ - векторное пр-во р-ти m над $\mathbb{F}_p$

7. Мульт. группа кон. поля - циклическая. Т.е. $\exists \gamma \in \mathbb{F}$ - примитивный эл-т, т.ч. $\forall x \in \mathbb{F}$ может быть выбран из эл-тов $\{\gamma^0 = 1, \gamma^1, \dots \gamma^{|\mathbb{F}|-1}\}$
   $\mathbb{F}$ содержит $\varphi(|\mathbb{F}|-1)$ примитивных эл-тов

8. эл-ты $\mathbb{F}_{p^m}$ - это p^m различных корней мн-на $x^{p^m} - x \in \mathbb{F}_p[x]$

9. $\forall k | m$, $\mathbb{F}_{p^m}$ содержит единственное подполе р-ра p^k, состоящее из корней мн-на $x^{p^k} - x \in \mathbb{F}_p[x]$.

10. Мн-н $x^{p^m} - x = \prod f_i$
    $f_i \in \mathbb{F}[x]$ - неприв
    $\deg f_i | m$

I Код Рида-Соломона: определение

Опр. 1 Для целых $1 \le k < n$, $\mathbb{F}$-поля р-ра $|\mathbb{F}| \geq n$ и мн-ва $S = \{d_1 \dots d_n\} \subset \mathbb{F}$, код Рида-Соломона это

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

Чтобы закодировать сообщение $m = (m_0 \dots m_{k-1}) \in \mathbb{F}^k$:

1. Построим $p_m(x) = m_0 + m_1 x + \dots + m_{k-1} x^{k-1} \in \mathbb{F}[x]$
2. Вычисляем значения $p_m(x)$ в точках $d_1 \dots d_n$.

Лемма 1 Докажем, что $RS_{\mathbb{F},S}[n,k]$ — это лин. код.

$\triangle$

$$\begin{array}{l} c = (p_m(d_1) \dots p_m(d_n)) \\ + \\ c' = (p_{m'}(d_1) \dots p_{m'}(d_n)) \end{array}$$

$$(\underbrace{p_m(d_1) + p_{m'}(d_1)}, \dots, \underbrace{p_m(d_n) + p_{m'}(d_n)}_{\text{значение } p_{m+m'} \text{ в т. } d_n})$$

$$\begin{array}{l} m_0 + m_1 d_1 + m_2 d_1^2 + \dots m_{k-1} d_1^{k-1} \\ + \\ m_0' + m_1' d_1 + m_2' d_1^2 + \dots + m_{k-1}' d_1^{k-1} \end{array} = (m_0 + m_0') + (m_1 + m_1') d_1 + \dots + (m_{k-1} + m_{k-1}') d_1^{k-1} =$$

$= p_{m+m'}(d_1)$ — значение другого мн-на степени $\le k-1$ в т. d_1.

$\deg p_{m+m'} \le \max\{\deg p_m, \deg p_{m'}\} \le k-1$.

Аналог., скалирование на эл-т из $\mathbb{F}$. $\blacktriangleright$

Процедура кодирования сообщения m — это вычисление значений $p_m(x)$ в точках $d_1 \dots d_n$ $=$ умножение вектора-сообщения m на матрицу Вандермонда для $d_1 \dots d_n$

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ d_1 & d_2 & \dots & d_n \\ d_1^2 & d_2^2 & \dots & d_n^2 \\ \vdots & & & \\ d_1^{k-1} & d_2^{k-1} & \dots & d_n^{k-1} \end{pmatrix}$$

— образующая / порождающая матрица кода Рида-Соломона

$$RS_{\mathbb{F},S}[n,k] = m \cdot G$$

Теорема 2 (min. расстояние $RS_{\mathbb{F},S}[n,k]$)

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

◁ Покажем, что $\forall \underset{\neq 0}{c} \in RS_{\mathbb{F},S}[n,k]$, $wt(c) \geq n-k+1$.

$\exists (m_0 .. m_{k-1}) \neq 0 \rightarrow p_m(x) = m_0 + m_1 x + \dots m_{k-1} \cdot x^{k-1} \Rightarrow p_m(x)$ имеет не более чем $(k-1)$ корней в $\mathbb{F}_p \Rightarrow c = (p(\alpha_1) \dots p(\alpha_n))$ содержит не более $(k-1)$ нулей

$$\left.\begin{array}{l} wt(c) \geq n-k+1 \\ d \leq n-k+1 \text{ по границе Синглтона (лекция №3)} \end{array}\right\} \Rightarrow wt(c) = n-k+1$$

▶

Вывод: Код RS достигает границу Синглтона $\Rightarrow$ MDS код.
maximal distance separating

II Проверочная матрица кода RS

Рассмотрим $\mathbb{F} = \mathbb{F}_q$, α - примитивный, $q = n+1$, т.е. $S = \{\underset{\alpha^0}{\overset{\shortparallel}{1}}, \alpha, .., \alpha^{n-1}\} = \mathbb{F}_q^*$

Теорема 3 Для целых $1 \leq k < n$, $|\mathbb{F}| = q = n+1$, α - прим. в $\mathbb{F}$, $S = \{1, .., \alpha^n\}$, код RS

$$RS_{\mathbb{F},S}[n,k] = \{(c_0 .. c_{n-1}) \in \mathbb{F}_q^n \mid c(x) = c_0 + c_1 x + .. c_{n-1} x^{n-1} : c(\alpha) = c(\alpha^2) = .. = c(\alpha^{n-k}) = 0\}$$

Т.е. проверочная матрица имеет вид

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & .. & \alpha^{n-1} \\ \vdots & \alpha^2 & \alpha^4 & & \alpha^{2(n-1)} \\ & \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & & \alpha^{(n-k)(n-1)} \end{bmatrix}$$

◁ Размерность и длина кода, заданного в опр. 1 и т-ме 3 совпадают.

Покажем, что $\forall c \in RS_{\mathbb{F},S}[n,k]$, удовлетворяющее опр-ию 1, также удовлетворяют $H \cdot c = 0$

$$H \cdot c = 0 \Leftrightarrow c \in RS_{\mathbb{F},S}[n,k], \; c = \underset{\text{строка}}{m} \cdot G = G^T \cdot \underset{\text{столбец}}{m}$$

$\Downarrow$

$$H \cdot G^T \cdot m = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & & \alpha^{(n-k)(n-1)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & \dots & & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{k-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(k-1)} \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)(k-1)} \end{bmatrix} \cdot m =$$

$$= \left\{ \begin{array}{l} \alpha^n = \alpha^{q-1} = 1 \\ \forall (i\text{-ая строка } H) \times (j\text{-ый столбец } G^T) \\ \begin{bmatrix} 1 & \alpha^i & \alpha^{2i} & \dots & \alpha^{i(n-1)} \end{bmatrix} \begin{bmatrix} 1 \\ \alpha^j \\ \alpha^{j \cdot 2} \\ \vdots \\ \alpha^{j(n-1)} \end{bmatrix} = \sum_{k=0}^{n-1} \alpha^{k \cdot i + kj} \underset{\text{сумма степ. ряда}}{=} \dfrac{1 - \overset{=1}{\alpha^{n(i+j)}}}{1 - \alpha^{i+j}} = 0 \end{array} \right\}$$

$$= 0 \cdot m = 0$$

III Декодирование кода RS: декодирование удалённых символов (Erasure decoding)

$$c = (p(\alpha_1) \dots p(\alpha_n)) \xrightarrow[\text{CHANNEL}]{\text{ERASURE}} c^* = (* \ * \ p(\alpha_i) \ * \ p(\alpha_j))$$

осталось t корректных символов, и мы знаем их координаты

задача декодера RS - восстановить сообщение m по парам

$$(\alpha_1, p(\alpha_1)), \ (\alpha_i, p(\alpha_i)), \dots \ (\alpha_t, p(\alpha_t))$$

так как $\deg p(x) \leq k-1 \Rightarrow p(x)$ можно восстановить при $t \geq k$.

Алгоритм интерполяции Лагранжа

$t = k$ (если $t > k$, выбираем $\forall k$ точек)

$$f_j(x) := \prod_{\substack{i=1 \\ i \neq j}}^{k} \frac{x - \alpha_i}{\alpha_j - \alpha_i} \qquad 1 \leq j \leq k$$

$$\underset{\text{восстановленный мн-н}}{p(x)} = \sum_{j=1}^{k} p(\alpha_j) \cdot f_j(x) \text{ - результат интерполяции}$$

Корректность следует из св-в $f_j(x)$: $\begin{cases} f_j(\alpha_l) = 0, & l \neq j \\ f_j(\alpha_j) = 1 \end{cases}$