Код Рида-Соломона

0. Предварительные сведения. Конечные поля.

$\mathbb{F}$ - конечное поле

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

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

3. p - простое
   $m \geq 1$, $g(x) \in \mathbb{F}_p[x]$ - неприв. 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 $< m$.

   $|\mathbb{F}_p[x]/g(x)| = p^m$

4. $\forall$ конечное поле изоморфно такому полю

5. $\forall p, m$ (простое), $\exists$ неприв. 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) т.ч. $\forall x \in \mathbb{F}$ может быть выбран из $\{\gamma^0 = 1, \gamma, .., \gamma^{|\mathbb{F}|-1}\}$

   $\mathbb{F}$ содержит $\varphi(|\mathbb{F}|-1)$ прим. элементов

8. эл-ты $\mathbb{F}_{p^m}$ — p^m-различные корни мн-на $x^{p^m}-x \in \mathbb{F}_p[x]$

9 $\forall k \mid m$ $\mathbb{F}_{p^m}$ содержит единств. подполе р-ра p^k, состоящее из корней мн-на $x^{p^k}-x$

10. Мн-н $x^{p^m}-x = \prod f_i$

$f_i \in \mathbb{F}_p[x]$ — неприводи

$\deg f_i \mid m$

I Код Рида — Соломона (Reed-Solomon Code)

Опр 1 Для целых $1 \le k < n$, $\mathbb{F}$ - поля р-ра $|\mathbb{F}| \ge n$ и мн-ва $S \in \{\alpha_1 .. \alpha_n\} \subseteq \mathbb{F}$, код Рида-Соломона это

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

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. Вычислить зн-ия $p(x)$ в $(\alpha_1 .. \alpha_n)$.

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

$\triangle$.

$$\begin{aligned} & c = (p_m(\alpha_1) \dots p_m(\alpha_n)) \\ + \; & c' = (p_{m'}(\alpha_1) \dots p_{m'}(\alpha_n)) \end{aligned}$$

$$(\underbrace{p_m(\alpha_1)+p_{m'}(\alpha_1)}_{''}, \dots, p_{m+m'}(\alpha_n))$$

$$+\begin{array}{l} m_0 + m_1\alpha_1 + \dots + m_{k-1}\alpha_1^{k-1} \\ m_0' + m_1'\alpha_1 + \dots + m_{k-1}'\alpha_1^{k-1} \end{array} = (m_0+m_0') + (m_1+m_1')\alpha_1 + \dots + (m_{k-1}+m_{k-1}') \cdot \alpha_1^{k-1}$$

$= p_{m+m'}(\alpha_1)$ — значение другого мн-на степени $\leq k-1$ в т. α_1

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

Аналог. скалирование.

Процедура кодирования сообщения m — это вычисление мн-на $p_m(x)$ в точках $\alpha_1 - \alpha_n$ = умн-ие вектора-сообщ. m на матрицу Вандермонда для $\alpha_1 \dots \alpha_n$:

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & & & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$ — образующая матрица кода Рида-Соломона.

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

Теорема 2 (min. расстояние) $d(RS_{\mathbb{F},S}[n,k]) = n-k+1$

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

$\exists (m_0 \dots m_{k-1}) \neq 0 \rightarrow p_m(x) = m_0 + m_1 x + \dots + m_{k-1} x^{k-1} \Rightarrow$

$\Rightarrow p_m(x)$ имеет не более, чем $k-1$ корней в $\mathbb{F}$

$\Rightarrow c = (p(\alpha_1) \dots, p(\alpha_n))$ содержит не более $(k-1)$ нулей

$wt(c) \geq n-k+1.$

Верхняя граница: $wt(c) \leq n-k+1$ может быть получена

- граница Синглтона: $d \leq n-k+1$ (см. лекцию 3)
- $p(x) = \prod_{i=1}^{k-1}(x-\alpha_i) \Rightarrow c = (\underbrace{p(\alpha_1) \dots p(\alpha_{k-1})}_{=0}, p(\alpha_k) \dots p(\alpha_n))$

$wt(c) = n-k+1. \blacktriangleright$

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

II Проверочная матрица кода RS

рассмотрим $\mathbb{F}=\mathbb{F}_q \Rightarrow (\forall \alpha_i = \alpha^i$, где α - примитивный$)$, $q=n+1$,

т.е. $S=\{1,\alpha,\dots,\alpha^{n-1}\}=\mathbb{F}_q^*$

Теорема 3 Для целых $1\le k<n$, $|\mathbb{F}|:=q=n+1$, α - прим. в $\mathbb{F}_q^*$

$S=\{1,\dots\alpha^{n-1}\}$, код Рида-Соломона:

$$RS_{\mathbb{F},S}[n,k]=\{(c_0,\dots,c_n)\in\mathbb{F}^n \mid c(x)=c_0+c_1x+\dots+c_{n-1}x^{n-1}: c(\alpha)=c(\alpha^2)=\dots=c(\alpha^{n-k})=0\}$$

т.е. проверочная матрица имеет вид:

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{bmatrix}\in\mathbb{F}_q^{n-k\times n}$$

$\triangleleft$ Размерность и длина кода, заданного в опр. 1 и т-ме 3 совпадают.

Покажем, что $\forall c\in RS_{\mathbb{F},S}[n,k]$, удовлетворяющие опр-ию 1, удовлетворяют: $Hc=0$.

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

$$\Updownarrow$$

$$H\cdot G^T\cdot m=\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & \vdots & & & \\ 1 & \alpha^{n-k} & \dots & & \alpha^{(n-1)(n-k)} \end{bmatrix}\cdot\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{k-1} \\ 1 & \alpha^2 & \dots & \alpha^{2(k-1)} \\ \vdots & & & \\ 1 & \alpha^{n-1} & \dots & \alpha^{(n-1)(k-1)} \end{bmatrix}\cdot m \quad \alpha_1=1$$

$$= \begin{cases} \alpha^{n} = \alpha^{q-1} = 1 \\ * \ i\text{-строка} \times j\text{-столбец} \\ \begin{bmatrix} 1 & \alpha^{i} & \alpha^{2i} & \dots & \alpha^{i(n-1)} \end{bmatrix} \begin{bmatrix} 1 \\ \alpha^{j} \\ \alpha^{j\cdot 2} \\ \vdots \\ \alpha^{j(n-1)} \end{bmatrix} = \sum_{k=0}^{n-1} \alpha^{k\cdot i + kj} = \text{сумма степ. ряда} \end{cases}$$

$$= \frac{1 - \overbrace{\alpha^{n(i+j)}}^{=1}}{1 - \alpha^{i+j}} = 0 \quad \Big\} = 0 \cdot m = 0.$$

III Декодирование кода RS.

Декодирование удалённых символов (erasure decoding)

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

- осталось t корректных символов, и мы знаем их местоположение.

Задача декодера Рида-Соломона — восстановить сообщение m по парам

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

Так многочлен $p(x)$ имеет степень $k-1 \Rightarrow p(x)$ можно восстановить по $t \geq k$ точкам

Алгоритм Интерполяции Лагранжа

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

$$p_j(x) = \prod_{\substack{i=1\\ i\neq j}}^{k} \frac{x-d_i}{d_j-d_i} \qquad 1\le j\le k$$

восстановленный мн-н →

$$f(x) = \sum_{j=1}^{k} p(d_j)\, p_j(x)$$

— результат интерполяции = исходное сообщение

$$p_j(d_e) = 0 \qquad p_j(d_j) = 1$$

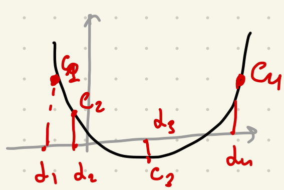
$e \neq j$

Корректность:

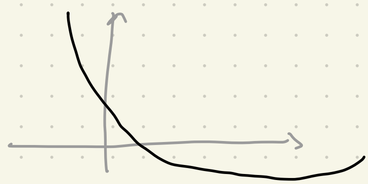
$$f(d_1) = p(d_1)\overset{=1}{p_1(d_1)} + p(d_1)\overset{=0}{p_2(d_1)} + \dots + p(d_k)\underset{=0}{p_k(d_1)} = p(d_1).$$

Интуиция $\quad \mathbb{F}_2,\ k=2$

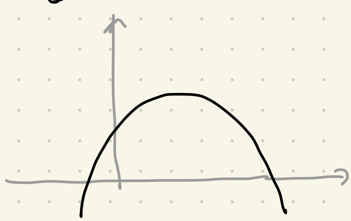
$m = 00$; $n=4 \Rightarrow d=3$



$m = 10$



$m = 01$



$m = 11$