Лекция №12
Код Гоппы

Опр-ие Зафикс. $m \geq 1$, $L = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$, α_i – различны, $g(x) \in \mathbb{F}_{q^m}[x]$, $\deg g(x) = r$, т.ч. $g(\alpha_i) \neq 0$ $\forall i$

Код Гоппы длины n:

$$C = \Gamma(L, g) = \left\{ c \in \mathbb{F}_q^n : \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod g \right\} \quad (1)$$

Замечание • $\Gamma(L, g)$ – линейный (если $c_1, c_2 \in C$, то $c_1 + c_2 \in C$; $c_1 \in C$, то $\lambda c_1 \in C$)

• $(x - \alpha_i)^{-1}$ $\exists$ в $\mathbb{F}_{q^m}[x]/g(x)$, т.к. α_i не являются корнями $g(x)$

В явном виде $(x-\alpha_i)^{-1} = -\dfrac{g(x) - g(\alpha_i)}{x - \alpha_i} g^{-1}(\alpha_i)$

Проверим: $(x - \alpha_i) \cdot \left(-\dfrac{g(x) - g(\alpha_i)}{x - \alpha_i} \right) g^{-1}(\alpha_i) = -g(x) \cdot g^{-1}(\alpha_i) + 1 \equiv$

$\equiv 1 \mod g(x)$

Из (1): $c \in \Gamma(L, g) \iff$ (2) $-\sum_{i=1}^{n} c_i \underbrace{\dfrac{g(x) - g(\alpha_i)}{x - \alpha_i}}_{\text{степень} < \deg g(x)} \cdot g^{-1}(\alpha_i) = 0$ в $\mathbb{F}_{q^m}[x]$

Т.к. сумма мн-ов степени $< \deg g(x)$ есть мн-н степени $< \deg(g(x))$.

Построим проверочную матрицу кода Гоппы

Пусть $g(x) = \sum_{j=0}^{r} g_j x^j$, $g_i \in \mathbb{F}_{q^m}$, $g_r \neq 0$

$$\frac{g(x)-g(d_i)}{x-d_i} = \frac{\sum_{j=0}^{r} g_j (x^j - d_i^j)}{x-d_i} = \frac{g_r(x^r - d_i^r) + g_{r-1}(x^{r-1} - d_i^{r-1}) + \ldots + \overbrace{g_0(1-1)}^{0}}{x-d_i}$$

$$\left\{ x^a - y^a = (x-y)(x^{a-1} + x^{a-2} y + \ldots + x \cdot y^{a-2} + y^{a-1}) \right\}$$

$$= g_r(x^{r-1} + d_i x^{r-2} + \ldots + d_i^{r-1}) + g_{r-1}(x^{r-2} + d_i x^{r-3} + \ldots + d_i^{r-2}) +$$

$$+ \ldots g_2 (x + d_i) + g_1$$

В (2) коэфф-ты при x^{r-1}: $g_r \cdot g^{-1}(d_1) \cdot c_1 + g_r g^{-1}(d_2) c_2 + \ldots + g_r g^{-1}(d_n) c_n$

—— " —— x^{r-2}: $(g_{r-1} + g_r d_1) \cdot g^{-1}(d_1) \cdot c_1 + \ldots +$

$(g_{r-1} + g_r d_n) g^{-1}(d_n) \cdot c_n$

$\vdots$

—— " —— x^0: $(g_1 + g_2 d_1 + \ldots + g_r d_1^{r-1}) \cdot g^{-1}(d_1) c_1 + \ldots +$

$(g_1 + g_2 d_n + \ldots + g_r d_n^{r-1}) g^{-1}(d_n) c_n$

$c \in \Gamma(L, g) \Leftrightarrow$ коэфф-ты при x^j в (2) $= 0$ $\forall j \Leftrightarrow$

$\overline{H} \cdot c = 0$, где

$$\overline{H} = \begin{array}{c|c} & \longleftarrow n \longrightarrow \\ \hline \begin{array}{c}\uparrow\\ r \\ \downarrow\end{array} & \begin{bmatrix} g_r \cdot g^{-1}(d_1) & g_r g^{-1}(d_2) & \dots & g_r g^{-1}(d_n) \\ (g_{r-1}+g_r d_1)g^{-1}(d_1) & & \dots & (g_{r-1} g_r d_n) g^{-1}(d_n) \\ \vdots & & & \vdots \\ (g_1+\dots+g_r d_1^{r-1})\, g^{-1}(d_1) & & \dots & (g_1 + g_r d_n^{r-1})\, g^{-1}(d_n) \end{bmatrix} \end{array}$$

$$= \underbrace{\begin{bmatrix} g_r & 0 & 0 & \dots & 0 \\ g_{r-1} & g_r & 0 & \dots & 0 \\ g_{r-2} & g_{r-1} & g_r & \dots & 0 \\ \vdots & & & & \\ g_1 & g_2 & g_3 & \dots & g_r \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} 1 & \dots & 1 \\ d_1 & \dots & d_n \\ \vdots & & \\ d_1^{r-1} & d_2^{r-1} \dots & d_n^{r-1} \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} g^{-1}(d_1) & 0 & \dots & 0 \\ 0 & g^{-1}(d_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & g^{-1}(d_n) \end{bmatrix}}_{Y}$$

(G: $r \times r$, X: $r \times n$, Y: $n \times n$)

Т.к. G – обратима, часто $\overline{H}$ умножают на G^{-1} слева, получаем

$$\overline{H}' := G^{-1} \cdot \overline{H} = \underbrace{\begin{bmatrix} g^{-1}(d_1) & \dots & g^{-1}(d_n) \\ d_1 g^{-1}(d_1) & \dots & d_n \cdot g^{-1}(d_n) \\ \vdots & & \\ d_1^{r-1} g^{-1}(d_1) & \dots & d_n^{r-1} g^{-1}(d_n) \end{bmatrix}}_{\in \mathbb{F}_{q^m}^{r \times n}}$$

Проверочная матрица с эл-тами из $\mathbb{F}_q$ получается из $\overline{H}'$ заменой каждого эл-та матрицы соответствующим вектором-столбцом длины m над $\mathbb{F}_q$. При такой замене, кол-во строк новой матрицы, назовём её H, есть $r \cdot m$. $\Rightarrow \operatorname{rank}(H) \le r \cdot m$

$\Rightarrow$ р-ть кода $k = n - \mathrm{rank}(H) \geq n - r\cdot m$.

Пример $\quad q=2$, $g(x) = x^2+x+1$

$m=3$

$L = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x+1)$, α - корень x^3+x+1

$L = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$

Построим $\Gamma(L,g)$; $\quad n = |L| = 8$

$k \geq 8 - 2\cdot 3 = 2$

$d \geq 4$

над $\mathbb{F}_{2^3}$

$$H' = \begin{bmatrix} \frac{1}{g(0)} & \frac{1}{g(1)} & \frac{1}{g(\alpha)} & \frac{1}{g(\alpha^2)} & \frac{1}{g(\alpha^3)} & \frac{1}{g(\alpha^4)} & \frac{1}{g(\alpha^5)} & \frac{1}{g(\alpha^6)} \\ \frac{0}{g(0)} & \frac{1}{g(1)} & \frac{\alpha}{g(\alpha)} & \frac{\alpha^2}{g(\alpha^2)} & \frac{\alpha^3}{g(\alpha^3)} & \frac{\alpha^4}{g(\alpha^4)} & \frac{\alpha^5}{g(\alpha^5)} & \frac{\alpha^6}{g(\alpha^6)} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{bmatrix} \Longrightarrow$$

$$\begin{array}{c} 1 \\ \alpha \\ \alpha^2 \\ 1 \\ \alpha \\ \alpha^2 \end{array} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \leftarrow \text{проверочная матрица для } \Gamma(L,g).$$

II Минимальное расстояние $\Gamma(L,g)$

Лемма 1 $d(\Gamma(L,g)) \geq r+1 \quad (\deg g(x) = r)$

$\triangleleft$ $\exists\, \underset{\neq 0}{c} \in \Gamma(L,g),\ wt(c) = w \Rightarrow c_i \neq 0 \quad i \in \{i_1, .. i_w\}$ – индексы ненулевых позиций в c

$$\sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod g(x) \quad \Big| \cdot \prod_{i \in \{i_1,..,i_w\}} (x-\alpha_i)$$

$$\| $$

$$\frac{\sum_{j=1}^{w} c_{i_j} \cdot \prod_{k=1, k\neq j}^{w} (x-\alpha_{i_k})}{\prod_{j=1}^{w} (x-\alpha_{i_j})} =: \frac{f(x)}{h(x)} \equiv 0 \mod g(x)$$

Т.к. α_{i_j} - не корни $g(x)$, то $g(x)$ делит числитель дроби, т.е. $g(x) \mid f(x)$.

$$\deg f(x) \leq w-1 \Rightarrow \deg g(x) \leq \deg(f(x)) \leq w-1$$

$$\Rightarrow r \leq w-1 \Rightarrow w \geq r+1 \quad \blacktriangleright$$

Лемма 2 Для $q=2$ и g - сепарабельный (т.е. в g нет корней кратности >1), $d(\Gamma(L,g)) \geq 2r+1$.

$\triangleleft$ из док-ва леммы 1: $\sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv 0 \mod g(x) \Leftrightarrow g(x) \mid f(x)$,

где $f(x) = \sum_{j=1}^{w} c_{i_j} \prod_{\substack{k=1\\k\neq j}}^{w} (x-\alpha_{i_k}) \overset{q=2}{=\!=} \sum_{j=1}^{w} \prod_{\substack{k=1\\k\neq j}}^{w} (x-\alpha_{i_k})$

$\exists\ h(x) = \prod_{j=1}^{\omega} (x-\alpha_{i_j})$ $\quad h'(x) = \sum_{j=1}^{\omega} \prod_{\substack{k=1 \\ k\neq j}}^{\omega} (x-\alpha_{i_k})$

$\left(\frac{h(x)}{\partial x}\right)$

$\Rightarrow f(x) = h'(x)$; Производная над $\mathbb{F}_2$ имеет только чётные степени (т.к. у всех нечётных степеней стоит чётный коэфф-т).

т.е. $f(x) = f_0 + f_2 x^2 + \ldots + f_{2u} \cdot x^{2u}$, $\quad 2u \leq \omega - 1$

$$= (\underbrace{k_0 + k_2 x + \ldots + k_{2u} \cdot x^u}_{k(x)})^2, \text{ где } k_i^2 = f_i$$

т.е. $g(x)$ делит $(k(x))^2$, $\deg k(x) = u$, $\quad 2u \leq \omega - 1$.

т.к. $g(x)$ - сепарабельный, т.е. не имеет корней кратности 2,

то $g(x) \mid k(x) \Rightarrow \deg g(x) \leq \deg k(x)$

$$r \leq u \quad (\Rightarrow 2u \geqslant 2r)$$

$$\omega - 1 \geqslant 2u \geqslant 2r \Rightarrow$$

$$\Rightarrow \omega \geqslant 2r+1 \quad \blacktriangleright$$

III Декодирование кодов Гоппы

$$y=(y_1 \dots y_n) = (c_1, \dots c_n) + (e_1 \dots e_n), \quad wt(e) = t \le \left\lfloor \frac{d-1}{2} \right\rfloor$$

$\exists B = \{ i \mid e_i \ne 0 \}$ – позиции ошибок, $|B| = t$

$\sigma(x) = \prod_{i \in B} (x - \alpha_i)$ – полином-локатор, $\deg \sigma(x) = t$

$$\omega(x) = \sum_{i \in B} e_i \prod_{\substack{j \in B \\ j \ne i}} (x - \alpha_j) \qquad \deg \omega(x) = t-1$$

$\gcd(\omega(x), \sigma(x)) = 1$ (α_i не является корнем $w(x)$ $\forall i$)

Синдром полученного y – многочлен $S(x) \in \mathbb{F}_{q^m}(x)/g(x)$ вида:

$$S(x) = \sum_{i=1}^{n} \frac{y_i}{x - \alpha_i} = \underbrace{\sum_{i=1}^{n} \frac{c_i}{x - \alpha_i}}_{\equiv 0 \bmod g(x)} + \sum_{i=1}^{n} \frac{e_i}{x - \alpha_i} \equiv \sum_{i \in B} \frac{e_i}{x - \alpha_i} \bmod g(x)$$

Лемма 3 1) $e_k = \dfrac{\omega(\alpha_k)}{\sigma'(\alpha_k)}$ $\forall k \in B$

$\boxed{\text{для } q=2, \text{ считаем } S(x) \bmod g^2(x)}$

2) $\sigma(x) \cdot S(x) \equiv \omega(x) \bmod g(x)$

Замечание: для $q=2$, имеем: $\sigma(x) \cdot S(x) \equiv \omega(x) \bmod g^2(x)$

$\triangleleft$ 1) $\sigma'(x) = \sum_{i \in B} \prod_{\substack{j \in B \\ j \ne i}} (x - \alpha_i)$, $\sigma'(\alpha_k) = \prod_{\substack{j \in B \\ j \ne k}} (\alpha_k - \alpha_j)$

$$\omega(\alpha_k) = \sum_{i \in B} e_i \prod_{\substack{j \in B \\ j \neq i}} (\alpha_k - \alpha_j) = e_k \prod_{\substack{j \in B \\ j \neq k}} (\alpha_k - \alpha_j)$$

$$\Rightarrow \frac{\omega(\alpha_k)}{\sigma'(\alpha_k)} = e_k$$

2) $$\sigma(x) \cdot S(x) = \prod_{i \in B} (x - \alpha_i) \cdot \sum_{i \in B} \frac{e_i}{x - \alpha_i} = \sum_{i \in B} e_i \prod_{\substack{j \in B \\ j \neq i}} (x - \alpha_j)$$

$$= \omega(x)$$

Замечание

$$\underbrace{\sigma(x)}_{\substack{\shortparallel \\ \sigma_0 + \sigma_1 x + \ldots + \sigma_{t-1} x^{t-1} + x^t}} \cdot \overbrace{S(x)}^{\text{известен}} \equiv \overbrace{\omega(x)}^{\substack{\omega_0 + \omega_1 x + \ldots + \omega_{t-1} x^{t-1} \\ \shortparallel}} \mod g(x)$$

$t + t = 2t$ неизвестных

$\deg g = r$ - неизвестных

$$2t \le r \qquad \left\{ \begin{array}{l} d \geq r + 1 \\ t \le \frac{d-1}{2} \le \frac{r}{2} \end{array} \right\}$$

$$t \le \frac{r}{2}$$

Пример

$q=3$

$m=2$

$\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2+2x+2)$, $\alpha^2+2\alpha+2=0$; α - примитивный

$r=2$, $g = x^2+\alpha x+2\alpha$; $\deg g(x)=2 \Rightarrow$ min. расстояние $\geq 3 \Rightarrow$ исправляет ≥ 1 ошибку

$L = \{1, 2, 2\alpha+2, \alpha, 2\alpha, \alpha+1, 2\alpha+1\}$, $|L| = 7 \Rightarrow$ длина кода $= 7$

$$\overline{H} = \begin{bmatrix} 1 & 2\alpha+2 & 1 & \alpha & 2\alpha+1 & \alpha+2 & 2\alpha+2 \\ 1 & \alpha+1 & 2\alpha+2 & \alpha+1 & 1 & \alpha & \alpha \end{bmatrix}$$

$$\downarrow$$

$$n-k \left\{ \begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 0 & 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 1 \end{bmatrix} \right. \in \mathbb{F}_3^{n-k \times n}$$

$K=3$

$y = [0\ 0\ 2\ 2\ 1\ 0\ 1]$

$$\frac{1}{x-1} \equiv 2x+2\alpha+2 \mod g(x)$$

$$\frac{1}{x-2} \equiv (\alpha+1)x+\alpha \mod g(x)$$

$$\frac{1}{x-(2\alpha+2)} \equiv 2x+1 \mod g(x)$$

$$\frac{1}{x-\alpha} \equiv 2\alpha \cdot x+\alpha+1 \mod g(x)$$

$$\frac{1}{x-2\alpha} \equiv (\alpha+2)x \mod g(x)$$

$$\frac{1}{x-(\alpha+1)} \equiv (2\alpha+1)x+2\alpha+2 \mod g(x)$$

$$\frac{1}{x-(2\alpha+1)} \equiv (\alpha+1)x+(\alpha+1) \mod g(x)$$

$$S_y = \sum_{i=0}^{6} \frac{y_i}{x - L[i]} \equiv x+2 \mod g(x)$$

$\deg \sigma(x) = 1 \Rightarrow \sigma(x) = x - \sigma_0$

$\deg \omega(x) = 0 \Rightarrow \omega(x) = \omega_0$

$$(x-\sigma_0)\cdot(x+2) \equiv \omega_0 \mod x^2+\alpha x+2\alpha$$

$$\underbrace{x^2}_{\equiv\, 2\alpha x+\alpha} + (2-\sigma_0)x - 2\sigma_0 \equiv \omega_0 \mod x^2+\alpha x+2\alpha$$

$$(2-\sigma_0+2\alpha)x - 2\sigma_0+\alpha \equiv \omega_0 \mod x^2+\alpha x+2\alpha$$

$$\Rightarrow \begin{cases} 2-\sigma_0+2\alpha = 0 \\ -2\sigma_0+\alpha = \omega_0 \end{cases} \qquad \begin{cases} \sigma_0 = 2\alpha+2 \\ 2\alpha+2+\alpha = \omega_0 \end{cases}$$

$\Rightarrow \omega_0 = 2$

$$e_2 = \frac{\overset{\omega_0}{\overset{\parallel}{\omega_0(\alpha_2)}}}{\underset{\underset{1}{\parallel}}{\sigma'(\alpha_2)}}$$

$\sigma(x) = x - (2\alpha+2) \Rightarrow$ ошибка во второй позиции

$\sigma'(x) = 1$

$e_2 = \frac{2}{1} = 2 \Rightarrow \quad c = y - [0,0,2,0,0,0,0] =$

$= [0,0,0,2,1,0,1].$