

**ПРАКТИКА № 9**  
**03.11.20**

---

## 1 Алгоритм декодирования кода Гоппы

Положим  $y = (y_1, \dots, y_n)$  - полученное искаженное сообщение кода Гоппы. Обозначим за  $B = \{i | e_i = 1\}$  – позиции ошибок в  $y$ ,  $|B| = t \leq \lfloor \frac{d-1}{2} \rfloor$ . Обозначим далее

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

$$\omega(x) = \sum_{i \in B} \prod_{j \in B, j \neq i} (x - \alpha_j), \quad \deg \omega = t - 1.$$

Докажите, что

1.  $e_k = \frac{\omega(\alpha_k)}{\sigma'(\alpha_k)} \forall k \in B$ ,
2.  $\sigma(x)s(x) \equiv \omega(x) \pmod{g(x)}$

Для кода Гоппы, заданного параметрами  $g(x) = x^2 + x + 1$ ,  $q = 2$ ,  $L = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1) = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$ , с помощью алгоритма, описанного ниже, декодируйте  $y = [1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]$ .

### Алгоритм декодирования кода Гоппы

1. Вычислить синдром  $s(x) = \sum_{i=1}^n \frac{y_i}{x - \alpha_i}$
2. Используя сравнение  $\sigma(x)s(x) \equiv \omega(x) \pmod{g(x)}$ , найти многочлены  $\sigma(x), \omega(x)$ .
3. Найти множество  $B = \{i | e_i = 1\}$  по корням  $\sigma(x)$  над  $\mathbb{F}_{q^m}$
4. Вычислить вектор ошибок  $e$ , где  $e_i = \frac{\omega(\alpha_i)}{\sigma'(\alpha_i)}$ .

Можете использовать следующие равенства

$\frac{1}{x - \alpha_1} \equiv x + 1 \pmod{g(x)}$	$\frac{1}{x - \alpha_5} \equiv \alpha^2 x + \alpha + 1 \pmod{g(x)}$
$\frac{1}{x - \alpha_2} \equiv x \pmod{g(x)}$	$\frac{1}{x - \alpha_6} \equiv \alpha x + \alpha^2 + 1 \pmod{g(x)}$
$\frac{1}{x - \alpha_3} \equiv \alpha^2 x + \alpha^2 + \alpha + 1 \pmod{g(x)}$	$\frac{1}{x - \alpha_7} \equiv \alpha x + \alpha^2 + \alpha + 1 \pmod{g(x)}$
$\frac{1}{x - \alpha_4} \equiv (\alpha^2 + \alpha)x + \alpha + 1 \pmod{g(x)}$	$\frac{1}{x - \alpha_8} \equiv (\alpha^2 + \alpha)x + \alpha^2 + 1 \pmod{g(x)}$