Практика № 12
05.12.22

1 Алгоритм декодирования кода Гоппы

Положим $y = (y_1, \ldots, y_n)$ - 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

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

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

Шаманов Юрий	$y = (0, 1, 1, 0, 1, 0, 1, 1)$
Белов Андрей	$y = (1, 1, 0, 0, 0, 0, 0, 1)$
Никита Мжачих	$y = (1, 1, 1, 1, 1, 1, 0, 1)$
Клементий Конрат	$y = (1, 1, 0, 1, 1, 1, 1, 1)$
Попов Никита	$y = (1, 0, 0, 0, 1, 1, 1, 1)$
Толпекин Максим	$y = (1, 0, 1, 0, 0, 1, 1, 1)$
Чубань Артем	$y = (1, 1, 0, 0, 0, 0, 0, 1)$
Микрюков Данила	$y = (1, 0, 0, 1, 1, 1, 0, 1)$
Тронина София	$y = (1, 0, 1, 0, 0, 0, 0, 1)$
Кунинец Артем	$y = (0, 0, 0, 1, 0, 1, 0, 1)$
Сацута Анатолий	$y = (1, 0, 1, 1, 0, 0, 1, 1)$
Плюснина Арина	$y = (1, 0, 1, 0, 1, 0, 0, 0)$
Меркулова Ольга	$y = (1, 0, 0, 1, 1, 1, 0, 1)$
Воронов Александр	$y = (0, 1, 1, 1, 1, 1, 0, 1)$
Кураленко Антон	$y = (1, 1, 0, 1, 1, 1, 1, 0)$
Тарасов Егор	$y = (1, 1, 0, 0, 1, 0, 1, 1)$

Алгоритм декодирования кода Гоппы

1. *Вычислить синдром* $s(x) = \sum_{i=1}^{n} \frac{y_i}{x-\alpha_i} \mod g^2(x)$
2. *Используя сравнение* $\sigma(x)s(x) \equiv \omega(x) \bmod g^2(x)$, *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 по модулю $g^2(x)$

$$\frac{1}{x-\alpha_1} \equiv x^3 + x \qquad \frac{1}{x-\alpha_5} \equiv \alpha^2 x^3 + (\alpha^2+1)x^2 + (\alpha^2+\alpha+1)x + \alpha^2$$

$$\frac{1}{x-\alpha_2} \equiv (\alpha^2+\alpha)x^3 + (\alpha^2+\alpha+1)x^2 + (\alpha+1)x + \alpha^2 + \alpha \qquad \frac{1}{x-\alpha_6} \equiv \alpha^2 x^3 + x^2 + (\alpha+1)x + \alpha$$

$$\frac{1}{x-\alpha_3} \equiv \alpha x^3 + (\alpha+1)x^2 + (\alpha^2+1)x + \alpha \qquad \frac{1}{x-\alpha_7} \equiv \alpha x^3 + x^2 + (\alpha^2+\alpha+1)x + \alpha^2 + \alpha$$

$$\frac{1}{x-\alpha_4} \equiv (\alpha^2+\alpha)x^3 + x^2 + (\alpha^2+1)x + \alpha^2 \qquad \frac{1}{x-\alpha_8} \equiv x^3 + x^2$$