Индивидуальная работа № 4
11.12.23

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

Бакиновский	$y = (1, 1, 0, 1, 0, 1, 1, 0)$
Воробьев	$y = (1, 1, 1, 0, 0, 0, 1, 1)$
Уткин	$y = (0, 1, 1, 1, 0, 1, 1, 1)$
Орлов	$y = (0, 1, 0, 0, 1, 0, 0, 1)$
Флягин	$y = (1, 0, 0, 1, 1, 1, 1, 1)$
Нецветайлов	$y = (1, 1, 1, 0, 0, 1, 1, 0)$
Гервятович	$y = (1, 0, 1, 1, 1, 1, 1, 0)$
Коршунов	$y = (0, 1, 1, 1, 1, 1, 0, 1)$
Кулигин	$y = (0, 1, 1, 0, 1, 1, 1, 1)$
Борзенко	$y = (0, 0, 1, 1, 0, 0, 1, 1)$
Затирахин	$y = (1, 1, 1, 1, 1, 1, 0, 1)$
Винников	$y = (1, 1, 0, 0, 0, 0, 0, 1)$
Попков	$y = (1, 1, 1, 1, 1, 1, 1, 0)$
Куртев	$y = (0, 0, 0, 0, 1, 1, 0, 1)$

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 $g^2(x)$

$$\begin{aligned}
\frac{1}{x} &\equiv x^3 + x \\
\frac{1}{x-1} &\equiv x^3 + x^2 \\
\frac{1}{x-\alpha} &\equiv (\alpha^2+\alpha)x^3 + x^2 + \alpha^2 * x + 1 \\
\frac{1}{x-\alpha^2} &\equiv (\alpha+1)x^3 + x^2 + (\alpha^2+\alpha+1)x + \alpha^2 + \alpha \\
\frac{1}{x-(\alpha+1)} &\equiv (\alpha^2+\alpha)x^3 + (\alpha^2+\alpha+1)x^2 + \alpha x + \alpha^2 + \alpha \\
\frac{1}{x-(\alpha^2+\alpha)} &\equiv (\alpha^2+1)x^3 + x^2 + \alpha^2 x^2 + (\alpha^2+\alpha+1)x + \alpha^2 + 1 \\
\frac{1}{x-(\alpha^2+\alpha+1)} &\equiv (\alpha^2+1)x^3 + x^2 + \alpha x + \alpha + 1 \\
\frac{1}{x-(\alpha^2+1)} &\equiv (\alpha+1)x^3 + \alpha x^2 + \alpha + 1
\end{aligned}$$