Лекция 13

Ilya Yaroshevskiy

24 ноября

Содержание

1 Альтернантные коды

Теорема 1.1. $= (_0, \dots, c_{n-1})$ – кодовое слово кода Рида-Соломона над $GF(q)$ в узком смысле ттогда, когда $c_i = f(\alpha_i), 0 \le i < n$ (т.е. $c = ev(f)$), где $\deg f(x) < k, f(x) \in GF(q)[x]$

Доказательство. Доделать □

Определение. $n, k, n-k+1$ кодом Рида-Соломона называется множество векторов $c = (c_0, \dots, c_{n-1})$, где $c_i = f(a_i), \deg f(x) < k, f(x) \in GF(q)[x], a_i \in GF(q)$ – различные значения (локаторы)

Определение. Обобщенным $(n, k, d = n - k + 1)$ кодом Рида-Соломона $GRS(n, k, a, u)$ называется множество векторов $(c_0u_0, \dots, c_{n-1}u_{n-1})$, где $(c_0, \dots, c_{n-1})$ – кодовое слово $(n, k, n - k + 1)$ кода Рида-Соломона (т.е. $c_i = f(a_i), \deg f(x) < k, a_i$ – различные), и $u_0, \dots, u_{n-1}$ – ненулевые константы

Определение. Альтернантным кодом длины n над полем $GF(q)$ называется код $\mathcal{A}(n, r, a, u)$ с проверочной матрицей

$$H = \begin{pmatrix} a_0^0 & a_1^0 & \dots & a_{n-1}^0 \\ a_0^1 & a_1^1 & \dots & a_{n-1}^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{r-1} & a_1^{r-1} & \dots & a_{n-1}^{r-1} \end{pmatrix} (u_0, u_1, \dots, u_{n-1}) = (H_{i,j})$$

где $a_i \in GF(q^m)$ – различные элементы, $u_i \in GF(q^m) \setminus 0$

Замечание. Доделать

- Минимальное расстояние $d \ge r + 1$
- Размерность $n - r \ge k \ge n - mr$

Теорема 1.2. Пусть $m|(n - h)$. Существует альтернантный $(n, k \ge h, d \ge \delta)$ код над $GF(q)$ такой, что

$$\sum_{i=1}^{\delta-1} (q-1)^i C_n^i < (q^m - 1)^{\frac{n-h}{m}}$$

Замечание.

- Рассмотрим $\mathcal{A}(n, (n - h)/m, a, u) = GRS(n, n - (n - h)/m, a, v) \cap GF(q)^n$

Доделать

Общее количество альтернантных кодом больше чем количество плохих альтернантных кодов, значит есть хорошие альтернантные коды

Замечание.

$$\sum_{i=0}^{d-2} C_{n-1}^i (q-1)^i < \underbrace{\sum_{i=0}^{d-1} C_n^i (q-1)^i < (q^m - 1)^{\frac{n-h}{m}}}_{\text{Альтернантные коды}} < q^{n-h}$$

1.1 Коды Гоппы

Определение. Пусть задан многочлен (многочлен Гоппы) $G(x) \in GF(q^m)[x]$ и $a_0, \ldots, a_{n-1} \in GF(q^m)$, причем $G(a_i) \neq 0$. Кодом Гоппы называется множество $(c_0, \ldots, c_{n-1}) \in GF(q)^n$.

$$\sum_{i=0}^{n-1} \frac{c_i}{x - a_i} \equiv 0 \mod G(x)$$

Утверждение. *Коды Гоппы являются альтернантными*

Доказательство. Доделать □

Замечание. Двоичные коды Гоппы Доделать

1.2 Криптосистема Мак-Элиса

Доделать