

Практика № 6  
22.10.19

---

## 1 Альтернативное доказательство минимального расстояния кода Рида-Соломона

В этом упражнении мы докажем, что  $d(\text{RS}_{\mathbb{F},S}(n, k)) = n - k + 1$ .

1. Покажите, что умножение проверочной матрицы  $H$  любого линейного кода не меняет минимальное расстояние кода
2. Для ненулевых попарно различных  $(x_1, \dots, x_n)$  матрица Вандермонда – квадратная матрица  $n \times n$ , определённая

$$V = \text{Vand}(x_1, \dots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}.$$

Покажите, что  $\det(V) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$ .

Для доказательства можете использовать формулу Лейбница:  $\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(i), i}$ .

3. Проверочная матрица кода Рида-Соломона имеет вид

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ 1 & \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{n-1}^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_1^{n-k} & \alpha_2^{n-k} & \dots & \alpha_{n-1}^{n-k} \end{pmatrix}.$$

Используя тот факт, что минимальное расстояние кода есть наибольшее целое  $d$ , такое что, любые  $(d - 1)$  столбцы  $H$  линейно независимы (см. лекцию №2), докажите справедливость равенства  $d(\text{RS}_{\mathbb{F},S}(n, k)) = n - k + 1$ .

## 2 Пример кода Рида-Соломона

Код Рида-Соломона  $R_{\mathbb{F},S}(n, k)$  размерности  $k = 4$  определён над  $F = GF(3^2) = \mathbb{F}_2[x]/(x^2 + x + 2)$ . Обозначим  $\alpha$  – корень  $f(x) = x^2 + x + 2$  и положим  $S = \{1, \alpha, \alpha^2, \dots, \alpha^7\}$ .

1. Каково минимальное расстояние  $R_{\mathbb{F},S}(n, k)$ ?
2. Закодируйте сообщение  $m = [2, 0, \alpha + 1, 1]$
3. Докажите, что  $c = [2, 1, 2\alpha + 2, 0, \alpha, \alpha + 1, 2\alpha, \alpha + 2]$  принадлежит коду
4. Восстановите исходное сообщение по кодовому слову  $c = [\star, 1, \star, 0, \alpha, \star, 2\alpha, \star]$ , где  $\star$  обозначает, что символ кодового слова был стёрт.