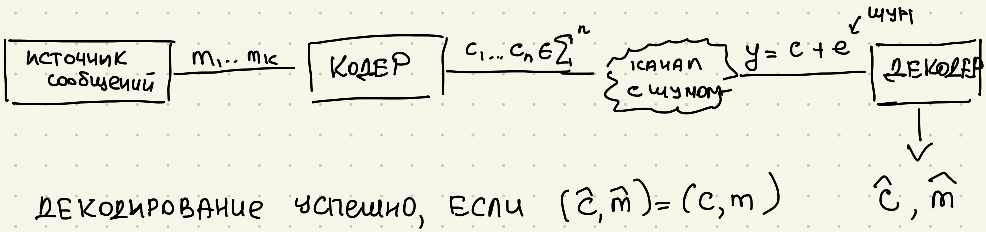
Лекция №1

Линейный код. Основные определения.

① Модель канала с шумом

Σ – конечный алфавит (например, $\Sigma = \mathbb{F}_q$)

$m \in \Sigma^k$ – сообщение



Декодирование успешно, если $(\hat{c}, \hat{m}) = (c, m)$

$m \in \Sigma^k$ – сообщение

$c \in \Sigma^n$ – кодовое слово

② Основные определения

2.1. Для векторов $x, y \in \Sigma^n$ расстояние Хэмминга м/д x и y, $\Delta(x, y)$ – кол-во позиций, в которых x и y различны.

$$\Delta(x, y) = |\{i : x_i \neq y_i\}|$$

относительное расстояние Хэмминга: $\delta(x, y) = \dfrac{\Delta(x, y)}{n}$

Расстояние Хэмминга определяет метрику на Σ^n.

2.2. Вес Хэмминга для $x \in \Sigma^n$ – кол-во ненулевых координат в x,

$$wt(x) = |\{i \mid x_i \neq 0\}|$$

$$wt(x - y) = \Delta(x, y)$$

$$wt(x) = \Delta(x, 0)$$

2.3. Блочный код C, исправляющий ошибки, длины n над конечным алфавитом Σ - это подмножество Σ^n

Элементы C - кодовые слова

Если $\Sigma = \mathbb{F}_q$, то C - q-арный код

$\Sigma = \mathbb{F}_2$, то C - бинарный код

Кодирующее отображение $\mathcal{E}: M \to C$

$m \mapsto c$

2.4. Параметры кода $C \subseteq \Sigma^n$

- скорость кода (code rate) $R(C) = \dfrac{\lg_2 |C|}{n \cdot \lg_2 |\Sigma|}$

- размерность кода (code dimension) $\dim = \dfrac{\lg |C|}{\lg |\Sigma|}$

- минимальное расстояние C - минимальное расстояние Хэмминга м/д двумя неодинаковыми кодовыми словами.

$$d(C) = \min_{\substack{x, y \in C \\ x \neq y}} \Delta(x, y)$$

(т.е. $\forall c_1, c_2 \in C$ отличаются на как min. $d(C)$ позиций)

относительное min. расстояние $\delta(C) = \dfrac{d(C)}{n}$.

ПРИМЕРЫ

1. Код проверки на чётность над $\mathbb{F}_2$ (parity check code)

$$\{0,1\}^k \to \{0,1\}^{k+1}$$

$$m_1 \ldots m_k \mapsto (m_1 \ldots m_k) \| \sum_{i=1}^{k} m_i \mod 2$$

$$R = \frac{\lg_2(2^k)}{n \cdot \lg_2 2} = \frac{k}{k+1}, \quad d = 2$$

2. Код с повторением (repetition code)

$$\{0,1\}^k \longrightarrow \{0,1\}^n \quad \left(\frac{n}{k} \in \mathbb{Z}\right)$$

$$m_1 \ldots m_k \longmapsto \underbrace{(m_1 \ldots m_k) \,\|\, (m_1 \ldots m_k) \ldots \,\|\, (m_1 \ldots m_k)}_{\frac{n}{k} \text{ раз}}$$

$$R = \frac{k}{n}, \quad d = \frac{n}{k}$$

3. Код Хэмминга (1950)

$$\{0,1\}^4 \longmapsto \{0,1\}^7$$

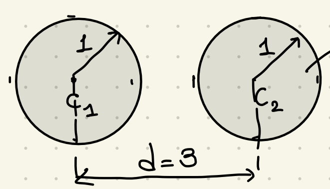
$$m_1 m_2 m_3 m_4 \longmapsto m_1 m_2 m_3 m_4 \,\|\, m_2 \oplus m_3 \oplus m_4 \,\|\, m_1 \oplus m_3 \oplus m_4 \,\|\, m_1 \oplus m_2 \oplus m_4$$

$R = \frac{4}{7}$, $d = 3$ (пока неочевидно).

"Исправление" ошибки = нахождение вектора ошибки $e \Rightarrow$ можем найти кодовое слово c.

Лемма 1 Код с минимальным расстоянием d исправляет $\left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок. Если d - чётное, C исправляет $\frac{d-2}{2}$ ошибок.

Например, если $d = 3$, то код исправляет 1 ошибку.



$$B(c_2, r) = \{x : \Delta(x, c_2) \leq r\}$$

$\forall y \in B(c, 1)$ – кодовое слово c является ближайшим кодовым словом.

③ Линейный код ($\Sigma = \mathbb{F}_q$, q – простое)

3.1. Для $n \geqslant k > 1$, $[n, k]_q$ – линейный код C – подпространство в $\mathbb{F}_q^n$ размерности k.

$\Downarrow$

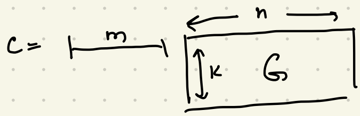
$\exists\, c_1 .. c_k$ – лин. независимы над $\mathbb{F}_q^n$ вектора, образующие базис C.

3.2. $C \subseteq \mathbb{F}_q^n$ – лин. код размерности k

Матрица $G \in \mathbb{F}_q^{k \times n}$ называется порождающей / образующей (generator matrix) матрицей кода C, если строки (!) G образуют базис C

$\Rightarrow$ Эквивалентное опр-е линейного кода:

$$C = \{ c \in \mathbb{F}_q^n : \; c = m \cdot G, \; m \in \mathbb{F}_q^k \}$$



Обозначение. Линейный $[n,k]_q$ код с min. расстоянием d обозначается $[n,k,d]_q$ - код.

Пример. Код Хэмминга $[7,4,3]_2$ – бинарный с порождающей мат-ей

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Так как $\operatorname{rank}(G) = k$, то $\exists$ k столбцов $G_{i_1} .. G_{i_k}$, т.ч. $[G_{i_1} | .. | G_{i_k}] \in \mathbb{F}_q^{k \times k}$ – обратима $\Rightarrow$ $\forall G$ имеет т.н.

систематическую форму

$$G = [\, I_k \mid \underset{\in \mathbb{F}_q^{k \times (n-k)}}{A} \,]$$

3.3. Проверочная матрица (parity-check) $[n,k,d]_q$-кода C – это матрица $H \in \mathbb{F}_q^{(n-k)\times k}$, т.ч. $H\cdot c = 0 \ \forall c \in C$

Эквивалентное опр-ие кода C: $C = \ker(H)$

$\operatorname{rank}(H) = n - \dim \ker H = n - k$

Справедливо: $H \cdot G^T = [\,]$, $G \cdot H^T = [\,]$

$\uparrow$ нулевая матрица

<u>Пример</u> Проверочная матрица кода Хэмминга:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$