Лекция 2

Код - набор. код. слов

Эффект: 1) длинная (n) - больше мин. расст.

2) сложн. кодера и декодера

Линейная ндп $\to G \quad m \cdot G = C$

Порожд. матр множ (n,k)-кода матрица размер $k \times n$, строки - базис. век-ра лин. простр

Код. слова - лин. комб. базисных векторов

$m = (m_1, \dots, m_k) \quad \vec{c} = \vec{m} \cdot G$

$\underbrace{(c_1, \dots c_n)}_{\hat{C}}$

$\vec{h} = (h_1, \dots, h_n) \quad \vec{c} \in \hat{C} \quad (\vec{c}, \vec{h}) = 0$

$c_1 h_1 + c_2 h_2 + \dots + c_n h_n = 0$

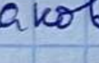
проверка

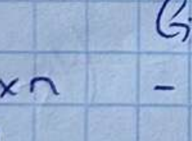
$G \cdot h^T = \underline{0} \quad k \times n \cdot (1 \times n)^T = k \times n \cdot n \times 1 = k \times 1$

Какова размерность лин. простр. проверки

$H \quad G H^T = 0$

$G \quad k \times n$ - k - лин-независ. строк, ранг $= k$

k  n $\Rightarrow$ в матр G $\exists$ k - лин-независ столбцов

G k  n

Индекс ЛН. столбцов = образ. информ. совокуп

остальн. индекс. столбцов образ провероч. совокуп.

$$G \cdot h^T = \begin{array}{c} \overbrace{\qquad\qquad\qquad}^{\text{информ}} \quad \overbrace{\qquad\qquad\qquad}^{\text{провер}} \\ \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1k} & g_{1,k+1} & \dots & g_{1,n} \\ & & \ddots & & & \dots & \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} & g_{k,k+1} & \dots & g_{k,n} \end{pmatrix} \end{array} \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ h_{k+1} \\ \vdots \\ h_n \end{pmatrix} \quad n-k$$

$h_{k+1} \dots h_n$ - задание

$x_1 \dots x_k$

$$\vec{g}_i = \begin{pmatrix} g_{1,i} \\ g_{2,i} \\ \vdots \\ g_{k,i} \end{pmatrix} \qquad \vec{g}_1 \cdot x_1 + \vec{g}_2 \cdot x_2 + \dots + \vec{g}_k \cdot x_k + \vec{g}_{k+1} h_{k+1} + \dots +$$

$$\vec{g}_1 \cdot x_1 + \vec{g}_2 \cdot x_2 + \dots + \vec{g}_k \cdot x_k = -(\vec{g}_{k+1} h_{k+1} + \dots + \vec{g}_n h_n)$$

$$\begin{pmatrix} g_{1,1} & g_{12} & \dots & g_{1,k} \\ & \ddots & & \vdots \\ g_{1,k} & g_{k1} & & g_{k,k} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = -(\vec{g}_{k+1} \cdot h_{k+1} + \dots + \vec{g}_n h_n)$$

$\det \neq 0$ $\quad GF(2)$ $\quad (h_{k+1}, \dots h_n)$

H $\quad r = n-k$ $\quad 2^{n-k}$

$H = (n-k) \times n$ $\quad r = n-k$ - избыточность кода

$G \cdot H^T = \varnothing$ $\quad$ эквивалент.

$$G_{k\times n} = [\, I_{k\times k} \;\; \underset{\longleftarrow r \longrightarrow}{P} \,] = [\, \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \; P \,]$$

$$c = m \cdot G = (\underbrace{m}_{k} \;\; \underbrace{m \cdot P}_{r = n-k}) \qquad H = (P^T \; I_r)$$

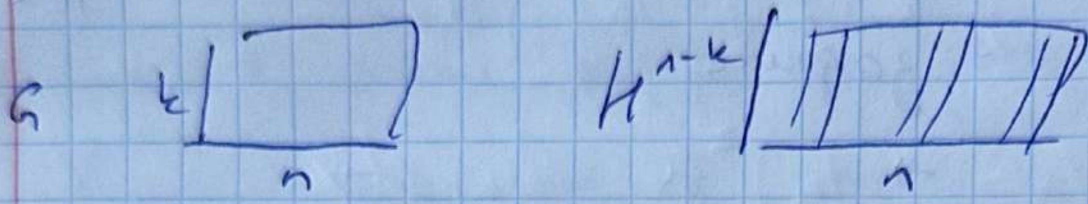
$GF(2)$

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow G_{сист} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} P$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad H_{сист} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$d_{min} = \min\limits_{m \neq 0} w(m \cdot G)$ $\cdot$ $Q^k - 1$ $\quad 2^k - 1$

(n, k) $\quad 2^k - 1$ $\quad R = \frac{k}{n} > \frac{1}{2}$ $\quad n-k$ $\quad k$



$c \cdot H^T = \varnothing$ $\qquad w(c) = 3$

$c = (1 .. 0 .. 1 .. 1 .. 0)$

Теорема: Мин. раст. линейн. (n,k)-кода равно d в том и только том случае, когда $\forall$ $d-1$ столбцы провер. матр. лин. независ. и сущ. напр. из d лин-завис. столбцов с коно в матр. H n изв. столбцов.

Теорема: Граница Синглтона

Мин. раст. лин. (n,k)-кода удовл. нер-ву $d \leq n-k+1$

Дуальный код к данному коду это код, порожд. матр. кот. явл. проверочн. матр данного кода

$G_1 \cdot H_1^T = \varnothing$ $\qquad G_2 = H_1$ $\qquad H_2 = G_1$

$(n, n-1)$-код $\qquad H = (1 .. 1)$

$$G = \begin{pmatrix} I_{n-1\times n-1} & \vdots \end{pmatrix} = \begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix}$$

код. с проверк. на четность может обнаружить все ошибки нечёт. веса

Строим код, кот. исправл. все одинар. ошибки

в $w(e) = 1$

m, $c = m \cdot G$, $c + e$

$$(c+e)\cdot H^T = \underbrace{c\cdot H^T}_{0} + e\cdot H^T = \underset{[0,\ldots 0 \ldots 1 \ldots 0]}{e\cdot H^T}$$

$$e \cdot \begin{bmatrix} \vdots & \vdots & h_j & \vdots & \vdots \end{bmatrix} = h_j \qquad \frac{n-k}{n}$$

$k = 2^n - 1 - n \qquad n = 2^k - 1$

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

Код Хэмминга

Дв. код Хэмминга оптимал в том смысле, что не сущ. кодов (даже нелин) с больш. числом код слов с раст $d = 3$ при такой же длине

$G = H_{Хэм}$ для дуал кодов кодов Хэм.

$d = 2^{n-1}$ Симплекс. код

Код Хэм $\rightarrow$ Дуал код Хэм

расшир код Хэм $\rightarrow$ дуал. расшир Хэм (Рида Маллера 1 пор)

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} = H \qquad (8,4) \quad 2^{n-1} \quad 2^{n-1} - r$$

$(n,k) = (7,4)$ - код Хэм