

Лекция 2

код - это набор кодовых слов

эквивалентные коды.

- длины (n) \rightarrow большое начальн. расстояние
- минимальное расстояние кодера и декодера

линейные коды; В $m \cdot G = C$

порождающая матрица линейного (n, k) к-ва

матрица размера $k \times n$, строки - базисные

вектора ин. пр-ва

кодовые слова - линейные комбинации

базисных векторов

$$\vec{m} = (m_1, \dots, m_n) \quad \vec{C} = \vec{m} \cdot G$$

$$\text{Проверка } \vec{h} = \begin{pmatrix} c_1, \dots, c_n \end{pmatrix}$$

$$= (h_1, \dots, h_n) : (\vec{C}, \vec{h}) = 0$$

$$\forall \vec{c} \in \mathbb{F}$$

$$\text{т.е. } c_1 h_1 + \dots + c_n h_n = 0$$

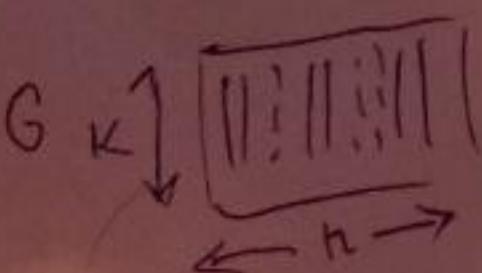
$$G h^T = 0 \quad \cancel{\text{тако}}$$

~~каково~~ какое \Rightarrow базисность линейного пр-ва проверок

$$H \quad \cancel{G \cdot H^T = 0}$$

$G: K^{k \times n} - \Leftrightarrow$ ин. незав. строк

ранг $K(G \times K \Rightarrow B)$ матр $G \models K$ ин. незав. строк.



- замкн. множ

индекси, к-е обрезают инф. совокупность оставшиеся индекси обрезают и просрочены совокупность (-)

$$G \cdot h^T = \underbrace{\begin{pmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,n+1} & \dots & g_{1,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ g_{k,1} & & & & & g_{k,n} \end{pmatrix}}_{\text{матр.}} \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ h_{n+1} \\ \vdots \\ h_n \end{pmatrix}}_{\text{пробл.}} + \text{реш.}$$

h_{n+1}, \dots, h_n - запуск

$$\vec{g}_c = \begin{pmatrix} g_{1,1} \\ g_{2,1} \\ \vdots \\ g_{n,1} \end{pmatrix} \quad \vec{g}_{1,x_1} + \vec{g}_{2,x_2} + \dots + \vec{g}_n \cdot h_n = \phi$$

нормализ.

$$\underbrace{\begin{pmatrix} g_{1,1} & \dots & \dots & g_{1,K} \\ \vdots & \vdots & \vdots & \vdots \\ g_{K,1} & \dots & \dots & g_{K,K} \end{pmatrix}}_{\det \neq 0} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_K \end{pmatrix} = (\vec{g}_{K+1} \cdot h_{K+1} + \dots + \vec{g}_n \cdot h_n)$$

если $\text{rank}(G) = K$ тогда $\vec{p}_1, \dots, \vec{p}_K$ независимы
ибо $\vec{p}_1 - \vec{p}_2, \dots, \vec{p}_K - \vec{p}_1$ независимы

$$r = n - K$$

независимые векторы

$$H \in F_2^{(n-K) \times K}$$

[Элементарные преобразования
(перемены мест) - инициализация
 K окружающие векторы

дано G \rightarrow $G = [I_K | P]$
равенство

$$C = mG = (m | mP)$$

$$\text{up. } H = [P^T | I_{n-K}]$$

пример

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \overline{1} & \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$$

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



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

$$d_{\min} = \omega(n \cdot G) \quad n \neq 0$$

имеет первое значение.

! при $R > \frac{1}{2}$ скорость кода $R = \frac{k}{n}$

то $n-k < k$ и H имеет значение G .
но это мы будем считать членом перед H

$I_h(0)$

минимальное расстояние $d(n, k)$ не равно $d - k + 1$ для $n-k+1$ строк, имеющих одинаковую сумму по модулю 2 .

I_h граничное значение

миним. расст. $d(n, k)$ - ког узлов
неравенство $d \leq n - k + 1$

• Оригинальный код. - код, порождаемый из матрицы которого является произведение матрического генераторного кода.

$$C_1L_1^t = \emptyset \quad G_2 = H_1 \quad H_2 = G_1 \quad \leftarrow \text{данные}$$

Примеры кодов:

1) $(n, n-1) \leftarrow$ код с проверкой на четность
 $H = (1 \times n) \quad H = [1, \dots, 1] \quad \left\{ \begin{array}{l} \text{использует обнаружение} \\ \text{одинички} \\ \text{нечётного бита} \end{array} \right.$

$$G(I_{n-1, n-1}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & \dots & 1 \end{pmatrix}$$

$$d_{\min} = 2$$

2) код который исправляет 1 ошибку одновременно
 $c = mB$ или $c = mB + e$
 $(c+e)H^T = \underbrace{cH^T}_{0} + eH^T = eH^T = h_j$
 \downarrow
 $[0, 0, 1, 2, 0, 0]$
 т.е., наличие ошибки

3) коды Хэмминга.

$$\frac{(n-k=3)}{n=k=3} \quad \text{или} \quad K = 2^n - 1 - n$$

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad n = 2^3 - 1$$

Пр. код Хемминга $n=7$ $k=4$ $d=3$
 смысле это \neq коды с ошибками в трех координатах и с расстоянием 3 при такой же длине

ког Хемк.

$d=3$ (с омнитка)



расширенный ког Хемк.

(может быть и
чтобы его)

НЕ

Одна ког Хэм

головок. $\leftarrow H$

столбце \leftarrow

строка из единиц

$$n \times n \rightarrow (n+1)(n+1)$$

1)

