

Лекция 2

код - это набор кодовых слов

эквивалентный код.

• длинные (n) → большое миним. расстояние

• ~~миним. сложность~~ сложность кодера и декодера

линейные коды; $\mathbf{C} \quad \mathbf{m} \cdot \mathbf{G} = \mathbf{C}$

Порождающая матрица линейного (n, k) кода
матрица размера $k \times n$, строки - базисные
векторы мин. нр-ва

кодовые слова - линейные комбинации
базисных векторов

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

Проверка $\vec{h} = (c_1, \dots, c_n)$

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

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

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

$$\mathbf{G} \mathbf{h}^T = 0$$

~~каков~~ \mathbf{h}^T = какова размерность
линейного нр-ва проверки?

$$\mathbf{h} \quad \mathbf{G} \cdot \mathbf{h}^T = 0$$

$\mathbf{G}: k \times n$ - k мин. независ. строк

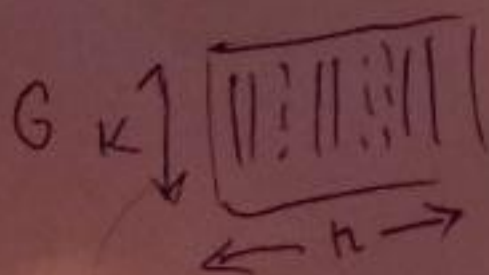
так $k(\mathbf{G}) = k \Rightarrow \mathbf{G}$ матрица $\exists k$ мин. независ. строк.

индексы лн образуют

нр. совокупность

остальные индексы образуют

проверочную совокупность (---)



| - зери. индекс

$$G \cdot h^T = \underbrace{\begin{pmatrix} g_{11} & g_{12} & g_{1k} & g_{1,k+1} & \dots & g_{1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{ki} & & & & & g_{kn} \end{pmatrix}}_{\text{матр.}} \cdot \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_k \\ h_{k+1} \\ \vdots \\ h_n \end{pmatrix}}_{\text{вектор}}$$

h_{k+1}, \dots, h_n — заданы

$$\vec{g}_i = \begin{pmatrix} g_{i1} \\ \vdots \\ g_{ki} \end{pmatrix} \quad \vec{g}_1 x_1 + \vec{g}_2 x_2 + \dots + \vec{g}_k x_k = \vec{0}$$

получаем.

$$\underbrace{\begin{pmatrix} g_{11} & \dots & g_{1k} \\ \vdots & \ddots & \vdots \\ g_{ki} & \dots & g_{kk} \end{pmatrix}}_{\det \neq 0} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \vec{g}_{k+1} h_{k+1} + \dots + \vec{g}_n h_n$$

$\exists \text{ ран}(G) = k$ тогда размерность
матр-цы $k \times k$ ненулевых

$$r = n - k$$

избыточность кода

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

Элементарные преобразования
(метод Гаусса) — приводят
к эквивалентным кодам

удобен вид

$$G = [I_k | P]$$

↑
единичная

тогда

$$C = uG = (u | uP)$$

чр. $H = [P^T | I_{n-k}]$

пример

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

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



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

$$d_{\min} = \min_{m \neq 0} w(m \cdot G)$$

правый перестор слонно

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

то $n - k \leq k$ и H меньше порядка G .
поэтому вычисления удобно делать через H

Th (0)

минимальное расстояние мин. (n, k) кода равно d в т.ч. и т.т.к. $\forall d-1$ столбцов, матрицы мин. кода и \exists набор из d мин. зависимых столбцов.

Th Граница Сэнглтона:

миним. расет. мин. (n, k) -код удовлетворяет неравенству $d \leq n - k + 1$

• Двойственный код - код, координатами которого является проверочная матрица данного кода.
 $C_1 C_1^T = 0$ $G_2 = H_1$ $H_2 = G_1$ ← дуальны

Примеры кодов:

1) $(n, n-1)$ ← код с проверкой на четность
 $H = (1 \times n)$ $H = [1, \dots, 1]$ (поиск обнаружения ошибок нечетного веса)
 $G(I_{n-1}, \begin{smallmatrix} 1 \\ \vdots \\ 1 \end{smallmatrix}) = \begin{pmatrix} 1 & 0 & \vdots \\ \vdots & \ddots & 0 \\ 0 & \vdots & 1 \end{pmatrix}$
 $d_{\min} = 2$

2) код, который исправляет 1 единичную ошибку $d_{\min} = 3$
 $m, c = mG$ $c + e$ (ошибка $w(e) = 1$)
 $(c+e)H^T = \underbrace{cH^T}_0 + eH^T = eH^T = \vec{h}_j$
 $[0, 0, \dots, 1, \dots, 0]$
 \downarrow
 h
 т.е. нашли ошибку

3) коды Хэмминга

$n-k=3$ $n-k$ n

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

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

$$n = 2^m - 1$$

Рв. код Хэмминга код Хэмминга
 смысл, что ~~А~~ кодов оптимальный в том
 кодовых слов с большим числом
 такой же длины с расстоянием $d=3$ при

код Хэмма.

$d=3$ (1 ошибка)

→ Оуал код Хэм



расширенный код Хэмминга.

(помогает в
числовом

добавк. к H

столбце

строки из единиц

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

~~НЕ~~

H

0 H
1 →

1)