• Код — это набор кодовых слов. Мы хотим научиться строить эффективный код: 12.02.26

— длинный (n) → большое мин. раст.

— сложности кодера и декодера.

Линейные коды (с простые) → $G: m \cdot G = C$

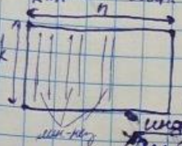
• Порождающая матрица линейного (n, k)-кода — матрица $(k \times n)$, строки — базисные вектора лин. пр-ва.

• Кодовые слова — лин. комб-ии базисных векторов.

$\vec{m} = (m_1, \dots, m_k)$, $\vec{c} = (c_1, \dots, c_n) = \vec{m} \cdot G$; проверка $\vec{h} = (h_1, \dots, h_n)$, $\vec{c} \in C: (\vec{c}, \vec{h}) = 0$; $G \cdot h^T = 0$

• Какова размерность линейного пр-ва проверок? $G \cdot H^T = 0$

$G_{k \times n}$: k — лин-независимых строк, ранг $= k \Rightarrow$ в $G \; \exists k$ — лин-нез. столбцов, т.к. ранги по строкам и столбцам совпадают



Индексы лин-нез. столбцов образуют информационную совокупность, а остальные образ. проверочную совокупность.

$$G \cdot h^T = \left(\underbrace{\begin{matrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} \\ g_{2,1} & g_{2,2} & & g_{2,k} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} \end{matrix}}_{\text{инф. сов-ть}} \; \underbrace{\begin{matrix} g_{1,k+1} & \dots & g_{1,n} \\ g_{2,k+1} & & g_{2,n} \\ \vdots & & \vdots \\ g_{k,k+1} & \dots & g_{k,n} \end{matrix}}_{\text{провер. сов-ть}}\right) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ h_{k+1} \\ \vdots \\ h_n \end{pmatrix} = \vec{g}_1 \cdot x_1 + \vec{g}_2 \cdot x_2 + \dots + \vec{g}_k \cdot x_k + \vec{g}_{k+1} \cdot h_{k+1} + \dots + \vec{g}_n \cdot h_n = 0 \Rightarrow$$

зафикс. знач. на поз. $h_{k+1} \dots h_n$ так, что $G \cdot h^T = 0$; $\exists \; \vec{g}_i^T = (g_{1,i} \; g_{2,i} \dots g_{k,i})$

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

$$\underbrace{\begin{pmatrix} g_{1,1} & \dots & g_{1,k} \\ \vdots & & \\ g_{k,1} & \dots & g_{k,k} \end{pmatrix}}_{\det \neq 0 \text{ (т.к. лин. нез.)}} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}^{\text{← нужно найти}} = -(\vec{g}_{k+1} \cdot h_{k+1} + \dots + \vec{g}_n \cdot h_n)$$

в $GF(2)$ 2^{n-k} способов представить $(h^{k+1} \dots h^n) \Rightarrow H = (n-k) \times n$

$r = n - k$ — избыточность кода. Эквивалент-е хар-ки — получены с помощью элементарных опер. над G

$G_{k \times n} = [I_{k \times k} \; P] = \left[\begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} \; P\right]$ — систематич. вид

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

• **Пример:** $G = \begin{pmatrix} 110100 \\ 011010 \\ 101001 \end{pmatrix}$, систем-й вид: $G_{sys} = \left(\begin{matrix} 100 \\ 010 \\ 001 \end{matrix} \; \underbrace{\boxed{\begin{matrix} 110 \\ 011 \\ 101 \end{matrix}}}_{P}\right)$ (поменяли местами столбцы)

$$H = \begin{pmatrix} 100101 \\ 010110 \\ 001011 \end{pmatrix} \Leftarrow H_{sys} = \begin{pmatrix} 101100 \\ 110010 \\ 011001 \end{pmatrix}$$

$c = m \cdot G$

• Характеристикой кода явл. $d_{min} = \min\limits_{m \neq 0} \omega(m \cdot G)$

Всего ненулевых код. слов $q^k - 1$ ($2^k - 1$ для $q=2$)

При $R = \frac{k}{n} > \frac{1}{2}$: $n-k < k$ ⇒ провер. матр. имеет размер меньше чем порожд.

Для поиска мин. код. расст. вместо перебора в этом случае:

$\exists\, \omega(c) = 3 \Rightarrow c \cdot H^T = 0 \Rightarrow$ столбцы H на „ненул. индексах" — лин. зав.

• Чтобы найти d_{min} достаточно найти мин. набор лин. зав. столбцов H.

• **Th.** Мин. расстояние лин. (n,k)-кода равно d в том и только том случае, когда $\forall\, d-1$ столбец провер. матрицы лин. независ. и существует набор из d лин. завис. столбцов.

• Сколько в H лин. не завис. столбцов? $\to n-k$

• **Th.** (Граница Синглтона). Мин. расстояние лин. (n,k)-кода удовлетв. нер-ву: $d \le \underbrace{n-k}_{r} + 1$

• Дуальный код к данному коду — это код, порожд. матр. которого явл. проверочной матр. данного кода.

$G_1 \cdot H_1^T = 0$; $G_2 = H_1$, $H_2 = G_1$

• **Примеры:** $(n, n-1)$ код: $H = (\overbrace{1 \ldots 1}^{n})$, $G = \left(I_{(n-1)\times(n-1)} \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix}\right) = \begin{pmatrix} 1 & & 0 & 1 \\ & 1 & & 1 \\ 0 & & 1 & 1 \end{pmatrix}$, $d_{min} = 2$

код с проверкой на четность ($\forall$ код. слово имеет чётный вес) — может обнаруж. $\forall$ ошибку нечетного веса

• Строим код, котор. исправляет $\forall$ одиночные ошибки

m, $c = m \cdot G$, $c + e^{\,\omega(e)=1}$, $(c+e) \cdot H^T = \underbrace{c \cdot H^T}_{0} + e \cdot H^T = e \cdot H^T \overset{h_j}{=}$ — получим столбец из H

$e \cdot [\;\; h_j \;\;] = h_j$

$$n-k=3 = r:\quad H = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \qquad \begin{matrix} k = 2^r - r - 1 \\ n = 2^r - 1 \end{matrix} \quad \text{— коды Хэмминга.}$$

$\forall H$ для кодов Хэм. число „1" в $\forall$ ~~столб.~~ строке: 2^{r-1}

• Двоичные коды Хэмминга оптимальны в том смысле, что не существует кодов (даже нелинейных) с большим числом кодовых слов с расстоянием $d=3$ при такой же длине.

$G = H_{хэм}$ Для дуальных кодов кодам Хэм.: $d = 2^{r-1}$ — симплексный код

Код Хэм. $\to$ дуал. код Хэм.
$p(d=3)$
$\downarrow$
расшир. код Хэм. $\to$ код Рида–Маллера (дуал. к расш. к. Х.)

Расш. код Хэм.: добавили к коду Хэм. нулев. столбец слева и единичн. стр. снизу

$$\begin{matrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

$(7,4)$ — к. Х.

$(8,4)$ — р. к. Х.