12/12/26.

Код – это набор кодовых слов

Эффект кода.

– длинные (n) → больше мин. расст.

– сложности кодера и декодера

Линейная кода → G $\quad m.G = C$

Порождающая матрица линейного (n,k)-кода матрица размер $k\times n$, строки – базисные в-ра лин. простр.

Кодовые слова – линейные комбинации базисных ~~код~~ векторов.

$m=(\underbrace{m_1,\dots,m_k}_{k})$ $\qquad \vec{c} = \vec{m}\cdot G$

$\leftarrow (\underbrace{c_1,\dots,c_n}_{n})$

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

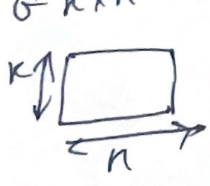
$c_1h_1+c_2h_2+\dots+c_nh_n=0$

проверка. $G\cdot h^T=0$ $\qquad k\times n\ (1\times n)^T = k\times n\cdot n\times 1 = k\times 1$.

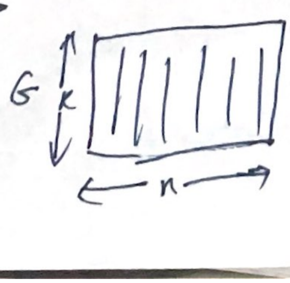
какова размерность линейного пространства проверки.

H $\qquad G\cdot H^T=0$

G $k\times n$ – k – линейно-независимых строк – Ранк $= k$



→ в матр G $\exists\, k$ – линейно независимых столбцов.



k ЛН столбцов = образуют информационную совокупность.

остальные столбцов образуют провер. совокупность.

$$G \cdot h^T = \begin{pmatrix} \overbrace{\begin{matrix} g_{1,1} & g_{1,2} & \cdots & g_{1,k} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,k} \\ \vdots & \vdots & & \\ g_{k,1} & g_{k,2} & & g_{k,k} \end{matrix}}^{\text{информац.}} & \overbrace{\begin{matrix} g_{1,k+1} & \cdots & g_{1,n} \\ g_{2,k+1} & \cdots & g_{2,n} \\ \vdots & & \vdots \\ g_{k,k+1} & \cdots & g_{k,n} \end{matrix}}^{\text{проверк.}} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ h_{k+1} \\ \vdots \\ h_n \end{pmatrix} \quad n-k$$

$h_{k+1}, \ldots, h_n \rightarrow$ зафиксирую.

$x_1, \ldots, x_k$

$$\vec{g_i} = \begin{pmatrix} g_{1,i} \\ g_{2,i} \\ \vdots \\ g_{k,i} \end{pmatrix} \quad \vec{g_1} \cdot x_1 + \vec{g_2} \cdot x_2 + \ldots + \vec{g_k}\, x_k + \vec{g_{k+1}}\, h_{k+1} + \ldots + \vec{g_n} \cdot h_n = 0$$

$$\vec{g_1} \cdot x_1 + \vec{g_2} \cdot x_2 + \ldots + \vec{g_k} x_k = -\left(\vec{g_{k+1}}\, h_{k+1} + \ldots + \vec{g_n} \cdot \vec{h_n}\right)$$

$$g_1 \cdot x_1 + \vec{g_2} \cdot x_2 + \ldots + \vec{g_k} x_k$$

$$\underbrace{\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,k} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,k} \end{pmatrix}}_{\det \neq 0} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = -\left(\vec{g_{k+1}} \cdot h_{k+1} + \ldots + \vec{g_n} h_n\right)$$

$GF(2) \quad (h_{k+1}, \ldots, h_n)$

2^{n-k}.

$H: \; r = n-k \qquad r = n-k$ — избыточность кода.

$H = (n-k) \times n.$ $\quad$ эквивалентные. систематический вид.

$G \cdot H^T = 0$

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

$$c = mG = (\underset{k}{m} \;\; \underset{r = n-k}{m \cdot P})$$

$$G_{sys} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H = (P^T \; I_r)$$

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

$$G_{sys} = \begin{pmatrix} \cancel{1 \; 0 \; 1 \; 1 \; 1 \; 0} \\ \cancel{0 \; 1 \; 1 \; 0 \; 1 \; 0} \\ \cancel{0 \; 1 \; 1 \; 1 \; 0 \; 1} \end{pmatrix}$$

$$H_{sys} = \begin{pmatrix} 1&0&1&1&0&0 \\ 1&1&0&0&1&0 \\ 0&1&1&0&0&1 \end{pmatrix}$$

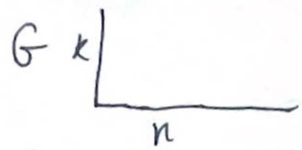
$$\boxed{d_{min} = \min_{m \neq 0} \omega(m \cdot G)}$$

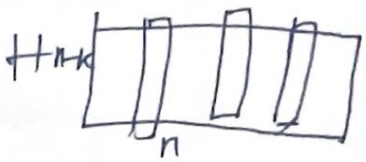
$c = m \cdot G$

$Q^k - 1 \quad 2^k - 1$

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

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





$C \cdot H^T = \phi$ ~~ω(C)~~ $\omega(c) = 3$

$c = (1 \ldots 0 \ldots 1 \ldots 1 \ldots 0)$

столбцы H – линейно зависим

чтобы найти d_{min} → найти минимальный набор из столбцов H.

Теорема: Минимальное расстояние линейного (n,k)-кода равно d в том и только в том случае, когда $\forall d-1$ столбцу провер матрицы линейно независим и существует набор из d линейно-зависимых столбцов

столбцов в матрица H линейно независим столбцов.

Теорема. Граница Синглтона.

минимальное расстояние линейного (n,k)-кода удовлетворяет неравенству $d \leq \underbrace{n-k}_{r} + 1$

дуальный код: к данному коду это код, порождающая матрица

Ко является проверочной матрицей данного кода.

$G_1 \cdot H_1^T = 0 \qquad G_2 = H_1 \qquad H_2 = G.$

Пример кодов.

$(n, n-1)$-код. $\quad H = (1 \ldots 1)$

$$G \left(\begin{array}{c|c} I_{n-1 \times n-1} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array} \right) = \begin{pmatrix} 1 & & 0 & 1 \\ & 1 & & 1 \\ 0 & & 1 & \vdots \\ & & 1 & 1 \end{pmatrix}$$

любое кодовое слово имеет чётное вес

код с проверкой на чётность

может обнаружить 1 ошибка нечетного веса.

Строим код который исправляет ∀ одинарные ошибки.

$m, \; c = m.$ $\quad , \; c + \vec{e} \quad w(e) = 1$

$(c+e) \cdot H^T = \underbrace{c \cdot H^T}_{0} + e \cdot H^T = e \cdot H^T = h_j$

$[0.0 \ldots 1 \ldots 0]$

$e \cdot \begin{bmatrix} \vdots & \vdots & \vdots & \vdots \end{bmatrix} = h_j$

h_j

$n-k$

n

$n - k = 3$ $\quad r$

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \end{array}$$

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

n

$k = 2^k - 1 - r \quad r = 2$

$n = 2^k - 1$

Кода Хэмминга

Код Хэмминга оптимальны в том смысле, что не существует кодов (даже нелинейных) с большим числом кодовых слов с расстоянием $d = 3$ при длине единиц.

$G = H_{Хэм}$ $\quad$ для дуальных кодов кодам Хэм $\quad d = 2^{r-1}$ симплексный код.

$d = 3$

код Хэм $\longrightarrow$ Дуал код Хэм

$\downarrow$

Расш. К Хэм.

$(n, k) = (7, 4)$ – код Хэмминга.

$(8, 4)$ – код Расш. Хэм.

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

2^{n-1} $\quad$ $2^{n-1} - r$

$\shortparallel$

$n - k$.

$\begin{bmatrix} \; \end{bmatrix}$