

Ex 1 $n=3, k=2$ $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ $H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$

Ex 2 $n=5, k=2$ $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

Св-ва линейного кода

1 Свойства матриц G и H :

$$G = (E_k | A_{n-k,k}) \quad \text{можно выделить}$$

канонический вид

$$H = (A_{n-k,k}^T | E_{n-k})$$

Д-во: $x = u \cdot G$ где E^k . Тогда x - код слово.

Но также $x \in E^n$ - код, если $Hx^T = 0$

$$Hx^T = H(uG)^T = H \cdot G^T \cdot u^T = \begin{vmatrix} A & E_{n-k} \\ E_k & A \end{vmatrix} \cdot \begin{matrix} u^T \\ u^T \end{matrix} = \begin{matrix} u^T \\ u^T \end{matrix} = 0 \quad a_1 \oplus a_n = 0$$

2 Кодовое расстояние мин. $[n, k]$ -кода - мин. из весов его канон. код. сио.

Д-во: $d = d(x, x') = |\chi \otimes \chi' \in L| = \text{wt}(\chi \otimes \chi')$

3 Мин. код имеет код. расст-е $d \Leftrightarrow$ любые $d-1$ столбцов H слнз и находятся в столбцах H , ктр. будут слз

Д-во: $Hx^T = 0 \quad H = (H^{(1)} | H^{(2)} | \dots | H^{(n)})$

$Hx^T = H^{(i_1)} \oplus H^{(i_2)} \oplus \dots \oplus H^{(i_d)}$, если i_1, \dots, i_d - все коэффициенты коор-т в x , где стоит '1'

$d - \min \text{вес} \Rightarrow$ не найдём $d-1$ слз столбцов. и d слз всегда найдутся

6.4. Декодирование мин. кода

Пусть по каналу связи было передано код. слово x , а получен на выходе канала связи об. вектор y .

Опред. Синдром вектора: $\text{Syn}(y) = Hy^T$

Заметим, что если $x \oplus e = y$, где e - единичн. вектор ошибок, то:

$$\text{Syn}(y) = Hx^T + He^T = He^T$$

Если $\text{Syn}(y) \neq 0$, то произошли ошибки. Пусть $t = \lfloor \frac{d-1}{2} \rfloor$
Рассматриваем $\text{Syn}(y)$ в сумму мин. числа столбцов H .

Пусть удалось и $\text{Syn}(y) = H^{(i_1)} \oplus \dots \oplus H^{(i_t)}$, где i - минимально

Если $S \leq t$, то ошибки произошли в коор-тах i_1, \dots, i_s

Если $s > t$, то число ошибок больше допустимого и декодируем "как-то", фиксируя, что произошла ошибка декодир-я.

6.5. Оценки ширины кода

Опк Код — координаты в координационном коде
 (n, m, d) $\xrightarrow{\text{ширина}} \text{ширина кода}$ $\xrightarrow{\text{коорд. расст.}}$ расстояние между кодами

Теорема Сингапура

Для кода справедливо: $M \leq 2^k$

Доказательство: Опк-и грани в коорд. коде. Задача: пронумеровать $n-d+1$ коорд. нктр вектора в E^n

Например, $(x_1, \dots, x_{n-d+1}, \dots, x_n)$ — грани радиуса $d-1$

Несложно заметить, что в любом таком граници (т.к. x_1, \dots, x_{n-d+1}) может содержаться не более одного код. слова.

Противоречие с противником, что грани содержат хотя бы 2 код. слова

$$x' = x_1, \dots, x_{n-d+1}, x_{n-d+2}, \dots, x_n \quad \Rightarrow \quad d(x', x'') < d \quad \leftarrow \text{противоречие}$$

$$x'' = x_1, \dots, x_{n-d+1}, x_{n-d+2}, \dots, x_n$$

$\Rightarrow M \leq \text{превосх. числа всех таких граници}$ (так, что все грани с выбором)
 например $1, 2, \dots, n-d+1$ не пересекаются $\Rightarrow M \leq 2^{n-d+1}$

Теорема Хемминга (принцип поиска упаковки)

Для любого (n, d) -кода справедливо $M \leq \sum_{i=0}^{2^n} C_n^i$, где $t = \lfloor \frac{d-1}{2} \rfloor$

Доказательство: $\sum_{i=0}^t C_n^i$ — ширина шара радиуса t в E^n . Шары радиуса t с центрами в код. словах не пересекаются. Для (n, d) -кода

Опк Код совершенный, если он достигает оценку Хемминга

$$\text{Ex } d=3, t=1 \quad \frac{2^n}{n+1} \rightarrow n=2^r-1 \quad n=23, t=3 \quad (d=7) \quad \text{Код Голея}$$

6.6. Код Хэмминга

Опк Код Хэмминга — мин. код, для которого содержатся все возможные различия между двоичными строками, высотой n .

$$H = (H^{(1)}, \dots, H^{(m)})_r \quad n = 2^r - 1 \quad d = 3 \Rightarrow t = 1 \quad [2^r-1, 2^r-r-1, 3]$$

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

$$\text{Ex } H = \begin{pmatrix} 0001111 \\ 0110001 \\ 1010101 \end{pmatrix} \simeq \begin{pmatrix} 0111100 \\ 1011010 \\ 1101001 \end{pmatrix} \simeq \begin{pmatrix} 1001110 \\ 0100111 \\ 1010011 \end{pmatrix} \leftarrow \text{цикл. код}$$

$$2^{2^r-r-1} \leq \frac{2^r}{2^r} = \frac{2^{2^r-1}}{2^r} = 2^{2^r-r-1}$$

Это значит, что совершенный код с точностью до эквивалентности

Задача Васильева построить $> 2^{2^r-1}$ совершенных кодов для $n=3$

$$C = \{f(u, u+v, u+v+\lambda v)\}, \quad u \in E^{\frac{n-1}{2}}, \quad v \in C - \text{сов. код.} \quad \frac{n-1}{2}$$