Лекция №2

Граница Хэмминга. Декодирование по классам смежности.

$[n, k, d]_q$ - лин. код $C \leq \mathbb{F}_q^n$

(n — длина, k — размерность, d — min. расстояние)

C исправляет $\left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок

$G \in \mathbb{F}_q^{k \times n}$ - порождающая матрица $\quad C = \{ c \in \mathbb{F}_q^n : c = uG, u \in \mathbb{F}_q^k \}$

$H \in \mathbb{F}_q^{n-k \times n}$ - проверочная матица $\quad c \in C \Leftrightarrow H \cdot c = 0$

I. Теорема 1 (граница Хэмминга) C - бинарный код длины n размерности k, то

$$|C| \leq \frac{2^n}{\sum\limits_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}} \qquad (1)$$

◁ $d = 3$ (min. расстояние)

Для $c \in C$, определим шар $B(c, \lfloor \frac{d-1}{2} \rfloor = 1) = \{ y \in \{0,1\}^n \mid \Delta(c,y) \leq 1 \}$

$B(c) \cap B(c') = \emptyset$

$$2^n \geq \left| \bigcup_{c \in C} B(c) \right| = \sum_{c \in C} \underbrace{|B(c)|}_{\substack{\shortparallel \\ (n+1) \text{ для } d=3}} = |C| (n+1)$$

В общем случае, $\left| B(c, \lfloor \frac{d-1}{2} \rfloor) \right| = \sum\limits_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} = 1 + \sum\limits_{i=1}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}$

$$2^n \geq |C| \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}$$

Коды, для которых граница (1) выполняется с равенством, называются <u>совершенными</u>.

II Min. расстояние кода через проверочную матрицу

<u>Лемма 2</u> H - проверочная матрица $C \neq \{0\}$.

Мин. расстояние кода C - наибольшее целое d, такое что $\forall$ $(d-1)$ столбцов H - лин. независимы.

$\triangleleft$ $H = \begin{bmatrix} | & & | \\ h_1 & \dots & h_n \\ | & & | \end{bmatrix}$ $c = (c_1 \dots c_n)$, $wt(c) > 0$, $Hc = 0$

$\exists J$ - это мн-во индексов, т.ч. $\forall j \in J$ $c_j \neq 0$, $|J| = wt(c) > 0$

$\Rightarrow \sum\limits_{j \in J} c_j h_j = 0 \Rightarrow$ мы нашли $wt(c)$ лин. зависимых столбцов.

Обратно, пусть $\exists$ t лин. завис. столбцов в $H \Rightarrow$ ненулевая лин. комбинация этих столбцов дают нулевой вектор $\Rightarrow$ коэфф-ты этой лин. комбинации есть кодовое слово ($H \cdot c = 0 \Rightarrow c \in C$)

Т.к. d - это наименьшее возможное значение для t, то $\nexists$ лин. комбинации, состоящей из $(d-1)$ столбцов H, дающей 0, т.к. $\nexists$ кодового слова веса $d-1$.

Хотя как минимум одно кодовое слово веса d существует. $\blacktriangleright$

<u>Примеры</u>

1. Код проверки на чётность $[n, n-1, 2]$ $H = 1\overset{n}{[\,1\ 1 \dots 1\,]}$

2. Код с повторением $[n, 1, n]$ $H = \left[\begin{array}{c|c} I_{n-1} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array} \right] \in \mathbb{F}_2^{n-1 \times n}$

3. Код Хэмминга $[7, 4, 3]_2$ $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{3 \times 7}$

$d = 3$

III Декодирование лин. кодов

Опр-ие Для C - лин. кода длины n над $\mathbb{F}_q$ и $v \in \mathbb{F}_q^n$, класс смежности

C, определённый v - это мн-во, состоящее из сдвигов C на v.

$$C+v = \{c+v : \forall c \in C\}$$

Пример: $C = \{000, 010, 101, 111\}$ $\quad C+000 = C$

$C+001 = \{001, 011, 100, 110\}$

$C+010 = C$

Теорема 3. $\rceil$ C - лин. код, $[n,k]_q$ - код. Тогда

1. $\forall v \in \mathbb{F}_q^n$: $\exists$ класс смежности C, содержащий v
2. $\forall u \in \mathbb{F}_q^n$: $|C+u| = |C| = q^k$
3. $\forall u, v \in \mathbb{F}_q^n$: $u \in C+v \Rightarrow C+u = C+v$
4. $\forall u, v \in \mathbb{F}_q^n$: либо $C+u = C+v$, либо $(C+u) \cap (C+v) = \emptyset$
5. Существует q^{n-k} различных классов смежности.
6. $\forall u, v \in \mathbb{F}_q^n$: $u - v \in C \Leftrightarrow u, v$ принадлежат одному классу смежности.

$\triangleleft$ 1-5 : см. практику

6. "$\Rightarrow$" $\rceil$ $u - v \in C$, обозначим $c := u - v$. Тогда $u = c + v \in C + v$

Кроме того, $v \in C + v$ (т.к. $0 \in C$) $\Rightarrow u, v$ лежат в $C+v$.

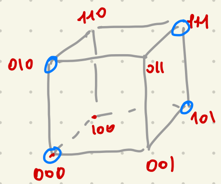
$C = \{0, c_1, c_2 \dots c_M\}$, $C+v = \{v, c_1+v, c_2+v \dots\}$

"$\Leftarrow$" $\rceil$ $\begin{cases} u \in C+x \\ v \in C+x \end{cases} \Rightarrow \begin{cases} u = c+x \\ v = c'+x \end{cases}$ $\quad u - v = c + x - c' - x = c - c' \in C$

$c, c' \in C$

$\blacktriangleright$

Замечание Т-ма 3. показывает, что классы смежности задают разделение пр-ва.



$\cong \mathbb{F}_2^3$

$C = \{000, 101, 010, 111\}$

$C \cup \{C + 110\} = \mathbb{F}_2^3$

Опр-ие Лидер класса смежности – это вектор в классе смежности min. веса Хэмминга.

Алгоритм декодирования по списку классов смежности.

C - лин. код

$y = c + e$ - полученное слово, декодирование = поиск e min. веса

$e = y - c \in C + y$

Задача алг-ма декодирования = поиск лидера в классе смежности $C+y$

Шаг 1 Составить таблицу:

1.1 Первая строка состоит из всех кодовых слов, начиная с нулевого

1.2. Каждая след. строка начинается со слова $e \in \mathbb{F}_q^n$ min. веса Хэмминга, не принадлежащего предыдущим строкам. Строка продолжается элементами вида $c+e$, $c \in C$, в порядке их появления в первой строке

Шаг 2 Для полученного y, найти строку, содержащую $y = c + e$. Тогда e - первый эл-т найденной строки, c - в столбце, содержащим y.

Пример $C = [4, 2, 3]_2$-код с порождающей матрицей

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad y = 0111$$

0000	1011	0101	1110
0001	1010	0100	1111
0010	1001	0111	1100
1000	0011	1101	0110

$$y = 0111 = \underbrace{0101}_{c} + \underbrace{0010}_{e}$$