Лекция № 2

Алгоритмы декодирования лин. кода

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

- n – длина кода
- k – размерность кода
- d – min. расстояние (C исправляет $\lfloor \frac{d-1}{2} \rfloor$ ошибок)
- порождающая матрица $G \in \mathbb{F}_q^{k \times n}$: $C = \{c \in \mathbb{F}_q^n : c = u \cdot G, u \in \mathbb{F}_q^k\}$
- проверочная матрица $H \in \mathbb{F}_q^{n-k \times n}$: $c \in C \Leftrightarrow H \cdot c = 0$

① Мин. расстояние кода через проверочную матрицу

Лемма 1 H – проверочная матрица кода $C \neq \{0\}$.
Мин. расстояние кода C – наиб. целое d, т.ч. $\forall$ $(d-1)$ столбцов H – лин. независимы.

◁

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

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

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

Обратно, $\exists$ t лин. завис. столбцов в H $\Rightarrow$ ненулевая лин. комб. этих столбцов обр. нулевой вектор $\Rightarrow$ коэфф. этой ненулевой лин. комб. есть кодовое слово. Т.к. d – это наим. возможное значение для t, то $\nexists$ кодового слова веса $d-1$, хотя как min. одно кодовое слово веса d существует. ▶

Экв. формулировка $d(C)$ = min. число лин. зависимых столбцов H.

ПРИМЕРЫ

1. Код проверки на чётность $[n, n-1, 2]$; $H = 1[\overbrace{1\ 1 \dots 1}^{n}] \in \mathbb{F}_2^{1 \times n}$
1 лин. независ. столбец

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

(n−1) лин. независ. столбцов

$d = n$

3. Код Хэмминга $[7,4,3]_2$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{3\times 7}$$

$d = 3$

② Декодирование лин. кодов

<u>Опр-ие</u> Для C — лин. кода длины n над $\mathbb{F}_q$ и $u \in \mathbb{F}_q^n$

класс смежности C, определённый u — это мн-во сдвигов C на u:

$$C + u = \{c + u, \ \forall c \in C\}.$$

<u>Пример</u>: $C = \{000, 010, 101, 111\}$; $C + 000 = C$

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

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

<u>**Теорема 2**</u> Пусть C — лин. $[n, k]_q$ - код. Тогда

1. $\forall u \in \mathbb{F}_q^n$: $\exists$ класс смежности C, содержащий u.
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 $(C+u) \cap (C+v) = \varnothing$
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.

◁ 1–5. — см. практику.

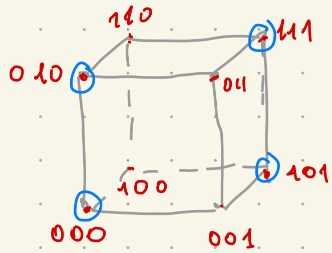
6. $\Rightarrow$ положим, $u - v \in C$, обозначим $c := u - v$. Тогда $u = c + v \in C + v$. Кроме того, $v \in C + v$ (т.к. $0 \in C$) $\Rightarrow u, v$ лежат в $C + v$.

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

$x \in \mathbb{F}_q^n$ $\qquad c, c' \in C$

▶

Замечание Т-ма 2 показывает, что классы смежности задают разделение пространства.



Например, $C \cup (C + \{001\}) = \mathbb{F}_2^3$.

ОПР **Лидер класса смежности** — вектор в классе смежности min. веса Хэмминга.

③ Алгоритм декодирования по списку классов смежности.

C - лин. код
$c \in C$ - код. слово; $y = c + e$ - 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 "стандартное расположение"

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 вектора y найти строку, содержащую $y = c + e$. Тогда вектор ошибок e — первый эл-т найденной строки, c – в столбце, содержащим y

Пример $C = [4, 2, 3]_2$ - лин. код C порожд. матрицей $G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

				$H \cdot e$
0000	1011	0101	1110	$\binom{0}{0}$
0001	1010	0100	1111	$\binom{0}{1}$
0010	1001	0111	1100	$\binom{1}{0}$
1000	0011	1101	0110	$\binom{1}{1}$

$y = 0111$

$y \in C + \{0010\}$

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

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$H \cdot y = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

④ Декодирование по синдрому.

<u>Опр-ие</u> Синдром для $y \in \mathbb{F}_q^n$ – это вектор $s \in \mathbb{F}_q^{n-k}$ т.ч. $s = H \cdot y$. (H – пров. матрица)

Кодовые слова обладают нулевым синдромом.

Кроме того, $\forall y_1, y_2 \in \mathbb{F}_q^n$: $y_1 - y_2 \in C \Leftrightarrow H \cdot y_1 = H y_2$;

y_1, y_2 лежат в одном классе смежности $\Leftrightarrow$ их синдромы совпадают.

Алгоритм декодирования по синдрому

<u>Шаг 1</u> Построить таблицу синдромов для всех лидеров классов смежности $(e, H \cdot e = s_e)$

<u>Шаг 2</u> Посчитать $s = H \cdot y$ для полученного y

<u>Шаг 3</u> Найти e в таблице синдромов, т.ч. $H \cdot e = s$. Соответствующий e – вектор ошибок в y.

<u>Замечание</u>

1. Алгоритм декодирования по синдрому быстрее алгоритма декодирования по списку классов смежности;

2. Таблица синдромов строится

   2.1. $\forall e$ т.ч. $wt(e) \le \left\lfloor \frac{d-1}{2} \right\rfloor$, добавляем $(e, H \cdot e)$ в список синдромов (если $H \cdot e$ ещё не занято)

   2.2. Сортируем список по значениям $H \cdot e$ (для быстрого поиска).

Всевозможных e: $\sum\limits_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i =: M$ – память

$T = O(M \cdot \log M)$. – время.