Лекция №4
Граница Гильберта - Варшамова

Напоминание (см. лекцию 1): • скорость кода $R(C) = \dfrac{\lg|C|}{n \cdot \lg|\Sigma|}$

для лин. кодов $R(C) = \dfrac{k}{n}$

• min. расстояние $d(C) = \min\limits_{\substack{x,y \in C \\ x \neq y}} \Delta(x,y) = \min\limits_{\substack{c \in C \\ c \neq 0}} wt(c)$

$\underset{k\to\infty}{R \to 1}$:) $\underset{k\to\infty}{d \to n}$:)

$\underset{k\to\infty}{R \to 0}$:($\underset{k\to\infty}{d \to \theta(1)}$:(

Существуют ли коды с $R \to 1$ и большим мин. расстоянием (в идеале + эффективный алгоритм декодирования).

Опр-ие Обозначим за $A_q(n,d)$ – максимальная мощность q-арного кода длины n, min. расстояния d;

$$A_q(n,d) := \max_C \{ |C| : \begin{array}{l} C \text{ длины } n, \ d(C) = d \\ C \subseteq \mathbb{F}_q^n \end{array} \}.$$

Код C, достигающий этот максимум, т.е. $|C| = A_q(n,d)$, называется *оптимальным*.

$B^n(c,r) = \{ v \in \mathbb{F}_q^n : \Delta(v,c) \le r \}$ – шар в $\mathbb{F}_q^n$ с центром в c и радиусом r.

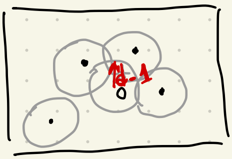
$$Vol_q^n(r) := Volume(B^n(c,r)) = \begin{cases} \sum\limits_{i=0}^{r} \binom{n}{i}(q-1)^i & 0 \le r \le n \\ q^n, & r > n \end{cases}$$

"Жадный" алгоритм построения кода с min. расс-ием $\geq d$ над $\mathbb{F}_q$

0. $C \leftarrow \{0\}$

1. Выбрать случайное слово $c_i \in \mathbb{F}_q^n$ т.ч. $d(C, c_i) \geq d$; добавить c_i в C.

2. Повторять шаг 1, пока возможно.



Допустим "жадный" алгоритм построил код $C \Rightarrow$ $\Rightarrow$ шары $B^n(c, d-1)$ $\forall c$ покрывают q^n (иначе, если $\exists \tilde{c} \notin B^n(c, d-1)$ $\forall c$, то мы бы добавили $\tilde{c}$ в C).

$\Rightarrow$ жадный метод даёт C, т.ч. $|C| \cdot Vol_q^n(d-1) \geq q^n$

Теорема 1 (граница Гильберта-Варшамова) Максимально возможная мощность q-арного кода длины n и min. расстояния d ограничена снизу

$$A_q(n,d) \geq \frac{q^n}{Vol_q^n(d-1)} = \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

Док-но Гильбертом в 1952г, независимо Варшамовым в 1957г.

Следствие №1 $\forall q > 1$, $n, d \in \mathbb{N}_+$, $1 \leq d \leq n$, справедливо

$$\frac{q^n}{Vol_q^n(d-1)} \leq A_q(n,d) \leq \frac{q^n}{Vol_q^n\left(\lfloor \frac{d-1}{2} \rfloor\right)}$$

граница Хэмминга (лек. №2)

Следствие №2 $\exists\, n, k, d \in \mathbb{N}_+$, т.ч. $\mathrm{Vol}_q^{n-1}(d-2) < q^{n-k}$, тогда $\exists$ линейный $[n,k]$-код с min. расстоянием $\geq d$.

$\triangleleft$ Построим проверочную матрицу $H \in \mathbb{F}_q^{n-k \times n}$, в которой $\forall (d-1)$ столбцы лин. независимы. (по Лемме из лекции №2 $\Rightarrow$ min. расстояние $\geq d$).

- начнём с Id_{n-k} (т.е. $\underset{\text{1-ый столбец матрицы } H}{h_1} = e_1,\ h_2 = e_2, \ldots, h_{n-k} = e_{n-k}$)

- на шаге i, добавим новый столбец h_i, т.ч. h_i линейно независим от $\forall\, (d-2)$-лин. комбинаций столбцов $h_1 \ldots h_{i-1}$.

Такой h_i существует. От обратного: $\exists\, h_i$ - лин. зависим от каких-либо $(d-2)$ векторов $h_1 \ldots h_{i-1}$

$\Leftrightarrow \exists\, x \in \mathbb{F}_q^{i-1}$ $wt(x) = d-2$

т.ч. $h_i = \begin{bmatrix} | & & | \\ h_1 & \cdot & h_{i-1} \\ | & & | \end{bmatrix} \cdot x$

\# возможных x'ов: $\mathrm{Vol}_q^{i-1}(d-2)$

\# возможных h_i: q^{n-k}

$\Rightarrow$ для того, чтобы $\exists$ столбец h_i - лин. независим от лин. комбинации $\{h_1 \ldots h_{i-1}\}$ веса $d-2$, необходимо

$$\mathrm{Vol}_q^{i-1}(d-2) < q^{n-k}$$

т.к. $\underbrace{\mathrm{Vol}_q^{i-1}(d-2) < \mathrm{Vol}_q^{i}(d-2)}_{\text{по ф-ле Vol()}} < \underbrace{\mathrm{Vol}_q^{n-1}(d-2) < q^{n-k}}_{\text{по усл-ию следствия}}$, то

н-во $\mathrm{Vol}_q^{i-1}(d-2) < q^{n-k}$ выполняется $\forall i \leq n$ $\blacktriangleright$

Теорема 2

Пусть $q > 1$, $n, k, d \in \mathbb{N}_+$ Определим
q-простое

$$\mathcal{P} := \frac{q^k - 1}{q-1} \cdot \frac{\mathrm{Vol}_q^n(d-1)}{q^n}.$$

Тогда $(1-p)$-доля линейных $[n,k]$ кодов код $\mathbb{F}_q$ обладают min. расстоянием d.

$\triangleleft$ Из практики №1: $\forall\, [n,k]$ кода над $\mathbb{F}_q$ кол-во порождающих матриц одинаково и равно $\prod\limits_{i=0}^{k} (q^k - q^i) \Rightarrow$ достаточно показать, что $(1-p)$ доля матриц $G \in \mathbb{F}_q^{k \times n}$ задаёт $[n,k]$ код с $d(C) = d$.

$$\mathcal{U} = \{ u \in \mathbb{F}_q^k : u_i = 1 \wedge u_j = 0 \ \ \forall j < i \} -$$

вектора с первой ненулевой координатой $= 1$.

$[1 \ x \ x \ldots x]$: таких векторов q^{k-1}
$[0 \ 1 \ x \ldots x]$: — || — q^{k-2}
$[0 \ 0 \ 1 \ldots x]$: — || — q^{k-3}
$\vdots$
$[0 \ldots \ldots 0 \ 1]$ — || — 1

$\Rightarrow |\mathcal{U}| = q^{k-1} + q^{k-2} + \ldots 1 = \dfrac{q^k - 1}{q-1}$

Назовём G "плохой", если $G \in \mathbb{F}_q^{k \times n}$ не является порождающей для $[n,k]$ кода с min. расс-ем $d \Leftrightarrow \exists u \in \mathcal{U} : \underbrace{u \cdot G}_{\text{код. слово}} \in B_q^n(d-1)$

$$\Pr_{G \xleftarrow{\$} \mathbb{F}_q^{k \times n}} [G - \text{"плохая"}] = \Pr_G \Big[\underset{u \in \mathcal{U}}{u \cdot G \in B_q^n(d-1)} \Big] \underset{\substack{\text{Н-во Буля} \\ \text{(union bound)}}}{\leq} \sum_{u \in \mathcal{U}} \Pr[\underbrace{u \cdot G}_{\in \mathbb{F}_q^n} \in B_q^n(d-1)]$$

$$= \sum_{u \in \mathcal{U}} \frac{\mathrm{Vol}_q^n(d-1)}{q^n} = |\mathcal{U}| \cdot \frac{\mathrm{Vol}_q^n(d-1)}{q^n} = \frac{q^k - 1}{q-1} \cdot \frac{\mathrm{Vol}_q^n(d-1)}{q^n}.$$

Т.е. с вероятностью $(1-p)$ случ. матрица $G \in \mathbb{F}_q^{k \times n}$ задаёт $[n,k]$ код с min. расстоянием $\geq d$. $\blacktriangleright$

Вывод: Если $Vol_q^n(d-1) < \frac{q-1}{2} q^{n-k}$ $\Rightarrow$ больше половины всех $[n,k]$ кодов над $\mathbb{F}_q$ обладают min. расстоянием d.

Теорема 3 (граница Синглтона) $\forall q > 1$, $n, d \in \mathbb{N}_+$, т.ч. $1 \le d \le n$, выполняется

$$A_q(n,d) \le q^{n-d+1}$$

для лин. кода: $|C| = q^k$: $k \le n-d+1$

$$d \le n-k+1$$

Опр-ие Лин. $[n,k,d]$ код, т.ч. $k = n-d+1$, называется кодом с максимальным расстоянием.