Лекция №4
Граница Плоткина

В предыдущей лекции $\dfrac{q^n}{Vol_q^n(d-1)} \le A_q(n,d) \le \dfrac{q^n}{Vol_q^n(\lfloor\frac{d-1}{2}\rfloor)}$

$\uparrow$
граница Г.-В.

Г.В. (достаточное условие существования кода): Если $Vol_q^{n-1}(d-2) < q^{n-k}$, то $\exists$ линейный $[n,k]$ код над $\mathbb{F}_q$ с min. расстоянием $\ge d$.

Опр-ие Для фикс. $n, d \in \mathbb{N}_+$, q – степени простого:

$$B_q(n,d) = \max\{q^k \mid \exists \text{ лин. } [n,k] \text{ код с min. расстоянием } d \text{ над } \mathbb{F}_q\}$$

$B_q(n,d)$ уточняет $A_q(n,d)$ для лин. кодов.

Следствие 1 (из Г.В.) Для $n, d \in \mathbb{N}_+$, $2 \le d \le n$ и q - степени простого,

$$B_q(n,d) \ge \frac{q^{n-1}}{Vol_q^{n-1}(d-2)}$$

$\triangleleft$ Положим k – макс. возможным таким, что граница Г.В. выполняется:

$$q^{n-k} > Vol_q^{n-1}(d-2)$$

$$(n-k)\lg q > \lg Vol_q^{n-1}(d-2)$$

$$k < n - \frac{\lg Vol_q^{n-1}(d-2)}{\lg q} = n - \lg_q Vol_q^{n-1}(d-2)$$

$$k = n - \lceil \lg_q Vol_q^{n-1}(d-2) \rceil$$

По следствию из т-мы Г.В. для такого k $\exists$ лин. $[n,k]$ код с min. расстоянием $d' \ge d$. Такой код обладает мощностью q^k.

$$q^k = q^{n - \lceil \log_q \mathrm{Vol}_q^{n-1}(d-2) \rceil} \geq q^{n-1-\log_q \mathrm{Vol}_q^{n-1}(d-2)} =$$

$$= \frac{q^{n-1}}{\mathrm{Vol}_q^{n-1}(d-2)}$$

Обозначение $\quad S^{n-1} \subseteq \mathbb{R}^n = \{x \in \mathbb{R}^n : \underbrace{\|x\|}_{\sqrt{\sum x_i^2}} = 1\}$

Лемма 2 $\quad \exists\, v_1 \dots v_m \in S^{n-1}$

1. Положим, для $\varepsilon > 0$, $\langle v_i, v_j \rangle \geq -\varepsilon \quad \forall\, 1 \leq i,j \leq m$, где $\langle v_i, v_j \rangle = \sum_{k=1}^{n} v_{i,k} \cdot v_{j,k}$.

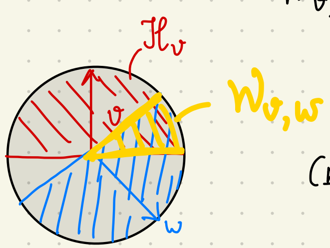
   Тогда $m \leq 1 + \frac{1}{\varepsilon}$

2. Положим $\langle v_i, v_j \rangle \leq 0 \quad \forall\, 1 \leq i,j \leq m$. Тогда $m \leq 2n$.

Δ. 1. См. практику

2. Обозначим $\mathcal{H}_v = \{x \in S^{n-1} \mid \langle v, x \rangle \geq 0\}$ – сферическая крышка (spherical cap)

$\mathcal{W}_{v,w} = \mathcal{H}_v \cap \mathcal{H}_w$ – сферический клин (spherical wedge)



ФАКТ: (без док-ва) $\quad \mathrm{vol}(W_{v,w})$, при условии $\langle v, w \rangle \leq 0$, максимален для $\langle v, w \rangle = 0$

Из факта следует, что максимальный набор векторов v_i достигается при $\langle v_i, v_j \rangle = 0 \quad \forall\, i \neq j$.

Покажем, что на S^{n-1} $\exists$ максимально $2n$ взаимно-ортогональных векторов.

] $v_1 \dots v_n$ — ортонорм. вектора стандартного базиса:

$v_1 = (1, 0 \dots 0)$
$v_2 = (0, 1, \dots 0)$
$\vdots$
$v_n = (0, 0, \dots, 1)$

$v_{n+1} = -v_1, \dots, v_{2n} = -v_n$

Тогда $\forall x \neq 0$, $x \notin \{v_1 \dots v_{2n}\}$ $\exists j$ $1 \leq j \leq 2n$, т.ч. $\langle x, v_j \rangle > 0$.

(т.е. x нельзя добавить в $\{v_1 \dots v_{2n}\}$.

$v_1 \dots v_n$ образуют базис в $\mathbb{R}^n$ $\Rightarrow$ $x = \sum_i \langle x, v_i \rangle v_i$.

Если $\exists i$, т.ч. $\langle x, v_i \rangle < 0$, то $\langle x, -v_i \rangle > 0$

Если $\forall i$ $\langle x, v_i \rangle = 0$ $\Rightarrow$ v_i - лин. зависимые $\lightning$ $(x \neq 0)$

$\blacktriangleright$

ТЕОРЕМА 3 (случай $d \geq \frac{n}{2}$)

] C — бинарный код длины n, min. расстояния d.

1. Если $d > \frac{n}{2}$, то $|C| \leq \frac{2d}{2d-n}$
2. Если $d \geq \frac{n}{2}$, то $|C| \leq 2n$.

$\triangle$] $m := |C|$

$c_1 \dots c_m \in \{0,1\}^n$ - все кодовые слова C

$\Delta(c_i, c_j) \geq d$ $\forall i \neq j$

Отобразим кодовые слова в единичные вектора $v_i \in \mathbb{R}^n$ так, чтобы $\langle v_i, v_j \rangle \leq 0$. А именно,

$$v_i := \frac{1}{\sqrt{n}} \left((-1)^{c_i[1]}, (-1)^{c_i[2]}, \dots, (-1)^{c_i[n]} \right),$$

где $c_i[l]$ — l-ая координата кодового слова c_i.

$$\langle v_i, v_j \rangle = \left\{ (-1)^{c_i[1]} \cdot (-1)^{c_j[1]} = (-1)^{c_i[1]+c_j[1]} = \begin{cases} -1, & c_i[1] \neq c_j[1] \\ 1, & \text{иначе} \end{cases} \right\}$$

$$= \frac{1}{n}\Big[(-1)\,\underbrace{\#\{\ell : c_i[\ell] \neq c_j[\ell]\}}_{\Delta(c_i, c_j)} + 1 \cdot (n - \Delta(c_i, c_j))\Big]$$

$$= \frac{1}{n}\left[-\Delta(c_i, c_j) + n - \Delta(c_i, c_j)\right] = \frac{1}{n}\left[n - \Delta(c_i c_j)\right] \leq \frac{n-2d}{n}$$

Лемма 2 (4.2)

Если $d \geq \frac{n}{2}$, то $\langle v_i, v_j \rangle \leq 0 \Rightarrow$ $m \leq 2n. \Rightarrow |C| \leq 2n.$

Если $d > \frac{n}{2}$, то $\langle v_i, v_j \rangle \leq -\underbrace{\frac{2d-n}{n}}_{\varepsilon} \Rightarrow m \leq 1 + \frac{1}{\varepsilon} = 1 + \frac{n}{2d-n} = \frac{2d}{2d-n}$

▶

ТЕОРЕМА 4 (случай $d < \frac{n}{2}$) $\exists$ C – бинарный код длины n, min. расстояния $d < \frac{n}{2}$. Тогда

$$|C| \leq d \cdot 2^{n-2d+2}.$$

◁ Положим $\ell := n - 2d + 1$

$S = \{1 \ldots \ell\}$, $\overline{S} = \{1..n\} \setminus S = \{\ell+1 .. n\}$

Определим для $\forall a \in \{0,1\}^{\ell}$: $C_a \hookrightarrow C$ – подкод C, спроецированный на $\overline{S}$, состоящий из всех кодовых слов $c \in C$ таких, что $c = a$ на ℓ координатах, т.е.

$$C_a = \{ c|_{\overline{S}} \mid c_i = a_i \ \ 1 \leq i \leq \ell \}$$

Пример: $C = \{0000, 0101, 1010, 1111\}$ $\ell = 1$

$S = \{1\}$, $\overline{S} = \{2, 3, 4\}$

$a = 0$ $C_a = \{000, 101\}$

$a = 1$ $C_a = \{010, 111\}$

C_a – бинарный код длины $n - \ell = 2d - 1$

$d(C) = d \Rightarrow d(C_a) = d$ (т.к. кодовые слова в C, соотв. кодовым словам в C_a могут отличаться только на $n-\ell$ координатах, т.к. C_a образован из C с одинаковыми координатами, которые "удалены" в C_a)

Для C_a справедливо: длина $n(C_a) = 2d-1$, $d(C_a) = d$ $\Rightarrow d(C_a) > \frac{n(C_a)}{2} \Rightarrow$

Теорема 3, п. 1 $\Rightarrow$ $|C_a| \le \frac{2d}{2d-2d+1} = 2d$

$$|C| = |\{a \in \{0,1\}^{\ell}\}| \cdot |C_a| \le 2^{\ell} \cdot 2d = 2^{n-2d+1} \cdot 2d = d \cdot 2^{n-2d+2}$$

▶