Лекция №4
Граница Плоткина

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

граница Г.В.
(покрытие шарами)

Гильберт-Варшамов: Если $Vol_q^{n-1}(d-2) < q^{n-k}$, то $\exists$ $[n,k]$ код над $\mathbb{F}_q$ с min. расс-ем $\geq d$. (достаточное условие $\exists$ кода)

Опр-ие для фикс. $n, d \in \mathbb{N}_+$, q - степени простого:
$$B_q(n,d) = \max\{q^k \mid \exists \text{ лин. } [n,k] \text{ код с min. расс-ем } d \text{ над } \mathbb{F}_q\}.$$

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

Δ Положим k - макс. возможным таким, что граница Г.-В. выполняется:
$$Vol_q^{n-1}(d-2) < q^{n-k}$$
$$(n-k)\lg q > \lg Vol_q^{n-1}(d-2)$$
$$k < n - (\lg Vol_q^{n-1}(d-2)/\lg q)$$
$$k = n - \lceil \lg_q(Vol_q^{n-1}(d-2))\rceil$$

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

По теореме Г.-В., $\exists$ лин. $[n,k,d']$ код с $d' \geq d$. Это код обладает мощностью q^k.

$$q^K = q^{n - \lceil \log_q (Vol_q^{n-1}(d-2)) \rceil} \geq$$

$$\geq q^{n-1-\log_q (Vol_q^{n-1}(d-2))} = \frac{q^{n-1}}{Vol_q^{n-1}(d-2)}$$

Обозначение $S^{n-1} \subseteq \mathbb{R}^n = \{x \in \mathbb{R}^n : \|x\| = 1\}$.

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

1. Положим для $\varepsilon > 0$, $\langle v_i, v_j \rangle \leq -\varepsilon$ $\forall\ 1 \leq i < j \leq m$. ($\langle v_i, v_j \rangle = \sum_{k=1}^{n} v_{ik} \cdot v_{jk}$)

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

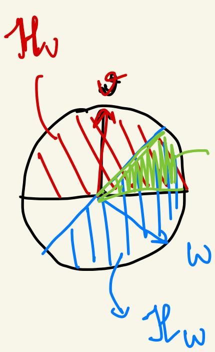
2. Положим $\langle v_i, v_j \rangle \leq 0$ $\forall\ 1 \leq i < j \leq m$. Тогда

   $m \leq 2n$.

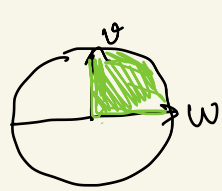
$\triangleleft$ 1. См. практику.

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): $vol(\mathcal{W}_{v,w})$, при условии $\langle v, w \rangle \leq 0$, максимален для $\langle v, w \rangle = 0$.



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

Покажем, что в $S^{n-1} \subseteq \mathbb{R}^n$ $\exists \le 2n$ взаимно-ортогональных векторов.

Пусть $v_1 \dots v_n$ – ортнорм. 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 $\forall x \neq 0 \notin \{v_1 \dots v_{2n}\}$ $\exists j$ $1 \le j \le 2n$, т.ч. $\langle x, v_j \rangle > 0$.

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

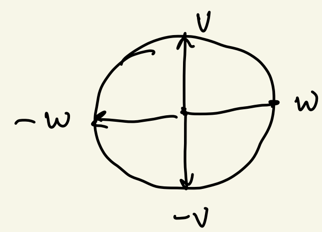
| $v_1 \dots v_n$ образуют базис в $\mathbb{R}^n \Rightarrow x = \sum \langle x_i, v_i \rangle \cdot v_i$

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

Если $\forall i$ $\langle x_i, v_i \rangle = 0 \Rightarrow v_i$ – лин. зависимы ↯

$(x \neq 0)$

Пример: $n = 2$ $\{v, w, -v, -w\}$



Теорема 3 (случай $d \ge \frac{n}{2}$)

Пусть C – бинарный код длины n, min. расстояния d.

1. Если $d > \frac{n}{2}$, то $|C| \le \dfrac{2d}{2d - n}$
2. Если $d \ge \frac{n}{2}$, то $|C| \le 2n$

$\triangleleft$ Пусть $m := |C|$

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

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

Отобразим кодовые слова в единичные вектора $v_i \in \mathbb{R}^n$ так, чтобы $\langle v_i, v_j \rangle < 0$ (т.е. угол м/у v_i и v_j больше, чем $\frac{\pi}{2}$). А именно,

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

$c_i[\ell]$ – ℓ-ый бит кодового слова c_i. Тогда

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

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

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

Если $d \geq \frac{n}{2}$, то $\langle v_i, v_j\rangle \le 0 \overset{\text{Лемма 2.4.2.}}{\Rightarrow} m \le 2n \Rightarrow$ $|C| \le 2n$.

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

$2d > n$ ▶

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

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

◀ Положим $\ell := n - 2d + 1$

$S = \{1, \dots, \ell\}$; $\bar{S} = \{1, \dots, n\} \setminus S = \{\ell+1, \dots, n\}$.

Определим для $\forall a \in \{0,1\}^\ell$: $C_a \hookrightarrow C$ – подкод C, спроецированный на $\bar{S}$, состоящий из всех кодовых слов C, таких что

$c = a$ на ℓ координатах, т.е.
$\in C$

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

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

$a = 0$; $S = \{1\}$, $\overline{S} = \{2, 3, 4\}$

$C_a = \{000, 101\}$

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

$d(C) = d \Rightarrow d(C_a) = d$ (т.к. кодовые слова в C, соответствующие кодовым словам в C_a, отличаются только на $n-\ell$ координатах, и т.к. кодовые слова из C_a образованы из кодовых слов C с одинаковыми координатами ($= a$ на ℓ позициях))

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

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

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

$$= d \cdot 2^{n - 2d + 2}$$

▶