Лекция №3

Граница Гильберта-Варшамова

Из лекции №1: • скорость кода $R(C) = \dfrac{\lg|C|}{n \cdot \lg|\Sigma|}$

для лин. кода р-ти k над $\mathbb{F}_q$: $R(C) = \dfrac{k \cdot \cancel{\lg q}}{n \cdot \cancel{\lg q}} = \dfrac{k}{n}$

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

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

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

Существуют ли коды с "хорошей" скоростью и большим min. расст-ем?

Основная задача теории кодирования: построить "оптимальный" код (т.е. $R \to 1$, d - максимально, + эфф. алг-м. декодировани)

Опр-ие Обозначим за $A_q(n,d)$ – максимальная мощность q-арного кода длины n, min. р-ия d, т.е.

$$A_q(n,d) := \max_{C} \{ |C| \mid C \text{ длины } n,\ d(C) = d \}$$

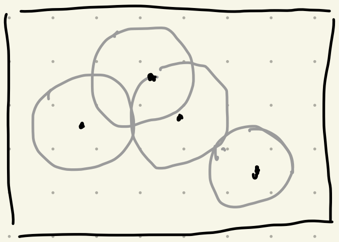
Код C, достигающий этот максимум, т.е. $|C| = A_q(n,d)$ называется **оптимальным**.

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

из лекции №1, $\mathrm{Vol}_q^n(r) := \mathrm{Vol}(B^n(c,r)) = \begin{cases} \sum\limits_{i=0}^{r} \binom{n}{i} (q-1)^i, & 0 \leq r \leq n \\ q^n, & r > n \end{cases}$

"Жадный" метод построения кода с min. расстоянием $\geq d$ над $\mathbb{F}_q$

0. $C \leftarrow \{0\}$
1. Выбрать случайное слово c_i из $\mathbb{F}_q^n$, т.ч. $d(C, c_i) \geq d$,
   добавить c_i в C
2. Повторять шаг 1 пока возможно.



Допустим, "жадный" алг-м построил код $C \Rightarrow$
$\Rightarrow$ шары $B^n(c, d-1)$ $\forall c \in C$ покрывают q^n
(иначе, если $\exists\, w \notin B^n(c, d-1)$ $\forall c \in C$, то мы могли бы w добавить в C).

$\Rightarrow$ жадный метод даёт C, т.ч. $|C| \cdot \mathrm{Vol}_q^n(d-1) \geq q^n$

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

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

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

Следствие 2 $\forall q > 1$, $n, d \in \mathbb{N}_+$, $1 \leq d < n$, справедливо

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

граница Хэмминга (см. лекцию N 1)

Следствие N3 $\exists\, n, k, d \in \mathbb{N}_+$, $q > 1$, т.ч. $\mathrm{Vol}_q^{n-1}(d-2) < q^{n-k}$. Тогда $\exists$ лин. $[n,k]$ код с min. расстоянием $\geq d$.

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

- начнём с Id_{n-k} (т.е. $h_1 = e_1$, $h_2 = e_2$, .. $h_{n-k} = e_{n-k}$, где h_i – i-ый столбец в H)

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

Такой h_i $\exists$-ет. $\neg h_i$ – лин. зависим от каких-либо $(d-2)$ векторов $h_1 \dots h_{i-1}$. $\Leftrightarrow \exists x \in \mathbb{F}_q^{i-1}$, $wt(x) \leq d-2$

т.ч. $h_i = [h_1 .. h_{i-1}] \cdot x$

$\#$ возможных x'в: $Vol_q^{i-1}(d-2)$ $\Rightarrow$

$\#$ возможных h_i : q^{n-k}

$\Rightarrow$ для того, чтобы $\exists$ столбец h_i – лин. независимый от лин. комби из $\{h_1 .. h_{i-1}\}$ веса $d-2$, необходимо, чтобы

$$Vol_q^{i-1}(d-2) < q^{n-k} \quad (*)$$

т.к. $Vol_q^{i-1}(d-2) < Vol_q^{i}(d-2)$ $(\forall i) \Rightarrow (*)$ выполняется $\forall i \leq n$ по условию следствия. ▶

Теорема 4 Пусть $q > 1$, – простое, $n, k, d \in \mathbb{N}_+$. Определим

$$p := \frac{q^k - 1}{q - 1} \cdot \frac{Vol_q^n(d-1)}{q^n}$$

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

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

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

вектора с первой ненулевой координатой, равной 1.

$$\begin{aligned} &[1 \ x \ x \dots x] \sim q^{k-1} \\ &[0 \ 1 \ x \dots x] \sim q^{k-2} \\ &\quad \vdots \\ &[0 \ 0 \dots 1] \sim 1 \end{aligned} \quad \Bigg| \quad \Rightarrow |\mathcal{U}| = q^{k-1} + q^{k-2} + \dots q + 1 = \frac{q^k - 1}{q - 1}$$

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

Полагая, что на мн-ве $\mathbb{F}_q^{k\times n}$ задано случайное равном. распр-ие и что $\forall u : uG$ - случайно равн-но распределено на $\mathbb{F}_q^n$, имеем для какого-то $\mathcal{U}$

$$\Pr_{G \xleftarrow{\$} \mathbb{F}_q^{k\times n}} [G - \text{"плохая" матрица}] = \Pr_{u \xleftarrow{\$} \mathcal{U}} [u \cdot G \in B_q^n(d-1)]$$

$$\underset{\substack{\text{Н-во Буля} \\ \text{(union bound)}}}{\leq} \sum_{u \in \mathcal{U}} \Pr[\underbrace{uG}_{\in \mathbb{F}_q^n} \in B_q^n(d-1)] = |\mathcal{U}| \cdot \frac{\mathrm{Vol}_q^n(d-1)}{q^n} =$$

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

▶

Вывод Если $\mathrm{Vol}_q^n(d-1) < \frac{q-1}{2} \cdot q^{n-k}$ $\Rightarrow$ больше половины всех $[n,k]$ лин. кодов над $\mathbb{F}_q$ обладают min. расст-ем d.

Теорема 5 (граница Синглтона) $\forall q > 1,\ n, d \in \mathbb{N}_+$ т.ч. $1 \le d < n$, выполняется:

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

В частности, для лин. n, k, d кода выполняется: $k \le n-d+1$ $(|C| = q^k)$

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