Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Коды

Пусть $\mathbb{A}_q$ — некоторый алфавит из q символов.

q-ичный код — это произвольное множество

$$C \subseteq \mathbb{A}_q^n$$

n — *длина кода* (длина кодовых слов)

$|C|$ — *мощность кода* (число кодовых слов)

Чаще всего рассматривают двоичные коды, т.е. когда $q = 2$ и $\mathbb{A}_q = \{0,1\}$.

Для произвольного двоичного слова $\boldsymbol{a}$ будем через $\|\boldsymbol{a}\|$ обозначать *вес слова*, т.е. величину

$$\#\{i \mid a_i \neq 0\}$$

Границы Хемминга и Синглтона

Теорема. (Граница Хемминга, граница сферической упаковки)
Для любого $(n, M, d)_q$-кода имеем $M \leq q^n / \left|S_{\lfloor (d-1)/2 \rfloor}(\mathbf{0})\right|$

Теорема. (В некотором смысле, обратная границе Хемминга)
Пусть числа $q, n, M, d \in \mathbb{N}$ таковы, что $M \leq q^n / |S_d(\mathbf{0})|$.
Тогда существует $(n, M, d)_q$-код.

Теорема. (R.C. Singleton)
Для любого $(n, M, d)_q$-кода имеем $M \leq q^{n-d+1}$.

Граница Плоткина

Теорема. (M. Plotkin)

Пусть $nr < d$, где $r \coloneqq 1 - \frac{1}{q}$. Тогда для любого $(n, M, d)_q$-кода

$$M \leq \left\lfloor \frac{d}{d - nr} \right\rfloor$$

Граница Плоткина

Доказательство:

Рассмотрим матрицу, в которой по строкам выписаны все кодовые слова:

$$\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_M \end{pmatrix}$$

Элементы этой матрицы будем обозначать a_{ij}.
Оценим снизу и сверху следующую сумму:

$$T := \sum_{\substack{1 \le k \le n \\ 1 \le i < j \le M}} \mathbb{1}_{a_{ik} \neq a_{jk}}$$

Граница Плоткина

Имеем

$$T = \sum_{1 \le i < j \le M} \sum_{1 \le k \le n} \mathbb{1}_{a_{ik} \neq a_{jk}} = \sum_{1 \le i < j \le M} d(\boldsymbol{a}_i, \boldsymbol{a}_j)$$

Отсюда

$$T \geq \frac{M \cdot (M-1)}{2} \cdot d$$

Граница Плоткина

С другой стороны

$$T = \sum_{1 \le k \le n} \sum_{1 \le i < j \le M} \mathbb{1}_{a_{ik} \neq a_{jk}}$$

Зафиксируем произвольное k.
Пусть среди кодовых слов ровно x_s слов имеют k-ю координату, равную s. Тогда

$$\sum_{1 \le i < j \le M} \mathbb{1}_{a_{ik} \neq a_{jk}} = \sum_{s' \neq s''} x_{s'} \cdot x_{s''}$$

Граница Плоткина

Имеем

$$\sum_{s' \neq s''} x_{s'} \cdot x_{s''} = \frac{1}{2} \cdot \left(\left(\sum_{s} x_s \right)^2 - \sum_{s} x_s^2 \right) = \frac{1}{2} \cdot \left(M^2 - \sum_{s} x_s^2 \right)$$

Минимум выражения $\sum_s x_s^2$ достигается, когда все x_s равны M/q (неравенство Коши—Буняковского).

Отсюда

$$\frac{1}{2} \cdot \left(M^2 - \sum_{s} x_s^2 \right) \leq \frac{1}{2} \cdot \left(M^2 - q \cdot \frac{M^2}{q^2} \right) = \frac{M^2}{2} \left(1 - \frac{1}{q} \right)$$

Граница Плоткина

При любом k мы получаем

$$\sum_{s' \neq s''} x_{s'} \cdot x_{s''} \leq \frac{M^2}{2}\left(1 - \frac{1}{q}\right)$$

Значит

$$T = \sum_{1 \leq k \leq n} \sum_{1 \leq i < j \leq M} \mathbb{1}_{a_{ik} \neq a_{jk}} \leq \frac{nM^2}{2}\left(1 - \frac{1}{q}\right)$$

Граница Плоткина

Сопоставим верхнюю и нижнюю оценки для T:

$$\frac{M \cdot (M-1)}{2} \cdot d \leq T \leq \frac{nM^2}{2}\left(1 - \frac{1}{q}\right)$$

Отсюда

$$(M-1) \cdot d \leq nrM \quad \Leftrightarrow \quad M(d - nr) \leq d$$

Так как $d - nr > 0$ по условию, и $M \in \mathbb{Z}$, то

$$M \leq \left\lfloor \frac{d}{d - rn} \right\rfloor$$

Вложение метрических пространств

Метрическое пространство — это множество с заданной на нём метрикой.

Примеры:

- $\left(\{0,1\}^n, d(\boldsymbol{a}, \boldsymbol{b})\right)$ — *метрическое пространство Хемминга* (здесь d — метрика Хемминга).
- $\left(\mathbb{R}^n, \tilde{d}(\boldsymbol{a}, \boldsymbol{b})\right)$ — евклидово метрическое пространство (здесь $\tilde{d}(\boldsymbol{a}, \boldsymbol{b}) \coloneqq \sqrt{\sum_i (a_i - b_i)^2}$ — обычная евклидова метрика).

Вложение метрических пространств

Вложение метрического пространства U в метрическое пространство V — это отображение $\phi: U \to V$, сохраняющее метрику:

$$\mathrm{dist}_U(x, y) = \mathrm{dist}_V\big(\phi(x), \phi(y)\big)$$

Вложение n-мерного хеммингова пространства в евклидово n-мерное пространство при $n > 1$ сделать не получится, но можно выполнить отображение, сохраняющее определённую информацию о метрике…

Вложение метрических пространств

Сопоставим каждому вектору $\boldsymbol{a} \in \{0,1\}^n$ вектор $\boldsymbol{x^a} \in \mathbb{R}^n$ по правилу:

$$x_i^{\boldsymbol{a}} = \begin{cases} 1, & \text{если } a_i = 1 \\ -1, & \text{если } a_i = 0 \end{cases}$$

При этом:

- $\tilde{d}\left(\boldsymbol{x^a}, \boldsymbol{x^b}\right) = 2 \cdot \sqrt{d(\boldsymbol{a}, \boldsymbol{b})}$
- $\left\langle \boldsymbol{x^a}, \boldsymbol{x^b} \right\rangle = n - 2 \cdot d(\boldsymbol{a}, \boldsymbol{b})$
- $\|\boldsymbol{x^a}\| = \sqrt{n}$ (здесь $\|\cdot\|$ — евклидова норма)

Лемма о векторах в $\mathbb{R}^n$

Лемма (о тупоугольной системе векторов).
Пусть $\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_m \in \mathbb{R}^n$ таковы, что выполнено

- $\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle > 0$ для $i = 1, \dots, m$
- $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle \leq 0$ при $i \neq j$

Тогда $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ линейно независимы и, в частности, $m \leq n$.

Доказательство леммы о векторах

Рассмотрим произвольную нулевую линейную комбинацию:

$$c_1\boldsymbol{x}_1 + \cdots + c_m\boldsymbol{x}_m = \mathbf{0}$$

Положим

$$\mathrm{Pos} \coloneqq \{\, i \mid c_i > 0 \,\}, \quad \mathrm{Neg} \coloneqq \{\, i \mid c_i < 0 \,\}$$

Нам нужно доказать, что $\mathrm{Pos} = \mathrm{Neg} = \emptyset$.

Допустим, что это не так, и придём к противоречию.

Пусть, например, $\mathrm{Pos} \neq \emptyset$ (быть может, при этом $\mathrm{Neg} = \emptyset$).

Доказательство леммы о векторах

$$c_1\boldsymbol{x}_1 + \cdots + c_m\boldsymbol{x}_m = \mathbf{0}$$

Положим

$$\boldsymbol{z} := \sum_{i\in\mathrm{Pos}} c_i\boldsymbol{x}_i = \sum_{j\in\mathrm{Neg}} \left(-c_j\right)\boldsymbol{x}_j$$

Имеем

$$\langle \boldsymbol{z}, \boldsymbol{y}\rangle = \sum_{i\in\mathrm{Pos}} c_i\langle \boldsymbol{x}_i, \boldsymbol{y}\rangle > 0$$

Отсюда следует, что $\boldsymbol{z} \neq \mathbf{0}$.

Доказательство леммы о векторах

$$c_1\boldsymbol{x}_1 + \cdots + c_m\boldsymbol{x}_m = \mathbf{0}$$

Имеем

$$\boldsymbol{z} \coloneqq \sum_{i\in\mathrm{Pos}} c_i\boldsymbol{x}_i = \sum_{j\in\mathrm{Neg}} \left(-c_j\right)\boldsymbol{x}_j \neq \mathbf{0}$$

Рассмотрим теперь соотношения

$$0 < \langle \boldsymbol{z}, \boldsymbol{z}\rangle = \left\langle \sum_{i\in\mathrm{Pos}} c_i\boldsymbol{x}_i\,,\ \sum_{j\in\mathrm{Neg}} \left(-c_j\right)\boldsymbol{x}_j \right\rangle =$$

$$= \sum_{\substack{i\in\mathrm{Pos}\\ j\in\mathrm{Neg}}} c_i\left(-c_j\right)\cdot\left\langle \boldsymbol{x}_i, \boldsymbol{x}_j\right\rangle \leq 0 \qquad \text{— противоречие!}$$

Граница Элайеса—Бассалыго

Теорема. (P. Elias, Л.А. Бассалыго)
Для любого (n, M, d)-кода, где $d \leq n/2$, выполнено неравенство

$$M \leq \frac{n2^n}{\left|S_{\lfloor \tau n - 1 \rfloor}\right|}$$

где $\tau = \frac{1-\sqrt{1-2\delta}}{2}$, $\delta = \frac{d}{n}$.

($S_{\lfloor \tau n - 1 \rfloor}$ — сокращённое обозначение для шара $S_{\lfloor \tau n - 1 \rfloor}(\mathbf{0})$)

Доказательство теоремы Э.—Б.

Пусть C — (n, M, d)-код, и пусть $t \in \mathbb{N}$.

Положим $\deg_t C \coloneqq \max\limits_{\boldsymbol{b} \in \{0,1\}^n} |C \cap S_t(\boldsymbol{b})|$.

Имеем

$$|C| \cdot |S_t| = \sum_{\boldsymbol{a} \in C} \sum_{\boldsymbol{b} \in \{0,1\}^n} \mathbb{1}_{d(\boldsymbol{a},\boldsymbol{b}) \leq t} = \sum_{\boldsymbol{b} \in \{0,1\}^n} \sum_{\boldsymbol{a} \in C} \mathbb{1}_{d(\boldsymbol{a},\boldsymbol{b}) \leq t} \leq 2^n \cdot \deg_t C$$

Отсюда $M \leq \frac{2^n \cdot \deg_t C}{|S_t|}$ для любого $t \in \mathbb{N}$.

Доказательство теоремы Э.—Б.

Пусть C — (n, M, d)-код.

Положим $\delta := \frac{d}{n}$, $\tau := \frac{1-\sqrt{1-2\delta}}{2}$ и $t := \lfloor \tau n - 1 \rfloor$.

Мы обосновали, что

$$M \leq \frac{2^n \cdot \deg_t C}{|S_t|}$$

Осталось доказать, что при выбранном t выполнено неравенство $\deg_t C \leq n$.

Доказательство теоремы Э.—Б.

$\delta := \frac{d}{n}$, $\tau := \frac{1-\sqrt{1-2\delta}}{2}$ и $t := \lfloor \tau n - 1 \rfloor$.

Пусть $\boldsymbol{b} \in \{0,1\}^n$, и $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \in C \cap S_t(\boldsymbol{b})$ ($\boldsymbol{a}_i \neq \boldsymbol{a}_j$ при $i \neq j$).

Нам нужно доказать, что $m \leq n$.

Сопоставим словам $\boldsymbol{b}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ вектора $\boldsymbol{y}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_m \in \mathbb{R}^n$ так (на примере $\boldsymbol{b}$):

$$y_i = \begin{cases} 1/\sqrt{n}, & \text{если } b_i = 1 \\ -1/\sqrt{n}, & \text{если } b_i = 0 \end{cases}$$

Доказательство теоремы Э.—Б.

$\delta \coloneqq \frac{d}{n}$, $\tau \coloneqq \frac{1-\sqrt{1-2\delta}}{2}$ и $t \coloneqq \lfloor \tau n - 1 \rfloor$.

Сопоставим словам $\boldsymbol{b}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ вектора $\boldsymbol{y}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_m \in \mathbb{R}^n$ так (на примере $\boldsymbol{b}$):

$$y_i = \begin{cases} 1/\sqrt{n}, & \text{если } b_i = 1 \\ -1/\sqrt{n}, & \text{если } b_i = 0 \end{cases}$$

При этом

$$\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle = \frac{1}{n}\big(n - 2d(\boldsymbol{a}_i, \boldsymbol{b})\big) \geq \frac{1}{n}(n - 2t) > 1 - 2\tau$$

и

$$\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle = \frac{1}{n}\Big(n - 2d\big(\boldsymbol{a}_i, \boldsymbol{a}_j\big)\Big) \leq \frac{1}{n}(n - 2d) = 1 - 2\delta$$

Доказательство теоремы Э.—Б.

$\delta \coloneqq \frac{d}{n}$, $\tau \coloneqq \frac{1-\sqrt{1-2\delta}}{2}$ и $t \coloneqq \lfloor \tau n - 1 \rfloor$.

Имеем

- $\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle > 1 - 2\tau$ при всех i
- $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle \leq 1 - 2\delta$ при $i \neq j$

Похоже, можно применить *лемму о векторах в* $\mathbb{R}^n$, но для этого придётся «подправить» вектора $\boldsymbol{y}$ и $\boldsymbol{x}_1, \ldots \boldsymbol{x}_m$.

Для этого перейдём к векторам

$$2\tau\boldsymbol{y}, \quad (\boldsymbol{x}_1 - (1-2\tau)\boldsymbol{y}), \quad \ldots, \quad (\boldsymbol{x}_m - (1-2\tau)\boldsymbol{y})$$

Доказательство теоремы Э.—Б.

$\delta := \frac{d}{n}, \ \tau := \frac{1-\sqrt{1-2\delta}}{2}$

- $\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle > 1 - 2\tau$ при всех i
- $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle \leq 1 - 2\delta$ при $i \neq j$

Для векторов

$$2\tau\boldsymbol{y}, \quad (\boldsymbol{x}_1 - (1-2\tau)\boldsymbol{y}), \quad \dots, \quad (\boldsymbol{x}_m - (1-2\tau)\boldsymbol{y})$$

получаем

$$\langle (\boldsymbol{x}_i - (1-2\tau)\boldsymbol{y}), 2\tau\boldsymbol{y} \rangle = 2\tau\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle - 2\tau(1-2\tau)\langle \boldsymbol{y}, \boldsymbol{y} \rangle =$$
$$= 2\tau\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle - 2\tau(1-2\tau) > 0$$

Доказательство теоремы Э.—Б.

$\delta := \frac{d}{n}, \ \tau := \frac{1-\sqrt{1-2\delta}}{2}$

- $\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle > 1 - 2\tau$ при всех i
- $\langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle \leq 1 - 2\delta$ при $i \neq j$

Имеем

$$\langle (\boldsymbol{x}_i - (1-2\tau)\boldsymbol{y}), (\boldsymbol{x}_j - (1-2\tau)\boldsymbol{y}) \rangle =$$
$$= \langle \boldsymbol{x}_i, \boldsymbol{x}_j \rangle + (1-2\tau)^2 \langle \boldsymbol{y}, \boldsymbol{y} \rangle - (1-2\tau)(\langle \boldsymbol{x}_i, \boldsymbol{y} \rangle + \langle \boldsymbol{x}_j, \boldsymbol{y} \rangle) \leq$$
$$\leq 1 - 2\delta + (1-2\tau)^2 - 2(1-2\tau)^2 = -2(2\tau^2 - 2\tau + \delta) = 0$$

Доказательство теоремы Э.—Б.

Для векторов

$$2\tau \boldsymbol{y}, (\boldsymbol{x}_1 - (1-2\tau)\boldsymbol{y}), \dots, (\boldsymbol{x}_m - (1-2\tau)\boldsymbol{y})$$

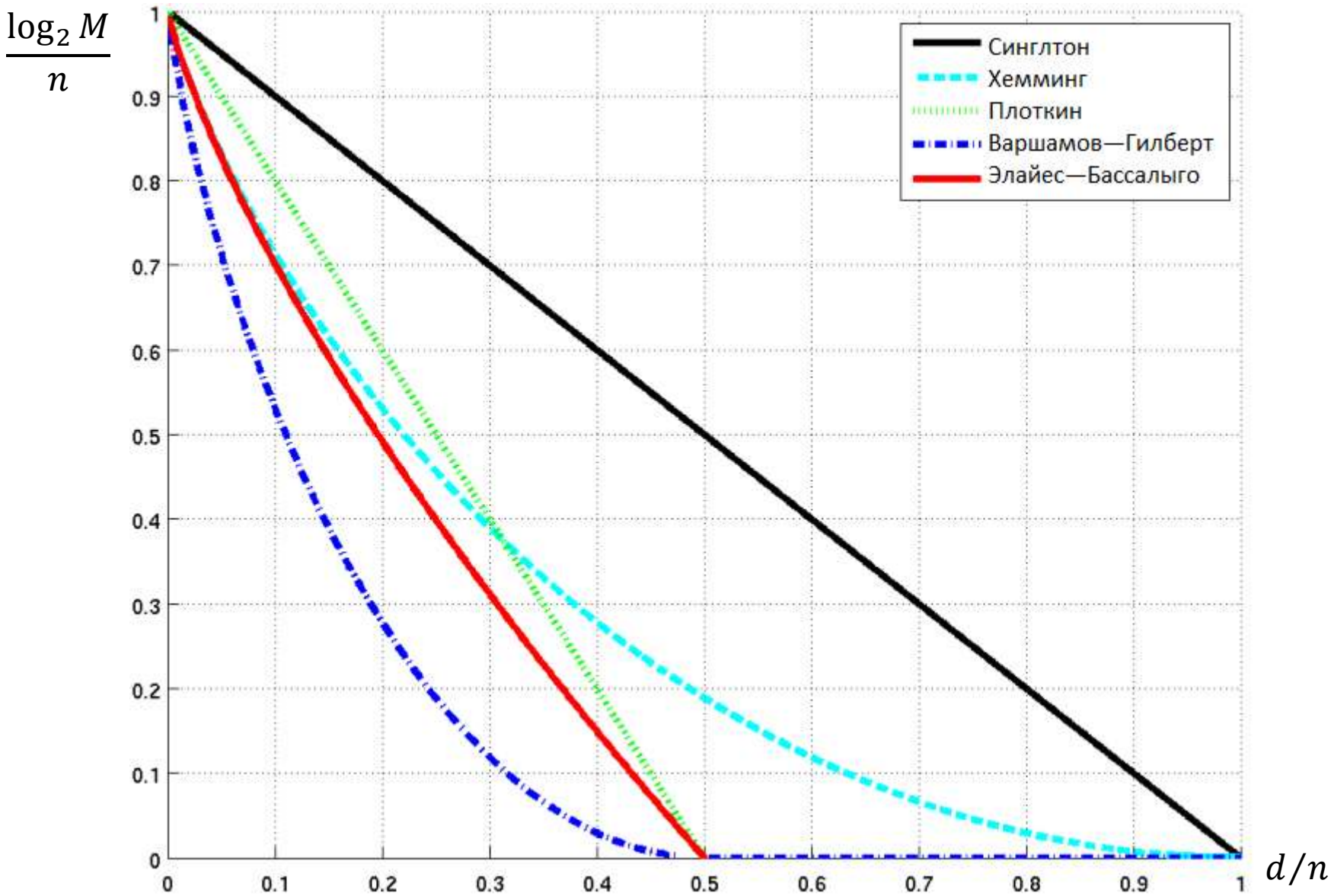
мы доказали соотношения

$$\langle (\boldsymbol{x}_i - (1-2\tau)\boldsymbol{y}), 2\tau \boldsymbol{y} \rangle > 0$$
$$\left\langle (\boldsymbol{x}_i - (1-2\tau)\boldsymbol{y}), \left(\boldsymbol{x}_j - (1-2\tau)\boldsymbol{y}\right) \right\rangle \leq 0$$

и отсюда, по лемме о тупоугольной системе векторов, следует, что $m \leq n$.

Мы доказали, что $\deg_t C \leq n$, и тем самым доказали теорему.

Сравнение границ для (n, M, d)-кодов



Что было и что будет

На лекции мы рассмотрели:

- Граница Плоткина
- Вложение метрических пространств
- Граница Элайеса—Бассалыго

В следующий раз:

- Линейные коды