Лекция 2: Пропускная способность канала. Блочные коды.

Алексей Фролов

al.frolov@skoltech.ru

Сколковский институт науки и технологий (Сколтех)

Современные методы теории информации, оптимизации и управления

Сочи, Россия

2–23 августа, 2020

Skoltech
Skolkovo Institute of Science and Technology

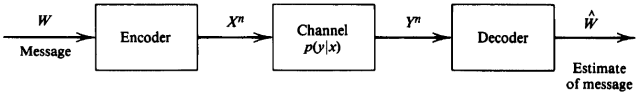
Содержание

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Дискретные каналы без памяти



Определение

Дискретный канал без памяти определяется так:

- $\mathcal{X}$ – *входной алфавит (конечный);*
- $\mathcal{Y}$ – *выходной алфавит (конечный);*
- *матрица переходных вероятностей* $P(y|x)$.

Определение

Канал без памяти, если

$$P(y^n|x^n) = \prod_{i=1}^{n} P(y_i|x_i).$$

Пропускная способность ДКбП

Определение

$$C = \max_{P_X} \{I(X;Y)\},$$

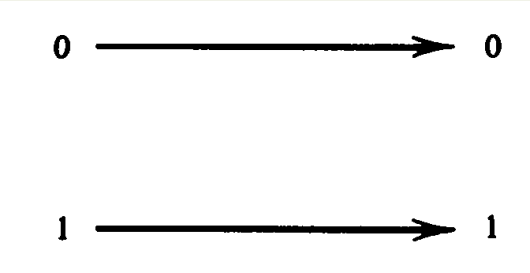
где максимум берется по всем входным распределениям P_X.

Пропускная способность – это наибольшая скорость (в битах за одно использование канала), при которой информация может быть передана со сколь угодно малой вероятностью ошибки.

Skoltech
Skolkovo Institute of Science and Technology

Примеры каналов

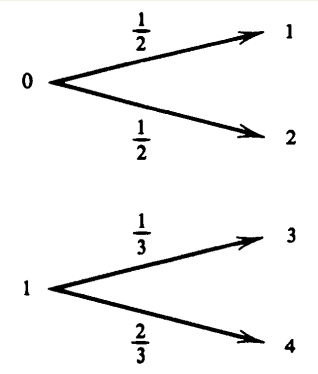
Пример (Бесшумный канал)



Skoltech
Skolkovo Institute of Science and Technology

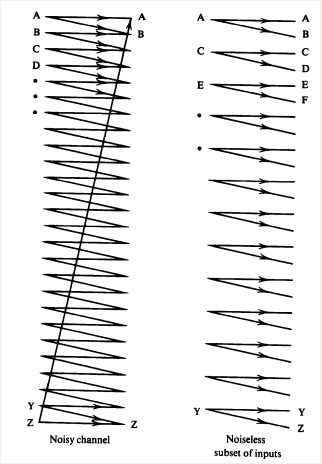
Примеры каналов

Пример (Канал с непересекающимися выходами)



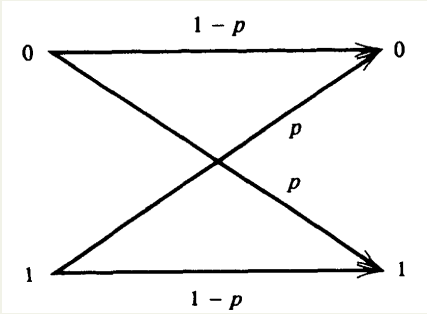
Пример (Шумная печатная машинка)

$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) - 1 \\
&= \log 26 - 1 = \log 13
\end{aligned}
$$



Пример (Двоичный симметричный канал)

$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) - \sum_{x \in \mathcal{X}} P(x) H(Y|X = x) \\
&= H(Y) - \sum_{x \in \mathcal{X}} P(x) h(p) \\
&\leq 1 - h(p).
\end{aligned}
$$



Пример (Двоичный стирающий канал)

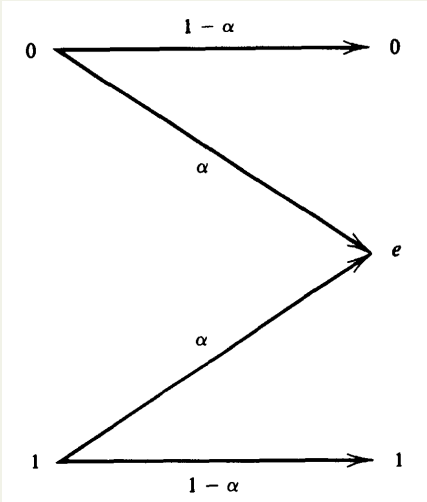
$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) - \sum_{x \in \mathcal{X}} P(x) H(Y|X = x) \\
&= H(Y) - h(\alpha)
\end{aligned}
$$

Пусть E – это индикатор $I_{\{Y=e\}}$ и $\pi = \Pr(X = 1)$.

$$
\begin{aligned}
H(Y) &= H(Y, E) = H(E) + H(Y|E) \\
&= h(\alpha) + (1 - \alpha) h(\pi).
\end{aligned}
$$

Таким образом,

$$
I(X;Y) = (1 - \alpha) h(\pi).
$$



Симметричный канал

Пример

$$P(y|x) = \begin{bmatrix} 0.3 & 0.2 & 0.5 \\ 0.5 & 0.3 & 0.2 \\ 0.2 & 0.5 & 0.3 \end{bmatrix}$$

Skoltech
Skolkovo Institute of Science and Technology

Симметричный канал

Предположим, что все строки в матрице переходных вероятностей являются перестановками друг друга, тогда (через $\mathbf{r}$ обозначим произвольную строку)

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H(Y) - H(\mathbf{r}) \\ &\leq \log|\mathcal{Y}| - H(\mathbf{r}). \end{aligned}$$

Skoltech
Skolkovo Institute of Science and Technology

Симметричный канал

Предположим, что суммы по столбцам одинаковы и равны c, тогда $P(x) = 1/|\mathcal{X}|$ приводит к равномерному распределени/ на Y, т.е.

$$P(y) = \sum_{x \in \mathcal{X}} P(y|x)p(x) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} P(y|x) = \frac{c}{|\mathcal{X}|}.$$

Skoltech
Skolkovo Institute of Science and Technology

Симметричный канал

Определение

Канал называется симметричным, если строки матрицы переходных вероятностей являются перестановками друг друга и столбцы также являются перестановками друг друга.

Канал называется слабо симметричным, если строки матрицы переходных вероятностей являются перестановками друг друга, и суммы по столбцам одинаковы.

Skoltech
Skolkovo Institute of Science and Technology

Симметричный канал

Пример (Слабо симметричный канал)

$$P(y|x) = \begin{bmatrix} 1/3 & 1/6 & 1/2 \\ 1/3 & 1/2 & 1/6 \end{bmatrix}$$

Skoltech
Skolkovo Institute of Science and Technology

Симметричный канал

Теорема

Для слабо симметричного канала,

$$C = \log |\mathcal{Y}| - H(\mathbf{r})$$

достигается на равномерном входном распределении.

Skoltech
Skolkovo Institute of Science and Technology

Свойства пропускной способности

- $C \geq 0$;
- $C \leq \log |\mathcal{X}|$;
- $C \leq \log |\mathcal{Y}|$;
- $I(X;Y)$ непрерывная функция $P(x)$;
- $I(X;Y)$ выпукла по $P(x)$;

Локальный минимум является глобальным и максимум существует и конечен.

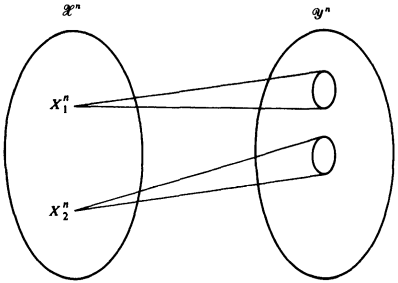
Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Идея

Основная идея: канал имеет подмножество входов, которые производят непересекающиеся последовательности на выходе.



Skoltech
Skolkovo Institute of Science and Technology

Определение

- $\{1, 2, \ldots, M\}$ – множество сообщений;
- $W \in \{1, 2, \ldots, M\}$ – сообщение;
- $X^n(W) = enc(W)$ – кодовое слово;
- $Y^n \sim P(y^n|x^n)$ – принятая последовательность;
- $\hat{W} = dec(Y^n)$ – правило декодирования.

Skoltech
Skolkovo Institute of Science and Technology

Определение (Код)

(M, n) *код для канала* $(\mathcal{X}, P(y|x), \mathcal{Y})$ *состоит из:*

- *множества сообщений* $\{1, 2, \ldots, M\}$;
- *функции кодирования* enc: $\{1, 2, \ldots, M\} \to \mathcal{X}^n$;
- *функции декодирования* dec: $\mathcal{Y}^n \to \{1, 2, \ldots, M\}$.

Определение (Вероятность ошибки)

$$\lambda_i = \Pr(dec(Y^n) \neq i | X^n = X^n(i)).$$

$$\lambda^{(n)} = \max_{i \in \{1,2,\ldots,M\}} \lambda_i$$

$$P_e^{(n)} = \frac{1}{M} \sum_{i=1}^{M} \lambda_i$$

Определение

Определение

Скорость R (M, n) кода определяется след образом

$$R = \frac{\log M}{n}.$$

Определение

Скорость R достижима, если существует последовательность кодов$(2^{Rn}, n)$, таких что $\lambda^{(n)} \to 0$ as $n \to \infty$.

Определение

Пропускная способность канала – супремум по всем достижимым скоростям.

Skoltech
Skolkovo Institute of Science and Technology

Совместно типичные последовательрности

$$
\begin{aligned}
A_\varepsilon^{(n)} \quad = \quad & \{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \\
& \left| -\frac{1}{n} \log P(x^n) - H(X) \right| < \varepsilon \\
& \left| -\frac{1}{n} \log P(y^n) - H(Y) \right| < \varepsilon \\
& \left| -\frac{1}{n} \log P(x^n, y^n) - H(X,Y) \right| < \varepsilon \Bigg\},
\end{aligned}
$$

где $P(x^n, y^n) = \prod_{i=1}^{n} P(x_i, y_i)$.

Skoltech
Skolkovo Institute of Science and Technology

Теорема

Пусть (X^n, Y^n) *– это последовательности длины* n*, выбранные независимо и из* $P(x^n, y^n)$*, тогда*

1. $\Pr((x^n, y^n) \in A_\varepsilon^{(n)}) \to 1$ *при* $n \to \infty$*;*
2. $|A_\varepsilon^{(n)}| \leq 2^{n(H(X,Y)+\varepsilon)}$*;*
3. *Если* $\hat{X}^n$ *и* $\hat{Y}^n$ *независимые с распределениями, совпадающими с маргинальными распределениями* $P(x^n, y^n)$*, тогда*

$$\Pr((\hat{x}^n, \hat{y}^n) \in A_\varepsilon^{(n)}) \leq 2^{-n(I(X;Y)-3\varepsilon)}$$

and

$$\Pr((\hat{x}^n, \hat{y}^n) \in A_\varepsilon^{(n)}) \geq (1-\varepsilon)2^{-n(I(X;Y)+3\varepsilon)}$$

Skoltech
Skolkovo Institute of Science and Technology

Теорема

- *Все скорости меньше C достижимы. В частности для любой скорости $R < C$, существует последовательность $(2^{Rn}, n)$ кодов с $\lambda^{(n)} \to 0$.*
- *Обратно, любая последовательность $(2^{Rn}, n)$ кодов с $\lambda^{(n)} \to 0$ удовлетворяет $R \leq C$.*

Skoltech
Skolkovo Institute of Science and Technology

Определение (Ансамбль кодов)

$$\mathcal{C} = \begin{bmatrix} x_1(1) & x_2(1) & \dots & x_n(1) \\ x_1(2) & x_2(2) & \dots & x_n(2) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(2^{Rn}) & x_2(2^{Rn}) & \dots & x_n(2^{Rn}) \end{bmatrix}$$

Каждый элемент выбирается независимо из $P(x)$.

Декодирование методом типичных множеств

Получатель заявляет, что был передан индекс $\hat{W}$, если выполняются следующие условия:

- пара $(X^n(\hat{W}), Y^n)$ является совместно типичной;
- нет другого i, такого что пара $(X^n(i), Y^n)$ является совместно типичной.

Skoltech
Skolkovo Institute of Science and Technology

Пусть $\Pr(\mathcal{E})$ – это средняя (по выбору кодовой книги) вероятность ошибки.

$$\begin{aligned}
\Pr(\mathcal{E}) &= \sum_{\mathcal{C}} P(\mathcal{C}) P_e^{(n)}(\mathcal{C}) \\
&= \sum_{\mathcal{C}} P(\mathcal{C}) \frac{1}{2^{Rn}} \sum_{w=1}^{2^{Rn}} \lambda_w(\mathcal{C}) \\
&= \frac{1}{2^{Rn}} \sum_{w=1}^{2^{Rn}} \sum_{\mathcal{C}} P(\mathcal{C}) \lambda_w(\mathcal{C}) \\
&= \sum_{\mathcal{C}} P(\mathcal{C}) \lambda_1(\mathcal{C}) \text{ (симметрия)} \\
&= \Pr(\mathcal{E}|W=1).
\end{aligned}$$

Skoltech
Skolkovo Institute of Science and Technology

Определим

$$E_i = \{(X^n(i), Y^n) \in A_\varepsilon^n\}.$$

$$\begin{aligned} \Pr(\mathcal{E}|W=1) &\leq \Pr(E_1^c) + \sum_{i=2}^{2^{Rn}} \Pr(E_i) \\ &\leq \varepsilon + \left(2^{Rn} - 1\right) 2^{-n[I(X;Y)-3\varepsilon]} \end{aligned}$$

Таким образом, если $R < I(X;Y)$, то можно выбрать ε и n, такие что $\Pr(\mathcal{E})$ меньше, чем ε'.

Skoltech
Skolkovo Institute of Science and Technology

Обратная теорема

Цепь Маркова:

$$W \to X^n(W) \to Y^n \to \hat{W}.$$

Converse.

Неравенство Фано

$$H(W|Y^n) \leq 1 + P_e^{(n)} nR$$

и $I(X^n; Y^n) \leq nC$

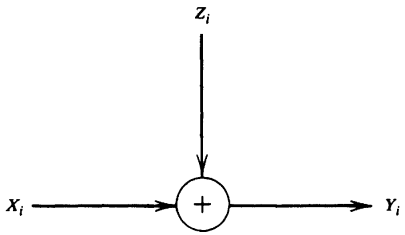
$$\begin{aligned} nR &= H(W) = H(W|Y^n) + I(W; Y^n) \\ &\leq H(W|Y^n) + I(X^n(W); Y^n) \\ &\leq 1 + P_e^{(n)} nR + I(X^n(W); Y^n) \\ &\leq 1 + P_e^{(n)} nR + nC. \end{aligned}$$

□

Outline

Skoltech
Skolkovo Institute of Science and Technology

Гауссовский канал



$$Y_i = X_i + Z_i, \;\; Z_i \sim N(0, N).$$

Ограничение на мощность

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P.$$

Skoltech
Skolkovo Institute of Science and Technology

Signal-to-noise ratio

$$SNR = \frac{P}{N} \quad \text{(линейный)}$$

$$SNR = 10 \log_{10} \frac{P}{N} \quad \text{(dB)}$$

Skoltech
Skolkovo Institute of Science and Technology

Пропускная спссобность

Определение

Пропускная способность гауссовского канала при ограничении P определяется как

$$C = \max_{p(x):\mathbb{E}[X^2] \leq P} I(X;Y).$$

Теорема

$$C = \frac{1}{2}\log(1 + SNR).$$

Skoltech
Skolkovo Institute of Science and Technology

Доказательство.

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) \\ &= h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z|X) \\ &= h(Y) - h(Z) \\ &= h(Y) - \frac{1}{2}\log 2\pi eN \end{aligned}$$

$$\mathbb{E}[Y^2] = \mathbb{E}[(X+Z)^2] = \mathbb{E}[X^2] + \mathbb{E}[Z^2] + 2\mathbb{E}[X]\mathbb{E}[Z] = P + N$$

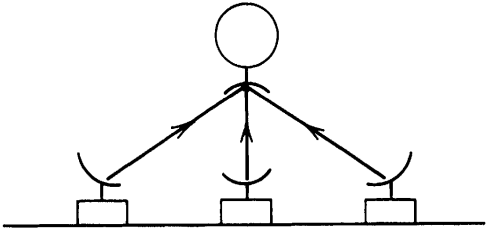
Таким образом,

$$h(Y) = \frac{1}{2}\log 2\pi e(P+N).$$

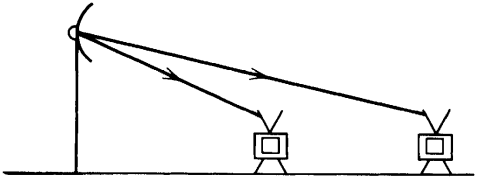
Outline

Skoltech
Skolkovo Institute of Science and Technology

Многопользовательские каналы



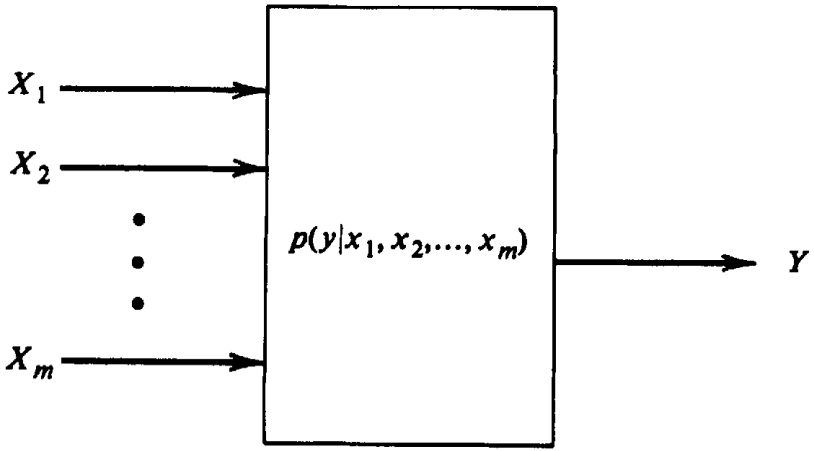
(a) MAC



(b) Широковещательный канал

Skoltech
Skolkovo Institute of Science and Technology

MAC с m пользователями



Skoltech
Skolkovo Institute of Science and Technology

MAC с m пользователями

Пусть $S \subseteq \{1, 2, \ldots, m\}$, $R(S) = \sum_{i \in S} R_i$ и $X(S) = \{X(i), i \in S\}$.

Теорема

Область пропускной способности многопользовательского канала – это выпуклая оболочка

$$R(S) \leq I(X(S); Y | X(S^c)) \quad \forall S \subseteq \{1, 2, \ldots, m\}.$$

для $P_1(x_1)P_2(x_2)\ldots P_m(x_m)$.

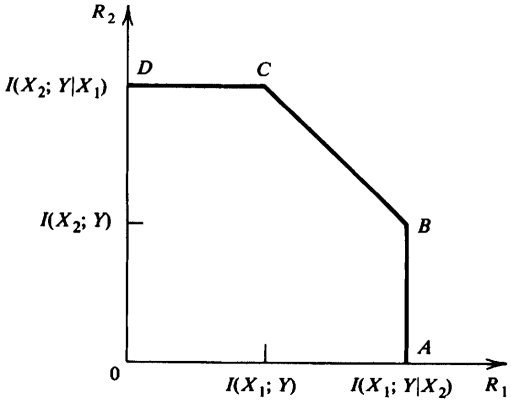
Skoltech
Skolkovo Institute of Science and Technology

MAC с двумя пользователями

$$
\begin{aligned}
R_1 &\leq I(X_1; Y|X_2) \\
R_2 &\leq I(X_2; Y|X_1) \\
R_1 + R_2 &\leq I(X_1, X_2; Y)
\end{aligned}
$$

Skoltech
Skolkovo Institute of Science and Technology

MAC с двумя пользователями



Skoltech
Skolkovo Institute of Science and Technology

Гауссовский MAC с двумя пользователями

$$Y = X_1 + X_2 + Z.$$

$$C(x) = \frac{1}{2}\log(1 + x).$$

$$\begin{aligned} R_1 &\leq C\left(\frac{P_1}{N}\right) \\ R_2 &\leq C\left(\frac{P_2}{N}\right) \\ R_1 + R_2 &\leq C\left(\frac{P_1 + P_2}{N}\right) \end{aligned}$$

Skoltech
Skolkovo Institute of Science and Technology

Проекты

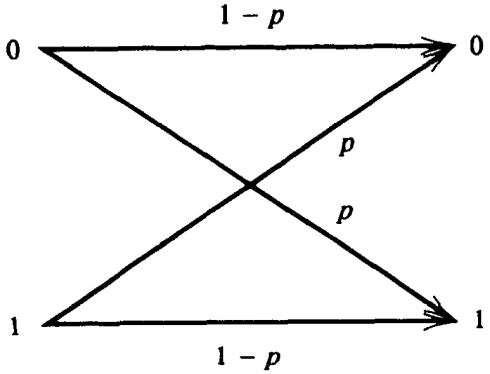
- Подсчет пропускной способности для ДНК-каналов
- Граница случайного кодирования для канала массового некоординированного множественного доступа (случай конечной длины)

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Двоичный симметричный канал



Скорость кода

- $\{1, 2, \ldots, M\}$ – множество сообщений;
- $Q = \{0, \ldots, q-1\}$;
- $\mathbf{x} = \Psi(i) \in Q^n$ – кодовое слово;
- $\mathcal{C} = \{\mathbf{x} = \Psi(i), i = 1, \ldots, M\}$ – код;
- кодовая книга;
- $\mathbf{y} \sim P(y^n | x^n)$ – принятая последовательность;
- $\hat{i} = \Psi^{-1}(\mathbf{y})$ – правило декодирования.
- $R = \frac{\log_q M}{n} = \frac{k}{n}$.

Skoltech
Skolkovo Institute of Science and Technology

Как декодировать?

$$\Psi : \begin{cases} 00 \to 00001 \\ 01 \to 01010 \\ 10 \to 10111 \\ 11 \to 11100 \end{cases}$$

$$\mathbf{y} = 10101$$

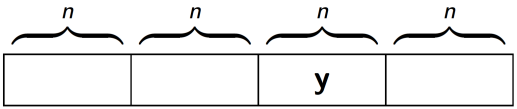
$\mathbf{x}$	$P(\mathbf{y}\|\mathbf{x})$
00001	$p^2(1-p)^3$
01010	p^5
10111	$p(1-p)^4$
11100	$p^2(1-p)^3$

$$p^5 < p^2(1-p)^3 < p(1-p)^4$$

$$\Rightarrow \mathbf{x} = 10111, \mathbf{i} = 10$$

Skoltech
Skolkovo Institute of Science and Technology

Декодирование по максимуму правдоподобия



$\cdots$ «$\Psi^{-1}(\mathbf{y}) = ?$»

Декодирование по максимуму правдоподобия:

1. $\mathbf{x} = \arg\max_{\mathbf{x} \in \mathcal{C}} P(\mathbf{y}|\mathbf{x})$;
2. $i = \Psi^{-1}(\mathbf{x})$.

Лемма

Пусть $\mathcal{C} = \{x_i\}$, $p < 0.5$ *и* $P(\mathbf{y}|\mathbf{x}) = \max_i P(\mathbf{y}|\mathbf{x}_i)$, *тогда*

$$d(\mathbf{y}, \mathbf{x}) = \min_i d(\mathbf{y}, \mathbf{x}_i),$$

где $d(\mathbf{y}, \mathbf{x})$ *обозначает число позиций, в которых* $\mathbf{y}$ *и* $\mathbf{x}$ *отличаются.*

Расстояние Хэмминга

Определение

Пусть $\alpha, \beta \in Q^n$.

$$d(\alpha, \beta) = |\{i : \alpha(i) \neq \beta(i)\}|.$$

Пример

$$\begin{aligned} \alpha &= 01101 \\ \beta &= 00111 \end{aligned}$$

$$d(\alpha, \beta) = 2.$$

Вес и номер набора

Определение

- $||\alpha|| = d(\alpha, \mathbf{0})$ – *вес* α;
- $|\alpha| = \sum_{i=1}^{n} \alpha_i q^{n-i}$ – *номер (лексикографический порядок)* α;

Skoltech
Skolkovo Institute of Science and Technology

Шар и сфера

Определение

$$B_r(\alpha) = \{\beta \in Q^n : d(\alpha, \beta) \leq r\}$$

and

$$S_r(\alpha) = \{\beta \in Q^n : d(\alpha, \beta) = r\}$$

Skoltech
Skolkovo Institute of Science and Technology

Шар и сфера

$$|S_r(\alpha)| = \binom{n}{r}(q-1)^r$$

и

$$|B_r(\alpha)| = \sum_{i=0}^{r} |S_r(\alpha)| = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$$

Skoltech
Skolkovo Institute of Science and Technology

Определение

- *Код* $\mathcal{C} \subseteq Q^n$;
- *Минимальное расстояние*

$$d(\mathcal{C}) = \min_{a,b \in \mathcal{C}; a \neq b} d(a, b).$$

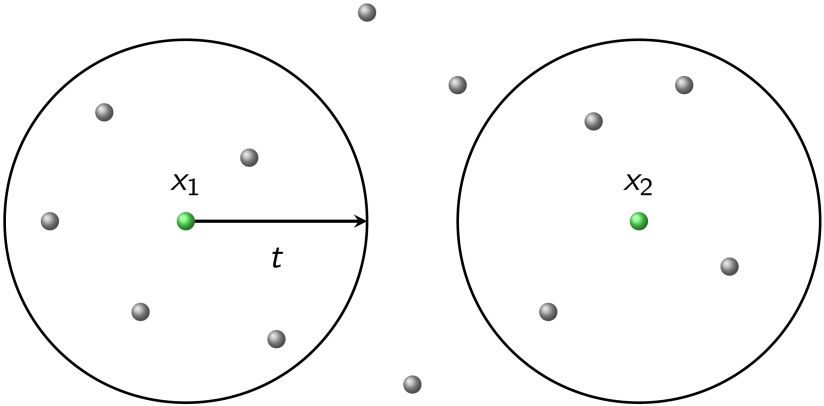
Skoltech
Skolkovo Institute of Science and Technology

Теорема

Пусть код $\mathcal{C}$ может исправить любые t ошибок, тогда

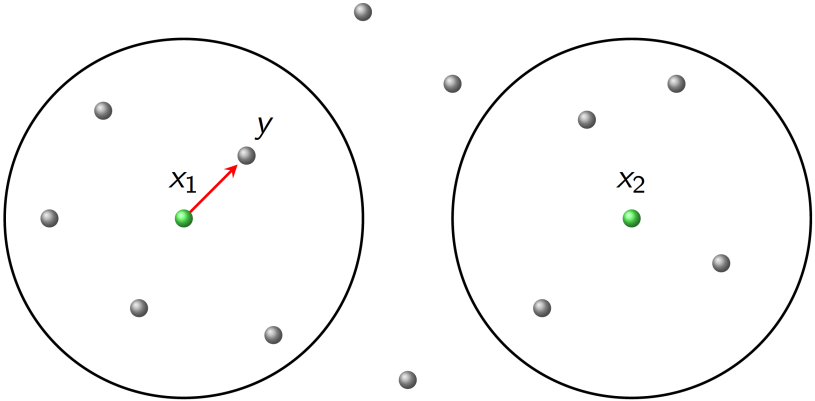
$$d(\mathcal{C}) \geq 2t + 1.$$

Геометрическая интерпретация



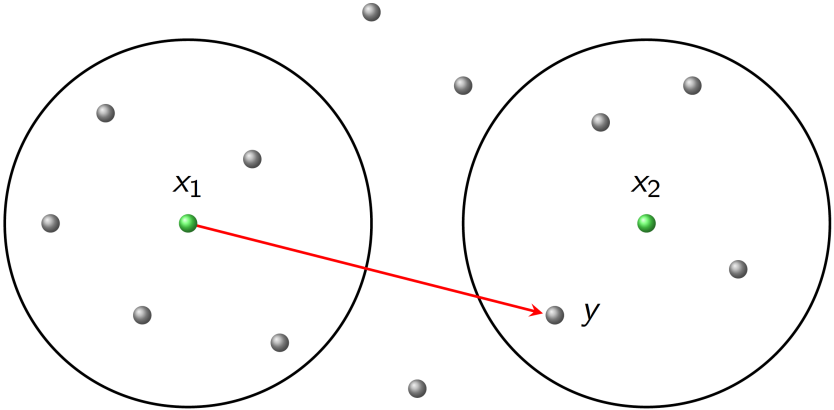
Skoltech
Skolkovo Institute of Science and Technology

Ошибка исправлена



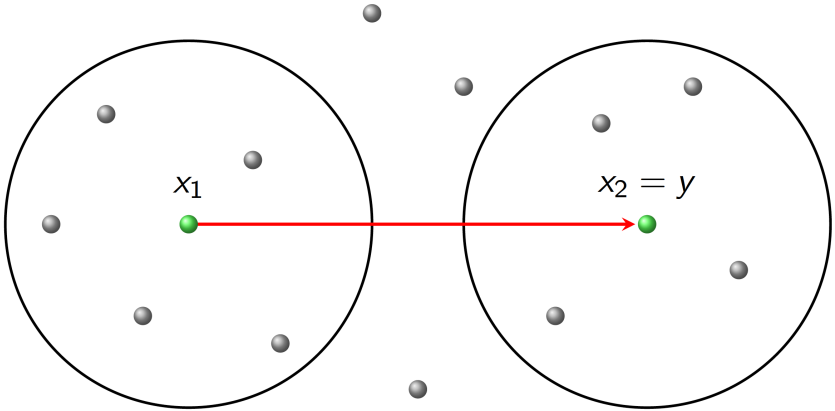
Skoltech
Skolkovo Institute of Science and Technology

Ошибка обнаружена



Skoltech
Skolkovo Institute of Science and Technology

Ошибка не обнаружена



Skoltech
Skolkovo Institute of Science and Technology

Теорема

Пусть $d(\mathcal{C}) = d$, *тогда*

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

и

$$s = d - 1.$$

Outline

Skoltech
Skolkovo Institute of Science and Technology

Определение $A_q(n, d)$

Определение

$$A_q(n, d) = \max_{\mathcal{C} \subseteq Q^n, d(\mathcal{C}) = d} |\mathcal{C}|.$$

Отметим, что максимизация мощности и скорости при фиксированном n – одинаковые задачи.

Далее будем опускать индекс q при $q = 2$.

Skoltech
Skolkovo Institute of Science and Technology

Граница Хэмминга

Пусть $\alpha \in Q^n$. Введем обозначение

$$V_t = V_q(t) = |B_t(\alpha)| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

Теорема (Граница Хэмминга)

$$A_q(n, d) \leq \frac{q^n}{V_t}.$$

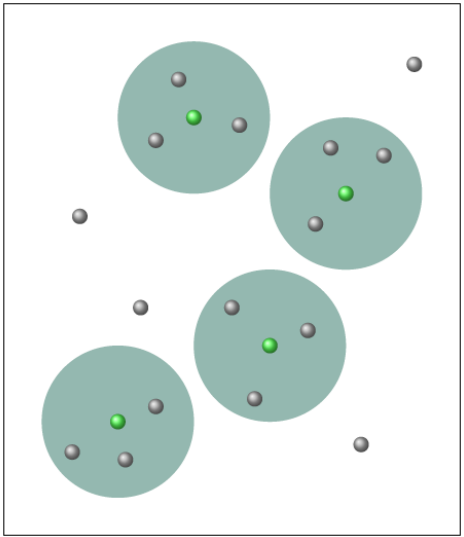
Определение

Код называется совершенным, если $|\mathcal{C}| = \frac{q^n}{V_t}$.

Пример

Код $\mathcal{C} = \{000, 111\} \subset \{0, 1\}^3$ *является совершенным.*

Доказательство границы Хэмминга



Шары радиуса t не пересекаются!

$$A_q(n,d)V_q(t) \leq q^n.$$

Skoltech
Skolkovo Institute of Science and Technology

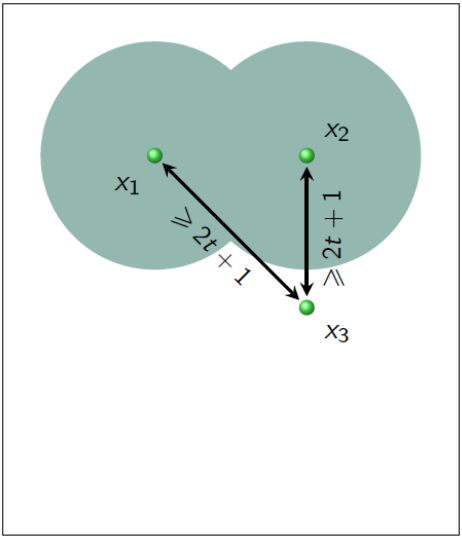
Граница Гилберта

Теорема (Граница Гилберта)

$$A_q(n, d) \geq \frac{q^n}{V_{2t}}.$$

Skoltech
Skolkovo Institute of Science and Technology

Proof



$$\mathbf{x}_3 \notin B_{2t}(\mathbf{x}_1) \cup B_{2t}(\mathbf{x}_2)$$

$\mathcal{C}_3 = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\}$ исправляет t ошибок.

Пусть мы построили m кодовых слов и не можем добавить новое слово

$$q^n = |\bigcup_{i=1}^{m} B_{2t}(\mathbf{x}_i)| \leq mV_{2t}.$$

Skoltech
Skolkovo Institute of Science and Technology

Асимптотический режим, $n \to \infty$

$\frac{d}{n} \to \delta$, $\frac{\log_q M}{n} = \frac{k}{n} \to R$

Определение

Семейство $\{\mathcal{C}_n\}$ называется асимптотически хорошим, если $R, \delta > 0$:

- $\frac{\log_q M_n}{n} = \frac{k_n}{n} \geq R > 0$;
- $\frac{d_n}{n} \geq \delta > 0$;

Skoltech
Skolkovo Institute of Science and Technology

Асимптотический режим, $n \to \infty$, $q = 2$

Граница Хэмминга

$$R \leq 1 - h(\delta/2).$$

Граница Гилберта

$$R \geq 1 - h(\delta).$$

Граница Синглтона

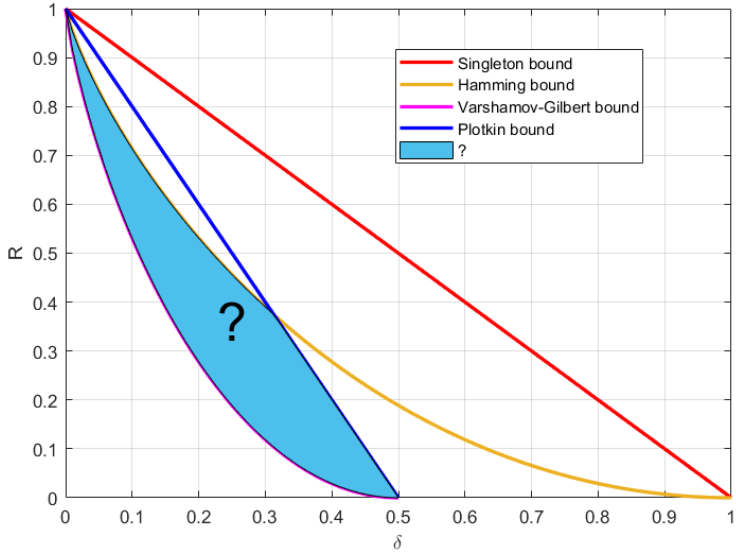
$$R \leq 1 - \delta.$$

Граница Плоткина

$$R \leq 1 - 2\delta.$$

Skoltech
Skolkovo Institute of Science and Technology

Асимптотический режим, $n \to \infty$



Outline

Skoltech
Skolkovo Institute of Science and Technology

Определение

Подгруппа Абелевой группы $\mathbb{F}_q^n$ называется групповым кодом.

Определение

Подпространство $\mathcal{C}$ линейного пристранства $\mathbb{F}_q^n$ называется линейным (n, k) кодом, где $k = \dim \mathcal{C}$.

Определение

G – порождающая матрица $\mathcal{C}$, если ее строки образуют базис $\mathcal{C}$.

Skoltech
Skolkovo Institute of Science and Technology

Минимальное расстояние

Лемма

Пусть $\mathcal{C}$ – это линейный код, тогда

$$d(\mathcal{C}) = \min_{a \in \mathcal{C}, a \neq 0} ||a||.$$

Skoltech
Skolkovo Institute of Science and Technology

Дуальный код и проверочная матрица

Определение (Дуальный код)

$$C^{\perp} = \{v \in \mathbb{F}_q^n : v \perp \mathcal{C}\}.$$

Определение (Проверочная матрица)

H – это базис $C^{\perp}$.

Skoltech
Skolkovo Institute of Science and Technology

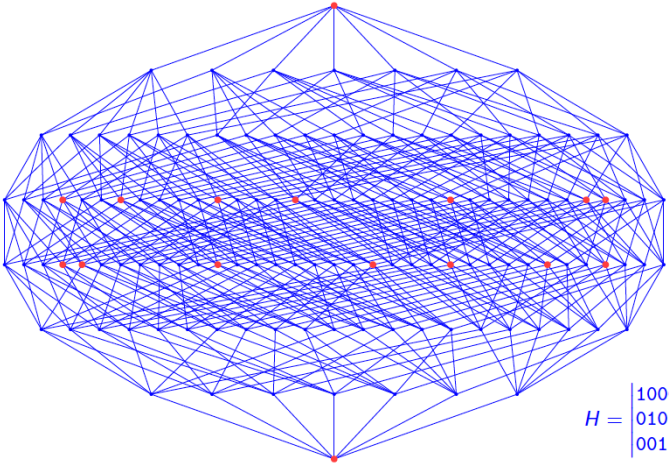
Код Хэмминга

Параметры:

$$n = 2^m - 1, k = 2^m - m - 1, d = 3.$$

Skoltech
Skolkovo Institute of Science and Technology

Код Хэмминга



$$H = \begin{vmatrix} 1000111 \\ 0101011 \\ 0011101 \end{vmatrix}$$

Skoltech
Skolkovo Institute of Science and Technology

Код Хэмминга

$$H_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

$$H_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Skoltech
Skolkovo Institute of Science and Technology

Проекты

- Применение нейронных сетей для декодирования линейных кодов. Подход на основе синдрома
- Применение нейронных сетей для декодирования линейных кодов. Подход на основе графа Таннера
- Построение помехоустойчивых кодов с помощью машинного обучения
- Постквантовая (кодовая) криптография
- Кодовые распределенные вычисления для задач машинного обучения.

Skoltech
Skolkovo Institute of Science and Technology

Спасибо за внимание!

Skoltech
Skolkovo Institute of Science and Technology