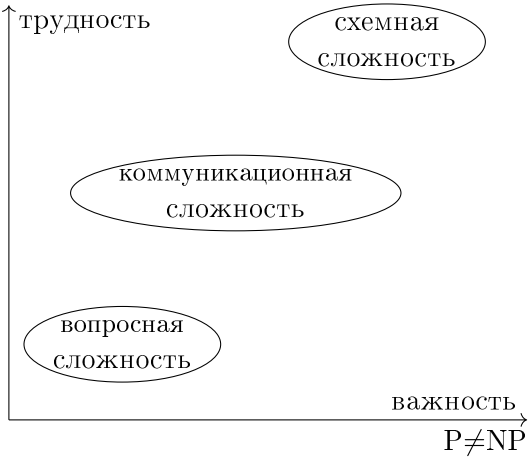
# Экспандеры и связь коммуникационной и вопросной сложности.

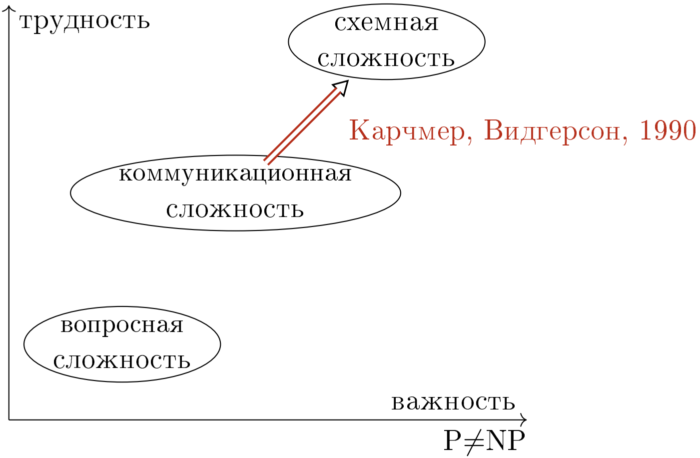
Н. К. Верещагин, А. Н. Козачинский

Семинар кафедры математической логики и теории алгоритмов, 10 октября

# Нижние оценки

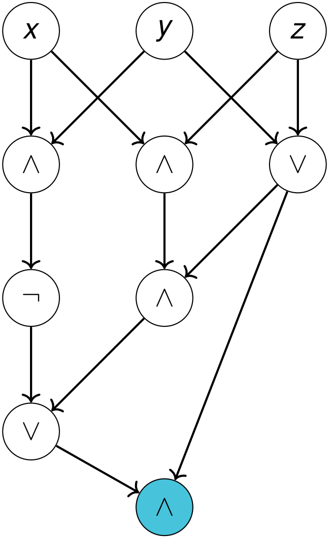


# Нижние оценки



# Нижние оценки

# Схемы




Размер := количество вершин
Глубина := длина самого длинного пути

Рассмотрим $f : \{0,1\}^n \to \{0,1\}$.

$$s(f) = \min\{s : \exists \text{ схема размера } s \text{ вычисляющая } f\}$$

$$d(f) = \min\{d : \exists \text{ схема глубины } d \text{ вычисляющая } f\}$$

# Сложностные классы

$$\mathrm{P/poly} = \{\{f_n\} \subset \{0,1\}^* : \{f_n\} \text{ вычислима последовательностью схем размера } \mathrm{poly}(n)\}$$

$$\mathrm{NC}^i = \{\{f_n\} \subset \{0,1\}^* : \{f_n\} \text{ вычислима последовательностью схем размера } \mathrm{poly}(n) \text{ и глубины } O(\log^i n)\}$$

$$\mathrm{NC}^1 \subset \mathrm{NC}^2 \subset \ldots \subset \mathrm{NC} \subset \mathrm{P/poly}.$$

# Сложностные классы

$$\mathrm{P/poly} = \{\{f_n\} \subset \{0,1\}^* : \{f_n\} \text{ вычислима последовательностью схем размера } \mathrm{poly}(n)\}$$

$$\mathrm{NC}^i = \{\{f_n\} \subset \{0,1\}^* : \{f_n\} \text{ вычислима последовательностью схем размера } \mathrm{poly}(n) \text{ и глубины } O(\log^i n)\}$$

$$\mathrm{NC}^1 \subset \mathrm{NC}^2 \subset \ldots \subset \mathrm{NC} \subset \mathrm{P/poly}.$$

Неизвестно, верно ли, что $\mathrm{NC}^1 \neq \mathrm{P/poly}$.

# Монотонные аналоги

Монотонные схемы — схемы без отрицания. Вычисляют только монотонные булевы функции.

Ко всем обозначениям обозначениям добавляем m:

$$d^m(f), s^m(f), \mathrm{mNC}^i, \mathrm{mNC}, \mathrm{mP/poly}\ldots$$

$$\mathrm{mNC}^1 \subsetneq \mathrm{mNC}^2 \subsetneq \ldots \subsetneq \mathrm{mNC} \subsetneq \mathrm{mP/poly}\ !$$

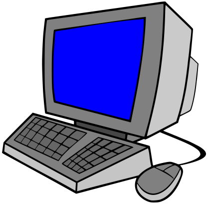
- $\mathrm{mNC}^1 \subsetneq \mathrm{mNC}^2$ — Карчмер и Видгерсон, 1990;
- Остальное — Раз и Маккинзи, 1997.

# Коммуникационная сложность

Дано: $R \subset \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ (множества $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ — конечные).

Алиса

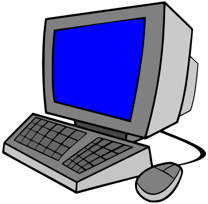
$x \in \mathcal{X}$



$z : (x, y, z) \in R$

Боб

$y \in \mathcal{Y}$



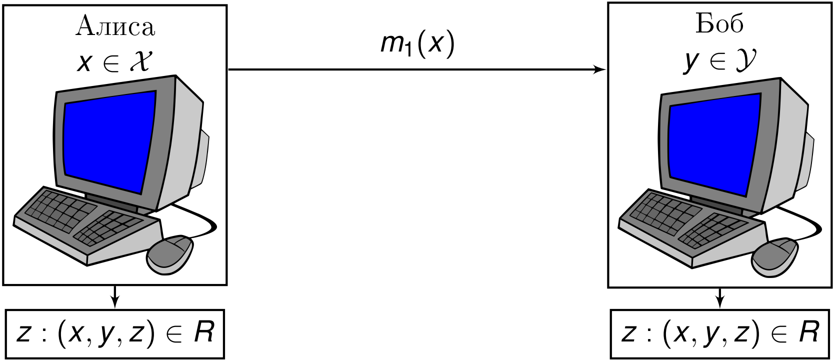
$z : (x, y, z) \in R$

Коммуникационная длина протокола := максимум по $(x, y) \in \mathcal{X} \times \mathcal{Y}$ суммы длин всех сообщений на $(x, y)$.

$CC(R)$ := минимальное $d$, для которого найдется протокол коммуникационной длины не больше $d$, вычисляющий $R$.

# Коммуникационная сложность

Дано: $R \subset \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ (множества $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ — конечные).

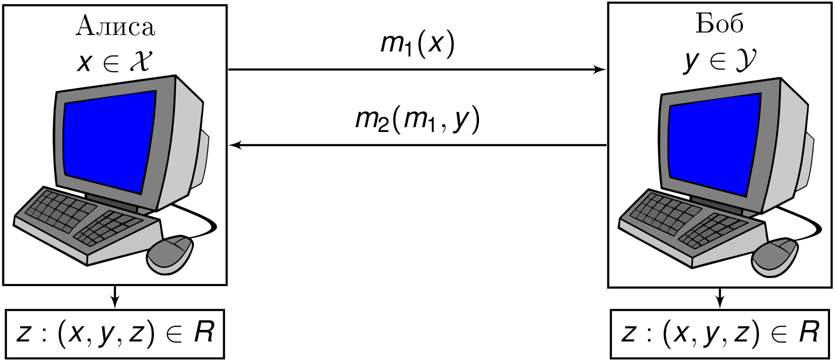



Коммуникационная длина протокола := максимум по $(x, y) \in \mathcal{X} \times \mathcal{Y}$ суммы длин всех сообщений на $(x, y)$.

$CC(R)$ := минимальное $d$, для которого найдется протокол коммуникационной длины не больше $d$, вычисляющий $R$.

# Коммуникационная сложность

Дано: $R \subset \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ (множества $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ — конечные).

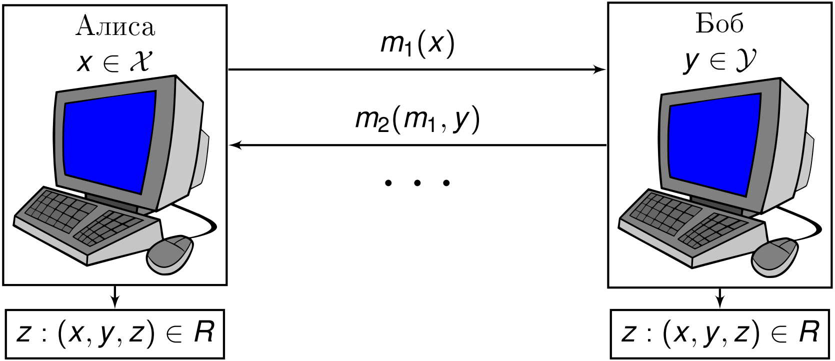



Коммуникационная длина протокола := максимум по $(x, y) \in \mathcal{X} \times \mathcal{Y}$ суммы длин всех сообщений на $(x, y)$.

$CC(R)$ := минимальное $d$, для которого найдется протокол коммуникационной длины не больше $d$, вычисляющий $R$.

# Коммуникационная сложность

Дано: $R \subset \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ (множества $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ — конечные).




Коммуникационная длина протокола := максимум по $(x, y) \in \mathcal{X} \times \mathcal{Y}$ суммы длин всех сообщений на $(x, y)$.

$CC(R)$ := минимальное $d$, для которого найдется протокол коммуникационной длины не больше $d$, вычисляющий $R$.

# Пример

$$\mathcal{X} = \{x \in \{0,1\}^n : x_1 + \ldots + x_n \text{ нечетно}\},$$
$$\mathcal{Y} = \{y \in \{0,1\}^n : y_1 + \ldots + y_n \text{ четно}\},$$
$$\mathcal{Z} = \{1, 2, \ldots, n\}.$$

$$R = \{(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} : x_z \neq y_z.\}$$

# Пример

$$\mathcal{X} = \{x \in \{0,1\}^n : x_1 + \ldots + x_n \text{ нечетно}\},$$
$$\mathcal{Y} = \{y \in \{0,1\}^n : y_1 + \ldots + y_n \text{ четно}\},$$
$$\mathcal{Z} = \{1, 2, \ldots, n\}.$$

$$R = \{(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} : x_z \neq y_z.\}$$

Алиса
$x \in \{0,1\}^n$ т. ч.
$x_1 + \ldots + x_n$ нечетно

Боб
$y \in \{0,1\}^n$ т. ч.
$y_1 + \ldots + y_n$ четно

Выдать какой-нибудь $z$ т. ч. $x_z \neq y_z$

# Пример

$\mathcal{X} = \{x \in \{0,1\}^n : x_1 + \ldots + x_n \text{ нечетно}\}$,
$\mathcal{Y} = \{y \in \{0,1\}^n : y_1 + \ldots + y_n \text{ четно}\}$,
$\mathcal{Z} = \{1, 2, \ldots, n\}$.

$$R = \{(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} : x_z \neq y_z.\}$$

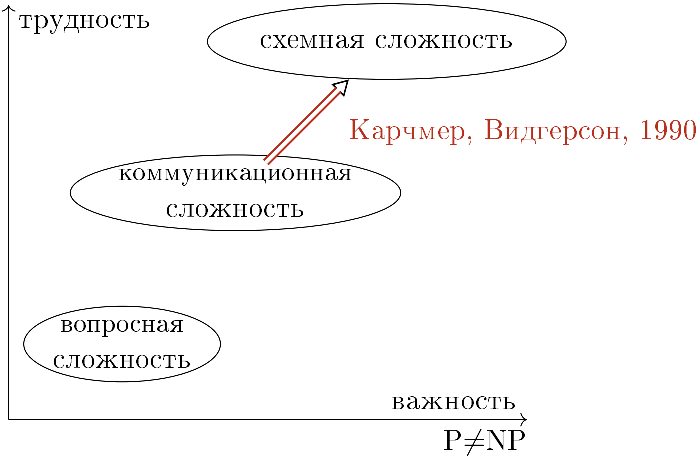
Алиса
$x \in \{0,1\}^n$ т. ч.
$x_1 + \ldots + x_n$ нечетно

Боб
$y \in \{0,1\}^n$ т. ч.
$y_1 + \ldots + y_n$ четно

Выдать какой-нибудь $z$ т. ч. $x_z \neq y_z$

$CC(R) = O(\log n)$ (бинарный поиск)

# Нижние оценки



# Отношения Карчмера — Видгерсона

Дано: $f\colon \{0,1\}^n \to \{0,1\}$.

Алиса
$x \in \{0,1\}^n$ т. ч.
$f(x) = 1$

Боб
$y \in \{0,1\}^n$ т. ч.
$f(y) = 0$

Выдать какой-нибудь $z \in \{1, 2, \ldots, n\}$ т. ч. $x_z \neq y_z$

**Теорема**

$d(f) = CC(\mathrm{KW}(f))$.

# Монотонные отношения Карчмера — Видгерсона

Дано: монотонная $f\colon \{0,1\}^n \to \{0,1\}$.

Алиса
$x \in \{0,1\}^n$ т. ч.
$f(x) = 1$

Боб
$y \in \{0,1\}^n$ т. ч.
$f(y) = 0$

Выдать какой-нибудь $z \in \{1, 2, \ldots, n\}$ т. ч. $x_z = 1, y_z = 0$

**Теорема**

$d^m(f) = CC(\mathrm{mKW}(f))$.

# Функция из $\mathrm{mNC}^2 \setminus \mathrm{mNC}^1$

$$\text{st-Conn}_n$$

Вход: $G : \{1, 2, \ldots, n\}^2 \to \{0, 1\}$ (ориентированный граф на $n$ вершинах)

Вопрос: Есть ли в $G$ ориентированный путь из $1$ в $n$?

# Функция из $\mathrm{mNC}^2 \setminus \mathrm{mNC}^1$

$$\text{st-Conn}_n$$

Вход: $G : \{1, 2, \ldots, n\}^2 \to \{0, 1\}$ (ориентированный граф на $n$ вершинах)

Вопрос: Есть ли в $G$ ориентированный путь из $1$ в $n$?

## Предложение

$\{\text{st-Conn}_n\} \in \mathrm{mNC}^2$.

# Функция из $\mathrm{mNC}^2 \setminus \mathrm{mNC}^1$

$$\text{st-Conn}_n$$

Вход: $G : \{1, 2, \ldots, n\}^2 \to \{0, 1\}$ (ориентированный граф на $n$ вершинах)

Вопрос: Есть ли в $G$ ориентированный путь из $1$ в $n$?

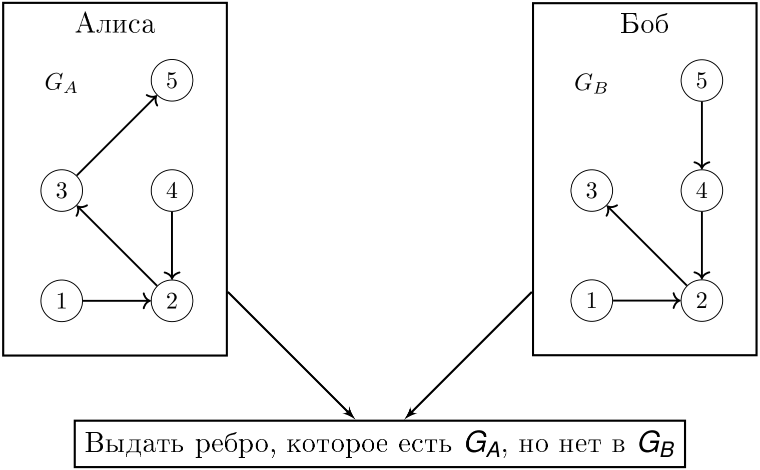
**Предложение**

$\{\text{st-Conn}_n\} \in \mathrm{mNC}^2$.

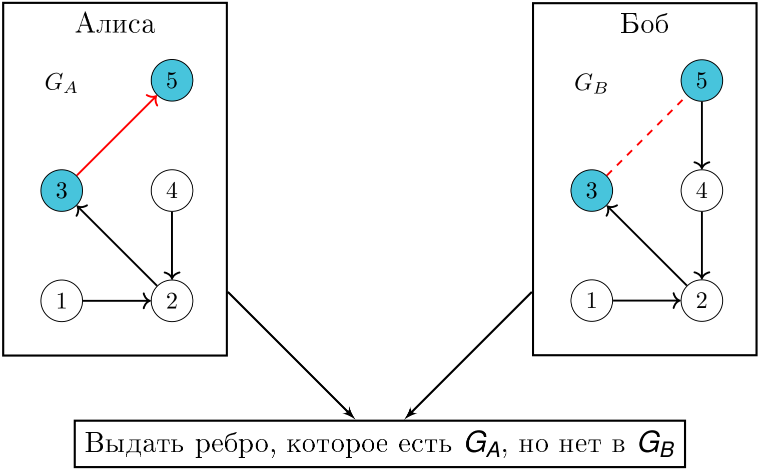
**Теорема (Карчмер, Видгерсон)**

$d^m(\text{st-Conn}_n) = \Omega(\log^2 n)$.

# монотонное KW-отношение для st-Conn$_n$



# монотонное KW-отношение для st-Conn$_n$



# План нижней оценки для $\mathrm{st\text{-}Conn}_n$.

$\Omega(\log^2 n)$ на монотонную глубину $\mathrm{st\text{-}Conn}_n$.

# План нижней оценки для st-Conn$_n$.

$\Omega(\log^2 n)$ на монотонную глубину st-Conn$_n$.

$$\Uparrow$$

$\Omega(\log^2 n)$ на комм. сложность монотонного KW-отношения для st-Conn$_n$.

# План нижней оценки для st-Conn$_n$.

$\Omega(\log^2 n)$ на монотонную глубину st-Conn$_n$.

$$\Uparrow$$

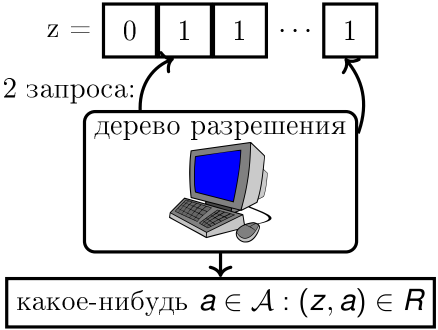
$\Omega(\log^2 n)$ на комм. сложность монотонного KW-отношения для st-Conn$_n$.

$$\Uparrow$$

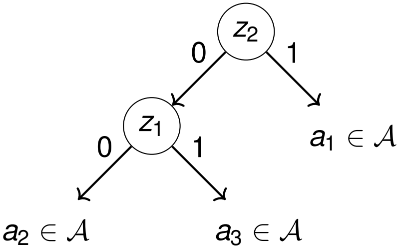
вопросная сложность

# Деревья разрешения

$R \subset \{0,1\}^n \times \mathcal{A}$ (назовем $n$ арностью $R$)




Деревья разрешения (пример для $n = 2$).



# Вопросная сложность

$Q(R) :=$ минимальное $d$, для которого найдется дерево разрешения глубины $d$ (т. е. делающее не более $d$ запросов), вычисляющее $R$.

# Пример: отношение $\mathrm{SEARCH}_n$

$$z = \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{1}$$

$\mathrm{SEARCH}_n$

$= \{(z, i) \in \{0,1\}^n \times \{0, 1, \ldots, n\}$ :

либо $i = 0, z_1 = 1$

либо $1 \leq i < n,\ z_i = 0, z_{i+1} = 1$

либо $i = n, z_n = 0\}$.

$Q(\mathrm{SEARCH}_n) = \Theta(\log n)$

Верхняя оценка — бинарный поиск.

Нижняя оценка — $n$ возможных ответов.

# Пример: отношение SEARCH$_n$

| z = | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|

SEARCH$_n$
$= \{(z, i) \in \{0,1\}^n \times \{0,1,\ldots,n\}$ :
либо $i = 0, z_1 = 1$
либо $1 \leq i < n,\ z_i = 0, z_{i+1} = 1$
либо $i = n, z_n = 0\}$.

$Q(\mathrm{SEARCH}_n) = \Theta(\log n)$

Верхняя оценка — бинарный поиск.

Нижняя оценка — $n$ возможных ответов.

# Пример: отношение SEARCH$_n$

$$z = \boxed{0}\,\boxed{0}\,\boxed{1}\,\boxed{0}\,\boxed{0}\,\boxed{0}\,\boxed{1}$$

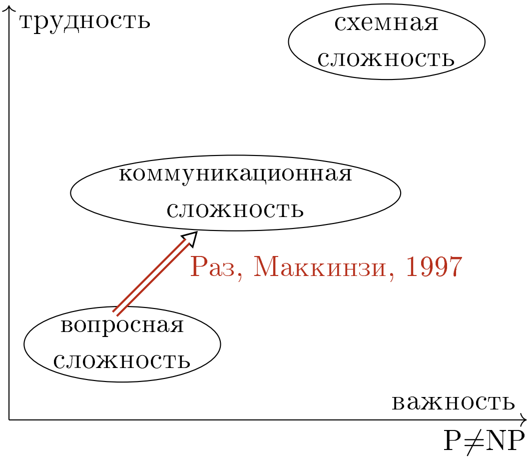
SEARCH$_n$
$= \{(z, i) \in \{0,1\}^n \times \{0, 1, \dots, n\}$ :
либо $i = 0, z_1 = 1$
либо $1 \le i < n,\ z_i = 0, z_{i+1} = 1$
либо $i = n, z_n = 0\}$.

$Q(\mathrm{SEARCH}_n) = \Theta(\log n)$

Верхняя оценка — бинарный поиск.

Нижняя оценка — $n$ возможных ответов.

# Нижние оценки



# Связь при помощи композиции

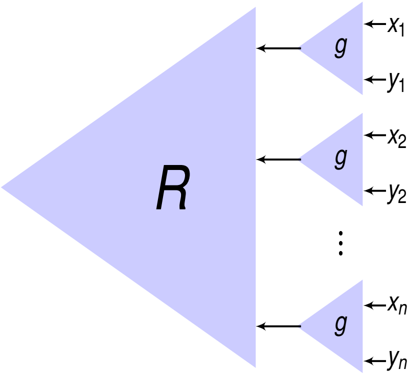
внешнее отношение:

$R \subset \{0,1\}^n \times \mathcal{A}$,

гаджет:

$g\colon \mathcal{X} \times \mathcal{Y} \to \{0,1\}$

$R \circ g =$




## Предложение

$CC(R \circ g) \leq Q(R) \cdot CC(g)$.

# Теорема Раза — Маккинзи

$$\mathrm{IND}_k : [k] \times \{0,1\}^k \to \{0,1\}, \qquad \mathrm{IND}_k(x,y) = y_x.$$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 3 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

Рис.: $M_{\mathrm{IND}_3}$

$$CC(\mathrm{IND}_k) = \Theta(\log k).$$

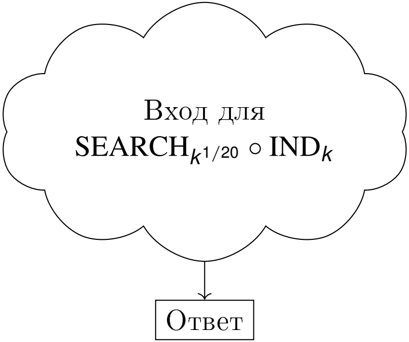
### Теорема ( RM97, GPW15)

Для всех $R$ арности не более $k^{1/20}$ выполнено

$$CC(R \circ \mathrm{IND}_k) = \Omega(Q(R) \cdot CC(\mathrm{IND}_k)).$$

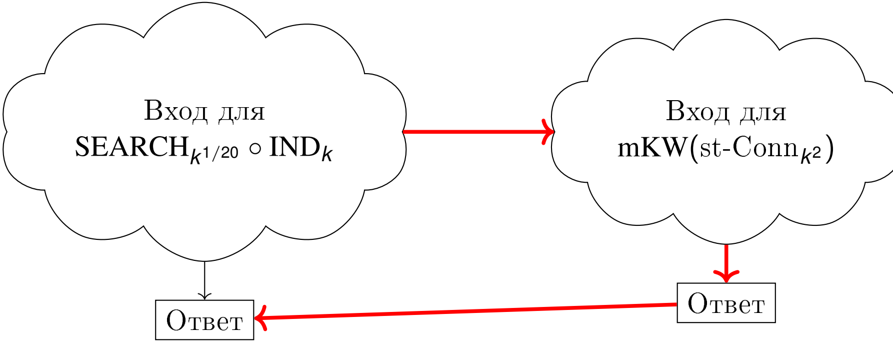
# Применение: нижняя оценка st-Conn$_n$

$$\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k \leq \mathrm{mKW}(\text{st-Conn}_{k^2})$$



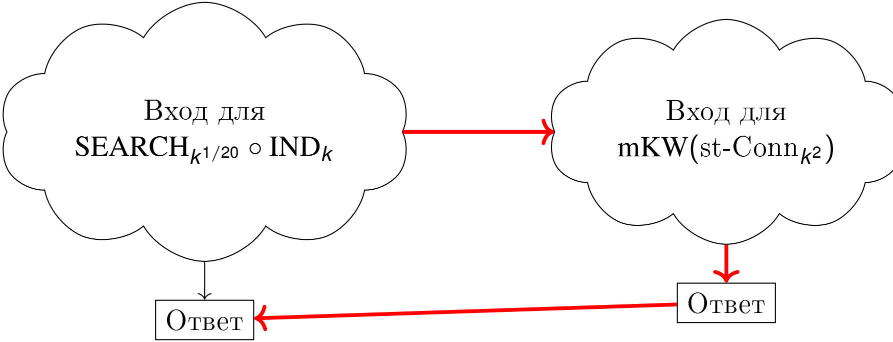
# Применение: нижняя оценка st-Conn$_n$

$$\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k \le \mathrm{mKW}(\text{st-Conn}_{k^2})$$



# Применение: нижняя оценка st-Conn$_n$

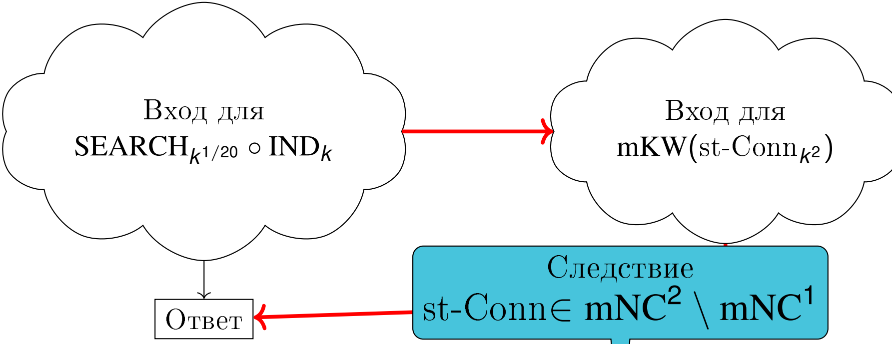
$$\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k \le \mathrm{mKW}(\text{st-Conn}_{k^2})$$




$$\begin{aligned}
d^m(\text{st-Conn}_{k^2}) &= CC(\mathrm{mKW}(\text{st-Conn}_{k^2})) && \text{К. — В.}\\
&\ge CC(\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k) && \text{сведение}\\
&= \Omega(Q(\mathrm{SEARCH}_{k^{1/20}}) \cdot CC(\mathrm{IND}_k)) && \text{Р. — М.}\\
&= \Omega(\log^2(k)).
\end{aligned}$$

# Применение: нижняя оценка st-Conn$_n$

$$\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k \leq \mathrm{mKW}(\text{st-Conn}_{k^2})$$




$$
\begin{aligned}
d^m(\text{st-Conn}_{k^2}) &= CC(\mathrm{mKW}(\text{st-Conn}_{k^2})) && \text{К. — В.}\\
&\geq CC(\mathrm{SEARCH}_{k^{1/20}} \circ \mathrm{IND}_k) && \text{сведение}\\
&= \Omega(Q(\mathrm{SEARCH}_{k^{1/20}}) \cdot CC(\mathrm{IND}_k)) && \text{Р. — М.}\\
&= \Omega(\log^2(k)).
\end{aligned}
$$

# Можно ли усилить теорему Раза — Маккинзи?

$$\mathrm{IND}_k : [k] \times \{0,1\}^k \to \{0,1\}, \qquad \mathrm{IND}_k(x,y) = y_x.$$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 3 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

Рис.: $M_{\mathrm{IND}_3}$

$$CC(\mathrm{IND}_k) = \Theta(\log k).$$

**Теорема ( RM97, GPW15)**

Для всех $R$ арности не более $k^{1/20}$ выполнено

$$CC(R \circ \mathrm{IND}_k) = \Omega(Q(R) \cdot CC(\mathrm{IND}_k)).$$

# Можно ли усилить теорему Раза — Маккинзи?

$$\mathrm{IND}_k : [k] \times \{0,1\}^k \to \{0,1\}, \qquad \mathrm{IND}_k(x,y) = y_x.$$

$$\begin{array}{c|cccccccc}
 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}$$

Рис.: $M_{\mathrm{IND}_3}$

$$CC(\mathrm{IND}_k) = \Theta(\log k).$$

Можно ли для других гаджетов
с длиной входа $k$
усилить оценку на арность $R$?

**Теорема ( RM97, GPW15)**

Для всех $R$ арности не более $k^{1/20}$ выполнено

$$CC(R \circ \mathrm{IND}_k) = \Omega(Q(R) \cdot CC(\mathrm{IND}_k)).$$

# Результаты

- Новый гаджет $g$ с длиной входа $k$, для которого неравенство:

$$CC(R \circ g) = \Omega(Q(R) \cdot CC(g))$$

  выполнено для всех $R$ арности не более $2^{k/2}$. Используются экспандеры.
- С текущей техникой оценку лучше $2^{k/2}$ получить нельзя.

# Результаты

- Новый гаджет $g$ с длиной входа $k$, для которого неравенство:

$$CC(R \circ g) = \Omega(Q(R) \cdot CC(g))$$

выполнено для всех $R$ арности не более $2^{k/2}$. Используются экспандеры.

- С текущей техникой оценку лучше $2^{k/2}$ получить нельзя.

Новый гаджет.

$$\mathrm{SQR}^q : \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \{0, 1\}, \qquad \mathrm{SQR}^q(x, y) = \begin{cases} 1 & x - y \text{ квадрат,} \\ 0 & \text{иначе.} \end{cases}.$$

Спасибо за внимание!