Введение в теорию сложности вычислений

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

СПбГУ и ПОМИ РАН

лекция 10 декабря 2020 г.

P-полнота

Теорема

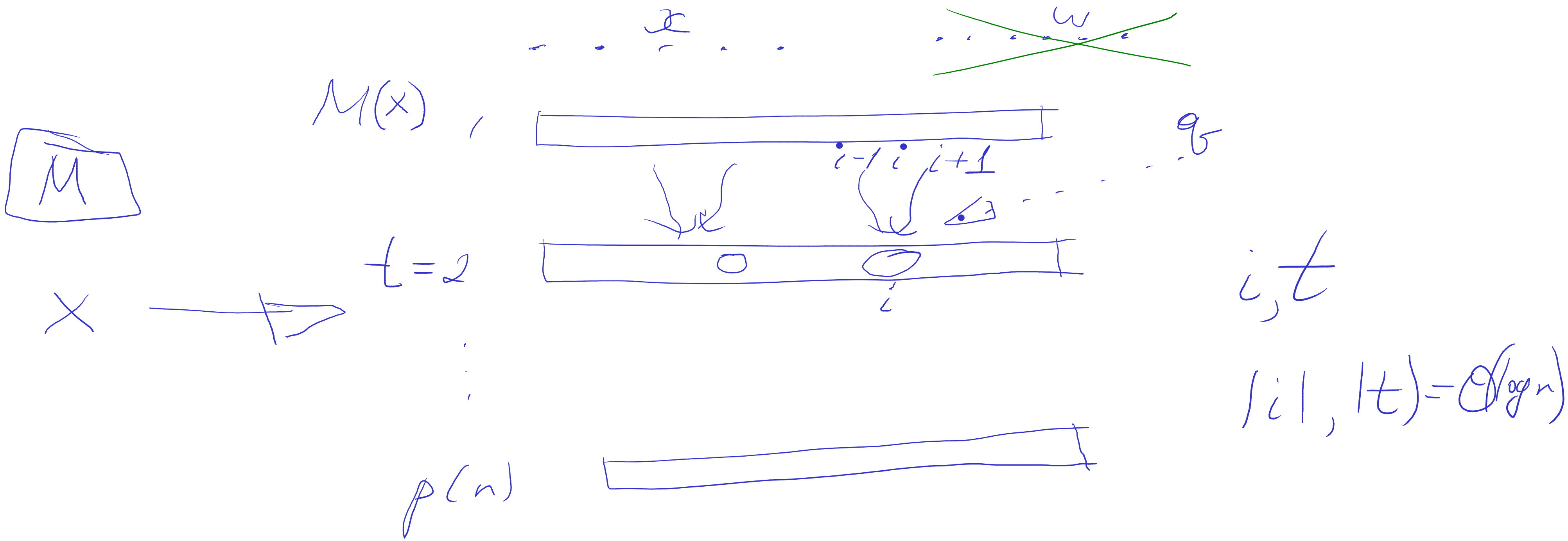
Если L — **P**-полный, то

logspace reductions

- $L \in \mathbf{L} \iff \mathbf{P} = \mathbf{L}$.

P-полный язык:

$$\mathrm{CIRCUIT\_EVAL} = \{(\text{схема } C, \text{вход } x) \mid C(x) = 1\}.$$



Параллельные вычисления и логарифмическая память

Теорема

$\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

Параллельные вычисления и логарифмическая память

Теорема

$\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

Пусть logspace НМТ M принимает $L \in \mathbf{NL}$.

- Интересует достижимость в графе конфигураций M.
- Для конкретной входной ленты их полиномиальное число k.

Параллельные вычисления и логарифмическая память

Теорема

$\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

Пусть logspace НМТ M принимает $L \in \mathbf{NL}$.

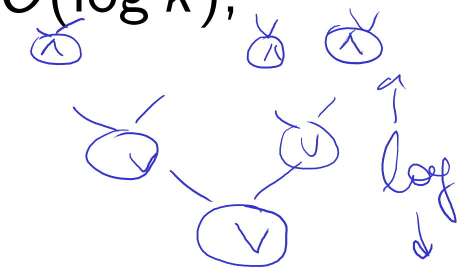
- Интересует достижимость в графе конфигураций M.
- Для конкретной входной ленты их полиномиальное число k.
- A — матрица смежности $(k \times k)$. A A^2 – за 2 шага
- Достаточно вычислить A^k.

Теорема

$\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

Пусть logspace НМТ M принимает $L \in \mathbf{NL}$.

- Интересует достижимость в графе конфигураций M.
- Для конкретной входной ленты их полиномиальное число k.
- A — матрица смежности $(k \times k)$. log k возведение
- Достаточно вычислить A^k.
- Это $\log k$ последовательных умножений: A^2, $(A^2)^2$, ...
- Умножение пары булевых матриц: схема глубины $O(\log k)$,



Параллельные вычисления и логарифмическая память

Теорема

$\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2$.

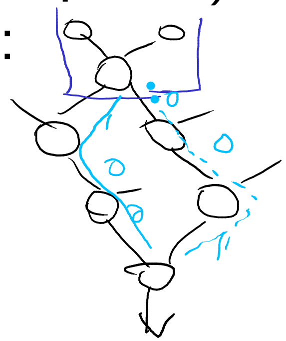
$\{C_n\}$

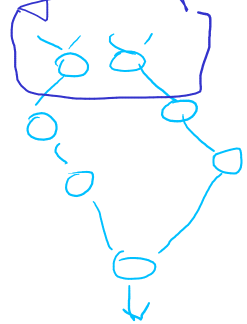
$C_n(x)$

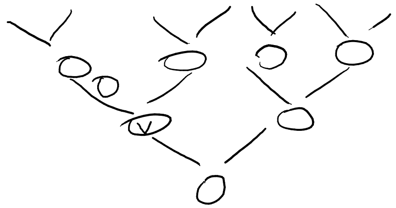
log depth

$x \overset{?}{\in} L \in \mathbf{NC}^1$. Строим композицию трёх logspace функций с логарифмической памятью.

1. Строим схему (семейство было logspace-равномерным).
2. Преобразуем схему в формулу (dag $\to$ дерево):
   - гейт $\to$ путь от выхода (битовая строка),
   - поиск в глубину — логарифмическая память,
   - для возврата идём заново от корня.
3. Вычисляем значение формулы на входе x.
   - Снова поиск в глубину.







Ещё о **P**-полноте

$L \subseteq NC \subseteq P \subseteq NP \subseteq PSPACE$

$\neq$

Теорема

Если L — **P**-полный, то

- $L \in \mathbf{NC} \iff \mathbf{P} = \mathbf{NC}$ (всё параллелизуется);

$L' \in P$

$L' \xrightarrow{\text{logspace}} L \in NC^i$

NC^{i+2}

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in \mathbf{co\text{-}NL}$

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in \mathbf{co\text{-}NL}$ $\overline{STCON} \in NL$

- Сертифицируем отсутствие пути между вершинами s и t.

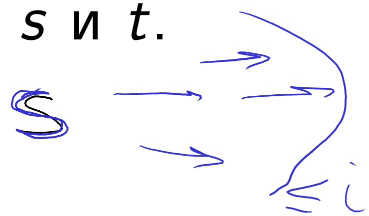
Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in \textbf{co-NL}$

- Сертифицируем отсутствие пути между вершинами s и t.
- $S_i = \{$вершин на расстоянии $\leq i$ от $s\}$.



Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in \mathbf{co}\text{-}\mathbf{NL}$

- Сертифицируем отсутствие пути между вершинами s и t.
- $S_i = \{$вершин на расстоянии $\leq i$ от $s\}$.
- Сертификат принадлежности $(x \in S_i)$ — путь.

$s \xrightarrow[\leq i]{} x$

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in$ **co-NL**

- Сертифицируем отсутствие пути между вершинами s и t.
- $S_i = \{$вершин на расстоянии $\leq i$ от $s\}$.
- Сертификат принадлежности ($x \in S_i$) — путь.
- Сертификат непринадлежности ($x \notin S_i$):
  - $|S_i|$ (тоже надо сертифицировать!),
  - все вершины S_i с сертификатами принадлежности.

$\boxed{t \notin S'_{|V|-1}}$

x_1
x_2
1) $x_3 \in S_i$ w_3, $x_3 \neq x$
$\vdots$
2) $\vdots$ E кол-во $= |S_i|$
x_k

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

STCON $\in$ **co-NL**

- Сертифицируем отсутствие пути между вершинами s и t.
- $S_i = \{$вершин на расстоянии $\leq i$ от $s\}$.
- Сертификат принадлежности ($x \in S_i$) — путь.
- Сертификат непринадлежности ($x \notin S_i$):
  - $|S_i|$ (тоже надо сертифицировать!),
  - все вершины S_i с сертификатами принадлежности.
- Сертификат размера $|S_i|$:
  - знаем $|S_{i-1}|$ (сертифицируем по индукции),
  - перебираем все вершины u, выясняя $u \in S_i$ так:

$u_1 \overset{?}{\in} S_i$
u_2
$\vdots$
u_k

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

STCON $\in$ **co-NL**

$t \notin S_{n-1}$ $|S_{n-1}|$, пути для $u \in S_{n-1}$ проверили $|S_{n-2}|$, пути

- Сертифицируем отсутствие пути между вершинами s и t.
- $S_i = \{$вершин на расстоянии $\leq i$ от $s\}$.
- Сертификат принадлежности ($x \in S_i$) — путь.
- Сертификат непринадлежности ($x \notin S_i$):
  - $|S_i|$ (тоже надо сертифицировать!),
  - все вершины S_i с сертификатами принадлежности.
- Сертификат размера $|S_i|$:
  - знаем $|S_{i-1}|$ (сертифицируем по индукции),
  - перебираем все вершины u, выясняя $u \in S_i$ так:
    - перебираем все вершины v, проверяя $(v, u) \in E$ и требуя сертификат принадлежности (путь) для $v \in S_{i-1}$. либо 0 ($v \notin S_{i-1}$)
    - заодно подсчитываем количество правильных сертификатов, должно сойтись с $|S_{i-1}|$.

$u \in S_i$?

v_1

$s \rightsquigarrow v_2 \to u$ $v_2 \in S_{i-1}$

v_k

u v' $S_i \ldots, v$ $S_i \ldots v'$

память
- переписывание
- арифметика $|S_i|$
- сч. вершин в пути
- обр. к входу

$u \notin S_i$ когда перебрали все v, $|S_{i-1}|$, не нашлось

Замкнутость **NSpace** относительно дополнения

Immerman, Szelepcsényi

Теорема

$\mathtt{STCON} \in \mathbf{co\text{-}NL}$

Следствие

Если $s(n) = \Omega(\log n)$, то $\mathbf{NSpace}[s(n)] = \mathbf{co\text{-}NSpace}[s(n)]$.

M

достижимость, $2^{s(n)}$ конф.

$\log 2^{s(n)} = s(n)$

PSPACE = NPSPACE