Введение в теорию сложности вычислений

Эдуард Алексеевич Гирш

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

СПбГУ и ПОМИ РАН

лекция 3 декабря 2020 г.

Теорема Карпа-Липтона

Теорема

NP $\subseteq$ **P**/**poly** $\Rightarrow$ **PH** $= \Sigma^2\mathbf{P}$.

Покажем, что $\Sigma^3\mathbf{P}$-полный язык

$$\mathtt{QBF}_3 = \{F - \text{формула в КНФ} \mid \exists x \forall y \exists z \; F(x, y, z)\}.$$

лежит в $\Sigma^2\mathbf{P}$.

Теорема Карпа-Липтона

Теорема

NP $\subseteq$ **P**/**poly** $\Rightarrow$ **PH** $= \Sigma^2\mathbf{P}$.

Покажем, что $\Sigma^3\mathbf{P}$-полный язык

$$\mathtt{QBF}_3 = \{F - \text{формула в КНФ} \mid \exists x \forall y \exists z\ F(x, y, z)\}.$$

лежит в $\Sigma^2\mathbf{P}$.

Проверка корректности схем для SAT:

$$C_{|G|}(G) \stackrel{?}{=} C_{|G[x_1:=0]|}(G[x_1 := 0]) \vee C_{|G[x_1:=1]|}(G[x_1 := 1])$$

и проверка корректности для тривиальных формул.

Теорема Карпа-Липтона

Теорема

$\mathbf{NP} \subseteq \mathbf{P/poly} \Rightarrow \mathbf{PH} = \Sigma^2\mathbf{P}$.

Покажем, что $\Sigma^3\mathbf{P}$-полный язык

$$\mathtt{QBF}_3 = \{F \text{ — формула в КНФ} \mid \exists x \forall y \exists z\ F(x, y, z)\}.$$

лежит в $\Sigma^2\mathbf{P}$.

$\exists x_1 \exists x_2 \cdots \quad \forall y_1 \forall y_2 \cdots$

$(\exists x \forall y \exists z\ F) \in \mathtt{QBF}_3 \Leftrightarrow$
$\exists$ схемы $C_1, \ldots, C_{|F|}$ (размера $\le$ пр полин. из условия)
$\exists x$
$\forall y$
$\forall G$ — булевой формулы длины $\le |F|$
(семейство $\{C_i\}$ корректно для G) $\wedge\ C_{|F|}(F(x, y, z)) = 1$.

Σ_2

Схемы фиксированного полиномиального размера

Теорема

$\forall k \quad \Sigma^4\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

(не P/poly) 2^{2^n} vs $2^{k \log n}$

Из соображений мощности имеется $f : \{0,1\}^n \to \{0,1\}$, зависящая от первых $c \cdot k \cdot \log n$ битов, для которой нет булевой схемы размера n^k.

Сконструируем такую функцию в $\Sigma^4\mathbf{P}$.

$$y \in L \iff \exists f \; \forall c \; (\text{схемы размера } n^k) \qquad \exists x \qquad :$$
$$\underbrace{f(x) \neq c(x)}_{\text{не принимается схемой}} \qquad .$$

Схемы фиксированного полиномиального размера

Теорема

$\forall k \;\; \Sigma^4\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

Из соображений мощности имеется $f : \{0,1\}^n \to \{0,1\}$, зависящая от первых $c \cdot k \cdot \log n$ битов, для которой нет булевой схемы размера n^k.

Сконструируем такую функцию в $\Sigma^4\mathbf{P}$.

$$y \in L \iff \exists f \; \forall c \; (\text{схемы размера } n^k) \quad \exists x \quad : \underbrace{f(x) \neq c(x)}_{\text{не принимается схемой}} \wedge \underbrace{f(y) = 1}_{\text{значение}}.$$

Схемы фиксированного полиномиального размера

Теорема

$\forall k \;\; \Sigma^4\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

Из соображений мощности имеется $f : \{0,1\}^n \to \{0,1\}$, зависящая от первых $c \cdot k \cdot \log n$ битов, для которой нет булевой схемы размера n^k.

Сконструируем такую функцию в $\Sigma^4\mathbf{P}$.

$$y \in L \iff \exists f \; \forall c \; (\text{схемы размера } n^k) \; \forall f' \; \exists x \exists c' \; (\text{схема}\ldots) \;\; \forall x' : \underbrace{f(x) \neq c(x)}_{\text{не принимается схемой}} \;\; \wedge \underbrace{((f \leq f') \vee f'(x') = c'(x'))}_{\text{первая такая } f} \;\; \wedge \underbrace{f(y) = 1}_{\text{значение}}.$$

Схемы фиксированного полиномиального размера

Теорема

$\forall k \;\; \Sigma^4\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

Из соображений мощности имеется $f : \{0,1\}^n \to \{0,1\}$, зависящая от первых $c \cdot k \cdot \log n$ битов, для которой нет булевой схемы размера n^k.

Сконструируем такую функцию в $\Sigma^4\mathbf{P}$.

$$y \in L \iff \exists f \; \forall c \; (\text{схемы размера } n^k) \; \forall f' \; \exists x \exists c' \; (\text{схема}\ldots) \;\; \forall x' : \underbrace{f(x) \neq c(x)}_{\text{не принимается схемой}} \wedge \underbrace{((f \leq f') \vee f'(x') = c'(x'))}_{\text{первая такая } f} \wedge \underbrace{f(y) = 1}_{\text{значение}}.$$

Остаётся превратить n^k в $O(n^k)$.

Схемы фиксированного полиномиального размера

Теорема

$\forall k \quad \Sigma^4\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

Следствие

$\forall k \quad \Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$.

$\Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \subseteq \mathbf{Size}[n^k] \Rightarrow$
$\mathbf{NP} \subseteq \mathbf{P/poly} \Rightarrow$ Т. Карпа-Липтона
$\mathbf{PH} = \Sigma^2\mathbf{P} \cap \Pi^2\mathbf{P} \subseteq \mathbf{Size}[n^k]$.

Σ^4 ?

Открыто: $NP \stackrel{?}{\subseteq} Size[n^k]$

Классы

$\mathbf{DTime}(f(n))$ $\mathbf{DSpace}(f(n))$

$\mathbf{NTime}(f(n))$ $\mathbf{NSpace}(f(n))$

NSpace

$$\mathbf{NSpace}[f(n)] = \{L \mid L \text{ принимается НМТ с памятью } O(f(n))\}.$$

Замечание

- $f(n)$ должна быть конструируемая по памяти,
- входная лента read-only, выходная лента write-only, память там не в счёт,
- **в определении НМТ “с подсказкой” лента подсказки читается слева направо!**

$$\mathbf{NPSPACE} = \bigcup_{k \geq 0} \mathbf{NSpace}[n^k].$$

Классы

$\mathbf{DTime}(f(n))$	$\mathbf{DSpace}(f(n))$
$\mathbf{NTime}(f(n))$	$\mathbf{NSpace}(f(n))$

P	**PSPACE**
NP	**NPSPACE**
co-NP	**co-NPSPACE**
EXP	**EXPSPACE**

Классы

$\mathbf{DTime}(f(n))$	$\mathbf{DSpace}(f(n))$
$\mathbf{NTime}(f(n))$	$\mathbf{NSpace}(f(n))$

$\mathbf{P}$	$\mathbf{PSPACE}$
$\mathbf{NP}$	$\mathbf{NPSPACE}$
$\mathbf{co\text{-}NP}$	$\mathbf{co\text{-}NPSPACE}$
$\mathbf{EXP}$	$\mathbf{EXPSPACE}$

$$\mathbf{L} = \mathbf{DSpace}(\log n)$$
$$\mathbf{NL} = \mathbf{NSpace}(\log n)$$

STCON; **NSpace** vs **DSpace**

$$\texttt{STCON} = \{(G, s, t) \mid G \text{ — ор.граф, } s \rightsquigarrow t\}.$$

Лемма

$\texttt{STCON} \in \mathbf{DSpace}[\log^2 n]$.

? PATH(s,t, log|V|)

$$\mathrm{PATH}(x, y, i) = \exists \text{ путь из } x \text{ в } y \text{ длины не более } 2^i.$$

$$\mathrm{PATH}(x, y, i) = \bigvee_z (\mathrm{PATH}(x, z, i-1) \wedge \mathrm{PATH}(z, y, i-1)).$$

PATH(x,y,0) = ((x,y)∈E) ✓

PATH(x,x,i) = 1

(s,t) for z = z1, z2 ...

(s,z1) (z1,z2) ... (zi-1,t) (z1,p1) (p1,t) ... (zi-2,t) (zi-2,t)

= 1

STCON; **NSpace** vs **DSpace**

$$\texttt{STCON} = \{(G, s, t) \mid G \text{ — ор.граф, } s \rightsquigarrow t\}.$$

Лемма

$\texttt{STCON} \in \mathbf{DSpace}[\log^2 n]$.

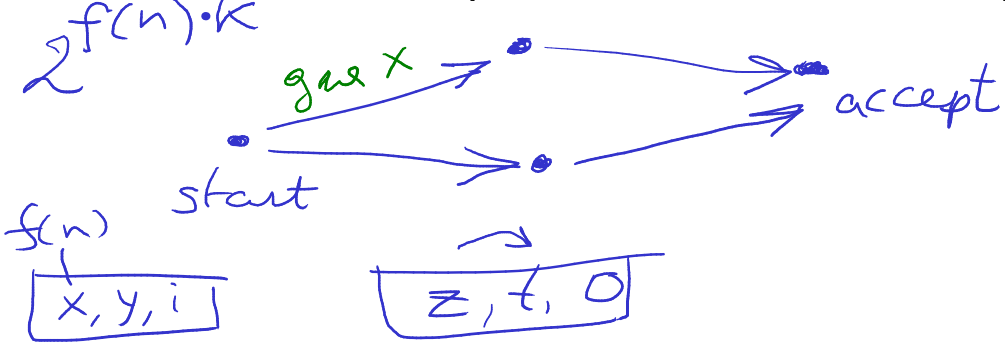
Теорема

$\mathbf{NSpace}(f) \subseteq \mathbf{DSpace}(f^2)$ для $f(n) = \Omega(\log n)$.

НМТ M $M(x)=1$

Достижимость в графе псевдоконфигураций (вх., вых. не входят).

1) состояние q
2) содержимое раб. лент
3) положение головок (в т.ч. на вх.)



Следствие

$\mathbf{PSPACE} = \mathbf{NPSPACE}$.

STCON; **NSpace** vs **DSpace**

$$\texttt{STCON} = \{(G, s, t) \mid G \text{ — ор.граф, } s \rightsquigarrow t\}.$$

Лемма

$\texttt{STCON} \in \mathbf{DSpace}[\log^2 n]$.

Лемма

STCON является **NL**-полной (относительно logspace-сведéний!).

$\in NL$

$s - x_1 - x_2 - \ldots t$

не храним

$NL \to STCON$

НМТ M, log space

$M(x) = 1 \iff$ start $\rightsquigarrow$ accept

Сведение $x \longmapsto$ граф, ребро есть/нет с учётом x

STCON; **NSpace** vs **DSpace**

$$\texttt{STCON} = \{(G, s, t) \mid G \text{ — ор.граф, } s \rightsquigarrow t\}.$$

Лемма

$\texttt{STCON} \in \mathbf{DSpace}[\log^2 n]$.

Лемма

STCON является **NL**-полной (относительно logspace-сведéний!).

Факт: для неор.графов: $\texttt{USTCON} \in \mathbf{L}$ [Reingold, 2004].

Вопрос на засыпку: а кто **L**-полная?

Классы

$\mathbf{DTime}(f(n))$	$\mathbf{DSpace}(f(n))$
$\mathbf{NTime}(f(n))$	$\mathbf{NSpace}(f(n))$

$\mathbf{P}$	$\mathbf{PSPACE}$
$\mathbf{NP}$	$\mathbf{NPSPACE}$
$\mathbf{co\text{-}NP}$	$\mathbf{co\text{-}NPSPACE}$
$\mathbf{EXP}$	$\mathbf{EXPSPACE}$

$$\mathbf{L} = \mathbf{DSpace}(\log n)$$
$$\mathbf{NL} = \mathbf{NSpace}(\log n)$$

Классы

$\mathbf{DTime}(f(n))$	$\mathbf{DSpace}(f(n))$
$\mathbf{NTime}(f(n))$	$\mathbf{NSpace}(f(n))$

$\mathbf{P}$	$\mathbf{PSPACE}$
$\mathbf{NP}$	$\mathbf{NPSPACE}$
$\mathbf{co\text{-}NP}$	$\mathbf{co\text{-}NPSPACE}$
$\mathbf{EXP}$	$\mathbf{EXPSPACE}$

$$\mathbf{L} = \mathbf{DSpace}(\log n)$$
$$\mathbf{NL} = \mathbf{NSpace}(\log n)$$

$\mathbf{P/poly}$	(non-uniform)

Равномерные полиномиальные схемы

. . . и параллельные вычисления

Семейство схем $\{C_n\}_{n\in\mathbb{N}}$ равномерно,
если имеется полиномиальный алгоритм A, т.ч. $A(1^n) = C_n$.

Замечание

Ясно, что равномерные полиномиальные схемы задают **P**.

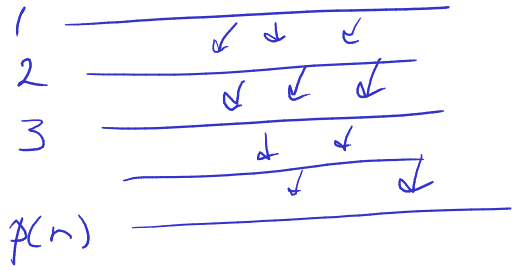
$M(x)$: $C := A(1^{|x|})$

$C(x)$

M – полин. МТ

$n = |x|$

$p(n)$



Равномерные полиномиальные схемы

. . . и параллельные вычисления

Семейство схем $\{C_n\}_{n\in\mathbb{N}}$ равномерно,
если имеется полиномиальный алгоритм A, т.ч. $A(1^n) = C_n$.

Замечание

Ясно, что равномерные полиномиальные схемы задают $\mathbf{P}$.

Logspace-равномерные: A использует память $O(\log n)$.

Равномерные полиномиальные схемы

. . . и параллельные вычисления

Семейство схем $\{C_n\}_{n\in\mathbb{N}}$ равномерно,
если имеется полиномиальный алгоритм A, т.ч. $A(1^n) = C_n$.

Замечание

Ясно, что равномерные полиномиальные схемы задают $\mathbf{P}$.

Logspace-равномерные: A использует память $O(\log n)$.

Глубина схемы $\sim$ время параллельного вычисления.

Nick's class

$$\mathbf{NC}^i = \left\{ L \;\middle|\; \begin{array}{l}\text{для } L \text{ есть logspace-равномерные} \\ \text{схемы глубины } O(\log^i n)\end{array} \right\}.$$

$$\mathbf{NC} = \bigcup_i \mathbf{NC}^i \subseteq \mathbf{P}.$$

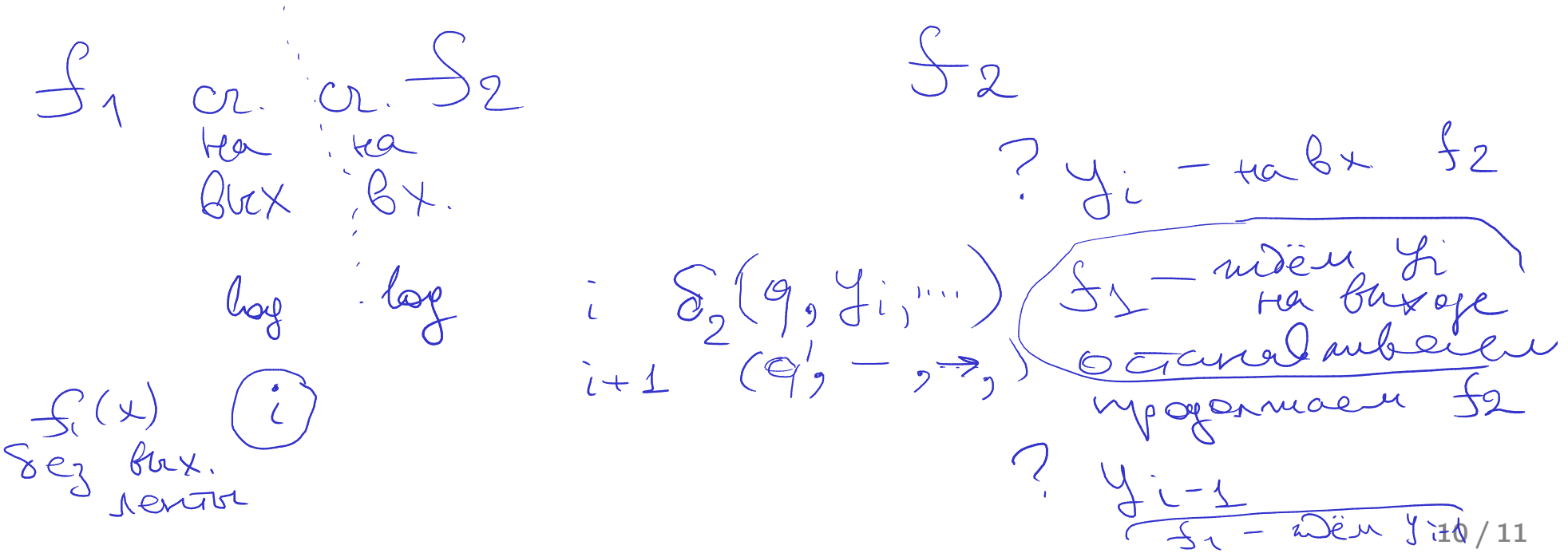
P-полнота

Лемма

Композиция двух logspace функций $f_2(f_1(x))$ в logspace.

- Сделать выходную ленту f_1 входной лентой f_2 нельзя.
- Храним только счётчики позиций.
- Нужен очередной бит входа f_2 — ~~продолжим работу~~ запустим f_1.
  (Если лента не write-once, можно доводить до конца каждый раз.)

$t_2 \cdot t_1$



P-полнота

Лемма

Композиция двух logspace функций $f_2(f_1(x))$ в logspace.

- Сделать выходную ленту f_1 входной лентой f_2 нельзя.
- Храним только счётчики позиций.
- Нужен очередной бит входа f_2 — продолжим работу f_1.
  (Если лента не write-once, можно доводить до конца каждый раз.)

Теорема

Если L — **P**-полный, то

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