Введение в теорию сложности вычислений

Эдуард Алексеевич Гирш

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

СПбГУ и ПОМИ РАН

лекция 12 ноября 2020 г.

НМТ

Инструкции k-ленточной ДМТ можно записать как функцию (таблицу)

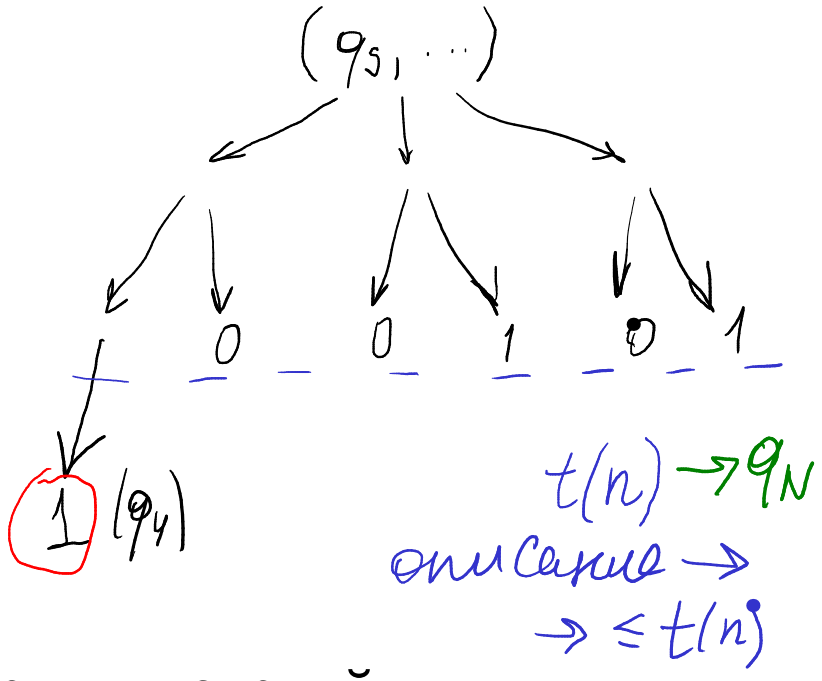
$$\delta\colon Q \times \Sigma^k \to Q \times \Sigma^k \times \{\leftarrow, \rightarrow, \cdot\}^k.$$

время ~ длина самого длинного пути

Недетерминированная машина Тьюринга (НМТ) допускает больше одной инструкции для данных $q \in Q$ и $c_1, \ldots, c_k \in \Sigma$, т.е. δ для неё — многозначная функция.

$(q, c) \to (q', c')$
$\searrow (q'', c'')$

Так появляется дерево вычислений...



В машины (ДМТ, НМТ) с заведомо ограниченным временем работы можно встроить будильник и считать время вычислений на входах одной длины всегда одним и тем же.

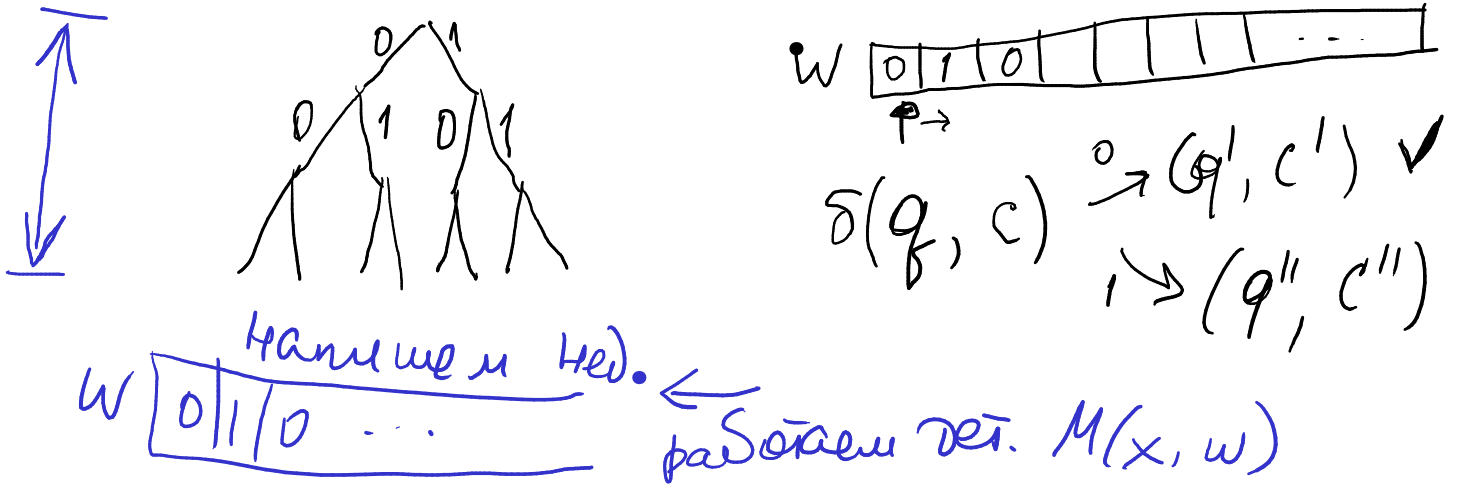
НМТ принимает вход, если $\exists$ путь в дереве вычислений, заканчивающийся q_Y.

НМТ и **NP** — другие определения (эквивалентные)

Недетерминированная машина Тьюринга (НМТ) — это просто ДМТ, у которой есть дополнительный аргумент (подсказка w) на второй ленте).

НМТ M принимает вход x, если $\exists w$, для которой вычисление заканчивается в q_Y (пишем $M(x, w) = 1$).

Вычислительный путь в старом определении $\sim$ подсказка в новом.
Можно считать, что длина подсказки определяется длиной входа.



НМТ и **NP** — другие определения (эквивалентные)

Недетерминированная машина Тьюринга (НМТ) — это просто ДМТ, у которой есть дополнительный аргумент (подсказка w на второй ленте).

НМТ M принимает вход x, если $\exists w$, для которой вычисление заканчивается в q_Y (пишем $M(x, w) = 1$).

Вычислительный путь в старом определении $\sim$ подсказка в новом.
Можно считать, что длина подсказки определяется длиной входа.

Ещё одно определение **NP**:
NP — класс языков, принимаемых полиномиальными по времени НМТ.

$x \in L \Leftrightarrow \exists w R(x, w)$

Сведéния (Сводимости)

many-one

Сведение языков по Карпу: $L_1 \to L_2$, если имеется полиномиально вычислимая f:

- $\forall x\ x \in L_1 \Leftrightarrow f(x) \in L_2$.

f, h
A, MT
output tape

Сведение задач поиска по Левину: $R_1 \to R_2$, если $\exists f, g, h\ \forall x_1, y_1, y_2$

- $R_1(x_1, y_1) \Rightarrow R_2(f(x_1), g(x_1, y_1))$,
- $R_1(x_1, h(f(x_1), y_2)) \Leftarrow R_2(f(x_1), y_2)$,
- f и h полиномиально вычислимы, а g ~~ограничена полиномом~~.

y_1 длина → $g(x_1, y_1)$

тоже

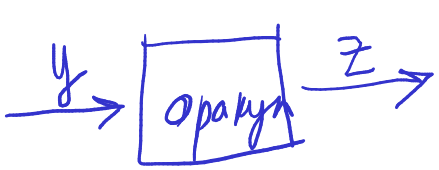
Классы **P**, **NP**, $\widetilde{\mathbf{P}}$, $\widetilde{\mathbf{NP}}$ замкнуты относительно этих сведений.

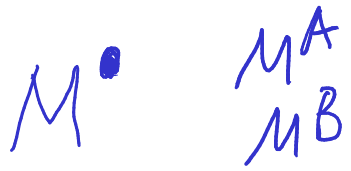
$R_2 \in \mathcal{P}$, $\widetilde{NP}$ $\quad R_1 \to R_2 \quad \Rightarrow \quad R_1 \in \widetilde{P}$, $\widetilde{NP}$

R_2 - п.о. h.n. $x \to y$

R_1 - п.о. h.n.

Сведéния (Сводимости)



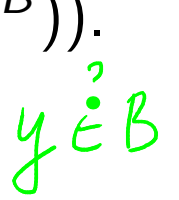


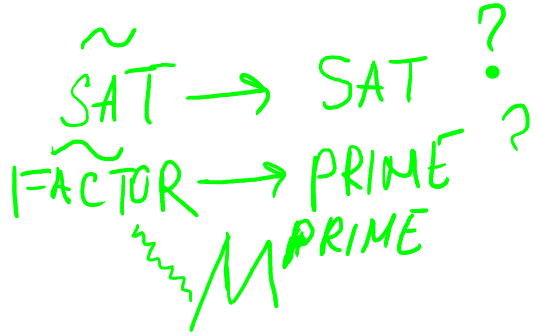
Оракульная МТ имеет доступ к оракулу, который за 1 шаг даёт ей ответ на вопрос.

Формально: состояния q_{in}, q_{out} и "фантастический переход" из q_{in} в q_{out}, заменяющий содержимое [третьей] ленты на ответ оракула.

M^B — оракульная машина M, которой дали конкретный оракул B.

Сведение чего угодно по Тьюрингу: $A \to B$, если имеется оракульная полиномиальная по времени машина $M^{\bullet}$, такая, что M^B решает A (например, если A — язык, то $A = L(M^B)$).





Сведéния (Сводимости)

Сведение языков по Карпу: $L_1 \to L_2$, если имеется полиномиально вычислимая f:

- $\forall x\ x \in L_1 \Leftrightarrow f(x) \in L_2$.

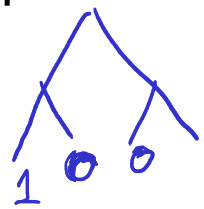
Сведение задач поиска по Левину: $R_1 \to R_2$, если $\exists f, g, h\ \forall x_1, y_1, y_2$

- $R_1(x_1, y_1) \Rightarrow R_2(f(x_1), g(x_1, y_1))$,
- $R_1(x_1, h(f(x_1), y_2)) \Leftarrow R_2(f(x_1), y_2)$,
- f и h полиномиально вычислимы, а g ограничена полиномом.

$B = SAT \quad M^O(x) = \overline{x \in O}$

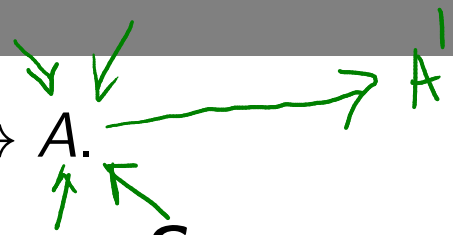
$A = UNSAT$

Сведение чего угодно по Тьюрингу: $A \to B$, если имеется оракульная полиномиальная по времени машина $M^\bullet$, такая, что M^B решает A (например, если A — язык, то $A = L(M^B)$).



Классы $\mathbf{P}$, $\widetilde{\mathbf{P}}$ замкнуты относительно этих сведений.
Классы $\mathbf{NP}$, $\widetilde{\mathbf{NP}}$ могут быть незамкнуты относительно сведений по Тьюрингу.

Трудные и полные задачи



Задача A — трудная для класса $\mathbf{C}$, если $\forall C \in \mathbf{C} \quad C \to A$.

Задача — полная для $\mathbf{C}$, если она трудная и принадлежит $\mathbf{C}$.

Теорема

Если

- A — $\mathbf{NP}$-трудная,
- $A \in \mathbf{P}$,

то $\mathbf{P} = \mathbf{NP}$.

Следствие

Если A — $\mathbf{NP}$-полная, то

$$A \in \mathbf{P} \Leftrightarrow \mathbf{P} = \mathbf{NP}.$$

NP-полная задача: BH

Задача об ограниченной остановке:

$\widetilde{\mathrm{BH}}(\langle M, x, 1^t \rangle, w) =$ НМТ M с подсказкой w принимает вход x за $\leq t$ шагов

Теорема

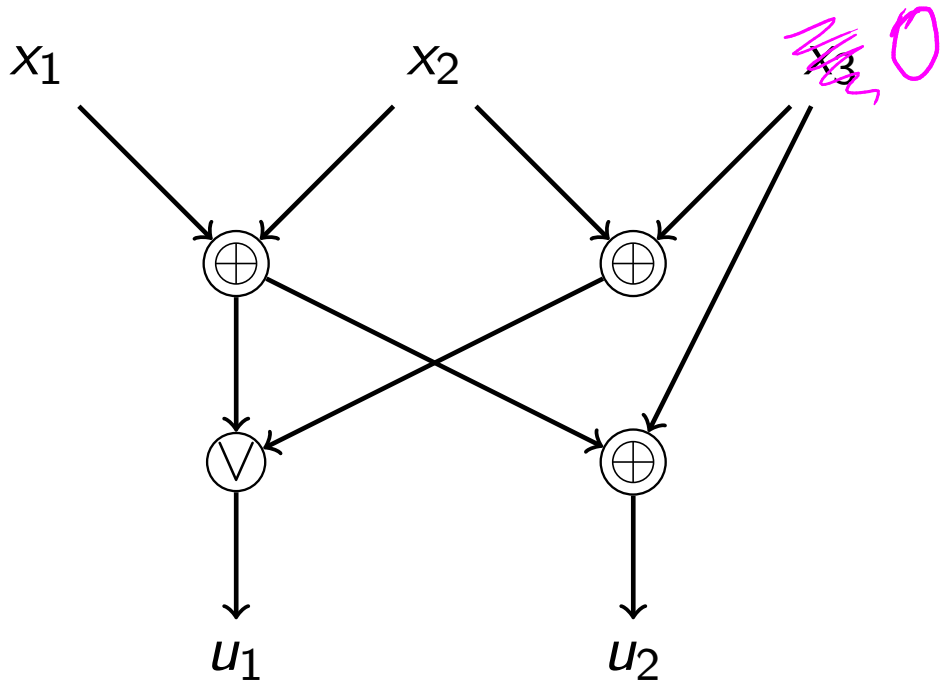
Задача об ограниченной остановке — $\widetilde{\mathbf{NP}}$-полная,
а соответствующий язык — **NP**-полный.

Замечание

Принадлежность $\widetilde{\mathbf{NP}}$ использует существование универсальной ДМТ, которая может эффективно промоделировать вычисление ДМТ, описание которой дано ей на вход.

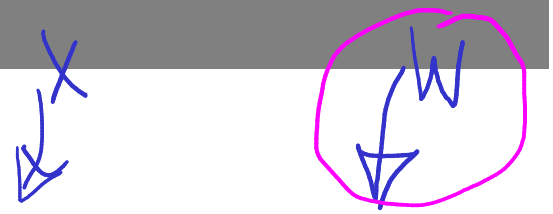
Булева схема

- Ориентированный граф без циклов.
- Бинарные (и унарные, 0-арные) операции над битами: $\wedge$, $\vee$, $\oplus$, ...
- Пример (4 гейта):



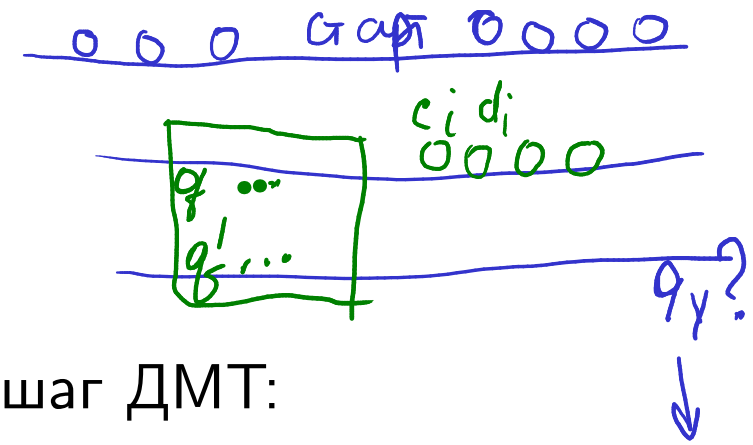
NP-полная задача: CIRCUIT_SAT

$$\widetilde{\text{CIRCUIT\_SAT}} = \{(C, w) \mid C \text{ — схема},\ C(w) = 1\}.$$



BH $\to$ CIRCUIT_SAT:

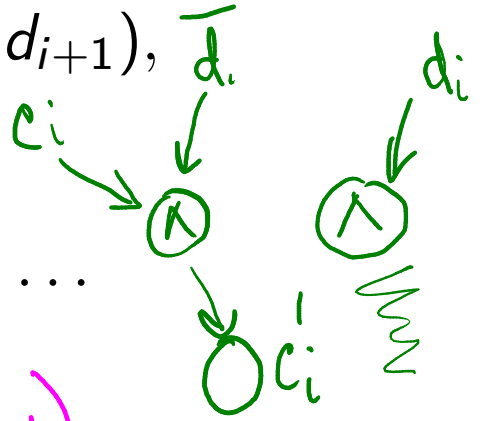
- этаж схемы — конфигурация ДМТ;
- время $t \Rightarrow t$ больших этажей схемы;
- время $t \Rightarrow t$ ячеек на этаже;
- переход между этажами реализует один шаг ДМТ:



$$(q', c_i', d_i') \leftarrow\!\shortmid (q, c_{i-1}, c_i, c_{i+1}, d_{i-1}, d_i, d_{i+1}),$$

где d_j, d_j' — «головка в j-й позиции»:

c :	c_1	c_2	$\dots$	c_{i-1}	c_i	c_{i+1}	$\dots$
d :	·	·		·	↑	·	
					q		



- входы схемы — подсказка НМТ (вход НМТ уже подставлен).
- выход схемы — попадание в q_Y.