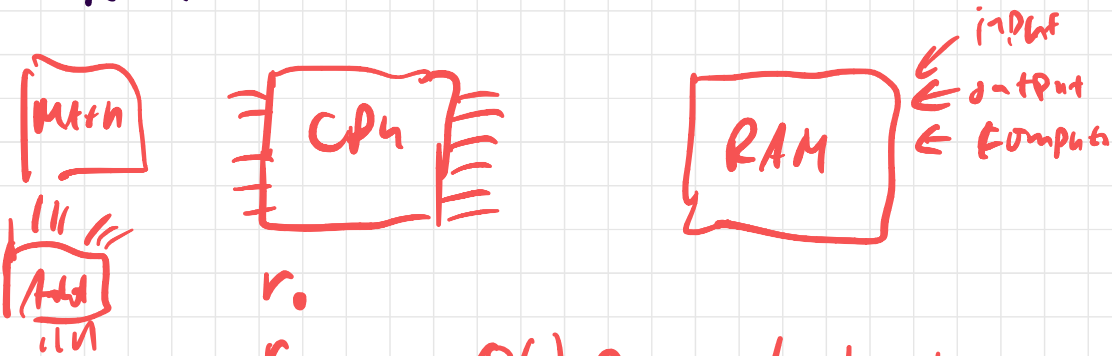
Теория сложности

Модели вычислений

$O(n^2)$, $O(n)$

RAM



r_0

r_1

$\vdots$

r_{15}

неогр. битности

$O(1)$ r_0 = load r_1

// r_0 = RAM[r_1]

$O(1)$ put r_1 r_0

// RAM[r_1] = r_0

$O(1)$ r_0 = add r_1 r_2

$O(1)$ * r_0 = mult r_1 r_2

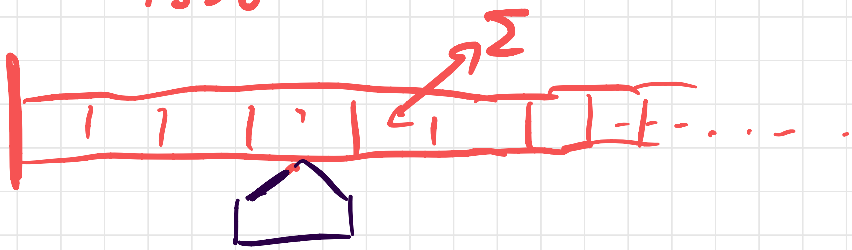
word-RAM

$r_0 \ldots r_{15}$ ограничены W-бит

$w > \log_2$ input

Машина Тьюринга

1936



$q \in Q$ – конечное

– мн-во состояний

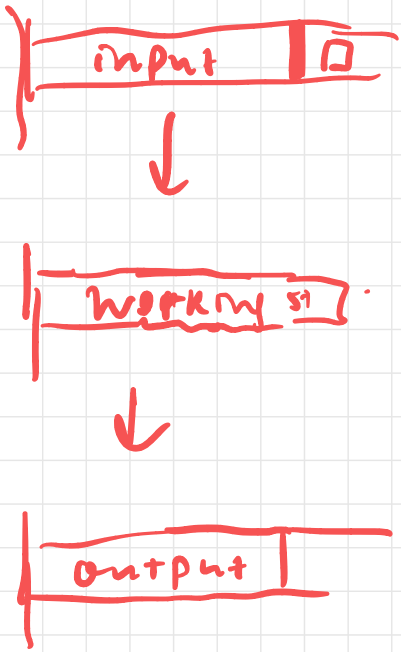
вычислителя

$$\delta : \Sigma \times Q \to \{\leftarrow, \cdot, \rightarrow\} \times \Sigma$$

$q_{stop} \in Q$

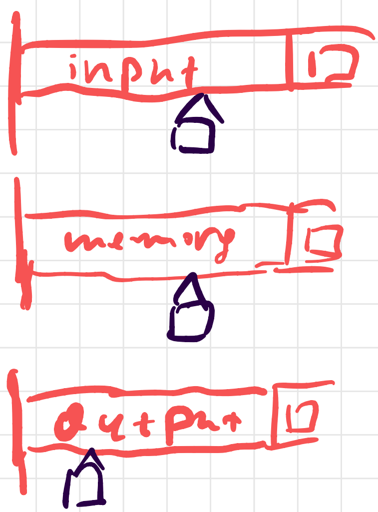
и всё останавливается когда

М.Т. переходит q_{stop}



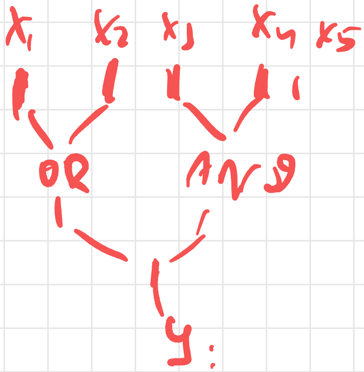
$q = q_{stop}$

Многоленточная М.Т.

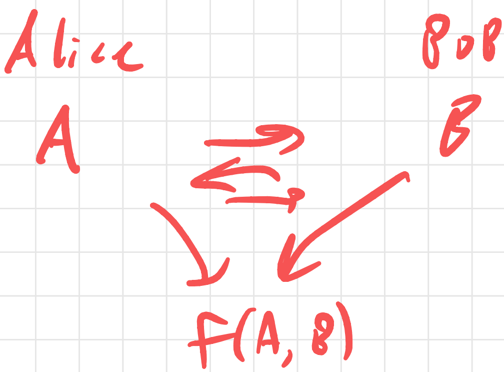


$$\delta : Q \cdot \Sigma^3 \to \{\leftarrow, \cdot, \to\}^3 \cdot \Sigma^3$$

Схемная сложность



Коммуникац. сложность

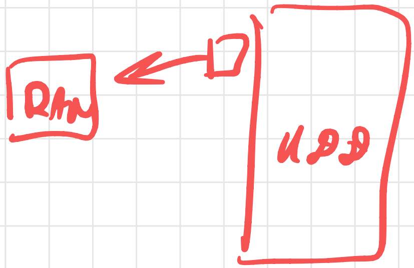


$A \subseteq V(G)$ — клика

$B \subseteq V(G)$ — нез. мн-во

$$A \cap B \stackrel{?}{=} \emptyset$$

Внешняя память



1TB int sort

4GB int

Decision и Search

decision: input → {0, 1}

NO/YES

G → ∃ гц в G

гам. путь

Search: input → output

output соотв. input

G, s, t → кр. путь от s до t как последов. вершин.

пример: G, k → ∃ ли в графе незав. мн-во $\geq k$

decision

пример: G → max k, что ∃ незав. мн-во размера k

search

search → decision

⇓

изучаем decision задачи

decision : $f: \{0,1\}^* \to \{0,1\}$

$L = \{ s \in \{0,1\}^* \mid f(s) = 1 \}$

Теория сложности (decision задачи)

$DTime(f) = \{ L \subseteq \{0,1\}^* \mid$ L можно решить за $O(f) \}$ (М. Т.)

$DTime(n)$ = можно решить за $O(n)$

$$P = \bigcup_{k=1}^{\infty} DTime(n^k)$$

$$EXP = \bigcup_{k=1}^{\infty} DTime(2^{n^k})$$

$P \subseteq EXP$, т.к. $DTime(n^k) \subseteq DTime(2^n)$

Класс P

Утв: P не зависит от того poly(n) - время работы на М.Т или на RAM.

Временная иерархия

Утв: $DTime(f) \subsetneq DTime(f \log^2 f)$

Rem: "$\log^2 f$" следств. исп. М.Т. Для других моделей может быть другой фактор

Следств: $P \subsetneq EXP$

$$DTime(n^k) \subseteq DTime(2^n)$$
$$\Downarrow$$
$$P \subseteq DTime(2^n) \subsetneq DTime(2^{n^2}) \subseteq EXP$$

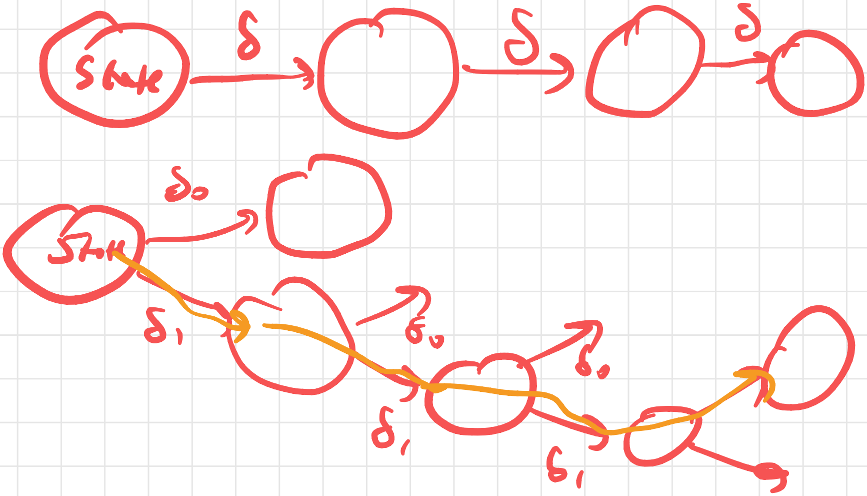
Класс NP

М.Т. : $\delta : Q \cdot \Sigma \to \{\leftarrow, \cdot, \to\} \times \Sigma$

Н.М.Т. : $\delta_0, \delta_1 : Q \cdot \Sigma \to \{\leftarrow, \cdot, \to\} \times \Sigma$

М.Т.

Н.М.Т.



М.Т. $x \in L$, если М.Т. остановилась в q_{stop} и на ленте записано $\boxed{1}$

Н.М.Т. $x \in L$, если $\exists$ посл недетерм. выборов, что мы остановились с

$$\boxed{1}$$

$$P = \{ L \mid \exists \text{ М.Т. решающая } L \text{ за } poly(n) \}$$

$$NP = \{ L \mid \exists \text{ Н.М.Т. решающая } L \text{ за } poly(n) \}$$

$$P = \bigcup_{k=1}^{\infty} DTime(n^k)$$

$$NP = \bigcup_{k=1}^{\infty} NTime(n^k)$$

Альтернативное определение

P: $prog(x) = 1/0$, prog раб. за poly(n)

$$L_{prog} = \{x \in \{0,1\}^* \mid prog(x) = 1\}$$

NP: $prog(x, y) = 1/0$

инпут (x), подсказка (y)

prog работает за $poly(|x|)$

$$L_{prog} = \{x \in \{0,1\}^* \mid \exists y \in \{0,1\}^*,$$
что $prog(x,y) = 1\}$

Утв: HAMPATH $\in$ NP

HAMPATH = $\{G \mid \exists$ гам. путь в $G\}$

Д-во: $prog(G, y) =$

| если y явл. посл.

вершин в G, обр.
гам. путь, вернуть 1
иначе вернуть 0

$$L_{prog} = \{ G \mid \exists y : \ prog(x, y) = 1 \}$$

$SAT \in NP$

SAT: $(x \vee y) \wedge (\neg x \vee y \vee z) = \varphi$

$SAT \in NP$, потому что

$prog(\varphi, y) =$

проверить, правда ли
что y явл. вып.
набором для φ.
если да вернуть Y,
иначе N

$P \subseteq NP$

$P \overset{1}{\subseteq} NP \overset{2}{\subseteq} EXP$

$y \leq g(|x|)$ $\quad 2^{|y|}$

$P \subsetneq EXP$

никто не знает про 1 и 2

$P \overset{?}{=} NP$, $NP \overset{?}{=} EXP$

Эквив. двух определений NP

#2

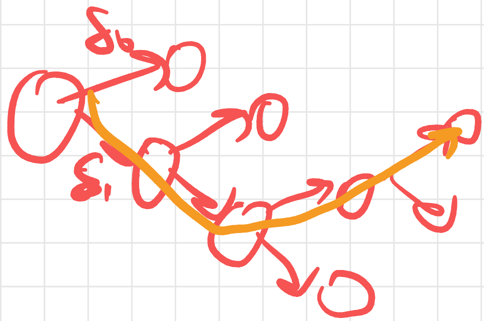
Prog работает за $poly(|x|) = g$

$L_{prog} = \{x \in \{0,1\}^* \mid \exists y \in \{0,1\}^*,$

что $prog(x,y) = 1\}$

#1

$NP = \{ L \mid \exists$ Н.М.Т решающая L за $Poly(n) \}$



Форм. редукция

#1 → #2

$L \in NP_1$: $\exists$ Н.М.Т. решающая L

$\Downarrow$

$L \in NP_2$: $\exists$ prog :

$x \in L \iff \exists y$: $prog(x, y) = 1$

prog(x, y):

```
for y_i ∈ y
    if y_i = 0
        сделать переход δ_0 в Н.М.Т
```

else
сделать переход δ_1 в Н.М.Т.

#2 → #1

$L \in NP_1$: $\exists$ Н.М.Т. решающая L

$\Uparrow$

$L \in NP_2$: $\exists$ prog :

$x \in L \Leftrightarrow \exists y: prog(x, y) = 1$

Prog, нужно построить Н.М.Т.

Н.М.Т. будет $poly(|x|)$ шагов выбирать был переход по δ_0 или δ_1

назовём это y.

Полиномиальное сведение

$L_A, L_B \subseteq \{0,1\}^*$

Def $L_A \leq_p L_B$, если

$\exists f : \{0,1\}^* \to \{0,1\}^*$,

$f(s)$ вычислима за $poly(|s|)$

и

$x \in L_A \iff f(x) \in L_B$

пример

$L_A = \{(G,k) \mid$ что в G $\exists$ нез. мн-во размера $k\}$

$L_B : \{(G,k) \mid$ что в G $\exists$ клика размера $k\}$

$L_A \leq L_B$

$G = \Delta$

$(G, 3) \in L_B, \quad (G, 3) \notin L_A$

$(G, k) \in L_A \Leftrightarrow (\bar{G}, k) \in L_B$

$f((G, k)) = (\bar{G}, k)$

$3\text{-}SAT \leq SAT$

$f(\varphi) = \varphi$

$\varphi \in 3\text{-}SAT \Leftrightarrow f(\varphi) \in SAT$

$(x \vee y \vee z)$

$$f(\varphi) = \begin{cases} \varphi, & \text{если } \varphi \text{ синт. корр.} \\ x \wedge \neg x, & \text{если синт. некорр.} \end{cases}$$

NP hard, NP complete

$$NP\text{hard} = \{ L \subseteq \{0,1\}^* \mid \forall L' \in NP \quad L' \leq_{f_{L',L}} L \}$$

$$NP\text{complete} = NP\text{hard} \cap NP$$

Утв: (Stephen Cook, Levin, 1971)

$SAT \in NP\text{complete}$

// $SAT \in NP$

// интересно $NP \neq \emptyset$

// $SAT \in NPh$

Утв: (Richard Karp, 1972)

3-SAT, VERTEX COVER, SET-COVER, KNAPSACK, MAX-CUT, HAM CYCLE, ...

(21 задача)

$\Uparrow$

NP complete

Ни для одной из этих задач неизвестно Poly решение, но при этом если $\exists$ poly решение для одной из них, то оно $\exists$ и для всех остальных.

CoNP

$NP = \{L \mid \exists\ prog(x,y) : (x \in L \Leftrightarrow$

$\exists y : prog(x,y) = 1)\}$

$$coNP = \{L \in \{0,1\}^* \mid \overline{L} \in NP\}$$

$$coA = \{L \subseteq \{0,1\}^* \mid \overline{L} \in A\}$$

<u>Пример.</u> $SAT \in NP$

$$\overline{SAT} \in coNP$$

$$coNP = \{L \mid \exists prog(x,y) : (x \notin L \Leftrightarrow \exists y : prog(x,y) = 1)\}$$

<u>Пример!</u> $\overline{SAT} \in coNP$.

Сертификат того, что $\varphi \notin \overline{SAT}$
||
выпл. набор