Booleovské obvody a výpočty s nápovědou

3 January, 2022 08:55

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

uniformní algoritmus A: $\forall x \in \{0,1\}^* \to A(x) = f(x)$

neuniformní algoritmus A pro f: $A = \{A_n\}_{n \geq 0}$

$f = \{f_n\}_{n \geq 0}$

$F_n = f | \{0,1\}^n$

A_n počítá F_n

tj. $\forall x \in \{0,1\}^n \to A_n(x) = f_n(x) = F(x)$

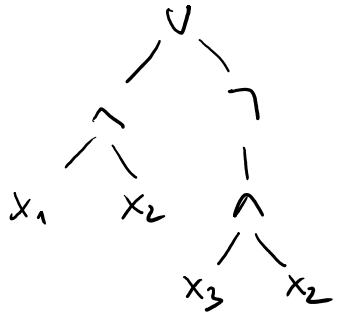
Př: 1) A_n má v sobě tabulku hodnot pro f_n

2) A_n má v sobě prvočíslo pro hešování dat velikosti n.

3) A_n používá jiný postup na vstupech sudé a liché délky

neuniformní modely výpočtu:

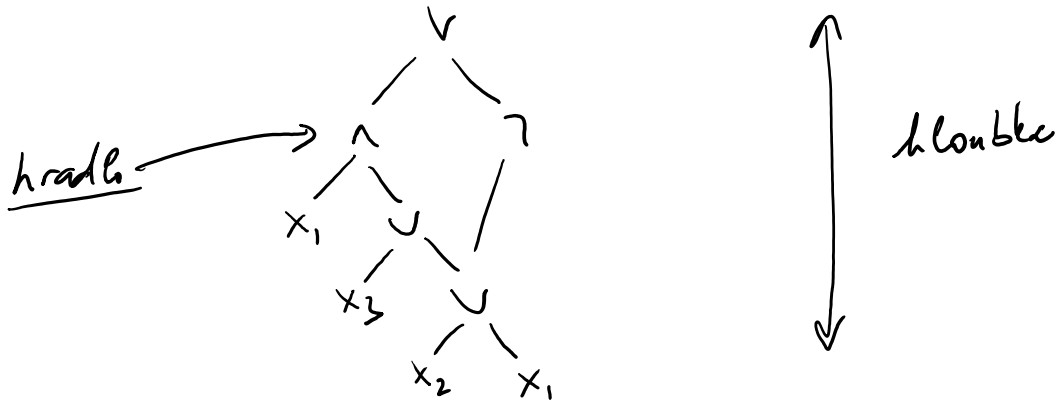
- Booleovská formule



$f_5(x_1 x_2 x_3) = \dots$

posloupnost formulí $\{\phi_n\}_{n \geq 0}$, ϕ_n počítá f_n.

- **Booleovské obvody**



velikost obvodu ... počet hradel

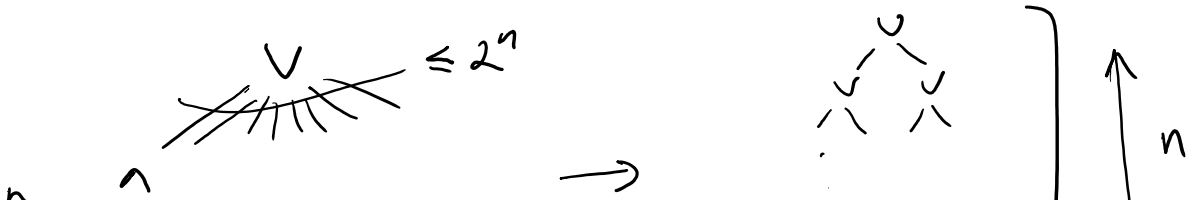
posloupnost obvodů $\{C_n\}_{n\geq 0}$, C_n počítá f_n

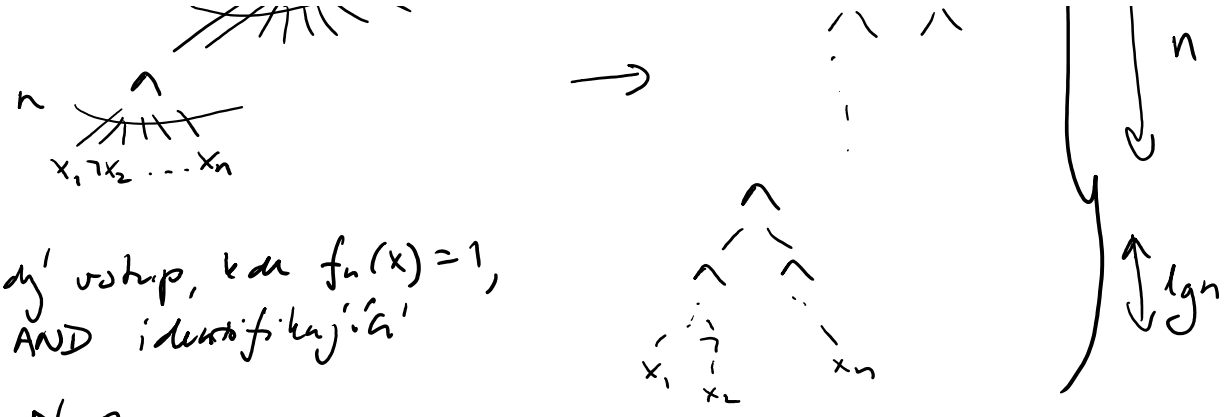
- **další modely**: rozhodovací stromy (decision trees),
  branching programy
  aritmetické výrazy
  polynomy
  ...

→ **zajímá nás** velikost, hloubka, šířka, ... obvodu, fle, ...
jak roste s velikostí vstupu.

Věta: $\forall f_n : \{0,1\}^n \to \{0,1\}$ existuje obvod složený z binárních hradel AND, OR a unárního NOT, který počítá f_n a je velikosti $\leq 10n2^n$.

Dk: Obvod implementuje DNF nebo CNF formuli pro f_n.





pro každý vstup, kde $f_n(x) = 1$, jedno AND identifikující tento vstup.

- velikost obvodu se dá zlepšit na $O(2^n/n)$.

Věta: $\exists f_n : \{0,1\}^n \to \{0,1\}$ t.ž. nejmenší obvod s binárním AND, OR a unárním NOT, který počítá f_n, je velikosti alespoň $\frac{2^n}{10n}$.

Dk: počítací argument

- 2^{2^n} různých fcí $F_n : \{0,1\}^n \to \{0,1\}$
- počet obvodů velikosti s

$$\leq s^{2s} \cdot (n+3)^s = (*)$$

(s^{2s}: # spojnic / grafů obvodu; $(n+3)^s$: # možných hradel)

pro $s = \frac{2^n}{10n}$ je $(*) \leq \left(2^n\right)^{2 \cdot \frac{2^n}{10n}} \cdot (n+3)^{\frac{2^n}{10n}}$

$$\leq 2^{\frac{2^n}{5}} \cdot 2^{\frac{2^n}{10}} \ll 2^{2^n}$$

$\Rightarrow$ většina funkcí $f_n : \{0,1\}^n \to \{0,1\}$ potřebuje obvod velikosti $\frac{2^n}{10n}$.

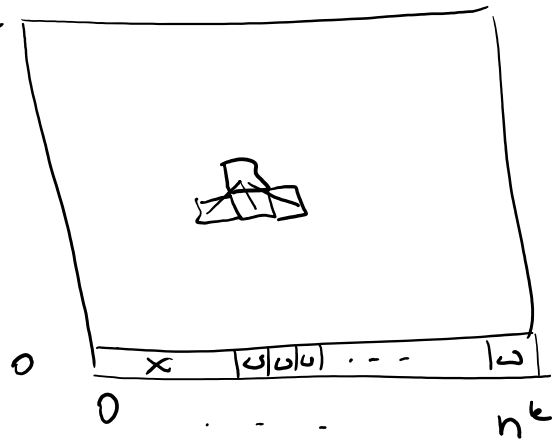
• $\forall f : \{0,1\}^* \to \{0,1\}$ existuje posloupnost obvodů $\{C_n\}_{n\geq 0}$ počítající f, kde velikost $C_n \leq O(2^n/n)$.

Otázka: $f \in NP \Rightarrow f$ má posloupnost obvodů polynomiální velikosti ?
(t.j. $|C_n| \leq n^{O(1)}$.)

Domněnka: SAT nelze počítat obvody polynomiální velikosti.

Věta: $f \in P \Rightarrow f$ má polynomiálně velké obvody.

Dk:



$\longrightarrow$ obvod velikosti $O(n^{2k}) = O(1) \cdot n^k \times n^k$ ∎

Důsledek: NP nemá polynomiálně velké obvody $\Longrightarrow P \neq NP$.

Domněnka (Kolmogorov): Funkce v P mají lineárně velké obvody.

" nejlepší dolní odhad: $\exists f \in P$ t.ž. že její obvody jsou velikosti $\geq 5n$.

Def: $s(n) : \mathbb{N} \to \mathbb{N}$ $\quad SIZE(s(n)) = \{ f : \{0,1\}^* \to \{0,1\},$
$\exists \{c_n\}_{n \geq 0}$, c_n počítá f_n
a $|c_n| \leq s(n) \}$

$$P \subseteq \bigcup_{k \geq 0} SIZE(n^k + k)$$

Zpět k algoritmům: radící fce $g : \mathbb{N} \to \{0,1\}^*$

- algoritmus A + radící fce g
- pr: výpočet na vstupu délky n dostane A zadarmo $g(n)$, t.j. A dostane $(x, g(|x|))$ jako svůj vstup.
- měříme délku $|g(n)|$

$P/poly$ ... funkce pro které existuje algoritmus A pracující v polynomiálním čase s radící fcí $g : \mathbb{N} \to \{0,1\}^*$, kde $|g(n)| \leq n^k$, pro nějakou konstantu k.

obecněji:

$P/f(n)$ ... —//—

$|g(n)| \leq f(n)$.

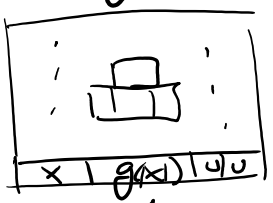
Věta: $\forall f : \{0,1\}^* \to \{0,1\}$ $\quad f \in P/poly \iff$
f má obvody polynomiální velikosti.

Dk:

Dk:

$^n\Leftarrow^n$ ... $g(n)$ = popis obvodu C_n
A vyhodnotí $C_{|x|}$ na vstupu x.

$^n\Rightarrow^n$ ... $g(n)$ se "zadrátuje" do obvodu vzniklého z výpočetní tabulky do prvního řádku



Věta: $\forall k \geq 0 \quad \exists f \in EXP$ tž. $f \notin SIZE(n^k + k)$.

Dk: Algoritmus A pro f:

na vstupu x délky n

mějme $a_0 = \overbrace{00\ldots0}^{n}$, $a_1 = 00\ldots01$, ... $a_{2^n-1} = \overbrace{11\ldots1}^{n}$.

$C_0 = \{C : C$ je obvod velikosti $\leq n^k + k$ a vstupy $x_1, \ldots x_n\}$

$i = 0$

opakuj dokud $C_i \neq \emptyset$ & $i < 2^n$:

- pokud většina obvodů v C_i dává na a_i výstup 0, definuj $t_i = 1$ jinak $t_i = 0$.
- $C_{i+1} = \{C \in C_i : C(a_i) = t_i\}$
- $i = i + 1$.

Pokud vstup $x = a_j$ pro $j < i$, pak výstup t_j, jinak výstup 0.

· Algoritmus A je v EXP, pracuje v $DTIME(2^{n^{2k}})$

· Žádná posloupnost obvodů $\{C_n\}_{n\geq 0}$ velikosti $\leq n^k + k$ nepočítá stejnou fci jako A

Věta: $\exists f \in DTIME(2^{n \lg n})$ t.ž. $\forall k$ $f \notin SIZE(n^k + k)$
t.j. $f \notin P/poly$.

Dk: modifikace důkazu výše pro obvody velikosti $n^{\frac{\lg n}{2}}$.

$\Rightarrow$ $EEXP \not\subseteq P/poly$

Otázka: $NP \not\subseteq P/poly$?