Redukcie

kuko

24.2.2021

Pokročilá teória zložitosti

- Čo je ťažšie: násobenie $x \cdot y$, alebo umocňovanie na druhú: x^2?
- Čo je ťažšie: utriediť n čísel alebo spočítať konvexný obal množiny bodov?
- Čo je ťažšie: ofarbiť planárny graf 3 farbami (pričom susedné vrcholy musia mať rôznu farbu) alebo ofarbiť ľubovoľný graf?

- Čo je ťažšie: násobenie $x \cdot y$, alebo umocňovanie na druhú: x^2?
- Čo je ťažšie: utriediť n čísel alebo spočítať konvexný obal množiny bodov?
- Čo je ťažšie: ofarbiť planárny graf 3 farbami (pričom susedné vrcholy musia mať rôznu farbu) alebo ofarbiť ľubovoľný graf?

- Čo je ťažšie: násobenie $x \cdot y$, alebo umocňovanie na druhú: x^2?
- Čo je ťažšie: utriediť n čísel alebo spočítať konvexný obal množiny bodov?
- Čo je ťažšie: ofarbiť planárny graf 3 farbami (pričom susedné vrcholy musia mať rôznu farbu) alebo ofarbiť ľubovoľný graf?

Redukcie

Definícia

A je polynomiálne redukovateľný na B, píšeme $A \leq_{\mathrm{m}}^{\mathrm{P}} B$, ak existuje zobrazenie σ vypočítateľné v polynomiálnom čase:
$x \in A \Longleftrightarrow \sigma(x) \in B$.
Podobne A je logspace redukovateľný na B, $A \leq_{\mathrm{m}}^{\mathrm{log}} B$, ak sa zobrazenie σ dá vypočítať v logaritmickom priestore.

Redukcie

Definícia

A je polynomiálne redukovateľný na B, píšeme $A \leq_{\mathrm{m}}^{\mathrm{P}} B$*, ak existuje zobrazenie* σ *vypočítateľné v polynomiálnom čase:*
$x \in A \Longleftrightarrow \sigma(x) \in B$.
Podobne A je logspace redukovateľný na B, $A \leq_{\mathrm{m}}^{\mathrm{log}} B$*, ak sa zobrazenie* σ *dá vypočítať v logaritmickom priestore.*

Redukcie

Definícia

- *L je* NP*-ťažký, ak* $A \leq_{\mathrm{m}}^{\log} L$ *pre každý* $A \in$ NP.
- *L je* NP*-úplný, ak je* NP*-ťažký a patrí do* NP
- *všeobecne, ak* $\leq$ *je redukcia a* $\mathscr{C}$ *trieda problémov, tak*
- *L je* $\mathscr{C}$*-ťažký (pri* $\leq$ *redukcii), ak* $A \leq L$ *pre každé* $A \in \mathscr{C}$
- *L je* $\mathscr{C}$*-úplný, ak L navyše patrí do* $\mathscr{C}$

Redukcie

Definícia

- *L je* NP*-ťažký, ak* $A \leq_{\mathrm{m}}^{\log} L$ *pre každý* $A \in$ NP*.*
- *L je* NP*-úplný, ak je* NP*-ťažký a patrí do* NP
- *všeobecne, ak* $\leq$ *je redukcia a* $\mathscr{C}$ *trieda problémov, tak*
- *L je* $\mathscr{C}$*-ťažký (pri* $\leq$ *redukcii), ak* $A \leq L$ *pre každé* $A \in \mathscr{C}$
- *L je* $\mathscr{C}$*-úplný, ak L navyše patrí do* $\mathscr{C}$

Redukcie

Definícia

- *L je* NP*-ťažký, ak* $A \leq_{\mathrm{m}}^{\log} L$ *pre každý* $A \in \mathrm{NP}$.
- *L je* NP*-úplný, ak je* NP*-ťažký a patrí do* NP
- *všeobecne, ak $\leq$ je redukcia a $\mathscr{C}$ trieda problémov, tak*
- *L je $\mathscr{C}$-ťažký (pri $\leq$ redukcii), ak $A \leq L$ pre každé $A \in \mathscr{C}$*
- *L je $\mathscr{C}$-úplný, ak L navyše patrí do $\mathscr{C}$*

Redukcie

Definícia

- *L je NP-ťažký, ak $A \leq_{\mathrm{m}}^{\log} L$ pre každý $A \in$ NP.*
- *L je NP-úplný, ak je NP-ťažký a patrí do NP*
- *všeobecne, ak $\leq$ je redukcia a $\mathscr{C}$ trieda problémov, tak*
- *L je $\mathscr{C}$-ťažký (pri $\leq$ redukcii), ak $A \leq L$ pre každé $A \in \mathscr{C}$*
- *L je $\mathscr{C}$-úplný, ak L navyše patrí do $\mathscr{C}$*

Redukcie

Definícia

- L *je* NP-*ťažký, ak* $A \leq_{\mathrm{m}}^{\log} L$ *pre každý* $A \in$ NP.
- L *je* NP-*úplný, ak je* NP-*ťažký a patrí do* NP
- *všeobecne, ak* $\leq$ *je redukcia a* $\mathscr{C}$ *trieda problémov, tak*
- L *je* $\mathscr{C}$-*ťažký (pri* $\leq$ *redukcii), ak* $A \leq L$ *pre každé* $A \in \mathscr{C}$
- L *je* $\mathscr{C}$-*úplný, ak* L *navyše patrí do* $\mathscr{C}$

NP-úplné

Veta (Cook-Levin)

SAT *je* NP*-úplný.*

Výpočet

$\vdash$	$\overset{\rightarrow}{\mathtt{a}}$	$\mathtt{b}$	$\mathtt{b}$	$\mathtt{a}$	$\dashv$
$\vdash$	$\sqcup$	$\overset{\vec{\mathtt{a}}}{\mathtt{b}}$	$\mathtt{b}$	$\mathtt{a}$	$\dashv$
$\vdash$	$\sqcup$	$\mathtt{b}$	$\overset{\vec{\mathtt{a}}}{\mathtt{b}}$	$\mathtt{a}$	$\dashv$
$\vdash$	$\sqcup$	$\mathtt{b}$	$\mathtt{b}$	$\overset{\vec{\mathtt{a}}}{\mathtt{a}}$	$\dashv$
$\vdash$	$\sqcup$	$\mathtt{b}$	$\mathtt{b}$	$\mathtt{a}$	$\overset{\vec{\mathtt{a}}}{\dashv}$
$\vdash$	$\sqcup$	$\mathtt{b}$	$\mathtt{b}$	$\overset{\mathtt{a}}{\mathtt{a}}$	$\dashv$
$\vdash$	$\sqcup$	$\mathtt{b}$	$\overset{\leftarrow}{\mathtt{b}}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\overset{\leftarrow}{\mathtt{b}}$	$\mathtt{b}$	$\sqcup$	$\dashv$
$\vdash$	$\overset{\leftarrow}{\sqcup}$	$\mathtt{b}$	$\mathtt{b}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\overset{\rightarrow}{\mathtt{b}}$	$\mathtt{b}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\overset{\vec{\mathtt{b}}}{\mathtt{b}}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\mathtt{b}$	$\overset{\vec{\mathtt{b}}}{\sqcup}$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\overset{\mathtt{b}}{\mathtt{b}}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\overset{\leftarrow}{\sqcup}$	$\sqcup$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\overset{\rightarrow}{\sqcup}$	$\sqcup$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\sqcup$	$\overset{a}{\sqcup}$	$\dashv$
$\vdash$	$\sqcup$	$\sqcup$	$\sqcup$	$\sqcup$	$\overset{a}{\dashv}$
$\vdash$	$\sqcup$	$\sqcup$	$\sqcup$	$\sqcup$	$\overset{A}{\dashv}$

Premenné

- $Q^q_{i,j}$ – v i-tom kroku je hlava na j-tom políčku v stave q a
- $S^a_{i,j}$ – v i-tom kroku je na j-tom políčku symbol a.

Klauzuly

- na každom políčku je práve jeden symbol:

$$\bigvee_{a \in \Gamma} S^a_{i,j} \qquad \textit{(aspoň jeden)}$$

$$\text{pre } a \neq b: \qquad \overline{S^a_{i,j}} \vee \overline{S^b_{i,j}} \qquad \textit{(najviac jeden).}$$

- hlava je v každom kroku na práve jednom políčku v práve jednom stave:

$$\bigvee_{\substack{q \in Q \\ 0 < j \leq N+1}} Q^q_{i,j} \qquad \textit{(aspoň jeden)}$$

$$\text{pre } j \neq j',\ p \neq q: \qquad \overline{Q^p_{i,j}} \vee \overline{Q^q_{i,j'}} \qquad \textit{(najviac jeden).}$$

Klauzuly

- na každom políčku je práve jeden symbol:

$$\bigvee_{a\in\Gamma} S^a_{i,j} \qquad \textit{(aspoň jeden)}$$

$$\text{pre } a \neq b: \qquad \overline{S^a_{i,j}} \vee \overline{S^b_{i,j}} \qquad \textit{(najviac jeden).}$$

- hlava je v každom kroku na práve jednom políčku v práve jednom stave:

$$\bigvee_{\substack{q\in Q\\ 0<j\leq N+1}} Q^q_{i,j} \qquad \textit{(aspoň jeden)}$$

$$\text{pre } j \neq j',\ p \neq q: \qquad \overline{Q^p_{i,j}} \vee \overline{Q^q_{i,j'}} \qquad \textit{(najviac jeden).}$$

Klauzuly

- počiatočná konfigurácia začína v stave q_0 (podľa M) a na páske je $\vdash x_1 x_2 \cdots x_n \sqcup\sqcup\sqcup \cdots \sqcup \dashv$:

$$Q_{1,1}^{q_0} \wedge S_{1,0}^{\vdash} \wedge S_{1,1}^{x_1} \wedge S_{1,2}^{x_2} \wedge \cdots \wedge S_{1,n}^{x_n} \wedge \bigwedge_{n<j\leq N} S_{1,j}^{\sqcup} \wedge S_{1,N+1}^{\dashv}$$

- ak na políčku j nie je hlava, v nasledujúcom kroku bude na políčku rovnaký symbol:

$$(S_{i,j}^{a} \wedge (\overline{Q_{i,j}^{q_1}} \wedge \cdots \wedge \overline{Q_{i,j}^{q_k}})) \to S_{i+1,j}^{a}$$

- ak $\delta(p,a) = (q,b,d)$, tak

$$(S_{i,j}^{a} \wedge Q_{i,j}^{p}) \to (S_{i+1,j}^{b} \wedge Q_{i+1,j+d}^{q}).$$

- výpočet je akceptačný:

$$Q_{N,1}^{ACCEPT}.$$

Klauzuly

- počiatočná konfigurácia začína v stave q_0 (podľa M) a na páske je $\vdash x_1 x_2 \cdots x_n \sqcup\sqcup\sqcup \cdots \sqcup \dashv$:

$$Q^{q_0}_{1,1} \wedge S^{\vdash}_{1,0} \wedge S^{x_1}_{1,1} \wedge S^{x_2}_{1,2} \wedge \cdots \wedge S^{x_n}_{1,n} \wedge \bigwedge_{n<j\leq N} S^{\sqcup}_{1,j} \wedge S^{\dashv}_{1,N+1}$$

- ak na políčku j nie je hlava, v nasledujúcom kroku bude na políčku rovnaký symbol:

$$(S^a_{i,j} \wedge (\overline{Q^{q_1}_{i,j}} \wedge \cdots \wedge \overline{Q^{q_k}_{i,j}})) \rightarrow S^a_{i+1,j}$$

- ak $\delta(p,a) = (q,b,d)$, tak

$$(S^a_{i,j} \wedge Q^p_{i,j}) \rightarrow (S^b_{i+1,j} \wedge Q^q_{i+1,j+d}).$$

- výpočet je akceptačný:

$$Q^{ACCEPT}_{N,1}.$$

Klauzuly

- počiatočná konfigurácia začína v stave q_0 (podľa M) a na páske je $\vdash x_1 x_2 \cdots x_n \sqcup\sqcup\sqcup \cdots \sqcup \dashv$:

$$Q_{1,1}^{q_0} \wedge S_{1,0}^{\vdash} \wedge S_{1,1}^{x_1} \wedge S_{1,2}^{x_2} \wedge \cdots \wedge S_{1,n}^{x_n} \wedge \bigwedge_{n<j\leq N} S_{1,j}^{\sqcup} \wedge S_{1,N+1}^{\dashv}$$

- ak na políčku j nie je hlava, v nasledujúcom kroku bude na políčku rovnaký symbol:

$$(S_{i,j}^{a} \wedge (\overline{Q_{i,j}^{q_1}} \wedge \cdots \wedge \overline{Q_{i,j}^{q_k}})) \to S_{i+1,j}^{a}$$

- ak $\delta(p,a) = (q,b,d)$, tak

$$(S_{i,j}^{a} \wedge Q_{i,j}^{p}) \to (S_{i+1,j}^{b} \wedge Q_{i+1,j+d}^{q}).$$

- výpočet je akceptačný:

$$Q_{N,1}^{ACCEPT}.$$

Klauzuly

- počiatočná konfigurácia začína v stave q_0 (podľa M) a na páske je $\vdash x_1 x_2 \cdots x_n \sqcup\sqcup\sqcup \cdots \sqcup \dashv$:

$$Q_{1,1}^{q_0} \wedge S_{1,0}^{\vdash} \wedge S_{1,1}^{x_1} \wedge S_{1,2}^{x_2} \wedge \cdots \wedge S_{1,n}^{x_n} \wedge \bigwedge_{n<j\leq N} S_{1,j}^{\sqcup} \wedge S_{1,N+1}^{\dashv}$$

- ak na políčku j nie je hlava, v nasledujúcom kroku bude na políčku rovnaký symbol:

$$(S_{i,j}^{a} \wedge (\overline{Q_{i,j}^{q_1}} \wedge \cdots \wedge \overline{Q_{i,j}^{q_k}})) \rightarrow S_{i+1,j}^{a}$$

- ak $\delta(p,a) = (q,b,d)$, tak

$$(S_{i,j}^{a} \wedge Q_{i,j}^{p}) \rightarrow (S_{i+1,j}^{b} \wedge Q_{i+1,j+d}^{q}).$$

- výpočet je akceptačný:

$$Q_{N,1}^{ACCEPT}.$$

Veta (Cook-Levin)

SAT *je* NP*-úplný.*

■ **Dôkaz.** Pre ľubovoľný jazyk $L \in \mathrm{NP}$ a NTS M, ktorý ho akceptuje, vieme spraviť formulu $\phi_M(x)$ takú, že

$$\phi_M(x) \in \textsc{Sat} \iff M(x) = 1 \iff x \in L.$$

□

NP-úplné

Veta

Nasledujúce problémy sú NP-*úplné:*

- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \textit{ je NTS, ktorý akceptuje } x \textit{ na } t \textit{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \textit{ je DTS} \wedge \exists\pi \in \{0,1\}^n : M(\pi) \textit{ akceptuje na } t \textit{ krokov}\}$,

NP-úplné

Veta

Nasledujúce problémy sú NP-*úplné:*

- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \textit{ je NTS, ktorý akceptuje } x \textit{ na } t \textit{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \textit{ je DTS} \wedge \exists \pi \in \{0,1\}^n : M(\pi) \textit{ akceptuje na } t \textit{ krokov}\}$,

NP-úplné

Veta

Nasledujúce problémy sú NP*-úplné:*

- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \textit{ je NTS, ktorý akceptuje } x \textit{ na } t \textit{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \textit{ je DTS} \wedge \exists\pi \in \{0,1\}^n : M(\pi) \textit{ akceptuje na } t \textit{ krokov}\}$,

NP-úplné

Veta

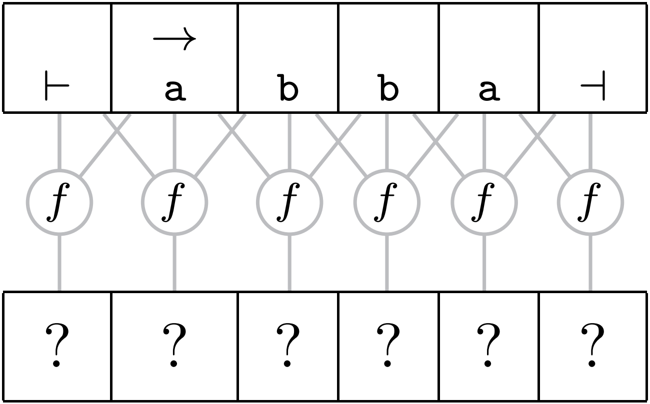
Nasledujúce problémy sú NP-*úplné:*

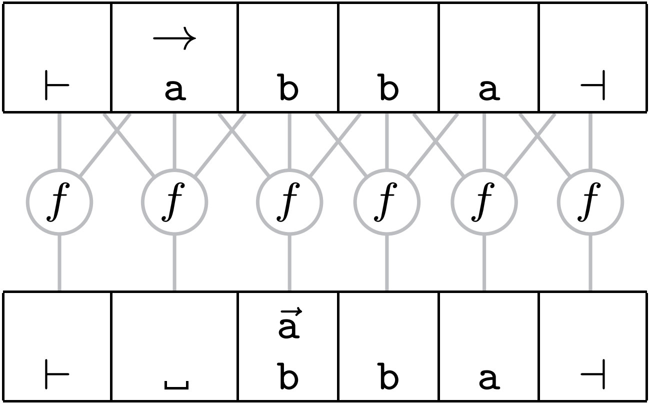
- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \textit{ je NTS, ktorý akceptuje } x \textit{ na } t \textit{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \textit{ je DTS} \wedge \exists\pi \in \{0,1\}^n : M(\pi) \textit{ akceptuje na } t \textit{ krokov}\}$,
- $\textsc{CircuitSat}$ – *daný je booleovský obvod* C*; existuje vstup, ktorý akceptuje?*

NP-úplné

⊢	→ a	b	b	a	⊣
⊢	␣	$\vec{\mathtt{a}}$ b	b	a	⊣
⊢	␣	b	$\vec{\mathtt{a}}$ b	a	⊣
⊢	␣	b	b	$\vec{\mathtt{a}}$ a	⊣
⊢	␣	b	b	a	$\vec{\mathtt{a}}$ ⊣
⊢	␣	b	b	a a	⊣
⊢	␣	b	← b	␣	⊣
⊢	␣	← b	b	␣	⊣
⊢	← ␣	b	b	␣	⊣
⊢	␣	→ b	b	␣	⊣
⊢	␣	␣	$\vec{\mathtt{b}}$ b	␣	⊣
⊢	␣	␣	b	$\vec{\mathtt{b}}$ ␣	⊣
⊢	␣	␣	b b	␣	⊣
⊢	␣	← ␣	␣	␣	⊣
⊢	␣	␣	→ ␣	␣	⊣
⊢	␣	␣	␣	a ␣	⊣
⊢	␣	␣	␣	␣	a ⊣
⊢	␣	␣	␣	␣	A ⊣

NP-úplné




⊢
→
a
b
b
a
⊣
f
f
f
f
f
f
⊢
␣
a⃗
b
b
a
⊣

NP-úplné

Veta

Nasledujúce problémy sú NP*-úplné:*

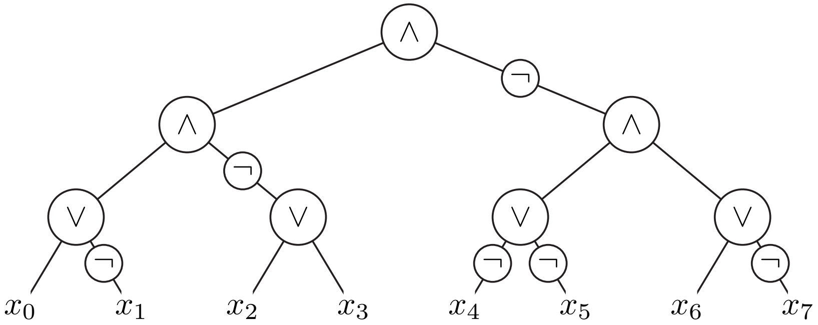
- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \textit{ je NTS, ktorý akceptuje } x \textit{ na } t \textit{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \textit{ je DTS} \wedge \exists\pi \in \{0,1\}^n : M(\pi) \textit{ akceptuje na } t \textit{ krokov}\}$,
- $\textsc{CircuitSat}$ – *daný je booleovský obvod C; existuje vstup, ktorý akceptuje?*
- $\textsc{Sat}$ – *je daná formula ϕ v CNF splniteľná?*

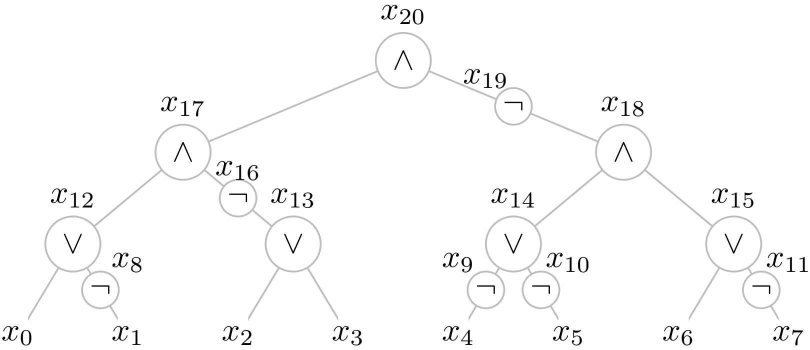
NP-úplné

Veta

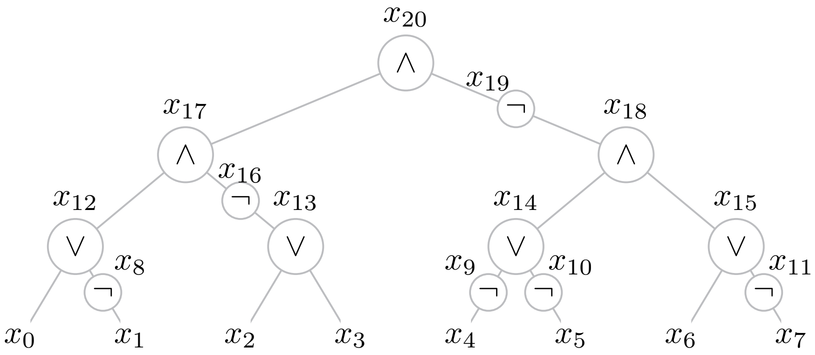
Nasledujúce problémy sú NP-úplné:

- $\textsc{NtmAcc} = \{\langle M\rangle\#x\#1^t \mid M \text{ je NTS, ktorý akceptuje } x \text{ na } t \text{ krokov}\}$,
- $\textsc{TmSat} = \{\langle M\rangle\#1^n\#1^t \mid M \text{ je DTS} \wedge \exists\pi \in \{0,1\}^n : M(\pi) \text{ akceptuje na } t \text{ krokov}\}$,
- $\textsc{CircuitSat}$ – *daný je booleovský obvod C; existuje vstup, ktorý akceptuje?*
- $\textsc{Sat}$ – *je daná formula ϕ v CNF splniteľná?*

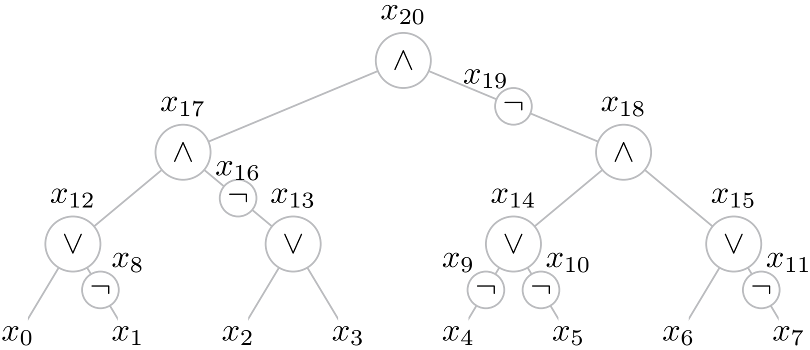

∧
¬
∧
∧
¬
∨
∨
∨
∨
¬
¬
¬
¬
x_0
x_1
x_2
x_3
x_4
x_5
x_6
x_7



- $x_{20} \wedge$
- $(x_{20} \leftrightarrow x_{17} \wedge x_{19}) \wedge$
- $(x_{19} \leftrightarrow \overline{x_{18}}) \wedge \cdots$



- $x_{20} \wedge$
- $(x_{17} \wedge x_{19} \to x_{20}) \wedge (\overline{x_{17}} \to \overline{x_{20}}) \wedge (\overline{x_{19}} \to \overline{x_{20}}) \wedge$
- $(x_{18} \to \overline{x_{19}}) \wedge (\overline{x_{18}} \to x_{19}) \wedge \cdots$



- $x_{20} \wedge$
- $(\overline{x_{17}} \vee \overline{x_{19}} \vee x_{20}) \wedge (x_{17} \vee \overline{x_{20}}) \wedge (x_{19} \vee \overline{x_{20}}) \wedge$
- $(\overline{x_{18}} \vee \overline{x_{19}}) \wedge (x_{18} \vee x_{19}) \wedge \cdots$

PSPACE-úplné

Veta

Nasledujúce problémy sú PSPACE-*úplné:*

- $\textsc{TmAcc}_{\textsc{Space}} = \{\langle M\rangle\#x\#1^s \mid M \text{ akceptuje } x \text{ v pamäti } s\}$,
- $\textsc{LbaAcc}$ – *daný je lineárne ohraničený automat M a vstup x; chceme zistiť, či M akceptuje x;*
- $\textsc{CsgGen}$ – *daná je kontextová gramatika G a slovo x; chceme zistiť, či G generuje x;*

Veta

Nasledujúce problémy sú PSPACE-*úplné:*

- $\textsc{TmAcc}_{\textsc{Space}} = \{\langle M\rangle\#x\#1^s \mid M \textit{ akceptuje } x \textit{ v pamäti } s\}$,
- $\textsc{LbaAcc}$ – *daný je lineárne ohraničený automat* M *a vstup* x; *chceme zistiť, či* M *akceptuje* x;
- $\textsc{CsgGen}$ – *daná je kontextová gramatika* G *a slovo* x; *chceme zistiť, či* G *generuje* x;

Veta

Nasledujúce problémy sú PSPACE-*úplné:*

- $\textsc{TmAcc}_{\textsc{Space}} = \{\langle M\rangle \# x \# 1^s \mid M \text{ akceptuje } x \text{ v pamäti } s\}$,
- $\textsc{LbaAcc}$ – *daný je lineárne ohraničený automat M a vstup x; chceme zistiť, či M akceptuje x;*
- $\textsc{CsgGen}$ – *daná je kontextová gramatika G a slovo x; chceme zistiť, či G generuje x;*

Veta

Nasledujúce problémy sú PSPACE-*úplné:*

- $\textsc{TmAcc}_{\textsc{Space}} = \{\langle M\rangle\#x\#1^s \mid M \text{ akceptuje } x \text{ v pamäti } s\}$,
- $\textsc{LbaAcc}$ – *daný je lineárne ohraničený automat M a vstup x; chceme zistiť, či M akceptuje x;*
- $\textsc{CsgGen}$ – *daná je kontextová gramatika G a slovo x; chceme zistiť, či G generuje x;*

Veta

Problém QBF *je* PSPACE-*úplný.*

Dôkaz.

- $\phi_i(a, b)$ – ak sa z konfigurácie a vieme dostať do b na $\leq i$ krokov
- ϕ_1 ako v Cook-Levinovej vete
- $x \in L \iff \phi_{2^{n^k}}(c_0, c_f) \in \mathrm{QBF}$.

Veta

Problém QBF *je* PSPACE-*úplný.*

■ **Dôkaz.**

- $\phi_i(a, b)$ – ak sa z konfigurácie a vieme dostať do b na $\leq i$ krokov
- ϕ_1 ako v Cook-Levinovej vete
- $x \in L \Longleftrightarrow \phi_{2^{n^k}}(c_0, c_f) \in \mathrm{QBF}.$

Veta

Problém QBF *je* PSPACE*-úplný.*

■ **Dôkaz.**

- $\phi_i(a, b)$ – ak sa z konfigurácie a vieme dostať do b na $\leq i$ krokov
- ϕ_1 ako v Cook-Levinovej vete
- $x \in L \iff \phi_{2^{n^k}}(c_0, c_f) \in \mathrm{QBF}$.

Veta

Problém QBF *je* PSPACE*-úplný.*

■ **Dôkaz.**

- $\phi_i(a, b)$ – ak sa z konfigurácie a vieme dostať do b na $\leq i$ krokov
- ϕ_1 ako v Cook-Levinovej vete
- $x \in L \iff \phi_{2^{n^k}}(c_0, c_f) \in \mathrm{QBF}$.

$\vdash$	$\rightarrow$ a	b	b	a	$\dashv$
$\vdash$	␣	$\vec{a}$ b	b	a	$\dashv$
$\vdash$	␣	b	$\vec{a}$ b	a	$\dashv$
$\vdash$	␣	b	b	$\vec{a}$ a	$\dashv$
$\vdash$	␣	b	b	a	$\vec{a}$ $\dashv$
$\vdash$	␣	b	b	a a	$\dashv$
$\vdash$	␣	b	$\leftarrow$ b	␣	$\dashv$
$\vdash$	␣	$\leftarrow$ b	b	␣	$\dashv$
$\vdash$	$\leftarrow$ ␣	b	b	␣	$\dashv$
$\vdash$	␣	$\rightarrow$ b	b	␣	$\dashv$
$\vdash$	␣	␣	$\vec{b}$ b	␣	$\dashv$
$\vdash$	␣	␣	b	$\vec{b}$ ␣	$\dashv$
$\vdash$	␣	␣	b b	␣	$\dashv$
$\vdash$	␣	$\leftarrow$ ␣	␣	␣	$\dashv$
$\vdash$	␣	␣	$\rightarrow$ ␣	␣	$\dashv$
$\vdash$	␣	␣	␣	a ␣	$\dashv$
$\vdash$	␣	␣	␣	␣	a $\dashv$
$\vdash$	␣	␣	␣	␣	A $\dashv$

ako v Savitchovej vete

$$\phi_{2i}(a,b) \equiv \exists c : \phi_i(a,c) \wedge \phi_i(c,b)$$

bez copy-pasty:

$$\phi_{2i}(a,b) \equiv \exists c : \phi_i(x,y), \text{ kde } (x,y) \text{ je buď } (a,c), \text{ alebo } (c,b)$$

$$\phi_{2i}(a,b) \equiv \exists c : \forall x,y : ([x,y] = [a,c] \vee [x,y] = [c,b]) \Rightarrow \phi_i(x,y)$$

$\square$

bez copy-pasty:

$$\phi_{2i}(a,b) \equiv \exists c : \phi_i(x,y), \text{ kde } (x,y) \text{ je buď } (a,c), \text{ alebo } (c,b)$$

$$\phi_{2i}(a,b) \equiv \exists c : \forall x,y : ([x,y]=[a,c] \vee [x,y]=[c,b]) \Rightarrow \phi_i(x,y)$$

$\square$

Veta

Problém ekvivalencie regulárnych výrazov (tzn. pre dané r_1, r_2, je $L(r_1) \neq L(r_2)$?) je PSPACE*-úplný.*

Dôkaz.

- patrí do PSPACE
- ťažkosť – redukciou z $\textsc{LbaAcc}$:
- $L(r_1) = \Gamma^*$, r_2 bude matchovať *všetko okrem* akceptačného výpočtu $M(x)$
- akceptačný výpočet zapíšeme ako reťazec

$$v = \#C_0\#C_1\#C_2\#\cdots\#C_t\#$$

nad abecedou $\Gamma = Q \cup \Sigma \cup \{\#\}$

Veta

Problém ekvivalencie regulárnych výrazov (tzn. pre dané r_1, r_2, je $L(r_1) \neq L(r_2)$?) je PSPACE*-úplný.*

■ **Dôkaz.**

- patrí do PSPACE
- ťažkosť – redukciou z LbaAcc:
- $L(r_1) = \Gamma^*$, r_2 bude matchovať *všetko okrem* akceptačného výpočtu $M(x)$
- akceptačný výpočet zapíšeme ako reťazec

$$v = \#C_0\#C_1\#C_2\#\cdots\#C_t\#$$

nad abecedou $\Gamma = Q \cup \Sigma \cup \{\#\}$

Veta

Problém ekvivalencie regulárnych výrazov (tzn. pre dané r_1, r_2, je $L(r_1) \neq L(r_2)$?) je PSPACE*-úplný.*

■ **Dôkaz.**

- patrí do PSPACE
- ťažkosť – redukciou z $\textsc{LbaAcc}$:
- $L(r_1) = \Gamma^*$, r_2 bude matchovať *všetko okrem* akceptačného výpočtu $M(x)$
- akceptačný výpočet zapíšeme ako reťazec

$$v = \#C_0\#C_1\#C_2\#\cdots\#C_t\#$$

nad abecedou $\Gamma = Q \cup \Sigma \cup \{\#\}$

Veta

Problém ekvivalencie regulárnych výrazov (tzn. pre dané r_1, r_2, je $L(r_1) \neq L(r_2)$?) je PSPACE*-úplný.*

■ **Dôkaz.**

- patrí do PSPACE
- ťažkosť – redukciou z $\textsc{LbaAcc}$:
- $L(r_1) = \Gamma^*$, r_2 bude matchovať *všetko okrem* akceptačného výpočtu $M(x)$
- akceptačný výpočet zapíšeme ako reťazec

$$v = \#C_0\#C_1\#C_2\#\cdots\#C_t\#$$

nad abecedou $\Gamma = Q \cup \Sigma \cup \{\#\}$

Veta

Problém ekvivalencie regulárnych výrazov (tzn. pre dané r_1, r_2, je $L(r_1) \neq L(r_2)$?) je PSPACE*-úplný.*

■ **Dôkaz.**

- patrí do PSPACE
- ťažkosť – redukciou z LbaAcc:
- $L(r_1) = \Gamma^*$, r_2 bude matchovať *všetko okrem* akceptačného výpočtu $M(x)$
- akceptačný výpočet zapíšeme ako reťazec

$$v = \#C_0\#C_1\#C_2\#\cdots\#C_t\#$$

nad abecedou $\Gamma = Q \cup \Sigma \cup \{\#\}$

ako vyzerajú slová, ktoré *nie sú* akceptačným výpočtom $M(x)$?

- zle začínajú:

$$s = (\Gamma \mid \varepsilon)^{n+2} \mid (\Gamma - \#)\Gamma^* \mid \#(\Gamma - q_0)\Gamma^* \mid \cdots \mid (\# q_0 x_1 \cdots x_{i-1}(\Gamma - x_i)\Gamma^*)$$

- alebo neakceptujú:

$$f = (\Gamma - q_f)^*$$

- alebo nejaké dve konfigurácie na seba nenadväzujú:

$$m = \bigcup_{(a,b,c,d,e,f) \in ZK} \Gamma^* abc \Gamma^{n-2} def \Gamma^*,$$

  pre „zlú kombináciu“ písmenok a, b, c, d, e, f

- výsledný regex je $r_2 = s \mid f \mid m$.

ako vyzerajú slová, ktoré *nie sú* akceptačným výpočtom $M(x)$?

- zle začínajú:

$$s = (\Gamma \mid \varepsilon)^{n+2} \mid (\Gamma - \#)\Gamma^* \mid \#(\Gamma - q_0)\Gamma^* \mid \cdots \mid (\#q_0 x_1 \cdots x_{i-1}(\Gamma - x_i)\Gamma^*)$$

- alebo neakceptujú:

$$f = (\Gamma - q_f)^*$$

- alebo nejaké dve konfigurácie na seba nenadväzujú:

$$m = \bigcup_{(a,b,c,d,e,f)\in ZK} \Gamma^* abc\Gamma^{n-2} def \Gamma^*,$$

pre „zlú kombináciu“ písmenok a, b, c, d, e, f

- výsledný regex je $r_2 = s \mid f \mid m$.

ako vyzerajú slová, ktoré *nie sú* akceptačným výpočtom $M(x)$?

- zle začínajú:

$$s = (\Gamma \mid \varepsilon)^{n+2} \mid (\Gamma - \#)\Gamma^* \mid \#(\Gamma - q_0)\Gamma^* \mid \cdots \mid (\# q_0 x_1 \cdots x_{i-1}(\Gamma - x_i)\Gamma^*)$$

- alebo neakceptujú:

$$f = (\Gamma - q_f)^*$$

- alebo nejaké dve konfigurácie na seba nenadväzujú:

$$m = \bigcup_{(a,b,c,d,e,f) \in ZK} \Gamma^* abc \Gamma^{n-2} def \Gamma^*,$$

pre „zlú kombináciu“ písmenok a, b, c, d, e, f

- výsledný regex je $r_2 = s \mid f \mid m$.

ako vyzerajú slová, ktoré *nie sú* akceptačným výpočtom $M(x)$?

- zle začínajú:

$$s = (\Gamma \mid \varepsilon)^{n+2} \mid (\Gamma - \#)\Gamma^* \mid \#(\Gamma - q_0)\Gamma^* \mid \cdots \mid (\# q_0 x_1 \cdots x_{i-1}(\Gamma - x_i)\Gamma^*)$$

- alebo neakceptujú:

$$f = (\Gamma - q_f)^*$$

- alebo nejaké dve konfigurácie na seba nenadväzujú:

$$m = \bigcup_{(a,b,c,d,e,f)\in ZK} \Gamma^* abc \Gamma^{n-2} def \Gamma^*,$$

pre „zlú kombináciu“ písmenok a, b, c, d, e, f

- výsledný regex je $r_2 = s \mid f \mid m$.

ako vyzerajú slová, ktoré *nie sú* akceptačným výpočtom $M(x)$?

- zle začínajú:

$$s = (\Gamma \mid \varepsilon)^{n+2} \mid (\Gamma - \#)\Gamma^* \mid \#(\Gamma - q_0)\Gamma^* \mid \cdots \mid (\# q_0 x_1 \cdots x_{i-1}(\Gamma - x_i)\Gamma^*)$$

- alebo neakceptujú:

$$f = (\Gamma - q_f)^*$$

- alebo nejaké dve konfigurácie na seba nenadväzujú:

$$m = \bigcup_{(a,b,c,d,e,f)\in ZK} \Gamma^* abc \Gamma^{n-2} def \Gamma^*,$$

  pre „zlú kombináciu“ písmenok a, b, c, d, e, f

- výsledný regex je $r_2 = s \mid f \mid m$.

$\square$

NL-úplné

Veta

Problém zistiť, či existuje cesta medzi dvoma vrcholmi v danom orientovanom grafe je NL*-úplný pri logspace redukcii.*