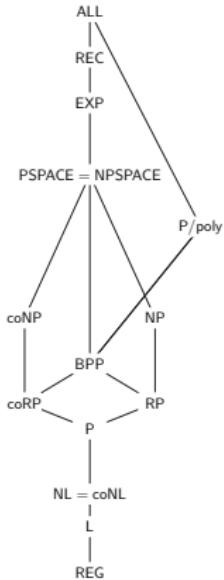


Rýchle paralelné algoritmy a malá pamäť

kuko

17.3.2021

Pokročilá teória zložitosti



P

- lineárne programovanie • parsovanie
- maximálny tok • editačná vzdialenosť
- perfektné párovanie • násobenie matíc
- hľadanie najkratšej cesty v grafe
- je graf acyklický? • 2SAT • triedenie
- je graf bipartitný? • násobenie
- sčítanie

Definícia

$\text{NC} = \text{jazyky s efektívnymi paralelnými algoritmami}$

- PRAM, poly procesorov, polylog čas, alebo
- obvody poly veľkosti, polylog hĺbky.

Veta

$\text{NC} \subseteq \text{P}$

Definícia

$\text{NC} = \text{jazyky s efektívnymi paralelnými algoritmami}$

- PRAM, poly procesorov, polylog čas, alebo
- obvody poly veľkosti, polylog hĺbky.

Veta

$\text{NC} \subseteq \text{P}$

Definícia

NC^k :

- uniformné
- \wedge, \vee, \neg
- hradlá \wedge a \vee majú 2 vstupy
- polyn vel'kosť
- $O(\log^k n)$ hĺbka

$\text{NC} = \bigcup_k \text{NC}^k$

Definícia

NC^k :

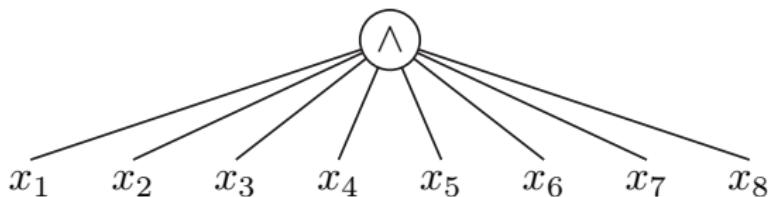
- uniformné
- \wedge, \vee, \neg
- hradlá \wedge a \vee majú 2 vstupy
- polyn vel'kosť
- $O(\log^k n)$ hĺbka

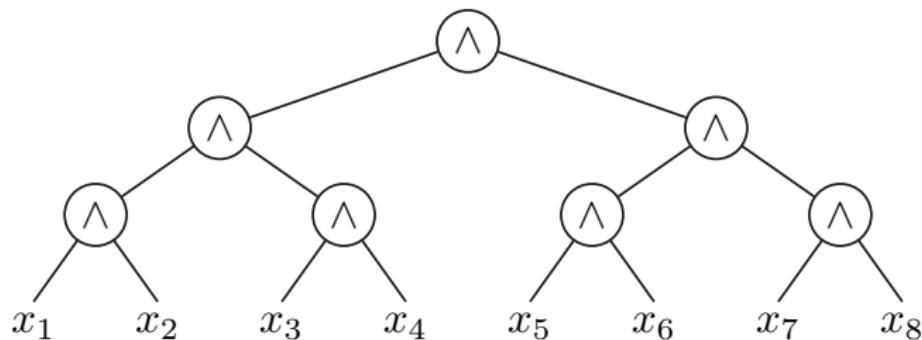
$\text{NC} = \bigcup_k \text{NC}^k$

Definícia

AC^k:

- uniformné
- \wedge, \vee, \neg
- polyn velkosť
- $O(\log^k n)$ hĺbka
- hradlá \wedge a \vee majú neobmedzený počet vstupov





$$\text{NC}^k \subseteq \text{AC}^k \subseteq \text{NC}^{k+1}$$

Sčítanie

1	0	0	1	0	1	1	0	1	0	1	
1	0	0	0	1	1	0	0	1	1	0	0

↑ ↑

Veta

ADDITION $\in \text{AC}^0$.

■ Dôkaz.

$$c_i = \bigvee_{j < i} a_j \wedge b_j \wedge \left(\bigwedge_{j < k < i} a_k \vee b_k \right).$$



Násobenie

$$\begin{array}{r}
 & 0 & 1 & 0 & 0 & 1 & 1 \\
 + & 0 & 1 & 1 & 0 & 0 & 1 \\
 + & 1 & 0 & 1 & 0 & 0 & 1 \\
 \hline
 & 1 & 0 & 0 & 0 & 1 & 1 \\
 + & 0 & 1 & 1 & 0 & 0 & 1
 \end{array}$$

súčty mod 2

prenosy do vyššieho rádu

$$\begin{array}{r}
 & 11 & 9 & 17 & 5 & 12 & 18 \\
 + & 6 & 12 & 9 & 10 & 8 & 18 \\
 \hline
 & 17 & 21 & 26 & 15 & 20 & 36 \\
 & 7 & 1 & 6 & 5 & 0 & 16 \\
 + & 1 & 2 & 2 & 1 & 2 & 2 \\
 \hline
 & 1 & 9 & 3 & 7 & 7 & 2 & 16
 \end{array}$$

redundantný zápis: 10-tková sústava
s ciframi [0..18]

medzivýsledok má cifry [0..36]

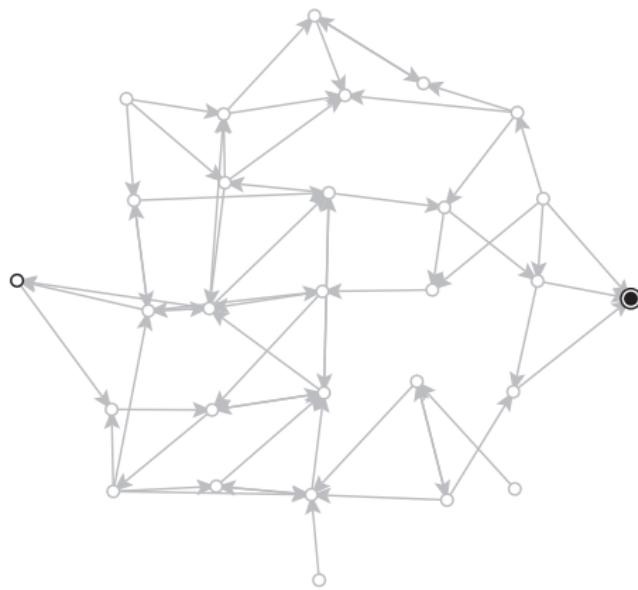
rozložíme ich na $10 \times [0..2] + [0..16]$

(tu sú prenosy do vyššieho rádu) a sčítame
cifry výsledku budú opäť [0..18]

Veta

MULTIPLICATION $\in \text{NC}^1$.

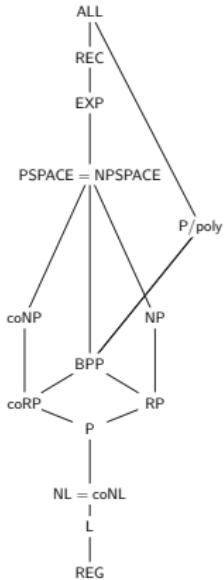
Hľadanie cesty v grafe



Veta

Zistíť, či existuje cesta medzi dvoma vrcholmi v (orientovanom) grafe sa dá v AC¹.

Vzťah medzi L, NL a NC



Veta

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

Veta

$\text{NC}^1 \subseteq \text{L} \subseteq \text{NL} \subseteq \text{AC}^1 \subseteq \text{NC}^2$.

Charakterizácia cez alternáciu

$$\text{NL} \subseteq \text{NC} \subseteq \text{P} = \text{AL}$$

Definícia

Trieda STA($s(n)$, $t(n)$, $Xa(n)$) Napríklad

$$L = STA(\log, *, 0)$$

$$P = STA(*, \text{poly}, 0) = STA(\log, *, *) = AL$$

$$NP = STA(*, \text{poly}, \Sigma_1)$$

$$\Pi_k^P = STA(*, \text{poly}, \Pi_k)$$

$$PSPACE = STA(\text{poly}, *, 0) = STA(*, \text{poly}, *) = AP$$

Definícia

Trieda STA($s(n)$, $t(n)$, $X_a(n)$) Napríklad

$$L = STA(\log, *, 0)$$

$$P = STA(*, \text{poly}, 0) = STA(\log, *, *) = AL$$

$$NP = STA(*, \text{poly}, \Sigma_1)$$

$$\Pi_k^P = STA(*, \text{poly}, \Pi_k)$$

$$PSPACE = STA(\text{poly}, *, 0) = STA(*, \text{poly}, *) = AP$$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

Dôsledok

$$\text{NL} = \text{STA}(\log, *, \Sigma_1)$$

$$\cap$$

$$\text{AC}^1 = \text{STA}(\log, *, \log)$$

$$\cap$$

$$\text{NC} = \text{STA}(\log, *, \text{polylog})$$

$$\cap$$

$$\text{P} = \text{STA}(\log, *, *)$$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

Dôsledok

$$\text{NL} = \text{STA}(\log, *, \Sigma_1)$$

$$\cap$$

$$\text{AC}^1 = \text{STA}(\log, *, \log)$$

$$\cap$$

$$\text{NC} = \text{STA}(\log, *, \text{polylog})$$

$$\cap$$

$$\text{P} = \text{STA}(\log, *, *)$$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

Dôsledok

$$\text{NL} = \text{STA}(\log, *, \Sigma_1)$$

$$\cap$$

$$\text{AC}^1 = \text{STA}(\log, *, \log)$$

$$\cap$$

$$\text{NC} = \text{STA}(\log, *, \text{polylog})$$

$$\cap$$

$$\text{P} = \text{STA}(\log, *, *)$$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}

\supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}
 \supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}

\supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}
 \supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}
 \supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}

\supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}
 \supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}
 \supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

$$\text{NC} = \text{STA}(\log, \text{polylog}, *) = \text{STA}(\log, *, \text{polylog})$$

Pre $k \geq 1$:

$$\text{AC}^k = \text{STA}(\log, *, \log^k)$$

■ **Dôkaz.** \subseteq : AC-obvod \implies monotónny obvod so vstupmi x, \bar{x}

\supseteq : násobenie matíc:

- $S_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) = \text{typ}(\beta)$ a
- $T_x(\alpha, \beta) \iff \alpha \vdash \beta \wedge \text{typ}(\alpha) \neq \text{typ}(\beta)$;
- $M_x = S_x^* T_x$
- $M_x(\alpha, \beta) = 1 \iff \alpha \vdash^* \gamma \vdash \beta$, pričom počas výpočtu bol typ stavov rovnaký, až v poslednom kroku sa zmenil
- vektor a_i : $a_i(C) = 1$ ak C je akcept. konfig. na i -tej úrovni
- \exists -úrovne: $a_{i+1} = M_x a_i$
- \forall -úrovne: $a_{i+1} = \neg(M_x(\neg a_i))$
- akceptujeme, ak $a_{\log^k n}(C_0) = 1$

Parsovanie

Veta

Regulárne jazyky sa dajú akceptovať v NC¹.

Veta

Bezkontextové jazyky vieme akceptovať v $\text{AC}^1 = \text{STA}(\log, *, \log)$.

- Hra Alice (\exists) a Boba (\forall), kde A chce dokázať:

$$\sigma \Rightarrow_G^* w$$

- tah A: (α, i, j)

$$\sigma \Rightarrow_G^* w_{1,i} \alpha w_{j,n} \quad \text{a} \quad \alpha \Rightarrow_G^* w_{i,j}$$

- tah B: vyberie si, ktoré tvrdenie chce dokázať

Veta

Bezkontextové jazyky vieme akceptovať v $\text{AC}^1 = \text{STA}(\log, *, \log)$.

- Hra Alice (\exists) a Boba (\forall), kde A chce dokázať:

$$\sigma \Rightarrow_G^* w$$

- tah A: (α, i, j)

$$\sigma \Rightarrow_G^* w_{1,i} \alpha w_{j,n} \quad \text{a} \quad \alpha \Rightarrow_G^* w_{i,j}$$

- tah B: vyberie si, ktoré tvrdenie chce dokázať

Veta

Bezkontextové jazyky vieme akceptovať v $\text{AC}^1 = \text{STA}(\log, *, \log)$.

- Hra Alice (\exists) a Boba (\forall), kde A chce dokázať:

$$\sigma \Rightarrow_G^* w$$

- tah A: (α, i, j)

$$\sigma \Rightarrow_G^* w_{1,i} \alpha w_{j,n} \quad \text{a} \quad \alpha \Rightarrow_G^* w_{i,j}$$

- tah B: vyberie si, ktoré tvrdenie chce dokázať

Veta

Bezkontextové jazyky vieme akceptovať v $\text{AC}^1 = \text{STA}(\log, *, \log)$.

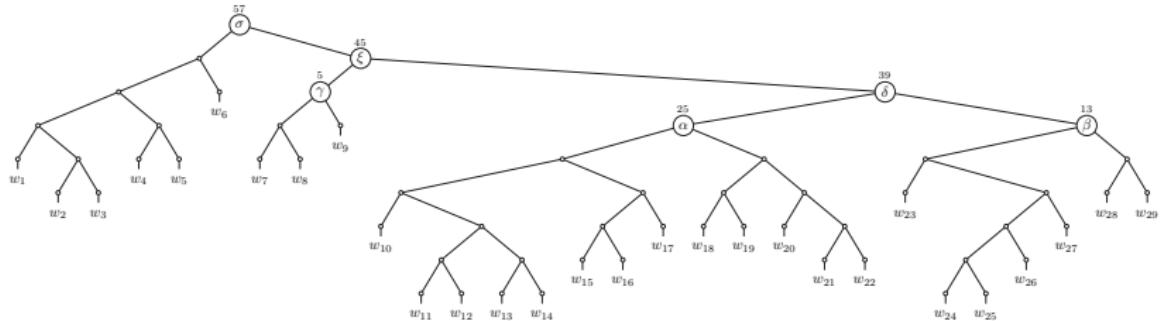
- Hra Alice (\exists) a Boba (\forall), kde A chce dokázať:

$$\sigma \Rightarrow_G^* w$$

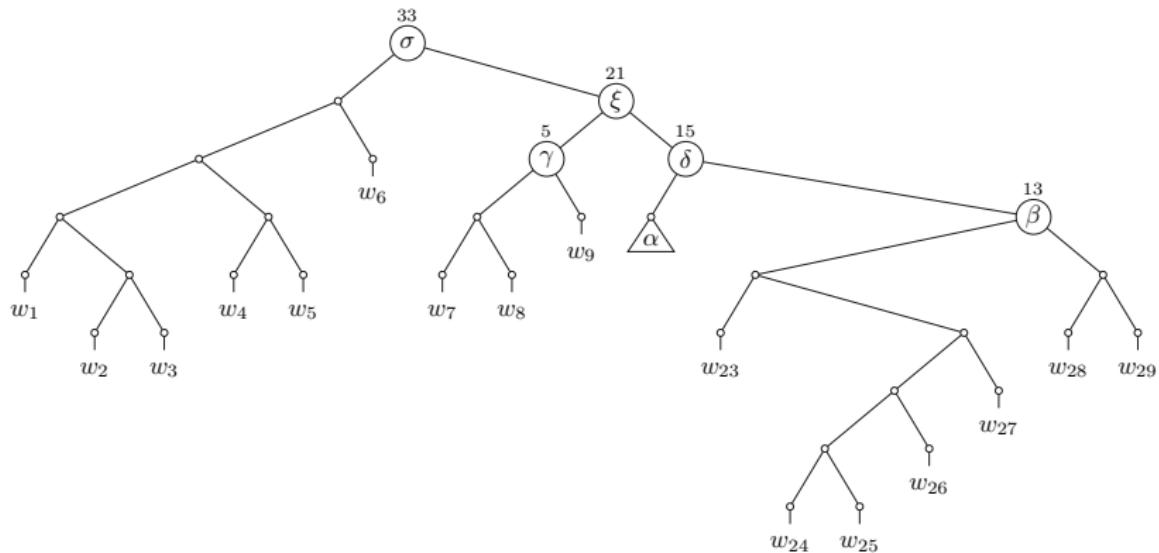
- tah A: (α, i, j)

$$\sigma \Rightarrow_G^* w_{1,i} \alpha w_{j,n} \quad \text{a} \quad \alpha \Rightarrow_G^* w_{i,j}$$

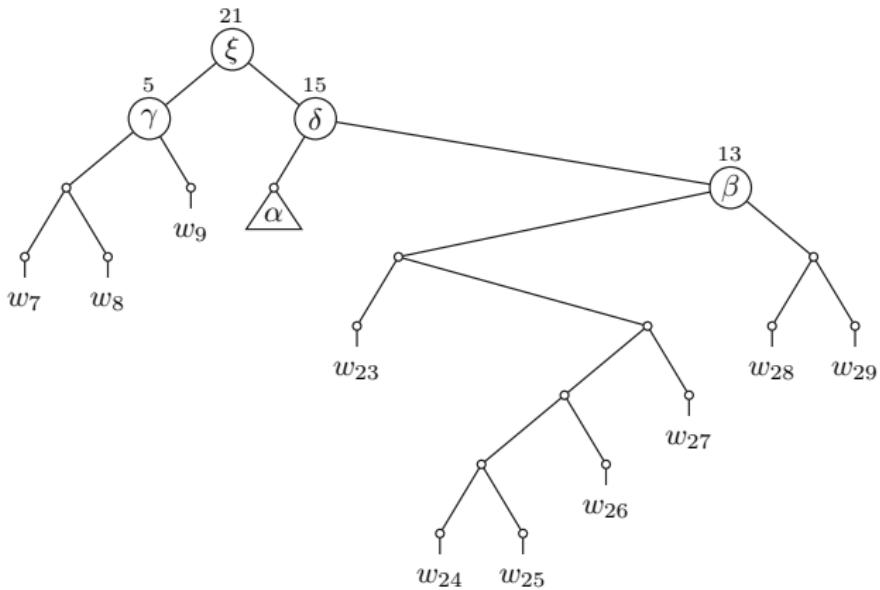
- tah B: vyberie si, ktoré tvrdenie chce dokázať



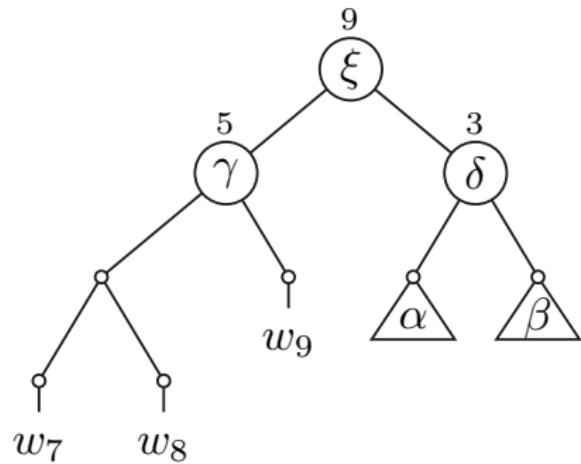
Obr.: A: $(\alpha, 10, 23)$; B: hore



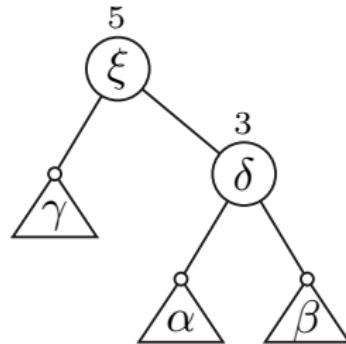
Obr.: A: $(\xi, 7, 30)$; B: dolu



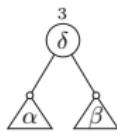
Obr.: A: $(\beta, 10, 30)$; B: hore



Obr.: A: $(\gamma, 7, 10)$; B: hore



Obr.: A: $(\delta, 10, 30)$; B: dolu



Obr.: $\delta \rightarrow \alpha\beta$ je pravidlo G , vyhráva A

pozícia hry:

$$\sigma \Rightarrow_G^* w_{i_1, i_2} \alpha_1 w_{i_3, i_4} \alpha_2 w_{i_5, i_6} \alpha_3 \cdots \alpha_k w_{i_{2k+1}, i_{2k+2}}$$

Veta

Nasledujúce problémy sú P-úplné:

- CVP – *vyhodnotenie daného boolovského obvodu na danom vstupe*
- HORNSAT – *problém splniteľnosti pre Hornove formule (v CNF, každá klausula má najviac jeden pozitívny literál)*
- DFS – *daný je graf a dva vrcholy u, v ; ak na grafe spustíme prehľadávanie do hĺbky (pričom zoznam susedov prehľadávame vo fixnom poradí danom na vstupe), ktorý vrchol z dvojice u, v navštívime ako prvý?*
- ...

Veta

- ...
- MAXFLOW – *daný je ohodnotený graf, vrcholy s, t a číslo f; existuje s-t-tok veľkosti aspoň f?*
- LP – *lineárne programovanie: existuje pre danú maticu A a vektor b riešenie nerovníc $Ax \leq b$, $x > 0$ v racionálnych číslach?*
- CFGMEM – *w ∈ L(G)? pre danú bezkontextovú gramatiku G a slovo w (pozor, toto je úplne iný problém, ako rozhodovať jazyk L(G) pre fixnú bezkontextovú gramatiku)*
- ITERATEDMOD – *dané a, b₁, ..., b_n ∈ ℤ; je ((⋯((a mod b₁) mod b₂)⋯) mod b_n) = 0?*