Myhill-Nerodova věta

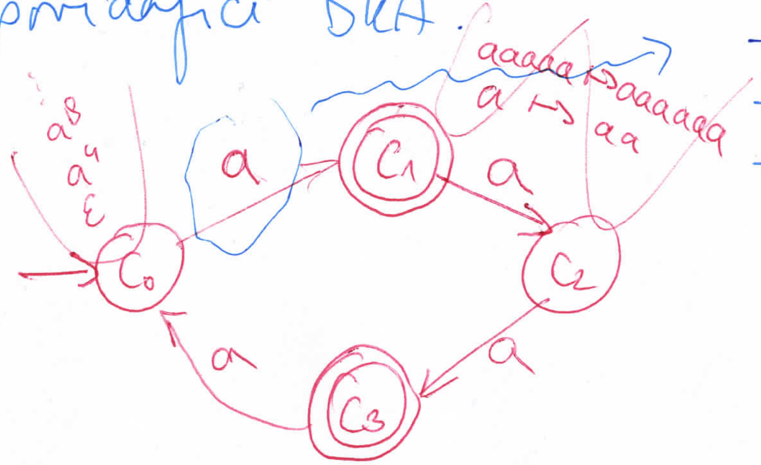
- Pravá kongruence nad Σ^*: ekvivalence $\sim \subseteq \Sigma^* \times \Sigma^*$ taková, že
  $\forall u, v \in \Sigma^*: u \sim v \Rightarrow \forall w \in \Sigma^*: uw \sim vw$.

- Mějme pravou kongruenci $\sim \subseteq (\{a\}^*)^2$ takovou, že

$$\{a\}^* \backslash \sim \; = \{ \{a^{4\cdot i} \mid i \geq 0\}^{c_0}, \{a^{4\cdot i+1} \mid i \geq 0\}^{c_1}, \{a^{4\cdot i+2} \mid i \geq 0\}^{c_2}, \{a^{4\cdot i+3} \mid i \geq 0\}^{c_3} \}$$

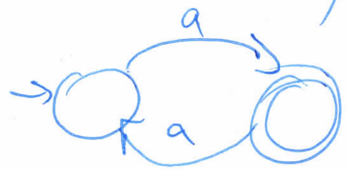
Dále uvažme, že $L = \{a^{4i+1} \mid i \geq 0\} \cup \{a^{4i+3} \mid i \geq 0\} = c_1 \cup c_3$

Sestavte odpovídající DKA.



- vzali jsme $\varepsilon \in c_0$
- prodloužili o $a \in \Sigma$
- $\varepsilon \cdot a = a \in c_1$,
  $a = a^{4\cdot 0+1} = a^1$.

- Prefixová ekvivalence pro $L \subseteq \Sigma^*$ je ekv. $\sim_L \subseteq (\Sigma^*)^2$ taková, že
$\forall u,v \in \Sigma^*: \ u \sim_L v \Leftrightarrow \forall w \in \Sigma^*: (uw \in L \Leftrightarrow vw \in L)$

- minimální DKA pro výše uvedený jazyk je 

sestavte odpovídající třídy $\sim_L$:

$$\{a\}^* / \sim_L = \{ \overset{C_0}{\{a^{2i} \mid i \geq 0\}}, \overset{C_1}{\{a^{2i+1} \mid i \geq 0\}} \},$$

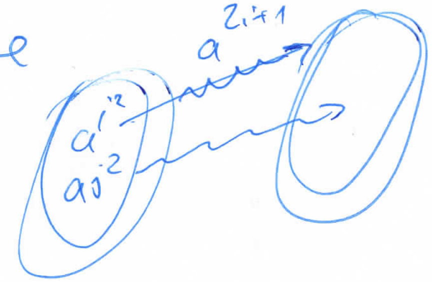
přičemž $L = C_1$

Tedy $\sim_L = \{ (\varepsilon,\varepsilon), (\varepsilon,aa), (\varepsilon,aaaa), \dots,$
$\cup \quad (a,a), (a,aaa), \dots \}$
$\sim \ = \{ (\varepsilon,\varepsilon), (\varepsilon,aaaa), \dots \}$

Dokažte pomocí Myhill-Nerodovy věty, že $L = \{a^{n^2} \mid n \geq 0\} \notin \mathcal{L}_3$

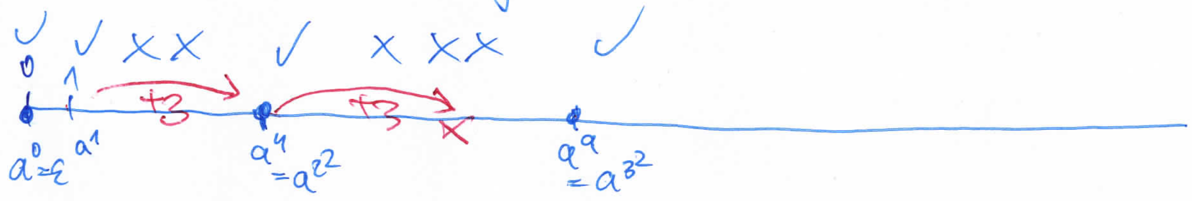
Důkaz sporem:
- Předp., že $L \in \mathcal{L}_3$.
- Pak dle M.-N. věty má relace $\sim_L$ konečný index.
- Uvažme ale libovolné $i < j$ a řetězce $a^{i^2}, a^{j^2} \in L$.

- Tyto řetězce nemohou být v jedné ekvivalenční třídě relace $\sim_L$. Konečně!
  - Řetězec $a^{(i+1)^2} \in L$. Tento řetězec vznikne z a^{i^2} prodloužením o a^{2i+1}.



  - Ovšem pak také $a^{j^2} \cdot a^{2i+1} \in L$
  - Ovšem nejbližší delší řetězec než a^{j^2}, který patří do L, je $a^{(j+1)^2} = a^{j^2+2j+1}$
  - Neboli a^{j^2} musíme prodloužit minimálně o $2j+1$, abychom padli do L.
  - Ale $i < j$ a tedy $2i+1 < 2j+1$.
  - Neboli $a^{j^2+2i+1} \notin L$.
- Řetězce a^{i^2}, a^{j^2} pro $i < j$ tedy nemohou být ve stejné ekv. třídě.
- Ovšem máme ∞-mnoho dvojic i, j takových, že $i < j$. Tedy $\sim_L$ má ∞ index. SPOR. □

VIZUALIZACE



P.L. pro $\mathcal{L}_2$

$\forall \Sigma : \Sigma$ kon. ab. $\forall L \subseteq \Sigma^* : L \in \mathcal{L}_2 \Rightarrow \exists k > 0 : \forall z \in L :$
$|z| \geq k \Rightarrow \exists u, v, w, x, y \in \Sigma^* : z = u\underline{v}w\underline{x}y \wedge vx \neq \varepsilon \wedge |vwx| \leq k \wedge$
$\forall i \geq 0 : u v^i w x^i y \in L$.

Dokažte, že $L = \{ a^n b^m c^{n \cdot m} \mid n, m \geq 0 \} \notin \mathcal{L}_2$.

Důkaz sporem:

- Předp., že $L \in \mathcal{L}_2$.
- Dle P.L. $\exists k > 0 : \forall z \in L : |z| \geq k \Rightarrow \exists u, v, w, x, y \in \{a, b, c\}^* :$
  $z = uvwxy \wedge vx \neq \varepsilon \wedge |vwx| \leq k \wedge \forall i \geq 0 : uv^iwx^iy \in L$.
- Uvažme libovolné k, pro které výše uvedené platí.
- Zvolme $z = a^k \cdot b^k \cdot c^{k^2} \in L$, $|z| = 2k + k^2 \geq k$.
- Tedy $\exists u, v, w, x, y \in \{a, b, c\}^* : a^k b^k c^{k^2} = uvwxy \wedge vx \neq \varepsilon \wedge$
  $\wedge |vwx| \leq k \wedge \forall i \geq 0 : uv^iwx^iy \in L$!
- Pokud zvolíme v či x tak, že zahrne více než 1 symbol
  z $\{a, b, c\}$, pak pro $i > 1$ nebude $uv^iwx^iy \notin a^*b^*c^*$, tedy

nebude v L. Nelze.

- Pokud naopak $vx \in a^+ \cup b^+ \cup c^+$ (víme, že $vx \neq \varepsilon$), pak pro $i > 1$ vzroste v $z' = uv^iwx^iy$ počet pouze jednoho ze symbolů a, b, či c a tedy nutně $\#_a(z') \cdot \#_b(z') = \#_c(z')$. Tedy $z' \notin L$. NELZE.
- Nutno tedy volit v i x z řetězců nad jedním symbolem, ovšem pro v a x různých.
- Nelze ale volit $v \in a^+$ a $x \in c^+$, neboť v tom případě by bylo $|vwx| > k$
- Pokud zvolíme $v \in a^+$ a $x \in b^+$, pak pro $i > 1$ vzroste v $z' = uv^iwx^iy$ hodnota $\#_a(z'), \#_b(z')$, ale nikoliv $\#_c(z')$. Tedy $\#_a(z') \cdot \#_b(z') \neq \#_c(z')$, $z' \notin L$. NELZE.
- Je tedy zřejmé, že $v \in b^+$ a $x \in c^+$ (nelze volit $v = \varepsilon \vee x = \varepsilon$, neboť v tom případě bychom měli $vx \in a^+ \cup b^+ \cup c^+$, což jsme již vyloučili)
- Zvolme např. $i = 2$ a předp., že $|v| = l_1$ a $|x| = l_2$.

- Dle P.L. $z' = uv^2wx^2y \in L$.
- pro z' ale platí:

$$\#_a(z') = k,$$
$$\#_b(z') = k + l_1,$$
$$\#_c(z') = k^2 + l_2$$

- Musí tedy platit, že $k(k+l_1) = k^2 + l_2$.

Tedy $k^2 + k \cdot l_1 = k^2 + l_2$,

$$k \cdot l_1 = l_2$$

- Vzhledem k tomu, že $k > 0$, lze psát, že $l_1 = \frac{l_2}{k}$.
- Ale $l_1 \geq 1$ ($v \in b^+$),

$l_2 < k$ ($|vwx| \leq k$, $|w| \geq 1$, $|x| = l_2$)

Pak ale $\frac{l_2}{k} < 1$. SPOR (nelze $l_1 = l_2/k \wedge l_1 \geq 1 \wedge l_2/k < 1$)

POLYNOMIÁLNÍ REDUKCE

- Mějme graf $G = (V, E)$, mn-u $S \subseteq V$ nazveme nezávislou mn-ou, jestliže pro každé $e \in E$ platí, že e má v S nanejvýš jeden uzel.

- Problém nezávislé mn-y: Má daný graf G nezávislou mn-u o k uzlech?
- Tento problém je NP-úplný.
- Důkaz (HRUBÁ IDEA)

a) členství v NP

- Lze řešit NTS M tak, že M nedeterministicky zvolí k uzlů grafu, které mají tvořit nezávislou mn-u, a následně průchodem všemi hranami ověří, že se opravdu jedná o nezávislou mn-u.
- Evidentně lze řešit pomocí konečného počtu zanořených cyklů „for" s horní mezí danou velikostí vstupu.

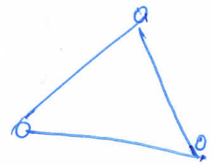
b) NP-těžkost

polynom. → redukcí z některého NP-úplného problému, např. ze 3SAT.

- Budeme uvažovat formule 3SAT $F = C_1 \wedge C_2 \wedge \dots \wedge C_k$, $k \geq 1$,

př.

G:



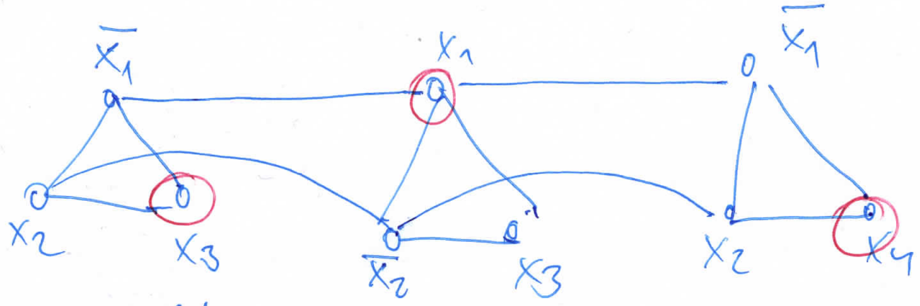
má nezávislou mn-u velikosti k?

- $k=1$: ✓
- $k=2$ ✗

pro $C_i = l_{i1} \vee l_{i2} \vee l_{i3}$, kde $l_{ij} = x$ v
$l_{ij} = \neg x$ pro $x \in Var$.

- Idea redukce na příkladu:

$F = (\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee x_4)$



chceme najít nezávislou mn-u vel. 3
(počet klauzulí k)

- Obecně redukce z formule F vytvoří graf o
3·k uzlech s následujícími hranami:
  - mezi každými dvěma uzly literálů z téže klauzule bude hrana
  - uzly odpovídající literálům z různých klauzulí propojíme hranou $\iff$ si příslušné literály odporují (tedy x a $\neg x$ pro $x \in Var$)

Ke grafu G dodá hodnotu k, by vznikla inst. problém nezávislosti:

- Tuto redukci lze snadno implementovat úplným DTS pracujícím v polynomiálním čase. Konečně generuje lineární počet uzlů a vůči nim nanejvýš kvadratický počet hran. K vygenerování každého uzlu/hrany stačí příp. zanořené for cykly s horní mezí danou velikostí vstupu.

- Je zapotřebí ukázat, že F je SAT $\iff$ G obsahuje nezávislou mn-u velikosti k.

„$\Leftarrow$"

  - Vzhledem k tomu, že uzly odpovídající jedné klausuli jsou všechny propojeny, musí být v nezávislé mn-ě vždy jen jeden uzel z nich.
  - Z nezávislosti pak plyne, že zvolené uzly nekolidují (resp. jim odpovídající literály nekolidují) — jinak by byly propojeny hranou.
  - Lze sestavit splňující ohodnocení celé formule tak, že nezávisle splní každý ze zvolených literálů.

"$\Rightarrow$" - Máme splňující přiřazení F.

- To musí v každé klauzuli splnit alespoň 1 literál tak, aby si ohodnocení těchto literálů neodporovala.
- Nezávislou mn-u tvoří vrch. odpovídající těmto zvoleným splněným literálům. $\square$