Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Strukturální složitost I
BONUS

Peter Černo, 2010
petercerno@gmail.com

Garant: doc. RNDr. Václav Koubek, DrSc.
E-mail: Vaclav.Koubek@mff.cuni.cz

Anotace: Pokračování předmětu Složitost II, otázka "NP=P?"z různých pohledů, vlastnosti SAT, jiné přístupy ke složitosti, hierarchie složitostních tříd.

Sylabus:

1. Základní modely a pojmy, základní třídy problémů, polynomiální redukce, úplné a těžké problémy
2. Řídké množiny a množiny nad jednoprvkou abecedou, separace tříd DEXT a NEXT
3. Turingovská polynomiální redukce
4. Boolovské obvody, Shannonova věta, třídy P/poly, NP/poly, P/log, NP/log a jejich vztah k ostatním třídám problémů
5. Pravděpodobnostní algoritmy, třídy PP, BPP, RP a ZPP. Vztah BPP k neuniformní složitosti
6. Polynomiální hierarchie, úplné problémy pro její třídy, zařazení BPP do polynomiální hierarchie

Cíl předmětu: Naučit základy strukturální složitosti.

Literatura:

1. Balcázar, Díaz, Gabarró, Structural Complexity I, Springer Verlag, Berlin, 1988
2. Balcázar, Díaz, Gabarró, Structural Complexity II, Springer Verlag, Berlin, 1990
3. Schöning, Complexity and Structure, Lecture Notes in Computer Science, Springer Verlag, Berlin, 1985
4. Allender, Limitations of the upward separation technique, Mathematical Systems Theory 24 (1991), 53-67

5. Seiferas, Fischer, Meyer, Separating nondeterministic time complexity classes, Journal of the Association for Computing Machinery 25 (1978), no. 1, 146-167

This page is intentionally left blank.

PETER ČERNO

POUŽITÁ LITERATÚRA:
J. L. BALCÁZAR, J. DÍAZ, J. GABARRÓ -
STRUCTURAL COMPLEXITY I + II

Mějme Turingův stroj M se vstupní abecedou Σ, výstupní páskou a výstupní abecedou Ω (to znamená, že na výstupní pásku může psát jen symboly z Ω). Řekneme, že M počítá parciální funkci $f : \Sigma^* \to \Omega^*$, když $f(x)$ je definováno, právě když M přijímá x, a když M přijímá x, pak na výstupní pásku napíše $f(x)$.

Označme PF množinu parciálních funkcí spočitatelnou deterministickým Turingovým strojem v polynomiálním čase a $PSPACEF$ množinu parciálních funkcí spočitatelnou deterministickým Turingovým strojem v polynomiálním prostoru. Mějme funkci $f : \Sigma^* \to \Omega^*$, pak funkce $g : \Omega^* \to \Sigma^*$ je <u>inverzní funkce</u> k f, když $g(y)$ pro $y \in \Omega^*$ je definováno, právě když existuje $x \in \Sigma^*$ takové, že $f(x)$ je definováno a $y = f(x)$, a když $g(y)$ je definováno, pak f je definováno na $g(y)$ a platí $f(g(y)) = y$. Funkce $f : \Sigma^* \to \Omega^*$ je <u>honest</u>, když existuje polynom p a pro každé $y \in \Omega^*$ takové, že $y = f(x)$ pro nějaké $x \in \Sigma^*$, existuje $x \in \Sigma^*$ takové, že $f(x) = y$ a $|x| \le p(|y|)$.

Dokažte

√ (1) $P = PSPACE$, právě když $PF = PSPACEF$;

√ (2) $P = NP$, právě když každá honest funkce $f \in PF$ má inverzní funkci v PF;

√ (3) když $f \in PF$, pak pro každou $A \in P$ je $f^{-1}(A) \in P$;

√ (4) $A \in NP$, právě když existuje honest funkce $f \in PF$ taková, že $A = \{f(x) \mid x \text{ je v definičním oboru } f\}$.

Nechť f je časově zkonstruovatelná funkce z přirozených čísel do sebe. Dokažte

√ (5) když $P = NP$, pak platí $DTIME(f^{O(1)}) = NTIME(f^{O(1)})$ a $DTIME(2^{O(f)}) = NTIME(2^{O(f)})$;

√ (6) když $P = PSPACE$, pak $DTIME(f^{O(1)}) = DSPACE(f^{O(1)})$ a $DTIME(2^{O(f)}) = DSPACE(2^{O(f)})$;

√ (7) když $DTIME(2^{cn}) \subseteq NP$ pro nějaké $c > 0$, pak $DEXT \subsetneq NP = PSPACE = EXPTIME$ a $DTIME(2^{cn}) \neq NP$ pro každé $c > 0$;

√ (8) $DEXT \neq PSPACE$ (uvažte vlastnosti m-redukce na těchto třídách);

√ (9) ukažte, že následující problém je $NLOG$-úplný vzhledem k m-redukci omezené na výpočet v LOG-prosoru:
Vstup: Graf $G = (V, E)$ a dva různé vrcholy $u, v \in V$.
Odpověď: ano, když existuje cesta mezi vrcholy u a v v grafu G;

? (10) ukažte, že následující problém je $PSPACE$-úplný vzhledem k m-redukci omezené na výpočet v LOG-prostoru:
Vstup: Kontextová gramatika G nad abecedou Σ a slovo $\alpha \in \Sigma^*$.
Odpověď: ano, když G vygeneruje α;

√ (11) ukažte, že NP je uzavřená vzhledem k $\le_T$ (tj. když $A \in NP$ a $B \le_T A$, pak $B \in NP$), právě když NP je uzavřená na doplňky.

Pro jazyk A definujme jazyky $K(A)$, $KS(A)$ a $KE(A)$.

$$K(A) = \{< M, x, 1^t > | M \text{ kód nedeterministického Turingova stroje s orakulem, } x \text{ slovo, které přijímá } M \text{ s orakulem } A \text{ v čase } t\},$$

$$KS(A) = \{< M, x, 1^t > | M \text{ kód nedeterministického Turingova stroje s orakulem, } x \text{ slovo, které přijímá } M \text{ s orakulem } A \text{ v prostoru } t\},$$

$$KE(A) = \{< M, x, t > | M \text{ kód } \cancel{\text{ne}}\text{deterministického Turingova stroje s orakulem, } x \text{ slovo, které přijímá } M \text{ s orakulem } A \text{ v čase } t\},$$

kde v definici $KE(A)$ je t zadáno v binárním tvaru.

Dokažte

(12) $K(A)$ je $NP(A)$-úplný jazyk vzhledem k m-redukci;
(13) $KS(A)$ je $PSPACE(A)$-úplný jazyk vzhledem k m-redukci;
(14) $KE(A)$ je $EXPTIME(A)$-úplný jazyk vzhledem k m-redukci;
(15) $A \in NP(B)$, právě když $A \leq_m K(B)$;
(16) ukažte, že následující vztahy jsou ekvivalentní:
$B \leq^{SN} A$,
$K(B) \leq_m K(A)$,
$NP(B) \subseteq NP(A)$;
(17) ukažte, že když T je tally množina taková, že $DEXT(T) = DEXT$, pak $T \in P$;
(18) ukažte, že když M je Turingův stroj dokazující, že jazyk A je selfreducibilní a když $B = L(M, B)$, pak $A = B$.

Připomínám, že $A \leq^{SN} B$, právě když $A \in NP(A) \cap co-NP(A)$, a $A \leq_m B$, právě když existuje funkce f taková, že $x \in A$, právě když $f(x) \in B$ a f je spočitatelná v polynomiálním čase (pak mluvíme o m-reducibilitě). Často se používá silnější požadavek, že f je spočitatelná v LOG.

Připomínáme, že problém A je self-reducibilní (samoredukující), když existuje deterministický Turingův stroj M s oraculem pracující v polynomiálním čase takový, že $A = L(M, A)$ a pro vstup délky n M dává dotazy délky nejvýše $n - 1$.

Ukažte, že

(19) problémy SAT a QBF jsou self-reducibilní;
(20) když je problém A self-reducibilní, pak $A \in PSPACE$.

√1. Pro $k > 0$ označme k-QBF množinu uzavřených boolských formulí takových, že kvantifikování začíná existenčním kvantifikátorem a kvantifikování nejvýše k-krát změnilo kvantifikování (stejné kvantifikátory mohou být vedle sebe, počítají se za jeden kvantifikátor). Dokážte, že k-QBF je Σ_k-úplný problém.

√ 2. Dokažte

když $PSPACE \neq PH$, pak existuje jazyk $A \in PSPACE \setminus PH$, který není $PSPACE$-úplný;
když $\Sigma_{k+1} \neq \Sigma_k$, pak existuje jazyk $A \in \Sigma_{k+1} \setminus \Sigma_k$, který není Σ_{k+1}-úplný;
když $\Sigma_{k+1} \neq \Sigma_k$, pak existuje jazyk $A \in \Sigma_{k+1} \setminus \Sigma_k$, který není NP-těžký.

√3. Ukažte, že třídy jazyků $PSPACE \setminus PH$, $PSPACE \setminus \Sigma_k$ a $\Sigma_{k+1} \setminus \Sigma_k$ jsou rekurzivně prezentovatelné jedině když jsou prázdné.

√4. Množina A se nazývá NP-ekvivalentní, když $P(A) = P(SAT)$. Ukažte, že množina A je NP-ekvivalentní, právě když je Δ_2-úplná vzhledem k polynomiální Turingovské redukci. Když NP není uzavřeno na doplňky, tak existuje $A \in \Delta_2 \setminus (NP \cup co - NP)$, která není NP-ekvivalentní. Dokažte.

√5. Dokažte

√ $\Sigma_k/poly = \bigcup\{\Sigma_k(S) \mid S \text{ je řídká}\}$;
√ $\Pi_k/poly = \bigcup\{\Pi_k(S) \mid S \text{ je řídká}\}$;
√ $\Delta_k/poly = \bigcup\{\Delta_k(S) \mid S \text{ je řídká}\}$;
√ $PH/poly = \bigcup\{PH(S) \mid S \text{ je řídká}\}$;
√ $\Sigma_k/poly = \Pi_k/poly$ implikuje $\Sigma_k/poly = PH/poly$;
√ $\Sigma_k/poly = \Pi_k/poly$ implikuje $\Sigma_{k+2} = \Pi_{k+2}$.

√6. Dokažte, že následující tvrzení jsou ekvivalentní

(a) polynomiální hierarchie kolapsuje;
(b) pro každou množinu $A \in PH$ polynomiální hierarchie relativní k A kolapsuje;
(c) existuje množina $A \in PH$ taková, že polynomiální hierarchie relativní k A kolapsuje;
(d) existuje množina $A \in PH$ taková, že $P(A) = NP(A)$.

Dokažte, že

(1) Následující množiny nejsou rekurzivně prezentovatelné: množina rekurzivních množin, množina řídkých rekurzivních množin, množina rekurzivních množin v $P/poly$, množina rekurzivních NP-těžkých množin, $NP \setminus P$, množina NP-neúplných množin v NP, množina nekonečných množin v P.

(2) Mějme rekurzivně prezentovatelné třídy $\mathcal{C}_1$ a $\mathcal{C}_2$ takové, že $\mathcal{C}_1 \cap \mathcal{C}_2$ obsahuje nějakou množinu B a všechny její konečné variace. Pak $\mathcal{C}_1 \cap \mathcal{C}_2$ je rekurzivně prezentovatelná.

(3) Nechť $\mathcal{C}_1$ je rekurzivně prezentovatelná třída uzavřená na $\leq_m$.[1] Když $\mathcal{C}_2$ a $\mathcal{C}_3$ jsou rekurzivně prezentovatelné takové, že $\mathcal{C}_1 = \mathcal{C}_2 \cup \mathcal{C}_3$, pak buď $\mathcal{C}_1 = \mathcal{C}_2$ nebo $\mathcal{C}_1 = \mathcal{C}_3$. Když $\mathcal{C}_2$ je rekurzivně prezentovatelná, co můžeme říct o $\mathcal{C}_1 \setminus \mathcal{C}_2$?

(4) Když $\mathcal{C}$ je rekurzivně prezentovatelná, pak uzávěr $\mathcal{C}$ na konečnou variaci je také rekurzivně prezentovatelný.

(5) Když $\mathcal{C}_1$ a $\mathcal{C}_2$ jsou rekurzivně prezentovatelné, $\mathcal{C}_1$ obsahuje jen nekonečné množiny a $\mathcal{C}_2$ je uzavřená na konečnou variaci a nechť $B \notin \mathcal{C}_2$, pak existuje $D \in P$ taková, že $B \cap D \notin \mathcal{C}_1 \cup \mathcal{C}_2$.

(6) Když $PSPACE \neq PH$, pak existuje v $PSPACE \setminus PH$ množina, která není $PSPACE$-úplná.

(7) Když $\Sigma_{k+1} \neq \Sigma_k$ pak existuje v $\Sigma_{k+1} \setminus \Sigma_k$ množina, která není Σ_{k+1}-úplná.

(8) Nechť $k - QBF$ je množina všech splněných uzavřených formulí, kde je první kvantifikátor $\exists$ a je nejvýše k výměn kvantifikátoru. Ukažte, že $k - QBF$ je Σ_k-úplný problém vzhledem k $\leq_m$.

(9) $\Sigma_k/poly = \bigcup\{\Sigma_k(S) \mid S \text{ je řídká množina}\}$,
$\Pi_k/poly = \bigcup\{\Pi_k(S) \mid S \text{ je řídká množina}\}$,
$\Delta_k/poly = \bigcup\{\Delta_k(S) \mid S \text{ je řídká množina}\}$,
$PH/poly = \bigcup\{PH(S) \mid S \text{ je řídká množina}\}$.

(10) Ukažte, že existuje orakulum A takové, že $P(A) \neq NP(A) \cap co-NP(A)$.

(11) Nechť g je funkce z přirozených čísel do sebe. Pak $P(A)_g$ je množina jazyků L takových, že existuje nedeterministický Turinguv stroj M přijímající L v polynomiálním čase s orakulem A a každý výpočet M nad x provede nejvýše $g(|x|)$ nedeterministických kroků. Ukažte, že pro každé $\ell > 0$ existuje orakulum B takové, že $P(B)_{n^\ell} \neq P(B)_{n^{\ell+1}}$.

(12) Ukažte, že $P(A) = PQUERY(A)$, právě když A je $PSPACE$-těžké. (VZHĽADOM K $\leq_T$)

(13) Ukažte, že existuje orakulum A, že $NPQUERY(A) \neq PSPACE(A)$ a že existuje orakulum B, že $PQUERY(B) \neq NPQUERY(B)$.

(14) Nalezněte orakulum A, že $NP(A) \neq NP_b(A)$.

(15) Ukažte, že $P/log \subseteq \bigcup_A P_l(A) \subseteq \Delta_{\cancel{4}}^{2}/log$.

? (16) Nalezněte orakulum A takové, že $A \notin P_l(A)$.

(17) Když $P/log \neq \bigcup_A P_l(A)$, pak $P \neq NP$.

ERRATA

1) C_1 NETRIVIÁLNA, UZAVRETÁ NA $\oplus$,
C_2 A C_3 UZAVRETÉ NA KON. VARIÁCIE

(1) Ukažte, že pro množinu $A \subseteq \Sigma^*$ existují obvody polynomiální velikosti rozpoznávající A, právě když existuje tally množina T taková, že $A \in P(T)$.

(2) Ukažte, že $DEXT \neq EXPSPACE$, právě když $PSPACE \cap (P/poly) \neq P$.

(3) Generátor je obvod G s n vstupy, m výstupními hradly a speciálním hradlem indikátorem. G počítá parciální funkci $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ takovou, že $f(\alpha)$ pro $\alpha \in \{0,1\}^n$ je definováno, právě když výstup na indikátoru při vstupu α je 1 a vektor $f(\alpha)$ je výstupních hradlech. Množina $A \subseteq \Sigma^*$ je generovaná posloupnosti generátorů $\{G_i \mid i \in \mathbb{N}\}$, když G_i má i výstupních hradel a $A \cap \{\Sigma^i\}$ je obor funkčních hodnot parciálnífunkce počítané G_i. Pokud existuje polynom p takový, že G_i má nejvýše $p(i)$ hradel pro každé i, pak A má generátor polynomiální velikosti. Dokažte

   (a) když množina je rozpoznávaná obvody polynomiální velikosti, pak má generátor polynomiální velikosti;

   (b) rozhodnout pro generátor G s n výstupními hradly a slovo $w \in \Sigma^n$ zda existuje α takové, že pro funkci f počítanou G platí $f(\alpha) = w$ je NP-úplné (zformalizujte a dokažte).

   (c) ukažte ekvivalenci těchto tvrzení:
   A má generátor polynomiálnívelikosti;
   $A \in NP/poly$;
   existuje tally množina T, že $A \in NP(T)$;
   existuje řídká množina S, že $A \in NP(S)$.

   (d) existuje množina $A \in EXPSPACE$, která nemá generátor polynomiální velikosti.

(4) Pro jazyk $A \in PP$ zkonstruujte pravděpodobnostní Turingův stroj přijímající A v polynomiálním čase takový, že pro žádné vstupní slovo α neexistuje přesně polovina přijímajících výpočtů. Ukažte, že v definici PP lze použít libovolné číslo v intervalu $(0,1)$. Zformalizujte a dokažte.

(5) Dokažte, že $A \in PP$ právě když existuje $Q \in P$ a polynom p takové, že $x \in A$, právě když existuje více než polovina slov y takových, že $|y| \leq p(|x|)$ a $< x, y > \in Q$.

(6) Dokažte, že $\#SAT$ je self-reducibilní.

(7) Ukažte, že $NP \subseteq BPP$ implikuje $NP = R$.

(8) BPP a ZPP jsou uzavřené na m-redukci, dokažte. Rozhodněte a zdůvodněte zda jsou také uzavřené ma polynomiální Turingovu redukci.

(9) Ukažte, že $P \neq R$ implikuje, že $DEXT \neq EXPSPACE$.

(10) Ukažte, že pro každé přirozené číslo k platí
$\Sigma_k/poly = \bigcup\{\Sigma_k(S) \mid S$ je řídká množina$\}$,
$\Pi_k/poly = \bigcup\{\Pi_k(S) \mid S$ je řídká množina$\}$,
$\Delta_k/poly = \bigcup \Delta_k(S) \mid S$ je řídká množina$\}$,
$PH/poly = \bigcup\{PH(S) \mid S$ je řídká množina$\}$.

(11) Ukažte, že když $\Sigma_k/poly = \Pi_k/poly$ pro nějaké k, pak $\Sigma_k/poly = PH/poly$ a $\Sigma_{k+2} = \Pi_{k+2}$.

(12) Ukažte, že následující tvrzení jsou ekvivalentní:

   (a) polynomiální hierarchie kolapsuje;

   (b) pro každou množinu $A \in PH$, polynomiální hierarchie pro A kolapsuje;

   (c) existuje množina $A \in PH$, že polynomiální hierarchie pro A kolapsuje;

   (d) existuje $A \in PH$ taková, že $P(A) = NP(A)$.

1/4

22.02.2010 Mo.
PETER ČERNO

EXAM: STRUKTURÁLNI SLOŽITOST I

(1) $P = PSPACE \Leftrightarrow PF = PSPACEF$.

$\boxed{\Leftarrow)}$ NECH $L \in PSPACE$, TJ. EXISTUJE DTS M PRACUJÚCI V POLYNOMIÁLNOM PRIESTORE TAKÝ, ŽE $L(M) = L$. UVAŽUJME DTS N, KTORÝ VZNIKNE Z M PRIDANÍM VÝSTUPNEJ PÁSKY, NA KTORÚ N ZAPÍŠE 1 $\Leftrightarrow$ M PRIJÍMA VSTUPNÉ SLOVO. V OPAČNOM PRÍPADE N ZAPÍŠE NA VÝSTUPNÚ PÁSKU 0.

POZNÁMKA: MÔŽEME PREDPOKLADAŤ, ŽE M SA VŽDYCKY ZASTAVÍ. AK BY TOMU TAK NEBOLO, TAK SI STAČÍ UVEDOMIŤ, ŽE AK M POTREBUJE NA VSTUP DĹŽKY n PRIESTOR NAJVIAC $s(n)$, POTOM POČET KONFIGURÁCII M NA VSTUPE DĹŽKY n JE OHRANIČENÝ ZHORA ČÍSLOM $2^{c \cdot s(n)}$, PRE NEJAKÚ KONŠTANTU c. NA DTS M PRIDÁME ŠPECIÁLNU PÁSKU, KTORÚ NA ZAČIATKU VÝPOČTU VYNULUJEME $s(n)$ NULAMI, A NÁSLEDNE NA NEJ POČÍTAME VYKONANÉ KROKY V SÚSTAVE O ZÁKLADE c. AK SA TENTO COUNTER ZAPLNÍ, TJ. AK SME VYKONALI $2^{c \cdot s(n)}$ KROKOV, VÝPOČET SA ZACYKLIL, A MÔŽME SKONČIŤ V ODMIETAJÚCOM STAVE.

ĽAHKO NAHLIADNUŤ, ŽE N POČÍTA CHARAKTERISTICKÚ FUNKCIU c_L JAZYKA L.

NAVIAC N PRACUJE V POLYNOMIÁLNOM PRIESTORE, TAKŽE PODĽA PREDPOKLADU $C_L \in PF$.

$\Rightarrow$ EXISTUJE DTS N' PRACUJÚCI V POLYNOMIÁLNOM ČASE, KTORÝ POČÍTA C_L. K N' TRIVIÁLNE ZOSTROJÍME DTS M', KTORÝ PRIJÍMA VSTUPNÉ SLOVO $\Leftrightarrow$ N' VYPÍŠE NA VÝSTUPNÚ PÁSKU 1, (A V OPAČNOM PRÍPADE ZAMIETA VSTUPNÉ SLOVO)

ZREJME N' PRACUJE V POLYNOMIÁLNOM ČASE A $L(N') = L$, TAKŽE $L \in P$.

DOKÁZALI SME, ŽE $PSPACE \subseteq P$.

OPAČNÁ INKLÚZIA $P \subseteq PSPACE$ PLATÍ TRIVIÁLNE.

$\boxed{\Rightarrow)}$ NECH f JE ĽUBOVOĽNÁ FUNKCIA SPOČÍTATEĽNÁ V POLYNOMIÁLNOM PRIESTORE.

DEFINUJME $\underline{\underline{prefix(f)}} = \{ \langle x, y \rangle \mid \exists z : f(x) = yz \}$.

$prefix(f) \in PSPACE$, PRETOŽE $f(x)$ VIEME SPOČÍTAŤ V POL. PRIESTORE VZHĽADOM K DĹŽKE SLOVA x A TÝM PÁDOM AJ VZHĽADOM K DĹŽKE CELÉHO VSTUPU $\langle x, y \rangle$.

PODĽA PREDPOKLADU $prefix(f) \in P$.

POMOCOU NASLEDUJÚCEHO ALGORITMU SPOČÍTAME $f(x)$ V POLYNOMIÁLNOM ČASE

(TÁTO METÓDA SA TIEŽ NAZÝVA „PREFIX SEARCHING").

22.02.2010 M.
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

```
VSTUP x
Y := λ
loop
  | if <x, Y0> ∈ prefix(f) then Y := Y0
  | else if <x, Y1> ∈ prefix(f) then Y := Y1
  | else break loop
end loop
output Y
```

VONKAJŠÍ CYKLUS JE VYKONANÝ $|f(x)|$ - KRÁT, ČO JE POLYNOMIÁLNE VZHĽADOM K $|x|$.
KAŽDÁ ITERÁCIA SA DOTAZUJE NA prefix$(f) \in P$, PRIČOM DĹŽKA DOTAZU:
$|\langle x, Y? \rangle|$ JE POLYNOMIÁLNA VZHĽADOM K $|x|$.
$\Rightarrow$ f JE SPOČÍTATEĽNÁ V POLYNOMIÁLNOM ČASE, TJ. $f \in PF$.

DOKÁZALI SME $PSPACEF \subseteq PF$.
OPAČNÁ INKLÚZIA $PF \subseteq PSPACEF$ PLATÍ TRIVIÁLNE.

□

22.02.2010 Po
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(2) $P = NP \iff$ KAŽDÁ HONEST FUNKCIA $f \in PF$ MÁ INVERZNÚ FUNKCIU V PF.

$\boxed{\Rightarrow)}$ $f \in PF$ JE HONEST A p JE PRÍSLUŠNÝ POLYNÓM.

UVAŽUJME NASLEDUJÚCU MNOŽINU:

$\text{prefix-inv}(f) := \{ \langle x, y \rangle \mid x$ JE PREFIX TAKÉHO z, ŽE $|z| \leq p(|y|)$ A $f(z) = y \}$.

NASLEDUJÚCI ALGORITMUS DOKAZUJE $\text{prefix-inv}(f) \in NP$:

- VSTUP $\langle x, y \rangle$
- UHÁDNI z TAKÉ, ŽE $|z| \leq p(|y|)$
- SKONTROLUJ, ŽE x JE PREFIX z
- SKONTROLUJ, ŽE $f(z) = y$
- AK SÚ OBE PODMIENKY SPLNENÉ, POTOM PRIJMI

VZHĽADOM K PREDPOKLADU $P = NP$ MÁME $\text{prefix-inv}(f) \in P$.

NASLEDUJÚCI ALGORITMUS POČÍTA INVERZNÚ FUNKCIU K f:

- VSTUP y
- $x := \lambda$

⋮

⋮

```
loop
  if <x0, y> ∈ prefix-inv(f) then x := x0
  else if <x1, y> ∈ prefix-inv(f) then x := x1
  else break loop
end loop
if f(x) = y then output x
else reject
```

VONKAJŠÍ CYKLUS JE VYKONANÝ NAJVIAC $p(|y|)$-KRÁT.
KAŽDÁ ITERÁCIA SA DOTAZUJE NA prefix-inv$(f) \in P$,
PRIČOM DĹŽKA DOTAZU JE POLYNOMIÁLNA VZHĽADOM K $|y|$.
PODMIENKU $f(x) = y$ MOŽNO SKONTROLOVAŤ
V POLYNOMIÁLNOM ČASE VZHĽADOM K $|y|$,
PRETOŽE $|x| \leq p(|y|)$.

$\Rightarrow$ ALGORITMUS PRACUJE V POL. ČASE VZHĽADOM K $|y|$.
ĽAHKO NAHLIADNUŤ, ŽE POČÍTA INVERZNÚ FUNKCIU K FUNKCII f:

$g(y)$ JE DEFINOVANÉ $\Leftrightarrow \exists x : (f(x)$ JE DEF. A $f(x) = y)$
(VYPLÝVA Z POSLEDNEJ PODMIENKY if $f(x) = y$ then ...)
NAVIAC AK $\exists x : (f(x)$ JE DEF. A $f(x) = y)$ PRE DANÉ y,
POTOM (PODĽA DEFINÍCIE prefix-inv(f))
ALGORITMUS NÁJDE TAKÉ x, PRE KTORÉ $|x| \leq p(|y|)$
(PRETOŽE f JE HONEST PRE POLYNÓM p).

22.02.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

$\boxed{\Leftarrow)}$ NECH M JE NEDETERMINISTICKÝ TS PRACUJÚCI V POLYNOMIÁLNOM ČASE.
NECH p JE POLYNÓM TAKÝ, ŽE DO $p(n)$ SYMBOLOV DOKÁŽEME ZAKÓDOVAŤ VÝPOČET M NAD ĽUBOVOĽNÝM VSTUPOM DĹŽKY n.
DEFINUJME:

$\mathrm{comp}(M) = \{ \langle x, y \rangle \mid x$ KÓDUJE PRIJÍMAJÚCI VÝPOČET M NA VSTUPE y A $|x| \leq p(|y|) \}$

$$f(\langle x,y \rangle) = \begin{cases} y & \text{AK } \langle x,y \rangle \in \mathrm{comp}(M) \\ \text{NEDEFINOVANÉ} & \text{INAK} \end{cases}$$

IHNEĎ VIDÍME, ŽE $\mathrm{comp}(M) \in P \Rightarrow f$ JE SPOČÍTATEĽNÁ V POLYNOMIÁLNOM ČASE, TJ. $f \in PF$.
NAVIAC AK y JE V OBORE HODNÔT f, POTOM EXISTUJE $\langle x,y \rangle$: $f(\langle x,y \rangle) = y$, TJ. $\langle x,y \rangle \in \mathrm{comp}(M)$ A DĹŽKA $\langle x,y \rangle$ JE $O(p(|y|) + |y|)$, ČO JE POLYNÓM VZHĽADOM K $|y|$.
$\Rightarrow f$ JE HONEST A JE SPOČÍTATEĽNÁ V POLYNOMIÁLNOM ČASE.
PODĽA PREDPOKLADU K NEJ EXISTUJE INVERZNÁ FUNKCIA g SPOČÍTATEĽNÁ V POLYNOMIÁLNOM ČASE.

PODĽA DEFINÍCIE INVERZNEJ FUNKCIE g K FCII. f
y JE V OBORE HODNÔT FUNKCIE f $\Leftrightarrow$
$g(y)$ JE DEFINOVANÉ. NAVYAC $f(g(y)) = y$.
TOTO JE ROZHODNUTEĽNÉ V POLYNOMIÁLNOM ČASE, PRETOŽE OBE FUNKCIE f AJ g $\in PF$.
$\Rightarrow$ OBOR HODNÔT FUNKCIE f $\in P$.

NAKONIEC SI STAČÍ VŠIMNÚŤ, ŽE y JE V OBORE HODNÔT FUNKCIE f $\Leftrightarrow$ EXISTUJE x KÓDUJÚCE PRIJÍMAJÚCI VÝPOČET M NAD SLOVOM y.
$\Rightarrow$ $L(M) \in P$.

DOKÁZALI SME $NP \subseteq P$.
OPAČNÁ INKLÚZIA $P \subseteq NP$ PLATÍ TRIVIÁLNE. $\square$

23.02.2010 Tu
PETER ČERNO

EXAM: STRUKTURÁLNI SLOŽITOST I

(3) $f \in PF \Rightarrow \forall A \in P : f^{-1}(A) \in P$

MAJME $f \in PF$ A $A \in P$

$f^{-1}(A) = \{ x \mid f(x) \in A \}$

VEZMIME ĽUBOVOĽNÉ SLOVO x ZO VSTUPNEJ ABECEDY FUNKCIE f. NASLEDUJÚCI ALGORITMUS OVERÍ, ČI $x \in f^{-1}(A)$:

```
VSTUP x
Y := f(x)   (V PRÍPADE, ŽE f NIE JE DEFINOVANÁ
             NA VSTUPE x, ODMIETNEME, TJ. Reject)
if Y ∈ A then Accept
else Reject
```

Y VIEME SPOČÍTAŤ V POLYNOMIÁLNOM ČASE $p(|x|)$ (PRETOŽE $f \in PF$) $\Rightarrow$ DĹŽKA $|Y|$ JE OHRANIČENÁ ZHORA POLYNÓMOM $p(|x|)$.

DOTAZ $Y \in A$ SPOČÍTAME V POLYNOMIÁLNOM ČASE VZHĽADOM K $|Y|$ $\Rightarrow$ AJ VZHĽADOM K $|x|$.

$\Rightarrow$ CELÝ ALGORITMUS PRACUJE V POLYNOMIÁLNOM ČASE, TAKŽE $f^{-1}(A) \in P$. $\square$

(4) $A \in NP \iff \exists$ HONEST $f \in PF : A = \{ f(x) \mid x \in D(f) \}$

$\boxed{\Rightarrow)}$ NECH $A \in NP$ A M JE NTS PRACUJÚCI V POLYNOMIÁLNOM ČASE TAKÝ, ŽE $L(M) = A$.

VYUŽIJEME MYŠLIENKU, KTORÚ SME POUŽILI AJ V PRÍKLADE (2), TJ. NECH p JE POLYNÓM TAKÝ, ŽE DO $p(n)$ SYMBOLOV DOKÁŽEME ZAKÓDOVAŤ VÝPOČET M NAD ĽUBOVOĽNÝM VSTUPOM DĹŽKY n.

DEFINUJME:

$\text{comp}(M) = \{ \langle x, y \rangle \mid x$ KÓDUJE PRIJÍMAJÚCI VÝPOČET M NAD VSTUPOM y A $|x| \leq p(|y|) \}$

$$f(\langle x, y \rangle) = \begin{cases} y & \text{AK } \langle x, y \rangle \in \text{comp}(M) \\ \text{NEDEFINOVANÉ} & \text{INAK} \end{cases}$$

AKO SME UŽ UKÁZALI V PRÍKLADE (2), f JE HONEST FUNKCIA SPOČÍTATEĽNÁ V POL. ČASE.

DOKÁŽME, ŽE $A = \{ f(w) \mid w \in D(f) \}$

a) $y \in A \Rightarrow$ EXISTUJE PRIJÍMAJÚCI VÝPOČET M NAD VSTUPOM y, KTORÝ MOŽNO ZAKÓDOVAŤ DO SLOVA x, A NAVIAC $|x| \leq p(|y|)$.

$\Rightarrow \langle x, y \rangle \in \text{comp}(M) \Rightarrow f(\langle x, y \rangle) = y$.

b) VEZMIME SI ĽUBOVOĽNÉ SLOVO w, PRE KTORÉ JE DEFINOVANÉ $f(w)$ A $f(w) = y$. POTOM w JE NUTNE TVARU $w = \langle x, y \rangle$, KDE x JE KÓD PRIJÍMAJÚCEHO VÝPOČTU M NAD $y \Rightarrow y \in A$.

23.02.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNA SLOŽITOST I

$\boxed{\Leftarrow)}$ NECH $f \in PF$ JE HONEST FUNKCIA A p JE PRÍSLUŠNÝ DOSVEDČUJÚCI POLYNÓM, TJ. PRE KAŽDÉ y Z OBORU HODNÔT f EXISTUJE x : $f(x) = y$ A $|x| \leq p(|y|)$.

NECH $A = \{ f(x) \mid x$ JE V DEFINIČNOM OBORE $f \}$

NASLEDUJÚCI NEDETERMINISTICKÝ ALGORITMUS PRIJÍMA PRÁVE MNOŽINU A :

- VSTUP y
- UHÁDNI x TAKÉ, ŽE $|x| \leq p(|y|)$
- AK $f(x) = y$ POTOM PRIJMI.

ĽAHKO NAHLIADNUŤ, ŽE UVEDENÝ ALGORITMUS POPISUJE PRÁCU NTS M PRACUJÚCEHO V POLYNOM. ČASE A NAVIAC $L(M) = A$. $\Rightarrow A \in NP$. $\square$

V NASLEDUJÚCOM PREDPOKLADÁME, ŽE f JE ČASOVO SKONŠTRUOVATEĽNÁ FUNKCIA $\mathbb{N} \to \mathbb{N}$.

(5) $P = NP \Rightarrow$

a) $DTIME(f^{O(1)}) = NTIME(f^{O(1)})$

b) $DTIME(2^{O(f)}) = NTIME(2^{O(f)})$

a) NECH $L \in NTIME(f^{O(1)})$ A NECH M JE NTS PRIJÍMAJÚCI L V ČASE $f^c(n)$ PRE NEJAKÚ KONŠTANTU c.
DEFINUJME $L' = \{ w10^{f^c(|w|)} \mid w \in L \}$.
POTOM EXISTUJE NTS PRIJÍMAJÚCI L' V LINEÁRNOM ČASE - NAJSKÔR NÁJDE 1, KTORÁ JE NAJVIAC VPRAVO, A POTOM SIMULUJE M NA SLOVE w NAČAVO OD TEJTO 1. - ještě musí otestovat zda za 1 je $f^c(|w|)$ 0. !!
PODĽA PREDPOKLADU $L' \in P$.
NECH M' JE DTS PRIJÍMAJÚCI L' V POLYN. ČASE.
Z M' ZOSTROJÍME DTS PRIJÍMAJÚCI L V ČASE $f^{O(1)}$, KTORÝ NAJSKÔR K VSTUPU w PRILEPÍ CHVOST $10^{f^c(|w|)}$, A POTOM SIMULUJE POLYNOMIÁLNY DTS M' NA TOMTO ROZŠÍRENOM VSTUPE $\Rightarrow L \in DTIME(f^{O(1)})$.

b) DOKAZUJE SA TAK ISTO AKO a), AKURÁT VŠADE NAMIESTO $10^{f^c(|w|)}$ PÍŠEME $10^{2^{cf(|w|)}}$, A NAMIESTO $f^{O(1)}$ PÍŠEME $2^{O(f)}$. $\square$

POZNÁMKA: OPAČNÉ INKLÚZIE PLATIA TRIVIÁLNE

24. 02. 2010 We
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(6) $P = PSPACE \Rightarrow$

a) $DTIME(f^{O(1)}) = DSPACE(f^{O(1)})$

b) $DTIME(2^{O(f)}) = DSPACE(2^{O(f)})$

a) NECH $L \in DSPACE(f^{O(1)})$ A NECH M JE DTS PRIJÍMAJÚCI L V PRIESTORE $f^c(n)$ PRE NEJAKÚ KONŠTANTU c.

DEFINUJME $L' = \{ w10^{f^c(|w|)} \mid w \in L \}$.

POTOM EXISTUJE DTS PRIJÍMAJÚCI L' V LINEÁRNOM PRIESTORE – NAJSKÔR NÁJDEME 1, KTORÁ JE NAJVIAC VPRAVO, A POTOM SIMULUJEME M NA SLOVE w NALAVO OD TEJTO 1. – overiť počet 0!

PODĽA PREDPOKLADU $L' \in P$.

NECH M' JE DTS PRIJÍMAJÚCI L' V POL. ČASE.

Z M' ZOSTROJÍME DTS PRIJÍMAJÚCI L V ČASE $f^{O(1)}$, KT. NAJSKÔR K VSTUPU w PRILEPÍ CHVOST $10^{f^c(|w|)}$, A POTOM SIMULUJE POLYNOMIÁLNY DTS M' NA TOMTO ROZŠÍRENOM VSTUPE $\Rightarrow L \in DTIME(f^{O(1)})$.

b) DOKAZUJE SA TAK ISTO AKO a), AKURÁT VŠADE NAMIESTO $10^{f^c(|w|)}$ PÍŠEME $10^{2^{c f(|w|)}}$, A NAMIESTO $f^{O(1)}$ PÍŠEME $2^{O(f)}$. □

POZNÁMKA: OPAČNÉ INKLÚZIE PLATIA TRIVIÁLNE.

(7) $DTIME(2^{cn}) \subseteq NP$ PRE NEJAKÉ c $\Rightarrow$

a) $DEXT \subset NP = PSPACE = EXPTIME$

b) $\forall c > 0 : DTIME(2^{cn}) \neq NP$.

a) ZREJME PLATÍ $NP \subseteq PSPACE \subseteq EXPTIME$

STAČÍ DOKÁZAŤ, ŽE $EXPTIME \subseteq NP$,

POTOM BUDE $NP = PSPACE = EXPTIME$

A KEĎŽE $DEXT \subset EXPTIME$, IHNEĎ DOSTANEME a)

NECH $L \in EXPTIME$, TJ. $L \in DTIME(2^{n^k})$

PRE NEJAKÉ PRIRODZENÉ $k > 0$.

DEFINUJME $L' = \{ w10^{\lceil 1/c \rceil \cdot |w|^k} \mid w \in L \}$

NECH M JE DTS PRACUJÚCI V ČASE 2^{n^k} PRIJÍMAJÚCI L.

POTOM EXISTUJE DTS PRIJÍMAJÚCI L' V ČASE $O(2^{cn})$

NAJSKÔR NÁJDEME NAJPRAVEJŠIU 1, A POTOM

SIMULUJEME M NA SLOVE w NAČALO OD TEJTO 1

ješte 0 !

SIMULÁCIA PREBEHNE V ČASE :

$$2^{|w|^k} \leq 2^{c \cdot \lceil 1/c \rceil \cdot |w|^k} \leq 2^{c \cdot |\underbrace{w10^{\lceil 1/c \rceil |w|^k}}_{\text{VSTUPNÉ SLOVO DĹŽKY } n}|}$$

TJ. TENTO DTS SKUTOČNE PRACUJE V ČASE $O(2^{cn})$.

$\Rightarrow L' \in DTIME(2^{cn})$ A PODĽA

PREDPOKLADU NUTNE $L' \in NP$.

NECH M' JE NTS PRIJÍMAJÚCI L' V POL. ČASE.

K M' ZOSTROJÍME NTS PRIJÍMAJÚCI L V POL. ČASE

TAK, ŽE KU VSTUPNÉMU w NAJSKÔR PRIPOJÍME

CHVOST $10^{\lceil 1/c \rceil \cdot |w|^k}$ A POTOM SPUSTÍME M'.

24.02.2010 We
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

VIDÍME, ŽE $L \in NP$, ČÍM SME DOKÁZALI ROVNOSŤ $NP = PSPACE = EXPTIME$.

a) PLYNIE Z $DEXT \subset EXPTIME$.

b) NECH PRE NEJAKÉ $c > 0$: $DTIME(2^{cn}) = NP$. POTOM (PODĽA a)) $NP = PSPACE = EXPTIME$, T.J. $DTIME(2^{cn}) = EXPTIME$, ČO JE V ROZPORE S VETOU O ČASOVEJ HIERARCHII, PRETOŽE UŽ $2^{n^2} \in \omega(2^{cn} \cdot \log(2^{cn})) = \omega(n\, 2^{cn})$. $\square$

25.02.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOSŤ I

(8) DEXT $\neq$ PSPACE

PREDPOKLADAJME DEXT = PSPACE (PRE SPOR)
POTOM ŠPECIÁLNE $DTIME(2^{cn}) \subseteq PSPACE$ PRE ĽUBOVOĽNÉ $c > 0$. VEZMIME NAPR. $c = 1$.
DOKÁŽME (PODOBNE AKO V PRÍKLADE (7)) IMPLIKÁCIU
$$DTIME(2^n) \subseteq PSPACE \Rightarrow PSPACE = EXPTIME.$$
NECH L JE ĽUBOVOĽNÝ JAZYK Z EXPTIME, TJ. $L \in DTIME(2^{n^k})$, KDE k JE NEJAKÉ PRIR. ČÍSLO > 0.
DEFINUJME $L' = \{ w10^{|w|^k} \mid w \in L \}$.
NECH M JE DTS PRIJÍMAJÚCI L V ČASE 2^{n^k}.
PODOBNE AKO V PRÍKLADE (7) ZOSTROJÍME DTS PRIJÍMAJÚCI L' V ČASE $O(2^n)$.
PODĽA PREDPOKLADU $L' \in PSPACE$. A KEĎŽE $L \leq_m L'$ A TRIEDA PSPACE JE UZAVRETÁ NA m-REDUKCIE, NUTNE $L \in PSPACE$.
TO DOKAZUJE $EXPTIME \subseteq PSPACE$, TJ. PSPACE = EXPTIME.
AVŠAK DEXT $\subset$ EXPTIME, ČO JE SPOR S PREDPOKLADOM DEXT = PSPACE. $\square$

<u>INÝ DÔKAZ</u>: PSPACE JE UZAVRETÝ NA $\leq_m$, KDEŽTO DEXT NIE JE. TO, ŽE DEXT NIE JE UZAVRETÝ NA $\leq_m$ VYPLÝVA Z PRÍKLADU (14), V KTOROM DOKÁŽEME, ŽE KE JE EXPTIME-ÚPLNÝ JAZYK, A NAVIAC KE $\in$ DEXT. NAVIAC VIEME, ŽE DEXT $\subset$ EXPTIME.
$KE = \{ \langle M, x, t \rangle \mid M$ JE KÓD DTS; x SLOVO, KT. PRIJÍMA M V ČASE $t \}$.

25.02.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(9) OPRAVENÉ RIEŠENIE:

NAJSKÔR UKÁŽEME, ŽE $L \in NLOG$:

VSTUP: $z = \langle G, u, v \rangle$, KDE G JE KÓD GRAFU $G = (V, E)$ A $u, v \in V$.
ODPOVEĎ: ÁNO, AK EXISTUJE CESTA $u \rightsquigarrow v$ V G.

- - - - - - - - - -

NECH i JE INDEX VRCHOLU u VO V
A j JE INDEX VRCHOLU v VO V
actual $\leftarrow i$
counter $\leftarrow 0$, $n \leftarrow |V|$
AK $i = j$, POTOM PRIJMI A SKONČI
DOKEDY counter $< n$ VYKONAJ:
    NEDETERMINISTICKY UHÁDNI next INDEX DO V
    AK (actual, next) $\in E_i$, POTOM
        AK next $= j$, POTOM PRIJMI A SKONČI
        INAK actual $\leftarrow$ next
    counter $\leftarrow$ counter $+ 1$
KONIEC CYKLU
ODMIETNI A SKONČI

> E_i OZNAČUJE MNOŽINU HRÁN E, KDE NAMIESTO VRCHOLOV BERIEME ICH INDEXY

ALGORITMUS PRACUJE V PRIESTORE $O(\log |z|)$:

1. INDEX VRCHOLU $\in V$ ZABERÁ PRIESTOR NAJVIAC $\lceil \log_2 n \rceil$.

2. V PRIEBEHU CELÉHO ALGORITMU POUŽÍVAME IBA INDEXY i, j, actual, next, KTORÉ SPOLU ZABERAJÚ LOGARITMICKÝ PRIESTOR

3. counter $\leq n \leq |z|$, TAKŽE OBE PREMENNÉ counter AJ n MOŽNO KÓDOVAŤ V LOGARITMICKOM PRIESTORE.

KOREKTNOSŤ ALGORITMU JE ZREJMÁ, POSTUPNE BUDUJEME CESTU Z u DO v. VŽDY SI PAMÄTÁME POSLEDNÝ VRCHOL CESTY: actual A NEDETERM. VOLÍME ĎALŠÍ VRCHOL CESTY: next. AK SÚ u A v V JEDNEJ KOMPONENTE, POTOM MEDZI NIMI ZREJME EXISTUJE CESTA O NAJVIAC n VRCHOLOCH.

ĎALEJ UKÁŽEME, AKO K VRCHOLU u (RESP. v) NÁJDEME JEHO INDEX i (RESP. j) V MNOŽINE V:

KAŽDÚ BUNKU (BIT) VSTUPNÉHO SLOVA z MOŽNO INDEXOVAŤ V LOG. PRIESTORE $O(\log_2 |z|)$.
NAJSKÔR POLOŽÍME $i \leftarrow 1$ A POKÚSIME SA OVERIŤ, ČI PRVÝ (VO VŠEOBECNOSTI i-TY) VRCHOL u_i MNOŽINY V JE ZHODNÝ S u. TO UROBÍME TAK, ŽE VRCHOLY u_i A u POROVNÁME BUNKU PO BUNKE (BIT PO BITE). MÔŽEME POUŽIŤ NAPR. NEJAKÝ INDEX bit, KTORÝ INDEXUJE, KTORÚ BUNKU (BIT) POROVNÁVAME. PODSTATNÉ JE, ŽE INDEX bit ZABERÁ PRIESTOR NAJVIAC $O(\log_2 |z|)$.
POSTUPNE SKÚŠAME $\forall$ INDEXY, AŽ NÁJDEME $u_i = u$.

25.02.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

PODOBNE MOŽNO V LOG. PRIESTORE OVERIŤ, ČI (actual, next) $\in E_i$: PRECHÁDZAME POSTUPNE HRANY $(x,y) \in E$ NA VSTUPE z, A PRE KAŽDÚ OVERÍME, ČI:

$u_{actual} = x$ A $u_{next} = y$.

AK ÁNO, POTOM PLATÍ (actual, next) $\in E_i$.

VIDÍME, ŽE VŠETKY OPERÁCIE ALGORITMU PRACUJÚ V LOG. PRIESTORE, ČÍM SME DOKÁZALI, ŽE $L \in NLOG$.

DOKÁŽME EŠTE, ŽE L JE NLOG-ÚPLNÝ VZHĽADOM K m-REDUKCII OBMEDZENEJ NA VÝPOČET V LOG-PRIESTORE.

NECH $A \in NLOG$, TJ. EXISTUJE NTS M PRACUJÚCI V PRIESTORE $c \cdot \log n$ TAKÝ, ŽE $A = L(M)$.

PRE DANÉ VSTUPNÉ SLOVO x ZOSTROJÍME ZADANIE $f(x) = \langle G, u, v \rangle$ PRE PROBLÉM L TAKÉ, ŽE $x \in A \Leftrightarrow f(x) \in L$.

$G = (V, E)$ BUDE GRAF VŠETKÝCH KONFIGURÁCIÍ M NAD VSTUPNÝM SLOVOM x,

u BUDE INICIÁLNA KONFIGURÁCIA M NAD x

A v BUDE ŠPECIÁLNA PRIJÍMAJÚCA KONFIGURÁCIA, DO KTOREJ VEDÚ HRANY ZO VŠETKÝCH PRIJÍMAJÚCICH KONFIGURÁCIÍ M NAD SLOVOM x.

TAKÝ GRAF MOŽNO K DANÉMU VSTUPNÉMU SLOVU x VYGENEROVAŤ V LOG. PRIESTORE $O(\log |x|)$:

1. KAŽDÁ KONFIGURÁCIA M NAD x ZABERÁ PRIESTOR NAJVIAC $c \log |x|$ + PRIESTOR NA ULOŽENIE POZÍCIE HLAVY NA VSTUPNEJ PÁSKE $\Rightarrow$ TJ. SPOLU $(c+1) \log |x|$ BUNIEK.
2. PRE KAŽDÉ SLOVO DLHÉ $(c+1) \log |x|$ BUNIEK (BITOV) VIEME V LOG. PRIESTORE OVERIŤ, ČI SA JEDNÁ O KOREKTNÚ KONFIGURÁCIU M NAD x, A NAVIAC ČI JE TÁTO KONFIGURÁCIA INICIÁLNA ALEBO PRIJÍMAJÚCA
3. PRE KAŽDÚ HRANU, TJ. DVOJICU (I_1, I_2) KONFIG. VIEME V LOG. PRIESTORE OVERIŤ, ČI MOŽNO PREJSŤ Z I_1 V JEDNOM KROKU DO I_2 V SÚLADE S PRECHODOVOU FUNKCIOU M NAD SLOVOM x.

$\Rightarrow$ DOKÁŽEME VYGENEROVAŤ $f(x) = \langle G, u, v \rangle$ V LOG. PRIESTORE $O(\log |x|)$, ČÍM SME DOKÁZALI, ŽE $A \leq_m^{\log} L$, TAKŽE L JE NLOG-ÚPLNÝ PROBLÉM.

$\square$

28.02.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

(11) NP JE UZAVRETÁ VZHĽADOM K $\leq_T$
$\Leftrightarrow$ NP JE UZAVRETÁ NA DOPLNKY.

$\boxed{\Rightarrow)}$ NECH $A \in NP$ A M JE NTS PRACUJÚCI V POL. ČASE TAKÝ, ŽE $L(M) = A$.
DOKÁŽEME, ŽE $\bar{A} \in NP$.
UVAŽUJME NASLEDUJÚCI DTS N S ORÁKULOM PRACUJÚCI V POL. ČASE (DOKONCA V LINEÁRNOM)

VSTUP x, ORÁKULUM A
if $x \in A$ then Reject
else Accept

ZREJME $L(N, A) = \bar{A}$, TJ. $\bar{A} \leq_T A$.
PODĽA PREDPOKLADU $\bar{A} \in NP$.

$\boxed{\Leftarrow)}$ NECH $A \in NP$, $B \leq_T A$. CHCEME DOKÁZAŤ, ŽE $B \in NP$. NECH M_1 JE DTS PRACUJÚCI V POL. ČASE TAKÝ, ŽE $B = L(M_1, A)$.
NECH M_2 JE NTS PRACUJÚCI V POL. ČASE PRIJÍMAJÚCI JAZYK A, A KEĎŽE PODĽA PREDPOKLADU $\bar{A} \in NP$, NECH M_3 JE NTS PRACUJÚCI V POL. ČASE PRIJÍMAJÚCI JAZYK $\bar{A}$.
NASLEDUJÚCI NTS M PRACUJE V POL. ČASE A PRIJÍMA JAZYK B:

M SIMULUJE PRÁCU STROJA M_1 NA VSTUPE x, A VŽDY KEĎ M_1 VSTÚPI DO STAVU QUERY (DOTAZ), M ZAVOLÁ NASLEDUJÚCU SUBRUTINU, ABY ZODPOVEDAL NA DOTAZ:

NECH w JE DOTAZOVACIE SLOVO
NEDETERMINISTICKY UHÁDNI ODPOVEĎ ÁNO ALEBO NIE
AK BOL ODHAD ÁNO, POTOM:
  SIMULUJ M_2 NA w
  AK M_2 PRIJÍMA w, POTOM POKRAČUJ
    V PRÁCI STROJA M VO VETVE YES (ÁNO)
  V OPAČNOM PRÍPADE SKONČI VÝPOČET
    V ODMIETAJÚCOM STAVE, TJ. Reject
AK BOL ODHAD NIE, POTOM:
  SIMULUJ M_3 NA w
  AK M_3 PRIJÍMA w, POTOM POKRAČUJ
    V PRÁCI STROJA M VO VETVE NO (NIE)
  V OPAČNOM PRÍPADE SKONČI VÝPOČET
    V ODMIETAJÚCOM STAVE, TJ. Reject
KONIEC SUBRUTINY

ĽAHKO NAHLIADNUŤ, ŽE M PRIJÍMA PRÁVE JAZYK $L(M_1, A) = B$ V NEDETERMINISTICKY POL. ČASE, TJ. $B \in NP$. $\square$

28.02.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(12) $K(A)$ JE $NP(A)$-ÚPLNÝ JAZYK VZHĽADOM K m-REDUKCII.

NAJSKÔR UKÁŽEME, ŽE $K(A) \in NP(A)$:

VSTUP $z = \langle M, x, 1^t \rangle$, ORÁKULUM A
NEDETERMINISTICKY UHÁDNI SLOVO w, $|w| \leq t^2$
SKONTROLUJ, ČI w KÓDUJE POSTUPNOSŤ NAJVIAC t KONFIGURÁCIÍ M NAD SLOVOM x TAKÝCH, ŽE PRVÁ KONFIGURÁCIA JE INICIÁLNA KONFIGURÁCIA M NAD SLOVOM x A KAŽDÁ ĎALŠIA KONFIGURÁCIA REŠPEKTUJE PRECHODOVÚ FUNKCIU STROJA M, POPR. ODPOVEĎ ORÁKULA A NA PRÍSLUŠNÝ DOTAZ.
SKONTROLUJ, ČI POSLEDNÁ KONFIGURÁCIA JE V PRIJÍMAJÚCOM STAVE.
AK BOLI SPLNENÉ VŠETKY PODMIENKY, TAK PRIJMI z INAK ODMIETNI.

ĎALEJ UKÁŽME, ŽE $K(A)$ JE $NP(A)$-ÚPLNÝ VZHĽADOM K m-REDUKCII. NECH $L \in NP(A)$ A M JE NTS S ORÁKULOM A PRIJÍMAJÚCI L V POL. ČASE $p(|x|)$. DEFINUJME:

$$f(x) := \langle M, x, 1^{p(|x|)} \rangle$$

POTOM PLATÍ:

1. f VIEME SPOČÍTAŤ V POL. ČASE:
KÓD M NEZÁVISÍ NA x, x SKOPÍRUJEME
ZO VSTUPU V LINEÁRNOM ČASE A
$1^{p(|x|)}$ MOŽNO VYPÍSAŤ V POL. ČASE.

2. $x \in L \iff M$ S ORÁKULOM A PRIJME
x ZA NAJVIAC $p(|x|)$ KROKOV $\iff$
$f(x) = \langle M, x, 1^{p(|x|)} \rangle \in K(A)$.

TÝM SME DOKÁZALI, ŽE $L \leq_m K(A)$
PROSTREDNÍCTVOM FUNKCIE f. $\square$

(13) $KS(A)$ JE PSPACE(A)-ÚPLNÝ JAZYK
VZHĽADOM K m-REDUKCII.

$KS(A) = \{ \langle M, x, 1^t \rangle \mid M$ JE KÓD NTS S ORÁKULOM,
x SLOVO, KTORÉ M S ORÁKULOM A PRIJÍMA
V PRIESTORE $t \}$.

NAJSKÔR UKÁŽME, ŽE $KS(A) \in PSPACE(A)$.
PREDNE, AK BY M KÓDOVAL DTS S ORÁKULOM,
TAK BY SME DOKÁZALI TRIVIÁLNE SIMULOVAŤ M
NAD VSTUPOM x A ORÁKULOM A V POLYNOM.
PRIESTORE VZHĽADOM K VSTUPU $\langle M, x, 1^t \rangle$.
MUSELI BY SME LEN KONTROLOVAŤ, ČI M NEPREKROČIL
PRIESTOR t, A NAVIAC BY SME POČÍTALI, ČI POČET
KONFIGURÁCII NEPREKROČIL NEJAKÚ VHODNÚ HORNÚ MEZ.

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

KEĎŽE VŠAK M JE KÓD <u>NTS</u> S ORÁKULOM, POMÔŽEME SI TRIKOM POUŽITÝM V DÔKAZE SAVITCHOVEJ VETY.

NA VSTUPE MÁME $\langle M, x, 1^t \rangle$, KDE M JE KÓD NTS S ORÁKULOM, x JE VSTUPNÉ SLOVO A t JE HORNÁ MEZ NA PRIESTOR.
POLOŽME $k := \max\{\lceil \log_2(x) \rceil, t\}$.
k JE PRIESTOR POTREBNÝ NA ZAKÓDOVANIE JEDNEJ KONFIGURÁCIE STROJA M NAD VSTUPOM x (A ORÁKULOM A).
PREDPOKLADAJME, ŽE POČET RÔZNYCH KONFIGURÁCII M NAD VSTUPOM x JE ZHORA OHRANIČENÝ $2^{c \cdot k}$, KDE c JE VHODNÁ KONŠTANTA (UNIVERZÁLNA PRE VŠETKY VSTUPY $\langle M, x, 1^t \rangle$).

NASLEDUJÚCI DTS SIMULUJE VÝPOČET M NA VSTUPE x S ORÁKULOM A V POL. PRIESTORE.
VYUŽÍVA PRITOM VOLANIA ŠPECIÁLNEJ SUBRUTINY Reachable(I_1, I_2, j), KTORÁ VRACIA true $\Leftrightarrow$ EXISTUJE VÝPOČET Z I_1 DO I_2 POZOSTÁVAJÚCI Z NAJVIAC 2^j KROKOV (KONFIGURÁCII M NAD x).
MUSÍME PRITOM DÁVAŤ POZOR, ABY KAŽDÁ KONFIGURÁCIA M NAD x VYUŽÍVALA PRIESTOR NAJVIAC t.

VSTUP $z = \langle M, x, 1^t \rangle$

$k := \max \{ \lceil \log_2(|x|) \rceil, t \}$

NECH I_i JE INICIÁLNA KONF. M NAD x.

PRE KAŽDÚ KONEČNÚ KONFIGURÁCIU I_f M NAD x,

PRI KTOREJ M VYUŽÍVA PRIESTOR NAJVIAC t:

AK Reachable (I_i, I_f, $c \cdot k$), POTOM

PRIJMI A SKONČI

ODMIETNI

FUNKCIA Reachable (I_1, I_2, j)

AK $j=0$ POTOM

AK $I_1 = I_2$, ALEBO I_2 JE DOSIAHNUTEĽNÁ

Z I_1 NA JEDEN KROK (RESPEKTUJÚC PRECHODOVÚ

FUNKCIU M, POPR. VÝSLEDOK DOTAZU NA A)

A V OBOCH KONFIGURÁCIACH M VYUŽÍVA

PRIESTOR NAJVIAC t, POTOM return true

V OPAČNOM PRÍPADE return false

AK $j > 0$ POTOM

PRE KAŽDÚ MOŽNÚ KONFIGURÁCIU I, PRI KT.

M VYUŽÍVA PRIESTOR NAJVIAC t:

AK Reachable (I_1, I, $j-1$) &

Reachable (I, I_2, $j-1$), POTOM

return true

return false

28.02.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI ZLOŽITOST I

KAŽDÚ KONFIGURÁCIU STROJA M NAD VSTUPOM x MOŽNO KÓDOVAŤ V PRIESTORE $O(k)$, KDE $k = \max\{\lceil \log_2(|x|) \rceil, t\}$.
PODOBNE, AKO V DÔKAZE SAVITCHOVEJ VETY, MOŽNO ARGUMENTOVAŤ, ŽE CELÁ SIMULÁCIA PREBEHNE V PRIESTORE $O(k^2)$, ČO JE POLYNOMIÁLNE VEĽA VZHĽADOM K DĹŽKE VSTUPU $|\langle M, x, 1^t \rangle|$.
TÝM SME DOKÁZALI, ŽE $KS(A) \in PSPACE(A)$.
TO, ŽE $KS(A)$ JE $PSPACE(A)$ - ÚPLNÝ VZHĽADOM K m-REDUKCII DOKÁŽEME ANALOGICKY AKO V PRÍKLADE (12).
NECH $L \in PSPACE(A)$ A M JE PRÍSLUŠNÝ DTS S ORÁKULOM A PRIJÍMAJÚCI L V POLYNOM. PRIESTORE $p(|x|)$. POTOM:

$$f(x) = \langle M, x, 1^{p(|x|)} \rangle$$

JE FUNKCIA DOKAZUJÚCA $L \leq_m KS(A)$. $\square$

01. 02. 2010 Mb
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

(14) KE(A) JE EXPTIME(A)-ÚPLNÝ JAZYK VZHĽADOM K m-REDUKCII.

TVRDENIE DOKÁŽEME PRE:

KE(A) = { ⟨M, x, t⟩ | M JE KÓD DTS S ORÁKULOM, x SLOVO, KT. PRIJÍMA M S ORÁKULOM A V ČASE t }.

NAJSKÔR UKÁŽEME, ŽE KE(A) ∈ EXPTIME(A).

UVAŽUJME NASLEDUJÚCI DTS SIMULUJÚCI PRÁCU M NAD x S ORÁKULOM A:

- VSTUP z = ⟨M, x, t⟩, ORÁKULUM A
- SIMULUJ t KROKOV PRÁCE STROJA M NAD x:
- AK M PRIJALO x, TAK PRIJMI,
- INAK ODMIETNI

JEDEN KROK M MOŽNO SIMULOVAŤ V ČASE $O(|M| + |x| + t)$, T. LINEÁRNE VZHĽADOM NA DĹŽKU |M| A DĹŽKU KONFIGURÁCIE M.

prečo je tady t a nikoliv log t?

CELKOVÝ ČAS JE POTOM $O(t(|M| + |x| + t))$

A KEĎŽE $t \leq 2^{|z|}$, DOSTÁVAME ČAS $O(2^{2|z|})$

- toto neplatí, zápis je log t a proto čas vychází $O(2^{\text{délka vstupu}})$!

VIDÍME, ŽE DOKONCA KE(A) ∈ DEXT(A).

NECH $L \in$ EXPTIME(A) A M JE DTS S ORÁKULOM PRACUJÚCI V ČASE 2^{n^i} PRE NEJAKÉ PRIRODZENÉ ČÍSLO i.

DEFINUJME:

$$f(x) = \langle M, x, 1\,0^{|x|^i - 1} \rangle$$

ne kedy se napíše binárně číslo 2^{n^i} by délky n^i bitů!

ĽAHKO NAHLIADNUŤ, ŽE $f(x)$ VIEME SPOČÍTAŤ V POLYN. ČASE VZHĽADOM K $|x|$.

NAVIAC $x \in L \iff M$ S ORÁKULOM A PRIJÍMA x V ČASE $2^{|x|^i} \iff f(x) \in KE(A)$.

$\Rightarrow$ KE(A) JE EXPTIME(A)-ÚPLNÝ. $\square$

01. 03. 2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(15) $A \in NP(B) \Leftrightarrow A \leq_m K(B)$

PRIPOMEŇME, ŽE $K(B) = \{ \langle M, x, 1^t \rangle \mid$ M JE KÓD NTS S ORÁKULOM, X SLOVO, KTORÉ PRIJÍMA M S ORÁKULOM B V ČASE t $\}$

$\boxed{\Rightarrow)}$ NECH $A \in NP(B)$, T.J. EXISTUJE NTS M S ORÁKULOM PRACUJÚCI V POLYNOMIÁLNOM ČASE p TAKÝ, ŽE $A = L(M, B)$.
UVAŽUJME $f(x) = \langle M, x, 1^{p(|x|)} \rangle$.
TRIVIÁLNE f MOŽNO SPOČÍTAŤ V POL. ČASE A $x \in A \Leftrightarrow f(x) \in K(B)$, T.J. $A \leq_m K(B)$.

$\boxed{\Leftarrow)}$ NECH PRE NEJAKÚ f SPOČÍTATEĽNÚ V POL. ČASE PLATÍ: $x \in A \Leftrightarrow f(x) \in K(B)$.
PRETOŽE $K(B) \in NP(B)$, NECH M JE NTS S ORÁKULOM PRACUJÚCI V POL. ČASE TAKÝ, ŽE $L(M, B) = K(B)$.
UVAŽUJME NASLEDUJÚCI NTS N S ORÁKULOM:

- VSTUP x, ORÁKULUM B
- SPOČÍTAJ $y = f(x)$
- SPUSTI NTS M NA VSTUPE y

M PRACUJE V NEDETERM. POLYNOMIÁLNOM ČASE VZHĽADOM K $|f(x)|$, PRIČOM $|f(x)|$ JE ZHORA OHRANIČ. POLYNÓMOM Z $|x|$. NAVIAC $L(N, B) = A$, TAKŽE $A \in NP(B)$.

$\square$

(16) UKÁŽTE, ŽE NASLEDUJÚCE VZŤAHY SÚ EKVIVALENTNÉ:

a) $B \leq^{SN} A$

b) $K(B) \leq_m K(A)$

c) $NP(B) \subseteq NP(A)$

$\boxed{a) \Rightarrow b)}$ NECH $B \in NP(A) \cap co\text{-}NP(A)$, TJ. EXISTUJÚ M_1 A M_2 NTS S ORÁKULOM PRACUJÚCE V POL. ČASE TAKÉ, ŽE $B = L(M_1, A)$, $\bar{B} = L(M_2, A)$.

AK M JE NTS S ORÁKULOM PRACUJÚCI V POL. ČASE. POTOM K NEMU VIEME NÁJSŤ NTS N PRACUJÚCI V POL. ČASE TAKÝ, ŽE $L(M, B) = L(N, A)$ PRESNE AKO V PRÍKLADE (11):

N SIMULUJE PRÁCU M NA DANOM VSTUPE x, A VŽDY KEĎ M VSTÚPI DO STAVU QUERY (DOTAZ), N ZAVOLÁ NASLEDUJÚCU SUBRUTINU:

NECH w JE DOTAZOVACIE SLOVO
NEDETERMINISTICKY UHÁDNI ODPOVEĎ guess ∈ {YES, NO}
AK guess = YES, POTOM
  SIMULUJ M_1 NA w. AK M_1 PRIJÍMA w, POTOM POKRAČUJ V PRÁCI STROJA M VO VETVE YES.
  V OPAČNOM PRÍPADE: Reject.
ANALOGICKY POSTUPUJEME V PRÍPADE AK guess = NO,
  TJ. SIMULUJEME M_2 NA w, A AK PRIJME, POKRAČUJEME V PRÁCI M VO VETVE NO ...

07.03.2010 Mo
PETER ČERNO

EXAM: STRUKTURÁLNÍ SLOŽITOST I

POVEDZME, ŽE CHCEME ROZHODNÚŤ, ČI NTS M S ORÁKULOM B PRIJÍMA DANÉ SLOVO x V ČASE t. TÚTO ÚLOHU PREVEDIEME NA PROBLÉM ČI PRÍSLUŠNÝ NTS N S ORÁKULOM A PRIJÍMA x V POLYNOMIÁLNOM ČASE $p(|x|)$ (KDE p JE HORNÁ MEDZ NA ČAS, KTORÝ POTREBUJE N), PRIČOM VŠAK DÁVAME POZOR, ABY M VYKONAL NAJVIAC t KROKOV.

PODSTATNÉ JE, ŽE Z KÓDU NTS M A VSTUPU x VIEME V POLYNOMIÁLNOM ČASE SPOČÍTAŤ KÓD NTS N A HORNÝ ODHAD $p(|x|)$ ČASOVEJ ZLOŽITOSTI N NA VSTUPE x (PRI POUŽITÍ ORÁKULA A): MÁME TOTIŽ HORNÉ ODHADY NA ČASOVÉ ZLOŽITOSTI STROJOV M_1 A M_2 A DOTAZOVACIE SLOVO w MÔŽE BYŤ NAJVIAC POLYNOMIÁLNE DLHÉ VZHĽADOM K DĹŽKE VSTUPU $|x|$.

FUNKCIA $f(\langle M, x, 1^t\rangle) = \langle N, x, 1^{p(|x|)}\rangle$ SPOČÍTATEĽNÁ V POLYNOMIÁLNOM ČASE DOKAZUJE $K(B) \leq_m K(A)$.

AK z NEKÓDUJE ŽIADNU TROJICU $\langle M, x, 1^t\rangle$, POTOM MÔŽEME POLOŽIŤ NAPR. $f(z) = z$.

Lepší zavést jazyk $Pom(A) = \langle M_1(M_2, M_3), x, t\rangle$ – M_1 spočítá x v čase t (kde se zpočítala dotaz jako 1), a M_2, M_3 řeší dotaz – ten jazyk patří do $NP(A)$, když $\langle M_1, x, t\rangle \in K(B)$ a když už $Pom(A) \leq_m K(A)$ – a hotovo!
a $K(B) \leq_m Pom(A)$

$\boxed{b) \Rightarrow c)}$

NECH $L \in NP(B)$, TJ. M JE NTS S ORÁKULOM PRACUJÚCI V POL. ČASE q TAKÝ, ŽE $L = L(M, B)$.
PODĽA PREDPOKLADU MÁME f PRACUJÚCU V DETERMINISTICKY POLYNOM. ČASE DOKAZUJÚCU $K(B) \leq_m K(A)$. TJ. f VIE ZO ZADANIA PROBLÉMU $\langle M, x, 1^t \rangle$ NAD ORÁKULOM B VYTVORIŤ V POLYN. ČASE EKVIVALENTNÉ ZADANIE PROBLÉMU $\langle N, x, 1^{p(|x|)} \rangle$ NAD ORÁKULOM A.
KEĎ POLOŽÍME $t := q(|x|)$ DOSTANEME

$$x \in L \Leftrightarrow \langle M, x, 1^t \rangle \in K(B) \Leftrightarrow \langle N, x, 1^{p(|x|)} \rangle \in K(A)$$

A KEĎŽE $K(A) \in NP(A)$, ĽAHKO NAHLIADNUŤ, ŽE AJ $L \in NP(A)$:

- VSTUP x, ORÁKULUM A
- V POL. ČASE ZOSTROJÍME $y = \langle M, x, 1^{q(|x|)} \rangle$
  (M JE PEVNE DANÉ, q JE POLYNÓM)
- V POL. ČASE SPOČÍTAME $z = f(y) = \langle N, x, 1^{p(|x|)} \rangle$
  (f PRACUJE V POL. ČASE VZHĽADOM K $|y| \Rightarrow$ AJ K $|x|$)
- AK $z \in K(A)$, POTOM Accept
- INAK Reject

(pozor na meze! – tady je to ok., ale přímo to nelze převést)!

01.03.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOSŤ I

$\boxed{c) \Rightarrow a)}$ NECH $NP(B) \subseteq NP(A)$.

CHCEME UKÁZAŤ, ŽE $B \in NP(A) \cap co\text{-}NP(A)$, TJ. $B \in NP(A) \wedge \overline{B} \in NP(A)$.

ĽAHKO NAHLIADNUŤ, ŽE $B \in NP(B)$ AJ $\overline{B} \in NP(B)$. DOKONCA $B \in P(B)$, $\overline{B} \in P(B)$. PODĽA PREDPOKLADU POTOM ALE NUTNE $B \in NP(A)$ AJ $\overline{B} \in NP(A)$, ČO BOLO TREBA DOKÁZAŤ. $\square$

(17) AK T JE TALLY MNOŽINA TAKÁ, ŽE $DEXT(T) = DEXT$, POTOM $T \in P$.

NECH $A = \{ n \mid 0^n \in T \}$, TJ. $T = tally(A)$.
NAJSKÔR SI VŠIMNIME, ŽE $A \in DEXT(T)$:

- VSTUP n, ORÁKULUM T
- SPOČÍTAJ $w = 0^n$
- AK $w \in T$, POTOM Accept,
- INAK Reject

SLOVO w ZOSTROJÍME V ČASE $n \leq 2^{\lceil \log n \rceil} = 2^{|n|}$, DOTAZ $w \in T$ TRVÁ KONŠTANTNE VEĽA $\Rightarrow A \in DEXT(T)$.
PODĽA PREDPOKLADU TIEŽ $A \in DEXT$, TAKŽE NUTNE $tally(A) = T \in P$. $\square$

(18) NECH M JE DTS S ORÁKULOM PRACUJÚCI V POL. ČASE DOKAZUJÚCI, ŽE A JE SELFREDUCIBILNÝ JAZYK. POTOM $B = L(M, B) \Rightarrow A = B$.

PREDNE $A = L(M, A)$ A NA KAŽDÝ VSTUP DĹŽKY n SA M DOTAZUJE IBA NA SLOVÁ DĹŽKY NAJVIAC $n-1$.

NECH $B = L(M, B)$. PRE SPOR NECH $A \neq B$. NECH w JE NAJKRATŠIE SLOVO TAKÉ, ŽE $w \in A \setminus B$ ALEBO $w \in B \setminus A$.

a) $w \in A \setminus B$, TJ. $w \in L(M, A)$, ALE $w \notin L(M, B)$. TO VŠAK NEMÔŽE NASTAŤ, PRETOŽE M SA V OBOCH PRÍPADOCH DOTAZUJE NA SLOVÁ DĹŽKY NAJVIAC $|w|-1$, A PODĽA DEFINÍCIE w PRE KAŽDÉ x, $|x| \leq |w|-1$ JE $x \in A \Leftrightarrow x \in B$.

PODOBNE DOSTANEME SPOR AJ V PRÍPADE

b) $w \in B \setminus A$.

NUTNE $A = B$. $\square$

1/2

02.03.2010 Ty
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

(19) PROBLÉMY SAT A QBF SÚ SELF-REDUCIBILNÉ.

SAT:

NASLEDUJÚCI DETERMINISTICKÝ ALGORITMUS PRACUJÚCI V POLYNOMIÁLNOM ČASE PRIJÍMA SAT, POKIAĽ MÁ SAT AKO ORÁKULUM. FORMULE KÓDUJEME TAK, ABY ZJEDNODUŠENIA $F|_{x:=0}$, $F|_{x:=1}$ BOLI VŽDY KRATŠIE AKO PÔVODNÁ FORMULA F.

VSTUP F, ORÁKULUM SAT
AK F NEOBSAHUJE PREMENNÉ, POTOM
  ZJEDNODUŠ F
  PRIJMI $\Leftrightarrow$ F SA ZJEDNODUŠÍ NA true
V OPAČNOM PRÍPADE NECH x JE PREMENNÁ
Z F S NAJMENŠÍM INDEXOM.
AK $F|_{x:=0} \in SAT$ ALEBO $F|_{x:=1} \in SAT$, POTOM
  PRIJMI
INAK ODMIETNI

PODOBNE PRE QBF:

VSTUP F, ORÁKULUM QBF

chybí diskuse o proměnné!

AK $F = \forall x F'$, POTOM
  PRIJMI $\Leftrightarrow$ $F'|_{x:=0} \in QBF \wedge F'|_{x:=1} \in QBF$
  INAK ODMIETNI
AK $F = \exists x F'$, POTOM
  PRIJMI $\Leftrightarrow$ $F'|_{x:=0} \in QBF \vee F'|_{x:=1} \in QBF$
  INAK ODMIETNI

⋮

⋮

AK $F = F_1 \wedge F_2$, POTOM
PRIJMI $\iff F_1 \in QBF \wedge F_2 \in QBF$
INAK ODMIETNI
AK $F = F_1 \vee F_2$, POTOM
PRIJMI $\iff F_1 \in QBF \vee F_2 \in QBF$
INAK ODMIETNI
AK $F = \neg F'$, POTOM
PRIJMI $\iff F' \notin QBF$
INAK ODMIETNI
AK F = true, POTOM PRIJMI
AK F = false, POTOM ODMIETNI

$\square$

(20) KEĎ A JE SELF-REDUCIBILNÝ JAZYK, POTOM $A \in PSPACE$.

NECH M JE DTS S ORÁKULOM PRACUJÚCI V POLYNOMIÁLNOM ČASE p TAKÝ ŽE $A = L(M, A)$, A PRE VSTUP DĹŽKY n DÁVA M DOTAZY DĹŽKY NAJVIAC $n-1$.

UVAŽUJME NASLEDUJÚCU ROZHODOVACIU PROCEDÚRU:

Simul (VSTUPNÉ SLOVO x) - VRACIA YES ALEBO NO
SIMULUJ PRÁCU STROJA M NAD SLOVOM x
AK M POLOŽÍ DOTAZ w, POTOM SPOČÍTAJ:

⋮

02.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

⋮

result := Simul(w)
POKRAČUJ V SIMULÁCII M VO VETVE result.
AK M PRIJME, TAK SKONČI A VRÁŤ YES
AK M ODMIETNE, TAK SKONČI A VRÁŤ NO.

JEDNÁ SA V PODSTATE O PREHĽADÁVANIE DO HĹBKY, PRIČOM VŽDY KEĎ SA ZANORÍME O ÚROVEŇ HLBŠIE, MÁME NA VSTUPE OSTRO KRATŠIE SLOVO. TOTIŽ $|w| \leq |x|-1$.

$\Rightarrow$ MAXIMÁLNA HĹBKA PREHĽADÁVANIA Simul(x) JE OHRANIČENÁ ZHORA DĹŽKOU VSTUPU $|x|$.

AK BY SME UVEDENÝ ALGORITMUS IMPLEMENTOVALI POMOCOU ZÁSOBNÍKA, TAK SIMULÁCIA M V KAŽDEJ ÚROVNI BY ZABRALA PRIESTOR NAJVIAC $p(|x|)$.

$\Rightarrow$ Simul(x) PRACUJE DETERMINISTICKY V PRIESTORE $|x| \cdot p(|x|)$.

ĽAHKO NAHLIADNUŤ, ŽE $x \in A \Leftrightarrow$ Simul(x) = YES, ČÍM SME DOKÁZALI, ŽE $A \in PSPACE$.

p – musí být neklesající a omezující délku výpočtu!

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

(1) DOKÁŽTE, ŽE k-QBF JE Σ_k-ÚPLNÝ PROBLÉM.

$k\text{-QBF} = \{ \varphi = \exists \vec{x}_1 \forall \vec{x}_2 \ldots Q(\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_k) \mid$
$\vec{x}_1, \ldots, \vec{x}_k$ SÚ VEKTORY BOOLEOVSKÝCH PREMENNÝCH, $Q(\vec{x}_1, \ldots, \vec{x}_k)$ JE VÝROKOVÁ FORMULA S PREMENNÝMI Z MNOŽINY $\{\vec{x}_1, \ldots, \vec{x}_k\}$, A φ PLATÍ $\}$.

JE ZREJMÉ, ŽE PRE DANÉ OHODNOTENIE PREMENNÝCH $\vec{x}_1, \ldots, \vec{x}_k$ VIEME V POL. ČASE ROZHODNÚŤ, ČI $Q(\vec{x}_1, \ldots, \vec{x}_k)$ PLATÍ, ALEBO NIE.
NAVIAC PRE DANÚ FORMULU φ TVARU:
$\exists \vec{x}_1 \forall \vec{x}_2 \ldots Q(\vec{x}_1, \ldots, \vec{x}_k)$ PLATÍ:

$|\vec{x}_i| \leq |\varphi|$, TAKŽE

jedná se o to aby y_i měly danou délku φ?

$\varphi \in k\text{-QBF} \Leftrightarrow \exists^{|\varphi|} \vec{y}_1 \forall^{|\varphi|} \vec{y}_2 \ldots (Q(\vec{x}_1, \ldots, \vec{x}_k)$ PLATÍ,
KDE φ JE TVARU $\exists \vec{x}_1 \forall \vec{x}_2 \ldots Q(\vec{x}_1, \ldots, \vec{x}_k)$,
PRIČOM ZA $\vec{x}_i$ DOSÁDZAME HODNOTY Z VEKTOROV $\vec{y}_i$)
VÝRAZ V ZÁTVORKE $\in P \Rightarrow k\text{-QBF} \in \Sigma_k$.

ZOSTÁVA UKÁZAŤ, ŽE k-QBF JE Σ_k-ŤAŽKÝ.
NECH $A \in \Sigma_k$. POTOM $\exists B \in P$ A POLYNÓM p TAKÝ, ŽE $x \in A \Leftrightarrow \exists^{p(|x|)} y_1 \forall^{p(|x|)} y_2 \ldots$
$\langle x, y_1, \ldots, y_k \rangle \in B$. BÚNO NECH B PRIJÍMA IBA KEĎ VŠETKY y_i SÚ DLHÉ PRÁVE $p(|x|)$.
(JE TO IBA OTÁZKA VHODNÉHO KÓDOVANIA)

Z DÔKAZU VETY: „SAT JE NP-ÚPLNÝ" VYPLÝVA, ŽE AK ZAFIXUJEME n DĹŽKU x, POTOM MOŽNO ZOSTROJIŤ V POL. ČASE $q(n)$ FORMULU Accepted TAKÚ, ŽE:

$$\langle x, y_1, \dots, y_k \rangle \in B \Leftrightarrow \text{Accepted}(x, y_1, \dots, y_k).$$

TOTIŽ PRE DANÉ n JE DĹŽKA $|\langle x, y_1, \dots, y_k \rangle|$ POLYNOMIÁLNE VEĽKÁ VZHĽADOM K n, A TVAR FORMULE Accepted ZÁVISÍ IBA NA DĹŽKE VSTUPU, NA KT. SA ZAMERIAME. SAMOTNÝ VSTUP VSTUPUJE DO FORMULE AKO PREMENNÁ.

$\Rightarrow$ PRE DANÉ x VIEME V POL. ČASE ZOSTROJIŤ FORMULU $\varphi = \exists \vec{y}_1 \forall \vec{y}_2 \dots \text{Accepted}(x, \vec{y}_1, \dots, \vec{y}_k)$ TAKÚ, ŽE $x \in A \Leftrightarrow \varphi$ PLATÍ $\Leftrightarrow \varphi \in k\text{-}\underline{Q}BF$

VEKTORY $\vec{y}_i$ SÚ DLHÉ $p(|x|)$ BITOV.

$\Rightarrow A \leq_m k\text{-}\underline{Q}BF$. $\square$

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(2) a) PSPACE $\neq$ PH, POTOM EXISTUJE $A \in$ PSPACE $\setminus$ PH, KT. NIE JE PSPACE-ÚPLNÝ.

OZNAČME $\mathcal{C}_1 = PH$, $\mathcal{C}_2 =$ PSPACE-COMPLETE

OBE TRIEDY SÚ REKURZÍVNE PREZENTOVATEĽNÉ:

i) $PH = \bigcup_{k \geq 0} \Sigma_k = \bigcup_{k \geq 0} \Delta_k$,

PRIČOM $\Delta_{k+1} = P(\Sigma_k) = P(k\text{-QBF})$.

(KEĎŽE AKO SME UKÁZALI V (1): k-QBF JE Σ_k-ÚPLNÁ).

VZHĽADOM K TOMU, ŽE $k\text{-QBF} \in \Sigma_k$, JE k-QBF REKURZÍVNA MNOŽINA, $\Rightarrow$

$P(k\text{-QBF})$ JE REKURZÍVNE PREZENTOVATEĽNÁ.

$\Delta_0 = P$ JE TAKTIEŽ REKURZÍVNE PREZENTOVATEĽNÁ.

NECH $M_{\langle k,0\rangle}, M_{\langle k,1\rangle}, \dots$ JE EFEKTÍVNA ENUMERÁCIA DTS DOKAZUJÚCA REK. PREZ. TRIEDY Δ_k, $k \geq 0$.

POTOM $\{M_{\langle k,i\rangle}\}_{k,i=0}^{\infty}$ JE ENUMERÁCIA DTS DOKAZUJÚCA REK. PREZ. TRIEDY PH.

ii) PSPACE = P(QBF) JE REK. PREZ. TRIEDA

$\Rightarrow$ PSPACE-COMPLETE $= \{ B \in \text{PSPACE} \mid \text{QBF} \leq_m B \}$ JE TAKTIEŽ REK. PREZ. TRIEDA.

ĽAHKO NAHLIADNUŤ, ŽE $\mathcal{C}_1$ A $\mathcal{C}_2$ SÚ UZAVRETÉ NA KON. VARIÁCIE. NECH TEDA PSPACE $\neq$ PH.

POLOŽME : $A_1 := QBF$, $A_2 := \emptyset$.

$A_1 \notin C_1$, PRETOŽE PH JE UZAVRETÁ NA $\leq_m$

TAKŽE $QBF \in PH \Rightarrow PSPACE \subseteq PH$

$A_2 \notin C_2$, AK $\emptyset$ JE PSPACE-COMPLETE $\Rightarrow$ $P = PSPACE \Rightarrow = PH$

PODĽA UNIFORM DIAGONALIZATION THEOREM

EXISTUJE A TAKÁ, ŽE : $A \notin C_1$, $A \notin C_2$

A $A \leq_m QBF \oplus \emptyset$, TJ. $A \in PSPACE \setminus PH$, A PRITOM

A NIE JE PSPACE-ÚPLNÁ. □

b) $\Sigma_{k+1} \neq \Sigma_k$, POTOM EXISTUJE $A \in \Sigma_{k+1} \setminus \Sigma_k$,

KTORÝ NIE JE Σ_{k+1}-ÚPLNÝ.

$\Sigma_l = \{B \in PSPACE \mid B \leq_m l\text{-}QBF\}$, $l \geq 1$

$\Rightarrow \Sigma_l$ JE REK. PREZENTOVATEĽNÁ

$\Sigma_0 = P$ JE TAKTIEŽ —||—

Σ_l-COMPLETE $= \{B \in \Sigma_l \mid l\text{-}QBF \leq_m B\}$, $l \geq 1$

JE ZREJME TAKTIEŽ REK. PREZENTOVATEĽNÁ.

POLOŽME $C_1 := \Sigma_k$, $C_2 := \Sigma_{k+1}$-COMPLETE (ZREJME C_1 AJ C_2 SÚ UZAVRETÉ NA KON. VARIÁCIE)

$A_1 := (k+1)\text{-}QBF$, $A_2 := \emptyset$.

$A_1 \notin C_1$, PRETOŽE Σ_k JE UZAVRETÁ NA $\leq_m$

TAKŽE $(k+1)\text{-}QBF \in \Sigma_k \Rightarrow \Sigma_{k+1} \subseteq \Sigma_k$

$A_2 \notin C_2$, AK $\emptyset$ JE Σ_{k+1}-COMPLETE, POTOM $P = \Sigma_{k+1} \Rightarrow$

$\Rightarrow P = NP$ A PH KOLAPSUJE ...

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

PODĽA UNIFORM DIAGONALIZATION THEOREM EXISTUJE A TAKÁ, ŽE $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$ A $A \leq_m (k+1)\text{-}QBF \oplus \emptyset$, TJ. $A \in \Sigma_{k+1} \setminus \Sigma_k$, A PRITOM A NIE JE Σ_{k+1} - ÚPLNÁ. $\square$

c) $\Sigma_{k+1} \neq \Sigma_k$, POTOM EXISTUJE $A \in \Sigma_{k+1} \setminus \Sigma_k$, KTORÝ NIE JE NP - ŤAŽKÝ.

POLOŽME $\mathcal{C}_1 := \Sigma_k$, $\mathcal{C}_2 := \{ B \in \Sigma_{k+1} \mid SAT \leq_m B \}$

$A_1 := (k+1)\text{-}QBF$, $A_2 := \emptyset$

OPÄŤ $A_1 \notin \mathcal{C}_1$, $A_2 \notin \mathcal{C}_2 \Rightarrow \exists A$ TAKÁ, ŽE $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$, $A \leq_m (k+1)\text{-}QBF \oplus \emptyset$, TJ. $A \in \Sigma_{k+1} \setminus \Sigma_k$, A PRITOM $\neg\, SAT \leq_m A$, TAKŽE A NIE JE NP - ŤAŽKÁ. $\square$

(3) UKÁŽTE, ŽE TRIEDY JAZYKOV PSPACE \ PH, PSPACE \ Σ_k, $\Sigma_{k+1} \setminus \Sigma_k$ SÚ REK. PREZENTOVATEĽNÉ JEDINE KEĎ SÚ PRÁZDNE.

a) PRE SPOR NECH PSPACE \ PH $\neq \emptyset$ JE REKURZÍVNE PREZENTOVATEĽNÁ

ZREJME QBF $\in$ PSPACE \ PH.

AK BY QBF $\in$ PH, POTOM BY Z UZAVRETOSTI PH NA $\leq_m$ VYPLYNULO PSPACE $\subseteq$ PH. .

POLOŽME $C_1 := PH$, $C_2 := PSPACE \setminus PH$

$A_1 := QBF$, $A_2 := \emptyset$.

ZREJME C_1 AJ C_2 SÚ UZAVRETÉ NA KON. VARIÁCIE

PRE C_2: NECH $B \in PSPACE \setminus PH$ A B' JE KONEČNÁ VARIÁCIA B. POTOM $B' \in PSPACE$. ZREJME TIEŽ $B' \notin PH$. TOTIŽ $B' \in PH \Rightarrow B \in PH \Rightarrow B \notin PSPACE \setminus PH$. ↯

NUTNE TEDA $B' \in PSPACE \setminus PH$.

PODĽA PREDPOKLADU SÚ C_1 A C_2 REK. PREZENTOVATEĽNÉ.

$A_1 \notin C_1$: $QBF \in PH \Rightarrow PSPACE \subseteq PH$ ↯

$A_2 \notin C_2$: $\emptyset \in PH \Rightarrow \emptyset \notin PSPACE \setminus PH$.

PODĽA UNIFORM DIAGONALIZATION THEOREM EXISTUJE A TAKÁ, ŽE $A \notin C_1$, $A \notin C_2$ A $A \leq_m QBF \oplus \emptyset$.

AVŠAK $A \leq_m QBF \oplus \emptyset \Rightarrow A \in PSPACE$, ČO JE V SPORE S $A \notin C_1$, $A \notin C_2$ ↯ □

b) PRE SPOR NECH $PSPACE \setminus \Sigma_k \neq \emptyset$ JE REKURZÍVNE PREZENTOVATEĽNÁ.

POLOŽME $C_1 := \Sigma_k$, $C_2 := PSPACE \setminus \Sigma_k$

$A_1 := QBF$, $A_2 := \emptyset$.

OPÄŤ Z UNIFORM DIAGONALIZATION THEOREM DOSTANEME A TAKÚ, ŽE $A \notin C_1$, $A \notin C_2$, $A \leq_m QBF \oplus \emptyset$, TJ. $A \in PSPACE$, ČO JE V SPORE S $A \notin C_1$, $A \notin C_2$ ↯ □

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

c) PRE SPOR NECH $\Sigma_{k+1} \setminus \Sigma_k \neq \emptyset$
JE REKURZÍVNE PREZENTOVATEĽNÁ.
POLOŽME $\mathcal{C}_1 := \Sigma_k$, $\mathcal{C}_2 := \Sigma_{k+1} \setminus \Sigma_k$,
$A_1 := (k+1)\text{-QBF}$, $A_2 := \emptyset$.
OPÄŤ Z UNIFORM DIAGONALIZATION THEOREM DOSTANEME
A TAKÚ, ŽE $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$, $A \leq_m (k+1)\text{-QBF} \oplus \emptyset$,
TJ. $A \in \Sigma_{k+1}$, ČO JE V SPORE S $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$. $\square$

(4) a) PRE MNOŽINU A PLATÍ: A JE NP-EKVIVAL., TJ.
$P(A) = P(SAT)$ $\Leftrightarrow$ A JE Δ_2-ÚPLNÁ VZHĽADOM K $\leq_T$.
b) KEĎ NP NIE JE UZAVRETÉ NA DOPLNKY, POTOM
EXISTUJE $A \in \Delta_2 \setminus (NP \cup \text{co-}NP)$, KTORÁ
NIE JE NP-EKVIVALENTNÁ.

a) $\Rightarrow$) NECH $P(A) = P(SAT)$.
KEĎŽE SAT JE Σ_1-ÚPLNÝ (VZHĽADOM K $\leq_m$),
NUTNE $P(SAT) = P(\Sigma_1) = \Delta_2$,
TAKŽE $A \in P(A) = P(SAT) = P(\Sigma_1) = \Delta_2$, TJ. $A \in \Delta_2$.
NECH $B \in \Delta_2$. DOKÁŽME, ŽE $B \leq_T A$, TJ. $B \in P(A)$.
TO JE VŠAK ZREJMÉ, PRETOŽE $P(A) = \Delta_2$.
$\Leftarrow$) NECH A JE Δ_2-ÚPLNÁ VZHĽADOM K $\leq_T$,
TJ. $A \in \Delta_2$ A PRE KAŽDÚ $B \in \Delta_2$: $B \leq_T A$,
TJ. $B \in P(A)$. ŠPECIÁLNE $SAT \leq_T A$ $\Rightarrow$

$P(SAT) \subseteq P(A)$. AVŠAK $P(SAT) = P(\Sigma_1) = \Delta_2$

PRIČOM $A \in \Delta_2 \Rightarrow P(A) \subseteq P(\Delta_2) = \Delta_2 = P(SAT)$.

TO ZNAMENÁ, ŽE $P(A) = P(SAT)$. $\square$

b) NECH $B \in NP \setminus co\text{-}NP$, TJ. $\overline{B} \in co\text{-}NP \setminus NP$

POLOŽME $C_1 := NP$, $C_2 := co\text{-}NP$,

$A_1 := \overline{B}$, $A_2 := B$.

KEĎŽE SÚ SPLNENÉ PODMIENKY UNIFORM DIAGONALIZATION THEOREM, NUTNE EXISTUJE A TAKÁ, ŽE

$A \notin C_1$, $A \notin C_2$, $A \leq_m B \oplus \overline{B}$

KEĎŽE $B \in \Sigma_1$, NUTNE $B, \overline{B} \in P(\Sigma_1) = \Delta_2$, TJ. TIEŽ $B \oplus \overline{B} \in \Delta_2$, ČO IMPLIKUJE $A \in \Delta_2$ (UZAVRETOSŤ NA $\leq_m$).

$A \notin NP$, ANI $A \notin co\text{-}NP$, TAKŽE NUTNE:

$A \in \Delta_2 \setminus (NP \cup co\text{-}NP)$. $\square$

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(5) DOKÁŽTE:

a) $\Sigma_k / POLY = \bigcup \{ \Sigma_k(S) \mid S \text{ RIEDKA} \}$

b) $\Pi_k / POLY = \bigcup \{ \Pi_k(S) \mid S \text{ RIEDKA} \}$

c) $\Delta_k / POLY = \bigcup \{ \Delta_k(S) \mid S \text{ RIEDKA} \}$

d) $PH / POLY = \bigcup \{ PH(S) \mid S \text{ RIEDKA} \}$

e) $\Sigma_k / POLY = \Pi_k / POLY \Rightarrow \Sigma_k / POLY = PH / POLY$

f) $\Sigma_k / POLY = \Pi_k / POLY \Rightarrow \Sigma_{k+2} = \Pi_{k+2}$

POLY OZNAČUJE MNOŽINU FUNKCIÍ f Z $\mathbb{N}$ DO Σ^* TAKÝCH, ŽE PRE NEJAKÝ POLYNÓM p : $|f(n)| \leq p(n)\ \forall n$

$$\mathcal{C}/\mathcal{F} = \{ B \mid \exists A \in \mathcal{C}\ \exists f \in \mathcal{F} : x \in B \Leftrightarrow \langle x, f(|x|) \rangle \in A \}$$

---

a) $\subseteq$) NECH $A \in \Sigma_k / POLY$, T.J. $\exists B \in \Sigma_k, f \in POLY$:
$x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in B$.

DEFINUJME S AKO:

$$S = \{ \langle 0^n, x \rangle \mid x \text{ JE PREFIX } f(n) \}$$

ZREJME PRE KAŽDÉ m EXISTUJE NAJVIAC $m+1$ RÔZNYCH SLOV $z = \langle 0^n, x \rangle \in S$ DLHÝCH m ZNAKOV. PRE n MÁME $m+1$ MOŽNOSTÍ: $n \in \{0, \dots, m\}$, x JE URČENÉ POTOM JEDNOZNAČNE AKO PREFIX $f(n)$ TAKÝ, ŽE $|\langle 0^n, x \rangle| = m$. $\Rightarrow$ S JE RIEDKA.

UVAŽUJME NASLEDUJÚCI ALGORITMUS:

```
VSTUP x      ORAKULUM S
n := |x|,   z := λ
loop
   if <0^n, z0> ∈ S then z := z0
   else if <0^n, z1> ∈ S then z := z1
   else break loop
end loop
return z
```

ALGORITMUS POČÍTA f A UKAZUJE, ŽE $f \in PF(S)$.

ĎALEJ $B \in \Sigma_k \Rightarrow \exists C \in P$ A POLYNÓM p T.Ž.

$$\langle x, z\rangle \in B \iff \exists^{p(|\langle x,z\rangle|)} y_1 \, \forall^{p(|\langle x,z\rangle|)} y_2 \dots$$

$$\langle x, z, y_1, \dots, y_k\rangle \in C$$

KEĎŽE ZA z BUDEME VŽDY DOSADZOVAŤ $f(|x|)$, ČO JE SLOVO POLYNOMIÁLNE VEĽKÉ VZHĽADOM K x, MÔŽME PREDPOKLADAŤ, ŽE EXISTUJE POLYNÓM q T.Ž.

$$\langle x, f(|x|)\rangle \in B \iff \exists^{q(|x|)} y_1 \, \forall^{q(|x|)} y_2 \dots$$

$$\underbrace{\langle x, f(|x|), y_1, \dots, y_k\rangle \in C}_{\text{ĽAHKO NAHLIADNUŤ, ŽE TOTO JE PREDIKÁT ROZHODNUTEĽNÝ V } P(S)}$$

$\Rightarrow A \in \Sigma_k(S)$.

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

⊇) NECH $A \in \Sigma_k(S)$, TJ. $\exists B \in P(S)$ A POLYNÓM p T. Ž.: $x \in A \Leftrightarrow \exists^{p(|x|)} y_1 \forall^{p(|x|)} y_2 \dots \langle x, y_1, \dots, y_k \rangle \in B$

NECH q JE POLYNÓM OHRANIČUJÚCI ČAS DTS M ROZHODUJÚCEHO MNOŽINU B. DEFINUJME RADIACU FUNKCIU f TAK, ŽE PRE KAŽDÉ n VRÁTI ZAKÓDOVANÚ MNOŽINU SLOV Z S DLHÝCH NAJVIAC $q(n)$. TOTO JE POLYNOMIÁLNE DLHÉ KÓDOVANIE.
M ZMODIFIKUJEME TAK, ŽE NAMIESTO VSTUPU x DOSTÁVA DVOJICU $\langle x, f(|x|) \rangle$, A POTOM POUŽIJE MNOŽINU ZAKÓDOVANÚ V $f(|x|)$ NA ODPOVEDANIE NA DOTAZY, NAMIESTO DOTAZOVANIA SA ORÁKULA.
TO DOKAZUJE, ŽE $B \in P/poly$, A TÝM PADOM AJ $A \in \Sigma_k/poly$. □

b) POSTUPUJEME ANALOGICKY AKO V PRÍPADE a) AKURÁT VŠADE NAMIESTO Σ_k PÍŠEME Π_k A POSTUPNOSŤ k POLYNOMIÁLNE OHRANIČ. KVANTIFIKÁTOROV VŽDY ZAČÍNAME OBECNÝM KVANT. $\forall$, A NIE EXISTENČNÝM $\exists$. □

c) PRÍPAD $k=0$ JE EKVIVALENTNÝ S a), b) PRE $k=0$.

$\Delta_{k+1}/poly = P(\Sigma_k)/poly =$

$= \{ A \mid \exists B \in P(\Sigma_k), f \in poly : x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in B \} =$

$= \{ A \mid \exists$ DTS M S ORÁKULOM PRACUJÚCI V POL. ČASE,

$\exists C \in \Sigma_k \; \exists f \in poly : x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in L(M, C) \}$

MAJME NEJAKÚ $A \in \Delta_{k+1}/poly$ A K NEJ PRÍSLUŠNÝ POLYNOMIÁLNY DTS M, $C \in \Sigma_k$ A $f \in poly$.

PODOBNE AKO V a) ZOSTROJÍME RIEDKU S TAKÚ, ŽE $f \in PF(S)$.

ĎALEJ POLOŽME $D := C \oplus S$.

ĽAHKO NAHLIADNUŤ, ŽE $D \in \Sigma_k(S)$ (PRETOŽE C AJ $S \in \Sigma_k(S)$)

UVAŽUJME NASLEDUJÚCI ALGORITMUS

- VSTUP x ORÁKULUM D
- NAJSKÔR SPOČÍTAJ $f(|x|)$ POMOCOU S OBSIAHNUTEJ V D
- POTOM SIMULUJ PRÁCU M NA VSTUPE $\langle x, f(x) \rangle$
- PRIČOM DOTAZY DELEGUJ NA C OBSIAHNUTÉ V D

JE ZREJMÉ, ŽE UVEDENÝ ALGORITMUS ROZPOZNÁVA A V POL. ČASE S ORÁKULOM D, TJ.

$A \in P(\Sigma_k(S)) = \Delta_{k+1}(S)$.

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

NAOPAK NECH $A \in \Delta_{k+1}(S)$, KDE S JE RIEDKA, TJ. $A \in P(\Sigma_k(S))$, TJ. $\exists$ DTS M S ORÁKULOM PRACUJÚCI V POL. ČASE $p(n)$, $B \in \Sigma_k(S)$ TAKÁ, ŽE $A = L(M, B)$. PODĽA a) $B \in \Sigma_k/poly$, TJ. $\exists C \in \Sigma_k$ A RADIACA FUNKCIA $g \in poly$ TAKÁ, ŽE $\forall x \in B \Leftrightarrow \langle x, g(|x|)\rangle \in C$.

PROBLÉM JE, ŽE M MÔŽE KLÁSŤ NA B DOTAZY RÔZNEJ DĹŽKY, NAJVIAC VŠAK DLHÉ $p(|x|)$.

DEFINUJME PRETO RADIACU FUNKCIU:

$$f(n) := \langle g(0), g(1), \dots, g(p(n))\rangle$$

ZREJME $f \in poly$. UVAŽUJME NASLEDUJÚCI ALGORITMUS:

- VSTUP $\langle x, f(|x|)\rangle$ ORÁKULUM C
- SIMULUJ M NA SLOVE x
- VŽDY KEĎ M DÁ DOTAZ $u \overset{?}{\in} B$
- ZISTI Z HODNOTY $f(|x|)$ ČOMU SA ROVNÁ $g(|u|)$
- A VYHODNOŤ $\langle u, g(|u|)\rangle \in C$ NAMIESTO $u \in B$

ĽAHKO NAHLIADNUŤ, ŽE UVEDENÝ ALGORITMUS DOKAZUJE $A \in \Delta_{k+1}/poly$. $\square$

d) $\subseteq$) $A \in PH/\text{POLY} \Rightarrow \exists B \in PH,\ f \in \text{POLY}$:

$x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in B$

$B \in PH \Rightarrow \exists k : B \in \Sigma_k$, TJ. $A \in \Sigma_k / \text{POLY}$

$\Rightarrow A \in \Sigma_k(S)$ PRE NEJAKÚ RIEDKU S

$\Rightarrow A \in PH(S)$.

$\supseteq$) $A \in PH(S) \Rightarrow \exists k : A \in \Sigma_k(S)$

$\Rightarrow A \in \Sigma_k / \text{POLY}$, TJ. $\exists B \in \Sigma_k$, $f \in \text{POLY}$:

$x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in B$

ZREJME $B \in PH$, TAKŽE TIEŽ $A \in PH/\text{POLY}$. $\square$

e) $PH/\text{POLY} = \bigcup \{ PH(S) \mid S \text{ JE RIEDKA} \} =$ (PODĽA d))

$= \bigcup \{ \bigcup_{k \geq 0} \Sigma_k(S) \mid S \text{ JE RIEDKA} \} =$

$= \bigcup \{ \bigcup_{S \text{ RIEDKA}} \Sigma_k(S) \mid k \geq 0 \} =$

$= \bigcup_{k \geq 0} (\Sigma_k / \text{POLY})$.

PODOBNE $PH/\text{POLY} = \bigcup_{k \geq 0} (\Pi_k / \text{POLY}) = \bigcup_{k \geq 0} (\Delta_k / \text{POLY})$.

DOKÁŽEME, ŽE $\Sigma_k/\text{POLY} = \Pi_k/\text{POLY} \Rightarrow$

$\forall j \geq 0 \quad \Sigma_{k+j}/\text{POLY} = \Pi_{k+j}/\text{POLY} = \Sigma_k/\text{POLY}$.

INDUKCIA PODĽA j. PRE $j=0$ PLATÍ TRIVIÁLNE.

INDUKČNÝ KROK $j \to j+1$:

8/9

30.03.2010 Ta
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

PREDPOKLADAJME, ŽE $\Sigma_{k+j}/\text{poly} = \Pi_{k+j}/\text{poly} = \Sigma_k/\text{poly}$.

(i) $\Sigma_{k+j+1}/\text{poly} \subseteq \Sigma_{k+j}/\text{poly}$

NECH $A \in \Sigma_{k+j+1}/\text{poly}$, TJ. $A \in \bigcup\{\Sigma_{k+j+1}(S) \mid S \text{ RIEDKA}\}$

$\Rightarrow \exists S_1$ RIEDKA TAKÁ, ŽE $A \in \Sigma_{k+j+1}(S_1)$.

AVŠAK $\Sigma_{k+j+1}(S_1) = \exists(\Pi_{k+j}(S_1))$, TJ. $A \in \exists(\Pi_{k+j}(S_1))$.

PODĽA PREDPOKLADU $\Sigma_{k+j}/\text{poly} = \Pi_{k+j}/\text{poly}$, TAKŽE PLATÍ $\Pi_{k+j}(S_1) \subseteq \Sigma_{k+j}/\text{poly} = \bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S)$

$$\Rightarrow \exists(\Pi_{k+j}(S_1)) \subseteq \exists\Big(\bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S)\Big).$$

NUTNE TEDA $A \in \exists\Big(\bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S)\Big)$, TJ. EXISTUJE

$B \in \bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S)$ A POLYNÓM p:

$$x \in A \Leftrightarrow \exists^{p(|x|)} y : \langle x, y\rangle \in B.$$

$B \in \bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S) \Rightarrow \exists S_2$ RIEDKA : $B \in \Sigma_{k+j}(S_2)$.

VIDÍME TEDA, ŽE $A \in \exists(\Sigma_{k+j}(S_2)) = \Sigma_{k+j}(S_2) \subseteq$
$\subseteq \bigcup_{S \text{ RIEDKA}} \Sigma_{k+j}(S) = \Sigma_{k+j}/\text{poly}$.

TÝM SME DOKÁZALI, ŽE $\Sigma_{k+j+1}/\text{poly} \subseteq \Sigma_{k+j}/\text{poly}$.

(ii) $\Sigma_{k+j}/\text{poly} \subseteq \Sigma_{k+j+1}/\text{poly}$ ... JE TRIVIÁLNA.

UKÁZALI SME, ŽE $\Sigma_{k+j+1}/\mathrm{POLY} = \Sigma_{k+j}/\mathrm{POLY}$,
A TÝM PÁDOM AJ: $\Sigma_{k+j+1}/\mathrm{POLY} = \Sigma_k/\mathrm{POLY}$.

ĎALEJ $\bigcup\{\Sigma_{k+j+1}(S) \mid S \text{ RIEDKA}\} = \bigcup\{\Sigma_{k+j}(S) \mid S \text{ RIEDKA}\}$
IMPLIKUJE (KEĎ PREJDEME K DOPLNKOM JAZYKOV):
$\bigcup\{\Pi_{k+j+1}(S) \mid S \text{ RIEDKA}\} = \bigcup\{\Pi_{k+j}(S) \mid S \text{ RIEDKA}\}$,
TJ. $\Pi_{k+j+1}/\mathrm{POLY} = \Pi_{k+j}/\mathrm{POLY}$

$\Rightarrow$ (PODĽA PREDPOKLADU)
$\Pi_{k+j+1}/\mathrm{POLY} = \Pi_{k+j}/\mathrm{POLY} = \Sigma_{k+j}/\mathrm{POLY} = \Sigma_{k+j+1}/\mathrm{POLY} =$
$= \Sigma_k/\mathrm{POLY}$, ČO BOLO TREBA DOKÁZAŤ.

UKÁZALI SME, ŽE $\Sigma_k/\mathrm{POLY} = \Pi_k/\mathrm{POLY} \Rightarrow$
$\forall j \geq 0 \;\; \Sigma_{k+j}/\mathrm{POLY} = \Sigma_k/\mathrm{POLY}$
PRE $j \leq k$ JE ZREJMÉ $\Sigma_j/\mathrm{POLY} \subseteq \Sigma_k/\mathrm{POLY}$.
$\Rightarrow \mathrm{PH}/\mathrm{POLY} = \bigcup_{j \geq 0} (\Sigma_j/\mathrm{POLY}) = \underline{\underline{\Sigma_k/\mathrm{POLY}}}$. $\square$

~~S: NECH~~ $\cancel{\Sigma_k/\mathrm{POLY} = \Pi_k/\mathrm{POLY}}$.
~~NECH~~ $\cancel{A \in \Sigma_{k+2}}$, ~~TJ.~~ $\cancel{\exists B \in \Sigma_k(\emptyset)}$
~~A POLYNÓM p T.Ž.~~
$\cancel{x \in A \Leftrightarrow \exists^{p(|x|)} y_1 \forall^{p(|x|)} y_2 \langle x, y_1, y_2 \rangle \in B}$.
$\cancel{B \in \Sigma_k(\emptyset) \Rightarrow \exists S \text{ RIEDKA}: B \in \Pi_k(S)}$

30.03.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

f) NECH $\Sigma_k / \text{POLY} = \Pi_k / \text{POLY}$. PODĽA DÔKAZU e) :
$\forall j \geq 0 \ \Sigma_{k+j} / \text{POLY} = \Pi_{k+j} / \text{POLY} = \Sigma_k / \text{POLY}$.

PLATÍ VETA: KEĎ A JE SELF-REDUCIBILNÁ A $A \in \Sigma_k(S)$, KDE S JE RIEDKA, POTOM $\Sigma_2(A) \subseteq \Sigma_{k+2}$.

NECH A JE Σ_{k+1}-ÚPLNÝ SELFREDUCIBILNÝ JAZYK. (NAPR. $(k+1)$-QBF).

$\Sigma_{k+1} = \Sigma_{k+1}(\emptyset) \Rightarrow \exists$ RIEDKA S : $\Sigma_{k+1}(\emptyset) = \Sigma_k(S)$ MOŽ.

$\Rightarrow \Sigma_{k+3} = \Sigma_2(\Sigma_{k+1}) = \Sigma_2(A) \subseteq \Sigma_{k+2}$,

PRETOŽE A JE SELF-REDUCIBILNÁ A ZÁROVEŇ $A \in \Sigma_k(S)$.

$\square$

05.04.2010 M.
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

(6) DOKÁŽTE, ŽE NASLEDUJÚCE TVRDENIA SÚ EKVIVAL.:

a) PH KOLAPSUJE
b) $\forall A \in PH$: $PH(A)$ KOLAPSUJE
c) $\exists A \in PH$: $PH(A)$ KOLAPSUJE
d) $\exists A \in PH$: $P(A) = NP(A)$

a) ⇒ b)) NECH PH KOLAPSUJE, TJ. EXISTUJE k T.Ž. $\Sigma_k = \Pi_k$. NECH $A \in PH$, TJ. $\exists l : A \in \Sigma_l$

AK $l = 0$, POTOM $A \in P$, TJ. $\Sigma_k(A) = \Sigma_k = \Pi_k = \Pi_k(A)$, PRETOŽE DOTAZY NA ORAKULUM MÔŽEME NAHRADIŤ DETERM. VÝPOČTOM S POLYNOMIÁLNOU ČASOVOU ZLOŽITOSŤOU.

VO VŠEOBECNOSTI:

$$\Sigma_k(A) \subseteq \Sigma_k(\Sigma_l) \subseteq \Sigma_{k+l} \subseteq \Sigma_k = \Pi_k \subseteq \Pi_k(A)$$

$$\Sigma_k(A) \subseteq \Pi_k(A) \Rightarrow co\text{-}\Sigma_k(A) \subseteq co\text{-}\Pi_k(A),$$

TJ. NUTNE PLATIA OBE INKLÚZIE, TJ. $\Sigma_k(A) = \Pi_k(A)$ A $PH(A)$ KOLAPSUJE.

b) ⇒ c)) PLATÍ TRIVIÁLNE

c) ⇒ d)) NECH $A \in PH$ A $PH(A)$ KOLAPSUJE, TJ.

$\exists k : \Sigma_k(A) = \Sigma_{k+1}(A)$ A $\exists l : A \in \Sigma_l$

UVAŽUJME MNOŽINU $B = K^k(A)$.

ZREJME B JE $\Sigma_k(A)$ - ÚPLNÁ VZHĽADOM K $\leq_m$.

$B \in \Sigma_k(A) \subseteq \Sigma_k(\Sigma_l) \subseteq PH$. TRIVIÁLNE $P(B) \subseteq NP(B)$, A TIEŽ

$NP(B) = NP(\Sigma_k(A)) = \Sigma_{k+1}(A) = \Sigma_k(A) \subseteq P(\Sigma_k(A)) = P(B)$.

d) $\Rightarrow$ a)) NECH $A \in PH$, TJ. $\exists \ell : A \in \Sigma_\ell$ A $P(A) = NP(A)$.

AK $\ell = 0$, TJ. $A \in P$, POTOM $P = NP$ A PH KOLAPSUJE.

ZREJME $P(A) = \Sigma_k(A)$ PRE ĽUBOVOĽNÉ $k \geq 1$.

DÔKAZ: PRE $k=1$ PLATÍ,

PRE $k > 1$: $\Sigma_k(A) = NP(\Sigma_{k-1}(A)) = NP(P(A)) = NP(A) = P(A)$, PRIČOM SME VYUŽILI IND. PREDPOKLAD $\Sigma_{k-1}(A) = P(A)$.

~~VEZMIME SI $B = K^{\ell+1}$. B JE $\Sigma_{\ell+1}$-ÚPLNÁ VZHĽADOM K $\leq_m$.~~

ZREJME $\Sigma_{\ell+2} \subseteq \Sigma_{\ell+2}(A) = P(A) = NP(A) \subseteq$
$\subseteq NP(\Sigma_\ell) = \Sigma_{\ell+1}$, TJ.

$\Sigma_{\ell+2} = \Sigma_{\ell+1}$ A PH KOLAPSUJE. $\square$

10.04.2010 So
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOSŤ I

(1) NASLEDUJÚCE MNOŽINY NIE SÚ REKURZÍVNE PREZENTOVATEĽNÉ:

a) MNOŽINA REKURZÍVNYCH MNOŽÍN
b) MNOŽINA RIEDKYCH REKURZÍVNYCH MNOŽÍN
c) MNOŽINA REKURZÍVNYCH MNOŽÍN V P/POLY
d) MNOŽINA REKURZÍVNYCH NP-ŤAŽKÝCH MNOŽÍN
e) NP \ P
f) MNOŽINA NP-NEÚPLNÝCH MNOŽÍN V NP
g) MNOŽINA NEKONEČNÝCH MNOŽÍN V P

(a) SPOROM PREDPOKLADAJME, ŽE $M_1, M_2, \dots$ JE EFEKTÍVNA ENUMERÁCIA DTS TAKÝCH, ŽE SA ZASTAVIA NA KAŽDOM VSTUPE, A $\mathcal{R} = \{L(M_i) \mid i=1,2,\dots\}$.
UVAŽUJME NASLEDUJÚCI ALGORITMUS

VSTUP x, $|x|=n$
SIMULUJ PRÁCU STROJA M_n NA VSTUPE x
PRIJMI $\Leftrightarrow$ M_n ZAMIETOL x, A NAOPAK.

ALGORITMUS PRIJÍMA REKURZÍVNU MNOŽINU, TJ. EXISTUJE DTS M, KTORÝ SA ZASTAVÍ NA KAŽDOM VSTUPE, A PRIJÍMA JAZYK POPÍSANÝ TÝMTO ALGORITMOM.

NAVIAC M SA LÍŠI OD M_n NA KAŽDOM VSTUPE x DĹŽKY n, PRE KAŽDÉ $n \geq 1$.
NUTNE $L(M) \notin \{L(M_i) \mid i=1,2,\dots\}$, ČO JE SPOR. ↯ □

(b) PODOBNE AKO V a) PRE SPOR PREDPOKLADAJME, ŽE EXISTUJE EFEKTÍVNA ENUMERÁCIA DTS $M_1, M_2, \dots$ TAKÝCH, ŽE SA ZASTAVIA NA KAŽDOM VSTUPE, A $\mathcal{R}_{SPARSE} = \{ L(M_i) \mid i = 1, 2, \dots \}$

UVAŽUJME ALGORITMUS:

- VSTUP x, $|x| = n$
- SIMULUJ M_n NA VSTUPE x
- AK JE x TVARU 0^n, POTOM
  - PRIJMI $\Leftrightarrow$ M_n ODMIETOL, A NAOPAK
- V OPAČNOM PRÍPADE ODMIETNI

ALGORITMUS PRIJÍMA REKURZÍVNU RIEDKU MNOŽINU S, KTORÁ SA VŠAK LÍŠI OD KAŽDEJ $L(M_n)$ NA VSTUPE 0^n, PRE VŠETKY $n \geq 1$.

NUTNE $S \notin \{ L(M_i) \mid i = 1, 2, \dots \}$, ČO JE SPOR. ↯ □

(c) NECH rekurzívne $P/poly = \{ L(M_i) \mid i = 1, 2, \dots \}$ DOKAZUJE REKURZÍVNU PREZENTOVATEĽNOSŤ TRIEDY rekurz. $P/poly$.

PODOBNE AKO V b) ZOSTROJME RIEDKU REKURZÍVNU S, KTORÁ SA LÍŠI OD VŠETKÝCH $L(M_i)$.

ZREJME $S \in P(S) \subseteq P/poly$, TJ. $S \in P/poly$, AVŠAK $S \notin \{ L(M_i) \mid i = 1, 2, \dots \}$, ČO JE SPOR. ↯ □

Tady pozor nejde o P/poly, to je triviální

vždyť P/poly obsahuje nerekurzivní jazyky!

10.04.2010 Sa
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

(d) PRE SPOR NECH $\{ L(M_i) \mid i = 1, 2, \dots \}$ nekonečne?
DOKAŽME REKURZÍVNU PREZENTOVATEĽNOSŤ
NP-ŤAŽKÝCH MNOŽÍN.

UVAŽUJME NASLEDUJÚCI ALGORITMUS

VSTUP x, $|x| = n$
AK x KÓDUJE BOOLEOVSKÚ FORMULU,
POTOM PRIJMI $\Leftrightarrow$ $x \in SAT$, TJ. x JE SPLNITEĽNÁ
V OPAČNOM PRÍPADE
PRIJMI $\Leftrightarrow$ M_n ODMIETOL x, A NAOPAK

ĽAHKO NAHLIADNUŤ, ŽE ALGORITMUS PRIJÍMA / prečo? !
NP-ŤAŽKÚ MNOŽINU A, PRETOŽE $SAT \leq_m A$. ľahko asi nie
NAVIAC PRE KAŽDÉ n SA A LÍŠI OD $L(M_n)$
V ASPOŇ JEDNOM VSTUPE x DĹŽKY n, PRETOŽE
PRE KAŽDÉ n NÁJDEME x DĹŽKY n, KTORÉ
NEKÓDUJE ŽIADNU BOOLEOVSKÚ FORMULU. $\lightning$ $\square$

(e) DOKÁŽEME, ŽE $NP \setminus P$ NIE JE REKURZÍVNE
PREZENTOVATEĽNÁ ZA PREDPOKLADU, ŽE $NP \setminus P \neq \emptyset$.

POLOŽME $\mathcal{C}_1 := P$, $\mathcal{C}_2 := NP \setminus P$, $A_1 := SAT$, $A_2 := \emptyset$

OBE TRIEDY $\mathcal{C}_1$ AJ $\mathcal{C}_2$ SÚ REK. PREZENTOVATEĽNÉ
A UZAVRETÉ NA KONEČNÉ VARIÁCIE

PRE TRIEDU $NP \setminus P$: AK $A \in NP \setminus P$, A' JE
KONEČNÁ VARIÁCIA A, POTOM $A' \in NP$.
AK BY $A' \in P$, POTOM AJ $A \in P$. AVŠAK $A \notin P$, TAKŽE $A' \in NP \setminus P$.

ĎALEJ $A_1 \notin \mathcal{C}_1$ (TOTIŽ $SAT \in P \Rightarrow P = NP$)
A PODOBNE $A_2 \notin \mathcal{C}_2$ ($\emptyset \in P \Rightarrow \emptyset \notin NP \setminus P$)
PODĽA UNIFORM DIAGONALIZATION THEOREM
EXISTUJE A TAKÁ, ŽE $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$ A $A \leq_m A_1 \oplus A_2$,
TJ. $A \leq_m SAT \oplus \emptyset$, TAKŽE $A \in NP$.
AVŠAK $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2 \Rightarrow A \notin NP$, ČO JE SPOR. ↯ □

(f) DOKÁŽME, ŽE $NP \setminus NP$-COMPLETE NIE JE
REKURZÍVNE PREZENTOVATEĽNÁ AK JE NEPRÁZDNA.
POLOŽME $\mathcal{C}_1 := NP \setminus NP$-COMPLETE, $\mathcal{C}_2 := NP$-COMPLETE.
OBE TRIEDY SÚ REK. PREZENTOVATEĽNÉ:
$\mathcal{C}_1$ PODĽA PREDPOKLADU A $\mathcal{C}_2 = \{B \in NP \mid SAT \leq_m B\}$
JE TIEŽ, KEĎŽE NP JE REK. PREZENT. TRIEDA.
OBE TRIEDY SÚ UZAVRETÉ NA KON. VARIÁCIE:
PRE $\mathcal{C}_2$: AK A JE NP-ÚPLNÁ A A' JE JEJ KON.
VARIÁCIA, POTOM ZREJME $A' \in NP$. NAVIAC $A \leq_m A'$,
TAKŽE A' JE NP-ÚPLNÁ.
PRE $\mathcal{C}_1$ TO VYPLÝVA Z TOHO, ŽE NP AJ NP-COMPLETE
SÚ UZAVRETÉ NA KON. VARIÁCIE (PODOBNE AKO V e))
POLOŽME $A_1 := SAT$, $A_2 := \emptyset$. ZREJME $A_1 \notin \mathcal{C}_1$, $A_2 \notin \mathcal{C}_2$.
PODĽA UNIFORM DIAG. THEOREM EXISTUJE A T.Ž.
$A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$ A $A \leq_m A_1 \oplus A_2$, TJ. $A \in NP$.
AVŠAK $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2 \Rightarrow A \notin NP$, ČO JE SPOR ↯. □

10.04.2010
PETER ČERNO

EXAM: STRUKTURÁLNI SLOŽITOST I

(9) OZNAČME $P_{FINITE} = \{ A \in P \mid A$ JE KONEČNÁ $\}$

$P_{INFINITE} = \{ A \in P \mid A$ JE NEKONEČNÁ $\}$

ZREJME P_{FINITE} JE REKURZÍVNE PREZENTOVATEĽNÁ:
KAŽDÚ KONEČNÚ MNOŽINU MOŽNO ZAKÓDOVAŤ DO KONEČNÉHO REŤAZCA, PRIČOM KONEČNÉ REŤAZCE MÔŽEME JEDNOZNAČNE REPREZENTOVAŤ PRIRODZENÝMI ČÍSLAMI. TAKŽE $P_{FINITE} = \{ L(M_i) \mid i = 1, 2, \dots \}$, KDE M_i PRIJÍMA PRÁVE TIE SLOVÁ, KTORÉ SÚ ZAKÓDOVANÉ V REŤAZCI REPREZENTOVANOM ČÍSLOM i.

PRE SPOR NECH $P_{INFINITE}$ JE TAKTIEŽ REK. PREZ.

POLOŽME $\mathcal{C}_1 := P_{FINITE}$, $\mathcal{C}_2 := P_{INFINITE}$.

OBE TRIEDY SÚ REK. PREZ. A UZAVRETÉ NA KON. VARIÁCIE.

ĎALEJ NECH $A_1 := \Sigma^*$, $A_2 := \emptyset$

ZREJME $A_1 \notin \mathcal{C}_1$, $A_2 \notin \mathcal{C}_2$.

PODĽA UNIFORM DIAG. THEOREM EXISTUJE A T.Ž. $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$ A $A \leq_m A_1 \oplus A_2$, TJ. $A \in P$.

AVŠAK $A \notin \mathcal{C}_1, A \notin \mathcal{C}_2 \Rightarrow A \notin P$, ČO JE SPOR ↯. □

(2) NECH $\mathcal{C}_1$ A $\mathcal{C}_2$ SÚ REK. PREZENTOVATEĽNÉ TRIEDY TAKÉ, ŽE $\mathcal{C}_1 \cap \mathcal{C}_2$ OBSAHUJE NEJAKÚ B A VŠETKY JEJ KONEČNÉ VARIÁCIE. POTOM $\mathcal{C}_1 \cap \mathcal{C}_2$ JE REK. PREZENT.

NECH $P_1, P_2, \ldots$ JE PREZENTÁCIA $\mathcal{C}_1$, $Q_1, Q_2, \ldots$ JE PREZENTÁCIA $\mathcal{C}_2$.

PRE $n = \langle i, j \rangle$ UVAŽUJME DTS M_n, KTORÝ FUNGUJE NASLEDOVNE:

VSTUP x
PRE KAŽDÉ y T.Ž. $|y| \leq |x|$
  OTESTUJ, ČI $y \in L(P_i) \Leftrightarrow y \in L(Q_j)$
AK PREŠLI VŠETKY TESTY, POTOM
  PRIJMI $x \Leftrightarrow x \in L(P_i)$
INAK PRIJMI $x \Leftrightarrow x \in B$

ĽAHKO NAHLIADNUŤ, ŽE PRE $\forall n$, $n = \langle i, j \rangle$:
BUĎ $L(M_n) = L(P_i) = L(Q_j)$,
ALEBO $L(M_n)$ JE KONEČNÁ VARIÁCIA B.

V OBOCH PRÍPADOCH $L(M_n) \in \mathcal{C}_1 \cap \mathcal{C}_2$.

NA DRUHEJ STRANE KAŽDÁ MNOŽINA Z $\mathcal{C}_1 \cap \mathcal{C}_2$ JE REPREZENTOVANÁ NEJAKÝM DTS M_n.

$\Rightarrow$ $\mathcal{C}_1 \cap \mathcal{C}_2 = \{ L(M_n) \mid n \geq 1 \}$

JE REK. REPREZENTÁCIA $\mathcal{C}_1 \cap \mathcal{C}_2$. $\square$

11.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(3) Nech $\mathcal{C}_1$ je rek. prezentovateľná trieda uzavretá na $\leq_m$. Keď $\mathcal{C}_2$ a $\mathcal{C}_3$ sú rekurzívne prezent. t. ž. $\mathcal{C}_1 = \mathcal{C}_2 \cup \mathcal{C}_3$, potom buď $\mathcal{C}_1 = \mathcal{C}_2$, alebo $\mathcal{C}_1 = \mathcal{C}_3$.

Pre spor nech $\mathcal{C}_2 \subset \mathcal{C}_1$ a $\mathcal{C}_3 \subset \mathcal{C}_1$.

<u>Poznámka</u>: Tvrdenie dokážeme za mierne zosilnených predpokladov – predpokladáme, že $\mathcal{C}_2$ aj $\mathcal{C}_3$ sú uzavreté na konečné variácie.

Ľahko sa totiž dá zostrojiť protipríklad bez týchto predpokladov, napr. $\mathcal{C}_1 = P$, $\mathcal{C}_2 = \{A \in P \mid \lambda \in A\}$, $\mathcal{C}_3 = \{A \in P \mid \lambda \notin A\}$.

$\mathcal{C}_1$ je uzavretá na kon. variácie:

Nech $A \in \mathcal{C}_1$ a A' je kon. variácia A.

Potom ak $A \neq \emptyset$, $A \neq \Sigma^*$ nutne $A' \leq_m A$, tj. $A' \in \mathcal{C}_1$.

Ak $A = \emptyset$, alebo $A = \Sigma^*$, potom <u>nedokážeme</u> $A' \in \mathcal{C}_1$. Musíme pridať predpoklad, že $\mathcal{C}_1$ je <u>netriviálna</u>, tj. existuje $B \in \mathcal{C}_1$ t. ž. $B \neq \emptyset$, $B \neq \Sigma^*$.

V takom prípade $\mathcal{C}_1$ obsahuje všetky konečné množiny a aj ich doplnky, pretože tieto mn. sú m-prevediteľné na B. Navyše sú to práve konečné variácie $\emptyset$ a Σ^*.

MÁME TEDA REK. PREZENT. TRIEDY $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ UZAVRETÉ NA KON. VARIÁCIE.

$\mathcal{C}_2 \subset \mathcal{C}_1 \Rightarrow \exists A_2 \in \mathcal{C}_1 \setminus \mathcal{C}_2$

$\mathcal{C}_3 \subset \mathcal{C}_1 \Rightarrow \exists A_3 \in \mathcal{C}_1 \setminus \mathcal{C}_3$.

PODĽA UNIFORM DIAG. THEOREM $\exists A$ T.Ž.

$A \notin \mathcal{C}_2$, $A \notin \mathcal{C}_3$ A $A \le_m A_2 \oplus A_3$.

AK PRIDÁME PREDPOKLAD, ŽE <u>$\mathcal{C}_1$ JE UZAVRETÁ NA $\oplus$</u>, POTOM

$$A \le_m A_2 \oplus A_3 \Rightarrow A \in \mathcal{C}_1$$

AVŠAK Z $\mathcal{C}_1 = \mathcal{C}_2 \cup \mathcal{C}_3$ A $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$ DOSTÁVAME $A \notin \mathcal{C}_1$, ČO JE SPOR.

$\Rightarrow$ NEMÔŽE BYŤ ZÁROVEŇ $\mathcal{C}_2 \subset \mathcal{C}_1$ AJ $\mathcal{C}_3 \subset \mathcal{C}_1$.

NUTNE TEDA BUĎ $\mathcal{C}_2 = \mathcal{C}_1$, ALEBO $\mathcal{C}_3 = \mathcal{C}_1$.

<u>DÔSLEDOK</u>: AK $\mathcal{C}_0$ JE UZAV. NA KON. VARIÁCIE & REK. PREZENTOVATEĽNÁ, POTOM $\mathcal{C}_1 \setminus \mathcal{C}_0$ JE REK. PREZ. $\Leftrightarrow$ $\mathcal{C}_1 \setminus \mathcal{C}_0 = \emptyset \lor \mathcal{C}_1 \setminus \mathcal{C}_0 = \mathcal{C}_1$.

<u>DÔKAZ</u>. PRE SPOR NECH $\mathcal{C}_1 \setminus \mathcal{C}_0 \neq \emptyset$ AJ $\mathcal{C}_1$ JE REK. PREZ.

POLOŽME $\mathcal{C}_2 := \mathcal{C}_1 \setminus \mathcal{C}_0$, $\mathcal{C}_3 := \mathcal{C}_1 \cap \mathcal{C}_0$

PODĽA (2) JE $\mathcal{C}_3$ REK. PREZENT., UZAVRETÁ NA KON. VAR.

NAVIAC $\emptyset \neq \mathcal{C}_2 \subset \mathcal{C}_1$, $\emptyset \neq \mathcal{C}_3 \subset \mathcal{C}_1$, $\mathcal{C}_1 = \mathcal{C}_2 \cup \mathcal{C}_3$

A TO JE SPOR S VYŠŠIE UVEDENÝM TVRDENÍM ↯ □

11.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

(4) KEĎ $\mathcal{C}$ JE REKURZÍVNE PREZENT., POTOM UZÁVER $\mathcal{C}$ NA KONEČNÚ VARIÁCIU JE TAKTIEŽ REK. PREZENT.

NECH $P_1, P_2, \dots$ PREZENTUJE $\mathcal{C}$.
PRE KAŽDÉ $n = \langle i, j \rangle$ NECH DTS M_n PRACUJE NASLEDOVNE:

> VSTUP x
> j KÓDUJE KONEČNÚ MNOŽINU STRINGOV S
> AK $x \in S$, POTOM
>   PRIJMI $x \iff x \notin L(P_i)$
> AK $x \notin S$, POTOM
>   PRIJMI $x \iff x \in L(P_i)$

$L(M_n)$ JE ZREJME KONEČNÁ VARIÁCIA $L(P_i)$
A NAOPAK PRE KAŽDÚ KONEČNÚ VARIÁCIU B JAZYKA $L(P_i)$ ZREJME EXISTUJE j T.Ž. $L(M_{\langle i,j \rangle}) = B$.

$\Rightarrow \{L(M_n) \mid n \geq 1\}$ REPREZENTUJE UZÁVER $\mathcal{C}$ NA KON. VARIÁCIU. $\square$

(5) NECH $\mathcal{C}_1$ A $\mathcal{C}_2$ SÚ REKURZÍVNE PREZ., $\mathcal{C}_1$ OBSAHUJE IBA NEKONEČNÉ MNOŽINY, $\mathcal{C}_2$ JE UZAVRETÁ NA KON. VARIÁCIE A NECH $B \notin \mathcal{C}_2$. POTOM EXISTUJE $D \in P$ T.Ž. $B \cap D \notin \mathcal{C}_1 \cup \mathcal{C}_2$.

~~ZREJME AK~~ $\cancel{B'}$ ~~JE KON. VARIÁCIA~~ $\cancel{B}$~~, POTOM~~ $\cancel{B' \notin \mathcal{C}_2}$. ~~(AK BY~~ $\cancel{B' \in \mathcal{C}_2}$~~, POTOM BY AJ~~ $\cancel{B \in \mathcal{C}_2}$~~.)~~
~~NECH~~ $\cancel{P_1, P_2, \ldots}$ ~~JE REPREZENTÁCIA~~ $\cancel{\mathcal{C}_1}$
~~A~~ $\cancel{Q_1, Q_2, \ldots}$ ~~JE REPREZENTÁCIA~~ $\cancel{\mathcal{C}_2}$.

BEZ UJMY NA OBECNOSTI MÔŽME PREDPOKLADAŤ, ŽE $\mathcal{C}_1$ JE UZAVRETÁ NA KONEČNÉ VARIÁCIE. AK BY NEBOLA, POTOM PODĽA (4) UZÁVER $\mathcal{C}_1$ NA KONEČNÉ VARIÁCIE JE REKURZÍVNE PREZENT., OBSAHUJE IBA NEKONEČNÉ MNOŽINY, A JE NADMNOŽINOU TRIEDY $\mathcal{C}_1$.

POLOŽME $A_1 := \emptyset$, $A_2 := B$. ZREJME $A_1 \notin \mathcal{C}_1$, $A_2 \notin \mathcal{C}_2$. PODĽA DÔKAZU UNIFORM DIAG. THEOREM MOŽNO ZOSTROJIŤ ČASOVO KONŠTRUOVATEĽNÚ FCIU. r T.Ž. MNOŽINA $A = (G[r] \cap A_1) \cup (\overline{G[r]} \cap A_2)$ SPĹŇA PODMIENKU $A \notin \mathcal{C}_1$, $A \notin \mathcal{C}_2$, KDE $G[r]$ JE TZV. GAP LANGUAGE GENEROVANÝ r. DÁ SA UKÁZAŤ, ŽE $G[r], \overline{G[r]} \in P$ A VZHĽADOM K TOMU, ŽE $A_1 = \emptyset$, STAČÍ POLOŽIŤ $D := \overline{G[r]}$, A DOSTÁVAME, ŽE $B \cap D \notin \mathcal{C}_1 \cup \mathcal{C}_2$, PRIČOM $B \in P$. $\square$

3/4

11.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOSŤ I

(10) UKÁŽTE, ŽE EXISTUJE ORÁKULUM B TAKÉ, ŽE $P(B) \neq NP(B) \cap co\text{-}NP(B)$.

DEFINUJME FUNKCIU $k(n) := 2^{n^n}$. DÁ SA UKÁZAŤ, ŽE k JE ČASOVO KONŠTRUOVATEĽNÁ, TJ. $\exists$ DTS M, KT. SA NA VSTUPE x ZASTAVÍ PRÁVE PO $k(|x|)$ KROKOCH.

ĽAHKO NAHLIADNUŤ, ŽE JE MOŽNÉ V POLYNOMIÁLNOM ČASE K DANÉMU VSTUPU 0^n OVERIŤ, ČI EXISTUJE m T.Ž. $n = k(m)$.

- SKÚŠAME $m = 0, 1, 2, \dots$
- PRE DANÉ m NECHÁME BEŽAŤ M NAJVIAC n KROKOV
- AK M SKONČIL PO PRÁVE n KROKOCH, TAK PRIJMEME
- AK M PO n KROKOCH NESKONČIL, TAK ZAMIETNEME
- AK M SKONČIL PO MENEJ AKO n KROKOCH, SKÚSIME ĎALŠIE m.

NAŠIM CIEĽOM JE ZOSTROJIŤ ORÁKULUM B T.Ž. $L(B) \notin P(B)$, KDE

$$L(B) = \{0^n \mid n = k(m) \ \&\ \exists x \in B : |x| = 2n\} =$$

$$= \{0^n \mid n = k(m) \ \&\ \forall x \in B : |x| \neq 2n+1\}$$

PRVÁ ROVNOSŤ IMPLIKUJE $L(B) \in NP(B)$, DRUHÁ $L(B) \in co\text{-}NP(B)$.

neprehľadné! - lepší $L_0(B) = \{0^n \mid n = k(m)$ pre nejaké m & $\exists x \in B, |x| = 2n\}$, $L_1(B) = \{y \mid y \neq 0^n\ \forall n$ t.ž. $n = k(m)$ pre nejaké m a $\exists x \in B, |x| = 2n+1\}$, $L_0(B), L_1(B) \in NP(B)$. Konštruujeme B, že $L_0(B) \notin P$ a $L_0(B) = co\text{-}L_1(B)$.

NECH $P_1, P_2, \ldots$ JE EFEKTÍVNA ENUMERÁCIA DTS S POLYNOMIÁLNYMI BUDÍKMI $p_i(n) = n^i$, KTORÁ NÁM UMOŽŇUJE REKURZÍVNE REPREZENTOVAŤ $P(A)$ PRE ĽUBOVOĽNÉ ORAKULUM A.

BUDEME KONŠTRUOVAŤ MNOŽINY $B(1), B(2), \ldots$ POSTUPNE VO FÁZACH $1, 2, \ldots$

FÁZA n: (KLADIEME $B(0) := \emptyset$)

NECH $w_0(n)$, RESP. $w_1(n)$ JE PRVÉ SLOVO DĹŽKY $2k(n)$, RESP. $2k(n)+1$, NA KTORÉ SA P_n NEDOTAZOVAL POČAS VÝPOČTU NAD $0^{k(n)}$.

AK $0^{k(n)} \in L(P_n, B(n-1))$, POTOM

$B(n) = B(n-1) \cup \{ w_1(n) \}$

V OPAČNOM PRÍPADE $B(n) = B(n-1) \cup \{ w_0(n) \}$.

KONIEC FÁZY

DEFINUJME $B := \bigcup_{n \geq 1} B(n)$.

1. $p_n(k(n)) < 2^{k(n)}$, PRETOŽE

$(2^{n^n})^n = 2^{n \cdot n^n} < 2^{2^{n^n}}$, PRETOŽE

$n^{n+1} < 2^{n^n}$, ČO PLATÍ PRE $n = 1, 2$

A PRE $n > 2$ STAČÍ POUŽIŤ:

$(n+1) \log_2 n \leq (n+1) n < n^n \quad \ldots$

11.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

P_n NAD SLOVOM $0^{k(n)}$ DOBEHNE V ČASE $p_n(k(n)) < 2^{k(n)}$ $\Rightarrow$ EXISTENCIA SLOV $w_i(n)$ JE VŽDY ZARUČENÁ.

2. $p_{n-1}(k(n-1)) < k(n)$, PRETOŽE

$$\left(2^{(n-1)^{(n-1)}}\right)^{n-1} = 2^{(n-1)^n} < 2^{n^n}$$

$\Rightarrow$ VÝPOČET P_n NAD $0^{k(n)}$ JE TAKÝ ISTÝ AJ V PRÍPADE, AK BY SME NAHRADILI ORÁKULUM $B(n-1)$ ORÁKULOM B. DÔVOD:

a) SLOVO $w_i(n)$, AK BOLO PRIDANÉ VO FÁZE n, NIE JE DOTAZOVANÉ STROJOM P_n

b) SLOVÁ $w_i(m)$ PRE $m > n$ SÚ PRÍLIŠ DLHÉ NA TO, ABY BOLI DOTAZOVANÉ STROJOM P_n.

TOTIŽ $p_n(k(n)) < k(n+1) < k(n+2) < \dots$

PLATÍ TEDA: $0^{k(n)} \in L(P_n, B(n-1)) \Leftrightarrow 0^{k(n)} \in L(P_n, B)$.

4. $\{0^n \mid n = k(m) \ \& \ \exists x \in B : |x| = 2n\} =$

$= \{0^n \mid n = k(m) \ \& \ \forall x \in B : |x| \neq 2n+1\}$.

NECH $n = k(m)$. AK $\exists x \in B : |x| = 2n$, POTOM SME VO FÁZE m PRIDALI SLOVO $w_0(m)$, A NEMOHLO SA DO B DOSTAŤ ŽIADNE SLOVO DLHÉ $2k(m)+1$.
AK $\neg\exists x \in B : |x| = 2n$, POTOM SME VO FÁZE m MUSELI DO B PRIDAŤ $w_1(m)$ DLHÉ $2k(m)+1$.

UKÁŽME EŠTE, ŽE $L(B) \notin P(B)$,

T. J. $\forall n : L(B) \neq L(P_n, B)$.

ZAFIXUJME ĽUBOVOĽNÉ n. POTOM $0^{k(n)} \in L(B) \Leftrightarrow$
$\Leftrightarrow \exists x \in B : |x| = 2k(n) \Leftrightarrow$ VO FÁZE n BOLO DO B PRIDANÉ SLOVO $w_0(n) \Leftrightarrow$
$\Leftrightarrow 0^{k(n)} \notin L(P_n, B(n-1)) \Leftrightarrow 0^{k(n)} \notin L(P_n, B)$,

T. J. $L(B) \neq L(P_n, B)$,

ČO BOLO TREBA DOKÁZAŤ. $\square$

15.04.2010 Th
Peter Černo

Exam: Štrukturálna zložitosť I

(11) Pre každé $\ell > 0$ existuje orákulum B také, že $P(B)_{n^\ell} \neq P(B)_{n^{\ell+1}}$.

Viď Theorem 7.9, J.L. Balcázar, J. Díaz, J. Gabarró: Structural Complexity II

Pre ľubovoľné orákulum definujme
$L(B) := \{ 0^n \mid \exists z \in B : |z| = n^{\ell+1} \}$
Ľahko nahliadnuť, že $L(B) \in P(B)_{n^{\ell+1}}$.
Dokážeme, že $\exists B$ t.ž. $L(B) \notin P(B)_{n^\ell}$.
Zrejme ku každému NTS môžme efektívne pridať budík, kt. počíta počet nedeterm. krokov, pričom výpočet je prerušený, ak počet týchto krokov prekročí n^ℓ.
Nech $Q_1, Q_2, \ldots$ je efektívna enumerácia NTS pracujúcich v polynomiálnom čase $p_1, p_2, \ldots$ s ohraničenými nedeterminizmom funkciou n^ℓ.
Uvažujme nasledujúci algoritmus:

Fáza 0
$B(0) := \emptyset, \quad k(0) := 0$

Fáza n
Nech $k(n)$ je najmenšie prir. číslo také, že:
$$2^{k(n)^\ell} \cdot p_n(k(n)) < 2^{k(n)^{\ell+1}} \text{ a } p_{n-1}(k(n-1)) < k(n)$$

P_n [illegible] z minulého základu?

AK $0^{k(n)} \in L(Q_n, B(n-1))$, POTOM $B(n) = B(n-1)$

V OPAČNOM PRÍPADE NECH $w(n)$ JE PRVÉ SLOVO DĹŽKY $k(n)^{l+1}$ T.Z. Q_n SA NEDOTAZOVAL NA $w(n)$ ORÁKULA $B(n-1)$ POČAS AKÉHOKOĽVEK VÝPOČTU NAD $0^{k(n)}$.

$B(n) := B(n-1) \cup \{w(n)\}$.

EXISTENCIA $k(n)$ JE ZARUČENÁ, PRETOŽE $p_n(x)$ RASTIE ASYMPTOTICKY POMALŠIE NEŽ $2^{x^{l+1}} - x^l$.
EXISTUJE NAJVIAC $2^{k(n)^l}$ RÔZNYCH VÝPOČTOV STROJA Q_n NAD SLOVOM $0^{k(n)}$, A KAŽDÝ VÝPOČET VYKONÁ NAJVIAC $p_n(k(n))$ DOTAZOV NA ORÁKULUM $B(n-1)$.
$\Rightarrow$ SPOLU NAJVIAC $2^{k(n)^l} \cdot p_n(k(n))$ DOTAZOV CEZ VŠETKY VÝPOČTY.
KEĎŽE POČET MOŽNOSTÍ PRE $w(n)$ JE $2^{k(n)^{l+1}}$, EXISTENCIA TAKÉHO $w(n)$, NA KTORÉ SA ŽIADEN VÝPOČET Q_n NAD $0^{k(n)}$ NEDOTAZOVAL, JE VĎAKA NEROVNOSTI $2^{k(n)^{l+1}} > 2^{k(n)^l} \cdot p_n(k(n))$ ZARUČENÁ.

POLOŽME $B := \bigcup_n B(n)$. PODOBNE AKO V PRÍKLADE (10) MOŽNO UKÁZAŤ, ŽE:

$$0^{k(n)} \in L(Q_n, B(n-1)) \Leftrightarrow 0^{k(n)} \in L(Q_n, B).$$

PRE ĽUBOVOĽNÉ n: $0^{k(n)} \in L(B) \Leftrightarrow \exists z \in B: |z| = k(n)^{l+1} \Leftrightarrow$ V O FÁZE n SME PRIDALI DO B $w(n)$ $\Leftrightarrow 0^{k(n)} \notin L(Q_n, B(n-1)) \Rightarrow L(B) \neq L(Q_n, B)$. $\square$

15.04.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

(12) UKÁŽTE, ŽE $P(A) = PQUERY(A) \iff$ A JE PSPACE-ŤAŽKÁ (VZHĽADOM K $\leq_T$)

PLATÍ: $PQUERY(A) = P(QBF \oplus A)$.
(VIĎ THEOREM 8.1 V STRUCTURAL COMPLEXITY II)

$\Leftarrow$) AK A JE PSPACE-ŤAŽKÁ, POTOM $QBF \leq_T A$
- INKLÚZIA $P(A) \subseteq P(QBF \oplus A)$ PLATÍ TRIVIÁLNE
A INKLÚZIA $P(QBF \oplus A) \subseteq P(A)$ JE TAKTIEŽ ZREJMÁ:
STAČÍ DOTAZY NA QBF VYRIEŠIŤ V POL. ČASE POMOCOU T-REDUKCIE NA A.
ČASOVÁ ZLOŽITOSŤ ZREJME ZOSTANE PO TEJTO ÚPRAVE POLYNOMIÁLNA.

$\Rightarrow$) PREDPOKLADAJME, ŽE $P(A) = P(QBF \oplus A)$.
CHCEME UKÁZAŤ, ŽE $QBF \leq_T A$.
ZREJME $QBF \in P(QBF \oplus A) \Rightarrow QBF \in P(A)$,
ČO BOLO TREBA DOKÁZAŤ. $\square$

(13) UKÁŽTE, ŽE EXISTUJE ORÁKULUM A T.Ž.:
a) $NPQUERY(A) \neq PSPACE(A)$
b) $NPQUERY(A) \neq PQUERY(A)$

- PLATÍ NASLEDUJÚCA VETA:
NECH $\{M_i\}$ JE EFEKTÍVNA ENUMERÁCIA NTS S ORÁKULOM A F JE TRIEDA ČASOVO SKONŠTR. FCIÍ.

PREDPOKLADAJME, ŽE PLATIA NASLEDUJÚCE PODMIENKY:

i) PRE KAŽDÝ NTS M_i EXISTUJE $f \in F$ T.Ž. PRE KAŽDÉ ORÁKULUM A A VSTUP x JE

$$|Q(M, A\ x)| \leq f(|x|)$$

(ii) EXISTUJE INJEKTÍVNA FUNKCIA $t \in F$ T.Ž. $2^{t(n)} > f(n)$ PRE KAŽDÚ $f \in F$ A PRE SKORO VŠETKY n.

POTOM EXISTUJE ORÁKULUM B T.Ž. $NTIME(F, B)$ NIE JE OBSIAHNUTÝ V $\{L(M_i, B) \mid i = 1, 2, \dots\}$.

KONKRÉTNE $L(B) \overset{def.}{:=} \{0^n \mid \exists x \in B \ \ |x| = t(n)\} \notin$

$Q(M, A, x)$ OZNAČUJE MNOŽINU $\forall$ SLOV w TAKÝCH, ŽE EXISTUJE VÝPOČET M NAD x S ORÁKULOM A T.Ž. M POLOŽÍ DOTAZ w NA ORÁKULUM.

→ VIĎ THEOREM 7.8, STRUCTURAL COMPLEXITY II

---

a) NPQUERY(A) JE TRIEDA MNOŽÍN PRIJÍMANÝCH NTS PRACUJÚCIMI V POL. PRIESTORE S ORÁKULOM A, PRIČOM POČET DOTAZOV JE V KAŽDOM VÝPOČTE OHRANIČENÝ POLYNÓMOM.

ZREJME NPQUERY(A) $\subseteq$ NSPACE(A) = PSPACE(A).

NÁJDEME ORÁKULUM C T.Ž.

NPQUERY(C) $\neq$ CO-NPQUERY(C).

AKO DÔSLEDOK DOSTANEME NPQUERY(C) $\neq$ PSPACE(C), PRETOŽE PSPACE(C) JE UZAVRETÁ NA DOPLNKY.

3/5

15.04.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

NECH $Q_1, Q_2, \ldots$ JE EFEKTÍVNA ENUMERÁCIA NTS S ORÁKULOM POPISUJÚCICH NPQUERY(A). STAČÍ ZOBRAŤ EFEKTÍVNU ENUMERÁCIU NTS $P_1, P_2, \ldots$ DOKAZUJÚCU REKURZÍVNU PREZENTOVATEĽNOSŤ TRIEDY NSPACE(A) A PRIDAŤ K NÍM POL. BUDÍKY $p_1, p_2, \ldots$ OHRANIČUJÚCE POČET DOTAZOV NA ORÁKULUM (V KAŽDOM VÝPOČTE).

NECH $C := \bigcup_n C(n)$, KDE $C(n)$ ZOSTROJÍME NASLEDOVNE:

FÁZA 0:

$C(0) := \emptyset$, $k(0) := 0$

FÁZA n:

NECH $k(n)$ JE NAJMENŠIE ČÍSLO T. Ž.

Lebo sa nájde?

$$p_n(k(n)) < 2^{k(n)} \text{ A } k(n) > q_{n-1}(k(n-1))$$

AK $0^{k(n)} \in L(Q_n, C(n-1))$, POTOM

ZAFIXUJME NEJAKÝ PRIJÍMAJÚCI VÝPOČET Q_n NA SLOVE $0^{k(n)}$, A NECH $w(n)$ JE PRVÉ SLOVO DĹŽKY $k(n)$, KT. NEBOLO DOTAZOVANÉ ORÁKULA $C(n-1)$ POČAS TOHTO VÝPOČTU.

$C(n) := C(n-1) \cup \{w(n)\}$

INAK $C(n) := C(n-1)$.

ZREJME $k(n)$ VŽDY EXISTUJE, PRETOŽE 2^x RASTIE RÝCHLEJŠIE AKO $p_n(x)$.

TAKTIEŽ EXISTENCIA $w(n)$ JE VŽDY ZARUČENÁ, PRETOŽE Q_n POČAS VÝPOČTU NAD $O^{k(n)}$ POLOŽÍ NAJVIAC $p_n(k(n))$ DOTAZOV, A $p_n(k(n)) < 2^{k(n)}$

Q_n MÔŽE POČÍTAŤ VEĽMI DLHO, AVŠAK VZHĽADOM K TOMU, ŽE POČÍTA V POLYNOMIÁLNE OHRANIČ. PRIESTORE q_n $\Rightarrow$ MÔŽME BEZ UJMY NA OBECN. PREDP., ŽE KAŽDÝ VÝPOČET JE KONEČNÝ.

TAKTIEŽ MOŽNO ĽAHKO NAHLIADNUŤ, ŽE VÝPOČET Q_n NAD $O^{k(n)}$ SA NEZMENÍ, AK NAMIESTO ORÁKULA $C(n-1)$ POUŽIJEME ORÁKULUM C.

q_i JE POLYNÓM OHRANIČUJÚCI PRACOVNÝ PRIESTOR Q_i
$\Rightarrow$ $q_i(k(i))$ JE TÝM PÁDOM:
HORNÁ HRANICA NA DĹŽKU DOTAZU, AKÝ MÔŽE POLOŽIŤ STROJ Q_i ORÁKULU PRI PRÁCI NAD $O^{k(i)}$ (PRE VŠETKY FÁZY $1, \dots, n-1$).

JE ZREJMÉ, ŽE KEĎ VO FÁZE n PRIDÁME DO C SLOVO $w(n)$ DĹŽKY $k(n)$, TAK STROJE $Q_1, \dots, Q_{n-1}$ HO TAKPOVEDIAC „NEVIDIA", PRETOŽE KLADÚ DOTAZY $< k(n)$.

TO, ŽE Q_n PRACUJE ROVNAKO S ORÁKULOM $C(n)$ AKO AJ S $C(n-1)$ JE VIDIEŤ Z DEFINÍCIE $w(n)$.

15.04.2010 Th
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOSŤ I

DEFINUJME $L(C) = \{0^n \mid \exists z \in C : |z| = n\}$.

PLATÍ $L(C) \in NP(C) \subseteq NPQUERY(C)$.

DOKÁŽME, ŽE $L(C) \in co\text{-}NPQUERY(C)$. asi $\notin$

NECH n JE ĽUBOVOĽNÉ PRIR. ČÍSLO.

$0^{k(n)} \in L(C) \iff \exists z \in C : |z| = k(n) \iff$?

VO FÁZE n SME DO C PRIDALI $w(n) \iff$

$0^{k(n)} \in L(Q_n, C(n-1)) \iff 0^{k(n)} \in L(Q_n, C)$.

$\Rightarrow L(C) \neq \overline{L(Q_n, C)}$.

TO ALE ZNAMENÁ, ŽE $L(C) \notin co\text{-}NPQUERY(C)$

$\Rightarrow NPQUERY(C) \neq co\text{-}NPQUERY(C)$

$\Rightarrow NPQUERY(C) \neq PSPACE(C)$. $\square$

b) $PQUERY(A)$ JE TRIEDA MNOŽÍN PRIJÍMANÝCH DTS PRACUJÚCIMI V POL. PRIESTORE S ORÁKULOM A, PRIČOM POČET DOTAZOV JE POLYNOM. OHRANIČENÝ, T.J. $Q(M, A, x)$ MÁ NAJVIAC $p(|x|)$ ČLENOV PRE NEJAKÝ POLYNÓM.

MÁME EFEKTÍVNU ENUMERÁCIU DTS POPISUJÚCU TRIEDU $PQUERY(A)$ – STAČÍ PRIDAŤ POLYN. BUDÍKY NA POČET DOTAZOV STROJOM $P_1, P_2, \ldots$ DOKAZUJÚCIM REK. PREZENTOVATEĽNOSŤ TRIEDY $PSPACE(A)$.

VYUŽIJEME VETU Z ÚVODU TOHTO PRÍKLADU.
POLOŽME $F :=$ MN. VŠETKÝCH POLYNÓMOV.
ĽAHKO NAHLIADNUŤ, ŽE SÚ SPLNENÉ OBA PREDPOKLADY i) AJ ii). STAČÍ POLOŽIŤ $t(n) = n$.
$\Rightarrow \exists$ ORÁKULUM C T.Ž. $NP(C)$ NIE JE PODMNOŽINOU $PQUERY(C)$.
KEĎŽE $NP(C) \subseteq NPQUERY(C)$, NUTNE
$NPQUERY(C) \neq PQUERY(C)$. $\square$

(14) NÁJDITE ORÁKULUM A T.Ž. $NP(A) \neq NP_b(A)$.
$NP_b(A)$ JE TRIEDA MNOŽÍN PRIJÍMANÝCH NTS PRACUJÚCIMI V POL. ČASE S ORÁKULOM A T.Ž. $|Q(M, A, x)| \leq p(|x|)$ PRE NEJAKÝ POLYNÓM p.

NAJSKÔR MUSÍME ZOSTROJIŤ EFEKTÍVNU ENUMERÁCIU NTS $Q_1, Q_2, \ldots$ REPREZENTUJÚCU TRIEDU $NP_b(A)$.
NECH $P_1, P_2, \ldots$ JE EFEKTÍVNA ENUMERÁCIA NTS DOKAZUJÚCA REKURZÍVNU PREZENTOVATEĽNOSŤ TRIEDY $NP(A)$, NECH P_i PRACUJE V ČASE p_i $\forall i$.
NAŠÍM CIEĽOM JE VYROBIŤ Z NTS P_i NTS Q_i TAK, ABY PRE KAŽDÉ ORÁKULUM A PLATILO $|Q(Q_i, A, x)| \leq p_i(|x|)$ PRE $\forall x$.
STROJ Q_i BUDE PRACOVAŤ NASLEDOVNE:

15.04.2010 Th
PETER ČERNO

EXAM: STRUKTURÁLNI SLOŽITOST I

VSTUP x ORÁKULUM A

NEDETERMINISTICKY UHÁDNI KONEČNÚ MNOŽINU STRINGOV q DLHÝCH NAJVIAC $p_i(|x|)$, O CELKOVOM POČTE NAJVIAC $p_i(|x|)$.

SIMULUJ PRÁCU STROJA P_i NA VSTUPE x, PRIČOM VŽDY KEĎ P_i POLOŽÍ DOTAZ w

NAJSKÔR SKONTROLUJ, ČI $w \in q$:

AK $w \in q$, POTOM

POKRAČUJ VO VETVE YES, RESP. NO,

PODĽA VÝSLEDKU DOTAZU $w \overset{?}{\in} A$

AK $w \notin q$, POTOM ODMIETNI.

to nevidím, co když uhodne mimo [illegible] dotazy? [illegible]

ĽAHKO NAHLIADNUŤ, ŽE $|Q(Q_i, A, x)| \leq p_i(|x|)$ $Q(M, A, x)$

NA DRUHEJ STRANE NECH M JE NTS PRACUJÚCI V POLYNOM. ČASE TAKÝ, ŽE PRE KAŽDÉ ORÁKULUM A JE $|Q(M, A, x)| \leq p(|x|)$ PRE $\forall x$, KDE p JE POLYNÓM.

ISTOTNE EXISTUJE i: P_i FUNGUJE PRESNE TAK ISTO AKO M, NAVIAC $p(|x|) \leq p_i(|x|)$ PRE ~~SKORO~~ VŠETKY VSTUPY x.

TREBA UKÁZAŤ, ŽE MODIFIKÁCIA P_i NA Q_i NIČ NEPOKAZÍ, TJ. $\forall A : L(M, A) = L(P_i, A) = L(Q_i, A)$.

AK Q_i NA ZAČIATKU UHÁDNE $q = Q(M, A, x)$,

POTOM ZVYŠOK PROGRAMU Q_i POČÍTA PRESNE TAK ISTO AKO P_i, T. J. M.

AK $q \neq Q(M, A, x)$, POTOM TO NAJHORŠIE, ČO SA NÁM MÔŽE STAŤ JE, ŽE Q_i NEPRIJME NIEKTORÉ VSTUPY, KTORÉ BY INAK PRIJAL. TO VŠAK NEDETERMINIST. STROJOM NEVADÍ, TAKŽE IHNEĎ DOSTÁVAME

$L(Q_i, A) = L(P_i, A)$.

$\Rightarrow \{Q_i\}$ JE EFEKTÍVNA ENUMERÁCIA NTJ S ORÁKULOM REPREZENTUJÚCICH $NP_b(A)$.

POLOŽME $F :=$ MNOŽINA $\forall$ POLYNÓMOV.

OPÄŤ SÚ SPLNENÉ PREDPOKLADY VETY Z ÚLOHY (13)

$\Rightarrow$ EXISTUJE ORÁKULUM B T. Ž. $NTIME(F, B) = NP(B)$ NIE JE OBSIAHNUTÝ V $\{L(Q_i, B) \mid i = 1, 2, \dots\}$

T. J. $NP(B) \neq NP_b(B)$. $\square$

to by vadilo, ale takhle vznikne jen menší množina přijímajících výpočtů nad slovem $x \in L(M)$ (ale nepřijme žádné jiné)

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

(15) UKÁŽTE, ŽE $P/\log \subseteq \bigcup_A P_\ell(A) \subseteq \Delta_2/\log$.

a) $P/\log \subseteq \bigcup_A P_\ell(A)$

$P_\ell(A)$ OZNAČUJE TRIEDU MNOŽÍN PRIJÍMANÝCH DTS PRACUJÚCIMI V POL. ČASE S ORÁKULOM A T.Ž.
$|QU(M,n)| \leq c \cdot \log n$ PRE NEJAKÚ KONŠTANTU c,
KDE $Q(M,x) = \bigcup_A Q(M,A,x)$ A $QU(M,n) = \bigcup_{x,\, |x|=n} Q(M,x)$.

NECH $L \in P/\log \Rightarrow \exists B \in P$ A f RADIACA FCIA.
T.Ž. $\forall n\ |f(n)| \leq c \cdot \log n$ PRE NEJAKÚ KONŠT. c, PRIČOM
$x \in L \Leftrightarrow \langle x, f(|x|) \rangle \in B$.

UVAŽUJME NASLEDUJÚCE ORÁKULUM:
$A = \{ \langle 0^n, 0^m, z \rangle \mid m\text{-TÝ ZNAK (BIT) } f(n) \text{ JE } z \}$
A NASLEDUJÚCI DTS M:

```
VSTUP x, ORÁKULUM A
w ← λ
LOOP
    IF <0^|x|, 0^(|w|+1), 0> ∈ A THEN w ← w0
    ELSE IF <0^|x|, 0^(|w|+1), 1> ∈ A, THEN w ← w1
    ELSE BREAK LOOP
    IF |w| > c·log n, THEN REJECT
ENDLOOP
ACCEPT ⇔ <x,w> ∈ B. ELSE REJECT.
```

JE ZREJMÉ, ŽE

$$QU(M,n) = \bigcup_A \bigcup_{x,|x|=n} Q(M,A,x)$$
$$\subseteq \{ \langle 0^n, 0^k, z \rangle \mid 1 \le k \le c \cdot \log n + 1, \ z \in \{0,1\} \}$$

$$\Rightarrow |QU(M,n)| \le 2(c \cdot \log n + 1) = O(\log n).$$

NAVIAC ĽAHKO NAHLIADNUŤ, ŽE NA KONCI CYKLU LOOP PLATÍ $w = f(|x|)$, TAKŽE $L(M,A) = L$.

$$\Rightarrow P/\log \subseteq \bigcup_A P_\ell(A). \quad \square$$

b) $\bigcup_A P_\ell(A) \subseteq \Delta_2/\log$.

$\Delta_2 = P(\Sigma_1) = P(K)$, KDE K JE NP-ÚPLNÁ MNOŽINA

$$\Delta_2/\log = \{ A \mid \exists B \in \Delta_2, f : \forall n : |f(n)| \le c \log n$$
$$x \in A \Leftrightarrow \langle x, f(|x|) \rangle \in B \}$$

NECH $L \in P_\ell(A)$ PRE NEJAKÉ (ĽUBOVOĽNÉ) A A NECH M JE DTS PRACUJÚCI V POL. ČASE r S ORÁKULOM, DOKAZUJÚCI $L \in P_\ell(A)$, T.J.

$L = L(M,A)$ A EXISTUJE KONŠTANTA c T.Ž.

$|QU(M,n)| \le c \log n$

~~PLATÍ NASLEDUJÚCA LEMMA:~~

~~(VIĎ LEMMA 8.1, STRUCTURAL COMPLEXITY II)~~

~~LEMMA: NECH M JE ĽUBOVOĽNÝ NTS PRACUJÚCI V POL. ČASE S ORÁKULOM, A ORÁKULUM A x VSTUP.~~

2/8 18.04.2010 Su
PETER ČERNO

EXAM: STRUKTURÁLNI SLOŽITOST I

DEFINUJME NASLEDUJÚCU MNOŽINU:

pref = { $\langle 0^n, z \rangle$ | z JE PREFIX SLOVA TVARU w#, KDE w BOLO DOTAZOVANÉ POČAS VÝPOČTU DTS M NAD NEJAKÝM VSTUPOM x, $|x| = n$ A NEJAKÝM ORÁKULOM A }.

TO, ŽE pref $\in$ NP DOKAZUJE NASL. ALGORITMUS:

VSTUP $u = \langle 0^n, z \rangle$
NEDETERMINISTICKY UHÁDNI x, $|x| = n$
NEDETERMINISTICKY UHÁDNI POMOCNÉ BINÁRNE SLOVO $y \in \{0,1\}^{r(|x|)}$ jak [illegible]
$i := 1$, $Y := \emptyset$, $N := \emptyset$
SIMULUJ PRÁCU DTS M NAD SLOVOM x
AK SA M ZASTAVÍ V PRIJÍMAJÚCOM, RESP. ODMIETAJÚCOM STAVE, TAK ODMIETNI
AK M POLOŽÍ DOTAZ w, TAK:
    AK z JE PREFIX w#, POTOM PRIJMI A SKONČI
    AK $w \in Y$, TAK POKRAČUJ VO VETVE YES, POPR.
    AK $w \in N$, TAK POKRAČUJ VO VETVE NO
    V OPAČNOM PRÍPADE:
        AK i-TY BIT y JE 1, POTOM
            $Y := Y \cup \{w\}$, $i := i+1$,
            A POKRAČUJ VO VETVE YES

AK i-TY BIT y JE 0, POTOM

$N := N \cup \{w\}$, $i := i+1$,

A POKRAČUJ VO VETVE NO.

není mi jasné k čemu je třeba y a N - jde to zabezpečit jen slovem?

UVEDENÝ ALGORITMUS ZREJME PRACUJE V NEDETERM. POLYNOMIÁLNOM ČASE, A ĽAHKO NAHLIADNUŤ, ŽE PRIJÍMA PRÁVE pref.

NASLEDUJÚCI ALGORITMUS POPISUJE KONŠTRUKCIU FUNKCIE $q \in PF(\text{pref})$, KTORÁ KU VSTUPU 0^n V POL. ČASE A S ORÁKULOM pref ZOSTROJÍ KÓD MNOŽINY $QU(M,n)$.

VSTUP x, ORÁKULUM pref

SKONTROLUJ, ČI x JE TVARU 0^n, INAK ODMIETNI

$qu := \emptyset$

AK $\langle 0^n, \lambda \rangle \in \text{pref}$, POTOM ZAVOLAJ SUBRUTINU

construct-from (λ)

VÝSTUP $:= qu$

- - - - - - - - - - - - - - -

construct-from (z) :

AK $\langle 0^n, z0 \rangle \in \text{pref}$, POTOM const.-from $(z0)$;

AK $\langle 0^n, z1 \rangle \in \text{pref}$, POTOM const.-from $(z1)$;

AK $\langle 0^n, z\# \rangle \in \text{pref}$, POTOM $qu := qu \cup \{z\}$.

- co tady přičítáte? - jeden prvek v $QU(M,n)$?

Něco mi tady nesedí.

18.04.2010 SU
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

KEĎŽE $|QU(M,n)| \leq c \log n$, NUTNE POČET SLOV MNOŽINY $\{\langle 0^n, z\rangle \in pref\}$ JE PRE DANÉ n NAJVIAC $c \cdot (n+1) \cdot \log n$, TJ. NAJVIAC POLYNOMIÁLNE VEĽA SLOV. / ?

Z TOHO ĽAHKO NAHLIADNÚŤ, ŽE g PRACUJE V POLYNOM. ČASE.

KOREKTNOSŤ ALGORITMU JE ZREJMÁ.

DEFINUJME EŠTE K':

$K' := \{ \langle M, x, 1^t, F \rangle \mid M$ JE KÓD NTS S ORÁKULOM, F JE KÓD KONEČNEJ MNOŽINY, M PRIJÍMA x V t KROKOCH S ORÁKULOM $F \}$.

ZREJME $K' \in NP$.

NAKONIEC DEFINUJME RADIACU FUNKCIU f:

$f(0^n) = y$, $|y| = |QU(M,n)| \leq c \cdot \log n$

i-TY BIT $y = 1 \Leftrightarrow$ i-TE SLOVO MNOŽINY $QU(M,n)$ V LEXIKOGRAF. USPORIADANÍ PATRÍ DO ORÁKULA A. V OPAČNOM PRÍPADE JE i-TY BIT $y = 0$.

NASLEDUJÚCI ALGORITMUS DOKAZUJE $L \in A_2/\log$:

VSTUP x

SPOČÍTAJ $qu := q(0^{|x|})$;

(qu KÓDUJE MNOŽINU $QU(M, |x|)$)

SPOČÍTAJ $y := f(0^{|x|})$

y JEDNOZNAČNE POPISUJE, KT. SLOVÁ MNOŽINY $QU(M, |x|)$ PATRIA DO A.

NECH F KÓDUJE KONEČNÚ MN. TÝCHTO SLOV.

(F VIEME SPOČÍTAŤ Z qu A Z y V POL. ČASE:

NAJSKÔR ZOTRIEDIME (LEXIKOGRAFICKY) SLOVÁ V qu → DOSTANEME qu_{lex}

i-TE SLOVO qu_{lex} PATRÍ DO $F \iff$ i-TY BIT y JE 1)

PRIJMI $\iff \langle M, x, 1^{r(|x|)}, F \rangle \in K'$.

KOREKTNOSŤ ALGORITMU JE ZREJMÁ, PRETOŽE F OBSAHUJE VŠETKY TIE SLOVÁ Z A, NA KT. SA M MOHOL POČAS VÝPOČTU NAD x DOTAZOVAŤ.

ĎALEJ $pref \in NP \Rightarrow pref \leq_m K$, TAKŽE

$q \in PF(pref) \Rightarrow q \in PF(K)$

NAKONIEC $K' \in NP \Rightarrow K' \leq_m K$.

$\Rightarrow$ POMOCOU ORÁKULA K A RADVACEJ FUNKCIE f VIEME ROZHODNÚŤ V POL. ČASE, ČI $x \in L$

$\Rightarrow L \in P(K)/log = \Delta_2/log$. $\square$

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(17) KEĎ $P/\log \neq \bigcup_A P_e(A)$, POTOM $P \neq NP$.

PODĽA (15) PLATÍ $P/\log \subseteq \bigcup_A P_e(A) \subseteq \Delta_2/\log$.

$P = NP \Rightarrow K \in P \Rightarrow \Delta_2 = P(\Sigma_1) = P(K) = P$

$\Rightarrow \Delta_2/\log = P/\log \Rightarrow$

$P/\log = \bigcup_A P_e(A)$, ČO BOLO TREBA DOKÁZAŤ. $\square$

(1) UKÁŽTE, ŽE $A \in P/poly \Leftrightarrow \exists T$ TALLY MNOŽINA T.Ž. $A \in P(T)$.

$\Leftarrow$) PLATÍ, ŽE $P/poly = \bigcup_{S \text{ RIEDKA}} P(S)$

VIĎ THEOREM 5.5, STRUCTURAL COMPLEXITY I

KAŽDÁ TALLY MNOŽINA T JE RIEDKA

$\Rightarrow P(T) \subseteq P/poly$.

$\Rightarrow$) $A \in P/poly \Rightarrow \exists S$ RIEDKA T.Ž. $A \in P(S)$

KU KAŽDEJ RIEDKEJ S EXISTUJE TALLY MNOŽINA T T.Ž. $S \leq_T T$.

VIĎ THEOREM 4.3, STRUCTURAL COMPLEXITY I

$\Rightarrow$ KAŽDÝ DOTAZ NA S MÔŽME VYRIEŠIŤ V POL. ČASE S ORÁKULOM T $\Rightarrow A \in P(T)$. $\square$

(2) UKÁŽTE, ŽE $DEXT \neq EXPSPACE$

$\Leftrightarrow PSPACE \cap (P/poly) \neq P$.

$DEXT = \bigcup_{c \geq 0} DTIME(2^{cn})$

$EXPSPACE = \bigcup_{c \geq 0} DSPACE(2^{c \cdot n})$

AK $A \in EXPSPACE$, POTOM $tally(A) \in PSPACE$

NECH M JE DTS PRACUJÚCI V EXPONENCIÁLNOM PRIESTORE PRIJÍMAJÚCI A.

UVAŽUJME NASLEDUJÚCI ALGORITMUS M':

{ VSTUP w

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

- AK w NIE JE TVARU 0^n, POTOM ODMIETNI
- INAK SIMULUJ M NA VSTUPE n
- PRIJMI $\Leftrightarrow$ M PRIJAL, INAK ODMIETNI.

ZREJME M' PRIJÍMA $tally(A)$. POTREBUJE K TOMU PRACOVNÝ PRIESTOR EXPONENCIÁLNY VZHĽADOM K $|n|$, TJ. $2^{c \cdot |n|}$. AVŠAK $|n| = \lceil \log_2 n \rceil \Rightarrow$ PRIESTOROVÁ ZLOŽITOSŤ JE n^c, TJ. $|w|^c$.
$\Rightarrow$ $tally(A) \in$ PSPACE.

PLATÍ TIEŽ OPAČNÁ IMPLIKÁCIA:
AK $tally(A) \in$ PSPACE, POTOM $A \in$ EXPSPACE.
NECH DTS M PRACUJÚCI V POL. PRIESTORE PRIJÍMA $tally(A)$.
UVAŽUJME NASLEDUJÚCI ALGORITMUS M':

- VSTUP n
- SIMULUJ M NA VSTUPE 0^n
- PRIJMI $\Leftrightarrow$ M PRIJAL, INAK ODMIETNI.

ZREJME M' PRIJÍMA A. POTREBUJE K TOMU PRACOVNÝ PRIESTOR $|0^n|^c = n^c$. AVŠAK $|n| = \lceil \log_2 n \rceil$, TAKŽE $n^c = 2^{c \cdot \log_2 n} \leq 2^{c \cdot \lceil \log_2 n \rceil} =$
$= 2^{c \cdot |n|}$, ČO JE EXPONENCIÁLNE VEĽA VZHĽADOM K DĹŽKE VSTUPU n. $\Rightarrow$ $A \in$ EXPSPACE.

SPOLU S PROPOSITION 4.6, STRUCTURAL COMPLEXITY I DOSTÁVAME:

(1) $A \in DEXT \Leftrightarrow tally(A) \in P$

(2) $A \in EXPSPACE \Leftrightarrow tally(A) \in PSPACE$

AKO DÔSLEDOK DOSTAVAME TVRDENIE:

$DEXT \neq EXPSPACE \Leftrightarrow \exists$ TALLY MNOŽINA $\in PSPACE \setminus P$

$\Rightarrow$) $DEXT \neq EXPSPACE \Rightarrow \exists A \in EXPSPACE \setminus DEXT$
$\Rightarrow tally(A) \in PSPACE \setminus P$

$\Leftarrow$) NECH $T \in PSPACE \setminus P$ JE TALLY MNOŽINA.
POLOŽME $A := \{ n \mid 0^n \in T \}$. ZREJME $tally(A) = T$
$\Rightarrow A \in EXPSPACE \setminus DEXT$. $\square$

ĎALEJ VYUŽIJEME THEOREM 4.3, STRUCT. COMPLEXITY I:
PRE KAŽDÚ RIEDKU S EXISTUJE TALLY T: $S \leq_T T$.
NAVIAC AK $S \in NP$, POTOM AJ $T \in NP$.
MY NAVIAC DOPLNÍME TVRDENIE, ŽE
AK $S \in PSPACE$, POTOM AJ $T \in PSPACE$.

MAJME S RIEDKU. PRE KAŽDÉ n LEXIKOGRAFICKY USPORIADAJME VŠETKY SLOVÁ S DĹŽKY n.
NECH $y_{n,j}$ JE j-TE SLOVO DĹŽKY n V TOMTO USPORIADANÍ.

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

NECH $C_S(n)$ OZNAČUJE POČET SLOV V S DĹŽKY n. PODĽA PREDPOKLADU EXISTUJE POLYNÓM p TAKÝ, ŽE $C_S(n) \leq p(n)$.

DEFINUJME MNOŽINU:

$$\text{bits}(S) = \{ \langle n, k, i, j, b \rangle \mid k \leq C_S(n),$$
$$i\text{-TY BIT } y_{n,j} \text{ JE } b \}$$

DÁ SA UKÁZAŤ, ŽE $S \in P(T)$, KDE $T = \text{tally}(\text{bits}(S))$.

DOKÁŽME EŠTE, ŽE AK $S \in$ PSPACE, POTOM AJ $T \in$ PSPACE.

NECH M JE DTS PRACUJÚCI V POL. PRIESTORE PRIJÍMAJÚCI MNOŽINU S.

UVAŽUJME NASLEDUJÚCI ALGORITMUS M':

VSTUP x
AK x NIE JE TVARU 0^t, TAK ODMIETNI
NECH $t = \langle n, k, i, j, b \rangle$
PRE KAŽDÚ k-TICU SLOV $y_{n,m}$ DĹŽKY n:
    SKONTROLUJ, ČI SÚ LEXIKOGRAF. USPORIADANÉ.
    AK ÁNO, POTOM SKONTROLUJ,
    ČI KAŽDÉ $y_{n,m} \in S$ (POMOCOU M)
    AK SÚ SPLNENÉ VŠETKY PODMIENKY
    A NAVIAC i-TY BIT $y_{n,j}$ JE b, TAK PRIJMI
INAK SKÚS ĎALŠIU k-TICU
ODMIETNI.

ĽAHKO NAHLIADNUŤ, ŽE M' PRIJÍMA T
V POLYNOMIÁLNOM PRIESTORE.

<u>DÔSLEDOK</u>: DEXT $\neq$ EXPSPACE $\Leftrightarrow$
$\exists$ RIEDKA $S \in$ PSPACE $\setminus$ P.

$\Rightarrow$) ZREJME PLATÍ, PRETOŽE DEXT $\neq$ EXPSPACE $\Rightarrow$
$\exists$ TALLY MNOŽINA $T \in$ PSPACE $\setminus$ P, TAKŽE
STAČÍ POLOŽIŤ $S := T$.
$\Leftarrow$) NECH $S \in$ PSPACE $\setminus$ P JE RIEDKA.
PODĽA VYŠŠIE UVEDENÉHO TVRDENIA EXISTUJE
TALLY MNOŽINA T TAKÁ, ŽE $S \leq_T T$ A
NAVIAC $T \in$ PSPACE. T NEMÔŽE BYŤ V P.
AK BY $T \in P$, POTOM $S \leq_T T \Rightarrow S \in P$, ČO
BY BOLO V SPORE S PREDPOKLADOM $S \in$ PSPACE $\setminus$ P.
MÁME TALLY MNOŽINU $T \in$ PSPACE $\setminus$ P, TAKŽE
NUTNE DEXT $\neq$ EXPSPACE. $\square$

NA DOKONČENIE PRÍKLADU NÁM STAČÍ UKÁZAŤ EKVIV.:

$\exists$ RIEDKA $S \in$ PSPACE $\setminus$ P $\Leftrightarrow$
PSPACE $\cap$ (P/POLY) $\neq$ P

VYUŽIJEME THEOREM 5.5, STRUCTURAL COMPLEXITY I:
P/POLY $= \bigcup_{S \text{ RIEDKA}} P(S)$.

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

$\Rightarrow$) $\exists$ riedka $S \in PSPACE \setminus P$,
potom tiež $S \in PSPACE \cap (P/poly)$,
pretože $S \in P(S) \subseteq P/poly$.
Avšak $S \notin P$, takže $PSPACE \cap (P/poly) \neq P$.

$\Leftarrow$) Nech $PSPACE \cap (P/poly) \neq P$, tj.
$\exists A \in PSPACE \cap (P/poly) \setminus P$, tj.
existuje riedka S : $A \in PSPACE \cap P(S) \setminus P$

Nech p je polynóm taký, že pre každé n
je $|C_S(n)| \leq p(n)$, kde
$C_S(n) = \{ w \in S \mid |w| \leq n \}$.

Nech M je DTS pracujúci v polynomiálnom čase $r(n)$ s orákulom, dokazujúci $A \in P(S)$, tj. $L(M, S) = A$.

V nasledujúcom zostrojíme riedku množinu $S' \in PSPACE$ takú, že $A \in P(S')$.

Najskôr si všimnime, že pre vstup dĺžky n položí DTS M najviac $r(n)$ dotazov, každý dotaz o dĺžke najviac $r(n)$.

$S' = \{ \langle 0^n, s \rangle \mid$ S JE PREFIX STRINGU t, KT. JE V LEX. USPORIADANÍ PRVÝ STRING KÓDUJÚCI KONEČNÚ MNOŽINU (OBSAHUJÚCU NAJVIAC $r(n)$ SLOV DĹŽKY NAJVIAC $r(n)$) TAKÚ, ŽE:

$$\forall x, |x|=n \quad x \in A \Leftrightarrow x \in L(M,t) \} .$$

ĽAHKO NAHLIADNUŤ, ŽE DĹŽKU STRINGU t MOŽNO ZHORA OHRANIČIŤ POLYNÓMOM ... POVEDZME $q(n)$

NASLEDUJÚCI ALGORITMUS DOKAZUJE $S' \in PSPACE$

- VSTUP x
- OVER, ČI $x = \langle 0^n, s \rangle$, INAK ODMIETNI
- POSTUPNE PRE KAŽDÝ STRING t DĹŽKY $q(n)$ V LEXIKOGRAFICKOM USPORIADANÍ VYKONAJ:
  - OVER, ČI t KÓDUJE KONEČNÚ MN. STRINGOV.
  - AK ÁNO, OVER, ČI PRE KAŽDÉ y, $|y|=n$ PLATÍ $y \in A \Leftrightarrow y \in L(M,t)$
  - AK SÚ SPLNENÉ VŠETKY PODMIENKY A NAVIAC S JE PREFIX t, TAK PRIJMI
  - AK SÚ SPLNENÉ VŠETKY PODMIENKY, ALE S NIE JE PREFIX t, TAK ODMIETNI
  - INAK SKÚS ĎALŠÍ STRING t
- ODMIETNI (TU SA ALE NIKDY NEDOSTANEME ...)

18.04.2010 Su
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

STRING t JE PRE DANÉ n JEDNOZNAČNE URČENÝ, TAKŽE PRE DANÉ n PATRÍ DO S' NAJVIAC $q(n)$ RÔZNYCH SLOV TVARU $\langle 0^n, s \rangle$ (PRE KAŽDÝ PREFIX s SLOVA t JEDNO SLOVO, $|t| \leq q(n)$)

PRE DANÉ m JE V S NAJVIAC $m+1$ SLOV DĹŽKY m, PRETOŽE n MÔŽE BYŤ IBA Z MN. $\{0, 1, 2, \dots, m\}$ A s JE URČENÉ JEDNOZNAČNE Z n + DĹŽKY SLOVA $|\langle 0^n, s \rangle| = m$.
$\Rightarrow$ S' JE RIEDKA MNOŽINA.

TO, ŽE $S' \in PSPACE$ JE VIDIEŤ Z POPISU ALGORITMU. DOTAZY $y \in A$, $y \in L(M, t)$ ZREJME MOŽNO ROZHODNÚŤ V POL. PRIESTORE.

NAKONIEC UKÁŽME, ŽE $A \in P(S')$.

VSTUP x, ORÁKULUM S'
$t := \lambda$;
V CYKLE VYKONAJ:
AK $\langle 0^{|x|}, t0 \rangle \in S'$, POTOM $t := t0$,
RESP. AK $\langle 0^{|x|}, t1 \rangle \in S'$, POTOM $t := t1$.
V OPAČNOM PRÍPADE UKONČI CYKLUS.
KONIEC CYKLU
PRIJMI $\Leftrightarrow$ $x \in L(M, t)$. INAK ODMIETNI.

NA KONCI CYKLU PLATÍ, ŽE PRE
KAŽDÉ y, $|y|=n$: $y \in A \Leftrightarrow y \in L(M,t)$.
TAKŽE ŠPECIÁLNE PRE x DOSTÁVAME, ŽE
ALGORITMUS KOREKTNE ROZHODNE, ČI $x \in A$.
TO, ŽE ALGORITMUS PRACUJE V POL. ČASE
JE ZREJMÉ.

MÁME TEDA RIEDKU $S' \in PSPACE$ T.Ž.
$A \in PSPACE \cap P(S') \setminus P$.

ĽAHKO NAHLIADNUŤ, ŽE $S' \notin P$.
TOTIŽ $S' \in P \Rightarrow P(S') = P \Rightarrow A \in P$, ČO JE SPOR.

NAŠLI SME RIEDKU $S' \in PSPACE \setminus P$,
ČO BOLO TREBA DOKÁZAŤ. $\square$

19.04.2010 M.
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

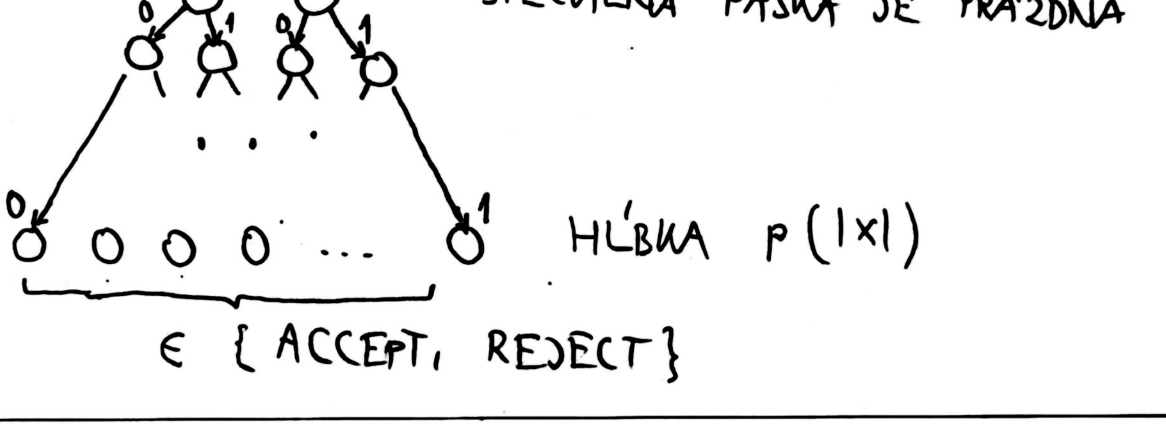
(4) a) PRE JAZYK $A \in PP$ SKONŠTRUUJTE PRAVDEPOD. TURINGOV STROJ PRIJÍMAJÚCI A V POL. ČASE T.Z. PRE ŽIADNE VSTUPNÉ SLOVO α NEEXISTUJE PRESNE POLOVICA PRIJÍMAJÚCICH VÝPOČTOV

b) UKÁŽTE, ŽE V DEFINÍCII PP MOŽNO POUŽIŤ ĽUBOVOĽNÉ ČÍSLO V INTERVALE $(0,1)$.

a) NECH M JE PRAVDEPODOBNOSTNÝ TS PRACUJÚCI V POLYNOMIÁLNOM ČASE p DOKAZUJÚCI $A \in PP$. MÔŽME PREDPOKLADAŤ, ŽE M V KAŽDOM KROKU ZAPÍŠE NA ZVLÁŠTNU PÁSKU 0, RESP. 1 PODĽA TOHO AKÚ ZVOLIL NASLEDUJÚCU KONFIGURÁCIU (VŽDY MÁ NA VÝBER 2 MOŽNOSTI)

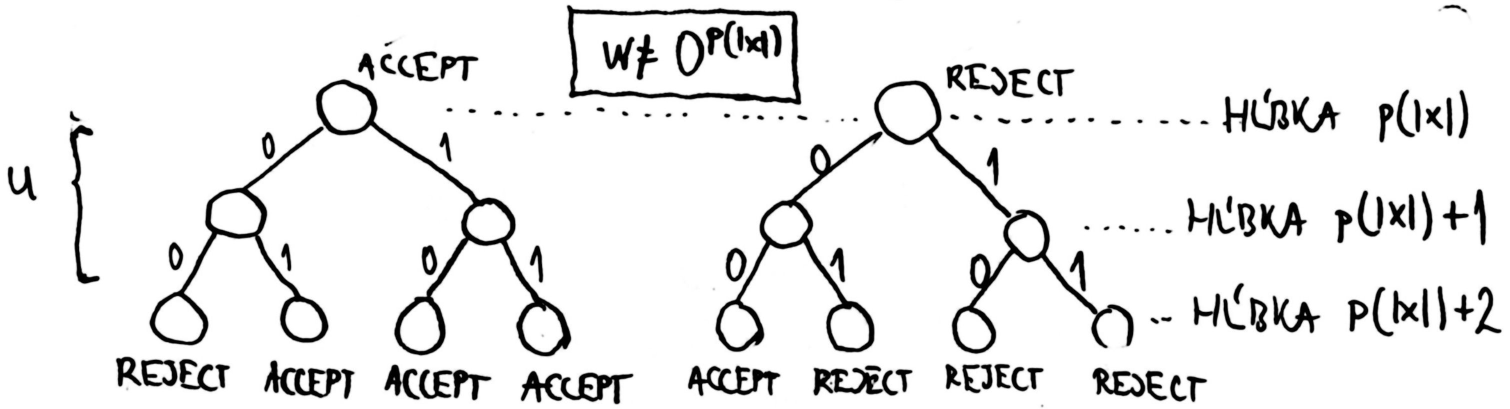
PO POSLEDNOM KROKU JE NA TEJTO PÁSKE SLOVO $w \in \{0,1\}^{p(|x|)}$ POPISUJÚCE CESTU VÝPOČTU, A M SA NACHÁDZA BUĎ V STAVE ACCEPT, ALEBO V STAVE REJECT.

STROM VÝPOČTU M NAD SLOVOM x MÔŽME ZNÁZORNIŤ NASLEDOVNE:



ZOSTROJÍME DTS M', KTORÝ PRACUJE PRESNE AKO M AŽ DO HĹBKY $p(|x|)$, PRIČOM V HĹBKE $p(|x|)$ EŠTE VYKONÁ 2 KROKY, TJ. NA ŠPECIÁLNU PÁSKU ZAPÍŠE EŠTE ĎALŠIE 2 BITY, TJ. SLOVO $u \in \{0,1\}^2$.

NAKONIEC SKONČÍ V STAVE ACCEPT / REJECT PODĽA NASLEDUJÚCEHO PRAVIDLA:

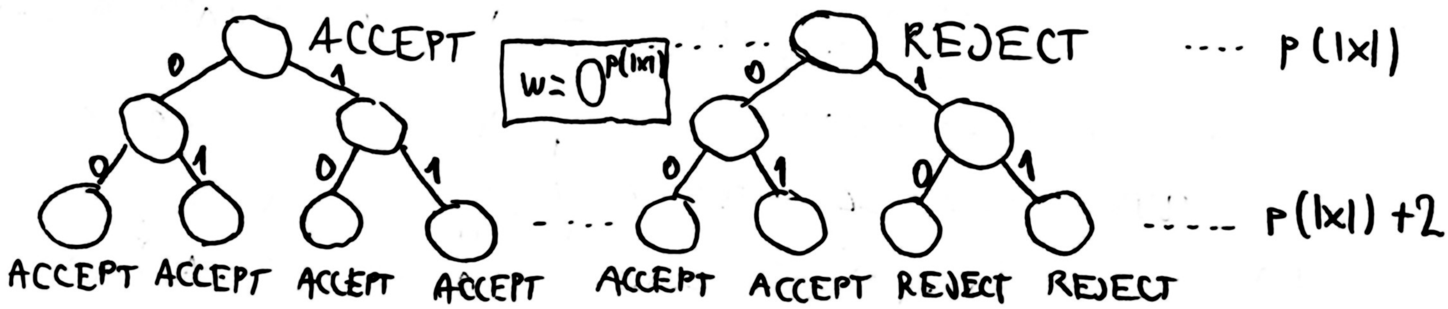


AK JE NA ŠPECIÁLNEJ PÁSKE $w \neq 0^{p(|x|)}$ A M JE V STAVE ACCEPT, TAK M' V HĹBKE $p(|x|)+2$ SKONČÍ V STAVE ACCEPT $\Leftrightarrow$ $u > 00$

A V STAVE REJECT $\Leftrightarrow$ $u = 00$

PODOBNE PRE REJECT ... VIĎ OBRÁZOK VYŠŠIE.

AK JE NA ŠPECIÁLNEJ PÁSKE PRÁVE SLOVO $0^{p(|x|)}$, TAK SA ZACHOVAJ NASLEDOVNE:



19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

NECH PRE DANÝ VSTUP x JE V HĹBKE $p(|x|)$ PRÁVE a VRCHOLOV V STAVE ACCEPT, T.J. $r = 2^{p(|x|)} - a$ VRCHOLOV V STAVE REJECT.

STROJ M' PRACUJE TAK, ŽE Z KAŽDÉHO VRCHOLU V STAVE ACCEPT V HĹBKE $p(|x|)$ UROBÍ 3 VRCHOLY V STAVE ACCEPT A JEDEN V STAVE REJECT V HĹBKE $p(|x|)+2$. PODOBNE PRE REJECT VRCHOL V HĹBKE $p(|x|)$. JEDINÚ VÝNIMKU TVORÍ NAJĽAVEJŠIA VETVA, KDE JE V OBOCH PRÍPADOCH O 1 ACCEPT VRCHOL VIAC A TÝM PÁDOM O 1 REJECT VRCHOL MENEJ (V HĹBKE $p(|x|)+2$).

$\Rightarrow$ V HĹBKE $p(|x|)+2$ MÁME:

$$a' = 3a + (2^{p(|x|)} - a) + 1 = 2^{p(|x|)} + 2a + 1$$

PRIJÍMAJÚCICH VRCHOLOV, A:

$$r' = 3(2^{p(|x|)} - a) + a - 1 = 3 \cdot 2^{p(|x|)} - 2a - 1$$

ODMIETAJÚCICH VRCHOLOV.

ABY SME DOKÁZALI, ŽE M' PRIJÍMA TEN ISTÝ JAZYK AKO M STAČÍ UKÁZAŤ, ŽE

$$a \geq r \iff a' \geq r'.$$

$\Rightarrow$) $\quad a \geq 2^{p(|x|)} - a \Rightarrow$

$4a \geq 2 \cdot 2^{p(|x|)} \Rightarrow$

$2a + 2^{p(|x|)} \geq 3 \cdot 2^{p(|x|)} - 2a \Rightarrow$

$2a + 2^{p(|x|)} + 1 \geq 3 \cdot 2^{p(|x|)} - 2a - 1$, D.

$a' \geq r'$

$\Leftarrow$) $\quad a' \geq r'$, D.

$2a + 2^{p(|x|)} + 1 \geq 3 \cdot 2^{p(|x|} - 2a - 1 \Rightarrow$

$4a \geq 2 \cdot 2^{p(|x|)} - 2 \Rightarrow$

$2a \geq 2^{p(|x|)} - 1 \Rightarrow$ (KEĎŽE $a \in \mathbb{N}$)

$2a \geq 2^{p(|x|)} \Rightarrow$

$a \geq 2^{p(|x|)} - a \Rightarrow$

$a \geq r$.

NAKONIEC SI VŠIMNIME, ŽE NIKDY NEMÔŽE NASTAŤ $a' = r'$.

TOTIŽ $a' = r' \Rightarrow$

$2a + 2^{p(|x|)} + 1 = 3 \cdot 2^{p(|x|)} - 2a - 1 \Rightarrow$

$2a = 2^{p(|x|)} - 1$, ČO JE SPOR.

(PREDPOKLADÁME, ŽE $p(|x|) \geq 1$). $\square$

(tady předpokládáte, že M přijímá $\iff a \geq r$!)

19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

b) POVIEME, ŽE PRAVDEPODOBNOSTNÝ TS. M PRIJÍMA JAZYK L S POMEROM $r \in (0,1)$, AK PLATÍ:

$x \in L \Leftrightarrow$ POČET PRIJÍMAJÚCICH STAVOV M PRI VÝPOČTE NAD x V HĹBKE $p(|x|)$ JE $\geq$ $r \times$ CELKOVÝ POČET STAVOV V HĹBKE $p(|x|) =$
$= r \cdot 2^{p(|x|)}$, KDE p JE ČASOVÁ ZLOŽITOSŤ M.

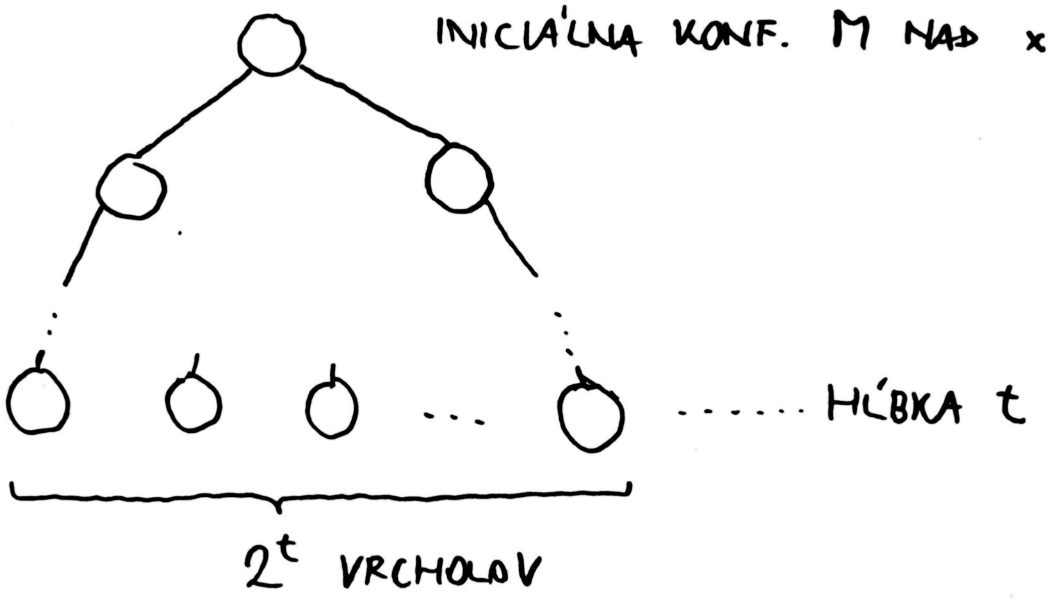
UKÁŽEME, ŽE ĽUBOVOĽNÝ DTS M S POMEROM $r = \frac{1}{2}$ JE MOŽNÉ TRANSFORMOVAŤ NA EKVIVALENTNÝ PRAV. TS. M' S ĽUBOVOĽNÝM POMEROM $r' \in (0,1)$, A NAOPAK, ZA PREDPOKLADU, ŽE BINÁRNY ZÁPIS r' MÁME K DISPOZÍCII AKO ORÁKULUM. NAVIAC: AK M PRACUJE V POL. ČASE, POTOM AJ M' BUDE PRACOVAŤ V POLYN. ČASE, A NAOPAK.

1) NAJSKÔR TRANSFORMÁCIA $r = \frac{1}{2} \to r' \in (0,1)$.

PREDPOKLADAJME, ŽE $r' < \frac{1}{2}$,
BINÁRNY ZÁPIS $r' = 0{,}r_1 r_2 r_3 \dots$,
$r_i \in \{0,1\}\ \forall i$, (ZREJME $r_1 = 0$) A
ČÍSLA $r_1 r_2 \dots$ MÁME K DISPOZÍCII AKO ORÁKULUM.

NAJSKÔR MYŠLIENKA KONŠTRUKCIE:

UVAŽUJME STROM VÝPOČTU M NAD x A OZNAČME $t = p(|x|)$.



KAŽDÝ VRCHOL V HĹBKE t SA NACHÁDZA V STAVE ACCEPT, ALEBO REJECT

OZNAČME a POČET LISTOV V STAVE ACCEPT A $n = 2^t - a$ POČET LISTOV V STAVE REJECT

STROJ M' BUDE AŽ DO HĹBKY t PRACOVAŤ PRESNE TAK ISTO AKO M. V HĹBKE t VYKONÁ EŠTE ĎALŠÍCH k KROKOV NAVYŠE,

PRIČOM SA RIADI PODĽA NASLEDUJÚCEHO PRAVIDLA:

i) AK BOL VRCHOL V HĹBKE t V STAVE REJECT, POTOM AJ KAŽDÝ LIST V HĹBKE $t+k$ POD TÝMTO VRCHOLOM BUDE V STAVE REJECT.

ii) AK BOL VRCHOL V HĹBKE t V STAVE ACCEPT, POTOM LIST V HĹBKE $t+k$ BUDE V STAVE ACCEPT $\Leftrightarrow$

$$u \leq 2 \cdot r_1 \cdots r_k + 1.$$

KDE $u \in \{0,1\}^k$ POPISUJE PRÍSL. CESTU K TOMUTO LISTU

19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

POČET VRCHOLOV V STAVE ACCEPT V HĹBKE $t+k$ JE POTOM $a' = a \cdot (2 \cdot r_1 \dots r_k + 1 + 1) =$
$= a \cdot 2 \cdot (r_1 \dots r_k + 1)$, Z CELKOVÉHO POČTU 2^{t+k} VRCHOLOV.

NAJSKÔR SI VŠIMNIME, ŽE:

$$\frac{a}{2^t} \geq \frac{1}{2} \Rightarrow \frac{a'}{2^{t+k}} = \frac{a \cdot 2 \cdot (r_1 \dots r_k + 1)}{2^{t+k}} \geq$$

$$\geq \frac{1}{2} \cdot \frac{2 \cdot (r_1 \dots r_k + 1)}{2^k} = \frac{r_1 \dots r_k + 1}{2^k} > r' = 0{,}r_1 r_2 \dots$$

NA DRUHEJ STRANE, AK $\frac{a}{2^t} < \frac{1}{2}$, TJ.
$a < 2^{t-1}$, TJ. $a \leq 2^{t-1} - 1$, POTOM

$$\frac{a'}{2^{t+k}} = \frac{a \cdot 2 \cdot (r_1 \dots r_k + 1)}{2^{t+k}} \leq \frac{(2^{t-1} - 1) \cdot 2 \cdot (r_1 \dots r_k + 1)}{2^{t+k}} =$$

$$= \frac{2^t r_1 \dots r_k + 2 \cdot ((2^{t-1} - 1) - r_1 \dots r_k)}{2^{t+k}}$$

TRIK SPOČÍVA V TOM, ZVOLIŤ k TAKÝM SPÔSOBOM, ABY $(2^{t-1} - 1) - r_1 \dots r_k < 0$.

POTOM BY $\frac{a'}{2^{t+k}} < \frac{2^t \cdot r_1 \dots r_k}{2^{t+k}} \leq r' = 0{,}r_1 r_2 \dots$.

$2^{t-1} - 1$ MÁ BINÁRNY ZÁPIS: $\underbrace{11 \dots 1}_{(t-1)\times}$.

ZVOĽME $k > t$ A ZAPÍŠME V BIN. ZÁPISE POD SEBA TIETO ČÍSLA:

$$\begin{array}{ccccccc} r_1 & \dots & r_{k-t+1} & r_{k-t+2} & \dots & r_{k-1} & r_k \\ 0 & \dots & 0 & \underbrace{1 \quad \dots \quad 1 \quad 1}_{t-1} \end{array}$$

VIDÍME, ŽE STAČÍ ZVOLIŤ $k > n$ TAKÝM SPÔSOBOM, ABY $r_{k-t+1} = 1$.

NECH $\ell \geq 1$ JE PRVÉ ČÍSLO TAKÉ, ŽE $r_\ell = 1$.
POTOM DEFINUJME $k := t + \ell - 1$, TJ. $k = p(|x|) + \ell - 1$.
PODĽA VYŠŠIE UVEDENÉHO PLATÍ:

$$\frac{a}{2^t} \geq \frac{1}{2} \Rightarrow \frac{a'}{2^{t+k}} > r'$$

$$\frac{a}{2^t} < \frac{1}{2} \Rightarrow \frac{a'}{2^{t+k}} < r'$$

VIDÍME, ŽE M' S POMEROM r' PRIJÍMA TEN ISTÝ JAZYK AKO M S POMEROM $r = \frac{1}{2}$.

NAVIAC, AK M PRACOVAL V POLYN. ČASE $p(|x|)$, POTOM M' PRACUJE V POL. ČASE $2p(|x|) + \ell$.

PREDPOKLADAJME, ŽE $r' > \frac{1}{2}$.
OPÄŤ MAJME PRAVDEPODOBNOSTNÝ TS. M PRIJÍMAJÚCI L S POMEROM $r = \frac{1}{2}$.

19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

POMOCOU KONŠTRUKCIE V BODE a) VYTVORÍME PRAVD. TS. M' PRIJÍMAJÚCI L S POMEROM $\frac{1}{2}$ T.Ž.

$$x \in L \Rightarrow \frac{a}{2^{p(|x|)}} > \frac{1}{2}, \qquad x \notin L \Rightarrow \frac{a}{2^{p(|x|)}} < \frac{1}{2},$$

(T.J. TAKÝ, ŽE NIKDY NENASTANE $\frac{a}{2^{p(|x|)}} = \frac{1}{2}$)

KDE a OZNAČUJE POČET LISTOV V PRIJÍMAJÚCOM STAVE V STROME VÝPOČTU M NAD SLOVOM x.

PREHODENÍM STAVOV DOSTANEME PRAVD. TS M'' PRIJÍMAJÚCI $\overline{L}$ S POMEROM $\frac{1}{2}$ S TOU ISTOU VLASTNOSŤOU AKO M', T.J. PRE KAŽDÝ VSTUP x JE POČET PRIJÍMAJÚCICH STAVOV VŽDY RÔZNY OD POČTU ODMIETAJÚCICH STAVOV.

POMOCOU KONŠTRUKCIE V BODE b) ZOSTROJÍME Z M'' PRAVD. TS. M''' PRIJÍMAJÚCI $\overline{L}$ S POMEROM $r''' := 1 - r' < \frac{1}{2}$.

KEĎ SA POZRIEME NA DÔKAZ BODU b), ĽAHKO NAHLIADNEME, ŽE PLATÍ:

$$\boxed{\begin{array}{l} \frac{a}{2^t} > \frac{1}{2} \Rightarrow \frac{a'}{2^{t+k}} > r' \\ \frac{a}{2^t} < \frac{1}{2} \Rightarrow \frac{a'}{2^{t+k}} < r' \\ \text{... VIĎ PÔVODNÉ ZNAČENIE} \end{array}}$$

TO VŠAK ZNAMENÁ, ŽE PRE KAŽDÝ VSTUP x

JE $\frac{a'''}{a'''+n'''} \neq r'''$, KDE a''', RESP. n'''

ZNAČÍ POČET PRIJÍMAJÚCICH, RESP. ODMIETAJÚCICH LISTOV V STROME VÝPOČTU M''' NAD x.

OPÄŤ PREHODENÍM STAVOV V LISTOCH M''' DOSTANEME PRAVD. TS. M'''' PRIJÍMAJÚCI L S POMEROM $r'''' = 1 - r''' = r'$.

TOTIŽ PREHODENÍM STAVOV DOSTANEME PRE DANÝ VSTUP x :

$a'''' = n'''$, $n'''' = a'''$, TAKŽE :

$$\frac{a''''}{a''''+n''''} = \frac{n'''}{a'''+n'''} = 1 - \frac{a'''}{a'''+n'''}$$

D. $x \in L \Rightarrow \frac{a'''}{a'''+n'''} < r''' \Rightarrow \frac{a''''}{a''''+n''''} > 1 - r''' = r''''$

$x \notin L \Rightarrow \frac{a'''}{a'''+n'''} > r''' \Rightarrow \frac{a''''}{a''''+n''''} < 1 - r''' = r''''$

VŠETKY ÚPRAVY ZACHOVÁVAJÚ POL. ČASOVÚ ZLOŽITOSŤ, TAKŽE AK M PRACOVAL V POL. ČASE, BUDE AJ M'''' PRACOVAŤ V POL. ČASE.

19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

2) $r \in (0,1) \to r' = \frac{1}{2}$

MÁME PRAVD. TS. M ROZPOZNÁVAJÚCI L S POMEROM r S ČASOVOU ZLOŽITOSŤOU p. CHCEME ZOSTROJIŤ PRAVD. TS. M' ROZPOZNÁVAJÚCI L S POMEROM $\frac{1}{2}$.

NAJSKÔR PREDPOKLADAJME, ŽE $r > \frac{1}{2}$.

NECH $0{,}r_1 r_2 r_3 \ldots$ JE BINÁRNY ZÁPIS r, KTORÝ MÁME K DISPOZÍCII AKO ORÁKULUM. PREDPOKLADAJME, ŽE V POSTUPNOSTI $r_1 r_2 r_3 \ldots$ SA NACHÁDZA NEKONEČNE VEĽA 1. AK BY TOMU TAK NEBOLO, TJ. r BY BOLO TVARU $0{,}r_1 r_2 \ldots r_\ell 1 0 0 \ldots$, POTOM HO MÔŽEME NAHRADIŤ ZÁPISOM $0{,}r_1 r_2 \ldots r_\ell 0 1 1 1 \ldots$.

DEFINUJME $R_k = 0{,}r_1 r_2 \ldots r_k$. ZREJME $R_k < r \quad \forall k \geq 1$.

ĎALEJ DEFINUJME $\gamma_k := \frac{1}{2} \cdot \frac{1}{R_k}$, TJ. $\gamma_k \cdot R_k = \frac{1}{2}$.

ZREJME $R_k \geq \frac{1}{2} \quad \forall k \geq 1$, PRETOŽE $r > \frac{1}{2} \Rightarrow r_1 = 1$.

$\Rightarrow \frac{1}{R_k} \leq 2 \Rightarrow \gamma_k = \frac{1}{2} \cdot \frac{1}{R_k} \leq 1$.

NECH $\gamma_k = 0{,}s_1 s_2 s_3 \ldots$ JE BINÁRNY ZÁPIS OBSAHUJÚCI NEKONEČNE VEĽA 1.
($\gamma_k = 1$ MÔŽEME ZAPÍSAŤ AKO $0{,}111\ldots$)

DÁ SA UKÁZAŤ, ŽE PRE ĽUBOVOĽNÉ $m \geq 1$ VIEME SPOČÍTAŤ $s_1 \ldots s_m$ V POL. ČASE VZHĽADOM K m (KLASICKÝM ALGORITMOM DELENIA, POMOCOU ORÁKULA r).

POLOŽME $S_k^{(m)} = 0{,}s_1 \dots s_m$, KDE $\mathcal{S}_k = 0{,}s_1 s_2 s_3 \dots$

ZREJME $S_k^{(m)} \cdot R_k \le \frac{1}{2}$. PLATÍ DOKONCA, ŽE:

$$\mathcal{S}_k \cdot R_k - S_k^{(m)} \cdot R_k \le 2^{-m} \cdot R_k < 2^{-m},$$ TAKŽE

$$\frac{1}{2} - 2^{-m} < S_k^{(m)} \cdot R_k \le \frac{1}{2}.$$

AK $S_k^{(m)} \cdot R_k < \frac{1}{2}$, POTOM POLOŽME $\tilde{S}_k^{(m)} := S_k^{(m)}$

AK $S_k^{(m)} \cdot R_k = \frac{1}{2}$, POTOM POLOŽME $\tilde{S}_k^{(m)} := S_k^{(m)} - 2^{-m}$.

ĽAHKO NAHLIADNUŤ, ŽE VŽDY:

$$\frac{1}{2} - 2^{-m} \le \tilde{S}_k^{(m)} \cdot R_k < \frac{1}{2}$$

K DANÉMU k CHCEME NÁJSŤ m TAKÉ, ŽE $\tilde{S}_k^{(m)} \ge 2^{k-m}$. UVAŽUJME IBA $m \ge k > 1$.

NECH $1 \le l_1 < l_2$ SÚ PRVÉ DVA INDEXY T.Ž. $s_{l_1} = s_{l_2} = 1$.
URČITE EXISTUJÚ, PRETOŽE V BIN. ROZVOJI $\mathcal{S}_k = 0{,}s_1 s_2 \dots$ SA NACHÁDZA NEKONEČNE VEĽA 1.

POLOŽME $m := k + l_2$.

POTOM $\tilde{S}_k^{(m)} = \tilde{S}_k^{(k+l_2)} \ge S_k^{(k+l_2)} - 2^{-(k+l_2)}$

PRIČOM ISTOTNE $S_k^{(k+l_2)} \ge 2^{-l_1} + 2^{-l_2}$,

TAKŽE $\tilde{S}_k^{(m)} \ge 2^{-l_1} + 2^{-l_2} - 2^{-(k+l_2)} > 2^{-l_1} > 2^{k-m}$.

l_1 AJ l_2 MOŽNO OHRANIČIŤ ZHORA KONŠTANTOU L, KTORÁ ZÁVISÍ IBA NA r.
(AJ KEĎ l_1 A l_2 MÔŽU BYŤ RÔZNE PRE RÔZNE k.)

7/9

19.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

ROZHODNE NAPR. $\ell_1 \leq 2$.
AK BY TOMU TAK NEBOLO, EXISTOVALO BY
$k \geq 1$ T. Ž. $\varphi_k = 0{,}00\,s_3 s_4 \dots$
TO VŠAK NIE JE MOŽNÉ, PRETOŽE:
$\varphi_k \cdot R_k = \frac{1}{2}$ A $\varphi_k \cdot R_k < 2^{-2} \cdot R_k < 2^{-2} = \frac{1}{4}$,
ČO JE SPOR.

PODOBNE PRE ℓ_2:
VIEME, ŽE $r > \frac{1}{2}$. NECH $r \leq 1 - 2^{-\ell}$, PRE $\ell \geq 1$.
POTOM $\ell_2 \leq \ell + 1$:
AK BY $\ell_2 > \ell + 1$, POTOM BY EXISTOVALO $k \geq 1$ T. Ž.

$$\varphi_k = 0{,}10 \dots 00\, s_{\ell+2}\, s_{\ell+3} \dots, \quad \text{POPR.}$$
$$\varphi_k = 0{,}01 \dots 00\, s_{\ell+2}\, s_{\ell+3} \dots .$$

V OBOCH PRÍPADOCH JE $\varphi_k \leq 2^{-1} + 2^{-(\ell+1)}$,
$\varphi_k \cdot R_k = \frac{1}{2}$ A $\varphi_k \cdot R_k \leq \varphi_k \cdot r \leq$

$$\leq (2^{-1} + 2^{-(\ell+1)}) \cdot (1 - 2^{-\ell}) = 2^{-1} - 2^{-\ell-1} + 2^{-\ell-1} - 2^{-2\ell-1} =$$
$$= 2^{-1} - 2^{-2\ell-1} < \frac{1}{2}, \text{ ČO JE SPOR.}$$

TÝM SME UKÁZALI, ŽE ℓ_1 AJ ℓ_2 MOŽNO ZHORA OHRANIČIŤ KONŠTANTOU L, KTORÁ ZÁVISÍ IBA NA r.
VŠIMNITE SI, ŽE SME NEUKÁZALI, KTORÉ ℓ_1 A ℓ_2 SPĹŇA $s_{\ell_1} = 1$, $s_{\ell_2} = 1$, PRETOŽE TO MÔŽE ZÁVISIEŤ NA k.

TERAZ UŽ PREJDEME K SAMOTNEJ KONŠTRUKCII M'.

VSTUP x, ORÁKULUM $r = 0, r_1 r_2 \ldots$

POLOŽME $k := p(|x|)$ ... JE TO POČET KROKOV VÝPOČTU M NAD SLOVOM x.

SPOČÍTAJME $S_k^{(k+L)} = 0, s_1 s_2 \ldots s_{k+L}$.

NÁJDIME PRVÉ DVA INDEXY $1 \leq l_1 < l_2$ T.Ž. $s_{l_1} = s_{l_2} = 1$.

POLOŽME $m := k + l_2$. ZREJME $l_2 \leq L$, TAKŽE PLATÍ $S_k^{(m)} = 0, s_1 \ldots s_m$.

SPOČÍTAJME $\tilde{S}_k^{(m)} = 0, \tilde{s}_1 \ldots \tilde{s}_m$.

VIEME, ŽE:

$$\frac{1}{2} - 2^{-m} \leq \tilde{S}_k^{(m)} \cdot R_k < \frac{1}{2}$$

A NAVIAC $\tilde{S}_k^{(m)} \geq 2^{k-m} = 2^{-l_2}$

UVAŽUJME STROM VÝPOČTU M NAD SLOVOM x

OZNAČME a POČET LISTOV V PRIJÍMAJÚCOM STAVE.

AK $\frac{a}{2^k} \geq r$, TJ. AK M PRIJÍMA x,

POTOM $a \geq r_1 r_2 \ldots r_k, r_{k+1} r_{k+2} \ldots$, TJ.

$$a \geq r_1 r_2 \ldots r_k + 1,$$

(PRETOŽE BINÁRNY ROZVOJ r OBSAHUJE NEKONEČNE VEĽA 1.)

19.04.2010 $\mathcal{M}_0$
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

V OPAČNOM PRÍPADE JE

$$a \leq r_1 r_2 \dots r_k$$

STROM VÝPOČTU PREDĹŽIME EŠTE O m KROKOV, PRIČOM SA ZACHOVÁME PODĽA NASL. PRAVIDLA:

i) AK BOL VRCHOL V HĹBKE k V ODMIETAJÚCOM STAVE, TAK AJ VŠETKY LISTY POD TÝMTO VRCHOLOM V HĹBKE $k+m$ BUDÚ V ODMIET. STAVE.

ii) AK BOL VRCHOL V HĹBKE k V PRIJÍMAJÚCOM STAVE, TAK LIST POD TÝMTO VRCHOLOM V HĹBKE $k+m$ JE PRIJÍMAJÚCI $\Leftrightarrow$

$$u < \tilde{s}_1 \dots \tilde{s}_m, \quad \text{KDE} \quad \tilde{S}_k^{(m)} = 0, \tilde{s}_1 \dots \tilde{s}_m,$$

KDE $u \in \{0,1\}^m$ POPISUJE CESTU K TOMUTO LISTU.

$\Rightarrow$ POČET PRIJÍMAJÚCICH LISTOV V HĹBKE $k+m$ JE:

$$a' = a \cdot (\tilde{s}_1 \dots \tilde{s}_m).$$

AK $\frac{a}{2^k} \geq r$, TJ. AK $a \geq r_1 \dots r_k + 1$, POTOM

$$\frac{a'}{2^{k+m}} = \frac{a \cdot (\tilde{s}_1 \dots \tilde{s}_m)}{2^{k+m}} \geq \frac{(r_1 \dots r_k + 1)}{2^k} \cdot \frac{(\tilde{s}_1 \dots \tilde{s}_m)}{2^m} =$$

$$= (R_k + 2^{-k}) \cdot \tilde{S}_k^{(m)} = \tilde{S}_k^{(m)} \cdot R_k + 2^{-k} \cdot \tilde{S}_k^{(m)} \geq$$

$$\geq \frac{1}{2} - 2^{-m} + 2^{-k} \tilde{S}_k^{(m)} \geq \frac{1}{2} - 2^{-m} + 2^{-k} \cdot 2^{k-m} = \frac{1}{2}.$$

AK $\frac{a}{2^k} < r$, TJ. $a \leq r_1 \cdots r_k$, POTOM

$$\frac{a'}{2^{k+m}} = \frac{a \cdot (\tilde{s}_1 \ldots \tilde{s}_m)}{2^{k+m}} \leq \frac{(r_1 \ldots r_k)}{2^k} \cdot \frac{(\tilde{s}_1 \ldots \tilde{s}_m)}{2^m} =$$

$$= R_k \cdot \tilde{S}_k^{(m)} < \frac{1}{2} .$$

TÝM SME DOKÁZALI, ŽE M' PRIJÍMA L S POMEROM $\frac{1}{2}$. AK NAVIAC M PRACUJE V POLYN. ČASE, POTOM AJ M' PRACUJE V POLYN. ČASE, PRETOŽE

$m = k + L = p(|x|) + L$, KDE L JE KONŠTANTA.

A VŠETKY KROKY MAJÚ POLYN. ČASOVÚ ZLOŽITOSŤ.

NAKONIEC ZOSTÁVA PRÍPAD :

$r \in (0,1) \longrightarrow r' = \frac{1}{2}$,

KDE $r < \frac{1}{2}$.

MAJME M PRAVD. TS. ROZPOZNÁVAJÚCI L S POMEROM r S ČASOVOU ZLOŽITOSŤOU p.

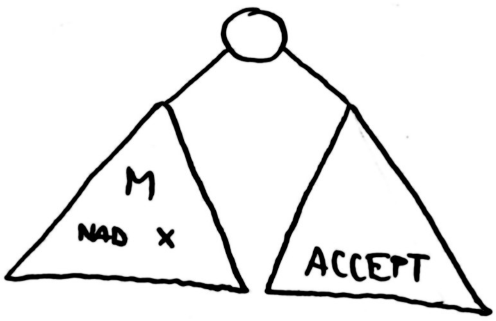
UVAŽUJME PRAVD. TS. M' PRACUJÚCI NASLEDOVNE

19.04.2010 Po
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

- VSTUP x
- S PRAVDEPODOBNOSŤOU $\frac{1}{2}$ PRIJMI
- INAK SIMULUJ M NAD SLOVOM x

STROM VÝPOČTU MÔŽME ZNÁZORNIŤ NASLEDOVNE:



VIDÍME, ŽE M' PRIJÍMA L S POMEROM $\frac{1}{2}r + \frac{1}{2} > \frac{1}{2}$
A S ČASOVOU ZLOŽITOSŤOU $p(|x|) + 1$.
NA M' MÔŽME APLIKOVAŤ PREDCHÁDZAJÚCI POSTUP A ZOSTROJIŤ TAK PRAVD. TS. M'' PRIJÍMAJÚCI L S POMEROM $\frac{1}{2}$, PRIČOM POLYN. ČAS. ZLOŽITOSŤ ZREJME ZOSTANE ZACHOVANÁ. □

26.04.2010 Mo
PETER ČERNO

asi lepší $|y| = p(|x|)$!

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(5) DOKÁŽTE, ŽE $A \in PP \iff \exists\, Q \in P$ A POLYNÓM p T. Ž. $x \in A \iff \exists$ VIAC NEŽ POLOVICA SLOV y TAKÝCH, ŽE $|y| \leq p(|x|)$ A $\langle x, y \rangle \in Q$. *

$\Rightarrow$) NECH M JE PRAVD. TS. DOKAZUJÚCI $A \in PP$ PRACUJÚCI V POLYNOMIÁLNOM ČASE p.

UVAŽUJME NASLEDUJÚCI DTS N

VSTUP $\langle x, y \rangle$

i) AK $y = \lambda$, POTOM PRIJMI A SKONČI.

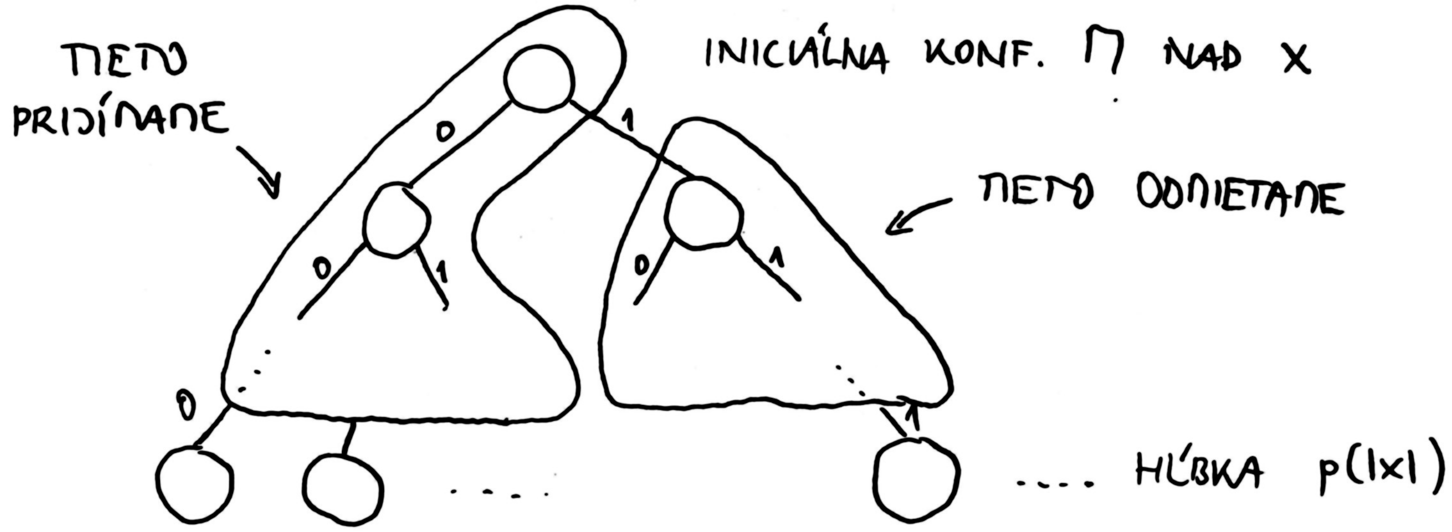
ii) INAK AK $|y| < p(|x|)$, POTOM PRIJMI $\iff$ PRVÝ BIT y JE 0 (V OPAČNOM PRÍPADE ODMIETNI)

iii) INAK AK $|y| = p(|x|)$, POTOM SIMULUJ PRÁCU M NA VSTUPE x PO VETVE y A PRIJMI $\iff$ M PRIJAL (V OPAČNOM PRÍPADE ODMIETNI)

ODMIETNI

UVAŽUJME VSTUP x A STROM VÝPOČTU M NAD TÝMTO SLOVOM x.

* PREDPOKLADÁME BINÁRNE KÓDOVANIE, TJ. $y \in \{0,1\}^*$



OZNAČME a POČET LISTOV V HĹBKE $p(|x|)$ V STAVE ACCEPT. CELKOVÝ POČET ICH JE $2^{p(|x|)}$.

KAŽDÉ $y \in \{0,1\}^{\leq p(|x|)}$ JEDNOZNAČNE POPISUJE VRCHOL V TOMTO STROME.

(NAPR. $y = \lambda$ POPISUJE KOREŇ, $y = 0$ JEHO ĽAVÉHO SYNA ..)

EXISTUJE $2^{p(|x|)+1} - 1$ RÔZNYCH REŤAZCOV $y \in \{0,1\}^{\leq p(|x|)}$.

SPOČÍTAJME, PRE KOĽKO Z NICH JE $\langle x,y \rangle \in L(N)$ ..

i) $y = \lambda$ 1

ii) $|y| < p(|x|)$ A PRVÝ BIT y JE 1 ... $2^{p(|x|)-1} - 1$

iii) $|y| = p(|x|)$ A PRÍSL. LIST JE ACCEPT ... a

SPOLU $1 + 2^{p(|x|)-1} - 1 + a = 2^{p(|x|)-1} + a$

ĽAHKO NAHLIADNUŤ, ŽE:

$x \in L(M) \Leftrightarrow a \geq 2^{p(|x|)-1} \Leftrightarrow$

$\Leftrightarrow 2^{p(|x|)-1} + a \geq 2^{p(|x|)} \Leftrightarrow 2^{p(|x|)-1} + a > \frac{1}{2}\left(2^{p(|x|)+1} - 1\right)$

26.04.2010 r.
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

POLOŽME $Q = L(N)$. DTS N ZREJME PRACUJE V POL. ČASE, TAKŽE $Q \in P$. NAVIAC, AKO SME PRÁVE UKÁZALI $x \in A = L(M) \iff \exists$ VIAC AKO POLOVICA $y \in \{0,1\}^{\leq p(|x|)}$ T.Ž. $\langle x, y \rangle \in Q$.

$\Leftarrow$) MAJME $Q \in P$ A POLYNÓM p T.Ž. $x \in A \iff \exists$ VIAC NEŽ POLOVICA $y \in \{0,1\}^{\leq p(|x|)}$ T.Ž. $\langle x, y \rangle \in Q$. DOKÁŽME, ŽE $A \in PP$.

UVAŽUJME NASLEDUJÚCI PRAVD. TS M:

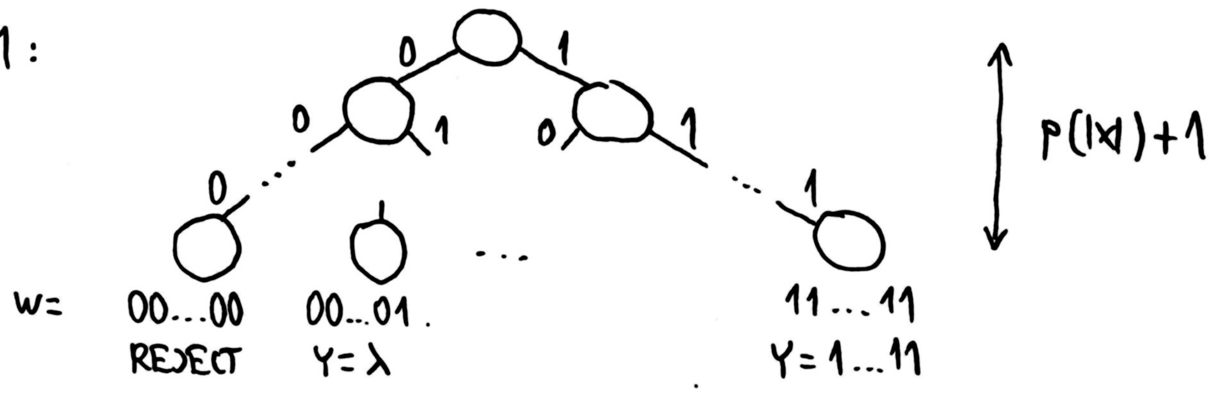
VSTUP x

VYKONAJ $p(|x|)+1$ NÁHODNÝCH KROKOV, A NECH $w \in \{0,1\}^{p(|x|)+1}$ POPISUJE PRÍSL. CESTU STROMOM VÝPOČTU

AK $w = 0^{p(|x|)+1}$, TAK ODMIETNI

INAK NECH w JE TVARU $w = 0^k 1 y$, $0 \leq k \leq p(|x|)$
PRIJMI $\iff \langle x, y \rangle \in Q$. INAK ODMIETNI.

M:



ĽAHKO NAHLIADNUŤ, ŽE KAŽDÝ LIST, PRE KTORÝ $w \neq 0^{p(|x|)+1}$, POPISUJE PRÁVE JEDNO $y \in \{0,1\}^{\leq p(|x|)}$ A NAOPAK.

NECH a OZNAČUJE POČET LISTOV V STAVE ACCEPT, TJ. a = POČET REŤAZCOV $y \in \{0,1\}^{\leq p(|x|)}$ T.Ž. $\langle x,y \rangle \in Q$.

POČET $\forall$ LISTOV JE $2^{p(|x|)+1}$

POČET $\forall$ REŤAZCOV $y \in \{0,1\}^{\leq p(|x|)+1}$ JE $2^{p(|x|)+1}-1$

VIDÍME, ŽE

$$a > \frac{1}{2}\left(2^{p(|x|)+1}-1\right) \iff a \geq 2^{p(|x|)} = \frac{1}{2}\,2^{p(|x|)+1}$$

TAKŽE $x \in L(M) \iff$ EXISTUJE VIAC AKO POLOVICA $y \in \{0,1\}^{\leq p(|x|)}$ T.Ž. $\langle x,y \rangle \in Q \iff x \in A$

TJ. $L(M) = A$, ČO BOLO TREBA DOKÁZAŤ.

TO, ŽE M PRACUJE V POL. ČASE JE ZREJMÉ. $\square$

26.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(6) DOKÁŽTE, ŽE #SAT JE SELF-REDUCIBILNÝ.

$\#SAT = \{ \langle i, F \rangle \mid$ F JE BOOLEOVSKÁ FORMULA T. Ž. F JE SPLNENÁ VIAC AKO i PRIRADENIAMI $\}$

i KÓDUJEME BINÁRNE, TAKŽE AK n JE POČET PREMENNÝCH V F, POTOM $\exists\ 2^n$ PRIRADENÍ. KEĎŽE $n \leq |F|$, MÔŽME PREDPOKLADAŤ, ŽE $|i| \leq |F|$.

FORMULE F KÓDUJEME TAKÝM SPÔSOBOM, ŽE PRE ĽUBOVOĽNÚ PREMENNÚ x FORMULE F SÚ OBE $F_{x:=0}$ AJ $F_{x:=1}$ KRATŠIE AKO F.

NASLEDUJÚCI ALGORITMUS DOKAZUJE SELF-RED. #SAT:

VSTUP $\langle i, F \rangle$, ORÁKULUM #SAT

AK F NEMÁ PREMENNÉ, POTOM VYHODNOŤ F
    AK $i = 0$ A F JE true, POTOM PRIJMI
    INAK ODMIETNI.

V OPAČNOM PRÍPADE NECH x JE PREMENNÁ F:

(i) AK $\langle i, F_{x:=0} \rangle \in \#SAT$, TAK PRIJMI;

(ii) AK $\langle i, F_{x:=1} \rangle \in \#SAT$, TAK PRIJMI;

(iii) POLOŽ $low := 0$, $high := i-1$

DOKEDY $low \leq high$ VYKONÁVAJ V CYKLE:

(iv) $j := \lfloor (low + high) / 2 \rfloor$

(v) AK $\langle j, F_{x:=0} \rangle \in \#SAT$ AJ
$\langle i-j-1, F_{x:=1} \rangle \in \#SAT$, POTOM PRIJMI

(vi) V OPAČNOM PRÍPADE:

a) AK $\langle j, F_{x:=0} \rangle \in \#SAT$, POTOM
POLOŽ $low := j+1$ A SKOČ NA ZAČ. CYKLU

b) AK $\langle i-j-1, F_{x:=1} \rangle \in \#SAT$, POTOM
POLOŽ $high := j-1$ A SKOČ NA ZAČ. CYKLU

c) AK NENASTALA ANI JEDNA Z TÝCHTO MOŽNOSTÍ, ODMIETNI

KONIEC CYKLU

PRIJMI $\Leftrightarrow$ ~~low ≤ i ∧~~ $\langle i-low, F_{x:=1} \rangle \in \#SAT$.

ALGORITMUS PRACUJE V POL. ČASE, PRETOŽE KAŽDÝ KROK MÁ POLYN. ČASOVÚ ZLOŽITOSŤ A VNÚTORNÝ CYKLUS REALIZUJÚCI BINÁRNE VYHĽADÁVANIE SA VYKONÁ NAJVIAC $\lceil \log_2(i+1) \rceil$ KRÁT, - ČO JE POLYNOMIÁLNE VEĽA VZHĽADOM K DĹŽKE $|i|$, TJ. AJ VZHĽADOM K DĹŽKE VSTUPU.

TAKTIEŽ VŠETKY DOTAZY NA ORÁKULUM #SAT SÚ KRATŠIE AKO VSTUP $\langle i, F \rangle$.

KOREKTNOSŤ ALGORITMU:

1) AK F NEMÁ ŽIADNE PREMENNÉ, POTOM SA ALGORITMUS ZREJME ZACHOVÁ KOREKTNE.

lze to udělat jednodušeji
for $j = 1, 2, \ldots, i-1$ do
if $\langle j, F_{x:=0} \rangle \in \#SAT$ a $\langle i-j, F_{x:=1} \rangle \in \#SAT$
then přijmi endif
end for
odmítni

26.04.2010 Mo
PETER ČERNO

EXAM: ŠTRUKTURÁLNÍ SLOŽITOST I

2) PREDPOKLADAJME, ŽE x JE PREMENNÁ F A F MÁ PRÁVE a SPLŇUJÚCICH OHODNOTENÍ.

ZREJME $\langle i, F \rangle \in \#SAT \Leftrightarrow a > i$

NECH a_b OZNAČUJE POČET SPLŇUJÚCICH OHODNOTENÍ FORMULE $F_{x:=b}$, KDE $b \in \{0, 1\}$.

ZREJME $a = a_0 + a_1$.

AK $a_b = 0$ PRE NEJAKÉ $b \in \{0,1\}$, TAK $a = a_{1-b}$, ČO OŠETRÍME V KROKOCH (i) A (ii)

ALGORITMUS TEDA VSTUPUJE DO KROKU (iii) S HYPOTÉZOU, ŽE $a_0 > 0$ AJ $a_1 > 0$.

VŽDY NA ZAČIATKU CYKLU, TJ. PRED KROKOM (iv) PLATÍ INVARIANT, ŽE: $\boxed{low \le a_0 \le high + 1}$

INVARIANT JE PLATNÝ PRI PRVOM PRIECHODE, KEĎ JE $low = 0$ A $high = i-1$, PRETOŽE

$$\langle i, F_{x:=0} \rangle \notin \#SAT \Rightarrow a_0 \le i = high + 1$$
$$\langle i, F_{x:=1} \rangle \notin \#SAT \Rightarrow a_1 \le i$$

AK PLATÍ PODMIENKA V KROKU (v), POTOM:

$$\langle j, F_{x:=0} \rangle \in \#SAT \Rightarrow a_0 \ge j+1$$
$$\langle i-j-1, F_{x:=1} \rangle \in \#SAT \Rightarrow a_1 \ge i-j-1+1$$

proč tam přidával 1?

$$\Rightarrow a = a_0 + a_1 \ge i+1 > i \Rightarrow \langle i, F \rangle \in \#SAT$$

TAKŽE ALG. SA ZACHOVÁ KOREKTNE

PREDPOKLADAJME, ŽE PODMIENKA V KROKU (v) NIE JE SPLNENÁ, TJ. VSTUPUJEME DO KROKU (vi).

AK a) $\langle j, F_{x:=0}\rangle \in \#SAT$, TJ. $\langle i-j-1, F_{x:=1}\rangle \notin \#SAT$,

POTOM NUTNE $a_0 > j$, TAKŽE KEĎ POLOŽÍME $low := j+1$, ZOSTANE INVARIANT V PLATNOSTI.

AK b) $\langle i-j-1, F_{x:=1}\rangle \in \#SAT$, TJ. $\langle j, F_{x:=0}\rangle \notin \#SAT$,

POTOM $a_0 \leq j$, TAKŽE KEĎ POLOŽÍME $high := j-1$, OPÄŤ INVARIANT ZOSTANE V PLATNOSTI.

AK c) $\langle j, F_{x:=0}\rangle \notin \#SAT$, ANI $\langle i-j-1, F_{x:=1}\rangle \notin \#SAT$,

POTOM $a_0 \leq j$, $a_1 \leq i-j-1 \Rightarrow a = a_0 + a_1 \leq i-1 < i$,

TJ. ALG. SA ZACHOVÁ KOREKTNE.

POSLEDNÝ PRÍPAD, KTORÝ TREBA OŠETRIŤ JE, KEĎ DÔJDE K PORUŠENIU PODMIENKY $low \leq high$,

TJ. $high = low - 1$, $\Rightarrow$ Z INVARIANTU $low \leq a_0 \leq high + 1$ DOSTÁVAME, ŽE $a_0 = low = high + 1$.

ZREJME $a > i \Leftrightarrow low + a_1 > i \Leftrightarrow a_1 > i - low \Leftrightarrow \langle i - low, F_{x:=1}\rangle \in \#SAT$,

TJ. ALGORITMUS SA ZACHOVÁ KOREKTNE.

JE ZREJMÉ, ŽE $i \geq low$, PRETOŽE NA ZAČIATKU JE $high = i-1$, A V PRIEBEHU VÝPOČTU MÔŽE high IBA KLESAŤ (A low STÚPAŤ)

$\Rightarrow low = high + 1 \leq i$. □

27.04.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

(7) UKÁŽTE, ŽE $NP \subseteq BPP \Rightarrow NP = R$.

NECH $NP \subseteq BPP$. POTOM $SAT \in BPP$.
PODĽA THEOREM 6.4, STRUCTURAL COMPLEXITY I
PRE KAŽDÝ POLYNÓM q EXISTUJE PRAVD. TS. M
PRACUJÚCI V POL. ČASE p T. Ž. M PRIJÍMA SAT
S PRAVDEPODOBNOSŤOU CHYBY $\leq \left(\frac{1}{2}\right)^{q(|F|)}$.

V ĎALŠOM BUDEME PREDPOKLADAŤ, ŽE FORMULE KÓDUJEME TAK, ABY PRE KAŽDÚ FORMULU F A JEJ PREMENNÚ x PLATILO:

$$|F_{x:=0}| = |F_{x:=1}| \doteq |F|.$$

UVAŽUJME NASLEDUJÚCI ALGORITMUS A:

VSTUP F

DOKEDY F OBSAHUJE PREMENNÚ OPAKUJ:
- NECH x JE PRVÁ PREMENNÁ F
- AK M PRIJÍMA $F_{x:=0}$, POTOM $F := F_{x:=0}$
- INAK AK M PRIJÍMA $F_{x:=1}$, POTOM $F := F_{x:=1}$
- INAK ODMIETNI

KONIEC CYKLU
VYHODNOŤ F
PRIJMI $\Leftrightarrow$ F SA VYHODNOTILO NA true
INAK ODMIETNI

ĽAHKO NAHLIADNUŤ, ŽE A POPISUJE PRAVDEP. TS. N PRACUJÚCI V POL. ČASE.
NAVIAC AK $F \notin SAT$, POTOM KAŽDÝ VÝPOČET N KONČÍ V STAVE REJECT, PRETOŽE F SA PO ŽIADNEJ SUBSTITÚCII NEVYHODNOTÍ NA true.

AK $F \in SAT$, POTOM A SIMULUJE PRÁCU M NAJVIAC $2 \times$(POČET PREMENNÝCH V F) $\leq 2 \cdot |F|$ KRÁT.
PRAVDEPODOBNOSŤ, ŽE SA ANI RAZ NEPOMÝLI JE ASPOŇ:

$$\left(1 - \left(\tfrac{1}{2}\right)^{q(|F|)}\right)^{2|F|} \geq 1 - 2|F| \cdot \frac{1}{2^{q(|F|)}}$$

T.J. AK ZVOLÍME NAPR. $q(n) := n+2$
DOSTANEME: $1 - 2n \cdot \frac{1}{2^{q(n)}} = 1 - 2n \frac{1}{2^{n+2}} = 1 - \frac{1}{2} \cdot \frac{n}{2^n} > \frac{1}{2}$

$\Rightarrow$ PRAVDEPODOBNOSŤ, ŽE N PRIJME F JE $> \frac{1}{2}$.

TÝM SME DOKÁZALI, ŽE $SAT \in R$.
V PRÍKLADE (8) UKÁŽEME, ŽE R JE UZAVRETÁ NA $\leq_m$, TAKŽE NUTNE $NP \subseteq R$.
INKLÚZIA $R \subseteq NP$ PLATÍ OBECNE.
CELKOVO TEDA DOSTÁVAME ROVNOSŤ: $NP = R$.

27.04.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNA ZLOŽITOSŤ I

(8) UKÁŽTE, ŽE ZPP, R, BPP SÚ UZAVRETÉ NA m-REDUKCIU. KTORÉ Z TÝCHTO TRIED SÚ UZAVRETÉ NA T-REDUKCIU, A PREČO?

NECH $A \in$ ZPP (RESP. R, BPP) A NECH $B \leq_m A$ PROSTREDNÍCTVOM f.

NECH M JE PRAVD. TS. PRACUJÚCI V POL. ČASE p DOKAZUJÚCI $A \in$ ZPP (RESP. R, BPP), A NECH M' JE DTS S VÝSTUPNOU PÁSKOU POČÍTAJÚCI f V POL. ČASE q.

UVAŽUJME PRAVDEPODOBN. TS., KTORÝ PRACUJE TAKTO: NA VSTUPE x DĹŽKY n SPOČÍTA $f(x)$, PRIČOM V KAŽDOM KROKU SA VÝPOČET ROZVETVÍ DO DVOCH IDENTICKÝCH VETIEV PO DOBU $q(n)$.

POTOM SIMULUJ M NA VÝSLEDKU $f(x)$. TÁTO SIMULÁCIA VYŽADUJE $p(q(n))$ KROKOV. CELKOVÝ ČAS JE $q(n) + p(q(n))$. ĽAHKO NAHLIADNUŤ, ŽE ZÁKLADNÉ CHARAKTERISTIKY TRIEDY ZPP (RESP. R, BPP) ZOSTANÚ ZACHOVANÉ, A ŽE TENTO STROJ PRIJÍMA PRÁVE B.

AK BY TRIEDA R BOLA UZAVRETÁ NA $\leq_T$,
POTOM BY BOLA UZAVRETÁ AJ NA DOPLNKY,
T.J. $\text{CO-}R = R$. TO JE VŠAK ZATIAĽ OTVORENÝ PROBLÉM, TAKŽE ANI UZAVRETOSŤ NA $\leq_T$ ZATIAĽ NIE JE DOKÁZANÁ, ANI VYVRÁTENÁ.

DOKÁŽEME, ŽE ZPP AJ BPP SÚ UZAVRETÉ NA $\leq_T$.
NECH $A \subseteq \Sigma^*$ A $\square \notin \Sigma$. DEFINUJME

$$A^{\square} := \{ w\square^k \mid k \geq 0 \ \& \ w \in A \}.$$

ZREJME AK $A \in ZPP$ (RESP. BPP),
POTOM AJ $A^{\square} \in ZPP$ (RESP. BPP).
SYMBOL $\square$ SLÚŽI AKO VYPCHÁVKA. (PADDING)
STAČÍ MODIFIKOVAŤ PRÍSL. PRAVD. TS. DOKAZUJÚCE $A \in ZPP$ (RESP. BPP) TAK, ŽE NAJSKÔR OVERIA, ČI JE VSTUP TVARU $w\square^k$, A POTOM PRACUJÚ UŽ IBA SO SLOVOM w.

PLATÍ VETA: NECH $A \in ZPP$ (RESP. BPP).
POTOM PRE KAŽDÝ POLYNÓM q EXISTUJE PRAVD. TS. DOKAZUJÚCI $A \in ZPP$ (RESP. $A \in BPP$) T.Ž. PRAVDEPODOBNOSŤ ODPOVEDE "NEVIEM" (RESP. PRAVD. CHYBY) JE $\leq \left(\frac{1}{2}\right)^{q(|x|)}$ NA VSTUPE x.

27.04.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

a) UZAVRETOSŤ ZPP NA $\leq_T$

MAJME $A \in ZPP$ A $B \in P(A)$. NECH DTS M PRACUJÚCI V POL. ČASE p S ORÁKULOM DOKAZUJE $B \leq_T A$. KAŽDÝ DOTAZ w TOHTO DTS M POLOŽENÝ ORÁKULU POČAS VÝPOČTU NAD x JE DLHÝ NAJVIAC $p(|x|)$.
ZMODIFIKUJME M TAKÝM SPÔSOBOM, ŽE KAŽDÝ DOTAZ w DOPLNÍ SYMBOLMI $\square$ TAK, ABY NOVÝ DOTAZ $w' = w\square^k$ BOL DLHÝ PRÁVE $p(|x|)$.
KEDŽE M POLOŽIL POČAS VÝPOČTU NAJVIAC $p(|x|)$ DOTAZOV, DOSTÁVAME NOVÝ DTS M' PRACUJÚCI V POL. ČASE r S ORÁKULOM T. Ž.

$$L(M, A) = L(M', A^{\square}),$$

PRIČOM M' POLOŽÍ POČAS VÝPOČTU NAD x NAJVIAC $p(|x|)$ DOTAZOV, VŠETKY ROVNAKEJ DĹŽKY $p(|x|)$.

$A \in ZPP \Rightarrow A^{\square} \in ZPP$, TJ. PRE KAŽDÝ POLYNÓM q EXISTUJE PRAVD. TS. N DOKAZUJÚCI $A^{\square} \in ZPP$ T. Ž. N ODPOVIE NA x "NEVIEM" S PRAVDEPODOBNOSŤOU $\leq \left(\frac{1}{2}\right)^{q(|x|)}$.

UVAŽUJME NASLEDUJÚCI ALGORITMUS $\mathcal{A}$:

VSTUP x

SIMULUJ PRÁCU M' NA VSTUPE x, PRIČOM VŽDY KEĎ M' POLOŽÍ DOTAZ w VYKONAJ:

SIMULUJ N NA VSTUPE w.

(i) AK JE ODPOVEĎ ACCEPT, RESP. REJECT, TAK POKRAČUJ VO VETVE YES, RESP. NO.

(ii) AK JE ODPOVEĎ "NEVIEM", TAK UKONČI VÝPOČET S ODPOVEĎOU "NEVIEM"

$\mathcal{A}$ ZREJME PRACUJE V POLYN. ČASE.

AK DÁ ODPOVEĎ ACCEPT / REJECT, TAK JE TÁTO ODPOVEĎ KONZISTENTNÁ S $L(M', A^{\square}) = L(M, A) = B$.

PRAVDEPODOBNOSŤ, ŽE N ODPOVIE NA DOTAZ w ACCEPT / REJECT JE ASPOŇ:

$$1 - \left(\frac{1}{2}\right)^{q(p(|x|))}, \quad \text{PRETOŽE } |w| = p(|x|).$$

$\Rightarrow$ PRAVDEPODOBNOSŤ, ŽE $\mathcal{A}$ ODPOVIE ACCEPT / REJECT JE ASPOŇ

$$\left(1 - \left(\frac{1}{2}\right)^{q(p(|x|))}\right)^{p(|x|)} \geq 1 - p(|x|) \cdot \frac{1}{2^{q(p(|x|))}}.$$

STAČÍ ZVOLIŤ $q(n) = n + 2$, A DOSTÁVAME, ŽE TÁTO PRAVDEPODOBNOSŤ JE $> \frac{1}{2}$.

27.04.2010 Tu
PETER ČERNO

EXAM: ŠTRUKTURÁLNI SLOŽITOST I

b) UZAVRETOSŤ BPP NA $\leq_T$.

DÔKAZ JE ANALOGICKÝ DÔKAZU a).
JEDINÝ ROZDIEL JE V TOM, ŽE N NEODPOVEDÁ "NEVIEM", ALE MÔŽE SA POMÝLIŤ.
PRAVDEP. CHYBY VIEME OHRANIČIŤ NA $\leq \left(\frac{1}{2}\right)^{q(|x|)}$.

PRÍSLUŠNÝ ALGORITMUS $\mathcal{A}'$ DOKAZUJÚCI $B \in BPP$ JE TAKÝ ISTÝ AKO $\mathcal{A}$ S TÝM ROZDIELOM, ŽE NEOBSAHUJE BOD (ii).

$\mathcal{A}'$ PRACUJE V POL. ČASE, AVŠAK MÔŽE DAŤ CHYBNÚ ODPOVEĎ, T.J. NEKONZISTENTNÚ S $L(M', A^{\square})$.

PODOBNOU ÚVAHOU AKO V a) SA DÁ UKÁZAŤ, ŽE PRAVDEPODOBNOSŤ CHYBY MÔŽME STIAHNUŤ POD $\frac{1}{2}$, ČÍM DOKÁŽEME, ŽE $B \in BPP$. $\square$

(9) UKÁŽTE, ŽE $P \neq R$ IMPLIKUJE $DEXT \neq EXPSPACE$.

MUŽIJEME VÝSLEDKU PRÍKLADU (2), TJ.

$DEXT \neq EXPSPACE \Leftrightarrow PSPACE \cap (P/poly) \neq P$

PLATÍ $P \subseteq R \subseteq PP \subseteq PSPACE$ (PROPOSITION 6.1)

$P \subseteq R \subseteq BPP \subseteq P/poly$ (COROLLARY 6.3)

VIĎ STRUCTURAL COMPLEXITY I.

$\Rightarrow \quad P \subseteq R \subseteq PSPACE \cap (P/poly)$.

$P \neq R \Rightarrow P \neq PSPACE \cap (P/poly) \Rightarrow$

$\Rightarrow$ $DEXT \neq EXPSPACE$, ČO BOLO TREBA DOKÁZAŤ. $\square$