Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Strukturální složitost II

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. Polynomiální izomorfismus, charakterizace polynomiálně izomorfních problémů se SAT
2. Imunní a biimunní množiny, jednoduché množiny, jádro problému
3. Relativizace tříd složitosti a jejich separace
4. Dolní a horní polynomiální hierarchie a vztah k ostatním třídám složitosti
5. Kolmogorovská polynomiální složitost
6. Důkazové systémy, rovnost IP=PSPACE, uzavřenost nedeterministických prostorových tříd na doplňky

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

22.03.2010 M_0
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

DOPÍSAT POZNÁMKY Z 15.03.2010

$L_i = \{A \in NP \mid \Sigma_i(A) \subseteq \Sigma_i\}$
$H_i := \{A \in NP \mid \Sigma_{i+1} \subseteq \Sigma_i(A)\}$

L JE LOW PRE T, KEĎ $T(L) = T(\emptyset)$.

VETA: RIEDKA MNOŽINA V NP PATRÍ DO L_2, JE TEDA Σ_2-LOW.

DÔKAZ $D \in \Sigma_2(S)$, S RIEDKA V NP

$\exists$ DET. TS. M_1 S ORÁKULOM PRACUJÚCI V POL. ČASE TAKÝ, ŽE $x \in D \Leftrightarrow \exists y \forall z \ \langle x,y,z\rangle \in L(M_1(S))$.

DĹŽKA $\langle x,y,z\rangle$ JE POLYNOMIÁLNE OHRANIČENÁ DĹŽKOU x. M_1 NAD $\langle x,y,z\rangle$ PRACUJE V POL. ČASE VZHĽADOM K x, A PRETO $\exists$ POLYNÓM r, KAŽDÝ DOTAZ POLOŽENÝ M_1 PRI VÝPOČTE NAD $\langle x,y,z\rangle$ MÁ DĹŽKU $\leq r(|x|)$.

$\Rightarrow$ S - ZAKÓDOVANÝ ZOZNAM VŠETKÝCH SLOV V S O DĹŽKE $\leq r(|x|)$ MÁ POLYNOMIÁLNU VEĽKOSŤ VZHĽADOM K x.

M_2 - VSTUP $\langle u, s\rangle$ - M_2 SIMULUJE M_1 NAD u A NAMIESTO DOTAZU $v \stackrel{?}{\in} S$ BUDE ZISŤOVAŤ $v \in s$.

$x \in D \Leftrightarrow \exists y \exists s \forall z \quad \langle x, y, z, s \rangle \in L(M_2)$
& s JE ZOZNAM VŠETKÝCH SLOV V S O DĹŽKE $\leq r(|x|)$.

M_2 PRACUJE V POL. ČASE.

MY VIEME, ŽE $S \in NP \Rightarrow \exists$ (~~NE~~)DETER. TS M_3 PRACUJÚCI V POL. ČASE A PLATÍ:
$u \in S \Leftrightarrow \exists v : \langle u, v \rangle \in L(M_3)$.

$\Rightarrow \quad x \in D \Leftrightarrow \exists y \exists s \exists t \forall z \quad \langle x, y, z, s \rangle \in L(M_2)$
& t JE ZOZNAM SLOV A OBSAHUJE ICH ROVNAKO VEĽA AKO s, PRE i-TE SLOVO s_i V s A i-TE SLOVO t_i V t PLATÍ $\langle s_i, t_i \rangle \in L(M_3)$ & KAŽDÉ SLOVO V S O DĹŽKE $\leq r(x)$ JE V s.

TERAZ SI STAČÍ UVEDOMIŤ, ŽE:
s OBSAHUJE VŠETKY SLOVÁ Z $S \Leftrightarrow$
$\forall w \forall v$ PLATÍ $(w$ JE V s ALEBO $\langle w, v \rangle \notin L(M_3))$

$x \in D \Leftrightarrow \exists y \exists s \exists t \forall z \forall w \forall v$ PLATÍ
$\langle x, y, z, s \rangle \in L(M_2)$ & { s A t SÚ ZOZNAMY ROVNAKEJ DĹŽKY A PRE i-TE SLOVO s_i A t_i PLATÍ $\langle s_i, t_i \rangle \in L(M_3)$ } &
$(w$ JE V s ALEBO $\langle w, v \rangle \notin L(M_2)$.

↳ POLYNOMIÁLNY PREDIKÁT

$\Rightarrow D \in \Sigma_2$. □

22.03.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

DŮSLEDOK 1: KEĎ EXISTUJE NP-ÚPLNÁ RIEDKA MNOŽINA VZHĽADOM K $\leq_m$, ALEBO $\leq_T$, ALEBO $\leq^{SN}$, POTOM PH KOLABUJE DO Σ_2.

H_0 - NP-ÚPLNÉ VZHĽADOM K $\leq_T$
H_1 - NP-ÚPLNÉ VZHĽADOM K $\leq^{SN}$
AK $L_i \cap H_i \neq \emptyset \Rightarrow$ PH KOLAPSUJE DO Σ_i
$H_0 \subseteq H_1 \subseteq H_2$. □

DŮSLEDOK 2: KEĎ NEXT $\neq$ DEXT,
POTOM $L_2 \neq P = L_0$.

VIĎ. POLYNOMIÁLNE OBVODY

VETA: KEĎ $A \in NP \cap P(S)$ PRE RIEDKU MNOŽINU S, POTOM $A \in L_3$.

PROBLÉM: S NEMUSÍME VEDIEŤ POPÍSAŤ

DÔKAZ. EXISTUJE DETER. TS. M_1 A M_2 PRACUJÚCE V POL-ČASE TAKÉ, ŽE

$x \in A \Leftrightarrow \exists y : \langle x, y \rangle \in L(M_1)$
$x \in A \Leftrightarrow x \in L(M_2(S))$

VEZMIME $D \in \Sigma_3(A)$

M_3 - TUR. STROJ - VSTUP $\langle u, s \rangle$ - M_3 SIMULUJE

M_2 NA u A NAMIESTO DOTAZU NA SLOVO v ZISŤUJE, ČI $v \in S$.

M_3 PRACUJE V POL. ČASE.

EXISTUJE DTS M_4 PRACUJÚCI V POL. ČASE A

$$x \in D \Leftrightarrow \exists y \forall z \exists t \quad \langle x, y, z, t \rangle \in L(M_4(A))$$

M_5 - VSTUP $\langle u, s \rangle$ - SIMULUJE M_4 NA u A KEĎ M_4 DÁ DOTAZ v, POTOM SIMULUJE M_3 NA $\langle v, s \rangle$ - ODPOVEĎ JE ÁNO, KEĎ M_3 PRIJME.

EXISTUJÚ POL. r A r_1, ŽE DOTAZY M_4 PRI VÝPOČTE NAD $\langle x, y, z, t \rangle$ MAJÚ DĹŽKU $\leq r_1(|x|)$ A VŠETKY DOTAZY POLOŽENÉ M_2 PRI PRÁCI NAD SLOVAMI O DĹŽKE $\leq r_1(|x|)$ MAJÚ DĹŽKU $\leq r(|x|)$.

$$x \in D \Leftrightarrow \exists y \exists s \forall z \exists t$$

$\langle x, y, z, t, s \rangle \in L(M_5)$ & s JE ZOZNAM VŠETKÝCH SLOV V S O DĹŽKE $\leq r(|x|)$.

CHCEME MUSIŤ:

$$w \in A \Leftrightarrow \langle w, s \rangle \in L(M_3)$$

$$w \in A \overset{\uparrow}{\Leftrightarrow} \exists v \ \langle w, v \rangle \in L(M_1) \overset{\uparrow}{\Leftrightarrow} \langle w, s \rangle \in L(M_3)$$

VIEME — CHCEME UKÁZAŤ

22.03.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

$$[(\forall v \ \langle w,v\rangle \notin L(M_1)) \vee (\langle w,s\rangle \in L(M_3))] \wedge$$
$$[(\langle w,s\rangle \notin L(M_3)) \vee (\exists q \ \langle w,q\rangle \in L(M_1))]$$

AK DOKÁŽEME TENTO VÝRAZ, POTOM BUDE PLATIŤ AJ EKVIV. $\langle w,v\rangle \in L(M_1) \Leftrightarrow \langle w,s\rangle \in L(M_3)$

TABUĽKA:	AK $w \in A$	AK $w \notin A$
$(\forall v \ \langle w,v\rangle \notin L(M_1))$	NEPLATÍ	PLATÍ
$(\langle w,s\rangle \in L(M_3))$	?	?
$(\langle w,s\rangle \notin L(M_3))$	?	?
$(\exists q \ \langle w,q\rangle \in L(M_1))$	PLATÍ	NEPLATÍ

→ ZLOŽENÝ VÝRAZ PLATÍ $\Leftrightarrow$ PLATÍ EKVIVALENCIA

$$w \in A \Leftrightarrow \langle w,s\rangle \in L(M_3).$$

$$x \in D \Leftrightarrow \exists y \exists s \forall z \forall w \forall v \exists t \exists q$$
$$\{(\langle x,y,z,t,s\rangle \in L(M_5)) \ \& \ (\langle w,v\rangle \notin L(M_1) \vee \langle w,s\rangle \in L(M_3)) \ \& \ (\langle w,q\rangle \in L(M_1) \vee \langle w,s\rangle \notin L(M_3))\}$$
$$\Rightarrow D \in \Sigma_3. \ \square$$

DÔSLEDOK: KEĎ EXISTUJE NP-ÚPLNÝ JAZYK A (VZHĽADOM K $\leq_m$, ALEBO $\leq_T$, ALEBO $\leq^{SN}$),

KTORÝ JE ROZPOZNATEĽNÝ POLYNOMIÁLNYMI OBVODMI, POTOM PH KOLAPSUJE DO Σ_3.

JAZYK A JE SELF-REDUCIBILNÝ $\Leftrightarrow$ EXISTUJE DTS T S ORÁKULOM PRACUJÚCI V POL. ČASE, KTORÝ NA VSTUPE DĹŽKY n DÁVA DOTAZY DĹŽKY $\leq n-1$ A $A = L(M(A))$.

PLATÍ: KEĎ M UKAZUJE, ŽE A JE SELF-REDUC. A $B = L(M(B)) \Rightarrow A = B$.

VETA: KEĎ $A \in \Sigma_h(S)$ PRE RIEDKU S A JE SELF-REDUCIBILNÁ, POTOM $\Sigma_2(A) \subseteq \Sigma_{h+2}$. (VIĎ NASLEDUJÚCA PREDNÁŠKA)

DÔSLEDKY: 1) POTOM $A \in \Sigma_{h+2} \cap \Pi_{h+2}$

2) $A \in NP$ JE SELF-RED. A $A \in P/POLY \Rightarrow A \in L_2$.

3) A JE NP-ÚPLNÁ, ROZPOZNATEĽNÁ POL. OBVODMI A SELF-REDUCIBILNÁ $\Rightarrow$ PH KOLAPSUJE DO Σ_2

29.03.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

VETA: A JE SELF-REDUCIBILNÁ, $A \in \Sigma_k(S)$ PRE RIEDKU MNOŽINU S, POTOM $\Sigma_2(A) \subseteq \Sigma_{k+2}$.

DÔKAZ: M_1 - TURINGOV STROJ UKAZUJÚCI, ŽE A JE SELF-REDUCIBILNÁ.

$A \in \Sigma_k(S) \Rightarrow$ EXISTUJE DTS M_2 S ORÁKULOM PRACUJÚCI V POL. ČASE A:

$$x \in A \Leftrightarrow \exists y_1 \forall y_2 \ldots : \langle x, y_1, \ldots, y_k \rangle \in L(M_2, S).$$

EXISTUJE POLYNÓM p_1:

$$|\langle x, y_1, \ldots, y_k \rangle| \leq p_1(|x|)$$

PRETO $\exists$ POLYNÓM p_2:

M_2 PRI VÝPOČTE NAD $\langle x, y_1, \ldots, y_k \rangle$ DÁVA DOTAZY DĹŽKY $\leq p_2(|x|)$.

TAKŽE $\exists s$ - ZAKÓDOVANIE VŠETKÝCH SLOV Z S O DĹŽKE $\leq p_2(|x|)$, TJ. EXISTUJE POLYNÓM p_3, $|s| \leq p_3(|x|)$, DTS M_3 - PRIJÍMA $\langle x, y \rangle$ - SIMULUJE M_2 NAD x A KEĎ M_2 DÁ DOTAZ v, TAK ZISTÍ, ČI $v \in y \ldots$ PRIJME $\Leftrightarrow$ M_2 PRIJME

M_3 PRACUJE V PÓL. ČASE. NECH:

$$B = \{ \langle x, s \rangle \mid \exists y_1 \forall y_2 \ldots : \langle x, y_1, \ldots, y_k, s \rangle \in L(M_3) \}$$

ZREJME $B \in \Sigma_k$.

VEDIE $D \in \Sigma_2(A)$.

$\exists$ DTS M_4 PRACUJÚCI V POL. ČASE TAKÝ, ŽE:

$x \in D \Leftrightarrow \exists z_1 \forall z_2 \langle x, z_1, z_2 \rangle \in L(M_4, A)$.

MÔŽEME PREPÍSAŤ NA:

$x \in D \Leftrightarrow \exists s \exists z_1 \forall z_2 \langle x, z_1, z_2, s \rangle \in L(M_5, A)$

& (s KÓDUJE VŠETKY SLOVÁ $\in S$ O DĹŽKE $\leq p_4(|x|)$.)

M_5 – PRIJÍMA SLOVÁ $\langle x, y \rangle$ – SIMULUJE M_4 NAD x KEĎ M_4 DÁ DOTAZ v, POTOM SIMULUJE $\langle v, y \rangle$ NA M_3.

p_4 POLYNÓM OHRANIČUJÚCI DĹŽKY SLOV, NA KTORÉ SA PÝTA M_2, KEĎ ROZHODUJE DOTAZ POLOŽENÝ M_4.

$x \in D \Leftrightarrow \exists s \exists z_1 \forall z_2 : \langle x, z_1, z_2 \rangle \in L(M_4, \{y \mid \langle y, s \rangle \in B\}) \wedge (\forall w : \langle w, s \rangle \in B \Leftrightarrow w \in A)$

ESTE SME NEVYUŽILI SELF-REDUCIBILITU A

$x \in D \Leftrightarrow \exists s \exists z_1 \forall z_2 \forall w : [\langle x, z_1, z_2 \rangle \in L(M_4, \{y, \langle y, s \rangle \in B\})] \wedge [\langle w, s \rangle \in B \Leftrightarrow w \in L(M_1, \{y, \langle y, s \rangle \in B\})]$

$\exists$: Σ_k ; $\Leftrightarrow$: Δ_{k+1}

□

DÔSLEDOK 1: A – SELF-REDUCIBILNÁ,

$A \in \Sigma_k(S) \Rightarrow A \in \Sigma_{k+2} \cap \Pi_{k+2}$

ATĎ... (VIĎ PREDCH. PREDNÁŠKA)

29.03.2010
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

VETA: $P=NP \Leftrightarrow \forall T$ TALLY : $P(T)=NP(T)$

DÔKAZ. $\Leftarrow$) ZREJMÉ, $\emptyset$ JE TALLY MNOŽINA.

$\Rightarrow$) VIEME, ŽE $P=NP \Rightarrow P(A)=NP_b(A)$ $\forall A$

$NP_b(A)$ - JAZYKY $L \in L(M,A)$, KDE M JE NTS PRACUJÚCI V POL. ČASE A EXISTUJE POLYNÓM p, $|\underbrace{Q(M,A,x)}| \leq p(|x|)$

MNOŽINA DOTAZOV KTORÉ POLOŽIL M PRI ORÁKULU A V NEJAKOM VÝPOČTE NAD x.

TAKŽE STAČÍ UKÁZAŤ, ŽE PRE TALLY MNOŽINU T PLATÍ $NP(T)=NP_b(T)$.

M - NTS PRACUJÚCI V POL. ČASE -

$L(M,T)=L(M_1,T)$, KDE M_1 - PRACUJE NAD x

ZAUJO: SIMULUJE M, A KEĎ M DÁVA DOTAZ v,

POTOM: a) KEĎ $v \notin 1^*$, ODPOVEĎ JE NIE

b) KEĎ $v \in 1^*$, SPÝTA SA.

POTOM $|Q(M_1,A,x)| \leq p(|x|)$, KDE p POL., KT. OHRANIČUJE DOBU VÝPOČTU M_1. $\square$

VETA (POZOR! V SKRIPTÁCH JE CHYBNE ZAPÍSANÁ)

NECH $\{M_i, i \in I\}$ JE SÚBOR DTS S ORÁKULOM TAKÉ, ŽE: (NEMUSÍ BYŤ ENUMEROVANÁ...)

a) $\forall i$ EXISTUJE POLYNÓM p TAKÝ, ŽE:
$\forall x \forall A$ PLATÍ $x \in L(M_i, A) \Leftrightarrow x \in L(M_i, A^{\leq p(|x|)})$.

b) $\forall i \exists j_i$ TAKÉ, ŽE $\forall$ KONEČNÚ MNOŽINU F,
KEĎ γ_F JE ZAKÓDOVANIE VŠETKÝCH SLOV V F, POTOM:
$x \in L(M_i, F) \Leftrightarrow \langle x, \gamma_F \rangle \in L(M_{j_i}, \emptyset)$

c) $\exists k \forall i \; L(M_i, \emptyset) \in \Sigma_k$.

POTOM PRE KAŽDÚ RIEDKU MNOŽINU S JE
$L(M_i, S) \in \Sigma_{\max\{k,2\}}(S)$, KDE k JE Z PODM. c).

DÔKAZ: MAJME $i \in I$ A RIEDKU MNOŽINU S,
$D = L(M_i, S)$. PODĽA a) EXISTUJE POLYNÓM p, ŽE
$x \in D \Leftrightarrow x \in L(M_i, S^{\leq p(|x|)})$.
PODĽA b) $\exists j_i \in I$ TAKÉ, ŽE $x \in L(M_i, F) \Leftrightarrow$
$\langle x, \gamma_F \rangle \in L(M_{j_i}, \emptyset)$, PRE KAŽDÚ KONEČNÚ F.
POLOŽME $B = L(M_{j_i}, \emptyset)$. PODĽA c) $B \in \Sigma_k$.
$N(S) = \{\langle \gamma, 0^n \rangle \mid \gamma$ JE ZAKÓDOVANIE VŠETKÝCH
SLOV V S O DĹŽKE $\leq n\}$.
$\langle \gamma, 0^n \rangle \in N(S) \Leftrightarrow \forall z: [(|z| \leq n \wedge z \in S) \Leftrightarrow z \in \gamma]$
$\Rightarrow N(S) \in \Pi_1(S)$
TERAZ IDE O TO, VHODNE PREFORMULOVAŤ
$x \in D \Leftrightarrow \exists \gamma \left(\langle x, \gamma \rangle \in B \;\&\; \langle \gamma, 0^{p(|x|)} \rangle \in N(S)\right)$

29.02.2010 Mo
PETER ČERNO

NTIN082 ŠTRUKTURÁLNÍ SLOŽITOST II

VIEME, ŽE $B \in \Sigma_k$, $N(S) \in \Pi_1(S)$
PRE $k \geq 2$ DOSTÁVAME VÝRAZ $\in \Sigma_2(S) =$
$= \Sigma_{\max\{k,2\}}(S)$.
PODOBNE PRE $k < 2$. □

VETA: NASLEDUJÚCE PODMIENKY SÚ EKVIVALENTNÉ:
a) POLYNOMIÁLNA HIERARCHIA KOLAPSUJE.
b) PRE KAŽDÚ RIEDKU MNOŽINU S, POLYNOMIÁLNA HIERARCHIA PRE S KOLAPSUJE.
c) EXISTUJE RIEDKA MNOŽINA S, ŽE POLYNOMIÁLNA HIERARCHIA PRE S KOLAPSUJE.

DÔKAZ: a) $\Rightarrow$ b)) $PH = \Sigma_k$, BÚNO $k \geq 2$
VEZMIME SÚBOR DTS $\{M_i \mid i \in I\}$ TAKÝCH, ŽE
PRE KAŽDÉ ORÁKULUM A JE:
$\{L(M_i, A) \mid i \in I\} = \Pi_k(A)$,
M_i DÁVA DOTAZY IBA POL. DĹŽKY VZHĽADOM K VSTUPU
A PLATÍ PODMIENKA b) Z PREDCH. VETY.

POTOM $\{M_i \mid i \in I\}$ SPĹŇA PODMIENKY a), b), c)
Z PREDCH. VETY PRE DANÉ k.
$\Rightarrow$ PRE KAŽDÚ RIEDKU MNOŽINU S PLATÍ
$\Pi_k(S) = \{L(M_i, S) \mid i \in I\} \subseteq \Sigma_k(S) \Rightarrow$
POL. HIERARCHIA PRE S KOLAPSUJE.

b) $\Rightarrow$ c)) PLATÍ TRIVIÁLNE

c) $\Rightarrow$ a)) MÁME RIEDKU MNOŽINU S TAKÚ, ŽE $PH(S) = \Sigma_k(S)$. $\exists$ SELF-REDUCIBILNÝ Σ_{k+1}-ÚPLNÝ JAZYK A. POTOM

$A \in \Sigma_{k+1} \subseteq \Sigma_{k+1}(S) = \Sigma_k(S)$.

$\Rightarrow \Sigma_2(A) \subseteq \Sigma_{k+2}$ (VIĎ PRVÁ VETA PREDNÁŠKY).

AVŠAK $\Sigma_2(A) = \Sigma_{k+3} \Rightarrow$ PH KOLAPSUJE. □

TAKTIEŽ NASLEDUJÚCE PODM. SÚ EKVIV.:

a) $PSPACE = PH$

b) $\forall$ RIEDKU S : $PSPACE(S) = PH(S)$

c) $\exists$ RIEDKA S : $PSPACE(S) = PH(S)$.

12.04.2010 M₀
PETER ČERNO

NTIN082 ŠTRUKTURÁLNI SLOŽITOST II

$A \subseteq \Sigma^*$, $B \subseteq \Gamma^*$, POLYNOMIÁLNY IZOMORFIZMUS Z A DO B JE BIJEKCIA $h: \Sigma^* \to \Gamma^*$ T. Ž.

a) h AJ h^{-1} SÚ POLYNOMIÁLNE SPOČÍTATEĽNÉ

b) PRE $x \in \Sigma^*$ PLATÍ $x \in A \Leftrightarrow h(x) \in B$

(1977 BERGMAN, HARTMANIS)

KEĎ EXISTUJE POLYNOMIÁLNY IZOMORFIZMUS Z A DO B, ČÍTAME $A \equiv B$.

ZOBRAZENIE $f: \Sigma^* \to \Gamma^*$ ZVÄČŠUJE DĹŽKY, KEĎ $|x| < |f(x)| \quad \forall x \in \Sigma^*$.

ZOBRAZENIE $f: \Sigma^* \to \Gamma^*$ JE 1-INVERTIBILNÉ, KEĎ JE PROSTÉ A f AJ f^{-1} (AKO PARCIÁLNE ZOBR.) SÚ POLYNOMIÁLNE.

VETA: KEĎ EXISTUJE 1-INVERTIBILNÁ, DĹŽKY ZVÄČŠUJÚCA REDUKCIA f Z A DO B, g Z B DO A, POTOM $A \equiv B$.

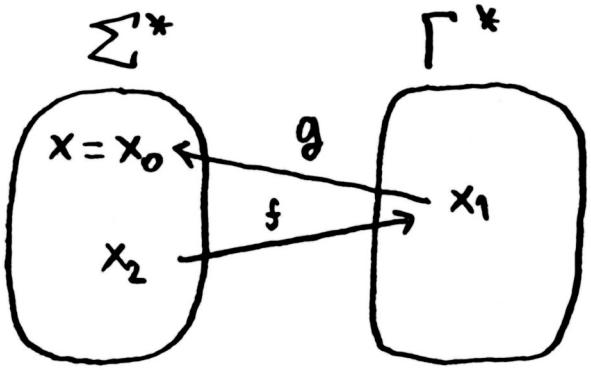
DÔKAZ. $x \in \Sigma^*$. POLOŽME $x = x_0$

KEĎ $g^{-1}(x_0) \neq \emptyset$, POTOM $x_1 = g^{-1}(x_0)$, INAK x_1 NIE JE DEFINOVANÉ

KEĎ $f^{-1}(x_1) \neq \emptyset$, POTOM $x_2 = f^{-1}(x_1)$, INAK x_2 NIE JE DEFINOVANÉ

ATĎ.

OBECNE: KEĎ $g^{-1}(x_{2i}) \neq 0$, POTOM $x_{2i+1} = g^{-1}(x_{2i})$, INAK x_{2i+1} NIE JE DEF. ATĎ.



PLATÍ: $|x| = |x_0| > |x_1| > |x_2| \ldots$

D. $\{x_i\}$ JE KONEČNÁ POSTUPNOSŤ.

R_1 = MNOŽINA $x \in \Sigma^*$ TAKÁ, ŽE POSLEDNÝ ČLEN POSTUPNOSTI PRE x JE PÁRNY

$R_2 = \Sigma^* \setminus R_1$ = —11— JE NEPÁRNY ...

PODOBNE PRE Γ^*, NECH $y \in \Gamma^*$, $y_0 = y$

KEĎ $f^{-1}(y_{2i}) \neq \emptyset$, POTOM $y_{2i+1} = f^{-1}(y_{2i})$, INAK y_{2i+1} NIE JE DEF.

KEĎ $g^{-1}(y_{2i+1}) \neq \emptyset$, POTOM $y_{2i+2} = g^{-1}(y_{2i+1})$, INAK y_{2i+2} NIE JE DEF.

S_1 = MNOŽINA $y \in \Gamma^*$ TAKÁ, ŽE POSTUPNOSŤ K PRVKU y KONČÍ V PÁRNOM ČLENE

$S_2 = \Gamma^* \setminus S_1$.

PLATÍ: $g(S_2) = R_1$, $f(R_2) = S_1$

MNOŽINY $S_1, S_2, R_1, R_2 \in P$.

$\exists$ NEKLESAJÚCI POLYNÓM p OHRANIČUJÚCI DOBU VÝPOČTU g^{-1} A f^{-1}.

12.04.2010 Po
PETER ČERNO

NTINO82 Štruktúrálni zložitosť II

$\Rightarrow$ pre x vypočítame prísl. postupnosť v čase $|x| \cdot p(|x|)$.

Definujme $h(x) = \begin{cases} g^{-1}(x), & \text{keď } x \in R_1 \\ f(x), & \text{keď } x \in R_2 \end{cases}$

$h : \Sigma^* \to \Gamma^*$.

Ukážme, že h je polynomiálny izomorfizmus:

1) $R_1 \cap R_2 = \emptyset$ ... h je korektne def.

2) $R_1 \cup R_2 = \Sigma^*$ ... h je totálne zobr.

3) h je prosté - g^{-1} aj f sú prosté, a keď $x \in R_1$, $x' \in R_2$, potom $h(x) \in S_2$, $h(x') \in S_1$ a $S_1 \cap S_2 = \emptyset$.

4) h je surjektívne - $y \in \Gamma^*$, potom $y \in S_1$ alebo $y \in S_2$.
keď $y \in S_1$, potom $x = f^{-1}(y)$ a $h(x) = y$
keď $y \in S_2$, potom $x = g(y)$ a $h(x) = y$

5) h je bijekcia

6) h aj h^{-1} sú polynomiálne spočítateľné
h ... zrejme
$h^{-1}(y) = \begin{cases} g(y), & \text{keď } y \in S_2 \\ f^{-1}(y), & \text{keď } y \in S_1 \end{cases}$

$\Rightarrow$ h^{-1} je pol. spočítateľné.

7) h JE REDUKCIA A NA B

$x \in \Sigma^*$, KEĎ $x \in R_2$, POTOM f JE REDUKCIA A NA B, A TEDA $x \in A \Leftrightarrow f(x) = h(x) \in B$

KEĎ $x \in R_1$, POTOM g JE REDUKCIA B NA A, A TEDA $h(x) \in B \Leftrightarrow g(h(x)) = h^{-1}(h(x)) = x \in A$.

$$\Sigma^* \times \Gamma^* = \{ \langle x, y \rangle \mid x \in \Sigma^*, y \in \Gamma^* \}$$

pad - JE PADDING FUNKCIE MNOŽINY $A \subseteq \Sigma^*$, KEĎ $pad : \Sigma^* \times \Sigma^* \to \Sigma^*$ A PLATÍ

$pad(x, y) \in A \Leftrightarrow x \in A$.

POTOM HOVORÍME, ŽE A JE PADDABLE MNOŽINA

A JE 1-INVERTIBLE PADDABLE MNOŽINA, KEĎ EXISTUJE 1-INVERTIBILNÁ PADDING FCIA. PRE A.

MNOŽINA JE p-CYLINDER (POLYNOMIÁLNY CYLINDER), KEĎ $A \equiv A \times \Sigma^*$. PROBLÉM: AKÁ JE ABECEDA $A \times \Sigma^*$?

$h : \Sigma^* \times \Sigma^* \to \Sigma^*$

↑ BIJEKCIA, h, h^{-1} POL. SPOČÍTATEĽNÁ, A

$x \in A \Leftrightarrow h(x, y) \in A \ \forall y$

KDE ZAVÁDZAME $|\langle x, y \rangle| = |x| + |y|$.

12.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

VĚTA: NÁSLEDUJÍCÍ PODMÍNKY NA $A \subseteq \Sigma^*$ JSOU EKVIVALENTNÍ:

a) A JE P-CYLINDER

b) $\exists B \subseteq \Gamma^*$ T.Ž. $A = B \times \Sigma^*$

c) $\exists$ 1-INVERTIBILNÍ PADDING FCE PRO A

d) KDYŽ $B \leq_m A$, POTOM $\exists$ 1-INVERTIBILNÍ DÉLKU ZVĚTŠUJÍCÍ REDUKCE f Z B NA A

e) EXISTUJE 1-INVERTIBILNÍ, DÉLKU ZVĚTŠUJÍCÍ PADDING FCE PRO A

DŮKAZ. a) $\Rightarrow$ b)) POLOŽÍME $B = A$

b) $\Rightarrow$ c)) NECHŤ $h : \Sigma^* \to \Sigma^* \times \Sigma^*$ JE POLYNOMIÁLNÍ IZOMORFISMUS Z A NA $B \times \Sigma^*$

PÍŠEME $h(x) = (h_1(x), h_2(x))$.

POTOM DEFINUJEME $pad(x,y) = h^{-1}(h_1(x), (h_2(x), y))$

PROTOŽE h JE POLYNOM. SPOČÍTATELNÁ, JE pad POLYNOM. SPOČÍTATELNÁ.

pad JE PROSTÁ: MÁJME $(x,y) \neq (x',y')$

a) KDYŽ $h_1(x) \neq h_1(x')$, POTOM $(h_1(x), (h_2(x), y)) \neq (h_1(x'), (h_2(x'), y'))$, A PROTOŽE h^{-1} JE BIJEKCE, TAK $pad(x,y) \neq pad(x',y')$.

b) PODOBNE KEĎ $h_1(x) = h_1(x')$, $h_2(x) \neq h_2(x')$, PLATÍ $pad(x,y) \neq pad(x',y')$

c) $h_1(x) = h_1(x')$ A $h_2(x) = h_2(x')$
PRETOŽE h JE PROSTÉ, TAK $x = x'$,
A PRETO $y \neq y'$, TAKŽE $pad(x,y) \neq pad(x',y')$.

ZOSTÁVA UKÁZAŤ, ŽE pad^{-1} JE POLYN. SPOČ.:

1) SPOČÍTANIE $h(z)$. KEĎ $\neg\exists v,t : h(z) = (v,t)$, ODMIETNEME ($pad^{-1}(z)$ NIE JE DEF.)
2) KEĎ $\neg\exists u,y : t = (u,y)$, ODMIETNEME
3) SPOČÍTANIE $h^{-1}(v,u) = x$ A VÝSLEDOK JE (x,y).

c $\Rightarrow$ d) NECH $B \leq_m A$ A f JE POLYNOMIÁLNE SPOČÍTATEĽNÁ REDUKCIA B NA A, (PREDP. $B \subseteq \Sigma^*$)
NECH pad JE 1-INVERTIBILNÁ PADDING FCIA. PRE A.
DEFINUJME $g(y) = pad\left((f(y), y\,10^{p(|y|)})\right)$,
KDE p JE NEKLESAJÚCI POLYNÓM OHRANIČUJÚCI DOBU VÝPOČTU pad^{-1}.

g JE POLYNOMIÁLNE SPOČÍTATEĽNÁ, PROSTÁ
g^{-1} JE —II—. (ZREJME)
g ZVÄČŠUJE DĹŽKU SLOV:

$$|u| \leq |\langle x,u\rangle| = |pad^{-1}(pad(x,u))| \leq p(pad(x,u)).$$

VEZMIME y, $x = f(y)$. $p(|y|) < |y\,10^{p(|y|)}| \leq$
$p(|pad(f(y), y\,10^{p(|y|)})|) = p(g(|y|)) \Rightarrow |y| < g(|y|)$.

19.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

NÁSLEDUJÚCE VLASTNOSTI SÚ EKVIVALENTNÉ:

a) A JE p-CYLINDER

b) KEĎ $B \in_m A$, POTOM EXISTUJE 1-INVERTIBILNÁ DĹŽKU ZVÄČŠUJÚCA REDUKCIA z B DO A

c) EXISTUJE 1 INVERTIBILNÁ PADDING FUNKCIA A

DÔSLEDOK 1: KEĎ $A \leq_m B \leq_m A$ A A AJ B SÚ p-CYLINDRE, POTOM $A \equiv B$.

DÔSLEDOK 2: KEĎ $A \equiv B$ A A JE p-CYLINDER, POTOM B JE TAKTIEŽ p-CYLINDER

pad - 1-INVERTIBILNÁ PADDING FCIA. A,
h POLYNOM. IZOMORFIZMUS z B DO A

$pad'(x,y) = h^{-1}(pad(h(x),y))$ ... 1-INVERTIBILNÁ PADDING FCIA. B.

LEMMA 3: SAT JE p-CYLINDER.

$pad(F, x) = F'$ - FORMULA, h - POČET PREM. V F

BOOL. FORMULA ↗ ↖ SLOVO

$$F' = F \wedge (x_{h+1} \vee \neg x_{h+1}) \wedge \left(\bigwedge_{j=1}^{|x|} z_{h+1+j} \right)$$

z_{h+1+j} - LITERÁL T. Z.

$z_{h+1+j} = x_{h+1+j}$ KEĎ j-TE PÍSMENO $y = 1$

$= \neg x_{h+1+j}$ KEĎ —11— $= 0$

F' JE SPOČÍTATEĽNÁ V POL. ČASE
pad JE PROSTÁ
pad^{-1} JE SPOČÍTATEĽNÁ V POL. ČASE

$F' \in SAT \Leftrightarrow F \in SAT$

$\Rightarrow$ pad JE 1-INVERTIBILNÁ PADDING FCIA. PRE SAT.

<u>DÔSLEDOK 4</u>: KEĎ A JE NP-ÚPLNÁ VZHĽADOM K $\leq_m$, POTOM JE POLYNOMIÁLNE IZOMORFNÁ SO SAT $\Leftrightarrow$ A JE P-CYLINDER.

$\Rightarrow$) Z DÔSLEDKU 2
$\Leftarrow$) Z DÔSLEDKU 1.

<u>BERMAN-HARTMANIS CONJECTURE</u>:
KEĎ $P \neq NP$, POTOM VŠETKY NP-ÚPLNÉ VZHĽADOM K $\leq_m$ SÚ POLYN. IZOMORFNÉ SO SAT.

<u>DÔSLEDOK 5</u>: RIEDKA MNOŽINA NIE JE P-CYLINDER.

SPOROM. S - RIEDKA, P-CYLINDER $\Rightarrow$
$\exists$ 1-INVERTIBILNÁ PADDING FCIA. pad,
$\exists$ POLYNÓM q OHRANIČUJÚCI DOBU VÝPOČTU pad,
$\exists$ POLYNÓM p OHRANIČUJÚCI $C_S(n)$

$x \in S$, $\quad pad(x \times \{0,1\}^n) \subseteq \{0,1\}^{\leq q(n)}$
$\quad pad(x \times \{0,1\}^n) \subseteq \{0,1\}^{\leq q(n)} \cap S$

19.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

$$|\{0,1\}^{\leq q(n)} \cap S| \leq p(q(n))$$

$$|x \times \{0,1\}^n| \geq 2^n$$

$\Rightarrow$ pad NEMÔŽE BYŤ PROSTÁ, A PRETO S NIE JE P-CYLINDER. □

ZOSILNENIE: KEĎ $C_S(n) \leq f(n)$ A $f(q(n)) = o(2^n)$ PRE V POLYNÓMY, POTOM S NIE JE P-CYLINDER.

F ... BOOL. FORMULA

$F \in SAT \Leftrightarrow F_{x:=0} \in SAT \vee F_{x:=1} \in SAT$

STROM REKURENCIE PRE VYHODNOTENIE F:
MÁME VRCHOL OZNAČENÝ F.

(1) KEĎ F NEMÁ PREMENNÚ, POTOM VYHODNOTÍME F A PRIJMEME $\Leftrightarrow$ VYHODNOTENIE JE true

(2) KEĎ F MÁ PREMENNÚ, POTOM VEZMEME PRVÚ PREMENNÚ x, ĽAVÉHO SYNA F OHODNOTÍME $F_{x:=0}$ A SKÚSIME VYHODNOTIŤ $F_{x:=0}$. KEĎ $F_{x:=0} \in SAT$, POTOM $F \in SAT$ A PRIJMEME, KONIEC.
INAK PRAVÉHO SYNA F OHODNOTÍME $F_{x:=1}$ A VYHODNOTÍME $F_{x:=1}$. F PRIJMEME $\Leftrightarrow$ $F_{x:=1}$ BOLO PRIJATÉ, KONIEC.

EXISTUJE POLYNÓM, KTORÝ OHRANIČUJE ČAS NA VYHODNOTENIE F, KEĎ DAN NEPOČÍTANIE REKURZIU

<u>VETA</u>: KEĎ co-SAT $\in_m S$ PRE RIEDKU MN. S, POTOM $P = NP$. OZNAČME f PRÍSL. REDUKCIU.

1) KEĎ F NEMÁ PREMENNÚ, POTOM JE LIST A F JE SPLNITEĽNÁ $\Leftrightarrow$ $F = true$.
2) KEĎ F MÁ PREMENNÚ A JEHO SYNOVIA NIE SÚ SPLNITEĽNÍ, POTOM F JE NESPLNITEĽNÁ
3) KEĎ F' NIE JE SPLNITEĽNÁ A $f(F) = f(F')$, POTOM F NIE JE SPLNITEĽNÁ.

ALGORITMUS NA VYHODNOTENIE BOOL. FORMULE:

VSTUP F ORÁKULUM S
$S := \emptyset$, Vyh(F)
KEĎ F NIE JE SPLNITEĽNÁ, ODMIETNEME
INAK PRIJMEME.

Vyh(F)
SPOČÍTAJ $f(F)$
KEĎ $f(F) \in S$, POTOM F NIE JE SPLNIT., KONIEC
KEĎ F NEMÁ PREMENNÚ, TAK SPOČÍTAME HODNOTU F

19.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

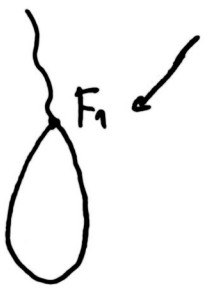
KEĎ HODNOTA F JE FALŠE, POTOM $f(F)$ PRIDÁME DO S, F NIE JE SPLNITEĽNÁ, KONIEC
V OPAČNOM PRÍPADE PRIJMEME F, KONIEC
KEĎ F MÁ PREMENNÉ, VEZMEME PRVÚ ... x
ZAVOLÁME $Vyh(F_{x:=0})$.
KEĎ VÝSLEDOK = PRIJAL F, POTOM PRIJMEME F, KON.
INAK KEĎ $f(F) \in S$, POTOM ODMIETNEME F, KONIEC
ZAVOLÁME $Vyh(F_{x:=1})$. KEĎ $F_{x:=1}$ BOLA ODMIETNUTÁ, PRIDÁME $f(F)$ DO S,
F NIE JE SPLNITEĽNÁ, D. ODMIETNEME F
INAK PRIJMEME F, KONIEC.

EXISTUJE POLYNÓM p T.Ž. $Vyh(F)$ BEZ REKURZÍVNEHO VOLANIA VŽDY ČAS $\leq p(|F|)$.

LEMMA: NECH F_1 A F_2 SÚ BOOLEOVSKÉ FORMULE, KTORÉ NEOHODNOCUJÚ LISTY V STROME REKURZÍVNEHO VOLANIA, A NECH $f(F_1) = f(F_2)$. POTOM F_1, F_2 LEŽIA NA NEJAKEJ CESTE Z KOREŇA DO LISTU.

DÔKAZ. NECH F_1 JE VOLANÁ SKÔR NEŽ F_2.
V TOMTO OKAMŽIKU $f(F_1) \notin S$.

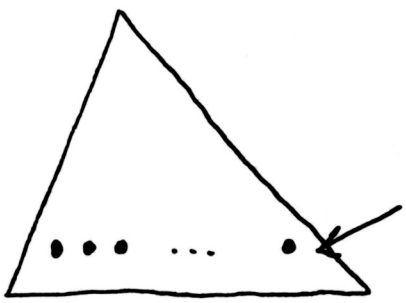
KEĎ SA VOLÁ F_2, POTOM $f(F_2) = f(F_1) \notin S$.



TU SA F_1 DOSTANE DO S

TO BY ALE ZNAMENALO, ŽE F_2 JE LIST ↯ □

POČET VRCHOLOV V STROME, KTORÍCH SYNOVIA SÚ LISTY, JE NAJVIAC $q(r(|F|))$, KDE q JE POLYNÓM OHRANICUJÚCI $C_S(n)$, r OHRANICUJE DĹŽKU VÝPOČTU f.



MAJÚ RÔZNU HODNOTU f

VÝSKA STROMU JE OHRANIČENÁ POČTOM PREM. V F.
$\Rightarrow$ POČET VN. VRCHOLOV JE POLYNOMIÁLNY VZHĽADOM K $|F|$.
$\Rightarrow$ ALGORITMUS POBEŽÍ V POL. ČASE $\Rightarrow$ $P = NP$. □

$A \leq_m^{P/\log} B \Leftrightarrow \exists f$ - FUNKCIA Z $\mathbb{N}$ DO Σ^* T.Ž.
$|f(n)| \leq c \log n$ PRE NEJAKÚ KONŠT. c, $\forall n$
$\exists$ POL. SPOČÍTATEĽNÁ g TAKÁ, ŽE
$x \in A \Leftrightarrow g(x, f(|x|)) \in B$.

19.04.2010 Mo
PETER ČERNO

NTINO82 STRUKTURÁLNI SLOŽITOSŤ II

VETA: KEĎ co-SAT $\leq_m^{P/\log} S$, S RIEDKA, POTOM $P = NP$.

NECH f, g DOKAZUJÚ co-SAT $\leq_m^{P/\log} S$,
$g_v(x) := g(x, f(|v|))$.

ALGORITMUS: F - BOOL. FORMULA
PRE KAŽDÉ SLOVO v, $|v| \leq c \cdot \log |F|$
POUŽIJEME PREDCHÁDZAJÚCI ALGORITMUS
S REDUKCIOU g_v.
AK PRIJME, POTOM PRIJMEME, KONIEC
AK PRE KAŽDÉ SLOVO v ODMIETNE, ODMIETNEME.

POZOR! PRI REKURZÍVNOM VOLANÍ SA NESMIE STRATIŤ VEĽKOSŤ, TJ. $|F_{x:=0}| = |F_{x:=1}| = |F|$.
KOREKTNOSŤ AJ ČAS. ZLOŽITOSŤ JE ZREJMÁ. □

VETA (ZIMNÝ SEMESTER):
KEĎ $S \leq_m^{P/\log} SAT$, POTOM co-$S \leq_m^{P/\log} SAT$.

26.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNI SLOŽITOST II

VETA: i) $co\text{-}SAT \leq_m S$, S RIEDKA $\Rightarrow P = NP$

ii) $co\text{-}SAT \leq_m^{P/log} S$, S RIEDKA $\Rightarrow P = NP$

iii) $S \leq_m^{P/log} SAT$, S RIEDKA $\Rightarrow co\text{-}S \leq_m^{P/log} SAT$

DÔKAZ. iii) $S \leq_m^{P/log} SAT \Rightarrow \exists f, g$:

$f : \mathbb{N} \to \Sigma^*$ T.Ž. $\exists$ KONŠT. $c > 0$: $|f(n)| \leq c \log n \ \forall n$

g POLYN. SPOČÍTATEĽNÁ T.Ž.:

$s \in S \iff g(s, f(|s|)) \in SAT$.

$\exists p$ POLYNÓM T.Ž. $|\{s \in S : |s| \leq n\}| \leq p(n) \ \forall n$

ALGORITMUS A

VSTUP $\langle x, \langle w, m \rangle \rangle$

OVERÍ, ŽE BIN. ČÍSLO URČENÉ m JE $\leq p(|x|)$,
$|w| \leq c \cdot \log(|x|)$

UHÁDNE NAVZÁJOM RÔZNE SLOVÁ:
$x_1, x_2, \ldots, x_m$ T.Ž. $|x| = |x_i|$ A
$x \neq x_i$ PRE $\forall i \in \{1, 2, \ldots, m\}$.

OVERÍ, ŽE $g((x_i, w)) \in SAT$ PRE $\forall i \in \{1, 2, \ldots, m\}$

KEĎ SÚ SPLNENÉ PODMIENKY, PRIJMI

INAK ODMIETNI.

L - JAZYK PRIJÍMANÝ A - PATRÍ DO NP.

$\Rightarrow \exists$ POLYN. SPOČÍTATEĽNÁ REDUKCIA g' z L NA SAT.

LEMMA: KEĎ $w = f(1^{|x|})$ A $m = |\{s \in S : |s| = |x|\}|$,
POTOM $\langle x, \langle w, m\rangle\rangle$ JE PRIDÍVANÉ $A \Leftrightarrow x \in co\text{-}S$.

$g'(1^{|x|}) := \langle f(x), |\{s \in S : |s| = |x|\}| \rangle \in \log$

PLATÍ: $x \in co\text{-}S \Leftrightarrow g'(x, f'(1^{|x|})) \in SAT$. □

DÔSLEDOK 1 (EORTUNE): KEĎ EXISTUJE
NP-ÚPLNÁ MNOŽINA A VZHĽADOM K $\leq_m$
A co-A JE RIEDKA, POTOM $P = NP$.

$SAT \leq_m A \Leftrightarrow co\text{-}SAT \leq_m co\text{-}A \Rightarrow P = NP$.

DÔSLEDOK 2 (BERMAN): KEĎ EXISTUJE NP-ÚPLNÁ
TALLY MNOŽINA T VZHĽADOM K $\leq_m$, POTOM $P = NP$.

DÔKAZ. $T \subseteq \{0\}^*$, $\overline{T} = \{0\}^* \setminus T$.
$SAT \leq_m T$ - f POLYN. REDUKCIA SAT NA T,
PRETOŽE T JE NP-ÚPLNÉ $\exists t \in \{0\}^* - T$.
ZMENÍME f - KEĎ $f(x) \in \{0\}^* \Rightarrow f'(x) := t$
INAK $f'(x) := f(x)$.
ZREJME f' - POL. SPOČ., $Im(f) \subseteq \{0\}^*$.
$x \in SAT \Leftrightarrow f(x) \in T \Leftrightarrow f'(x) \in T$.
$co\text{-}SAT \leq_m \overline{T} \Rightarrow SAT \leq_m co\text{-}\overline{T}$. □

NECH S JE RIEDKA, NP-ÚPLNÁ VZHĽADOM K $\leq_m$.
$\Rightarrow co\text{-}SAT \leq_m co\text{-}S \leq_m^{P/\log} SAT$

26.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

PRETOŽE $S \leq_m SAT \Rightarrow S \leq_m^{P/\log} SAT$.

ĎALEJ $SAT \leq_m S$.

DÁ SA UKÁZAŤ, ŽE TO IMPLIKUJE $co\text{-}SAT \leq S \Rightarrow$
$\Rightarrow P = NP$. □

PLATÍ: $A \in NP \Leftrightarrow \exists B \in P$ A $\exists$ POLYNÓM p
T.Z. $x \in A \Leftrightarrow \exists y,\ |y| = p(|x|),\ \langle x,y\rangle \in B$.

$$L(A,p) := \{\langle x,y\rangle \mid |y| = p(|x|),\ \langle x,y\rangle \in B\}$$

$$Left(A,p) := \{\langle x,y\rangle \mid |y| = p(|x|),$$
$$\exists y' : |y| = |y'|,\ y' \geq y \text{ V LEX. USP. A } \langle x,y'\rangle \in B\}$$

ZREJME AK $\langle x,y\rangle \in Left(A,p)$, $|\bar{y}| = |y|$
A $\bar{y} \leq y$, POTOM $\langle x,\bar{y}\rangle \in Left(A,p)$.

w^x_{max} — KEĎ $x \in A$, POTOM JE TO NAJVÄČŠIE SLOVO y DĹŽKY $p(|x|)$ T.Z. $\langle x,y\rangle \in B$
KEĎ $x \notin A$, POTOM NIE JE DEF.

$Left(A,p) \in NP$. (ZREJME)

NECH S JE RIEDKA, NP-ÚPLNÁ, p_S - POLYNÓM OHRANIČUJÚCI: $|\{s : |s| \leq n\}| \leq p_S(n)$.

$\exists f$ - POLYNOMIÁLNA REDUKCIA $Left(A,p)$ NA S,

P_f - POLYNÓM OHRANIČUJÚCI DOBU VÝPOČTU f,

$q = P_S \cdot P_f$ ... POČET f SA MÔŽE SPÝTAŤ NA NAJVIAC $q(|x|)$ SLOV.

DANÉ x - ALGORITMUS HĽADAJÚCI w^x_{max}

T_i - MNOŽINA NAJVÄČŠÍCH DISJUNKTNÝCH INTERVALOV VZHĽADOM K LEXIKOGRAF. USP. SLOV O DĹŽKE $P(|x|)$ T.Ž.

a) KEĎ w^x_{max} EXISTUJE, POČET JE V NEJAKOM INTERVALE

b) POČET INTERVALOV JE NAJVIAC $q(|x|)$

c) KAŽDÝ INTERVAL V T_i OBSAHUJE IBA $2^{P(|x|)-i}$ SLOV.

$T_0 = \langle 0^{P(|x|)}, 1^{P(|x|)} \rangle$

($\langle a, b \rangle$, KDE $|a| = |b|$ REPR. INTERVAL SLOV c: $|c| = |a|$ & $a \leq c \leq b$)

ZREJME T_0 SPĹŇA a), b) AJ c).

PRE $i = 0, 1, \ldots, p(|x|) - 1$ VYKONÁME:

(i) $T_{i+1} = \{ \langle a, \frac{a+b}{2} \rangle, \langle \frac{a+b}{2}, b \rangle \mid \langle a, b \rangle \in T_i \}$

AK $a < b$, POTOM $\frac{a+b}{2}$ JE SLOVO V STREDE MEDZI a A b.

26.04.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

ZREJME T_{i+1} SPĹŇA a) AŽ c).

(ii) KEĎ $\langle a,b\rangle, \langle c,d\rangle \in T_{i+1}$, $a < c$, $f(a) = f(c)$, POTOM ODSTRÁNIME $\langle a,b\rangle$ z T_{i+1}.

PODMIENKA a) ZOSTANE ZACHOVANÁ' ... AŽ c)

(iii) KEĎ T_{i+1} OBSAHUJE VIAC AKO q (1×1) INTERVALOV, TAK TAM NECHÁME IBA PRVÝCH NAJMENŠÍCH q(1×1) INTERVALOV.

⇒ PODMIENKA b) AŽ c) JE SPLNENÁ'

OTÁZKA JE, ČI PLATÍ PODMIENKA a) ...

NÁJDEME NAJVÄČŠÍ INTERVAL $\langle a,a\rangle \in T_{P(1\times1)}$ TAKÝ, ŽE $\langle x,a\rangle \in B$. AK EXISTUJE: POTOM $w^x_{max} = a$. INAK w^x_{max} NIE JE DEF.

OVERENIE, ŽE T_i SPĹŇAJÚ INVARIANT:

PLATÍ PRE T_0 ... ZREJME.

NECH PLATÍ PRE T_i. POTOM T_{i+1} PO KR. (i) OBSAHUJE DISJUNKTNÉ INTERVALY POKRÝVAJÚCE INTERVALY V T_i

⇒ PLATÍ a), A KEĎŽE SME INTERVALY POLILI, PLATÍ AJ c).

V KROKOCH (ii) A (iii) IBA MNECHÁVAME INTERVALY, TAKŽE SÚ STÁLE DISJ. A PLATÍ c)

PO KROKU (ii) PLATÍ a) A NAVIAC

KEĎ $\langle a,b\rangle$ A $\langle c,d\rangle$ SÚ V T_{i+1}, POTOM $f(a) \neq f(c)$. – PLYNIE Z KONŠTRUKCIE.

a) KEĎ w^x_{max} JE DEF. A $a \leq w^x_{max}$, POTOM $\langle x, a\rangle \in Left(A,p)$, ALE f JE REDUKCIA, A TEDA $\langle x, c\rangle \in Left(A,p)$, A TEDA $w^x_{max} \geq c$ – PRETO PO (ii) PLATÍ a).

PO KROKU (iii) PLATÍ AJ b) – PLYNIE Z KONŠTR.

ABY SME DOSTALI a), PREDPOKLADAJME, ŽE PO KROKU (iii) T_{i+1} OBSAHUJE $\langle a_j, b_j\rangle$, $j = 1,\dots,q(|x|)$ A w^x_{max} EXISTUJE (INAK JE a) SPLNENÉ TRIVIÁLNE)

NECH $w_{max} \in \langle a,b\rangle$, KDE $a > b_j$ $\forall j \in \{1,\dots,q(|x|)\}$

POTOM $\forall j$ $\langle x, a_j\rangle \in Left(A,p)$, $\langle x,a\rangle \in Left(A,p)$.

$\Rightarrow f(x,a_j) \in S$ $\forall j$ A $f(x,a) \in S$.

AVŠAK $f(x,a_j)$ $\forall j$, $f(x,a)$ SÚ NAVZÁJOM RÔZNE PRVKY O DĹŽKE $\leq p_f(|x|)$, ČO JE SPOR. ↯

c) PLYNIE Z TOHO, ŽE $T_{p(|x|)}$ OBSAHUJE IBA JEDNOPRVKOVÉ INTERVALY, A TEDA KOREKTNOSŤ PLYNIE Z a).

POLYN. ČAS: NÁJDENIE $\frac{a+b}{2}$ VYŽADUJE $O(p(|x|))$

(i) ... $O(q(|x|)\cdot p(|x|))$, $|T_{i+1}| \leq 2\,q(|x|)$

(ii) ... $O(q \cdot p_f)$

(iii) .... $O(q \cdot p_f)$. $\Rightarrow$ CELKOVO ... POL. ČAS. □

03.05.2010 Mo
PETER ČERNO

NTIN082 STRUKTÚRALNÁ SLOŽITOSŤ II

DÔSLEDOK: KEĎ EXISTUJE NP-ŤAŽKÁ RIEDKA MNOŽINA S VZHĽADOM K $\leq_m$, POTOM $P = NP$.

DÔKAZ. EXISTUJE POLYNOMIÁLNE SPOČÍTATEĽNÁ REDUKCIA f ZO SAT DO S. DEFINUJEME $S' = \{ f(x)10^{|x|}, x \in SAT \}$. ZREJME S' JE RIEDKA.

$g(x) := f(x)10^{|x|}$ .. REDUKCIA ZO SAT DO S'.

$S' \in NP$: **ALGORITMUS**:

- VSTUP y
- UHÁDNEME x
- OVERÍME, ŽE $g(x) = y$
- OVERÍME, ŽE $x \in SAT$
- PRIJMEME, AK PLATIA V PODMIENKY. □

MAJME U ... UNIVERZÁLNY TS. DEFINUJEME:

$K_U(x) := \min \{ |y| : U(y) = x \}$.

VLASTNOSŤ: $\exists c : K_U(x) \leq |x| + c \quad \forall x$

$\forall$ UNIVERZÁLNE U_1 A U_2 $\exists c : K_{U_2}(x) \leq K_{U_1}(x) + c$

$\forall m \leq n$ EXISTUJE NAJVIAC $2^{n-m+1} - 1$ SLOV DĹŽKY $\leq n$ TAKÝCH, ŽE MAJÚ KÓD $\leq n-m$.

$K(f, g)$ - MNOŽINA SLOV x, EXISTUJE SLOVO y, $|y| \leq f(|x|)$, $U(y) = x$, U POČÍTA V $g(|x|)$ KROKOCH.

PODOBNE $KS(f,g) = \dots$, U POUŽÍVA NAJVIAC $g(|x|)$ PAMÄTÍ.

$K(f,g,z)$ - MNOŽINA SLOV x, EXISTUJE SLOVO y, $|y| \leq f(|x|)$, $U(\langle y,z\rangle) = x$, U POČÍTA V $g(|x|)$ KROKOCH.

M - NEDETERM. TS. $x \in L(M)$, POTOM $Cte_M(x)$ - MNOŽINA KÓDOV PRIJÍMAJÚCICH VÝPOČTOV NAD x, KAŽDÝ KÓD OBSAHUJE x.

$Cte_M(x)$ ... CERTIFIKÁTY M PRE x.

VETA: $P = NP \Leftrightarrow \forall$ NTS M POČÍTAJÚCI V POL. ČASE $\exists$ KONŠTANTA c T.Ž. $\forall x \in L(M)$:
$Cte_M(x) \cap K(c \cdot \log n, n^c, x) \neq \emptyset$.

DÔKAZ: $\Rightarrow$: $P = NP$, f - FUNKCIA, KTORÁ CERTIFIKÁTU PRE x PRIRADÍ x, INAK NIE JE DEF.
f - JE POL. SPOČÍTATEĽNÁ A HONEST

PLATÍ: $P = NP \Leftrightarrow \forall$ POL. SPOČÍTATEĽNÚ HONEST FCIU. f EXISTUJE POL. SPOČÍTATEĽNÁ g T.Ž. KEĎ $g(x)$ JE DEF., POTOM $f(g(x)) = x$.
A $g(x)$ JE DEF. PRE $\forall x \in \mathrm{Im}\, f$.
↳ VEZMEME KÓD TS POČÍTAJÚCEHO g PRE TÚTO f.
POTOM KÓD $\in K(c \log n, n^c, x)$.

03.05.2010Mo
PETER ČERNO

NTIN082 STRUKTURÁLNI SLOŽITOST II

$\Leftarrow$) M - NTS POČÍTAJÚCI V POL. ČASE,
U UNIVERZÁLNY TS PRE K ...

VSTUP x
PRE KAŽDÉ SLOVO y, $|y| \leq c \cdot \log(|x|)$
SPOČÍTAJTE $U(x,y)$ A OVERÍTE VÝPOČTOM,
ČI $U(x,y)$ JE CERTIFIKÁT PRE M A x.
AK ÁNO, PRIJMITE.
AK SA TO NEPODARÍ PRE ŽIADNE y - ODMIETNITE.

$\Rightarrow$ POLYNOMIÁLNY DTS PRE L(M) $\Rightarrow$ P = NP. □

DEF.: S JE p-TLAČITEĽNÁ, KEĎ EXISTUJE POLYNÓM A $\forall n$ VIEME TLAČIŤ NN. $S^{\leq n}$ V ČASE p(n).
(S MUSÍ BYŤ NUTNE RIEDKA)

DEF: A JE MNOŽINA, POTOM RANKING FCIA NN. A JE FCIA. $r(x) = |\{y \in A \mid y \leq x\}|$
$\leq$ ... LEXIKOGRAF. USP.

LEMMA: KEĎ A MÁ POL. SPOČ. RANKING FCIU, POTOM JE POL. SPOČÍTATEĽNÁ FCIA. r^{-1} (VRACIAN K VÝSLEDKU)
KDE $r^{-1}(i) = \min\{x \mid r(x) = i\}$,
TJ. r^{-1} JE JEDINÉ SLOVO V A, ŽE VÝSLEDOK RANKING FCIE. NA NEHO JE i.

DÔKAZ: VSTUP k, NÁJDEME n, ŽE $r(1^{n-1}) < k \leq r(1^n)$. POTOM $r^{-1}(k)$ MÁ DĹŽKU n A NÁJDENIE n VYŽADUJE POL. ČAS VZHĽADOM K n.

KEĎ $r(0^n) = k$, POTOM $r^{-1}(k) = 0^n$, KONIEC.

INAK $d = 0^n$, $h = 1^n$, A OPAKUJEME DOKEDY $d+1 < h$:

- SPOČÍTAME $r\left(\frac{d+h}{2}\right)$, KEĎ $r\left(\frac{d+h}{2}\right) < h$,
- POTOM $d := \frac{d+h}{2}$, INAK $h := \frac{d+h}{2}$.

VÝSTUP $r^{-1}(k) = \begin{cases} d & \text{AK } r(d) = k \\ h & \text{AK } r(h) = k \end{cases}$.

ALGORITMUS VYŽADUJE POL. ČAS VZHĽADOM K n.

LEMA: S - RIEDKA MNOŽINA T. Ž. $S \in DTIME(T)$.
POTOM $\exists$ k - KONŠTANTA, ŽE

$$S \subseteq k(k \cdot \log n, k \cdot T(n) \cdot 2^n).$$

DÔKAZ. M - DTS ROZPOZNÁVAJÚCI S V ČASE $O(T)$.
PRE SLOVO $s \in S$ NECH i JE PORADOVÉ ČÍSLO s V $S^{=|s|}$. POTOM KÓD s JE (KÓD M', $|s|$, i), KDE M' POSTUPNE PREHĽADÁVA SLOVÁ DĹŽKY $|s|$:

- VSTUP (n, i)
- PRE $\forall$ SLOVÁ DĹŽKY n SIMULÁCIOU M OVER, či PATRÍ DO S. AKO VÝSTUP DAJ i-TE SLOVO V S O DĹŽKE n.

□

03.05.2010 M.
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

SETS - $K(f,g)$ - TO JE TRIEDA JAZYKOV A, ŽE $A - K(f,g)$ JE KONEČNÁ

SETS - $KS(f,g)$ - — " —

F, G MNOŽINY FUNKCIÍ, POTOM:

$$SETS - K(F,G) = \bigcup_{f \in F,\, g \in G} SETS - K(f,g).$$

LEMMA: $SETS - K(\log, poly)$ JE UZAVRETÁ NA POLYNOMIÁLNY IZOMORFIZMUS.

DÔKAZ: $A \in SETS - k(\log, poly) \Rightarrow \exists k, c:$
$A \in SETS - K(k \log n, n^c)$, $A = F$ - KONEČNÁ
h - POLYN. SPOČÍTATEĽNÁ BIJEKCIA $h: \Sigma^* \to \Sigma^*$
T.Z. h^{-1} JE TAKTIEŽ POLYN. SPOČÍTATEĽNÁ.
NECH M JE TS., KTORÝ PRE VSTUP y SPOČÍTA $h(U(y))$ - POKIAĽ $U(y)$ JE DEF., INAK NIČ.
$\exists c'$ - M POČÍTA V ČASE $|x|^{c'}$.
KEĎ $x \in F$ S KÓDOM y, POTOM $\langle M, y \rangle$ JE KÓD $h(x)$ SPOČÍTATEĽNÝ V $|y|^{c'}$.
POTOM $h(A) - K(k \log n, n^c) = h(F)$ - KONEČNÁ □

LEMMA: $\forall k, c: K(k \log n, n^c) \in P$.

DÔKAZ. ZREJMÝ. □

10.05.2010 M.
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

$u \leq v \iff$ BUĎ $|u| < |v|$, ALEBO $|u| = |v|$ A u JE v LEX USP. PRED v.

$SETS-K(f,g)$ - MNOŽINA JAZYKOV A T.Ž. $A \setminus K(f,g)$ JE KONEČNÁ,

$SETS-K(F,G) = \bigcup_{f \in F, g \in G} SETS-K(f,g)$.

VETA: PRE JAZYK S JE EKVIV.:

a) $S \in SET-K(\log, poly) \cap P$
b) S JE P-TLAČITEĽNÁ (P-PRINTABLE)
c) S JE RIEDKA A MÁ POL. SPOČÍTATEĽNÚ RANKING FUNKCIU
d) S JE POL. IZOMORFNÁ S TALLY MN. $T \in P$.

DÔKAZ: a) $\Rightarrow$ b) $S \in SETS-K(c \cdot \log n, n^k)$

- ALGORITMUS NA VYTLAČENIE (PRINT)

VSTUP n
VEZMEME $\forall$ SLOVA v T.Ž. $|v| < c \cdot \log n$
ZISTÍME, AKÉ SLOVO w KÓDUJE v V $K(c \log n, n^k)$
POTOM ZISTÍME, ČI $w \in S$ (SEP)
A AK ÁNO, VYTLAČÍME w.

b) $\Rightarrow$ c) S JE P-TLAČITEĽNÁ $\Rightarrow$ MUSÍ BYŤ RIEDKA, INAK BY NEŠLO $S^{\leq n}$ VYTLAČIŤ V POL. ČASE

KEĎ MÁME SLOVO s, TAK VYTLAČÍME VŠETKY SLOVÁ V S O DĹŽKE $\leq |s|$, A ZISTÍME (V POL. ČASE), KOĽKO SLOV JE PRED s.

d) $\Rightarrow$ a) T - TALLY MNOŽINA V P, POTOM $T \subseteq K(\log, \text{poly})$. $\Rightarrow T \in SETS - K(\log, \text{poly}) \cap P$. ALE $SETS - K(\log, \text{poly})$ AJ P SÚ UZAVRETÉ NA POLYNOMIÁLNY IZOMORFIZMUS.

c) $\Rightarrow$ d) S RIEDKA, r - POLYN. SPOČÍTATEĽNÁ RANKING FCIA. S.

r_2 - RANKING FCIA. DOPLNKU S, TJ.

$r_2(u) = 2^{|u|} + \underbrace{|u| - r(u)}_{\text{BIN. ZÁPIS}} \Rightarrow r_2$ JE POL. SPOČ.

S JE RIEDKA $\Rightarrow$ EXISTUJE NEKLESAJÚCI POL. p T.Z. $p(n) \geq r(1^n) - r(1^{n-1})$.

PRE $s \in S$, $h(s) = 0^{(n-1)} p(n-1) + r(s) - r(1^{n-1}) - 1$, $n = |s|$

$$0,\ 00,\ \underset{\uparrow}{000},\ \ldots,\ \underset{\uparrow}{\ldots},\ \ldots,\ \underset{\uparrow}{00\ldots0},\ \ldots$$

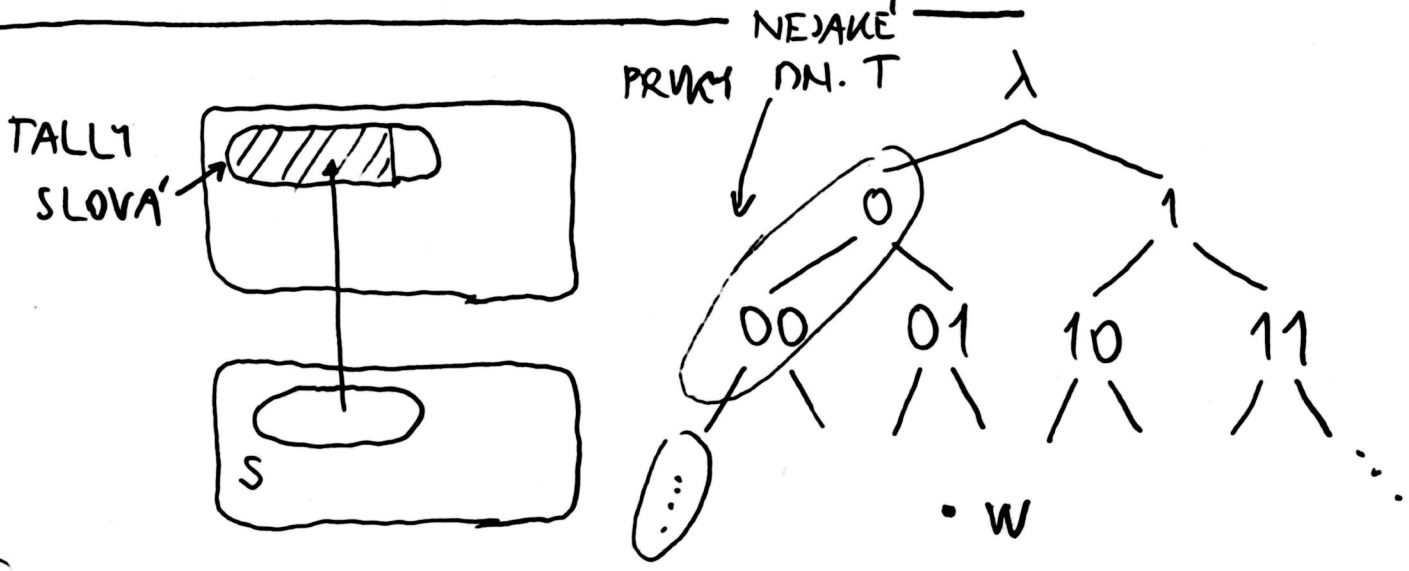
$1 \cdot p(1)$ $\quad$ $2 \cdot p(2)$ $\quad$ $(n-1)\ p(n-1)$

1) $|S^{\leq n}| \leq (n-1)\, p(n-1)$

2) $|s| = n$, KOĽKÁTE JE s V S MEDZI SLOVAMI DĹŽKY n ? ODPOVEĎ: $r(s) - r(1^{n-1})$

10.05.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II



$T = h(S)$, CHCEM SPOČÍTAŤ RANKING FUNKCIU DOPLNKU T.

VEZMEME SLOVO w. NÁJDEME n TAKÉ, ŽE $(n-1)\,p(n-1) \le |w| < n\,p(n)$ ...

NÁJDEME V POL. ČASE VZHĽADOM K $|w|$.

POČET SLOV $h(s)$, $s \in S$, $|s| < n$ JE $r(1^{n-1})$

NECH w JE q-TE SLOVO V USPORIADANÝCH VŠETKÝCH SLOVÁCH, TJ. $q = 2^{|w|} + w$ (BIN. ZÁPIS)

OD q MUSÍME ODPOČÍTAŤ $r(1^{n-1})$ A TAKTIEŽ $i = |w| - (n-1)\,p(n-1) - 1$.

POKIAĽ $i + r(1^{n-1}) \le r(1^n)$, TAK ODČÍTAME i, INAK ODČÍTAME $r(1^n) - r(1^{n-1})$.

$r_3(w) = 2^{|w|} + w - r(1^{n-1}) - \min\{ |w| - (n-1)\,p(n-1) - 1,$
$r(1^n) - r(1^{n-1}) \} \Rightarrow r_3$ JE POL. SPOČ.

PRE $w \notin S$, $h(w) = r_3^{-1}(r_2(w))$.

- SPOČÍTANIE POLYNOMIÁLNE VZHĽADOM K $|w|$
A POLYNOMIÁLNE VZHĽADOM K $|h(w)|$.

$|h(w)|$ JE POLYN. VZHĽADOM K $|w|$.

ZÁVER: h JE POLYN. SPOČÍTATEĽNÁ BIJEKCIA
T.Z. $h(S) = T$ - JE TALLY MNOŽINA.

$h^{-1}(w) = r_2^{-1}(r_3(w))$, KEĎ $w \notin T$.

$h^{-1}(w)$ PRE $w \in T$:

NÁJDEME n, ŽE $(n-1)\,p(n-1) \leq |w| < n\,p(n)$.

A $h^{-1}(w) = r^{-1}(r(1^{n-1}) + |w| - (n-1)\,p(n-1))$.

V OBOCH PRÍPADOCH POLYN. SPOČÍTATEĽNÉ. □

VETA: PRE JAZYK S JE EKVIVALENTNÉ:

a) $S \in SETS\text{-}K(log, poly)$

b) S JE POL. IZOMORFNÉ S TALLY MN. T

D: a) $\Rightarrow$ b)) $\exists\, c, k$ A KONEČNÁ F T.Z.

$S \subseteq K(c \cdot \log n, n^k) \cup F$.

POTOM $K(c \cdot \log n, n^k) \cup F \in SETS\text{-}K(log, poly) \cap P$

PODĽA PREDCH. VETY EXISTUJE TALLY MNOŽINA T
A POL. IZOMORFIZMUS h Z $K(c \log n, n^k) \cup F$
NA T.

10.05.2010 M.
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

Potom $h(S) = T' \subset T$, tedy T' je tally množina a h je pol. izomorfizmus mezi S a T'.

b) $\Rightarrow$ a)) T je polyn. izomorfná s S,
$\exists c, k$ t.ž. $T \subseteq K(c \log n, n^k) \in SETS\text{-}K(log, poly)$,
protože $SETS\text{-}K(log, poly)$ je uzavretá na pol. izomorfizmus. □

DÔSLEDOK: $P = NP \Leftrightarrow \forall A \in SETS\text{-}K(log, poly)$ platí $P(A) = NP(A)$.

Za predpokladu $P = NP$:

$NP_b(A) = NP(A) \Rightarrow NP_b(A) \subseteq P(A \oplus SAT) = P(A)$.

INTERAKTÍVNE PROTOKOLY

Dva DTS - M_P - dokazovateľ (Merlin)
M_V - overovateľ (Artuš)

Majú spoločnú read-only vstupnú pásku
spoločnú komunikujúcu pásku
spoločnú random pásku:
- obsahuje 0,1 podľa hádzania spravodlivou mincou

- DELÍ SA NA DVA PRÍSTUPY :

a) PÁSKA JE TAJNÁ - IBA PREČÍTA SYMBOL A HLAVA SA NEVRACIA

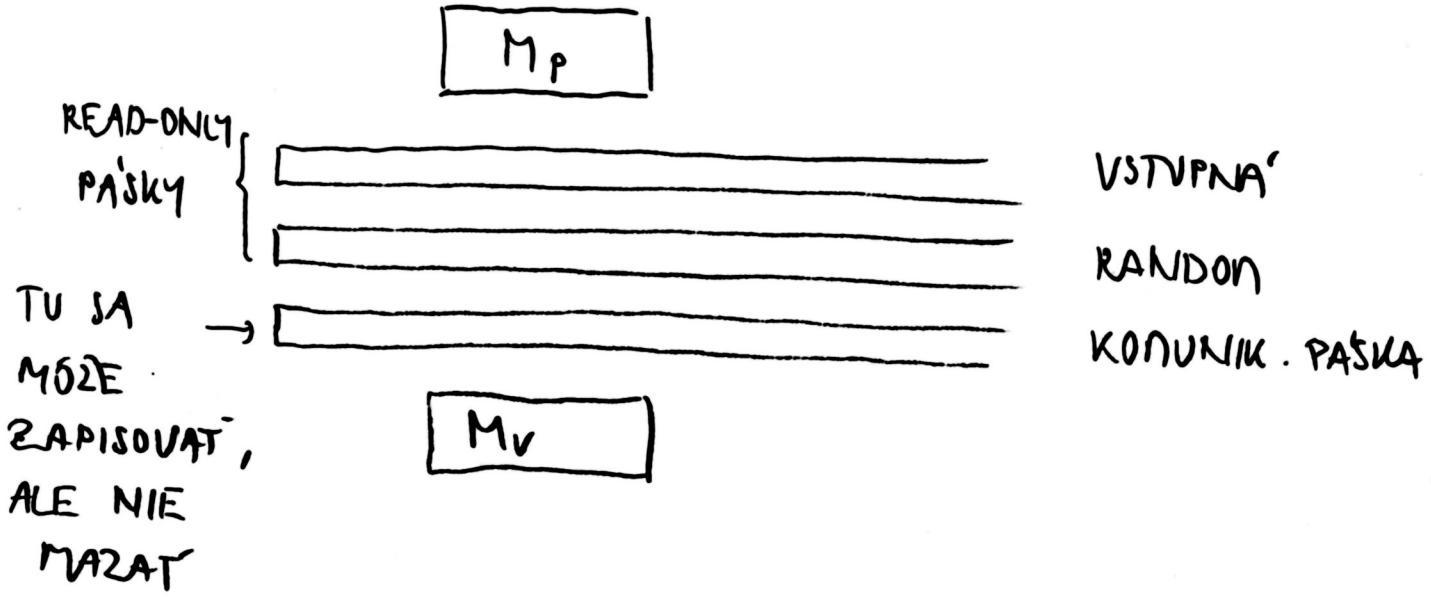
b) PÁSKA JE VEREJNÁ - IBA ČÍTA, ALE HLAVU MÔŽE VRACAŤ

M_P - NEMÁ OHRANIČ. VÝPOČTOVÚ SILU

M_V - PRACUJE IBA V POL. ČASE

- VÝPOČET PREBIEHA V CYKLE BEHOV :

V JEDNOM BEHU JEDEN Z TS POČÍTA (DRUHÝ STOJÍ), PRITOM MÔŽE BRAŤ VSTUPY Z RANDOM PÁSKY A NA KOMUNIKUJÚCU PÁSKU MÔŽE ZA PREDCHÁDZAJÚCU ČASŤ NAPÍSAŤ SVOJU SPRÁVU PRE DRUHÝ TS, ALE NESMIE MAZAŤ



OVERENIE VYKONÁ M_V

SÚČET $\forall$ ČASOV, KT. POUŽIL M_V VO $\forall$ BEHOCH JE OHRANIČ. POLYNÓMOM

10.05.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNI SLOŽITOST II

JAZYK A JE PRIJÍMANÝ OVEROVATEĽOM M_V, KEĎ

a) EXISTUJE DOKAZOVATEĽ M_P T.Ž. M_V A M_P TVORIA SYSTÉM, A PRE KAŽDÉ $x \in A$:

$P(\text{SYSTÉM PRIJÍMA } x) \geq \frac{2}{3}$ $\quad (\text{POPR. } \geq \delta > \frac{1}{2})$

KDE P SA POČÍTA CEZ $\forall$ VSTUPY NA RANDOM PÁSKE

b) PRE KAŽDÉHO DOKAZOVATEĽA M_P TAKÉHO, ŽE M_V A M_P TVORIA SYSTÉM A PRE KAŽDÉ $x \notin A$

$P(\text{SYSTÉM PRIJÍMA } x) \leq \frac{1}{3}$ $\quad (\text{POPR. } \leq \delta < \frac{1}{2})$

MOŽNO EŠTE UROBIŤ HIERARCHIU NA ZÁKLADE BEHOV:

M - BEH VYKONÁVANÝ MERLINOM
A - —II— ARTUROM

POTOM MAM... HOVORÍ, AKÉ MOHLI BYŤ BEHY.

PRÍKLADY: $A \in NP$ - POTOM $\exists$ NTS M PRIJÍMAJÚCI A V POLYN. ČASE

- POTOM M_V - BERIE VSTUP x ZO VSTUPNEJ PÁSKY, Y Z KOMUNIKUJÚCEJ PÁSKY A OVERÍ, ŽE Y JE KÓD POL. PRIJÍMAJÚCEHO VÝPOČTU M NAD x. AK ÁNO, PRIJME, INAK ODM.

M_p - Z BODU a) - PRE $x \in A$ NÁJDE KÓD POLYN. PRIJÍMAJÚCEHO VÝPOČTU M NAD x A NAPÍŠE HO NA PÁSKU.

<u>DÔSLEDOK</u> : $NP \subseteq M$.

17.05. 2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

$A = BPP$, $A\Pi = BP\Pi P$ (VIĎ NIŽŠIE)

$NOISO = \{ G_1, G_2 \mid G_1$ NIE JE IZOMORFNÉ S $G_2 \}$

ARTUŠ: KEĎ NOSNÉ MNOŽINY G_1 A G_2 MAJÚ RÔZNU VEĽKOSŤ, TAK PRIJME

n - VEĽKOSŤ NOSNEJ MNOŽINY

VEZME Z NÁHODNEJ PÁSKY n BITOV $c_1, \ldots, c_n$

PRE KAŽDÉ $i = 1, \ldots, n$ VYGENERUJE Z NÁH. PÁSKY NÁHODNÚ PERMUTÁCIU f_i n-PRVKOVEJ MNOŽINY

DEFINUJE $H_i = \begin{cases} f_i(G_1) & \text{KEĎ } c_i = 0 \\ f_i(G_2) & \text{KEĎ } c_i = 1 \end{cases}$

A POŠLE KÓDY GRAFOV $H_1, \ldots, H_n$ MERLINOVI.

MERLIN: KEĎ $G_1 \simeq G_2$, TAK VOĽÍ NÁHODNE $\alpha_i \in \{0,1\}$ PRE $i = 1, \ldots, n$.

KEĎ $G_1 \not\simeq G_2$, TAK $\alpha_i = 1 \Leftrightarrow H_i$ JE IZOMORFNÝ S G_2, $\alpha_i = 0$ KEĎ H_i JE IZOMORFNÝ S G_1.

POŠLE $\alpha_1, \ldots, \alpha_n$ ARTUŠOVI.

ARTUŠ: PRIJME, KEĎ $\alpha_i = c_i$ PRE KAŽDÉ i, INAK ODMIETNE.

□

NEDETERMINISTICKÝ PRAVD. TS :

- JE TO KLASICKÝ NEDETER. TS., ALE STAVY SÚ ROZDELENÉ NA :
  - DETERMINISTICKÉ
  - NEDETERMINISTICKÉ
  - PRAVDEPODOBNOSTNÉ (TU SÚ PRE PRECHODOVÚ FUNKCIU DANÉ PRAVDEPODOBNOSTI PRECHODU)
  - KONCOVÉ STAVY (PRIJÍMAJÚCE, ODMIETAJÚCE)

PRE KONFIGURÁCIE SA POČÍTA PRAVDEPODOBNOSŤ p, ŽE PRIJÍMA :

- PRE PRIJÍMAJÚCU KONF. s JE $p(s) = 1$
- PRE ODMIETAJÚCU KONF. s JE $p(s) = 0$
- KEĎ s JE DETERMINISTICKÁ A NASLEDUJÚCA KONFIGURÁCIA JE s', POTOM $p(s) = p(s')$
- KEĎ s JE NEDETERM., POTOM $p(s) = \max \{ p(s') \mid s' \text{ JE NASL. KONF. PRE } s \}$
- KEĎ s JE PRAVD., POTOM $p(s)$ JE VÁŽENÝ PRIEMER Z $p(s')$, KDE s' NASL. PO s

M PRIJÍMA $x \iff p(\text{INICIÁLNA KONF.}) > \frac{1}{2}$

BPNP - JAZYK L T.Ž. EXISTUJE NEDET. PRAVD. TS. M PRIJÍMAJÚCI L V POL. ČASE A EXISTUJE $\delta > 0$:

$x \in L \Rightarrow M$ PRIJÍMA S PR. $> \frac{1}{2} + \delta$

$x \notin L \Rightarrow M$ PRIJÍMA S PR. $< \frac{1}{2} - \delta$.

17.05.2010 M.
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

PLATÍ: $L \in BPP \Leftrightarrow \exists A \in P$, POLYNÓM p, $\delta \in (0, \frac{1}{2})$ T.Ž. (y BERIEME Z UNIF. ROZD.)

$x \in L \Leftrightarrow Prob\{ y \mid |y| = p(|x|), (x,y) \in B \} > \frac{1}{2} + \delta$

$x \notin L \Leftrightarrow$ —II— $< \frac{1}{2} - \delta$.

MAJME TRIEDU JAZYKOV $\mathcal{C}$. POTOM:

$BP(\mathcal{C})$ JE MNOŽINA JAZYKOV A T.Ž.

$\exists B \in \mathcal{C}$, POLYNÓM p A $\delta \in (0, \frac{1}{2})$ A PLATÍ

$x \in L \Leftrightarrow Prob\{ y \mid |y| = p(|x|), (x,y) \in B \} > \frac{1}{2} + \delta$

$x \notin L \Leftrightarrow$ —II— $< \frac{1}{2} - \delta$

LEMMA: MAJME $(0,1)$-POKUS E TAKÝ, ŽE VÝSLEDOK 1 JE S PRAVD. $\geq \frac{1}{2} + \delta$ PRE $\delta \in (0, \frac{1}{2})$. POTOM PRE t NEZÁVISLÝCH POKUSOV E PLATÍ, ŽE S PR. $\geq 1 - \frac{1}{2}(1 - 4\delta^2)^{t/2}$ JE ASPOŇ POLOVICA VÝSLEDKOV 1.

DÔKAZ. q_i - PRAVD., ŽE PRÁVE i POKUSOV SKONČILO S VÝSLEDKOM 1:

$$q_i = \binom{t}{i} (1/2 + \delta)^i (1/2 - \delta)^{t-i}.$$

KEĎ $i \leq \frac{t}{2}$, POTOM

$$q_i = \binom{t}{i}\left(\tfrac{1}{2}+\delta\right)^i\left(\tfrac{1}{2}-\delta\right)^{t-i} \le \binom{t}{i}\left(\tfrac{1}{2}+\delta\right)^{t/2}\left(\tfrac{1}{2}-\delta\right)^{t/2}.$$

POTOM PRAVDEPODOBNOSŤ, ŽE VO VÄČŠINE PRÍPADOCH MODE 1 JE: $1 - \sum_{i=0}^{\lfloor t/2 \rfloor} q_i \ge$

$$\ge 1 - \sum_{i=0}^{\lfloor t/2 \rfloor}\binom{t}{i}\left(1/2+\delta\right)^{t/2}\left(\tfrac{1}{2}-\delta\right)^{t/2} \ge$$

$$\ge 1 - 2^{t-1}\left(\tfrac{1}{4}-\delta^2\right)^{t/2} = 1 - \tfrac{1}{2}\left(1-4\delta^2\right)^{t/2}. \quad \square$$

VETA: $\mathcal{C}$ - TRIEDA JAZYKOV UZAVRETÁ NA $\le_m$ A NA OPERÁCIU MAJORIZÁCIE (T.J. KEĎ $A \in \mathcal{C}$, POTOM $B \in \mathcal{C}$, KDE $B = \{\langle u_1, \ldots, u_n\rangle \mid$ PRE ASPOŇ POLOVICU INDEXOV i PLATÍ $u_i \in A\}$).

POTOM PLATÍ: $\forall A \in BP(\mathcal{C})$ A $\forall$ POLYNÓM q EXISTUJE $B \in \mathcal{C}$ A POLYNÓM p TAKÝ, ŽE

$$x \in A \Rightarrow \text{Prob}\{y \mid |y| = p(|x|), \langle x,y\rangle \in B\} > 1 - 2^{-q(|x|)},$$

$$x \notin A \Rightarrow \text{Prob}\{-\text{''}-, \langle x,y\rangle \notin B\} < 1 - 2^{-q(|x|)}.$$

NIE JE EKVIVALENTNÉ S:

$$\text{Prob}\{x \in A \Leftrightarrow \exists y, |y| = p(|x|), \langle x,y\rangle \in B\} > 1 - 2^{-q(|x|)}.$$

DÔKAZ.

17.05.2010 Mo
PETER ČERNO

NTIN082 STRUKTURÁLNÍ SLOŽITOST II

VIETE: $A \in BP(\mathcal{C}) \Rightarrow \exists B' \in \mathcal{C}$ A POLYNÓM r

$x \in A \Rightarrow \text{Prob}\{y \mid \langle x,y\rangle \in B'\} \geq \frac{1}{2}+\delta$

$x \notin A \Rightarrow \text{Prob}\{y \mid \langle x,y\rangle \in B'\} \leq \frac{1}{2}-\delta$

KDE $|y| = r(|x|)$ JE VYBRANÉ Z ROVNOM. ROZDEL.

VEZMEME t SLOV $y_1, y_2, \ldots, y_t$, $|y_i| = r(|x|)$

A DEFINUJME JAZYK $B = \{(x, y_1, \ldots, y_t) \mid$ PRE ASPOŇ POLOVICU i PLATÍ, ŽE $(x, y_i) \in B'\}$.

PRETOŽE $B' \in \mathcal{C}$, A $\mathcal{C}$ JE UZAVRETÁ NA MAJORIZÁCIU $A \leq_m$, TAKŽE $B \in \mathcal{C}$.

$x \in A \Rightarrow \text{Prob}\{(x, y_1, \ldots, y_t) \in B\} \geq$

$\geq 1 - \frac{1}{2}(1-4\delta^2)^{t/2}$.

STAČÍ ZVOLIŤ t TAK, ABY: $1 - \frac{1}{2}(1-4\delta^2)^{t/2} \geq 1 - 2^{-q(|x|)}$,

NAPR. $t \geq \dfrac{2\,q(|x|)}{\log\left(\frac{1}{1-4\delta^2}\right)}$. □

LEMA: MAJME $E \subseteq \{0,1\}^m$ TAKÚ, ŽE

$|E| \geq (1-2^{-k})2^m$, KDE $2^k > m$.

POTOM PRE NÁHODNE ZVOLENÉ $u = (u_1, \ldots, u_m)$,

KDE $|u_i| = m$ S ROVNOMERNÝM ROZDELENÍM

PLATÍ:

$$\text{Prob}\{\exists v \mid |v|=m, \forall i=1,\dots,m \ (u_i \oplus v) \in E\} = 1$$

$$\text{Prob}\{\forall v \mid |v|=m, \exists i=1,\dots,m \ (u_i \oplus v) \in E\} > 1 - 2^{-m(k-1)}.$$

VETA: $BP(\Sigma_k) \subseteq \Pi_{k+1}$, $BP(\Pi_k) \subseteq \Sigma_{k+1}$.

DÔSLEDOK: $AM \subseteq \Pi_2$, $co\text{-}AM \subseteq \Sigma_2$.

VETA: KEĎ $\Pi_k \subseteq BP(\Sigma_k)$, POTOM $\Sigma_{k+1} = \Pi_{k+1}$.
KEĎ $\Sigma_k \subseteq BP(\Pi_k)$, POTOM $\Sigma_{k+1} = \Pi_{k+1}$.

VETA: $MAM \subseteq AM$.

VETA: $AM \supseteq$ A ...
M ...

VETA: $IP = PSPACE$.