Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Složitost II
BONUS

Peter Černo, 2010
petercerno@gmail.com

Garant: doc. RNDr. Ondřej Čepek, Ph.D.
E-mail: Ondrej.Cepek@mff.cuni.cz
Domácí stránka: `http://ktiml.mff.cuni.cz/~cepek/`

Anotace: Základní přednáška o strukturální složitosti. Zavedení jednotlivých tříd časové a prostorové složitosti, zkoumání vlastností těchto tříd a vztahů mezi nimi vzhledem k inkluzi.

Sylabus:

1. Definice výpočetních modelů (různé typy Turingových strojů).
2. Věty o lineárním zrychlení a kompresi. Redukce počtu pásek pro prostorovou složitost a pro časovou složitost.
3. Konstruovatelnost funkcí (časová/prostorová).
4. Třídy DTIME(t), NTIME(t), DSPACE(s), NSPACE(s), kde s,t jsou prostorově resp. časově konstruovatelné funkce.
5. Hierarchické věty pro DSPACE a DTIME.
6. Vzájemné vztahy mezi DTIME, NTIME, DSPACE, NSPACE, Savičova věta.
7. Translační lemma, nedeterministické hierarchie.
8. Borodinova věta o mezerách, Blumova věta o zrychlení.
9. Definice tříd LOG, NLOG, P, NP, PSPACE, NPSPACE, DEXT, NEXT, EXPSPACE a EXPTIME.
10. Polynomiální hierarchie, třídy NP, co-NP.

Cíl předmětu: Naučit další látku z teorie složitosti, třídy složitosti, jejich vlastnosti a vztahy.

Literatura:

1. Balcázar, Díaz, Gabarró : Structural Complexity I, Springer Verlag 1988

2. Hopcroft J. E., Ullman J. D.: Introduction to automata theory, languages, and computation (kapitola XII)

3. V. Majerech: Složitost a NP-úplnost (skripta v elektronické podobě http://ktiml.ms.mff.cuni.cz/vyuka/materialy.html)

This page is intentionally left blank.

21.06.2009 Su
PETER ČERNO

NTIN063 SLOŽITOST II - SKÚŠKA

VETA O LIN. PRIESTOROVEJ KOMPRESII

k-páskový DTS M, akc. priestor $S(n)$ ⟶ k-páskový DTS M', akc. priestor $\lceil \frac{1}{r} S(n) \rceil$

PODOBNE PRE NTS

r-tica ⟶ 1 symbol

V stave si odpamätám, kde som sa vrámci r-tice nachádzal

VETA O REDUKCII POČTU PÁSOK PRE PRIEST. ZLOŽITOSŤ

k-páskový DTS M, akc. priestor $S(n)$ ⟶ 1-páskový DTS M', akc. priestor $S(n)$

TO ISTÉ PRE NTS

k-pások

1 páska

k-tica symbolov

k-tica {0,1} pozície hláv

1 krok M' … $O(S(n))$ krokov M

M' je $2k\,S(n)$-krát pomalejší

hlava M' prejde celý prac. priestor a u tých znakov, kde sú hlavy stroja M, vykoná príslušné úpravy

prácu pre jednoduchosť rozdelíme do k fáz …

VETA O REDUKCII POČTU PÁSOK PRE ČAS. ZLOŽITOSŤ

k-páskový DTS M, akc. čas $T(n)$ ⟶ 1-páskový DTS M', akc. čas $c \cdot (T(n))^2$

PLATÍ AJ PRE NTS

M' pracuje v čase $2k \cdot S(n) \cdot T(n)$

M v čase $T(n)$ zaberie priestor najviac $k \cdot T(n)$

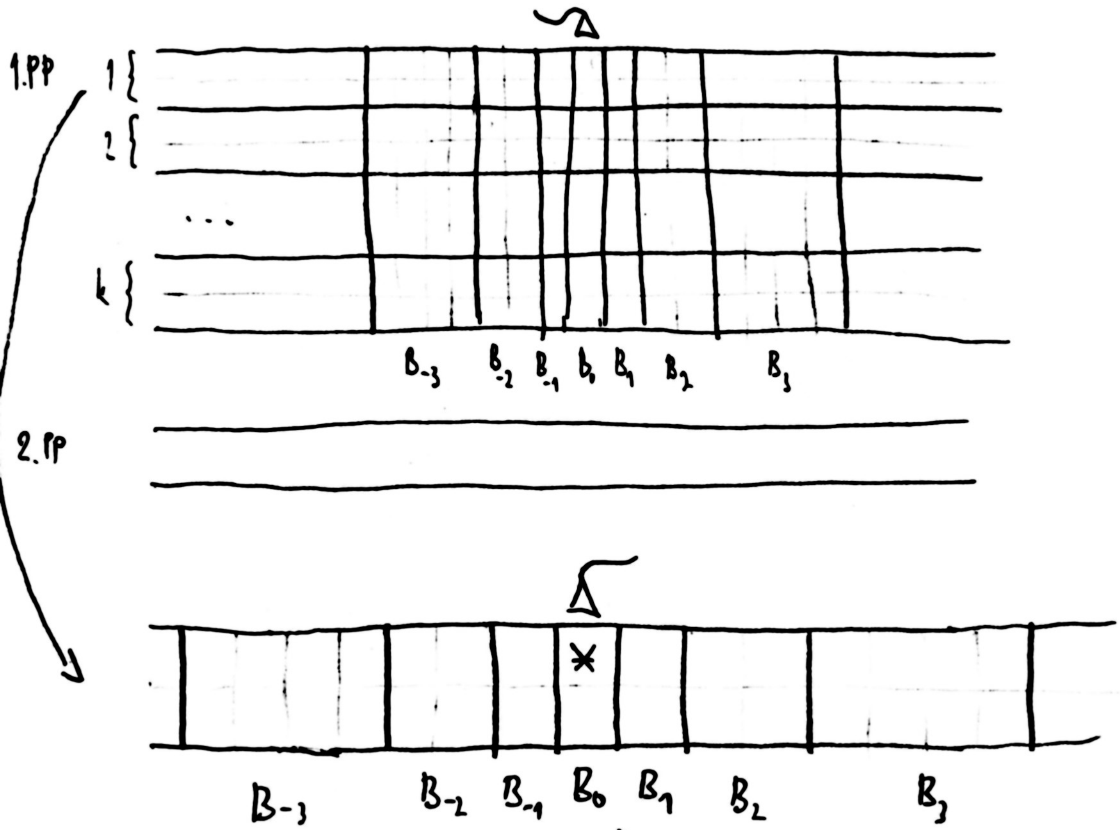
$\Rightarrow S(n) \leq k \cdot T(n) \quad \Rightarrow$ čas $2k^2 (T(n))^2$

$\boxed{\text{VETA}}$ O REDUKCII POČTU PÁSOK PRE ČAS. ZLOŽITOSŤ (II)

k-PÁSKOVÝ DTS M, AKC. ČAS $T(n)$	$\rightsquigarrow$	2-PRAC. PÁSKY DTS M', AKC. ČAS $c \cdot T(n) \cdot \log T(n)$

OBOJSMERNÉ POTENCIÁLNE NEKONEČNÉ PÁSKY

1. PRAC. PÁSKA ... 2k STÔP
2. PRAC. PÁSKA ... SLÚŽI PRE PRESUNY BLOKOV

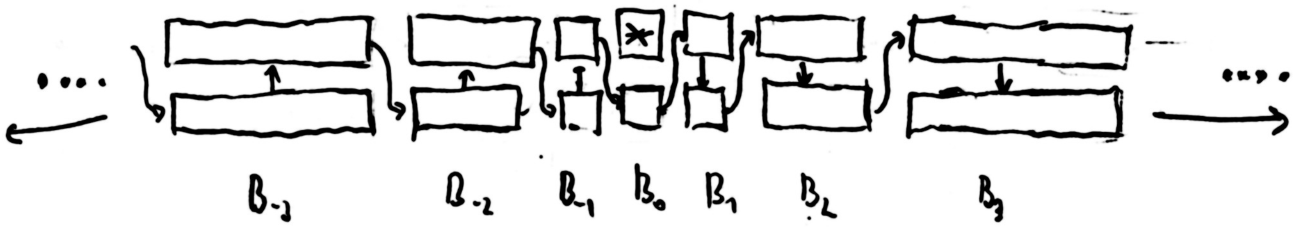


NEHÝBEME HLAVAMI
IBA DATAMI

INVARIANTY:

1. (i) B_i OBE PLNÉ B_{-i} OBE PRÁZDNE
   (ii) B_i OBE PRÁZDNE B_{-i} OBE PLNÉ
   (iii) B_i, B_{-i} DOLNÁ PLNÁ, HORNÁ PRÁZDNA

2.



3. B_0 .. *

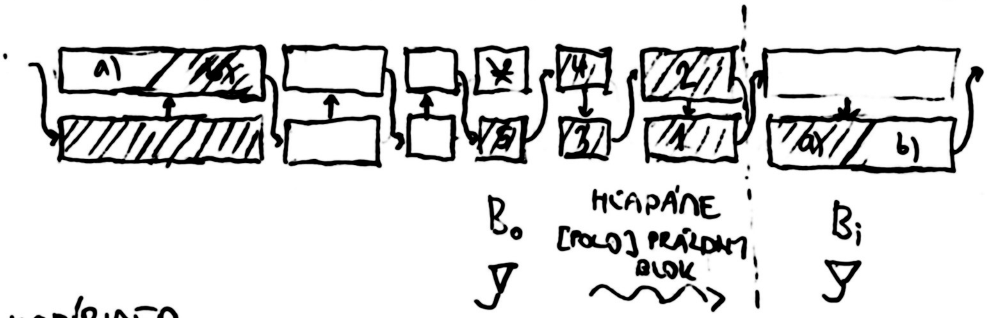
4. B_i JE NAĽAVO OD B_{i+1} ..

21.06.2009 S_1
PETER ČERNO

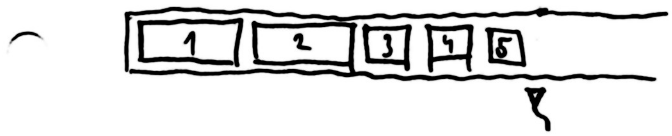
NTIN063 SLOŽITOST II - SKÚŠKA

POSUN HLAVY DOĽAVA V M = PRESUN DÁT DOPRAVA V M'

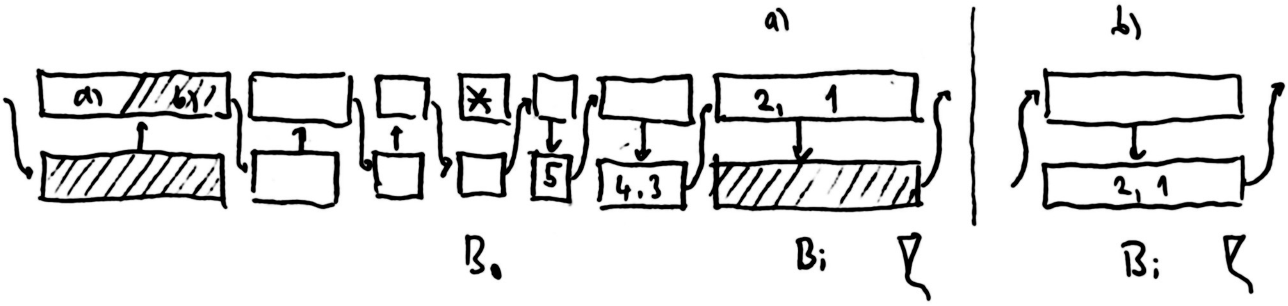
1.



2. KOPÍRUJEM BLOKY $B_{i-1}, \dots, B_0$ NA 2. PP



3. ZÁPIS



4. SPOČÍTAME i
5. NÁJDEME B_{-i}
6. KOPÍRUJEM $\left\langle \begin{matrix} a) & DS \\ b) & HS \end{matrix} \right\rangle$ B_i DO 2. PP
7. KOPÍRUJEM 2. PP DO DS $B_{-(i-1)} \dots B_0$

KROKY 1 - 7 $\equiv$ B_i - OPERÁCIA

TRVÁ $O(|B_i|)$ KROKOV $= O(2^{i-1})$

$\triangleleft$ PO VYKONANÍ B_i OP. NEMÔŽE BYŤ ĎALŠIA SKÔR NEŽ PO 2^{i-1} KROKOCH M

BLOKY $B_1, \dots, B_{i-1}$ SÚ POLOPLNÉ, MUSIA SA ZAPLNIŤ

B_i - OP. MÔŽE BYŤ SPUSTENÁ NAJVIAC $\left\lfloor \frac{T(n)}{2^{i-1}} \right\rfloor$ KRÁT

$\Rightarrow$ STAČÍ UVAŽOVAŤ $i \leq \lceil \log_2 T(n) \rceil$

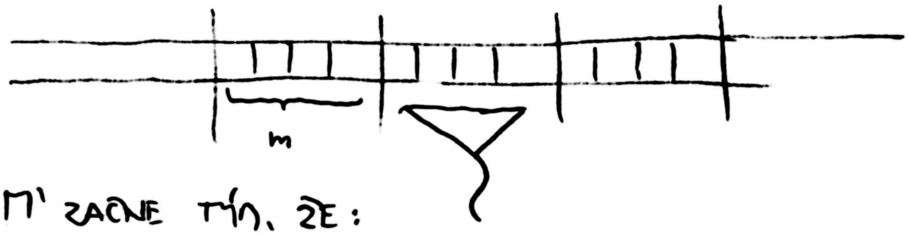
$$\Rightarrow \quad T'_j(n) = \sum_{i=1}^{\lceil \log_2 T(n) \rceil} O(|B_i|) \cdot \frac{T(n)}{2^{i-1}} = O(T(n) \log_2 T(n)).$$

$\boxed{\text{VETA}}$ O LIN. ZRÝCHLENÍ ČAS

k-PÁSKOVÝ, $k \overset{?}{\geq} 2$ DTS M, AKCEPTOR ČAS $T(n) \in \omega(n)$	$\overset{c>0}{\rightsquigarrow}$	$(k+1)$-PÁSKOVÝ DTS M', AKCEPTOR ČAS $c \cdot T(n)$		V NEDETERMIN. PRÍPADE SIMULUJEM M, ALE PO m KROKOCH HO STOPNEM

PÁSKU ROZSEKÁME NA m-TICE

POUŽÍVAME 3m TICE ($\Rightarrow$ ASPOŇ m KROKOV M)



M' ZAČNE TÝM, ŽE:

VSTUP PREPÍŠE NA $\underline{(k+1).\ \text{PÁSKU}}$, m-TICE KÓDUJE DO 1 SYMBOLU

1 KROK M':

4 POSUNY $\leftarrow, \rightarrow, \rightarrow, \leftarrow$ $\rightsquigarrow$ SIMULÁCIA M ASPOŇ m KROKOV $\rightsquigarrow$ 4 POSUNY NA ZÁPIS A PRÍPADNÝ PRESUN

$$T'(n) \leq n \text{ (NAČÍTANIE VSTUPU)} + \left\lceil \frac{n}{m} \right\rceil \text{ (NA ZAČIATOK (k+1). PÁSKY)} + 8 \left\lceil \frac{T(n)}{m} \right\rceil \text{ (SIMULÁCIA)} \leq \boxed{n + \frac{n}{m} + 8\frac{T(n)}{m} + 9}$$

$$T(n) \in \omega(n) \Rightarrow \forall d > 0\ \exists n_d\ \forall n \geq n_d\ T(n) \geq d \cdot n$$

PRE DOSTAT. VEĽKÉ n: m A d

$$\leq 2n + \frac{n}{m} + 8\frac{T(n)}{8} \leq T(n) \underbrace{\left(\frac{2}{d} + \frac{1}{md} + \frac{8}{m}\right)}_{\leq c}$$

$\varepsilon > 0$

k-PÁSKOVÝ, $k \overset{?}{\geq} 2$ DTS M, AKCEPTOR ČAS $T(n) = cn$	$\rightsquigarrow$	$(k+1)$-PÁSKOVÝ DTS M', AKCEPTOR ČAS $(1+\varepsilon)n$

$$T'(n) \leq \cancel{n} + \frac{n}{m} + 8\frac{T(n)}{m} + 9 \leq \ldots \leq (\cancel{1} + \varepsilon)n$$

PRE DOST. VEĽKÉ n A m:

$$\frac{n}{m} \leq \frac{1}{3}\varepsilon n, \quad 8\frac{T(n)}{m} = 8\frac{cn}{m} \leq \frac{1}{3}\varepsilon n, \quad 9 \leq \frac{1}{3}\varepsilon n$$

21.06.2009 Su
PETER ČERNO

NTIN063 SLOŽITOSŤ II - SKÚŠKA

f REKURZÍVNA, DTS: $1^n \rightsquigarrow 1^{f(n)}$ TRANSDUCER

VYČÍSLITEĽNÁ V ČASE $O(f)$
VYČÍSLITEĽNÁ V PRIESTORE $O(f)$ } f REK. A $\exists c \geq 1 \dots$

ČASOVO KONŠTRUOVATEĽNÁ (PREDP. $f(n) \geq n+1$)
PRIESTOROVO KONŠTRUOVATEĽNÁ } NEMÁME VÝSTUPNÚ PÁSKU

$\rightarrow$ DTS AKCEPTOR.

$\boxed{\begin{array}{l} f_1 + f_2,\ f_2 \text{ ČAS. KONŠTR.} \\ \exists\, \varepsilon > 0,\ n_0\ \forall n \geq n_0 \\ (*)\ f_1(n) \geq \varepsilon f_2(n) + (1+\varepsilon) n \end{array}}$ $\rightsquigarrow$ $\boxed{f_1 \text{ ČAS. KONŠTR.}}$

VETA $f(n)$, $\exists\, \varepsilon > 0,\ n_0\ \forall n \geq n_0 : f(n) \geq (1+\varepsilon) n$

$\boxed{f \text{ ČASOVO KONŠTR.}}$ $\Leftrightarrow$ $\boxed{f \text{ VYČÍSLITEĽNÁ V } O(f)}$

$\Leftarrow$) $f_1(n) := f(n)$, $f_2(n) := g(n)$ SKUTOČNÝ POČET KROKOV M NA VSTUPE 1^n

$f_1 + f_2$, f_2 SÚ ČASOVO KONŠTR., MUSÍME UKÁZAŤ, ŽE PLATÍ (*)

$\exists\ \varepsilon_1 > 0,\ n_0 \ :\ f(n) \geq (1+\varepsilon_1) n$ $\qquad g(n) \leq c f(n)$

$\exists\ \varepsilon_2 > 0 \ :\ (1+\varepsilon_1)(1-\varepsilon_2) > 1$

$\varepsilon_3 :=$ —"— $-1 > 0$

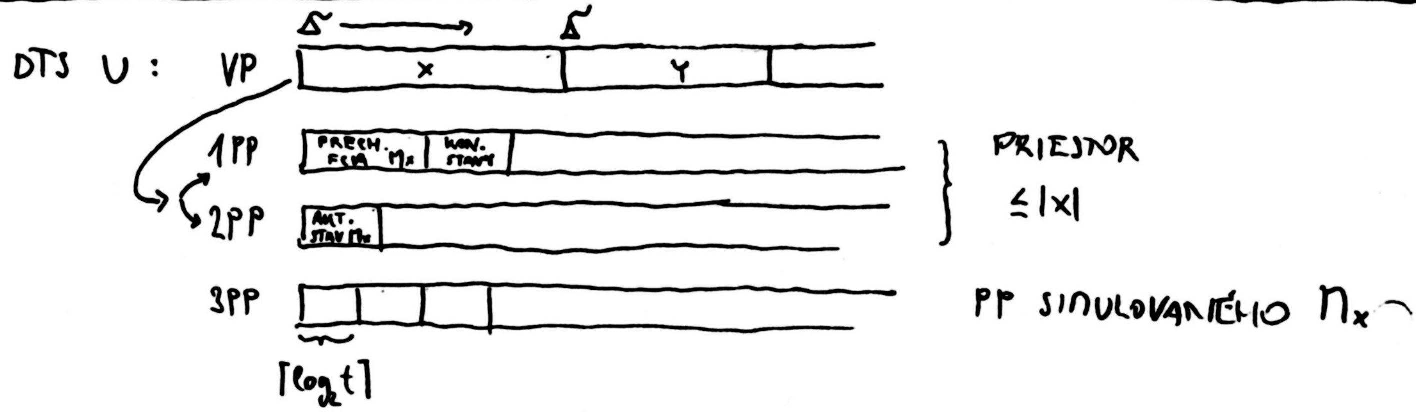
$\varepsilon_4 := \min\left\{\frac{\varepsilon_2}{c}, \varepsilon_3\right\}$

$$f(n) = \varepsilon_2 f(n) + (1-\varepsilon_2) f(n) \geq \frac{\varepsilon_2}{c} g(n) + (1-\varepsilon_2)(1+\varepsilon_1) n \geq$$
$$\geq \varepsilon_2/c\ g(n) + (1+\varepsilon_3) n$$

VETA $\boxed{f \text{ PRIESTOROVO KONŠTR.}}$ $\Leftrightarrow$ $\boxed{f \text{ VČ. V LIN. PRIESTORE}}$

$\Leftarrow$) $\boxed{\begin{array}{l} \text{DTS } M : 1^n \rightsquigarrow 1^{f(n)} \\ \text{PRIESTOR } c f(n),\ c \geq 1 \end{array}}$ $\rightsquigarrow$ NA VŠETKÝCH PP KOMPRESIA S KONŠT. $\lceil c \rceil$ $\rightsquigarrow$ VŠETKY PP + VÝSTUPNÚ PÁSKU SPLAČNEME DO 1 PP.

x = GÖDEL. ČÍSLO $\in \{0,1\}^*$ M_x DTS AKCEPTOR, 1 PP PRIESTOR $S(n)$ VSTUP. ABECEDA = $\{0,1\}$ PRAC. ABECEDA .. t SYMBOLOV	+	DATA $y \in \{0,1\}^*$	→	MOŽNO ODSIMULOVAŤ NA UNIVERZÁLNOM DTS U, AKCEPTOR, 3 PP → 1 PP PRIEST. $\max\{\lceil \log_2 t\rceil S(\lvert y\rvert), \lvert x\rvert\}$ VST. AB. = PRAC. AB. = $\{0,1\}$



SIMULÁCIA NA 1. A 2. PP ZABERIE PRIESTOR NAJVIAC $|x|$
NA 3. PP NAJVIAC $\lceil \log_2 t\rceil S(|y|)$

$\Rightarrow$ SPLÁCNUTÍM NA 1 PP DOSTÁVAME 1 PÁSKOVÝ UNIV. DTS.

$\boxed{\text{VETA}}$ O PRIESTOROVEJ HIERARCHII

$S_1, S_2 : \mathbb{N} \to \mathbb{N}$ FCIE. $S_1(n) \geq \log_2 n$ $S_2(n) \in \omega(S_1(n))$, S_2 PRIESTOROVO KONŠTR.	→	$\exists L \in$ DSPACE$(S_2(n)) \setminus$ DSPACE$(S_1(n))$		VYROBÍME M DTS AKC., 1 PP, $\{0,1\}^*$ PRIESTOR $S_2(n)$ OD KAŽDÉHO STROJA PRAC. V PRIEST. $S_1(n)$ SA LÍŠI ASPOŇ NA 1 VST.

VEZMIME $x \in \{0,1\}^*$ GÖDELOVE ČÍSLA VŠETKÝCH DTS AKCEPTOROV 1 PP, VST. AB. = $\{0,1\}$, PRAC AB. ... t SYMBOLOV

$10x$, $110x$, $1110x$, ... KÓDUJÚ TEN ISTÝ DTS AKO x

VYROBÍME M DTS AKC., 1PP, VST. AB. = PRAC. AB. = $\{0,1\}$

NA VSTUPE x, $|x| = n$: (1) OZNAČÍ $S_2(n)$ BUNIEK NA SVOJEJ P.P.

(2) SIMULUJE M_x NA VSTUPE x, M PRIJME $x \Leftrightarrow$

(i) SIMULÁCIA PREBEHNE VO VYHRADENOM PRIESTORE

(ii) M_x ZASTAVÍ A ODMIETNE x

$L := L(M)$

(α) $L \in$ DSPACE$(S_2(n))$. (β) NECH $L \in$ DSPACE$(S_1(n)) \Rightarrow \exists$ DTS $\hat{M}$ AKC., k PP, PRAC. AB. t SYM.,
⇝ $\boxed{\text{PREROBÍME NA DTS } M_x\text{, 1PP, PR. } S_1(n)}$, KTORÝ VŽDY ZASTAVÍ (#KONFIGURÁCIÍ, POČÍTAM KROKY NA NOVEJ PP)
⇝ $\bar{x} := 1^i 0x$ TAK, ABY M NA VSTUPE $\bar{x}$ NEVYLIEZOL Z PR. $S_2(|\bar{x}|)$, $\max\{\lceil \log_2 t\rceil S_1(\bar{x}), |x|\} \leq S_2|\bar{x}|$

22.06.2009 Mo
PETER ČERNO

NTIN063 SLOŽITOST II - SKÚŠKA

$\boxed{f \text{ JE ČAS. KONŠTR.}}$ ⇔ f JE VTČ. V ČASE $O(f)$ $\boxed{\Rightarrow}$
f JE VTČ. V PRIESTORE $O(f)$ ⇔ $\boxed{f \text{ JE PRIEST. KONŠTR.}}$

X = GÖDELOVO ČÍSLO $\in \{0,1\}^*$ M_x DTS AKCEPTOR, 2 PP ČAS $T(n)$ VSTUP. ABECEDA = $\{0,1\}$ PRAC. ABECEDA ... t SYMBOLOV	+	DATA $y \in \{0,1\}^*$	→ MOŽNO ODSIMULOVAŤ NA UNIVERZÁLNOM DTS U, AKCEPTOR, 4 PP ČAS $5|x| \cdot T(|y|)$ VST. AB. = PRAC. AB. = $\{0,1\}$

U VYZERÁ TAK ISTO AKO PREDTÝM, IBA TERAZ 3. A 4. PP ≡ PREKÓDOVANÁ 1. A 2. PP M_x

INICIALIZÁCIA: $2|x|$ KROKOV (SKOPÍROVANIE X, NÁVRAT HLÁV NA 1. A 2. PP)
SIMULÁCIA: 1 KROK SIM. M_x ≡ $3|x|$ KROKOV U

VETA O ČASOVEJ HIERARCHII

$\boxed{\begin{array}{l} T_1, T_2 : \mathbb{N} \to \mathbb{N} \text{ FCIE.} \\ T_2(n) \in \omega(T_1(n) \cdot \log T_1(n)) \\ T_2 \text{ ČASOVO KONŠTRUOVATEĽNÁ} \end{array}}$ → $\boxed{\begin{array}{l} \exists L \in \\ DTIME(T_2(n)) \setminus \\ DTIME(T_1(n)) \end{array}}$

VYROBÍME M DTS AKC., 4PP + PÁSKY NA SIMULÁCIU T_2, ČAS. $T_2(n)$, OD ∀ DTS $\in T_1(n)$ SA LÍŠI ASP. NA 1 VST.

VEZMIME $x \in \{0,1\}^*$ GÖDELOVE ČÍSLA VŠETKÝCH DTS AKC., 2PP, VST. AB. = $\{0,1\}^*$
10x, 110x, 1110x, ... KÓDUJÚ TEN ISTÝ DTS AKO X

VYROBÍME M NA VSTUPE X:
(1) NA EXTRA PÁSKACH SIMULUJE ČAS. KONŠTR. T_2
(2) PARALELNE NA 4 PÁSKACH SIMULUJE BEH M_x NA VSTUPE X
(a) AK SIMULÁCIA NEDOBEHNE V ČASE $T_2(|x|)$ ⇒ ODMIETNI
(b) AK DOBEHNE ⇒ M PRIJME X ⇔ M_x ODMIETNE X

$L := L(M)$

(A) $L \in DTIME(T_2(n))$ (B) NECH $L \in DTIME(T_1(n))$ ⇝ DTS $\hat{M}$ V ČASE $T_1(n)$
⇝ 2-PÁSKOVÝ DTS $\hat{M}$ V ČASE $c\,T_1(n) \log T_1(n)$ ⇝ M_x
HĽADÁME $\bar{x}$: $5|x| \cdot T_1(|\bar{x}|) \cdot \log T_1(|\bar{x}|) \leq T_2(|\bar{x}|)$
⇒ SIMULÁCIA $M_{\bar{x}}$ NA M NA VSTUPE $\bar{x}$ SA ZMESTÍ DO $T_2(|\bar{x}|)$ KROKOV ...

VETA O VZŤAHOCH

(a) $NTIME(f(n)) \subseteq DSPACE(f(n))$

(b) $LENSPACE(f(n)),\ f(n) \geq \log_2 n \Rightarrow \exists c_2 > 0 : LEDTIME(c_2^{f(n)})$

(a)

NTS M, k PP ČAS f(n)	⇝	DTS M', (k+1) PP PRIESTOR f(n)

NA (k+1). PÁSKE JE KÓD VYBRANEJ VETVY $(x_1, \dots, x_{f(n)})$

NA ŽIADNEJ PP NEZABERIEME VIAC AKO $f(n)$ SYMBOLOV

(b)

NTS M, 1 PP PRIESTOR f(n) PRAC. AB... t SYM.	⇝	GRAF KONFIGURÁCII M $\lvert V\rvert \leq c^{f(n)}$, $\lvert E\rvert \leq rc^{f(n)}$	⇝	DTS M' 2 PP

POČET KONFIGURÁCII V PRIESTORE $f(n)$:

$$\underset{\#\text{ STAVOV}}{s} \cdot \underset{\text{POZÍCIA VST. HLAVY}}{(n+1)} \cdot \underset{\text{POZÍCIA PRAC. HLAVY}}{f(n)} \cdot \underset{\#\text{ OBSAHOV PP}}{t^{f(n)}} \leq c^{f(n)}$$

$(f(n) \geq \log_2 n)$

1. VYGENERUJE POPIS G

$\boxed{\text{KONF.}}$ SUSED 1 SUSED 2 ...

...

$O(f(n) \cdot c^{f(n)})$

2. DEPTH-FIRST S. POTREBUJEME 2. PÁSKU

PRÁCA NA VRCHOL: $O(f(n))$, NA HRANU $O(f(n) \cdot c^{f(n)})$

CELKOVÁ PRÁCA $\lvert V\rvert \cdot O(f(n)) + \lvert E\rvert \cdot O(f(n) \cdot c^{f(n)}) \leq c_2^{f(n)}$

VETA SAVIČ

$S: \mathbb{N} \to \mathbb{N}$ $S(n) \geq \log_2 n$ S VYSLITEĽNÁ V LIN. PR.	→	$NSPACE(S(n)) \subseteq$ $\subseteq DSPACE((S(n))^2)$

NTS M PRIESTOR S(n)	⇝	M MÁ NAJVIAC $c^{S(n)}$ KONF. M PRIJÍMA x ⇒ ∃ VÝPOČET DĹŽKY $\leq 2^{\log_2 c \cdot S(n)}$

$I_1 \xrightarrow{i} I_2 \equiv$ Z KONF. I_1 DO KONF I_2 ZA NAJVIAC $\boxed{2^i}$ KROKOV

foreach PRIJÍMAJÚCA KONF. I do
  if TEST$(I_0, I, \log_2 c \cdot S(n))$ then accept
reject (VEĽKOSŤ AŽ $\leq kS(n)$) $\times$ ($\log_2 c\ S(n)$) $= O(S^2(n))$

TEST(I_1, I_2, i)
$i=0$: $(I_1 = I_2) \vee (I_1 \xrightarrow{0} I_2)$
$i>0$: $(I_1, I', i-1)$ & $(I', I_2, i-1)$

22.06.2009 M.
PETER ČERNO

NTIN063 SLOŽITOST II - SKÚŠKA

PLATÍ AJ PRE NTIME, DTIME

LEMMA TRANSLAČNÁ (NSPACE, DSPACE)

S_1, S_2, f PRIESTOROVO KONŠTR. FCIE., $S_2(n) \geq n$, $f(n) \geq n$

$\boxed{NSPACE(S_1) \subseteq NSPACE(S_2)} \Rightarrow \boxed{NSPACE(S_1 \circ f) \subseteq NSPACE(S_2 \circ f)}$

$L_1 \in NSPACE(S_1(f(n))) \rightsquigarrow$ NTS M_1, PRIJÍMA L_1 V PRIESTORE $S_1(f(n))$

$L_2 := \{ x \cdot \$^i \mid M_1$ PRIJME x V PRIESTORE $S_1(|x| + i) \}$

SKONŠTRUUJEME NTS M_2 PRIJÍMAJÚCI L_2 V PRIESTORE $S_1(n)$

$\curvearrowright$) PRE $i := f(|x|) - |x|$: $x \in L_1 \Leftrightarrow x . \$^i \in L_2$

EXISTUJE NTS M_3 ROZPOZNÁVAJÚCI L_2 V PRIESTORE $S_2(n)$

NTS $M_3 \rightsquigarrow$ NTS M_4 ROZPOZNÁVAJÚCI L_1 V PRIESTORE $S_2(f(n))$
(SIMULUJE PRÁCU M_3 NAD VSTUPOM $x . \$^i$ PRE $i := f(|x|) - |x|$)

VETA O NEDETERMINISTICKEJ PRIEST. HIERARCHII

$r \geq 1$, $\varepsilon > 0 \Rightarrow \boxed{NSPACE(n^r) \subsetneq NSPACE(n^{r+\varepsilon})}$

$r \leq \frac{s}{t} < \frac{s+1}{t} \leq r + \varepsilon$

PRE SPOR PREDPOKL. $NSPACE(n^{\frac{s+1}{t}}) \subseteq NSPACE(n^{\frac{s}{t}})$.

$S_1(n) := n^{\frac{s+1}{t}}$, $S_2(n) := n^{\frac{s}{t}}$, $f(n) := n^{(s+i).t}$ $i = 0, 1, \ldots, s$

PLATÍ AJ PRE DTIME

VETA BORODINOVA O MEDZERÁCH

NEBUDE PRIESTOROVO KONŠTRUOVATEĽNÁ

$\boxed{g(n) \geq n \text{ REKURZÍVNA}} \rightarrow \boxed{\begin{array}{l}\exists\, S(n) \text{ RASTÚCA REKURZÍVNA:} \\ DSPACE(S(n)) = DSPACE(g(S(n)))\end{array}}$

$M_1, M_2, \ldots$ OČÍSLOVANIE $\forall$ DTS (GÖDELOVO ČÍSLO)

$S_i(n) \ldots$ MAXIMÁLNY POČET BUNIEK POUŽITÝCH NA PÁSKACH M_i PRE $|x| = n$

CIEĽ: RASTÚCA REKURZÍVNA $S(n)$:

(*) $\forall k$: BUĎ: $S_k(n) \leq S(n)$ SKORO VŠADE
ALEBO: $g(S(n)) < S_k(n)$ NEKONEČNE ČASTO

$L \in DSPACE(g(S(n))) \rightsquigarrow$ DTS M_k, $\forall n$ $S_k(n) \leq g(S(n))$

$\overset{(*)}{\Rightarrow}$ $S_k(n) \leq S(n)$ SKORO VŠADE $\rightsquigarrow$ DTS M' ROZPOZNÁVAJÚCI L, PRIESTOR $S(n)$

KONŠTRUKCIA $S(n)$: TAK, ABY $\forall i \in \{1,\dots,n\}: S_i(n) \notin (S(n), g(S(n))\rangle$

$j := S(n-1)+1$ ($S(0):=0$, S JE RASTÚCA)

SPOČÍTAME $g(j)$ (g JE REKURZÍVNA)

PRE KAŽDÉ $i \in \{1,\dots,n\}$ SA PRESVEDČÍME, ŽE $\overbrace{S_i(n) \notin (j, g(j)\rangle}^{\text{REKURZÍVNA ZÁLEŽITOSŤ}}$

AK PRE NEJAKÉ i: $S_i(n) \in (j, g(j)\rangle$,

POLOŽÍME $j := S_i(n)$ A ITERUJEME (NAJVIAC n ITERÁCII)

$S(n) := j$

VEZMIME ĽUBOVOĽNÉ k

$\forall n \geq k$ M_k SA NACHÁDZA MEDZI $M_1, \dots, M_n$, TJ. $S_k(n) \notin (S(n), g(S(n))\rangle$

BUĎ NASTANE $g(S(n)) < S_k(n)$ NEKONEČNE VEĽA KRÁT

ALEBO IBA KONEČNE VEĽA KRÁT $\Rightarrow$ $S_k(n) \leq S(n)$ SKORO VŠADE

DÔSLEDOK: EXISTUJE REKURZÍVNA $h(n)$: $NSPACE(h(n)) \subseteq DTIME(h(n))$

$L \in NSPACE(f(n)) \Rightarrow \exists c_L : L \in DTIME(c_L^{f(n)}) \Rightarrow L \in DTIME(f(n)^{f(n)})$

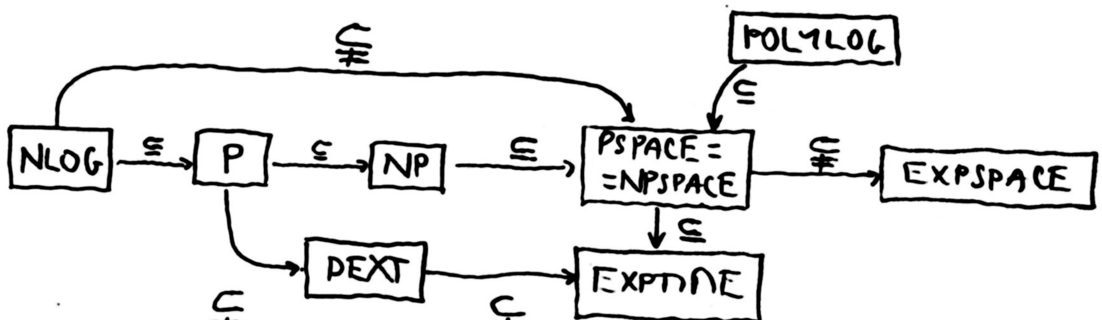
$h(n)$ JE ZARUČENÁ ČASOVOU VERZIOU BOR. VETY PRE $g(n) = n^n$.

VETA BLUMOVA

r(n) REKURZÍVNA $\longrightarrow$ $\exists$ REKURZÍVNY JAZYK L: PRE ĽUBOVOĽNÚ DTS M_i ROZPOZNÁVAJÚCU L V PRIESTORE $S_i(n)$ $\exists$ DTS M_j ROZP. L V PR. $S_j(n)$: $r(S_j(n)) \leq S_i(n)$ SKORO VŠADE

EXISTUJE AJ ČASOVÁ VERZIA

TRIEDY:
- PRIESTOR: LOG, NLOG, POLYLOG, PSPACE, NPSPACE, EXPSPACE
- ČAS: P, NP, DEXT, NEXT, EXPTIME, NEXPTIME



23.06.2009 Tu
PETER ČERNO

NTIN063 SLOŽITOST II - SKÚŠKA

$L_1 \leq_T L_2 \Leftrightarrow \exists$ DTS M, POL. ČAS. : $L_1 = L(M, L_2)$
$L_1 \leq_{NP} L_2 \Leftrightarrow \exists$ NTS M, POL. ČAS. : $L_1 = L(M, L_2)$
$P(A)$, $P(C)$, $NP(A)$, $NP(C)$

POLYNOMIÁLNA HIERARCHIA $PH = \bigcup_{k \geq 0} \Sigma_k$

$\boxed{\text{VETA}}$ $PH \subseteq PSPACE$

INDUKCIOU, $PSPACE(PSPACE) \subseteq PSPACE$

$\Sigma_k, \Pi_k, \Delta_k$

$\exists C$ ... $A \in \exists C \Leftrightarrow \exists B \in C$ A p : $x \in A \Leftrightarrow \exists^{p(|x|)} y : \langle x, y \rangle \in B$
$\forall C$ ... $A \in \forall C \Leftrightarrow \exists B \in C$ A p : $x \in A \Leftrightarrow \forall^{p(|x|)} y : \langle x, y \rangle \in B$
C UZAVRETÁ NA ZDVOJOVANIE : $A \in C \Rightarrow B = \{\langle x, y \rangle, x \in A\} \in C$

$\boxed{\text{VETA}}$ $co\text{-}\exists C = \forall(co\text{-}C) \equiv A \in \exists C \Leftrightarrow \bar{A} \in \forall(co\text{-}C)$

C UZAVRETÁ NA ZDVOJOVANIE $\Rightarrow C \subseteq \exists C, \forall C$

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

$\boxed{\text{VETA}}$ (a) $\exists P = NP$ (b) $\forall P = co\text{-}NP$

$$\left.\begin{array}{llll} \text{(c)} & \exists \Sigma_k = \Sigma_k & \text{(d)} & \forall \Pi_k = \Pi_k \\ \text{(e)} & \exists \Pi_k = \Sigma_{k+1} & \text{(f)} & \forall \Sigma_k = \Pi_{k+1} \end{array}\right\} k > 0$$

(a) ZREJMÉ (b) $\forall P = \forall co\text{-}P = co\text{-}\exists P = co\text{-}NP$

(c) $\subseteq$) $A \in \exists \Sigma_k \Rightarrow \exists B \in \Sigma_k, p : x \in A \Leftrightarrow \exists^{p(|x|)} y : \langle x, y \rangle \in B$
$B \in NP(\Sigma_{k-1}) \rightsquigarrow B = L(M_1, D) \rightsquigarrow A = L(M_2, D)$

(d) $\forall \Pi_k = \forall co\text{-}\Sigma_k = co\text{-}\exists \Sigma_k = co\text{-}\Sigma_k = \Pi_k$

(c) $\subseteq$) $L \in \exists\Pi_k \rightsquigarrow B \in \Pi_k, p \rightsquigarrow$ NTS $M : L = L(M, B) \rightsquigarrow L \in NP(\Pi_k)$

$\supseteq$) $\Sigma_{k+1} \subseteq \exists\Pi_k$ INDUKCIA PODĽA k

$A \in \Sigma_{k+1} = NP(\Sigma_k) \rightsquigarrow$ NTS M POL., $B \in \Sigma_k : A = L(M, B)$

CIEĽ: $A \in \exists\Pi_k$, TJ. $\exists C \in \Pi_k$, POL. p : $x \in A \Leftrightarrow \exists^{p(|x|)} y : \langle x, y\rangle \in C$

$x \in A \Leftrightarrow \exists$ PRIJÍMAJÚCI VÝPOČET M S ORÁKULOM B

$x \in A \Leftrightarrow \exists$ POL. VEĽKÝ CERTIFIKÁT y KÓDUJÚCI VÝPOČET M (POL. p)

$t_1, \dots, t_i$ SÚ ZODPOVEDANÉ ÁNO, $f_1, \dots, f_j$ ... NIE

DOKÁŽME, ŽE $C := \{\langle x, y\rangle \mid x \in A \wedge y$ JE KÓD PRIJÍM. VÝP. $\} \in \Pi_k$

AKO OVERÍME, ŽE $\langle x, y\rangle \in C$?

SPUSTÍME STROJ M NA VSTUPE x A SIMULUJEME JEHO CHOD S KÓDOM y (DETERMINISTICKÁ ZÁLEŽITOSŤ)

V STAVE DOTAZ:

(a) NA DOTAZOVACEJ PÁSKE JE $f_\ell \in \overline{B} \in \Pi_k$ ... TO JE OK

(b) $t_\ell \in B \in \Sigma_k$ ... PROBLÉM

$\Sigma_k \subseteq \exists\Pi_{k-1} \Rightarrow \exists D \in \Pi_{k-1}$, POL. q :

$t_\ell \in B \Leftrightarrow \exists^{p(|t_\ell|)} u : \langle t_\ell, u\rangle \in D$

$\Rightarrow$ OVERENIE $t_\ell \in B$ MÔŽME POMOCOU NTS S ORÁKULOM $D \in \Pi_{k-1}$

NAKONIEC ODPOVIEME NAOPAK $\boxed{2}$

$\boxed{\text{PREVODITEĽNOSŤ}}$ V POL. ČASE ... DTS TRANSDUCER, POL. ČAS — VŽDY ZASTAVÍ

V LOG. PRIESTORE ... DTS TRANS., POL. PRIESTOR

$\boxed{\text{VETA}}$ $\boxed{L\ \text{P-ÚPLNÝ}} \Rightarrow \boxed{L \in LOG \Rightarrow LOG = P}$

$L' \in P \rightsquigarrow M'$ LOG-SPACE TRANSDUCER $L' \xrightarrow{x \rightsquigarrow y,\ |y| \le |x|^k} L$, M'' ROZPOZNÁVA $L \in LOG$

STROJE NEMÔŽEME ZREŤAZIŤ PRIR. SPÔSOBOM

STROJ M' SPÚŠŤAME VŽDY, KEĎ POTREBUJEME ZNAK y

$\boxed{\text{VETA}}$ $\boxed{L\ \text{PSPACE-ÚPLNÝ}} \Rightarrow \boxed{L \in NP \Rightarrow NP = PSPACE}$

<u>QBF</u> QBF $\in$ PSPACE (PROCEDÚRA EVAL), <u>QBF</u> JE PSPACE-ÚPLNÝ

23.06.2009 Tu
PETER ČERNO

NTIN063 SLOŽITOST II - SKÚŠKA

1) VETA O LIN. PRIESTOROVEJ KOMPRESII
2) VETA O REDUKCII POČTU PÁSOK PRE PRIEST. ZLOŽITOSŤ
3) VETA O REDUKCII POČTU PÁSOK PRE ČAS. ZLOŽITOSŤ I, II
4) VETA O LIN. ZRÝCHLENÍ I, II
5) LEMMA O ČAS. KONŠTR.
6) VETA O ČAS. KONŠTR.
7) VETA O PRIEST. KONŠTR.
8) UNIV. TUR. STROJ PRE PRIEST. ZL. / ČAS ZLOŽ.
9) VETA O PRIEST. HIERARCHII
10) VETA O ČAS. HIERARCHII
11) VETA O VZŤAHOCH
12) VETA SAVIČ
13) VETA TRANSAKČNÁ
14) VETA O NEDET. PR. HIERARCHII
15) VETA BORODINOVA O MEDZERÁCH
16) VETA BLUMOVA
17) TRIEDY PRIEST. / ČAS. ZLOŽITOSTI
18) POLYNOMIÁLNA HIERARCHIA
19) PREVODITEĽNOSŤ

3/4

23.06.2009 Tu
PETER ČERNO

1) $\boxed{\text{k-páskový DTS } M \quad \text{PRIESTOR } S(n)} \overset{r>1}{\rightsquigarrow} \boxed{\text{k-páskový DTS } M' \quad \text{PRIESTOR } \lceil \frac{1}{r} S(n) \rceil}$ VETA O LIN. PRIEST. KOMPRESII

2) $\boxed{\text{k-páskový DTS } M \quad \text{PRIESTOR } S(n)} \rightsquigarrow \boxed{\text{1-páskový DTS } M' \quad \text{PRIESTOR } S(n)}$ VETA O REDUKCII POČTU PÁSOK PRE PRIEST. ZLOŽITOSŤ

3) $\boxed{\text{k-PP DTS } M \quad \text{ČAS } T(n)} \rightsquigarrow \boxed{\text{1-PP DTS } M' \quad \text{ČAS } c.(T(n))^2}$ VETA O REDUKCII POČTU PÁSOK PRE ČASOVÚ ZLOŽITOSŤ

$\rightsquigarrow \boxed{\text{2-PP DTS } M' \quad \text{ČAS } c.T(n).\log T(n)}$

4) $\boxed{\text{k-PP DTS } M \quad \text{ČAS } T(n) \in \omega(n)} \overset{c>0}{\rightsquigarrow} \boxed{(k+1)\text{-PP DTS } M' \quad \text{ČAS } cT(n)}$ VETA O LIN. ZRÝCHLENÍ

$\text{ČAS } T(n) = cn,\ c \geq 1 \overset{\varepsilon>0}{\rightsquigarrow} \text{ČAS } (1+\varepsilon)T(n)$

5) $f_1 + f_2$, f_2 ČAS. KONŠTR.
$\boxed{\exists \varepsilon>0, n_0}$ $f_1(n) \geq \boxed{(1+\varepsilon)} f_2(n) + \boxed{\varepsilon} n$ $\Rightarrow f_1$ ČAS. KONŠTR. LEMMA O ČAS. KONŠTR.

6) $f(n) \geq (1+\varepsilon)n$ f JE ČAS. KONŠTR. $\Leftrightarrow$ f JE VYČ. V LIN. ČASE

7) f JE PRIEST. KONŠTR. $\Leftrightarrow$ f JE VYČ. V LIN. PRIESTORE

8) PRIEST. ZL.

GÖDELOVE ČÍSLO x
M_x DTS, 1 PP
VST. AB. = $\{0,1\}$
PRAC. AB. = t SYM.
PRIESTOR $S(n)$

DATA + $y \in \{0,1\}^*$ $\rightsquigarrow$

UNIVERZÁLNY DTS U
3 PP $\rightarrow$ 1 PP
VST. AB. = PRAC. AB. = $\{0,1\}^*$
PRIESTOR $\max\{\lceil \log t \rceil S(|y|), |x|\}$

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

2 PP

ČAS $T(n)$

4 PP

ČAS $5|x|.T(|y|)$

9) $\boxed{\begin{array}{l} S_1, S_2 : \mathbb{N} \to \mathbb{N} \\ S_1(n) \geq \log_2 n \\ S_2(n) \in \omega(S_1(n)) \\ S_2(n) \text{ PRIEST. KONŠTR.} \end{array}} \to \boxed{\begin{array}{l} \exists L \in \\ DSPACE(S_2(n)) \setminus \\ DSPACE(S_1(n)) \end{array}}$

VETA O PRIEST. HIERARCHII

10) $\boxed{\begin{array}{l} T_1, T_2 : \mathbb{N} \to \mathbb{N} \\ T_2 \in \omega(T_1(n) \log T_1(n)) \\ T_2 \text{ ČASOVO KONŠTR.} \end{array}} \to \boxed{\begin{array}{l} \exists L \in \\ DTIME(T_2(n)) \setminus \\ DTIME(T_1(n)) \end{array}}$

VETA O ČASOVEJ HIERARCHII

11) $NTIME(f(n)) \subseteq DSPACE(f(n))$

$L \in NSPACE(f(n)),\ f(n) \geq \log_2 n \Rightarrow \exists c_L > 0$

$L \in DTIME(c_L^{f(n)})$

VETA O VZŤAHOCH

12) $\boxed{\begin{array}{l} S(n) \geq \log n \\ S(n) \text{ ČASOVO KONŠTR.} \end{array}} \to \boxed{NSPACE(S(n)) \subseteq DSPACE((S(n))^2)}$

SAVIČOVA VETA

13) S_1, S_2, f PRIEST. KONŠTR.

$S_2(n) \geq n, \quad f(n) \geq n$

TRANSLAČNÁ VETA

$\Rightarrow \boxed{NSPACE(S_1(n)) \subseteq NSPACE(S_2(n))}$

$\to \boxed{NSPACE(S_1(f(n))) \subseteq NSPACE(S_2(f(n)))}$

14) $r \geq 1, \quad \varepsilon > 0$

$\Rightarrow \boxed{NSPACE(n^r) \subsetneq NSPACE(n^{r+\varepsilon})}$

VETA O NEDETERMINISTICKEJ PRIEST. HIERARCHII

23.06.2009 Tu
PETER ČERNO

BORODINOVA VETA O MEDZERÁCH

15) $\boxed{\begin{array}{c} g(n) \geq n \\ \text{REKURZÍVNA} \end{array}} \longrightarrow \boxed{\begin{array}{c} \exists \text{ RASTÚCA REKURZÍVNA } S(n) \\ DSPACE(S(n)) = DSPACE(g(S(n))) \end{array}}$

BLUMOVA VETA

16) $\boxed{\begin{array}{c} r(n) \\ \text{REKURZÍVNA} \end{array}} \rightarrow \boxed{\begin{array}{l} \exists \text{ REKURZÍVNY JAZYK } L: \\ \forall M_i \text{ ROZPOZN. } L \text{ V PRIESTORE } S_i \\ \exists M_j \text{ -||- } S_j : r(S_j(n)) \leq S_i(n) \text{ SKORO VŠADE} \end{array}}$

17) PRIEST.: LOG, NLOG, POLYLOG, PSPACE, NPSPACE, EXPSPACE
ČAS: P, NP, DEXT, NEXT, EXPTIME

$$\begin{tikzcd}
 & & & POLYLOG \arrow[d, "\subseteq"] & \\
NLOG \arrow[r, "\subseteq"] \arrow[rrr, bend left, "\subsetneq"] & P \arrow[r, "\subseteq"] \arrow[d, "\subsetneq"'] & NP \arrow[r, "\subseteq"] & PSPACE = NPSPACE \arrow[r, "\subsetneq"] \arrow[d, "\subseteq"] & EXPSPACE \\
 & DEXT \arrow[rr, "\subsetneq"'] & & EXPTIME &
\end{tikzcd}$$

18) $\Sigma_0 = \Pi_0 = \Delta_0 = P$

$\Sigma_{k+1} = NP(\Sigma_k)$

$\Pi_{k+1} = co\text{-}NP(\Sigma_k)$

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

$PH = \bigcup_{k\geq 0} \Sigma_k \ (= \bigcup_{k\geq 0} \Pi_k = \bigcup_{k \geq 0} \Delta_k) \subseteq PSPACE$

$P(P) = P, \quad NP(P) = NP$

$\Sigma_1 = NP, \quad \Pi_1 = co\text{-}NP, \quad \Delta_1 = P, \quad \Pi_k = co\text{-}\Sigma_k$

$\Sigma_{k+1} = NP(\Pi_k), \quad \Pi_{k+1} = co\text{-}NP(\Pi_k)$

$\Sigma_{k+1} = NP(\Delta_{k+1}), \quad \Pi_{k+1} = co\text{-}NP(\Delta_{k+1})$

$\exists \mathcal{C}$, $\forall \mathcal{C}$, $co\text{-}\exists \mathcal{C} = \forall (co\text{-}\mathcal{C})$

$\exists P = NP$, $\forall P = co\text{-}NP$

$\exists \Sigma_k = \Sigma_k$, $\forall \Pi_k = \Pi_k$

$\exists \Pi_k = \Sigma_{k+1}$ $\forall \exists_k = \Pi_{k+1}$

$\Delta_k = co\text{-}\Delta_k$

$P(\Delta_k) = \Delta_k$

$\Sigma_k \cup \Pi_k \subseteq \Delta_{k+1}$

$\Delta_k \subseteq \Sigma_k \cap \Pi_k$

$\Sigma_k \subseteq \Pi_k \Rightarrow \Sigma_k = \Pi_k$

$\Pi_k \subseteq \Sigma_k \Rightarrow \Sigma_k = \Pi_k$

(19) PREVODITEĽNOSŤ V POL. ČASE, LOG. PRIESTORE

$\mathcal{C}$-ÚPLNOSŤ VZHĽADOM K ...

P-ÚPLNOSŤ, NP-ÚPLNOSŤ, PSPACE-ÚPLNOSŤ, ...

$\exists$ L P-ÚPLNÝ $\in$ LOG $\Rightarrow$ LOG = P

$\exists$ L PSPACE-ÚPLNÝ $\in$ NP $\Rightarrow$ NP = PSPACE