Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Vybrané kapitoly z výpočetní složitosti II (složitost, komunikační složitost)

Peter Černo, 2011
petercerno@gmail.com

Garant: Mgr. Michal Koucký Ph.D.
E-mail: Michal.Koucky@mff.cuni.cz
Domácí stránka: `http://www.math.cas.cz/~koucky/`

Anotace: Obsahem této přednášky jsou pokročilé partie z výpočetní složitosti. Každý semestr bude věnován jinému tématu. Mezi plánovaná témata patří oblast náhodnosti a pseudonáhodných generátorů, komunikační složitost a interaktivní protokoly, samoopravné kódy a jejich užití ve složitosti, dolní odhady, expandery a jejich použití a další. Přednáška je určena především studentům vyšších ročníků studia a doktorandům. Přednáška předpokládá základní znalosti z výpočetní složitosti, pravděpodobnosti a diskrétní matematiky.

Sylabus:

1. Náhodnost a pseudonáhodné generátory.
2. Komunikační složitost a interaktivní protokoly.
3. Samoopravné kódy.
4. Dolní odhady.
5. Expandery a jejich použití.

Literatura:

1. Sanjeev Arora and Boaz Barak: Computational Complexity: A Modern Approach (`http://www.cs.princeton.edu/theory/complexity/`)

Vybrané kapitoly z výpočetní složitosti II

Michal Koucký
<koucky@math.cas.cz>

LS 2010/2011

TIN086 - 2/1 Z, Zk

Čas konání: Pá 12:20.
Místo konání: S6

Obsahem této přednášky jsou pokročilé partie z výpočetní složitosti. Tento semestr bude věnován "klasičtějším" partiím výpočetní složitosti. Ukázali bychom některé základní, dnes již prakticky klasické výsledky, např. Todovu větu (Polynomiální hierarchie vs. #P), větu Immermana a Szelepcsényiho (NL=coNL), Reingioldovu větu (SL=L), zmínili se o pravděpodobnostních výpočtech a pseudonáhodných generátorech (Nisanův PRG), a dále bychom se věnovali základům komunikační složitosti.

Přednáška je určena především studentům vyšších ročníků studia a doktorandům. Přednáška předpokládá základní znalosti z výpočetní složitosti, pravděpodobnosti a diskrétní matematiky. Přednášku je možné si zapsat opakovaně.

Plán přednášky

- Deterministická, nedeterministická časová a prostorová hierarchie, polynomiální hierarchie
- Izolační lemma
- Todova věta
- NL=coNL
- Pseudonáhodné generátory
- SL=L
- Komunikační složitost

Literatura:

- Oded Goldreich, *Computational Complexity: A Conceptual Perspective*, Cambridge University Press 2008.
- Sanjeev Arora, Boaz Barak. *Complexity Theory: A Modern Approach.* Cambridge University Press 2008. Verze na webu http://www.cs.princeton.edu /theory/complexity/
- Eyal Kushilevitz, Noam Nisan, *Communication complexity*, Cambridge University Press 1997.

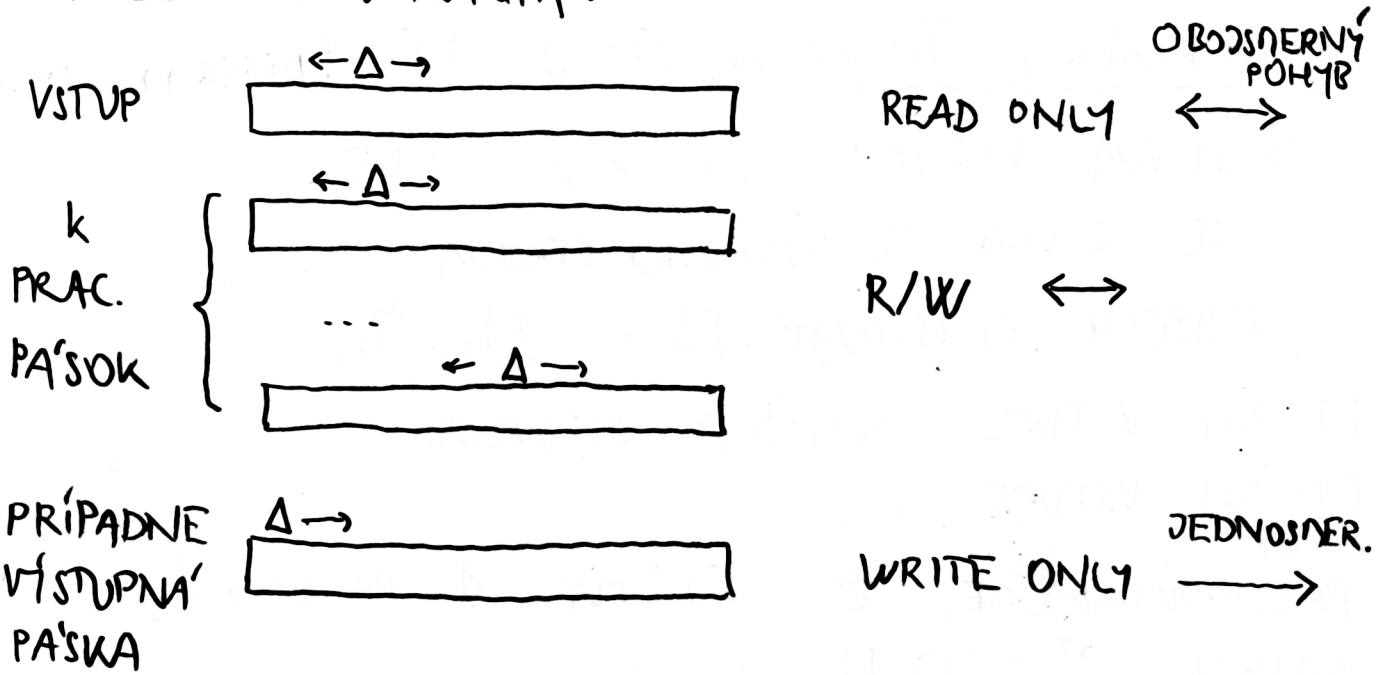
25.02.2011 Ft
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

1. ČASŤ PREDNÁŠKY:
- VETA O HIERARCHII
- IZOLAČNÁ LEMA: SAT → UNIQUE-SAT
- TODOVA VETA: $PH \subseteq P^{PP}$
- IMMERMAN-SZELEPCSÉNYI ($NL = coNL$)
- REINGOLDOVA VETA ($SL = L$)

2. ČASŤ PREDNÁŠKY:
- KOMUNIKAČNÁ ZLOŽITOSŤ

ZÁKLADNÝ VÝPOČTOVÝ MODEL: TURINGOV STROJ
- NASLEDUJÚCA VARIANTA:



ČAS VÝPOČTU: # KROKOV

PRIESTOR VÝPOČTU: # NAVŠTÍVENÝCH POLÍČOK NA PRACOVNÝCH PÁSKACH

AKO DLHO / KOĽKO PRIESTORU ATĎ. POTREBUJEME
≡ ZÁKLADNÁ OTÁZKA VÝP. ZLOŽITOSTI

CHURCH-TURINGOVA HYPOTÉZA : VŠETKO, ČO SA DÁ ALGORITMICKY SPOČÍTAŤ, SA DÁ SPOČÍTAŤ NA TS.

EFEKTÍVNA VERZIA : VŠETKO, ČO SA DÁ EFEKTÍVNE ALGORITMICKY SPOČÍTAŤ, SA DÁ EFEKTÍVNE SIMULOVAŤ NA TS ...

PROBLÉM : KVANTOVÉ POČÍTAČE ... NIE JE JASNÉ, ČI PLATÍ EFEKTÍVNA VERZIA.

ĎALŠIE MODELY : RAM, ...

UNIVERZÁLNY TURINGOV STROJ M (DETERMINISTICKÝ)

DOSTÁVA VSTUPY $\langle i, x \rangle$, KDE
i JE ČÍSLO TURINGOVHO STROJA

... MÔŽEME OČÍSLOVAŤ TS : $M_1, M_2, \ldots$

M NA VSTUPE $\langle i, x \rangle$ SIMULUJE
M_i NA VSTUPE x.

PREDPOKLADAJME, ŽE M MÁ 1 PRACOVNÚ PÁSKU, $\Sigma = \{0,1\}$.

M DOKÁŽE SIMULOVAŤ ĽUBOVOĽNÝ k-PÁSKOVÝ TURINGOV STROJ.

25.02.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

MÔŽME PREDPOKLADAŤ, ŽE AK M_i PRACUJE V ČASE $t(n)$, POTOM M PRACUJE V ČASE $O(t^2(n))$.
AK M_i PRACUJE V PRIESTORE $s(n)$, POTOM M PRACUJE V PRIESTORE $O(s(n))$.

EXISTUJE DOKONCA UNIV. TS., KT. SIMULUJE M_i V ČASE $O(t(n)\log(t(n)))$.
POTREBUJE VŠAK 2 PRAC. PÁSKY.
PRE 1 PRAC. PÁSKU JE $O(t^2(n))$ NAJLEPŠIA MOŽNÁ NEZ.

OTVORENÝ PROBLÉM: ... ČAS $O(t(n))$.

NEDETERMINISTICKÝ UNIV. TS DOKÁŽE SIMULOVAŤ V ČASE $O(t(n))$.

$DTIME(t(n))$ ... TRIEDA PROBLÉMOV (JAZYKOV) ROZHODNUTEĽNÝCH V ČASE $O(t(n))$.

$P = \bigcup_{k\geq 1} DTIME(n^k)$

$E = \bigcup_{k\geq 1} DTIME(2^{nk})$

$EXP = \bigcup_{k\geq 1} DTIME(2^{n^k})$.

$DSPACE(s(n))$ ... ... PRIESTOR $O(s(n))$.

$L = DSPACE(\log n)$, $L^2 = DSPACE(\log^2 n)$
... POLYLOGSPACE

$$PSPACE = \bigcup_{k \geq 1} DSPACE(n^k).$$

TRIVIÁLNE VZŤAHY:

$P \subseteq E \subsetneq EXP$

$L \subsetneq L^2 \subsetneq PSPACE$

$PSPACE \subseteq EXP$

$L \subseteq P$

OTVORENÝ PROBLÉM: $P \subseteq L$?

VETA O ČASOVEJ HIERARCHII

PRE ČASOVO KONŠTRUOVATEĽNÚ FUNKCIU T, A t T.Z. $t^2 \in o(T)$, $T \geq n$. PLATÍ:

$DTIME(t) \subsetneq DTIME(T)$.

DÔKAZ. ZOSTROJÍME TS M T.Z.

$L(M) \notin DTIME(T) \setminus DTIME(t)$.

M NA VSTUPE $x \in \{0,1\}^*$:

1) $n = |x|$
2) $n = \langle i, j \rangle$ ... $\langle \cdot, \cdot \rangle$ JE BIJEKCIA $\mathbb{N}^2 \leftrightarrow \mathbb{N}$
3) M SIMULUJE M_i NA x
   # KROKOV = $T(n)$
4) M SA ZACHOVÁ PRESNE NAOPAK NEŽ M_i.

25.02.2011 Fr
PETER ČERNO

NTIN086 Vybrané kapitoly z výp. složitosti II

Zrejme M pracuje v čase $O(T)$.

Ak rozhoduje $L(M) \in DTIME(t)$,
potom $\exists i$: M_i rozhoduje $L(M)$
v čase $O(t)$.

Pre dostatočne veľké j stihne
M odsimulovať M_i na vstupe x
kde $|x| = n = \langle i, j \rangle$, pretože
simulácia M_i beží v čase $O(t^2(n))$
a $t^2 \in o(T)$.

Avšak M sa zachová na vstupe x
inak než M_i, t.j. $L(M) \neq L(M_i)$. ↯ □

Veta o priestorovej hierarchii

Pre priestorovo konštruovateľnú funkciu S
a s t.ž. $s \in o(S)$, $S \geq \log n$ platí:
$DSPACE(s) \subsetneq DSPACE(S)$.

Pre nedeterministické TS ...
máme problém s negáciou!

PRE TRIEDU BPP NIE JE ZNÁMA INDEXÁCIA (ENUMERÁCIA) PRAVDEPOD. TURINGOVÝCH STROJOV ... TJ. ANI UNIVERZÁLNY (PRAVD.) TURINGOV STROJ.

NIE JE ZNÁMA VETA O HIERARCHII TYPU:

$$BPTIME(t) \subsetneq BPTIME(T)$$

... SAMOZREJME PRE $2^t < T$ PLATÍ $\subsetneq$.

NEDETERMINISTICKÉ TURINGOVE STROJE:

$x \in L(M) \Leftrightarrow \exists$ PRIJÍMAJÚCI VÝPOČET M NAD x

ČAS ... MAXIMUM CEZ VŠETKY VÝPOČTY

PRIESTOR ... —||—

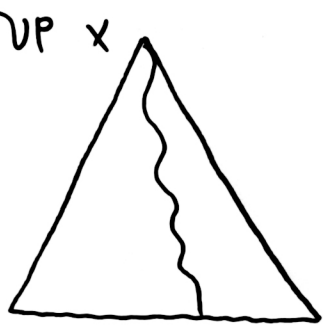
VÝSTUP ... —||—

<u>OTVORENÝ PROBLÉM</u>: $P \overset{?}{=} NP$

11.03.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. II

MINULE: VETA O HIERARCHII ... ČASOVÁ, PRIEST.



NEDETERMINISTICKÝ VÝPOČET
... ŠPECIÁLNA PÁSKA NA KT.
ZAPISUJEME ROZHODNUTIA NTS

VSTUP JE PRIJATÝ, KEĎ ASPOŇ 1 VÝPOČET PRIJME.
ČAS ... DĹŽKA CESTY ... AK JE ČASOVO KONŠTR.,
MÔŽEME STROM OHRANIČIŤ (KONŠT. HĹBKA)

NP-ÚPLNÉ PROBLÉMY:
SAT, HAM-CYCLE, 3-COLOR, ...
MOŽNO RIEŠIŤ NEDET. V POL. ČASE.

NTIME(t) = ROZHODOVACIE PROBLÉMY (JAZYKY)
RIEŠITEĽNÉ V ČASE t NA NTS.

PRE NTS S VÝSTUPNOU PÁSKOU ...
PROBLÉM S DEFINÍCIOU (RÔZNE PRÍSTUPY)

co-NTIME(t) ... DOPLNKY JAZYKOV
Z NTIME(t).

M^c ... TS S PREHODENÍM ACCEPT ↔ REJECT
$L^c = \{0,1\}^* \setminus L$.

co-NP-ÚPLNÉ PROBLÉMY : TAUT,
GRAFY BEZ HAM-CYKLU, ...

$NP = \bigcup_{k\geq 1} NTIME(n^k)$

$NE = \bigcup_{k\geq 1} NTIME(2^{kn})$

$NEXP = \bigcup_{k\geq 1} NTIME(2^{n^k})$

EXISTUJE UNIVERZÁLNÍ NTS s 2 PÁSKAMI T.Ž.
NA VSTUPE $\langle i, x\rangle$ PRIJME $\Leftrightarrow$
N_i PRIJME x. $N_1, N_2, \ldots$ JE ENUMERÁCIA
NTS... i JE KÓD POPISU N_i.
KEĎ N_i PRIJÍMA x V ČASE $t_i(|x|)$ POTOM
N PRIJÍMA $\langle i, x\rangle$ V ČASE $O(t_i^2(|x|))$
... KONŠTANTA V $O(\cdot)$ ZÁVISÍ NA i.
... PODOBNE PRE PRIESTOR.

HOMEWORK : ČAS MOŽNO SPRAVIŤ LINEÁRNY,
T.J. $O(t_i(|x|))$.

VETA O NEDET. ČASOVEJ HIERARCHII :

t, T ... ČASOVO KONŠTR.
$t^2(n+1) = o(T(n))$
POTOM $NTIME(t) \subsetneq NTIME(T)$.

11.03.2017 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. II

◁) $NP \subseteq EXP \subsetneq EEXP \subseteq NEEXP$

$EEXP = \bigcup_{k \geq 1} DTIME(2^{2^{nk}})$, PODOBNE $NEEXP$.

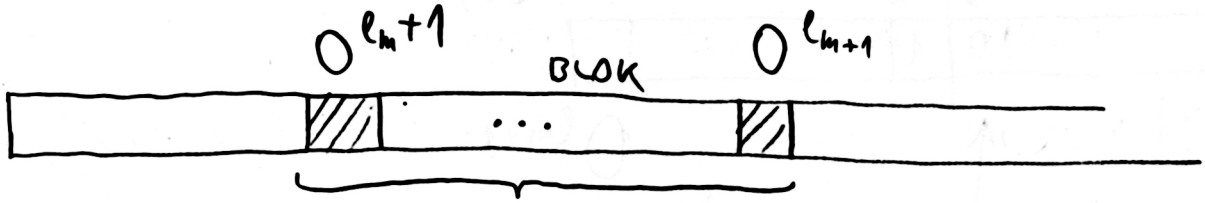
DÔKAZ. (ŽÁK) ZOSTROJÍME $L \subseteq \{0\}^*$,

$L \in NTIME(T) \setminus NTIME(t)$

MÁME PROBLÉM S NEGÁCIOU!

RIEŠI SA POMOCOU ODLOŽENEJ DIAGONALIZÁCIE.

BUDEME DIAGONALIZOVAŤ NA CELOM BLOKU REŤAZKOV (NIE LEN NA 1 VSTUPE):



$m = \langle i, j \rangle$, KDE $\langle \cdot, \cdot \rangle : \mathbb{N}^2 \xleftrightarrow{1:1} \mathbb{N}$

NA VSTUPE $x = 0^n$ NÁJDI m T.Ž.:

$l_m < n \leq l_{m+1}$ $\qquad l_m \overset{def.}{:=} 2^{2^{T(l_{m-1})}}$

ROZLOŽ: $m =: \langle i, j \rangle$

KEĎ $n < l_{m+1}$, POTOM SIMULUJ N_i (NEDETERM.)

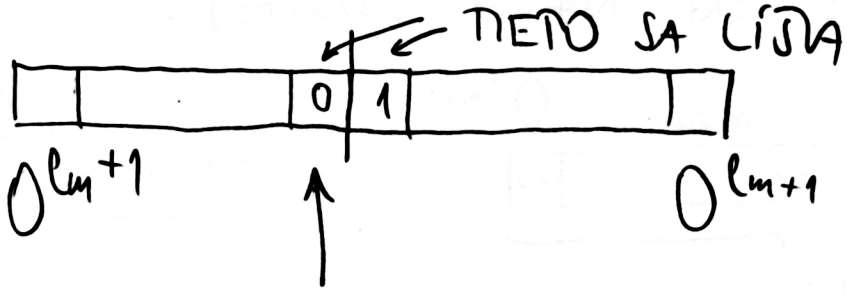
NA VSTUPE 0^{n+1} PO $T(n)$ KROKOCH SIMULÁCIE

KEĎ $n = \ell_{m+1}$, POTOM SPOČÍTAJ, ČI N_i PRIJÍMA $0^{\ell_{m+1}}$, A ZACHOVAJ SA OPAČNE.

CHCEME UKÁZAŤ, ŽE PRÍSLUŠNÝ JAZYK NIE JE V NTIME(t).

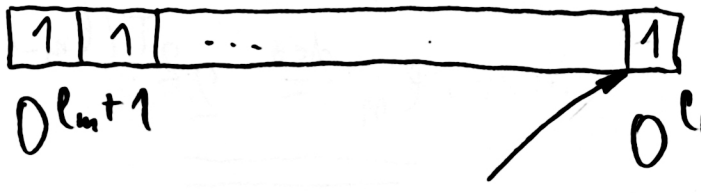
UVAŽUJME N_i PRACUJÚCI V ČASE $t(n)$ SÚ 3 MOŽNOSTI, AKO N_i ROZHODUJE ÚSEK $0^{\ell_{m+1}} \ldots 0^{\ell_{m+1}}$:

1) NIEKTORÉ SLOVÁ PRIJÍMA, NIEKTORÉ NEPRIJÍMA:



TU SA ZACHOVÁME INAK AKO N_i

2) VŠETKY SLOVÁ PRIJÍMA:



MÁME DOSŤ ČASU NA SIMULÁCIU N_i NA $0^{\ell_{m+1}} \ldots$

TU SA OPÄŤ ZACHOVÁME INAK AKO N_i

3) VŠETKY SLOVÁ ODMIETA ... PODOBNE AKO 2).

18.03.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II

BUDÚCI TÝŽDEŇ 25.03.2011 PREDNÁŠKA ODPADÁ!
08.04.: 2 PREDNÁŠKY! 12^{20}–15^{30}
DO 01.04.: ODOVZDAŤ 1. SÉRIU DOMÁCICH ÚLOH

$L \in NP \Leftrightarrow \exists L' \in P$, POLYNÓM p:

$\forall x \in \{0,1\}^*: x \in L \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)} (x,y) \in L'$

y ... SVEDOK (WITNESS)

$L \in PP \Leftrightarrow \exists L' \in P$, POLYNÓM p:

$x \in L \Leftrightarrow \exists$ ASPOŇ $2^{p(|x|)-1}$ $y \in \{0,1\}^{p(|x|)}$
TAKÝCH, ŽE $(x,y) \in L'$.

PODOBNE BPP.

POLYNOMIÁLNA HIERARCHIA Σ_k, Π_k, $k = 1, 2, \ldots$

$L \in \Sigma_k \Leftrightarrow \exists L' \in P$, POLYNÓM p:

$x \in L \Leftrightarrow \exists^{p(|x|)}_{y_1} \forall^{p(|x|)}_{y_2} \ldots Q^{p(|x|)}_{y_k} \; (x, y_1, \ldots, y_k) \in L'$.

PODOBNE Π_k.

$\Sigma_1 = NP$, $\Pi_1 = co\text{-}NP$

SAT : BOOL. FORMULA $\varphi \in SAT \Leftrightarrow$

$\exists x \in \{0,1\}^n : \varphi(x) = 1$

SAT JE NP-ÚPLNÝ VZHĽADOM K $\leq_m$.

φ JE TZV. Σ_1-KVANTIFIKOVANÁ B.F.

TJ. Σ_1-QBF.

PODOBNE Σ_2-QBF : $\exists x \in \{0,1\}^n \forall y \in \{0,1\}^n \varphi(x,y)$

... MÔŽETE DEFINOVAŤ Σ_k-SAT.

Σ_k-SAT JE Σ_k-ÚPLNÝ VZHĽADOM K $\leq_m$.

QBF ... KVANTIFIKOVANÉ BOOL. FORMULE

(NIE JE OHRANIČENÝ POČET KVANTIFIKÁTOROV)

QBF-SAT ... PSPACE-ÚPLNÝ.

$PH = \bigcup_{k \geq 1} \Sigma_k$ ... POLYN. HIERARCHIA

PLATÍ $PH \subseteq PSPACE$

PRÍKLAD: MAX-CLIQUE = { (G, m),

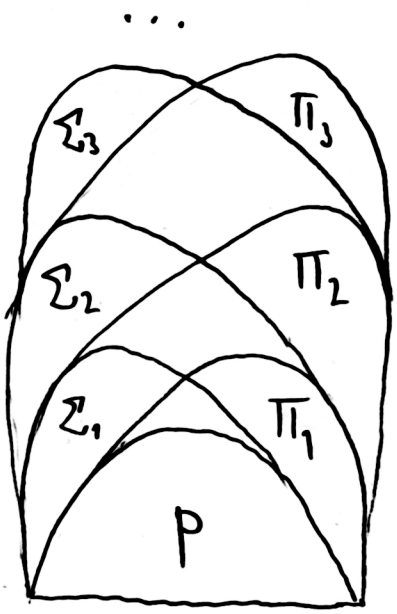
GRAF G MÁ NAJVÄČŠIU KLIKU VEĽKOSTI m }

PLATÍ MAX-CLIQUE $\in \Sigma_2 \cap \Pi_2$

AK MAX-CLIQUE $\in NP$, POTOM $NP = co\text{-}NP$.

18.03.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II



VETA : $P = NP \Rightarrow PH = P$

VETA : $\Sigma_k = \Pi_k \Rightarrow PH = \Sigma_{k+1}$

01.04.2011 Fr
PETER ČERNO

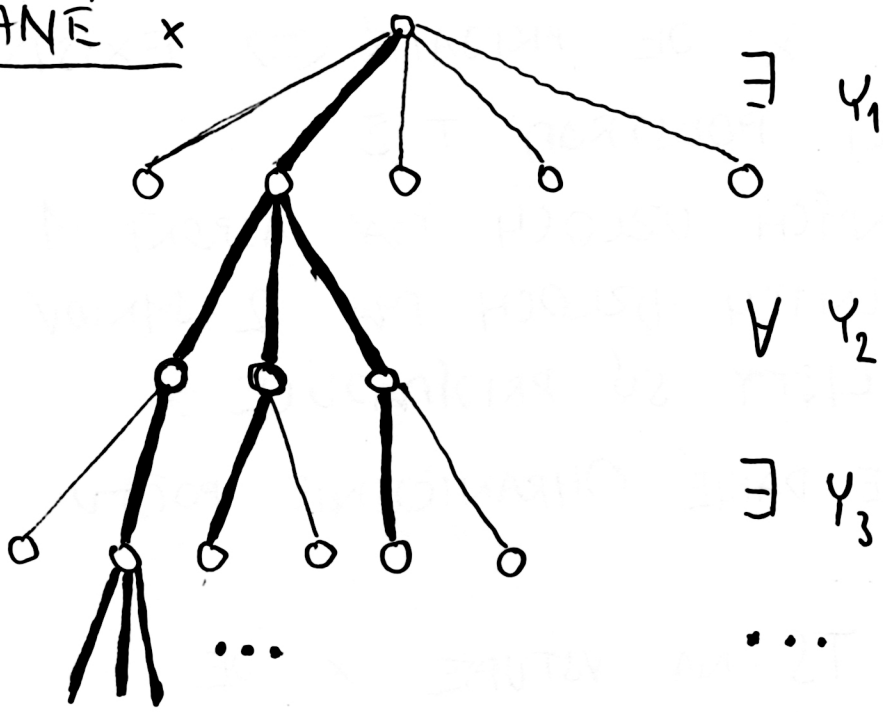
NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

MINULE SME DEFINOVALI TRIEDY Σ_k, Π_k ...

$L \in \Sigma_k \Leftrightarrow \exists L' \in P$:

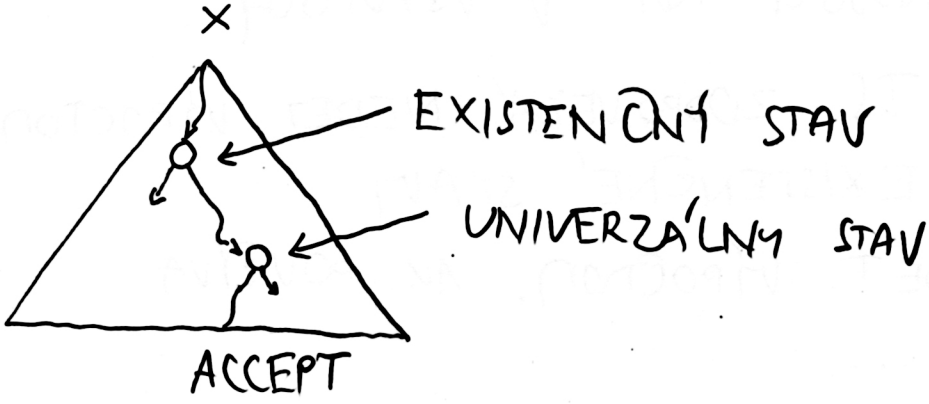
$x \in L \Leftrightarrow \exists^{p(|x|)} y_1 \forall^{p(|x|)} y_2 \dots (x, y_1, \dots, y_k) \in L'$

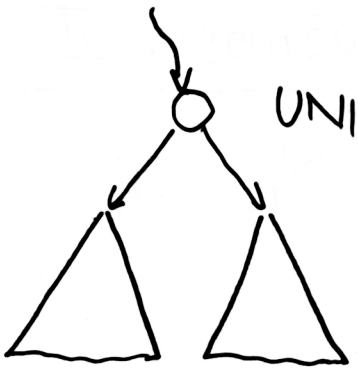
PRE DANÉ x



ZAVÁDZAJÚ SA TZV. ALTERNUJÚCE TURINGOVE STROJE ...

ROZLIŠUJEME $\leftarrow$ EXISTENČNÉ / UNIVERZÁLNE STAVY





UNIVERZÁLNY STAV

← POŽADUJEME, ABY OBA PODSTROMY BOLI PRIJÍMAJÚCE

⇒ PRIJÍMANIE x SA VYHODNOCUJE ODSPODU. x JE PRIJATÉ ⇔ EXISTUJE PRIJÍMAJÚCI PODSTROM T. Z.

V EXISTENČNÝCH UZLOCH MÁ ASPOŇ 1 SYNA,
V UNIVERZÁLNYCH UZLOCH MÁ 2 SYNOV
A VŠETKY LISTY SÚ PRIJÍMAJÚCE.

POZOR! NIE JE DANÉ OHRANIČENIE POČTU ALTERNÁCIÍ ...

ALTERNUJÚCI TS NA VSTUPE x JE k-ALTERNUJÚCI ⇔ NA KAŽDEJ CESTE DOJDE K NAJVIAC k STRIEDANIAM UNIVERZÁLNYCH A EXISTENČNÝCH STAVOV

ALTERNUJÚCI TS JE k-ALTERNUJÚCI ⇔ JE k-ALTERNUJÚCI NA ∀ VSTUPOCH

1-ALTERNUJÚCI TS ZODPOVEDÁ NEDET. VÝPOČTOM, AK POUŽÍVA IBA EXISTENČNÉ STAVY

RESP. CO-NEDET. VÝPOČTOM, AK POUŽÍVA IBA UNIV. STAVY ...

01.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

ATIME(t) = TRIEDA JAZYKOV ROZPOZN. ALTERNUJÚCIMI TS PRACUJÚCIMI V ČASE t.

$AP = \bigcup_{k \geq 1} ATIME(n^k)$.

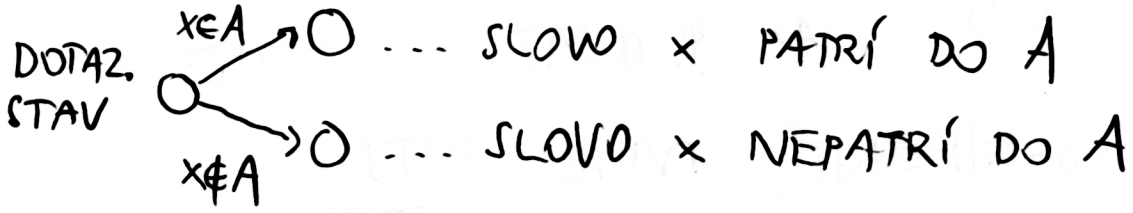
VETA: $AP = PSPACE$.

TURINGOVE STROJE S ORÁKULOM

ORÁKULUM MÔŽME CHÁPAŤ AKO $A \subseteq \{0,1\}^*$, POPR. AKO FUNKCIU $c_A : \{0,1\}^* \to \{0,1\}$.

TS MÁ NAVIAC TZV. ORÁKULOVÚ PÁSKU, KTORÁ JE W/O A TZV. DOTAZOVACÍ STAV

KEĎ JE NA ORÁKULOVEJ PÁSKE x A PREJDEM DO DOTAZ. STAVU, POTOM:



P^A ... POLYNOMIÁLNE DET. VÝPOČTY S VYUŽITÍM ORÁKULA A.

$P^{\mathcal{C}} = \bigcup_{A \in \mathcal{C}} P^A$ ... NAPR. P^{NP}

ZREJME $NP, co\text{-}NP \subseteq P^{NP}$

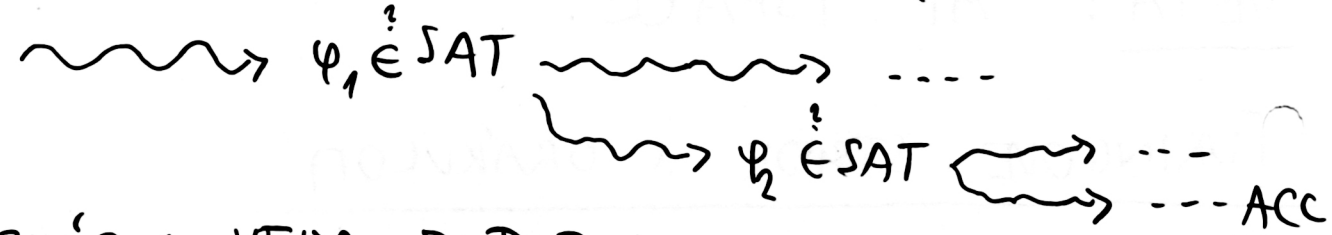
VETA: $NP = P^{NP} \Leftrightarrow NP = co\,NP$.

$\Rightarrow$) TRIVIÁLNE

$\Leftarrow$) CHCEME UKÁZAŤ $P^{NP} \subseteq NP$.

STAČÍ UKÁZAŤ $P^{SAT} \subseteq NP$.

AKO VYZERÁ VÝPOČET S ORÁKULOM SAT:



PROBLÉM: VEĽA DOTAZOV...

AK CHCEME POUŽIŤ IBA NP STROJ, MÔŽEME POSTUPOVAŤ NASLEDOVNE:

- UHÁDNEME VŠETKY DOTAZY φ_i
- UHÁDNEME, ČI PATRIA DO SAT ... (φ_i, y_i, w_i)

$$y_i = \begin{cases} 1 & \dots \text{AK } \varphi_i \in SAT \dots w_i \text{ JE CERTIFIKÁT} \\ 0 & \dots \text{AK } \varphi_i \notin SAT \quad \text{—II—} \end{cases}$$

KEĎŽE co-NP = NP, MÁME NTS

JAK PRE SAT, TAK AJ PRE $\overline{SAT}$.

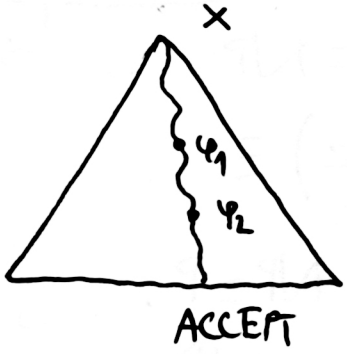
- NAKONIEC OVERÍME, ČI JE NÁŠ ODHAD KONZISTENTNÝ, A POTOM UŽ IBA ODSIMULUJEME PÔVODNÝ VÝPOČET, $\square$

01.04.2011 Fr
PETER ČERNO

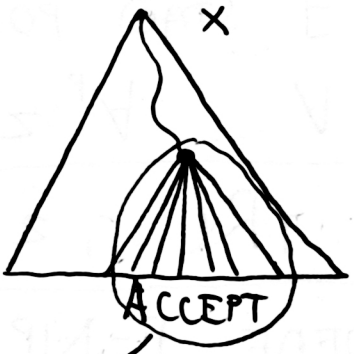
NTINO86 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

VETA: $NP^{NP} = \Sigma_2$.

$NP^{NP} = NP^{SAT}$



Σ_2



CELÝ TENTO PODSTROM SA DÁ ZABALIŤ DO 1 SAT DOTAZU:

NAPR. „∃ CESTA, KT. JE REJECT ?"

$\Rightarrow \Sigma_2 \subseteq NP^{NP}$.

DOKÁŽEME EŠTE $NP^{SAT} \subseteq \Sigma_2$. POSTUPUJEME PODOBNE AKO V PREDCHÁDZAJÚCEJ VETE, AVŠAK FORMULE, O KTORÝCH SI MYSLÍME, ŽE SÚ NESPLNITEĽNÉ, OVERÍME V PODSTROME:

□

VETA: $P = NP \Rightarrow P = PH$.

AK $P = NP$, POTOM $\Sigma_{k+1} \subseteq \Sigma_k \quad \forall k \geq 1$

$x \in L \Leftrightarrow \exists^P y_1 \, \forall^P y_2 \ldots \boxed{Q^P y_{k+1} \; (x, y_1, \ldots, y_{k+1}) \in L'}$

PRE $Q \equiv \exists$ STAČÍ POUŽÍT $P = NP$ ... $\hookrightarrow \in P$

PRE $Q \equiv \forall \ldots \forall^P z \; R(\ldots, z) \equiv$

$\neg \boxed{\exists^P z \; \neg R(\ldots, z)} \ldots \in NP = P$.

POPR. MUZJENE $P = NP \Rightarrow P = co\text{-}NP$. □

□

08.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

TODOVA VETA : $PH \subseteq P^{PP}$

MY SI UKÁŽEME $PH \subseteq BPP^{\#SAT}$.

$SAT = \{ \varphi(x_1, \dots, x_n) \mid \varphi$ JE SPLNITELNÁ$\}$

$\#SAT$: $\varphi(x_1, \dots, x_n) \rightarrow$ POČET SPLŇUJÍCÍCH OHODNOCENÍ

$\oplus SAT = \{ \varphi(x_1, \dots, x_n) \mid \varphi$ MÁ LICHÝ POČET SPLŇUJÍCÍCH OHODNOCENÍ $\}$.

$\equiv$ TZV. PARITY SAT

VĚTA : $\forall k \geq 1$ EXISTUJE PRAVDĚPODOBNOSTNÍ ALGORITMUS A_k, KT. PRO KAŽDOU FORMULI φ S k KVANTIFIKÁTOROVÝMI BLOKY VYPÍŠE FORMULI $A_k(\varphi)$ (V POLYNOMIÁLNÍM ČASE) T.Z.:

(i) φ JE PRAVDIVÁ $\Rightarrow \Pr[A_k(\varphi) \in \oplus SAT] \geq \frac{2}{3}$

(ii) φ JE NEPRAVDIVÁ $\Rightarrow \Pr[A_k(\varphi) \in \oplus SAT] = 0$

$\equiv$ SLABŠÍ VERZE TODOVY VĚTY, TJ.

$\Sigma_k\text{-}SAT \rightsquigarrow \#SAT$

1. KROK : SAT $\longrightarrow$ $\oplus$SAT

$\varphi(x_1, \dots, x_n) \rightsquigarrow \psi(\dots)$

$\varphi \in SAT \iff \psi \in \oplus SAT$

$\varphi \in SAT \rightsquigarrow \psi$ MÁ PRÁVE JEDNO SPĽŇUJÚCE OHODNOTENIE.

OZNAČME $\#\varphi$ ... POČET SPĽŇ. OHODNOTENÍ.

$(\neg z \,\&\, \varphi(\dots)) \vee (z \,\&\, \bar{x}_1 \,\&\, \dots \,\&\, \bar{x}_n) =: \varphi'$

$(\#\varphi) + 1 = (\#\varphi')$

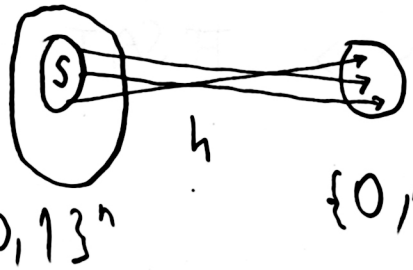
PRE $\varphi_1(x_1, \dots, x_n)$, $\varphi_2(y_1, \dots, y_m)$ DISJ. PREMENNÉ

$(\#\varphi_1) \cdot (\#\varphi_2) = \#(\varphi_1 \,\&\, \varphi_2)$

... TIETO POZOROVANIA PLATIA AJ PRE KVANTIFIKOVANÉ FORMULE. NAVYAC SA NEMENÍ # BLOKOV KVANTIFIKÁTOROV ...

$\#\varphi$ ... POČET OHODNOTENÍ VOĽNÝCH PREMENNÝCH SPĽŇUJÚCICH φ

HASHOVANIE :



08.04.2011 Fr
PETER ČERNO

NTINO86 VYBRANÉ KAPITOLY Z VÝP. SLOŽ. II

2-UNIVERZÁLNY HAŠOVACÍ SYSTÉM:

$$H = \{ h \mid h : \{0,1\}^n \to \{0,1\}^k \}$$

T.Z. $\forall x_1, x_2 \in \{0,1\}^n,\ x_1 \neq x_2$

$\forall y_1, y_2 \in \{0,1\}^k$:

$$Pr_{h \in H}\left[h(x_1) = y_1 \ \& \ h(x_2) = y_2 \right] = \frac{1}{2^{2k}}$$

JE TO TO ISTÉ, AKO KEBY H OBSAHOVAL ÚPLNE VŠETKY FUNKCIE ...

VŠETKÝCH FUNKCIÍ JE 2^{k2^n} ...

... D. NA POPÍSANIE 1 FCIE. POTREBUJEM ASPOŇ $k2^n$ BITOV (= PRÍLIŠ VEĽA)

EXISTUJÚ MENŠIE HAŠOVACIE SYSTÉMY:

$$H_{n,k} = \{ h_{A,b} \mid A \in \{0,1\}^{k \times n},\ b \in \{0,1\}^k \}$$

$$h_{A,b}(x) = Ax + b \quad \text{NAD } GF[2].$$

CVIČENIE: $H_{n,k}$ JE 2-UNIV. HAŠ. SYSTÉM.

... NA $h_{A,b}$ POTREBUJEM $O(k \cdot n)$ BITOV.

$H_{n,k}$ MÁ DOBRÉ VLASTNOSTI:

LEMMA: NECH $k, n \geq 1$, $S \subseteq \{0,1\}^n$ T.Ž. $2^{k-3} \leq |S| \leq 2^{k-2}$, NECH $H_{n,k}$ JE 2-UNIV. HAŠ. SYSTÉM, POTOM:

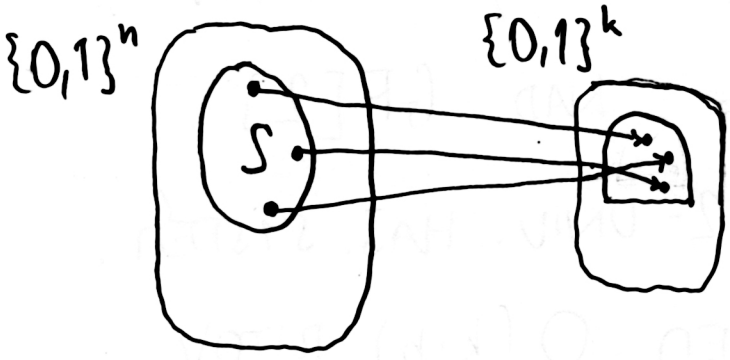
$$Pr_{h \in H_{n,k}} \left[|\{x \in S, h(x) = 0^k\}| = 1 \right] \geq \frac{1}{32}$$

PRE FORMULU $\varphi(x_1, \ldots, x_n)$ EXISTUJE $\tau_h \ldots$ FORMULA POPISUJÚCA FAKT, ŽE $h(x_1, \ldots, x_n) = 0^k$. MNOŽINA S JE MNOŽINA SPĹŇUJÚCICH OHODNOTENÍ FORMULE φ.

$\equiv$ TZV. **IZOLAČNÉ LEMMA** (VALIANT-VAZIRANI)

DÔKAZ (PRE SYSTÉM $H_{n,k}$, TJ. $h_{A,b}(x) = Ax + b$)

1) $$Pr_{h \in H_{n,k}} \left[|\{ y \in \{0,1\}^k \mid \exists! \, x \in S : h(x) = y \}| \geq \frac{|S|}{2} \right] \geq \frac{1}{2}$$



POČET KOLÍZIÍ:

$x_1, x_2 \in S$; $x_1 \neq x_2$

$h(x_1) = h(x_2)$

UVAŽUJME $K_{\{x_1, x_2\}} = \begin{cases} 1 & \text{AK } h(x_1) = h(x_2) \\ 0 & \text{INAK} \end{cases}$

08.04.2011 Fr
PETER CERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

$$\Pr_{h \in H_{n,k}}\left[\sum_{\substack{\{x_1,x_2\}\subseteq S \\ x_1 \neq x_2}} K_{\{x_1,x_2\}} \geq \frac{|S|}{4}\right] < \frac{1}{2} \quad (?)$$

$$E\left[\sum_{\substack{\{x_1,x_2\}\subseteq S \\ x_1 \neq x_2}} K_{\{x_1,x_2\}}\right] = \sum_{\substack{\{x_1,x_2\}\subseteq S \\ x_1 \neq x_2}} E\left[K_{\{x_1,x_2\}}\right] =$$

$$= \binom{|S|}{2} \cdot E\left[K_{\{x_1,x_2\}}\right] \quad \text{PRE NEJAKÉ } \begin{matrix} x_1, x_2 \in S \\ x_1 \neq x_2 \end{matrix}$$

$$\Pr_{h \in H_{n,k}}\left[h(x_1) = h(x_2)\right] = \frac{1}{2^k}$$

$$\binom{|S|}{2} \cdot \frac{1}{2^k} \leq \frac{|S|(|S|-1)}{2} \cdot \frac{1}{4|S|} = \frac{|S|-1}{8}$$

TERAZ UŽ STAČÍ POUŽIŤ MARKOVOVU NEROVN.

S PRAVDEPODOBNOSŤOU $\geq \frac{1}{2}$ NÁM ZOSTANE ASPOŇ $|S|/2$ PRVKOV S JEDINÝM (*) VZOROM ... CHCEME 0^k S JEDINÝM VZOROM

POLOVICA (A, b) NÁM DÁVA VLASTNOSŤ (*)

NA b TO NEZÁVISÍ ... $\dfrac{|S|/2 \text{ PRVKOV}}{2^k \text{ MOŽNOSTÍ PRE } b} \geq \dfrac{2^{k-3}/2}{2^k} = \dfrac{1}{16}$

MÁME IBA POLOVICU A ... DOSTANEME $\frac{1}{32}$. ∎

PEVNÉ $A \in \{0,1\}^{k \times n}$, $b \in \{0,1\}^k$

$x_1, \ldots, x_n$ BOOL. PREMENNÉ.

$\tau_h(x_1, \ldots, x_n)$ PRAVDIVÁ $\iff h_{A,b}(\vec{x}) = 0^k$

$Ax + b = 0 \quad \equiv \quad \forall i = 1, \ldots, k:$

$\sum_{j=1}^{n} a_{ij} x_j + b_i \equiv 0 \pmod 2$

↓

VYSELEKTUJE $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, T.

$\equiv (x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_{m(i)}} \oplus b_i \oplus 1)$

TO MOŽNO ZAVEDENÍM POMOCNÝCH PREMENNÝCH PREVIEST NA TROJICE:

$(1 \oplus x_{i_1} \oplus x_{i_2} \oplus y_1) \,\&\, (1 \oplus y_1 \oplus x_{i_3} \oplus y_2) \,\&\, \ldots$

TIETO PREMENNÉ y KVANTIFIKUJEME <u>EXISTENČNE</u>

$\varphi(x_1, \ldots, x_n) \longrightarrow \varphi(x_1, \ldots, x_n) \,\&$

ZVOL UNIFORMNE

NÁHODNE $\begin{cases} k \in_R \{1, \ldots, n\} \\ A \in_R \{0,1\}^{k \times n} \\ b \in_R \{0,1\}^k \end{cases}$ $\tau_h(x_1, \ldots, x_n, y_1, \ldots, y_m)$

S PRAVD. $\frac{1}{32n}$

PRÁVE 1 OHODNOTENIE

08.04.2011 Fr
PETER ČERNO

NTINO86 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

UVAŽUJME k - KVANTIFIKÁTOROVÝCH BLOKOV

$$\exists \vec{x}_1 \forall \vec{x}_2 \exists x_3 \dots Q \vec{x}_k \ \varphi(\vec{x}_1, \dots, \vec{x}_k)$$

$$\longrightarrow \psi(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_k, \vec{y}, \dots)$$

2. KROK : ZAVEDIEME TZV. PARITNÝ KVANTIF.

$\oplus y_1, \dots, y_m \ \varphi(y_1, \dots, y_m)$ JE PRAVDIVÁ

$\Leftrightarrow$ $\varphi(y_1, \dots, y_m)$ JE PRAVDIVÁ PRE NEPÁRNY POČET VOLIEB $y_1, \dots, y_m \in \{0,1\}^m$.

ZATIAĽ MÁME NASLEDUJÚCE :

$$\exists \vec{x} \ \varphi(\vec{x}) \rightsquigarrow \oplus \vec{x} \vec{y} \ (\varphi(\vec{x}) \ \& \ \tau_h(\vec{x}, \vec{y}))$$

$h \in_R H_{n,k}$

φ BEZ KVANTIF.

τ_h BEZ KVANTIF.

IDEA : TO, ŽE φ JE BEZ KVANTIFIKÁTOROV, NIE JE PODSTATNÉ

AK φ MÁ KVANTIFIKÁTORY, VIEME ICH VYSTRČIŤ PRED FORMULU ... TJ. DOSTÁVAME

$$\exists \vec{x}_1 \forall \vec{x}_2 \dots \varphi(\dots) \rightsquigarrow \oplus \vec{x}_1 \vec{y}_1 \forall \vec{x}_2 \dots (\dots)$$

S PRAVDEPODOBNOSŤOU $\geq \frac{1}{32n}$

$$\left(\oplus \vec{x}\ \psi(\vec{x})\right) \,\&\, \left(\oplus \vec{y}\ \varphi(\vec{y})\right) =$$

$$\oplus \vec{x}\,\vec{y}\ \left(\psi(\vec{x}) \,\&\, \varphi(\vec{y})\right)$$

$$\neg \oplus \vec{x}\ \left(\varphi(\vec{x})\right) = \oplus \vec{x}, z\ \varphi'(\vec{x}, z),$$

KDE $\#\varphi(\vec{x}) + 1 = \#\varphi'(\vec{x}, z)$

MÔŽME ZNAČIŤ $\varphi' = (\varphi + 1)$

$$\left(\oplus \vec{x}\ \varphi(\vec{x})\right) \vee \left(\oplus \vec{y}\ \psi(\vec{y})\right) =$$

$$\oplus \vec{x}, \vec{y}, \vec{z}\ \left((\varphi+1) \,\&\, (\psi+1) + 1\right)(\vec{x}, \vec{y}, \vec{z})$$

PROBLÉM : DISJUNKCIA VÄČŠIEHO MNOŽSTVA FORMULÍ ... VEĽKOSŤ $\varphi+1$ JE PRIBLIŽNE DVOJNÁSOBNÁ OPROTI φ ...

$$\left(\oplus \vec{x}_1\ \varphi_1(\vec{x}_1)\right) \vee \ldots \vee \left(\oplus \vec{x}_m\ \varphi_m(\vec{x}_m)\right) =$$

$$= \oplus \vec{x}_1 \ldots \vec{x}_m\, \vec{z}\left(\left((\varphi_1+1) \,\&\, \ldots \,\&\, (\varphi_m+1)\right) + 1\right)$$

... TJ. MÁME IBA LINEÁRNY NÁRAST VEĽKOSTI

AKO ZLEPŠIŤ PRAVDEPODOBNOSŤ $\frac{1}{32n}$?

POMOCOU OPAKOVANÍ ...

08.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

ZVOLÍME $m := 32n \cdot c$

m-KRÁT VYGENERUJ REDUKCIU $SAT \to \oplus SAT$

$$\oplus \vec{x}_1 \varphi_1(\vec{x}_1), \ldots, \oplus x_m \varphi(x_m)$$

POTOM VEZMEME DISJUNKCIU:

$$\left(\oplus \vec{x}_1 \varphi_1(\vec{x}_1)\right) \vee \ldots \vee \left(\oplus x_m \varphi(x_m)\right)$$

S AKOU PRAVDEPODOBNOSŤOU JE ASPOŇ 1 Z TÝCHTO FORMULÍ PRAVDIVÁ?

$$1 - \left(1 - \frac{1}{32n}\right)^m \geq 1 - e^{-c}$$

(PLATÍ TOTIŽ $1 - x \leq e^{-x}$)

UVAŽUJME $\exists \vec{x}_1 \forall \vec{x}_2 \ldots \varphi(\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_k)$

$\rightsquigarrow \oplus \vec{\vec{x}}_1 \forall \vec{\vec{x}}_2 \ldots \varphi'(\vec{\vec{x}}_1, \vec{\vec{x}}_2, \ldots, \vec{\vec{x}}_k)$

$\downarrow$

ZNEGUJME TÚTO FORMULU, T.J.

$$\oplus \vec{\vec{x}}_1 \neg\left(\forall \vec{\vec{x}}_2 \ldots \varphi'(\vec{\vec{x}}_1, \vec{\vec{x}}_2, \ldots, \vec{\vec{x}}_k)\right)$$

$$\oplus \vec{\vec{x}}_1 \neg\underbrace{\left(\exists \vec{\vec{x}}_2 \ldots \neg \varphi'(\text{—}''\text{—})\right)}$$

$$\oplus \vec{\vec{x}}_1 \neg\left(\oplus \vec{\vec{\vec{x}}}_2 \forall \vec{\vec{\vec{x}}}_3 \ldots \psi(\vec{\vec{x}}_1, \vec{\vec{\vec{x}}}_2, \ldots, \vec{\vec{\vec{x}}}_k)\right)$$

PREDPOKLADAJME, ŽE $\vec{\vec{x}}_1$ MÁ ℓ_1 PREMENNÝCH
AKÉ VEĽKÉ c_1 MUSÍME ZVOLIŤ PRE TEN
VNÚTRAJŠOK, ABY TO FUNGOVALO PRE $\forall \vec{\vec{x}}_1$?

$$c_1 := \ell_1 \log_e 10k$$

POTOM DOSTÁVAME PRAVDEPODOBNOSŤ PRE 1 $\vec{\vec{x}}_1$:

$$\geq 1 - e^{-\ell_1 \log_e 10k} \geq 1 - \frac{1}{2^{\ell_1} \cdot 10k}$$

PRAVDEPODOBNOSŤ, ŽE PRE VŠETKY VOĽBY $\vec{\vec{x}}_1$
TRANSFORMÁCIA ZACHOVALA PRAVDIVOSTNÚ
HODNOTU VNÚTRAJŠKU JE $\geq 1 - \frac{1}{10k}$

DOSTÁVAM TEDA FORMULU:

$$\oplus \vec{\vec{x}}_1 \left(\oplus \vec{\vec{x}}_2 z \; \forall \vec{\vec{x}}_3 \exists \ldots \psi' \left(\vec{\vec{x}}_1 \ldots \right) \right) =$$

$$= \oplus \vec{\vec{x}}_1 \vec{\vec{x}}_2 z \; \forall \vec{\vec{x}} \ldots \psi' \left(\vec{\vec{x}}_1 \ldots \right)$$

... MÁME O 2 KVANTIF. MENEJ

PO k KROKOCH ODSTRÁNIME VŠETKY KVANTIF.
PREDPOKLADAJME, ŽE ZA c_0 SME ZVOLILI $\log(10 \cdot k)$
... ĎALEJ $c_3 = \ell_3 \log(10k)$ ... ATĎ.

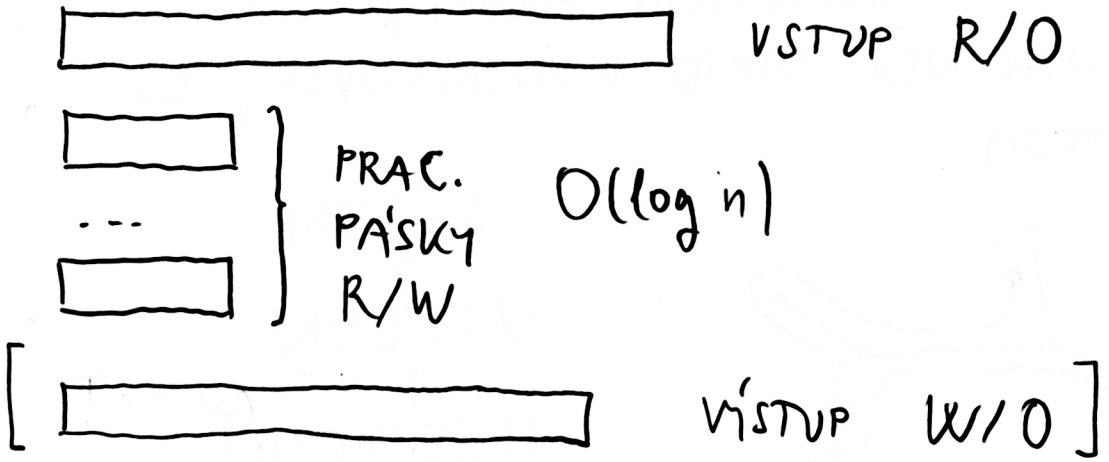
15.04.2011 Fr
PETER ČERNO

NTINO86 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

MINULE: $PH \subseteq BPP^{\oplus SAT}$ (TODDOVA VETA)

NÁHODNÉ VÝPOČTY & PSEUDONÁH. GENERÁTORY

BUDEME SA ZAUJÍMAŤ O NÁH. VÝPOČTY V MALOM PRIESTORE ...



... TRIEDA $DSPACE(\log n) =: L$.

PRÍKLADY PROBLÉMOV, KTORÉ SA DAJÚ RIEŠIŤ V log PRIESTORE:

- SČÍTANIE $x, y \longmapsto x + y$
- NÁSOBENIE MATÍC $A, B \longmapsto A \times B$
(POLYNOMIÁLNE VEĽKÉ ČÍSLA)

$STCON = \{ (G, s, t) \mid \exists$ CESTA $s \rightsquigarrow t$ V $G \}$

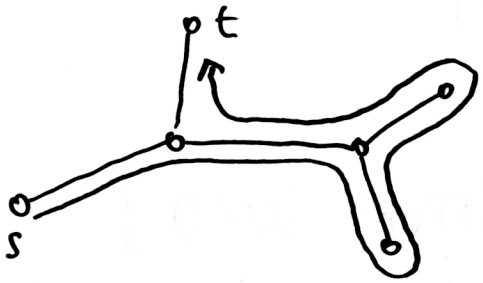
$STCON \in DSPACE(\log^2 n)$

$STCON$ JE $NL = NSPACE(\log n)$ - ÚPLNÝ.

EXISTUJÚ RÔZNE VARIANTY STCON :

TREESTCON = $\{(G, s, t) \in STCON \mid$
G JE NEORIENTOVANÝ STROM $\}$

DÁ SA UKÁZAŤ, ŽE TREESTCON $\in L$
(PRAVIDLO PRAVEJ RUKY - STAČÍ ZADEFINOVAŤ JEDNOZNAČNÚ ORIENTÁCIU HRÁN)
DÁ SA DOKONCA TAKTO KONTROLOVAŤ, ČI G JE STROM.



STCON
↑
USTCON
↑
TREESTCON

USTCON = $\{(G, s, t) \in STCON \mid$ G NEORIENT. $\}$

VETA (REINGOLD) : USTCON $\in L$. (2003)

USTCON SA DÁ ZREDUKOVAŤ NA TREESTCON ...
USTCON SA DÁ RIEŠIŤ V PRAVDEPOD. log-SPACE.

ALGORITMUS : VSTUP (G, s, t)

$u \leftarrow s$
OPAKUJ $6n^3$ KRÁT :
  $u \leftarrow$ NÁHODNÝ SUSED u
  AK $u = t$ TAK PRIJMI
ODMIETNI

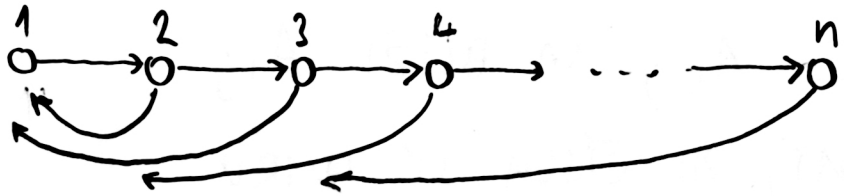
15.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

VETA: AK EXISTUJE CESTA $s \rightsquigarrow t$ V G, POTOM SA ALGORITMUS ZASTAVÍ A PRIJME S PRAVDEPODOBNOSŤOU $\geq 2/3$.

BEZ DÔKAZU ... POUŽÍVA SA TZV. COVERING TIME.

NIE JE MOŽNÉ TENTO VÝSLEDOK JEDNODUCHO PRENIESŤ NA ORIENTOVANÉ GRAFY:



OTVORENÝ PROBLÉM: $RL \stackrel{?}{=} L$.

TRIVIÁLNE POZOROVANIE: $L \subseteq RL \subseteq NL \subseteq L^2$.

DÁ SA UKÁZAŤ, ŽE $RL \subseteq L^{3/2}$.

$A_1, A_2, \ldots, A_n$ $n \times n$ MATICE

S ČÍSLAMI $0 < .. < 1$ (STOCHASTICKÉ)

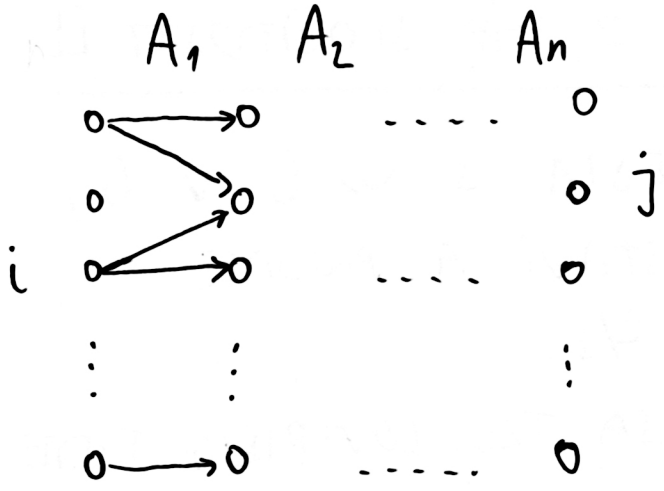
$\forall i \sum_{j=1}^{n} A_{ij} = 1$

CIEĽ: SPOČÍTAŤ $A_1 \times \ldots \times A_n$.

V RL JE MOŽNÉ SPOČÍTAŤ APROXIMÁCIU $\prod_{i=1}^{n} A_i$

TJ. A' T. Ž. PRE $A = \prod_{i=1}^{n} A_i$ PLATÍ:

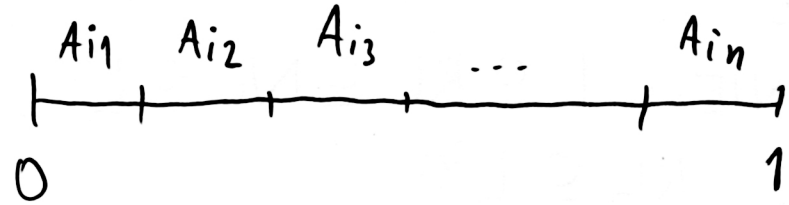
$\forall ij \; |A_{ij} - A'_{ij}| < \varepsilon$.



PRE KAŽDÉ i, j
ZOPAKUJ $O\left(\frac{n^2}{\varepsilon^2}\right)$ KRÁT
NÁHODNÚ PRECHÁDZKU
Z i ...
A'_{ij} JE PODIEL
PRECHÁDZOK, KT. DORAZIA
DO j.

DÁ SA UKÁZAŤ, ŽE A'_{ij} SA BLÍŽI A_{ij}.

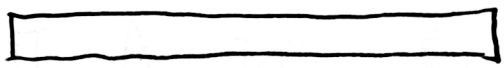
BUDEME PREDPOKLADAŤ, ŽE ČÍSLA SÚ TVARU
p/q, KDE $p, q \leq O(n^k)$



VYNÁSOBENÍM VHODNÝM ČÍSLOM DOSTANEM
CELÉ ČÍSLA ...

CELÝ TENTO ALG. MOŽNO IMPLEMENTOVAŤ
V LOGARITMICKOM PRIESTORE.

PRAVDEPODOBNOSTNÝ TURINGOV STROJ PRACUJÚCI
V log - PRIESTORE:

VSTUP $x \in \{0,1\}^n$ 

k PRAC. PÁSOK VEĽKOSTI $O(\log n)$

15.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

POČET KONFIGURÁCIÍ JE $n^{O(k)}$.

PSEUDONÁHODNÉ GENERÁTORY

$$f : \{0,1\}^l \to \{0,1\}^n$$

CHCELI BY SME $l = O(\log n)$

PRE VŠETKY TURINGOVE STROJE NA VSTUPE DĹŽKY n : $M(x, \sigma) \approx \Pi(x, f(t))$

$\sigma \in \{0,1\}^n$ $\quad$ $t \in \{0,1\}^l$

NISANOV PSEUDONÁHODNÝ GENERÁTOR

$$g : \{0,1\}^l \to \{0,1\}^n \quad l \approx O(\log^2 n)$$

PRE VÝPOČTY BEŽIACE V PRIESTORE $O(\log n)$
A ČASE $poly(n)$.

$A_1, A_2, \ldots, A_n$ $0/\frac{1}{2}$ MATICE $n \times n$, STOCHASTICKÉ

BUDEME SI NIEKEDY ZVOLIŤ ε ... POŽADOVANÁ CHYBA
TYPICKY $\varepsilon = \frac{1}{n^k}$.

2-UNIVERZÁLNY HAŠOVACÍ SYSTÉM :

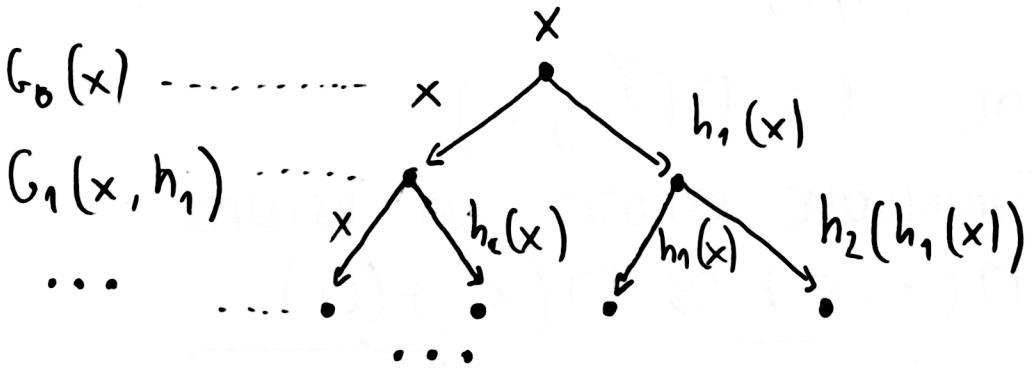
$$H = \{ h : \{0,1\}^m \to \{0,1\}^m \}$$

$x \in \{0,1\}^m$, $h_1, h_2, \ldots, h_k \in H$

$G_0(x) = x$

$G_{k+1}(x, h_1, h_2, \ldots, h_{k+1}) =$

$G_k(x, h_1, h_2, \ldots, h_k) \cdot G_k(h_{k+1}(x), h_1, \ldots, h_k)$



DĹŽKA VÝSTUPU G_k JE $2^k m$

VOLÍME $k = \log n$, $m = O(\log n)$.

NA POPIS KAŽDEJ FCIE. h JE $O(m)$ BITOV.

MINULE SME UVAŽOVALI MASKOVACÍ SYSTÉM

$Ax + b$

↑ $m \times m$ BITOV ↖ m BITOV

MY ALE POTREBUJEME m BITOV

TERAZ UVAŽUJEME $h_{a,b}(x) = a \circ x + b$

↑ $m+m-1$ ↑ m BITOV ↖ KONVOLÚCIA

$$(a \circ x)_i = \sum_{j=1}^{m} a_{i+j-1} \cdot x_j \pmod 2.$$

22.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II

$H = \{ h : \{0,1\}^n \to \{0,1\}^m \}$ ... 2-UNIVERZÁLNY HASHOVACÍ SYSTÉM

$x \neq x'$ $P[h(x)=y \;\&\; h(x')=y'] = 2^{-2m}$

$G_0(x) = x$

$G_k(x, h_1, \dots, h_k) = G_{k-1}(x, h_1, \dots, h_{k-1}) \cdot G_{k-1}(h_k(x), h_1, \dots, h_{k-1})$

RIEŠILI SME ÚLOHU: NA VSTUPE:

0-1-$\frac{1}{2}$ MATICE $A_1, \dots, A_n$

$(\forall i)(\forall r) \sum_{k=1}^{n} (A_i)_{r,k} = 1$.

ZAUJÍMA NÁS $A_1 \dots A_n$.

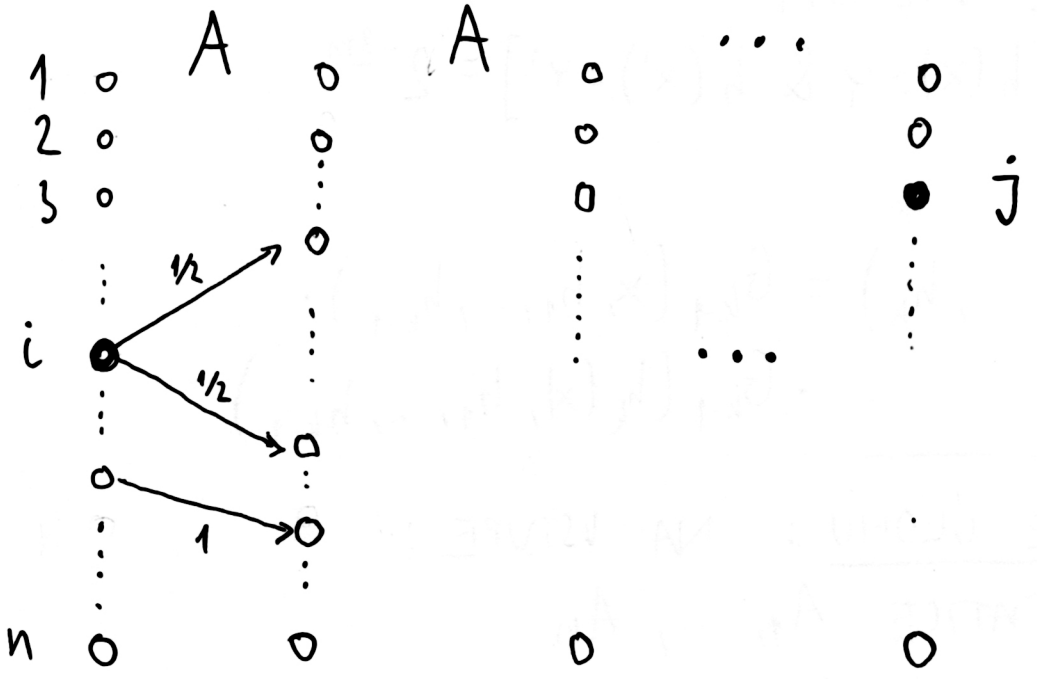
POPR. MÁME 0-1-$\frac{1}{2}$ MATICU A, CHCEME A^n.

$G_k(x, h_1, \dots, h_k)$ NÁM VRÁTI REŤAZEC BITOV DLHÝ $2^k \cdot m$ BITOV.

CHCEME APROXIMOVAŤ A^n.

NÁHODNÉ PRECHÁDZKY BUDEME APROXIMOVAŤ POUŽITÍM G_k PRE NEJAKÉ ZAFIXOVANÉ $h_1, \dots, h_k$. Z KAŽDEJ m-TICE NÁS ZAUJÍMA IBA 1. BIT, OSTATNÉ ZAHODÍME.

UKÁŽEME, ŽE KEĎ SI ZVOLÍME $h_1, \ldots, h_k$ NÁHODNE, TAK S VEĽKOU PRAVDEPODOBNOSŤOU DAJÚ DOBRÝ GENERÁTOR G_k PRE MATICU A.

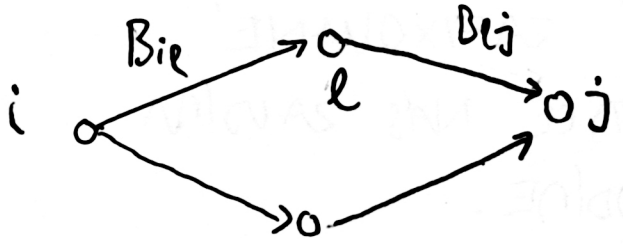


$(A^n)_{ij}$ APROXIMUJEME POČETNOSŤOU CIEST Z i DO j ... CEZ $\forall$ NÁH. PRECHÁDZKY

ODTERAZ UVAŽUJEME, ŽE NÁHODNÉ BITY BERIEME PO <u>m-TICIACH</u>.

D. VEZMEME $n.m$ BITOV, t.j.

$a_1, a_2, \ldots, a_n$ $\quad a_i \in \{0,1\}^m \ \forall i$



OZNAČME $Bil \subseteq \{0,1\}^m$ MNOŽINU RETIAZOK, KT. NÁS ZAVEDÚ Z i DO l ... PODOBNE Blj

22.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

DEFINUJME $B_{il} \cdot B_{ej} = \{ xy \mid x \in B_{il}, y \in B_{ej} \}$

ZAUJÍMÁ NÁS $\boxed{U_l B_{il} \cdot B_{ej}}$.

DEFINUJME HUSTOTU $\rho(B) = \frac{|B|}{2^m}$

UVAŽUJME $h \in H$, $A, B \subseteq \{0,1\}^m$, $\varepsilon \geq 0$.

h JE ε-DOBRÉ PRE (A, B), AK

$$\left| \frac{|\{ x \mid x \in A \ \& \ h(x) \in B \}|}{2^m} - \rho(A) \cdot \rho(B) \right| \leq \varepsilon .$$

VETA: $A \subseteq \{0,1\}^m$, $B \subseteq \{0,1\}^m$, H JE 2-UNIVERZÁLNY HAJHOVACÍ SYSTÉM, POTOM

$$P_{h \in H} [h \text{ NIE JE } \varepsilon\text{-DOBRÉ PRE } (A, B)] \leq \frac{\rho(A) \cdot \rho(B) \cdot (1 - \rho(B))}{2^m \cdot \varepsilon^2} .$$

VHODNOU VOĽBOU m MÔŽEME OVPLYVNIŤ DOLNÚ MEZ PRE ε. BUDEME POŽADOVAŤ (NA KONCI) $\varepsilon \approx \text{poly}(n)$.

DÔKAZ. MÁME $A, B \subseteq \{0,1\}^m$, $\rho(A)$, $\rho(B)$

h VYBERÁME NÁHODNE ...

PRE ZAFIXOVANÉ $x \in A$ NÁS ZAUJÍMA PRAVDEPODOBNOSŤ, ŽE $h(x) \in B$.

ZREJME $P_h[h(x) \in B] = S(B)$.

PRE $B = \{y_1, \dots, y_\ell\}$ JE

$$P_h[h(x) \in B] = \sum_{i=1}^{\ell} P_h[h(x) = y_i] = |B| \cdot 2^{-m}.$$

DEFINUJME

$$Y_x = \begin{cases} 1 & h(x) \in B \\ 0 & h(x) \notin B \end{cases} \qquad Y = \sum_{x \in A} Y_x.$$

ZREJME $Y = \#x$ T.Ž. $x \cdot h(x) \in A \cdot B$.

$E[Y] = |A| \cdot S(B)$. ... TOTO BY SME CHCELI.

OTÁZKA ZNIE, AKO ČASTO TO NASTÁVA ...

$$Pr_h[|Y - E[Y]| > t] = Pr[(Y - E[Y])^2 > t^2] \leq$$

$$\leq \frac{E[(Y - E[Y])^2]}{t^2} = \frac{Var[Y]}{t^2}$$

KDE $Var[Y] = |A| \cdot |B| \cdot 2^{-m} \left(1 - |B| \cdot 2^{-m}\right)$, pričom $|B| \cdot 2^{-m} \to S(B)$

KEĎŽE H JE 2-UNIVERZÁLNY ...

... Y_x SÚ PO DVOCH NEZÁVISLÉ.

TJ. $$Pr_h[|Y - E[Y]| > \varepsilon 2^m] \leq \frac{S(A)S(B)(1 - S(B))}{2^m \cdot \varepsilon}$$

■

22.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

TO ZNAMENÁ, AK SI ZVOLÍM $h \in H$ NÁHODNE, POTOM $P[x \cdot h(x) \in A \cdot B]$ SA CHOVÁ PODOBNE AKO $P[x \cdot y \in A \cdot B]$. NAMIESTO $2m$ NÁH. BITOV NÁM STAČÍ m NÁH. BITOV.

UVAŽUJME: A 0-1-½ STOCHASTICKÁ MATICA.

$$S_A(h_1, \ldots, h_k)_{ij} = \{x \in \{0,1\}^m \mid G_k(x, h_1, \ldots, h_k) \text{ MÁ PREVEDIE Z } i \text{ DO } j \text{ V } A^{2^k}\}.$$

$A(h_1, \ldots, h_k) = M$ MATICA, KDE:

$$M_{ij} = \frac{S_A(h_1, \ldots, h_k)_{ij}}{2^m}.$$

PRE MATICU M ZAVEDIEME NORMU:

$$\|M\| = \max_i \left(\sum_j |M_{ij}|\right).$$

ZAUJÍMA NÁS $\| A(h_1, \ldots, h_k) - A^{2^k} \|$ ...?

ZÁKLADNÉ VLASTNOSTI NORMY $\|\cdot\|$:

$$\|M + N\| \leq \|M\| + \|N\|$$

$$\|M \cdot N\| \leq \|M\| \cdot \|N\|.$$

M STOCHASTICKÁ $\Rightarrow \|M\| \leq 1$.

A ... 0-1-½ MATICA, $h_1, \ldots, h_k \in H$.

$h_1, \ldots, h_k$ JE ε-DOBRÁ PRE A $\Leftrightarrow$

$$\| A(h_1, \ldots, h_k) - A^{2^k} \| \leq \varepsilon .$$

VETA: AK H JE 2-UNIVERZÁLNY, $h_1, \ldots, h_k \in H$, A JE 0-1-½ STOCHASTICKÁ MATICA $n \times n$, $\varepsilon > 0$

$$P_{h_1, \ldots, h_k}\left[h_1, \ldots, h_k \text{ NIE JE } (2^k - 1)\varepsilon\text{-DOBRÁ PRE } A \right] \leq$$

$$\leq \frac{n^6 k}{\varepsilon^2 2^m}$$

PRE $k = \log_2 n$, $\varepsilon = \frac{1}{n^2}$, POTOM STAČÍ

NAPR. $m = 15 \log_2 n$, POTOM PRAVD. $\leq O\left(\frac{1}{n^3}\right)$.

$\Rightarrow$ $h_1, \ldots, h_k$ STAČÍ ZVOLIŤ NÁHODNE.

$\Rightarrow$ KEĎŽE m, k JE $O(\log n)$ JE MOŽNÉ

$h_1, \ldots, h_k$ NÁJSŤ DETERM. V POLYNOM. ČASE.

DÔKAZ. (INDUKCIOU PODĽA k).

PRE $k = 0$ JE TO TRIVIÁLNE ...

PREDPOKL., ŽE TVRDENIE PLATÍ PRE $k-1$.

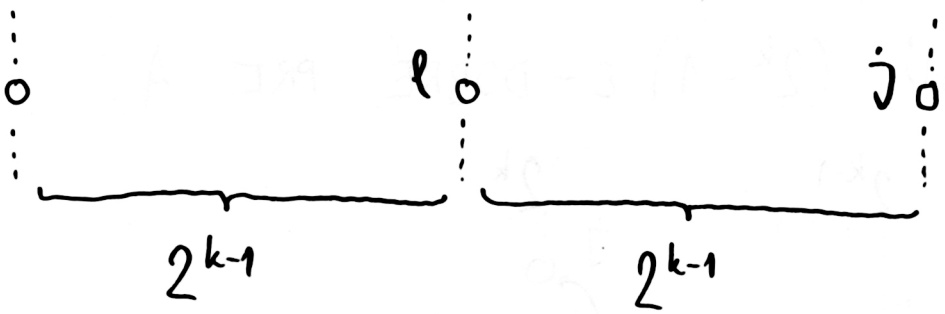
22.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

ZVOĽME $h_1, \ldots, h_k$ NÁHODNE. CHCEME:

(1) $h_1, \ldots, h_{k-1}$ SÚ $(2^{k-1}-1)\varepsilon$ - DOBRÉ PRE MATICU A.

(2) $(\forall i, j, \ell)$ h_k JE ε/n^2 - DOBRÉ PRE $(S_A(h_1, \ldots, h_{k-1})_{i,\ell}, S_A(h_1, \ldots, h_k)_{\ell,j})$



PRAVDEPODOBNOSŤ, ŽE (1) A (2) NASTÁVAJÚ JE $\geq 1 - \frac{n^6 k}{\varepsilon^2 2^m}$.

$P[\neg(1)] \leq \frac{n^6 (k-1)}{\varepsilon^2 2^m}$

MAJME $h_1, \ldots, h_{k-1}$ (SPĹŇAJÚCE (1))

$P_{h_k \in H}[\, h_k$ NIE JE $\frac{\varepsilon}{n^2}$ - DOBRÉ PRE $(S_A(h_1, \ldots, h_{k-1})_{i,\ell}, S_A(h_1, \ldots, h_k)_{\ell,j})\,] \leq$

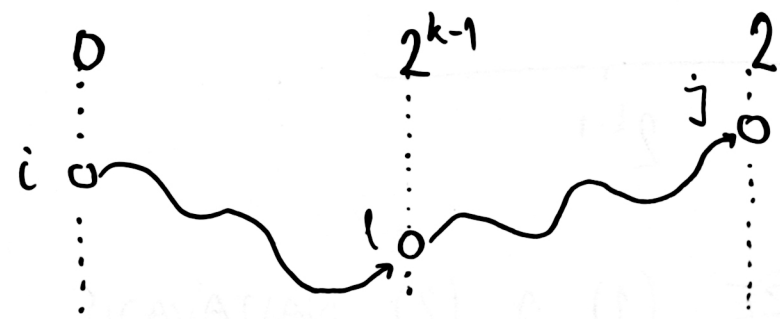
$\leq n^4 \cdot S(S_A(h_1, \ldots, h_{k-1})_{i,\ell}) / \varepsilon^2 2^m$ (i, ℓ, j SÚ FIXOVANÉ)

$\triangleleft$ $\sum_\ell S(S_A(h_1,\dots,h_{k-1})_{i\ell} = 1$

$\Rightarrow P_{h_k \in H}[h_k$ NIE JE $\frac{\varepsilon}{n^2}$ - DOBRÉ PRE NEJAKÉ $i,\ell,j \dots] \leq \frac{n^6}{\varepsilon^2 2^m}$.

TJ. $P[\neg(2)] \leq \frac{n^4}{\varepsilon^2 2^m}$.

POKIAĽ (1) & (2) NASTÁVAJÚ, POTOM $h_1,\dots,h_k$ SÚ $(2^k-1)\varepsilon$ - DOBRÉ PRE A.



$$\| A(h_1,\dots,h_k) - A^{2^k} \| \leq \underbrace{\| A(h_1,\dots,h_k) - (A(h_1,\dots,h_{k-1})) \|}_{\leq \varepsilon} + \underbrace{\| (A(h_1,\dots,h_{k-1}))^2 - A^{2^k} \|}_{\leq (2^k-2)\varepsilon}$$

PRE PEVNÉ i,j JE

$$(A(h_1,\dots,h_{k-1}))^2_{i,j} = \sum_\ell A(h_1,\dots,h_{k-1})_{i\ell} \cdot A(\dots)_{\ell j}$$

$$= \sum_\ell S(S_A(\dots)_{i\ell})\, S(S_A(\dots)_{\ell j})$$

CVIČENIE

22.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

OZNAČME $M = A(h_1, \dots, h_{k-1})$, $N = A^{2^{k-1}}$

$$\|M^2 - N^2\| \leq \|M\| \cdot \|M - N\| + \|M - N\| \cdot \|N\| \leq (2^{k-1} - 1)\varepsilon$$

- $\|M\|, \|N\| \leq 1$

$$\Rightarrow \|M^2 - N^2\| \leq (2^k - 2)\varepsilon$$

SPOLU DOSTÁVAME:

$$\|A(h_1, \dots, h_k) - A^{2^k}\| \leq (2^k - 1)\varepsilon,$$

ČO BOLO TREBA DOKÁZAŤ. ■

29.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

NISANOV PSEUDONÁHODNÝ GENERÁTOR (MINULE)

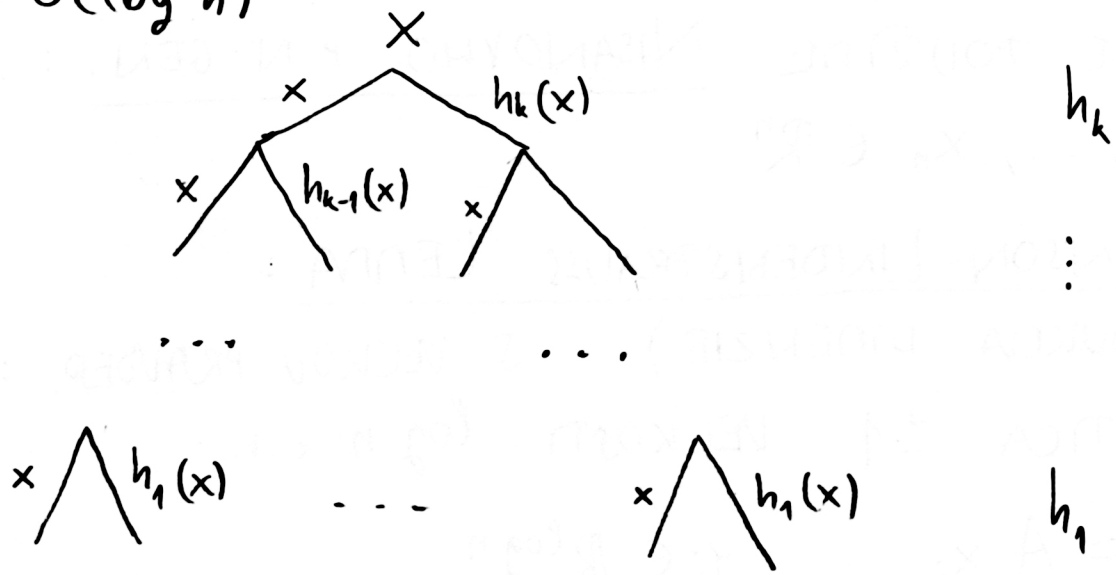
OTVORENÉ PROBLÉMY: MUSIA BYŤ $h_1, \dots, h_k$ RÔZNE?

NA KAŽDÚ HASH. FCIU $a \cdot x + b$

POTREBUJEM $3m-1$ BITOV ← $2m-1$ ← m BITOV

(KONVOLÚCIA)

$m, k \approx O(\log n)$



STAČÍ NÁM $O(\log n)$ PRIESTOR ...

$RL \subseteq LOG^2$

$RL \subseteq TISP(pol(n), \log^2(n))$

(DTIME, SPACE)

SAKS-ZHOU ... $RL \subseteq LOG^{3/2}$ (98')

... ZREDUKOVALI POČET HASH. FCII. NA $\sqrt{k}$.

TJ. SME SCHOPNÍ SPOČÍTAŤ $A^{2^{\sqrt{k}}}$ V LOG. PRIESTORE

VSIMLI SI, ŽE $A^{2^{\sqrt{k}}}$ JE BLÍZKO TOHO, ČO CHCEME. VÝSLEDOK ZAOKRÚHLIME A PROCES SPUSTÍME ZNOVU:

$$\left(A^{2^{\sqrt{k}}}\right)^{2^{\sqrt{k}}} = A^{2^{\sqrt{k}} \cdot 2^{\sqrt{k}}}$$

OPAKUJEME $\sqrt{k}$ - KRÁT... DOSTANEME A^{2^k}.

ĎALŠIE POUŽITIE NISANOVHO P. N. GEN.:

$x_1, \ldots, x_n \in \mathbb{R}^n$

JOHNSON-LINDENSTRAUSS LEMMA:
(REDUKCIA DIMENZIE) S VEĽKOU PRAVDEP.:

MATICA ± 1 VEĽKOSTI $\log n \times n$

$y_i = A x_i$, $y_i \in \mathbb{R}^{\log n}$

POTOM $\forall i,j \; \|x_i - x_j\|_2 \approx \|y_i - y_j\|_2 \cdot \log n$

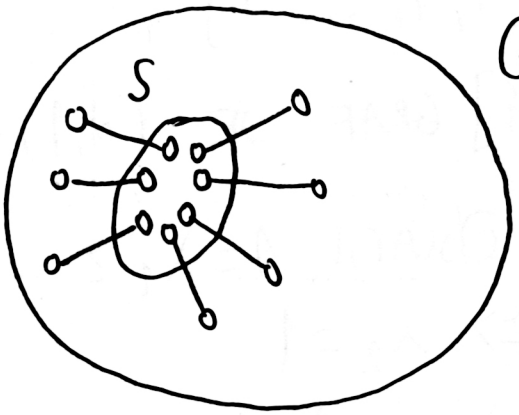
PRÍKLADY POUŽITIA: DATASTREAMOVÉ APLIKÁCIE,
POROVNÁVANIE DOKUMENTOV x_i ... DOKUMENT
POROVNÁVANIE OBRÁZKOV x_i ... OBRÁZOK

AKO NÁJSŤ DETERMINISTICKÝ A V LOG. PRIESTORE?
... PROBLÉM MOŽNO DERANDOMIZOVAŤ POMOCOU NISANOVHO PSEUDONÁH. GEN.
(SIVAKUMAR 2002)

29.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

GRAF G JE (d, ε) - EXPANDÉR



G d-REGULÁRNY, [SÚVISLÝ]
n VRCHOLOCH

$\Gamma(S) = (\text{SUSEDIA } S) \cup S$

ε ... KONŠTANTA

$$\forall S \subseteq V_G, |S| \leq \frac{n}{2} \Rightarrow |\Gamma(S)| \geq (1+\varepsilon)|S|$$

ZREJME PRIEMER GRAFU JE $O(\log n)$
... PREJNEJŠIE $2 \log_{1+\varepsilon} n$.

PRE s A t JE POČET CIEST Z s DĹŽKY NAJVIAC $2 \log_{1+\varepsilon} n$ POLYNOMIÁLNY ...

ALGEBRAICKÁ DEFINÍCIA : d-REGULÁRNY, [SÚVISLÝ]
GRAF G JE (d, λ) - EXPANDÉR $\Leftrightarrow$
DRUHÉ NAJVÄČŠIE VLASTNÉ ČÍSLO (V AB. HODN.) NORMALIZOVANEJ $\left(\times \frac{1}{d}\right)$ MATICE SUSEDNOSTI A'_G JE $\leq \lambda$. ZNAČÍME HO $\lambda(G)$.

MATICA $A'_G := \frac{1}{d} A_G$ JE STOCHASTICKÁ

ZREJME NAJVÄČŠIE VL. ČÍSLO A_G JE $= d$

TJ. MATICE A'_G JE $= 1$.

PRÍSLUŠNÝ VL. VEKTOR $= (1, 1, \ldots, 1)^T$.

$\Rightarrow$ KAŽDÝ d-REG. [SÚVISLÝ] GRAF JE $(d,1)$-EXP.

PRE d-REG. GRAF S VL. ČÍSLAMI $1 = \lambda_1 \geq \ldots \geq \lambda_n$

PLATÍ: (i) G JE SÚVISLÝ $\Leftrightarrow \lambda_2 = 1$

(ii) G JE BIPARTITNÝ $\Leftrightarrow \lambda_n = -1$

(iii) AK G JE SÚVISLÝ A NIE JE BIPARTITNÝ $\Rightarrow$

$\forall i \geq 2: |\lambda_i| \leq 1 - \frac{1}{n^3}$ (NETRIVIÁLNY DÔKAZ)

UVAŽUJME:

$(A_G)^2$ ... MATICA MULTIGRAFU, KT. JE

d^2-REGULÁRNY ... OZNAČME G^2

$A'_{G^2} = (A'_G)^2$ ... DÁ SA ZOBECNIŤ NA G^k

PRE d-REG., SÚVISLÝ, NEBIPARTITNÝ G

PRE $k = n^3$ JE $|\lambda_i|^{n^3} \leq \left(1 - \frac{1}{n^3}\right)^{n^3} \leq \frac{1}{e}$

... GRAF G^{n^3} JE ÚPLNÝ

ZIG-ZAG PRODUCT ... ZLOŽITÁ DEFINÍCIA

POUŽIJEME RV. REPLACEMENT PRODUCT

29.04.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

G
n VRCHOLOV
d-REGULÁRNY

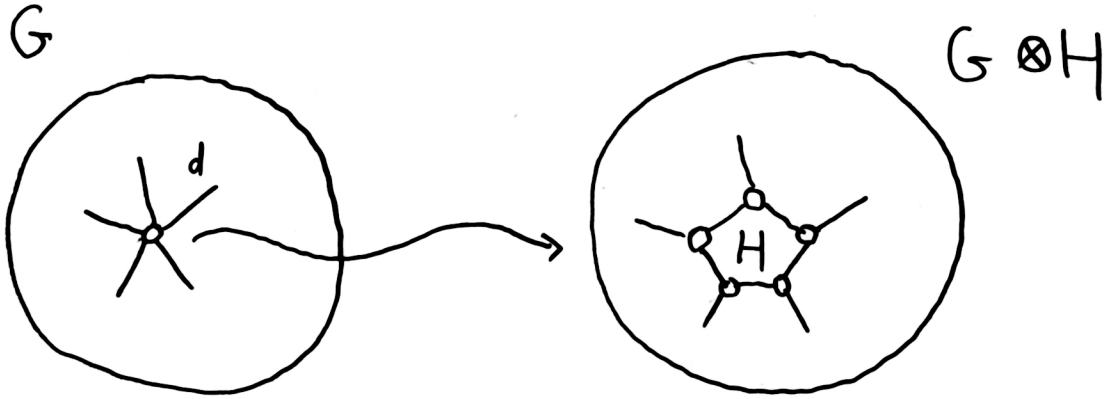
$\otimes$

H
d VRCHOLOV
d'-REGULÁRNY

↓

nd VRCHOLOV
(d'+1)-REGULÁRNY

(POZOR! $\otimes$ NIE JE DEF. JEDNOZNAČNE)



KEĎ H JE (d', λ')-EXPANDÉR, $\lambda' = \frac{1}{2}$,

POTOM $\lambda(G \otimes H) \approx \lambda(G)$.

PLATÍ NIEČO AKO $\frac{1}{2}(1 - \lambda(G)) \leq 1 - \lambda(G \otimes H)$

BUDEME OPAKOVANE UMOCŇOVAŤ GRAF
A VYKONÁVAŤ REPLACEMENT PRODUCT...
... VYKONÁME $O(\log n)$-KRÁT.
VÝSLEDNÝ GRAF BUDE POLYNOMIÁLNE VEĽKÝ
DOKONCA STAČÍ LOG. PRIESTOR...

06.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II

KOMUNIKAČNÁ ZLOŽITOSŤ

ALICA ⟶ BOB
$x \in \{0,1\}^n$ ⟵ $y \in \{0,1\}^n$
KOMUNIKÁCIA

f ĽUBOVOĽNÁ FUNKCIA ZNÁMA OBOM, NO ALICA NEPOZNÁ y A BOB x ...

ALICA A BOB CHCÚ SPOČÍTAŤ $f(x,y)$

$f: X \times Y \to Z$, KDE Z JE KONEČNÉ TELESO

ZAUJÍMAME SA O:
- POČET BITOV, KT. SI MUSIA VYMENIŤ
- POČET SPRÁV, KT. SI VYMENIA = POČET KÔL

PRÍKLAD: $f(x,y) = \begin{cases} 1 & \text{AK } x=y \\ 0 & \text{AK } x \neq y \end{cases}$

NAŠ MODEL: 1 SPRÁVA = 1 BIT

- KOĽKO INFORMÁCIE TREBA PRENIESŤ?
- $\leq n$, ČO DOLNÁ HRANICA? + 1 BIT ($\log |Z|$)
- OBECNE $n + \log |Z|$ BITOV

DOHODA: KTO MÁ KRATŠÍ VSTUP

STRIEDANIE: (KTO KEDY HOVORÍ?)

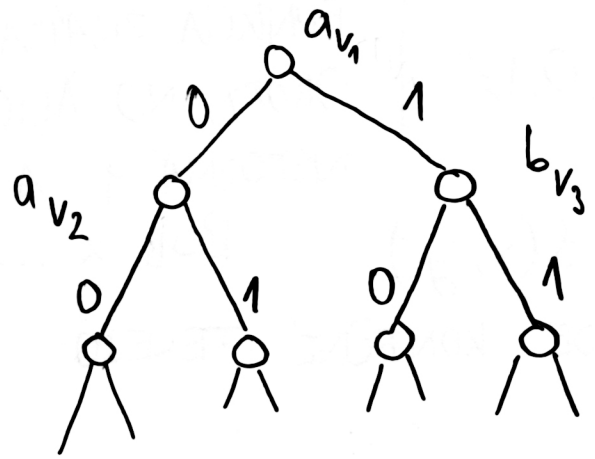
PROTOKOL: ZAKORENENÝ BINÁRNY STROM

PRE KAŽDÝ VNÚTORNÝ UZOL v MÁME FUNKCIU:

$a_v : X \to \{0,1\}$, ALEBO FUNKCIU

$b_v : Y \to \{0,1\}$

A KAŽDÝ LIST JE OHODNOTENÝ PRVKOM ZO Z



CENA PROTOKOLU $\equiv_{def}$ VÝŠKA STROMU PROTOKOLU

(NIEKTORÉ VETVY MÔŽU BYŤ NEDOSTUPNÉ ... ALE TO JE OK)

$\downarrow$

$z \in Z$ ... SPRÁVNA HODNOTA $f(x,y)$

KOMUNIKAČNÁ ZLOŽITOSŤ FUNKCIE f ...

$D(f)$:= CENA NAJLACNEJŠIEHO PROTOKOLU PRE f

$\forall f : D(f) \leq \log |X| + \log |Z|$

PRÍKLAD: $MAX_n(x,y) = \max(x \cup y)$,

KDE $X \subseteq \{1, \dots, n\}$

$D(MAX_n) \leq n + \lceil \log n \rceil$

$D(MAX_n) \leq 2\lceil \log n \rceil$

06.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI II

$MED_n(x,y)$ = MEDIÁN $x \cup_M y$

$\cup_M$ ... MULTIMNOŽINOVÉ ZJEDNOTENIE

$D(MED_n) = O(\log^2 n)$

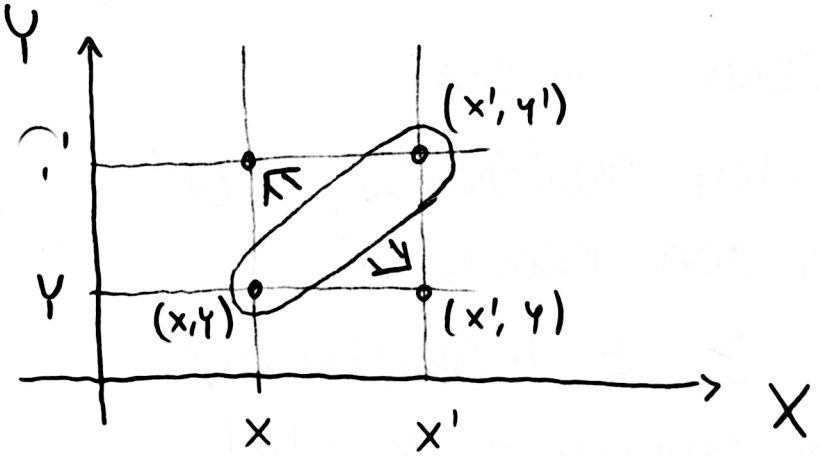
DÁ SA $O(\log n)$

KOMBINATORICKÉ OBDĹŽNIKY

X, Y; $A \times B \subseteq X \times Y$ JE KOMB. OBDĹŽNIK.

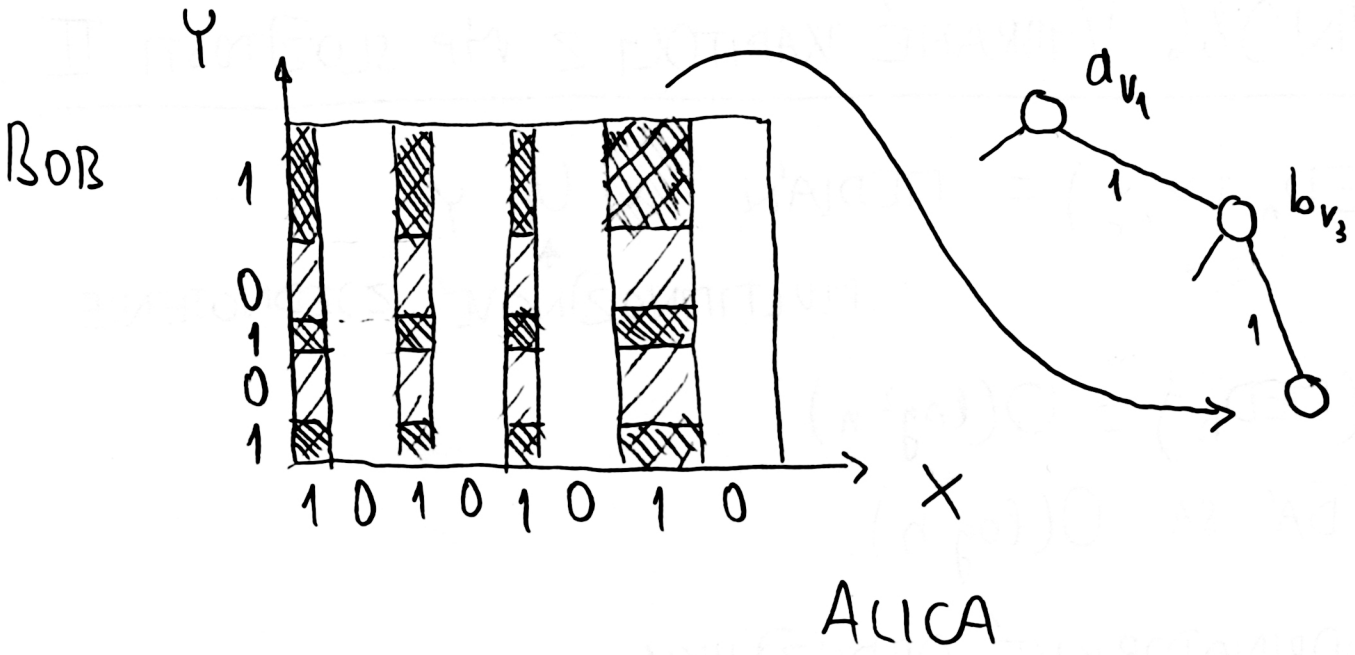
LEMMA: $V \subseteq X \times Y$ JE KOMB. OBDĹŽNIK $\Leftrightarrow$

$\forall (x,y),(x',y') \in V : (x',y) \in V$



OZNAČME $R_v = \{(x,y) \in X \times Y \mid$ NA VSTUPE (x,y) DÔJDENE DO VRCHOLU (UZLU) $v\}$

R_v JE KOMB. OBDĹŽNIK!



FUNKCIA f JE ROVNAKÁ V KAŽDOM OBDĹŽNIKU R_v, KT. ZODPOVEDÁ NEJAKÉMU LISTU v.

DOLNÉ ODHADY NA KOM. ZLOŽITOSŤ ...

VETIEV NA ROZLÍŠENIE ($\Theta(n)$ PRE EQ)

log # LISTOV = CENA = HĹBKA

log # MONOCHROMATICKÝCH OBDĹŽNIKOV, KTORÉ POTREBUJEM NA TO, ABY SOM POKRYL f ...

MONOCHR. OBDĹŽNIKOV $\geq$ # 1-OBDĹŽNIKOV

V PRÍPADE EQ: # 1-OBDĹŽNIKOV = $|X| = |Y|$

$\Rightarrow$ PROTOKOL MÁ $\geq |X|+1$ LISTOV

$\Rightarrow$ CENA $\geq \log(|X|+1) > n$

$\Rightarrow$ CENA $\geq n+1$

$D(EQ_n) \geq n+1 \Rightarrow D(EQ_n) = n+1$

06.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II

DETERMINISTICKÉ PROTOKOLY, ODHADY POČTU OBDĹŽNIKOV

$D(\text{PARITA}) = 2$

$DISJ_n(x,y) = [x \cap y = \emptyset]$, $x, y \subseteq \{1, \dots, n\}$

PRÍKLAD POUŽITIA: EXISTUJE TERMÍN, KEDY MAJÚ ALICA AJ BOB VOĽNO?

HORNÝ ODHAD $D(DISJ_n) \leq n+1$.

$\exists\, 2^n$ DVOJÍC $(A, \bar{A})$, $A \subseteq \{1, 2, \dots, n\}$.

MÔŽU MAŤ TEN ISTÝ KOMB. OBDĹŽNIK?

AK $A \neq B$, $(A, \bar{A}), (B, \bar{B}) \in V$, POTOM ZREJME $(B, \bar{A})$, ANI $(A, \bar{B}) \notin V$,

PRETOŽE $DISJ_n(A, \bar{A}) = DISJ_n(B, \bar{B}) = 1$, ALE $DISJ_n(B, \bar{A}) = DISJ_n(A, \bar{B}) = 0$.

$\Rightarrow \geq 2^n + 1$ OBDĹŽNIKOV $\Rightarrow$ $D(DISJ_n) = n+1$.

LEMMA: POKIAĽ ĽUBOVOĽNÉ ROZDELENIE $X \times Y$ NA MONOCHR. OBDĹŽNIKY PRE f OBSAHUJE ASPOŇ t OBDĹŽNIKOV, POTOM $D(f) \geq \log_2 t$.

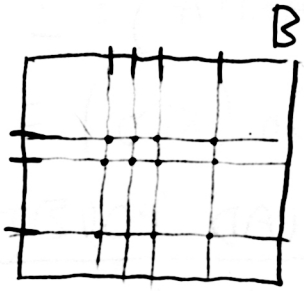
$DISJ_n(x,y) = \left(\sum_i x_i y_i = 0\right)$

DEFINUJME $\oplus P_n(x,y) := \left(\sum_i x_i y_i\right) \bmod 2$

$D(\oplus P_n) = n+1$ ... DOLNÝ ODHAD # MALÝCH OBD.

POČET 0-OBDĹŽNIKOV =

$\frac{1}{2} \cdot 2^n \cdot 2^n = \underline{\underline{2^{2n-1}}}$



$\langle A \rangle \times \langle B \rangle$ ... $GF[2]^n$

↳ SPAN 0-OBDĹŽNIK

$a \in A,\ b_1, b_2 \in B$

$\langle a | b_1 \rangle = \langle a | b_2 \rangle = 0 \Rightarrow \langle a | b_1 + b_2 \rangle = 0$

$a_1, \ldots, a_k$ JE BÁZA $A \Rightarrow \dim \langle B \rangle = n-k$,

PRETOŽE $\langle B \rangle$ JE ORTOGONÁLNY DOPLNOK $\langle A \rangle$.

$\Rightarrow |\langle A \rangle \times \langle B \rangle| \leq 2^{\dim \langle A \rangle + \dim \langle B \rangle} = \underline{\underline{2^n}}$

$\Rightarrow$ # OBDĹŽNIKOV $\geq \frac{2^{2n-1}}{2^n} + 1 = 2^{n-1} + 1$

↑ 1-OBDĹŽNIKY

$\Rightarrow$ ZLOŽITOSŤ n. $\square$

13.05.2011 Fr
PETER ČERNO

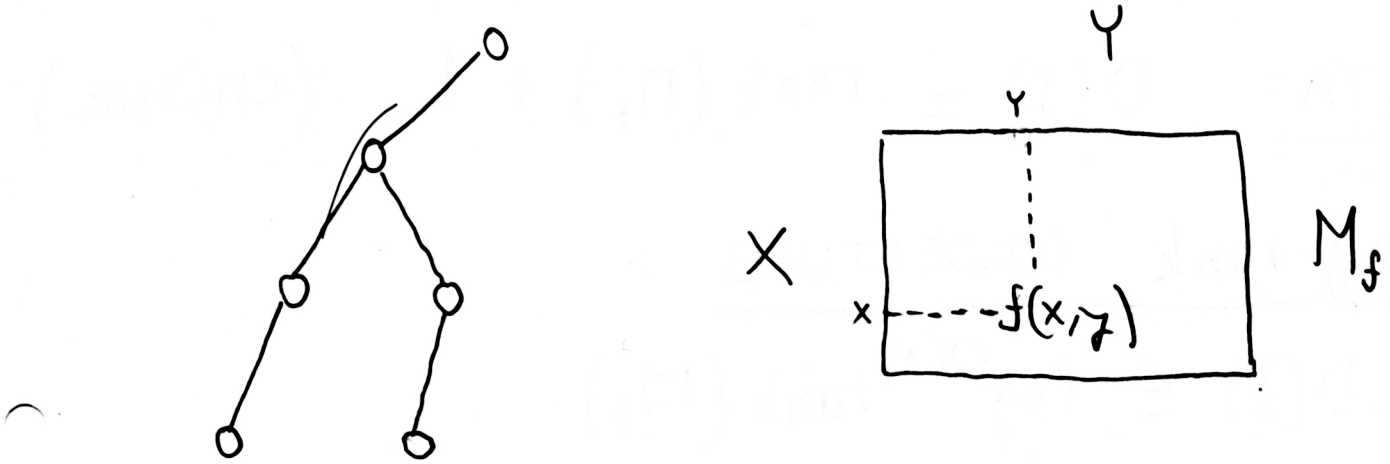
NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI II

DOPÍSAŤ POZNÁMKY ZO 06.05.2011

ALICA $\longrightarrow$ BOB POZNAJÚ f:
x $\longleftarrow$ y $X \times Y \to T$

$x \in X$
$y \in Y$ ALICA A BOB CHCÚ SPOČÍTAŤ $f(x,y)$

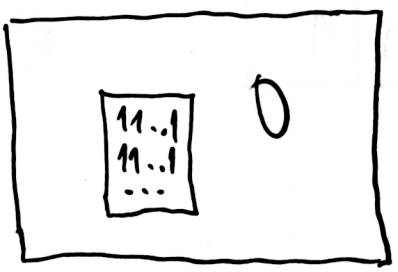
KOMUNIKAČNÝ PROTOKOL (STROM)



VETA: KOMUNIKAČNÁ ZLOŽITOSŤ $D(f) \geq$
$\geq \log \text{rank}(M_f)$

M_f SA DÁ VYJADRIŤ AKO SÚČET:

$M_{R_1} + M_{R_2} + \dots M_{R_n}$

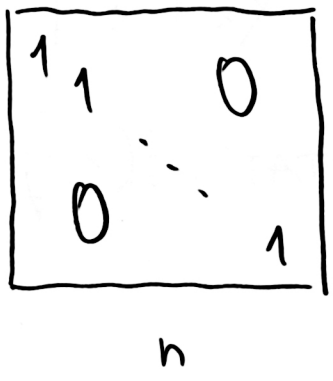


$\text{rank}(M_{R_i}) = 1$

ZREJME $\operatorname{rank}(M_f) \leq \sum_{i=1}^{n} \operatorname{rank}(M_{R_i})$.

PRÍKLAD: $f(x,y) := (x = y)$

EQ



$D(f) \geq \log n$.

POZNÁMKA:

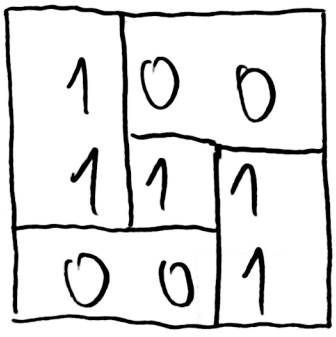
$\operatorname{rank}_{GF[2]}(M) \leq \operatorname{rank}_{\mathbb{R}}(M)$

VETA: $D(f) \leq \operatorname{rank}(M_f) + 1$. (CVIČENIE)

log-rank CONJECTURE:

$D(f) \leq \log^{O(1)} \operatorname{rank}(M_f)$

POZOR:



KAŽDÝ PROTOKOL ZODPOVEDÁ POKRYTIU OBDĹŽNIKMI, ALE NAOPAK TO NEPLATÍ

13.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI II

NEDETERMINISTICKÝ MODEL KOM. ZLOŽITOSTI

PRÍKLAD: PRE $\overline{EQ}$ STAČÍ, ABY ROZHODCA POSLAL ALICI A BOBOVI INDEX, KDE SA x LÍŠI OD y

⇒ NED. KOM. ZLOŽITOSŤ JE $\log n + 2$

VETA: EQ MÁ NED. KOM. ZLOŽITOSŤ $n+1$

NOTÁCIA: $N^0(f)$ ... NED. KOM. ZL. $\overline{f}$

$N^1(f)$ ... NED. KOM. ZL. f.

TVRDÍME, ŽE $N^0(EQ_n) \leq \log n + 2$

$N^1(EQ_n) = n \pm 1$ ...

DÁ SA ĽAHKO NAHLIADNUŤ, ŽE

$N^1(f) \leq \log($# JEDNOTKOVÝCH OBDĹŽNIKOV POKRÝVAJÚCICH JEDNIČKY $f) + 2$

DÁ SA UKÁZAŤ AJ OPAČNÁ NEROVNOSŤ:

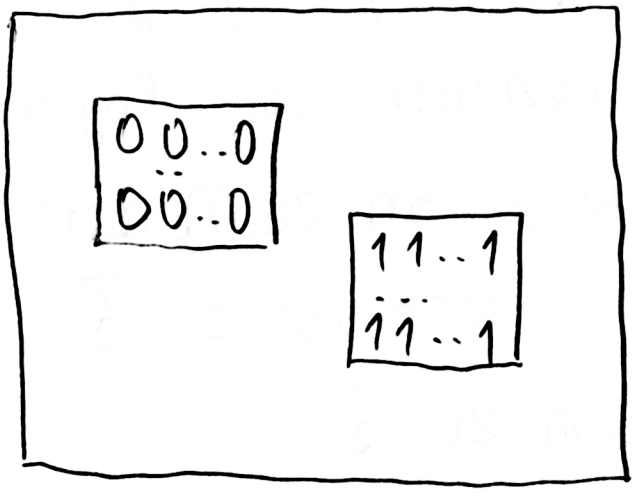
$$N^1(f) \geq \log\left(\text{MIN. \# OBDĹŽNIKOV ...}\right)$$

ROZHODCA VLASTNE URČÍ, AKÝ PROTOKOL MÁ ALICA A BOB POUŽIŤ...

PRE EQ JE MIN. # OBDĹŽNIKOV 2^n ..

VETA: $D(f) \leq O\left(N^0(f) \cdot N^1(f)\right)$

DÔKAZ.



1) VYZNAČENÉ OBDĹŽNIKY ZDIEĽAJÚ RIADOK
2) VYZNAČENÉ —II— STĹPEC
3) —II— NIČ NEZDIEĽAJÚ

PROTOKOL: POMOCOU 1-OBDĹŽNIKOV BUDEME V KAŽDOM KROKU ELIMINOVAŤ POLOVICU 0-OBDĹŽNIKOV

13.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. II

ALICA: - KEĎ VŠETKY 0-OBDĹŽNIKY SÚ PRÁZDNE ⇒ VÝSTUP 1

- INAK NÁJDE 1-OBDĹŽNIK, KTORÝ POKRÝVA x, A TENTO 1-OBDĹŽNIK POKRÝVA MAXIMÁLNE 1/2 ZVYŠNÝCH 0-OBDĹŽNIKOV (V RIADKOCH)
  ... PRÍSLUŠNÉ ČÍSLO POŠLE BOBOVI

BOB: - KEĎ ALICA NAŠLA 1-OBD.
  POKRAČUJE ĎALŠÍM KOLOM

- NÁJDE 1-OBDĹŽNIK, KT. POKRÝVA y
  .... (V STĹPCOCH)
- POKIAĽ ¬∃ ⇒ VÝSTUP 0
  INAK POŠLE ALICI PRÍSLUŠNÉ ČÍSLO

ZLOŽITOSŤ 1 KOLA JE $N^1(S)$.

OBDĹŽNIK SA STANE PRÁZDNYM, KEĎ HO NEPRETNE ODOSLANÝ 1-OBDĹŽNIK

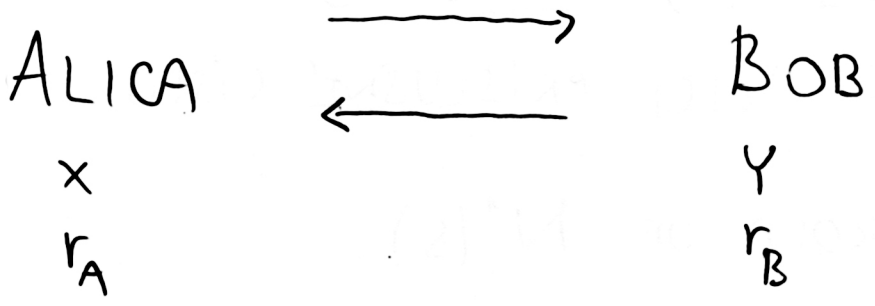
KEĎ $f(x,y)=1$, POTOM ALICA / BOB ZNÍŽIA POČET ZVYŠNÝCH 0-OBDĹŽNIKOV NA $\frac{1}{2}$.

TAKŽE PO $O(N^0(f))$ KOLÁCH ZABIJÚ VŠETKY 0-OBDĹŽNIKY A ALICA VRÁTI VÝSTUP 1.

KEĎ $f(x,y) = 0$, POTOM 0-OBDĹŽNIK OBSAHUJÚCI (x,y) NEMÔŽE NIKDY ZOSTRIEŤ
$\Rightarrow$ PO NAJVIAC $O(N^0(f))$ KROKOCH BOB VRÁTI VÝSTUP 0. □

PRAVDEPODOBNOSTNÁ KOMUNIKAČNÁ ZLOŽ.

- ALICA DOSTANE PRED SPUSTENÍM PROTOKOLU NÁHODNÝ REŤAZEC r_A
- BOB DOSTANE ... r_B



EXISTUJE VEĽA VARIÁNT PODĽA TOHO, ČO OD TOHO PROTOKOLU CHCEM ...

- CHYBA $\leq \varepsilon$ $R_\varepsilon(f)$
- JEDNOSTRANNÁ CHYBA ... $R^1_\varepsilon(f)$

13.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. II

PRÍKLAD: $R_{\varepsilon}(EQ)$

- JE MOŽNÉ APLIKOVAŤ SAMOOPRAVNÉ KÓDY D. NAJSKÔR APLIKUJEME SAM.OOP. KÓD A POTOM VYBERIEME A POROVNÁME TIETO KÓDY NA NA $\log n$ NÁH. POZÍCIACH
- AK BY BOLI NÁH. BITY ZDIEĽANÉ, POTOM STAČÍ POROVNAŤ PARITY NÁHODNE VYBRANÝCH PODMNOŽÍN (HADAMARDOV KÓD)
- ZVOLÍ SA NÁH. PRVOČÍSLO Z PRVÝCH n^2 PRVOČÍSIEL. ALICA INTERPRETUJE x AKO CELÉ ČÍSLO A POŠLE $(x \bmod p, p)$
- BOB ODPOVIE, ČI $x \equiv y \pmod p$.
(VID ČÍNSKA VETA O ZVYŠKOCH)

... PRÍSTUP PODOBNÝ HASHOVANIU ...

SÚKROMNÉ VS VEREJNÉ NÁHODNÉ BITY

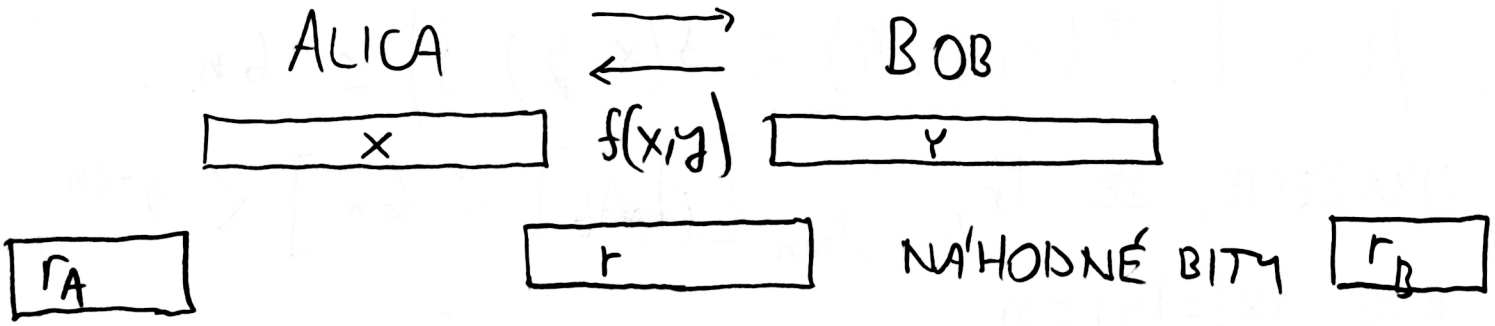
→ NASLEDUJÚCA PREDNÁŠKA

20.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. II

27.05.2011 ... PREDNÁŠKA ODPADÁ
4. SÉRIA ... NA WEBE → VYRIEŠIŤ NA SKÚŠKU
OD 1. AUGUSTA NIE JE MOŽNÉ ÍSŤ NA SKÚŠKU

KOMUNIKAČNÁ ZLOŽITOSŤ



AK SÚ NÁHODNÉ BITY ZDIEĽANÉ, POTOM

$$R^{pub}_{1/3}(EQ) = O(1)$$

PRE SÚKROMNÉ NÁHODNÉ BITY JE:

$$R^{priv}_{1/3}(EQ) = O(\log n)$$

OBECNE PLATÍ: $\forall f : R^{priv}_{1/3+\varepsilon}(f) \leq R^{pub}_{1/3}(f) + O(\log n)$

(NEWMAN 90') MÁME PROTOKOL PRE f, KT. POUŽÍVA VEREJNÉ NÁHODNÉ BITY A t BITOV KOMUNIKÁCIE
ZOSTROJÍME PROTOKOL SO SÚKROMNÝMI NÁH. BITMI A $t + O(\log n)$ BITMI KOMUNIKÁCIE

VYBERIEME $10n$ NÁH. RETAZKOV $r_1, \dots, r_{10n}$

PROTOKOL P: ALENKA NÁHODNE VYBERIE $i \in \{1, \dots, 10n\}$ A POSLE BOBOVI $A + B$ KONUNIKUJÚ AKO S NÁH. BITMI r_i

---

UVAZUJME PEVNÉ x, y. AKÁ JE PRAVD., ŽE PRE NÁHODNE ZVOLENÉ $r_1, \dots, r_{10n}$

$$\left| \{ i \mid P(x, y, r_i) = f(x, y) \} \right| \geq 6n .$$

UKÁŽEME, ŽE $Pr_{r_1, \dots, r_{10n}} [\, |\dots| < 6n \,] < 2^{-2n}$,

KDE $|x| = |y| = n$.

$$Pr_{r_1, \dots, r_{10n}} [\, |\dots| < 6n \,] =$$

$$p := \sum Pr [\, P(x, y, r) = f(x, y) \,] \geq \frac{2}{3}$$

$$= \sum_{S \subseteq \{1, \dots, 10n\}, |S| \geq 4n} p^{10n - |S|} (1-p)^{|S|} \leq \dots \leq 2^{-2n}$$

CVIČENIE

JE MOŽNÉ POUŽIŤ CHERNOFFOVU NEROVNOSŤ. □

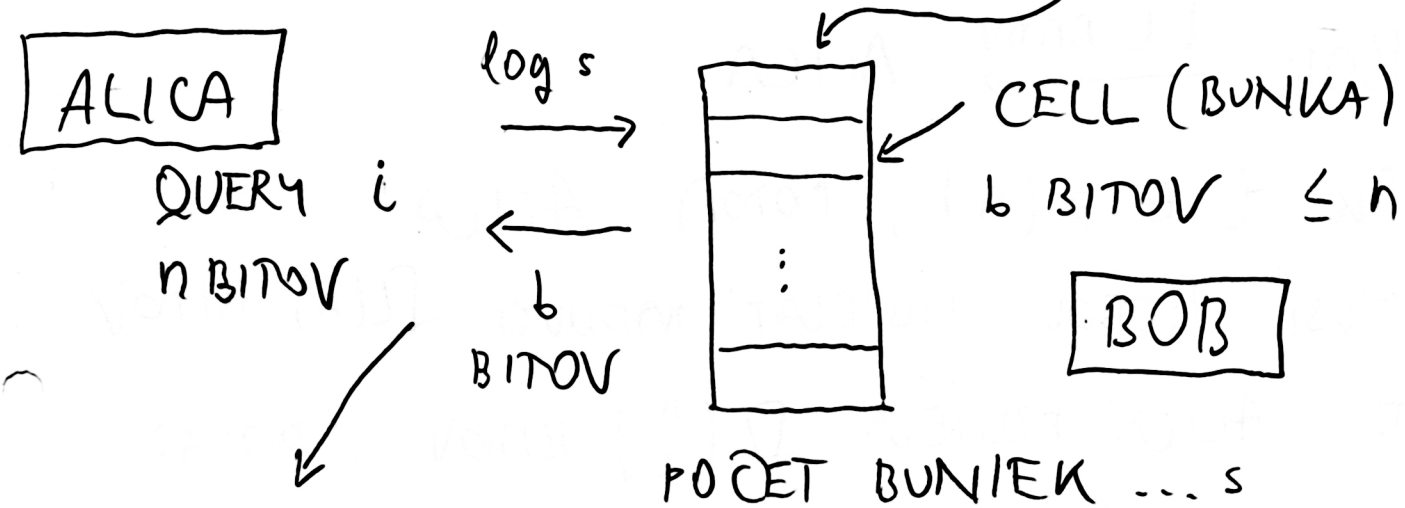
20.05.2011 Fr
PETER ČERNO

NTIN086 VYBRANÉ KAPITOLY Z VÝP. SLOŽ. II

POUŽITIE PRE DOLNÉ ODHADY PRE DÁTOVÉ ŠTRUKTÚRY (CELL PROBE MODEL)

$S \subseteq \{1, \ldots, N\}$ (NAPR. $|S| \sim \text{poly} \log(N)$)

CHCEME DAT. ŠTRUKTÚRU, KT. ODPOVEDÁ NA DOTAZY TYPU $i \in S$?



KOMUNIKÁCIA BEŽÍ t KÔL

DAT. ŠTRUKTÚRA OBSAHUJE POPIS NEJAKÉHO PODPRIESTORU $V \subseteq GF_2^n$

QUERY $i \in GF_2^n$ ... DOTAZ $i \in V$?

ALICA (i) $\rightleftharpoons$ BOB (V)

VETA: KAŽDÝ PROTOKOL POSIELA BUĎ RÁDOVO $\Omega(n)$ BITOV OD ALICI K BOBOVI, ALEBO $\Omega(n^2)$ BITOV OD BOBA K ALICI.

BEZ DÔKAZU. □

DÔSLEDOK: $s = 2^{\Omega(n/t)}$

UVAŽUJME $b = n$ A # DOTAZOV t

BOB $\xrightarrow{bt \text{ BITOV}}$ ALICA

AK $t \in o(n)$, POTOM ALICA MUSÍ BOBOVI POSIELAŤ RÁDOVO $\Omega(n)$ BITOV

T. ALICA POSIELA $\Omega(\frac{n}{t})$ BITOV / DOTAZ

$\Rightarrow \log s \geq \Omega(\frac{n}{t})$. □