# Kolmogorovská zložitosť

28.11.2013

honest funkcia $f$ — $f : \{0,1\}^* \to \{0,1\}^*$ ak $\exists k \in \mathbb{N}$, že $\forall x \in \{0,1\}^*$

$$l(f(x)) \leq l(x)^k + k, \; l(x) \leq l(f(x))^k + k$$

**Lemma**

*Nech $f$ je honest, počitateľná strojom $T$ v polytime. $\forall t \geq 1$ a takmer $\forall n$ (až na konečne veľa)*

$$f(C[\log\log n, n^t, \infty]) \subseteq C[\log n, n^{\log\log n}, \infty]$$

$\forall x \in C[\log\log n, n^t, \infty]$ $\exists y$ dĺžky $l(y) \leq \log\log n$, že $T'(y) = x$ v polytime

$f(x)$ počítame

- na základe $y$ $T$ $T'$ $\qquad C(f(x)) \leq l(y) + O(1) \leq \log n$
- čas
  - $y \rightsquigarrow x$ v $n^t$
  - $x \rightsquigarrow f(x)$ v polytime

  $\hookrightarrow$

  $n^{t_1} + n^{t_2} = O(n^{\log\log n})$

□

**Theorem**

*Existuje rekurzívne orákulum $A$ také, že $P^A \neq NP^A$* *//Baker-Gill-Solovay*

- $f(1) = 2$
  $f(k) = 2^{f(k-1)}$
- zoberme $B \subseteq \{1^{f(k)} : k \geq 1\}$ a $B \in DTIME[n^{\log n}] - P$

  $B \in NP^A, B \notin P^A$
- skonštruujeme $A$
  — $\forall k : \ 1^{f(k)} \in B$

  $A \leftarrow$ prvý reťazec dĺžky $f(k) \in C[\log n, n^{\log n}, \infty] - C[\log n, n^{\log \log n}, \infty]$

$\hookrightarrow T^?$ sa pýta na slová mimo $A$ alebo nie dlhšie ako $\log n$

$\hookrightarrow$ membership pre $l(y) \leq \log n$ v čase $O(\log n)^{\log \log n} = O(n^k)$

$B \in P^A \Rightarrow B \in P \Rightarrow$ spor s $B \notin P$

□

Množiny sú P-izomorfné, ak existuje polynomiálne počitateľná bijekcia medzi nimi

Bermann -Hartmanis predpoklad: $\forall$ NPÚ sú P-izomorfné

**Theorem**

*Ak existuje* $L \in P$ *taký, že* $L \subset SAT$ *a*

$$C[\log n, n^{\log n}, \infty] \cap SAT \subseteq L$$

*Potom* $SAT - L \in NPÚ$, *ale NIE JE P-izomorfný so SAT*

- $SAT - L \in NPU \rightsquigarrow$ redukciou $SAT \rightsquigarrow SAT - L$
  - $\forall x \in L \quad x \rightsquigarrow \omega \in SAT - L$
  - $\forall x \notin L \quad x \rightsquigarrow x$
- keby existoval P-izomorizmus $h$ medzi $SAT, SAT - L$, bol by honest fcia v $P$
  $\hookrightarrow \quad h(SAT \cap C[\log\log n, n^3, \infty]) \subseteq C[\log n, n^{\log\log n}, \infty]$
- keďže $SAT \cap C[\log\log n, n^3, \infty] \neq \emptyset$, $h(SAT \cap C[\log\log n, n^3, \infty]) \notin SAT - L$

□

množina $A$ je exponentially low ak $E^A = E,\ E = \cup_{C \in \mathbb{N}} DTIME(2^{cn})$

**Theorem**

*Existuje exponentially low riedka $A$, ktorá nie je v $P$.*

Nech $B = C[n/2, 2^{3n}, \infty], \overline{B} = B^C$

$A = \{x \mid x \text{ je lexikograficky prvé z } \overline{B} \text{ také, že } l(x) = 2^{\left.2^{\cdots^2}\right\}^m}, m > 0\}$

- $A \in E$
- $A \notin P$ SPOROM
  ak $T,\ L(T) = A \subseteq \overline{B}$ v polytime
  – $\log n$, popis $T$,
  hľadáme $x \in \{0,1\}^n, n > 2(l(T) + \log n)$, aby $x \in A$ $\hookrightarrow$ spor, $x \in B$
- $E^A = E$ nech $T^A$ počíta v $2^{cn}$

**Fakt**

*Pre $c' > 3c + 3$ $T^A$ sa nemôže pýtať na "$y \overset{?}{\in} A$ ak $l(y) \geq c'n, y \in A$"* $\hookrightarrow$

$A$ vieme simulovať BEZ orákula — dotaz na slovo

- dlhšie ako $c'n$ – NIE
- kratšia ako $c'n$ – prehľadávaním zistíme odpoveď □

Pre $c' > 3c + 3$ $T^A$ sa nemôže pýtať na "$y \overset{?}{\in} A$" ak $l(y) \geq c'n,\ y \in A$

SPORom — Nech $y$ je prvý v $A : l(y) > c'n$, na ktorý sa $T^A$ pýta //pri vstupe $x, l(x) = n$

že $y \in B$ : $//B = C[n/2, 2^{3n}, \infty], \overline{B} = B^C$

- zápis $A^{<c'n}$ v $2 \log c'n$
- rekonštrukcia $y$, na ktoré sa pýtame v čase $t < 2^{cn}$, simuláciou $T^A(x)$ po čas $t$

| | |
|---|---|
| - diskusia + popis $T^A$ | $O(1)$ |
| - $x$ | $n$ |
| - popis $A^{<l(y)} = A^{<c'n}$ | $2 \log c'n$ |
| - popis $t$ | $cn$ |

$$c' \frac{n}{2} > (c+1)n + 2 \log c'n + O(1)$$

- čas $\quad 2^{cn} < 2^{c'n} \leq 2^{l(y)} \quad y \in B = C[l(y)/2, 2^{3l(y)}, \infty]$

$y \in B \Rightarrow\ y \notin \overline{B}$, pričom $A \subseteq \overline{B}$ ◇

$L$ je **P-printable** ak $\exists k \in \mathbb{N}$ také, že $\forall$ prvky z $L^{\leq n}$ vypíšeme v čase $\mathbf{n^k + k}$

**Theorem**

$L \subseteq \{0,1\}^*$. *Nasledujúce podmienky sú ekvivalentné*

1. *L je P-printable*
2. *L je riedka a má P-time vypočitateľný ranking* //$r_L(x) = d(\{y; y \leq x\})$
3. *L je P-izomorfný s nejakou tally množinou* $\in P$ //tally $\subseteq \{a\}^*$
4. $L \in C[k \log n, n^k, \infty]$ *a* $L \in P$

$1 \Rightarrow 2$ ✓

$2 \Rightarrow 3$

- $L$ polytime ranking $r_1$, $d(L^{\leq n}) \leq p(n)$
- $\mathbf{r_2(x) = 1x - r_1(x)}$ je ranking pre $L^c$
- $T = \{0^{np(n)+i} : r_1(1^{n-1}) < i \leq r_1(1^n))\}$ je tally v P
- $\mathbf{r_3}$ ranking pre $\{0\}^* - T$
- p mapuje $x$ na $\begin{cases} 0^{np(n)+\mathbf{r_1}(x)}, & x \in L \\ r_3^{-1}(r_2(x)) & x \notin L \end{cases}$

  p je P-izomorfizmus
  – v P-time
  – $x \in L \rightsquigarrow$ jednoznačná hodnota v T; $0^{np(n)+\mathbf{r_1}(x)} \in T \rightsquigarrow$ jednoznačne $x \in L$

$3 \Rightarrow 4$ $//L$ je P-izomorfný s nejakou tally množinou $\in P \Rightarrow$ $L \in C[k \log n, n^k, \infty]$

- P izomorfizmus $f$, $f$ a $f^{-1}$ počitateľné v $n^c$, $L \leftrightarrow$tally T, $T \in P \quad \rightsquigarrow L \in P$
- $f$ počitateľná v $n^c$, $l(f(x)) \leq n^c, n = l(x)$
  - $\hookrightarrow$ binárna reprezentácia $f(x)$ $c \log n$
  - $\hookrightarrow$ namiesto $x$ povieme $f(x)$ $C[k \log n, n^k, \infty]$

$4 \Rightarrow 1$ $//L \in P$, $L \in C[k \log n, n^k, \infty]$ potom $L$ je P-printable

pre vstup $x, l(x) = n$

- simuluj $n^k$ krokov $\forall$ programu dĺžky $k \log n$
- ak stihol vypísať $y$, over či $y \in L, l(y) = n$; ak áno, vypíš $y$ $//y = x$
- $P$-time ✓

□

čiastočný program $p$ — $0,1,\perp$;
charakteristická funkcia množiny $A$ $\quad A(x) = 1 \Leftrightarrow x \in A$;
funkcia $p$ je konzistentná s $A$ ak $p(x) \neq \perp \Rightarrow p(x) = A(x)$

$time_T(p, y)$– čas stroja T, keď podľa programu $p$ spracováva vstup $y$

**Def.**

*(t-ohraničená) instance zložitosť reťazca $x$ vzhľadom k $T, A$*

$$ic^t_T(x : A) = \min\{l(p) : \; T(p, x) \neq \perp \; a \; \forall y T(p, y) \neq \perp \Rightarrow time^t_T(p, y) \leq t(l(y)), T(p, y) = A(y)\};$$
*resp. $\infty$, ak $p$ neexistuje*

**Fakt (invariance)**

*Existuje univerzálny TS $U$, že $\forall T \; \exists c \; \forall A, t, x$*
$ic^{t'}_U(x : A) \leq ic^t_T(x : A) + c$ *kde* $t'(n) = ct(n) \log t(n) + c$

**Example**

- $CD^t(x) = ic^t(x : \{x\})$
- $t'(n) = ct(n) \log(n) + c$
  $ic^{t'}(x : A) \leq C^t(x) + c$
  $ic^{t'}(x : A) \leq CD^t(x) + c$

domnienka Nech $t(n)$ je vypočitateľná v $t'(n) = ct(n) + c$, $A$ je rekurzívna množina. Ak $A \notin DTIME(t(n))$, potom $\exists c$ a nekonečne veľa $x$, že

$$ic^t(x : A) \geq C^{t'}(x) - c$$

## Lemma

*$A \in P \Leftrightarrow \exists$ polynóm $t$ a konštanta $c$, $\forall x$ $ic^t(x : A) \leq c$*

$\Rightarrow$ $A \in P \Rightarrow ic^t(x : A) \leq c$ pre polynóm $t$ ✓

$\Leftarrow$ $B$=$\{p \mid l(p) \leq c$, p je konzistentný s $A$, čas nanajvýš $t(n)\}$

$x \overset{?}{\in} A$ simuláciou $\forall p \in B$ □

## Def. (polynomiálne jadro)

*Nech $A$ je rekurzívna. Nekonečná množina $C$ je polynomiálne jadro $A$ ak každý totálny program $p$, ktorý rozhoduje $A$, a polynóm $t$, $time_p(x) > t(l(x))$ $\forall x \in C$ až na konečne veľa.*

*//$C$ nemusí byť podmnožina $A$!*

**Lemma**

*C je polynomiálne jadro A* $\Leftrightarrow$ $\forall$ *polynóm t a konštantu c*

$$ic^t(x : A) > c \text{ až na konečne veľa } x \in C$$

$\Rightarrow$

- nech by nekonečne veľa $x \in C : ic^t(x : A) \leq c$; $t$ polynóm
- $B$- programy $p$ konzistentné s $A$, $l(p) \leq c, time_p() \leq t(n)$

  $\hookrightarrow$ nekonečne veľa prvkov v $C$ identifikovaných simulovaním konečnej množiny programov SPOR

$\Leftarrow$

- ak $C$ NIE JE poly.jadro $A$, tak $\exists$ program

  $p$, polynóm $t$, že pre nekonečne veľa $x \in C$ $time_p(x) \leq t(l(x))$ // p konzistentný s A
- modifikácia $p$ – po $t(n)$ krokoch HALT

$$ic^{t'}(x : A) \leq c \text{ pre nekonečne veľa } x \in C$$

□

$IC[\log, poly]$ množiny $A$, pre kt. $ic^t(x : A) \leq c \log l(x) + c$, kde $t$ je polynóm
$SAT$ $\Phi(x_1, \ldots, x_k)$ v KNF, $l(\Phi(x_1, \ldots, x_k)) = n$; $k, n$ polynomiálne ekv.

**Theorem**

$SAT \in IC[\log, poly] \Rightarrow NP = P$

- $SAT \in IC[\log, poly] \Rightarrow ic^t(\Phi : SAT) \leq c \log l(\Phi) + c$
- pre $\Phi$ v KNF existuje $p_\Phi$ : $l(p_\Phi) \leq c \log(l(\Phi)) + c$, že korekte rozhodne $\Phi \stackrel{?}{\in} SAT$ a konzistentný so $SAT$
- $\Phi(x_1, \ldots, x_k)$, $l(\Phi) = n$
- $A = \{p : l(p) \leq c \log n + c\}$ $\quad$ $d(A) \leq q(n)$

Nech $p_0$ korektne rozhoduje $\Phi \stackrel{?}{\in} SAT$ potom procedúra SAT v polytime

– alebo korektne rozhodne $\Phi \stackrel{?}{\in} SAT$
– alebo z $A$ vyhodí $p \neq p_0$ nekonzistentný so $SAT$

## procedúra SAT

krok 1 simuluj všetky $p \in A$ nanajvýš $t(n)$ krokov so vstupom $\Phi(x_1, \ldots, x_k)$
ak žiaden program nezamieta, tak return(akceptuj)
ak žiaden program neakceptuje, tak return(zamietaj)

krok 2 //existujú aj akceptujúce aj zamietajúce programy
pre $i = 1, 2, \ldots, k$ postupne:
nech už máme $b_1, \ldots b_{i-1}$, $p \in A$ akceptuje $\Phi = \Phi(b_1, \ldots, b_{i-1}, x_i, \ldots, x_k)$

- simuluj $q \in A$ so vstupmi
  $\Phi_0 = \Phi(b_1, \ldots, b_{i-1}, 0, x_{i+1}, \ldots, x_k)$ a
  $\Phi_1 = \Phi(b_1, \ldots, b_{i-1}, 1, x_{i+1}, \ldots, x_k)$
- ak žiaden z programov neakceptuje, tak
  – $\Phi(b_1, \ldots, b_{i-1}, x_i, \ldots . x_k) \notin SAT$
  – $p \neq p_0$ nie je konzistentný so $SAT$ $A \leftarrow A - p$
- ak jeden zo vstupov JE akceptovaný, tak $b_i \leftarrow x_i$

koniec po kroku 1 ✓
koniec s $b_1, \ldots, b_k$:
**if** $\Phi(b_1, \ldots, b_k) = 1$ **then** return($\Phi \in SAT$)
**else** $A \leftarrow A - p$

□

$L = \{x_1 * x_2 * \cdots * x_k \# y_1 * y_2 * \cdots * y_\ell \# \# 0^i 1^j,\ x_i = y_j\}$

rozpoznávanie $L$

- na 2-páskovom on-line v lineárnom čase
- na 1-páskovom on-line vyžaduje čas $\Omega(n^{3/2}/\log n)$

↪ Simulácia lineárneho 2-páskového on-line na 1-páskovom on-line vyžaduje čas $\Omega(n^{3/2}/\log n)$

1páskový on-line T:

$h_1, h_2$ – pozícia hlavy na vstupe, resp. pracovnej páske
$S$ – súvislý segment vstupnej pásky
$R$ – súvislý segment pracovnej pásky

$T$ zobrazuje $S$ DO $R$, ak $h_2$ neopustí $R$ kým je $h_1$ v $S$
$T$ zobrazuje $S$ NA $R$, ak $h_2$ prečíta $R$ kým je $h_1$ v $S$

$x\# = x_1 * x_2 * \cdots * x_k\#, \ \forall i \ l(x_i) = l(x)/k$

$R$ je taký segment na p.páske, že $T$ zobrazuje $\forall$ segment z $S = \{x_{i_1}, \ldots, x_{i_\ell}\}$ do $R$

**Lemma**

*Obsah pracovnej pásky v čase, keď $h_1$ dorazila na $\#$ vieme zrekonštruovať, keď poznáme*

- $\overline{S} = \{x_i \mid 1 \leq i \leq k\} - S$
- *výsledný obsah segmentu $R$*
- *prechodové postupnosti okolo $R$* $l_R, r_R$
- *popis $T$ +diskusia*

miesta blokov z $S$ necháme prázdne

— zrekonštruujeme pásku naľavo od $r_L$

— zrekonštruujeme pásku napravo od $r_R$

NECH 1-páskový $T$ rozpoznáva $L$ v čase $T_1(n) < c^{-5} n^{3/2} / \log n$

- vezmime $x \in \{0,1\}^*,\ l(x) = n,\ C(x) \geq n,\ x = x_1 \ldots x_k,\ k = \sqrt{n},\ |x_i| = \sqrt{n} \forall i$
- uvažujme vstup $x_1 * x_2 * \ldots * x_k \#$ hlava na $\#$ v čase $t_\#$

$\Rightarrow$ ak sa viac ako $k/2$ z $x_i$ sa zobrazí NA segment veľkosti aspoň $n/c^3$, tak pre čas $T$

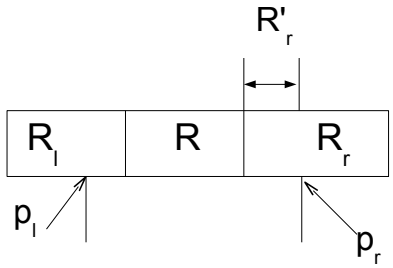
$$T_1 = \Omega(n/c^3 \cdot \underbrace{\sqrt{n}/2}_{k/2}) = \Omega\left(n^{3/2}\right)$$

$\Rightarrow$ teda $S$ obsahuje $k/2$ blokov $x_i$, ktoré sa zobrazia DO segmentu veľkosti $\leq n/c^3$
$x_m$ - medián pri usporiadaní podľa ľavých okrajov segmentov, do kt. sa zobrazia

1. veľa $x_i \in S$ sa zobrazí do malého $R$ //lema
2. neexistuje taký $R$ a segmenty sú rozložené "rovnomerne"
   //$y_j$ umiestnime ďaleko od $x_i$

1. existuje $k/c$ blokov $x_i \in S$ a segment $R$ dĺžky $n/c^2$, že sa všetky zobrazia do $R \rightsquigarrow \overline{S}$

$|R_l| = |R| = |R_r|$,
$p_l, p_r$ pozície PP v $R_l, R_r$, kt. sú najkratšie




AK $l(PP(p_r)), l(PP(p_l)) > \sqrt{n}/(c^2 \log n)$, potom čas aspoň $\sqrt{n}/(c^2 \log n) \cdot n/c^2$

PRETO $l(PP(p_r)), l(PP(p_l)) \leq \sqrt{n}/(c^2 \log n)$ :

krátky program pre $x$

- diskusia + popis $T_1$ — $O(1)$
- hodnoty $n, k, c, p_l, p_r$ — $O(\log n)$
- zreťazenie $\{x_i, \ldots, x_k\} - \overline{S}$ — $n - n/c$
- stav $T$ a pozícia $h_2$ v čase, keď $h_1$ sedí na $\#$ — $O(\log n)$
- 2 prechodové postupnosti na pozíciách $p_l, p_r$ v čase $t_\#$ — $2\sqrt{n}(l(T) + O(\log n))$
- obsah $R'_l R R'_r$ v $t_\#$ — $3n/c^2 + O(\log n)$

overíme, že kandidát $y = x$

- $l(x) = l(y)$
- rekonštrukcia pamäťovej pásky, keď $h_1$ prvýkrát vstúpila na $\#$
- $y \quad \hookrightarrow \quad y_1 * \ldots * y_k$;
  $\forall 0^i 1^i$ zbehneme simuláciu $T_1$ od $t_\#$
  akceptuje len ak $x = y$

$$C(x) \leq n - \frac{n}{c} + \underbrace{\frac{3n}{c^2} + O(\sqrt{n}\log n) + O(\log n)}_{\leq \frac{n}{c}} \leq \gamma n; \quad 0 < \gamma < 1$$

spor s $C(x) \geq n$

2. pre $\forall$ blok $R$ veľkosti $l(R) = n/c^2$ existuje nanajvýš $k/c$ blokov $x_i \in S$, kt. sa zobrazia do neho

- do $R_m$ sa zobrazí medián $x_m$
- aspoň $k/6$ napravo od $R_m \quad \hookrightarrow \quad S_r = \{x_{i_1}, \ldots, x_{i_{k/6}}\}$
  analogicky $S_l$ naľavo od $R_m \hookrightarrow \quad S_l = \{x_{j_1}, \ldots, x_{j_{k/6}}\}$
- $y_1 = x_{i_1}, y_2 = x_{j_1}, \ldots$ $\qquad$ $x_{j_s} = y_{2s}, \quad x_{i_s} = y_{2s-1}$
- pre vstup $I = x_1 * x_2 * \cdots * x_k \# y_1 * \cdots y_{k/3} \#$ existuje dvojica $y_{2s-1} * y_{2s}$, že sú namapované do segmentu menšieho ako $n/(4c^2)$ //inak čas aspoň $\frac{k}{6} \cdot \frac{n}{4c^2} = \frac{n^{3/2}}{24c^2}$
- $y_{2s-1}, y_{2s}$ vo vzdialenosti aspoň $n/c^3$ od $x_{i_s}$ alebo $x_{j_s}$, w.l.o.g. od $x_{i_s}$
  $\hookrightarrow x_{i_s} \ldots R \ldots y_{2s-1}$,
- suffix $0^{i_s} 1^{2s-1}$
- $l(R) = n/c^3$, $p$ pozícia najkratšej prechodovej postupnosti v $R$, kt. dĺžka je $\max \sqrt{n}/(c^2 \log n)$

krátky popis $x$

- diskusia + popis $T_1$ — $O(1)$
- $n, k, c$, pozícia $p$ — $O(\log n)$
- $S - \{x_{i_s}\}$ — $n - \sqrt{n}$
- index $i_s$ — $O(\log n)$
- prechodová postupnosť na pozícii $p$ — $\leq \sqrt{n}/c$
  // dľžka max $\sqrt{n}/(c^2 \log n)$

$$C(X) \leq n - \sqrt{n} + \sqrt{n}/c + O(\log n) \leq n - \gamma\sqrt{n}$$

spor s $C(x) \geq n$