Kolmogorovská zložitosť

14.11.2013

automorfizmus - permutácia vrcholov π taká, že $(\pi(u), \pi(v)) \in E \Leftrightarrow (u, v) \in E$

- grupa (skladanie, identita)
- $G, \pi(G)$ majú rovnaké štandardné kódovanie $E(G) = E(\pi(G))$

rigid/stabilný graf $\leftrightsquigarrow$ jediným automorfizmom je identita

$g(n)$ počet neočíslovaných n-vrcholových grafov

$\mathcal{G}_n$ trieda neorientovaných grafov na $\{0, 1, \ldots, n-1\}$
$\mathcal{G}_n = \mathcal{G}_n^0 \cup \mathcal{G}_n^1 \cup \mathcal{G}_n^n$ v $\mathcal{G}_n^m$ sa každým automorfizmom pohne m vrcholov

$S(n)$ grupa permutácií n-prvkovej množiny

$\overline{G}$ trieda grafov izomorfných s G

$Aut(G)$ grupa automorfizmov grafu G

Theorem

Počet neočíslovaných n-vrcholových grafov $g_n \sim \dfrac{2^{\binom{n}{2}}}{n!}$

- $g_n = \sum_{G \in \mathcal{G}_n} \dfrac{1}{d(\overline{G})}, \quad d(\overline{G}) = \dfrac{d(S_n)}{d(Aut(G))} = \dfrac{n!}{d(Aut(G))}$
- $g_n = \sum_{G \in \mathcal{G}_n} \dfrac{d(Aut(G))}{n!} = \dfrac{2^{\binom{n}{2}}}{n!} E_n, \; E_n = \sum_{G \in \mathcal{G}_n} Pr(G) d(Aut(G)); \; E_n > 1; \; \mathcal{G}_n^1 = \emptyset$

  F1 $\forall G \in \mathcal{G}_n^m, \; d(Aut(G)) \leq \binom{n}{m} m! \leq n^m = 2^{m \log n}$ ✓

  F2 $Pr(G \in \mathcal{G}_n^m) \leq 2^{-m(\frac{n}{2} - \frac{3m}{8} - 2 \log n)}$!!KZ

- $E_n = \sum_{m=0}^{n} Pr(G \in \mathcal{G}_n^m) Avg_{G \in \mathcal{G}_n^m} d(Aut(G)) \leq 1 + \sum_{m=2}^{n} 2^{-m(\frac{n}{2} - \frac{3m}{8} - 2 \log n)}$
  $\leq 1 + 2^{-n + 4 \log n + 2}$
- $\dfrac{2^{\binom{n}{2}}}{n!} \leq g(n) \leq \dfrac{2^{\binom{n}{2}}}{n!} \left(1 + \dfrac{4n^4}{2^n}\right)$

$F2 \quad Pr(G \in \mathcal{G}_n^m) \leq 2^{-m(\frac{n}{2} - \frac{3m}{8} - \log n)}$

- π, m vrcholov $i_1 < \dots i_m$ sa pohne $\quad \pi(\mathbf{i_1}), \dots, \pi(\mathbf{i_m})$ $\quad m \log n$
- $\pi \rightsquigarrow k$ cyklov veľkosti $c_1, \dots, c_k$, v každom najmenší zvolený

- nezvolený
  – netreba hrany do stabilných $\quad -(n-m)$
  – netreba niektoré hrany do nezvolených $\quad -\frac{m-k}{2}$

$$\sum_{i=1}^{k}(c_i - 1)(n - m + \frac{m-k}{2}) = (m-k)(n - \frac{m+k}{2})$$

$$m \log n - (\mathbf{m} - \mathbf{k})(\mathbf{n} - \frac{\mathbf{m}+\mathbf{k}}{\mathbf{2}}) = \underbrace{-\frac{m}{2}(n - \frac{3m}{4} - 2\log n)}_{\delta(n,m)} \qquad //k = m/2$$

efektívna enumerácia neočíslovaných grafov

$\mathcal{G} \leftarrow \emptyset$
for all očíslované grafy G–binárne reťazce **do**
  if G nevieme získať premenovaním $H \in \mathcal{G}$ **then**
    $\mathcal{G} \leftarrow \mathcal{G} \cup G$

$$\Downarrow \textit{odhad } g(n) + \textit{Stirling}$$

$$C(E(G)|n) \leq \binom{n}{2} - n \log n + O(n)$$

Theorem

Nech G je očíslovaný n-vrcholový, G_0 jeho neočíslovaná verzia. Potom existujú graf G' a permutácia π tak, že $G' = \pi(G)$ a (až na konštanty)

$$C(E(G')) = C(E(G_0)) \qquad C(E(G)|n) = C(E(G_0), \pi|n)$$

Theorem

ROUTOVANIE po najkratších cestách v $O(\log n)$-náhodných grafoch/sieťach sa dá spraviť s lokálnou pamäťou $6n$, celkovou $6n^2$ bitov.

- nanajvýš dĺžka 2; $u \rightsquigarrow v$ cez $\log n$ najmenších susedov u $\qquad \underline{O(n \log\log n)}$
- $v_i, \dots, v_m$ je $O(\log n)$ najmenších susedov u; $A_0 \subseteq V$ nesusedia u.
- $A_t \overset{def}{:=} \{w \in A_0 - \bigcup_{s=1}^{t-1} A_s : (v_t, w) \in E\}$
- $\mathbf{m_0} = d(A_0)$, $\mathbf{m_{t+1}} = m_t - d(A_{t+1})$
- Nech ℓ je min. také, že $m_\ell < n/\log\log n$
- konštrukcia lokálnej routovacej funkcie $F(u)$
  - tabuľka pre A_0:
    $$\text{pre } w \begin{cases} \in \bigcup_{s-1}^{t} A_s & \text{unárne } v0\text{: } (u,v) \in E, (v,w) \in E \\ \notin \bigcup_{s-1}^{t} A_s, & 0 \end{cases}$$
  - zvyšok (0 v prvej tab) - nanajvýš $m_\ell < n/\log\log n$ explicitne binárne

$O(\log n)$-náhodný graf
$v_i, \ldots, v_m$ je $O(\log n)$ najmenších susedov u;
$A_0 \subseteq V$ nesusedia u; $A_t \stackrel{def}{:=} \{w \in A_0 - \bigcup_{s=1}^{t-1} A_s : (v_t, w) \in E\}$
$\mathbf{m_0} = d(A_0)$, $\mathbf{m_{t+1}} = m_t - d(A_{t+1})$

Nech ℓ je min. také, že $m_\ell < n/\log\log n$. Potom $d(A_t) > m_{t-1}/3$ pre $1 \leq t \leq \ell$

Sporom – AK $\exists t, |d(A_t) - m_{t-1}/2| > m_{t-1}/6$ POTOM krátky popis G

+	u, v_t	$2\log n$
+	charakteristické postupnosti $A_0, \ldots, A_{t-1}$	$r = n-1+\cdots+n-(t-1)$
+	samoodeľujúco A_t v $A_0 - \bigcup_{s=1}^{t-1} A_s$	$m_{t-1} - \frac{2}{3}(1/6)^2 m_{t-1}\log e + O(\log m_{t-1})$
-	netreba hrany $\{v_t\} \times (A_0 - \bigcup_{s=1}^{t-1} A_s)$	$-m_{t-1}$
-	netreba hrany incidentné s $u, v_1, \ldots, v_t$	$-r$

$$n(n-1)/2 - O(\log n) \leq C(E(G)) \leq n(n-1)/2 + O(\log n) + m_{t-1} - \frac{2}{3}(1/6)^2 m_{t-1}\log e - m_{t-1}$$

$$m_{t-1} \leq O(\log n) \quad \bigwedge \quad m_{t-1} > n/\log\log n$$

$A_0 \subseteq V$ nesusedia u; $A_t = \{w \in A_0 - \bigcup_{s=1}^{t-1} A_s : (v_t, w) \in E\}$

ℓ je min. také, že $m_\ell < n/\log\log n$, $d(A_t) > m_{t-1}/3$ pre $1 \leq t \leq \ell$

konštrukcia lokálnej routovacej fcie $F(u)$

- tabuľka pre A_0:

$$\text{pre } w \begin{cases} \in \bigcup_{s-1}^{t} A_s & \text{unárne } v0\text{: } (u,v) \in E, (v,w) \in E \\ \notin \bigcup_{s-1}^{t} A_s, & 0 \end{cases}$$

$$n + \sum_{s=1}^{\ell} \frac{1}{3}\left(\frac{2}{3}\right)^{s-1} sn \leq n + \sum_{s=1}^{\infty} \frac{1}{3}\left(\frac{2}{3}\right)^{s-1} sn \leq 4n$$

- zvyšok (0 v prvej tab) - nanajvýš $m_\ell < n/\log\log n$ explicitne binárne

  $\log\log n + O(n)$ bitov na určenie poradia (mimo $v_1, \ldots, v_m$) $2n$

$$|F(u)| \leq 6n$$

Theorem

Routovanie po najkratších cestách v $o(n)$-náhodných grafoch/sieťach VYŽADUJE lokálnu pamäť $n/2 - o(n)$, celkovo $n^2/2 - o(n^2)$ bitov.

Uvažujme nasledujúci popis

- \+ u — $\log n$
- \+ samooddeľujúco $F(u)$ — $\dot{(}F(u)) + 2\log(d(F(u)))$
- \+ hrany medzi u a zvyškom
- – odstránime $(v, w) \in E$, keď $F(u, w) = v$

  $|d - \frac{(n-1)}{2}| = O(\sqrt{(\delta(n) + \log n)n})$ — ušetríme aspoň $n/2 - o(n)$

$$\frac{n(n-1)}{2} + O(1) + \underbrace{O(\log n) + 2\log(d(F(u)))}_{O(\log n)} + d(F(u)) - \frac{n}{2} + o(n) \geq C(E(G)) \geq \frac{n(n-1)}{2} - o(n)$$

$$d(F(u)) \geq \frac{n}{2} - o(n)$$

KZ s ohraničením

model TS— read-only vstup, write-only výstup, viacpáskový

$\Phi_1, \Phi_2, \ldots$ enumerácia rekurzívnych fcií $\qquad T_\Phi$ - TS, kt. počíta Φ

$C_\Phi^{t,s}(x|y) = \min\{l(p) : \Phi^{t,s}(p,y) = x\}$ $\qquad$ ak $y = \epsilon$, potom $C_\Phi^{t,s}(x)$

$\hookrightarrow$ TS počíta v čase $t(n)$ a priestore $s(n)$

Theorem (invariance theorem)

Existuje univerzálna čiastočne rekurzívna funkcia Φ_0 taká, že $\forall$ čiastočne rekurzívnu fciu Φ existuje konštanta $c, c = c(\Phi)$, pričom $C_{\Phi_0}^{ct\log t, cs}(x|y) \leq C_\Phi^{t,s}(x|y)$

- $T_1, T_2, \ldots$; Φ_i- PRE fcia, kt. počíta T_i, $\langle y, p\rangle = 1^{l(p)}0yp$
- Φ_0 – k UTS s dvomi páskami; $U(y, \langle i, p\rangle) = T_i(y, p)$
- $T_i(y, p) = x,\ t(n),\ s(n)$

$$\left.\begin{array}{ll} \text{prechod na dve pásky} & c' t\log t, c' s \\ \text{ťahanie kódu,} & c'' \end{array}\right\} c \quad \Phi_0^{ct\log t, cs}(\langle y, \langle i, p\rangle\rangle) = \Phi_i^{t,s}(y, p)$$

zložitostné triedy

- $C^{t,s}(x|y) = \min\{l(p) : \; U(\langle y, p\rangle) = x \text{ v čase } t(n) \text{ a priestore } s(n)\}$
- predikát – fcia s hodnotami $0, 1$

  $\Psi_1, \Psi_2, \ldots$ PRF enumerácia; $T_\Psi(x) \in \{0, 1\}$; $T_\Psi^{t,s}$
- $x, y, p \in \mathbb{N}$; Ψ PRF predikát; CD-zložitosť x vzhľadom k Ψ, y

  $CD_\Psi^{t,s}(x|y) = \min\{l(p) : \; \forall v \Psi^{t,s}(v, p, y) = 1 \text{ iff } v = x\}$
- $S \subseteq \mathbb{N}$, $C^{t,s}(x|S)$, $CD^{t,s}(x|S)$ TS s orákulom S
- zložitostné triedy

$$C_\Phi[f(n), t(n), s(n)] = \{x : \; C_\Phi^{t,s}(x) \leq f(n), n = l(x)\}$$

$$CD_\Phi[f(n), t(n), s(n)] = \{x : \; CD_\Phi^{t,s}(x) \leq f(n), n = l(x)\}$$

Theorem (vzťah $C^p - CD^q, K^p - KD^q$)

Nech p, q sú polynómy, $A \in NPU$.
(i.) $\forall p \, \exists q \; CD^q(x) \leq C^p(x) + O(1)$
(ii.) $\forall p \, \exists q \; C^q(x|A) \leq CD^p(x) + O(1)$

Dôkaz

(i.) vygeneruj a porovnaj ✓

(ii.) postupne generujeme bity $x_1, x_2, ..., x_n$, $x = x_1 \dots x_n$
TS T, $T(v) = 1$ iff $x = v$ v čase $p(n)$. K nemu skonštruujeme T^A
$x_1 \dots x_i \quad \rightsquigarrow \quad x_1 \dots x_i x_{i+1}$?akceptuje T slovo s prefixom $x_1 \dots x_i 0$?

$$\{\langle T, y, 1^t, 1^n : \; T \text{ axceptuje } yz \text{ v čase } t \text{ pre } z : l(yz) = n\rangle\} \in NP$$

□

analogicky pre $K^{t,s}$, $KD^{t,s}$

majorant KZ   co-enumerovateľná funkcia Φ taká, že $C(x) < \Phi(x) + c \quad \forall x; \quad c = c(\Phi)$

Example

Ak t je totálna rekurzívna, potom C^t je totálny rekurzívny majorant C.

- UTS beží na programoch dĺžky nanajvýš $l(x) + c$, pričom spraví nanajvýš $t(l(x))$ krokov

  $C^t(x)$ — dĺžka najkratšieho, ktorý vygeneruje x $C^t(x) \geq C(x) - O(1)$
- je to totálne rekurzívne

$C(x)$, $C^t(x)$ sa môžu exponenciálne líšiť

Theorem (blow-up)

Existuje RE množina A s charakteristickou postupnosťou χ, že pre každú totálne rekurzívnu t a $\forall n$ $C^t(\chi_{1:n}|n) \geq c_t n$; $0 < c_t < 1$.

//Barzdinova lema: Ak A je rekurzívne enumerovateľná, potom $C(\chi_{1:n}|n) \leq \log n + O(1)$

- štandardné číslovanie $T_1, T_2, \ldots$ zmeníme na $M = M_1, M_2, \ldots$ tak, že
  $M_i = T_k, i = 2^{k-1} + j2^k \; \forall k \geq 1,\; j \geq 0$ $\quad$ k max.také, že 2^{k-1} delí i

1	2	1	3	1	2	1	4	1	2	1	3	1	2	1	5	
1		1		1		1		1		1		1		1		2^1
	2				2				2				2			2^2

- konštrukcia A, resp. χ diagonalizáciou

  $i = 1, \chi_1 = 0$
  for all $i > 1$ **do** dovetail nasledujúce výpočty
  $\quad n \leftarrow 2^{i-1}$; $n' \leftarrow 2^{2^k} n$ pre $M_i = T_k$
  $\quad$ **if** $M_i(n')$ zastane s výstupom $t(n')$ **then**
  $\quad\quad$ UTS simuluje $\forall$ programy $p, l(p) \leq n-1$ počas $t(n')$ krokov
  $\quad\quad$ zvolíme $\chi_{n+1:2n}$ tak, že nie je na výstupe žiadneho z tých programov
  $\quad$ **else** $\chi_{n+1:2n} = 0^n$

Fakt ($\hookrightarrow$)

1. *$A \subseteq \mathbb{N}$, $x \in A \Leftrightarrow \chi_x = 1$. Potom A je RE.*
2. *χ je nestlačiteľná pre (wlog) monotónne rastúcu totálnu rekurzívnu funkciu t*

$c_t = 1/2^{2^k+1}$ pre index stroja k, kt. počíta t
$C^{t(n)}(\chi_{1:n}) \geq n/2^{2^k+1}$ $\square$

$A \subseteq \mathbb{N}$, $x \in A \Leftrightarrow \chi_x = 1$. Potom A je RE.

$\forall x$ dovetail

- nájdi $i: \ n+1 < x \leq 2n, \ n = 2^{i-1}$
- vypočítaj $\chi_{n+1:2n}$ simuláciou $M_i(n')$

if $M_i(n')$ nezastane **then** $\chi_{n+1:2n} = 0^n, x \notin A$ & $M_i(n') = \infty$
else $x \in A$ iff $\chi_x = 1$

$\square$

χ je nestlačiteľná pre (wlog) monotónne rastúcu totálnu rekurzívnu fciu t

- $t = T_k, M_{k_0} : k_0 = 2^{k-1}$ po prvýkrát a potom stále ďalej
  $I = \{k_0, k_0 + 2^k, k_0 + 2 \cdot 2^k, k_0 + 3 \cdot 2^k, \ldots\}$, $S = \{n | \ n = 2^{i-1}, i \in I\}$
- pre dosť veľké $n \in S$ existuje $m \in S: \ n/2^{2^k} \lll m \leq n/2$, pričom žiaden z programov dĺžky $m-1$ nedá ako výstup $\chi_{1:2m}$ v čase $t(m') = t(2^{2^k} m) \ggg t(n)$
  $$C^{t(m')}(\chi_{1:2m}) \geq m \qquad (*)$$
- pre SPOR $C^{t(n)}(\chi_{1:n}|n) \leq n/2^{2^k+1}$
  ak poznáme n, v čase $t(n) \lll t(m')$ vypočítame $\chi_{1:n}$ z programu dĺžky max $m/2$
  pridáme $\log m$ bitov a vieme m, $\chi_{1:2m}$ v lineárnom čase — spor s (*)

Theorem

Nech t, f sú neohraničené totálne rekurzívne fcie. Potom existuje rekurzívna postupnosť χ taká, že $C^t(\chi_{1:n}|n) \geq n - f(n)$ nekonečne veľa krát.

//analogicky pre K

(wlog)$f(n) < n$, $\lim_{n\to\infty} f(n) = \infty$. χ skonštruujeme diagonalizáciou

- $g(1) = 1,\ g(n+1) = \min\{m :\ f(m) > g(n)\}$

  g total. rekurzívna, neklesajúca, neohraničená

- $\chi_1 = 0$

  for all $n = 2, 3, \ldots$ **do** vypočítaj $\chi_{g(n-1)+1:g(n)}$ takto:
  simuluj $\forall$ programy dĺžky $< g(n) - g(n-1)$ počas $t(g(n))$ krokov
  $\chi_{g(n-1)+1:g(n)}$ zvolíme tak, že $\chi_{1:g(n)}$ sa nevyskytuje ako prefix žiadneho z výstupov

$$\left.\begin{array}{l} C^t(\chi_{1:g(n)}|g(n)) \geq g(n) - g(n-1) \\[1em] f(g(n)) > g(n-1) \end{array}\right\} C^t(\chi_{1:n}|n) \geq n - f(n)$$

□

Theorem

Nech χ je rekurzívna, $t(n) = \Omega(n)$ neohraničený totálne rekurzívny čas. Potom existuje neohraničená totálna f taká, že $C^t(\chi_{1:n}|n) \leq n - f(n)$

- χ rekurzívna — $T: \ T(n) = \chi_n$
- krátky program q pre UTS $U(\langle q, n\rangle) = \chi_{1:n}$
  1. simuluje T so vstupom $0, 1, \ldots$ v celkovom čase n krokov; nech dopočítal $T(0), T(1), \ldots, T(m)$ $\rightsquigarrow$ U pozná $\chi_{1:m}$
  2. povieme $\chi_{m+1:n}$ max $n - m + 1$ bitov
- $l(q) \leq n - m + 1 + c$ c je popis stroja (1-2)
- U počíta v lineárnom čase

□

Theorem (hierarchia ohraničenej KZ)

Nech f, g sú neohraničené totálne rekurzívne funkcie také, že $f(n) + g(n) \leq n$ a $\forall k$ vieme vypočítať najmenšie n také, že $f(n) = k$ v priestore $s(n) \geq \log n$ a čase $t(n) - n$. Potom pre dostatočne veľké n

$$C[f(n) + g(n), t(n), s(n)] - C[f(n), \infty, \infty] \neq \emptyset$$

Ukážeme, že $\forall UTS\ U\ \exists c = c(U), \underbrace{C[f(n) + c, t(n), s(n)]}_{A} - \underbrace{C[f(n), \infty, \infty]}_{B} \neq \emptyset$

Vezmeme x, $l(x) = f(n) + c/2$, $C(x) \geq l(x)$. Ukážeme, že $x0^{n-l(x)} \in A - B$

($\in A$) program $p = qx$ počíta $x0^{n-l(x)}$:

- nájde najmenšie n : $f(n) + c \geq l(p)$ $\qquad t(n) - n, s(n)$
- vypíše $x0^{n-l(x)}$ $\qquad$ čas $n - l(x)$

  $l(p) = l(x) + O(1) \leq f(n) + c/2 + O(1) \leq f(n) + c$

($\notin B$) **SPOROM** - nech by $x0^{n-l(x)} \in C[f(n), \infty, \infty]$. Potom rekonštrukcia x

- $x0^{n-l(x)}$ programom dĺžky $f(n)$
- oddelenie x: $l(x) = f(n) + c/2$, $f(n)$ poznáme, program dĺžky d vypočíta n

  $l(programu) = f(n) + 2\log c + d + 1 < f(n) + c/2$

Theorem

$s'(n) \geq 2n + s(n) + c$, $s(n)$ neklesajúca, počítateľná v priestore $s'(n)$, $f(n) \leq n$ neohraničená neklesajúca počítateľná v priestore $s'(n) - \log n$. Pre veľké n

$$C[f(n), \infty, s'(n)] - C[n-1, \infty, s(n)] \neq \emptyset$$

Budeme $\underbrace{\text{hľadať prvý reťazec}}_{p}$, ktorý nepatrí do $C[n-1, \infty, s(n)]$

- p vypočíta najmenšie $n: \; f(n) > l(p)$ priestor $s'(n) = (s'(n) - \log n) + \log n$
- vyhradenie priestoru $s(n)$ v $s'(n)$ vypočítame $s(n)$
- $\forall q$ dĺžky $l(q) \leq n-1$ simuluje $UTS(q)$; x je lexikograficky najmenší dĺžky n, kt. žiaden z nich nevygeneroval //$2n + s(n)$ diagonalizácia

stačí priestor $s'(n) \geq 2n + s(n) + c$ program p má dĺžku $l(p) < f(n)$

$\in C[f(n), \infty, s'(n)]$ ale $\notin C[n-1, \infty, s(n)]$

Theorem (kompresia pasky)

K ľubovoľnej totálne rekurzívne $g(n) \geq n$ existuje totálne rekurzívna $s(n)$ taká, že $\forall f(n) < n$ a dosť veľké n

$$C[f(n), \infty, s(n)] = C[f(n), \infty, g(s(n))]$$

- $s(n)$ je minimálne i také, že $\neg\exists p,\ l(p) \leq n-1$, ktorý použije priestor s_p : $i+1 \leq s_p < g(i)$ //vieme to počítať
- $x \in C[f(n), \infty, g(s(n))]$ $\rightsquigarrow$ p vypíše x v priestore $g(s(n))$
- $f(n) < n$, p nepoužije priestor s_p : $s(n)+1 < s_p < g(s(n))$

$$\Downarrow$$

p spotrebuje priestor nanajvýš $s(n)$

$\square$

Q — množina podmnožín množiny $\{0,1\}^*$. Množina A je Q-imúnna, ak je nekonečná a žiadna jej nekonečná podmnožina nepatrí do Q

Lemma

$f(n) < n$ je neohraničená totálna rekurzívna funkcia. Potom $\underbrace{\{0,1\}^* - C[f(n),\infty,\infty]}_{\mathbb{X}}$ je RE-imúnna.

NECH $\exists$ nekonečná RE množina akceptovaná TS T.
Uvažujme TS T'

- T' simuluje T a vymenováva prvky množiny $\mathbb{X}$;
  hľadá x aby $f(l(x)) > l(T')$
  $x \in \mathbb{X}$, $x \in C[f(n),\infty,\infty]$ a súčasne $\mathbb{X} \subseteq (C[f(n),\infty,\infty])^C$

SPOR

Theorem

Nech $\lim_{n\to\infty} s(n)/s'(n) \to 0$, U je UTS, $s'(n) \geq n$ neklesajúca. Nech $f(n)$ je neohraničená neklesajúca počítateľná v priestore $s(n)$. Potom

$$\{0,1\}^* - C[f(n), \infty, s'(n)] \text{ je } DSPACE(s(n))\text{-imúnna}$$

NECH

- nekonečná $A \in DSPACE(s(n)) \bigcap \{\{0,1\}^* - C[f(n), \infty, s'(n)]\}$
- T_A akceptuje A v priestore $O(s(n))$

Majme program p pre UTS, ktorý

- nájde najmenšie i také, že $f(i) > l(p)$ — v $s(n)$
- nájde prvé $x \in A$ také, že $l(x) \geq i$ — A nekonečná

  $x \in A$ a súčasne $x \in C[f(n), \infty, s'(n)]$ — spor

(priemerný) heapsort

$A[1..n]$ $\rightsquigarrow$ **halda**-otec väčší ako synovia $\rightsquigarrow$ triedenie $\rightsquigarrow$ $A[1] < \ldots A[n]$

Heapify

for $i = \lfloor n/2 \rfloor$ downto 1 **do**
kľúč pôvodne $A[i]$ padá na svoje miesto cez väčšieho syna

Sort

for $i = n$ downto 2 **do**
vymeň $k_i = A[1] \leftrightarrow A[i] = k$ a **preusporiadaj** $A[1..i-1]$ na haldu

Williams— porovaním oboch synov s výmenou cez väčšieho syna padá na svoje miesto **2d**

Floyd — porovnaním synov presun (bez výmeny) cez väčšieho syna do listu; potom hore (bez výmeny) na miesto j, ktoré treba vymeniť s koreňom ($A[j] \leq k$); výmena a posun všetkých na ceste z j do koreňa o 1 hore

$\mathbf{d} + \mathbf{2}\delta; \delta = \log \mathbf{n} - \mathbf{d}$

Theorem

Heapsort robí v priemere

$$\begin{array}{lll} \textit{presunov:} & n\log n + O(n) & \\ \textit{porovnaní:} & \textit{Wiliams} & 2n\log n - O(n) \\ & \textit{Floyd} & n\log n + O(n) \end{array}$$

n kľúčov, $n!$ listov // $n^n e^{-n}\sqrt{2\pi n}$

existuje permutácia p : $C(p|n) \geq n\log n - 2n$ (*)

Fakt

Nech h je halda po Heapify pri vstupe p podľa (*). Potom

$$C(h|n) \geq n\log n - 6n$$

(SPOROM) Nech by $C(h|n) < n\log n - 6n$. Krátky popis p:

- popis Heapify, kt. z p vyrobí h - popis cesty na svoje miesto

  $$n\log 3\sum_{i=1}^{\log n} i/2^{i+i} \leq 2n\log 3$$

- $C(p|n) \leq C(h|n) + 2n\log 3 + O(1) < n\log n - 6n + 2n\log 3 + O(1) < n\log n - 2n \diamond$

H popis činnosti v časti sort:
nová pozícia "koreňa" - cesta v strome: s_i $\qquad$ H zreťazenie s_i

$\hookrightarrow$ samooddeľujúco $\delta_i = \log n - l(s_i)$ a za to s_i $\qquad$ $l(s_i) + 2\log\delta_i$

$\hookrightarrow$ h vieme zrekonštruovať z H

(reverzným postupom zrekonštruujem alebo pri dostatku času nájdem permutáciu p)

$\diamond$

$C(h|n) \leq l(H) + O(1)$

$$n\log n - 6n \leq C(h|n) \leq l(H) + O(1) \quad \Rightarrow \quad \boxed{l(H) \geq n\log n - 6n}$$

$$l(H) = \sum_{i=1}^{n}(l(s_i) + 2\log\delta_i) = \sum_{i=1}^{n}\log n - \sum_{i=1}^{n}(\delta_i - 2\log\delta_i) \geq n\log n - 6n$$

$\sum_{i=1}^{n}\delta_i = O(n) \Rightarrow$ súčet priemerných ciest je $n\log n - nc$ $\qquad$ // # presunov v sort

$\Rightarrow$ # porovnaní Williams $\quad 2n\log n - O(n)$

$\Rightarrow$ # porovnaní Floyd $\quad n\log n + O(n)\square$

Najdlhší spoločný podreťazec

- $s = s_1 \dots s_m$, $t = t_1 \dots t_n$
  s je podreťazec t ak existuje $i_1 < \dots < i_m : \ s_j = t_{i_j}$

S-množina reťazcov

- $SCS(S)$ - najkratší reťazec s: $\forall s' \in S \ s'$ je podreťazec s
- $LCS(S)$ - najdlhší reťazec, ktorý je podreťazcom každého z S
  $\Sigma = \{a_1, \dots, a_k\}$, $lcs(S)$-dĺžka $LCS(S)$, $S \subseteq \Sigma^*$

Algoritmus Long-Run

1. nájdi maximálne m také, že (pre nejaké $a \in \Sigma$) a^m je podreťazec s $\forall s \in S$
2. return a^m

Theorem

Nech S je n-prvková množina reťazcov dĺžky n. Algoritmus Long-Run vypočíta spoločný podreťazec dĺžky $lcs(S) - O(lcs(S)^{1/2+\epsilon})$ pre aspoň $(1 - 1/n^2)$-tinu vstupov, a teda v priemere.

Algoritmus Long-Run

1. nájdi maximálne m také, že (pre nejaké $a \in \Sigma$) a^m je podreťazec s $\forall s \in S$
2. return a^m

Algoritmus Long-Run vypočíta spoločný podreťazec dĺžky $lcs(S) - O(lcs(S)^{1/2+\epsilon})$ pre aspoň $(1 - 1/n^2)$-tinu vstupov

$$S = \{x_1, \ldots, x_n\} \quad \rightsquigarrow \quad x = x_1 \ldots x_n : \ C(x) \geq (n^2 - 2\log n)\log k$$

Fakt

Ak $|\#_a(x_i) - n/k| > n^{1/2+\epsilon}$, *tak existuje* $\delta > 0$ *tak, že*

$$C(x_i|k) \leq (n - \delta n^{2\epsilon})\log k$$

//ak $C(x) \geq n - \delta(n)$ tak $|\#y(x) - pn| \leq \sqrt{\alpha pn}$, $\alpha = (K(y|n) + \log l(y) + \delta(n) + c)3l/loge$

resp. index do množiny veľkosti $\binom{n}{m}(k-1)^{n-m}$

Fakt ($\hookrightarrow$)

$$lcs(S) < \frac{n}{k} + n^{1/2+\epsilon}$$

$lcs(S) < n/k + n^{1/2+\epsilon}$ a

$\hookrightarrow$ každé $a \in \Sigma$ v každom x_i aspoň $(n/k) - O(n^{1/2+\epsilon})$

$\hookrightarrow$ a^m dĺžky $(n/k) - O(n^{1/2+\epsilon})$ je spoločný podreťazec

$\hookrightarrow$ $lcs(S) - l(m) = O(n^{1/2+\epsilon})$ $\quad l(m) = lcs(S) - O(lcs(S))^{1/2+\epsilon}$

$S = \{x_1, \ldots, x_n\} \quad \rightsquigarrow \quad x = x_1 \ldots x_n : \; C(x) \geq (n^2 - 2\log n) \log k$

$s = lcs(S)$, kvôli sporu $l(s) > \frac{n}{k} + n^{1/2+\epsilon}$ //chceme $lcs(S) < \frac{n}{k} + n^{1/2+\epsilon}$

krátky popis x :

- $s = s_1 \ldots s_p, s_i \in \Sigma$, fixujme $\mathbf{x_i}$
- vložíme s do x_i tak, že volíme najľavejší možný výskyt; $x_i = \underbrace{\alpha_1 s_1 \alpha_2 s_2 \ldots \alpha_p s_p}_{y} z$

  $\Rightarrow \alpha_j \in (\Sigma - s_j)^*$
- zameňme v y $s_i \to a_k$ a výskyt a_k v α_j nahradíme s_j

  $y' = \alpha'_1 a_k \alpha'_2 a_k \ldots \alpha'_p a_k \qquad \boxed{\#_{a_k}(y') \geq (n/k) + n^{1/2+\epsilon}}$
- $\#_{a_k}(y') \geq (n/k) + n^{1/2+\epsilon}$, preto $C(y'|k) \leq (l(y') - \delta n^{2\epsilon}) \log k$
- $C(x_i|k, s) \leq (n - \delta n^{2\epsilon}) \log k + O(\log n)$
- $C(x|k) \leq \sum C(x_i|k, s) + l(s) + \underbrace{n \log n}_{\text{oddeľovače}}$
- $C(x|k)/\log k < n^2 - 2\log n$ spor $\diamond$