

## PRAM

- globálnu pamäť tvorí  $M$  buniek
- každý procesor má lokálnu pamäť malej/resp. konštantnej veľkosti
- paralelné synchronizované kroky sú "trojkroky"
  - read z globálnej pamäte
  - lokálny výpočet
  - zápis do globálnej pamäte
- riešenie konfliktov nepripúšťa súčasný zápis - EREW, CREW
- polynomiálny počet procesorov a polylog čas; NC a RNC

RNC existuje PRAM  $A$  taký, že  $\forall x \in \Sigma^*$

- $x \in L \Rightarrow Pr[A(x) \text{ je akceptuj}] \geq 1/2$
- $x \notin L \Rightarrow Pr[A(x) \text{ je akceptuj}] = 0$
- polynomiálny počet procesorov
- polylogaritmickej čas

## ZNC

- algoritmus nerobí chybu
- polynomiálny počet procesorov
- *očakávaný* čas je polylogaritmickej

## pravdepodobnostný PQS

vstup:  $P_i$  je  $i$ -ty procesor

- náhodne pivot z  $\{1, \dots, n\}$
- každý  $P_i$  si určí vzťah k pivotu
- $j$  je rank pivota;  
ak  $j \notin [n/4, 3n/4]$  — krok je chybný a treba ho opakovať  
inak pivot sa presunie do  $P_j$
- menšie prvky sa presunú do  $P_i, i < j$
- väčšie prvky sa presunú do  $P_i, i > j$
- rekurzívne sa utriedi  $P_1 \dots P_{j-1}$  a  $P_{j+1} \dots P_n$

//  $j \in [n/4, 3n/4]$

čas  $O((\log n) \cdot (\log n))$

## BoxSort

- náhodne  $\sqrt{n}$  splitrov z množiny  $n$  vstupov
- triedenie splitrov v  $O(\log n)$  krokoch
- vloženie ostatných prvkov pomedzi splitre v  $O(\log n)$  krokoch
- ak je počet prvkov v jednom boxe  $> \log n$ , rekurzia v boxe  
inak LogSort  $m$  prvkov pomocou  $m$  procesorov v  $O(m)$  krokoch

SEL( $\ell+1, u, S$ )

//  $P_{\ell+1}$  zvolí náhodne jeden z klíčův  $K_{\ell+1}, \dots, K_u$  a uloží do  $S$

1. náhodne zvolí  $2^{\lceil \log(u - \ell) \rceil}$  bitův  $\rightsquigarrow$  číslo  $N$
2.  $m \leftarrow N \bmod (u - \ell) = N - (u - \ell) \left( \frac{N}{u - \ell} \right)$
3.  $S_{\ell+1} \leftarrow K_{\ell+1+m}$

lema(SEL)

Nech  $u - \ell \geq 2$ ,  $Q \subseteq K_{\ell+1}, \dots, K_u$ . Pravdepodobnosť, že SEL( $\ell+1, u, S$ ) zvolí prvok z  $Q$  je aspoň

$$\frac{|Q|}{(u - \ell + 2)}$$

$$x = 2^{\lceil \log(u - \ell) \rceil}$$

# prvokův z  $N$  s indexom v  $Q$  je aspoň  $|Q| \cdot \lfloor x / (u - \ell) \rfloor$

$$|Q| \cdot \frac{\lfloor x / (u - \ell) \rfloor}{x} \geq |Q| \cdot \left( \frac{1}{u - \ell} - \frac{1}{x} \right) \geq |Q| \cdot \left( \frac{1}{u - \ell} - \frac{1}{(u - \ell)^2} \right) \geq \frac{|Q|}{u - \ell + 2}$$

//  $z \geq 2 \rightsquigarrow 1/z - 1/z^2 \geq 1/(z + 2)$

ALLSUM( $\ell+1, u, C, D$ )

//  $P_i$  počíta  $\sum_{j=\ell+1}^i C_j$

1.  $[P_i \mid \ell + 1 \geq i \geq u] \quad F_i \leftarrow C_i, H_i \leftarrow \ell, D_i \leftarrow 0$

2. for  $k = 1, \dots, \lfloor \log(u - \ell) \rfloor$  do

$[P_{\ell+2^k \cdot i} \mid 1 \leq i \leq \lfloor (u - \ell) / 2^k \rfloor] \quad F_{\ell+2^k \cdot i} \leftarrow F_{\ell+2^k \cdot i} + F_{\ell+2^k \cdot i - 2^{k-1}}$

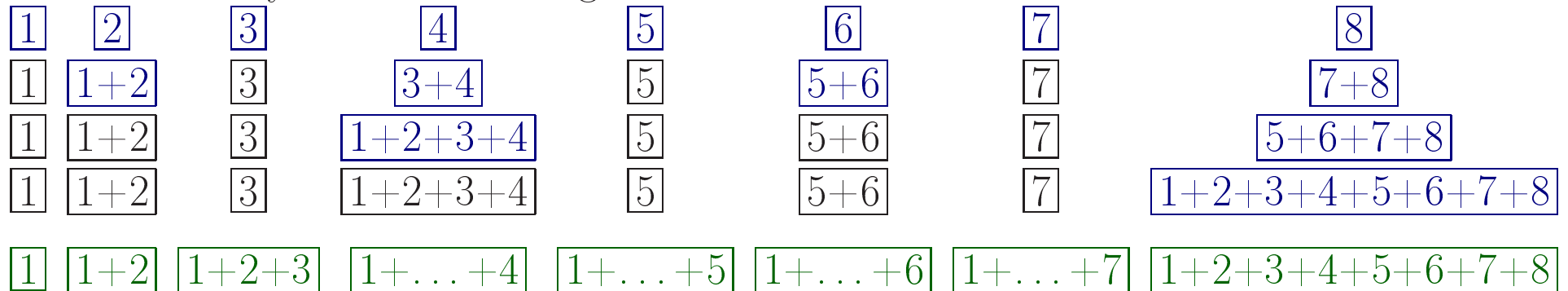
$$!! \ell + 1 \leq j \leq u : j = \ell + 2^k \cdot i, i \text{ nepárne} \quad \rightsquigarrow \quad F_j = \sum_{p=1}^{2^k} C_{\ell+2^k \cdot (i-1)+p}$$

3.  $[P_i \mid \ell + 1 \leq i \leq u]$

for  $k = \lfloor \log(u - \ell) \rfloor, \dots, 0$  do

if  $H_i + 2^k \leq i$  then  $H_i \leftarrow H_i + 2^k; D_i \leftarrow D_i + F_{H_i}$

sčítanie binárnym stromom v logaritmickej čase



## PPSORT( $\ell+1, u$ )

- triedi Box  $K_{\ell+1}, \dots, K_u$  pomocou procesorov  $P_{\ell+1}, \dots, P_u$
- $L, U$  sú globálne, udržiavajú dolnú a hornú hranicu príslušného boxu  
// PPSORT(1,n), L=1,U=n
- dodatočné globálne polia  $S, C, D, G^j$

1. ak je veľkosť boxu nanajvyš  $\log n$ , utried' lineárnym algoritmom a skonči

2.  $[P_i \mid \ell + 1 \leq i \leq u]$   $w \leftarrow \lfloor \sqrt{u - \ell} \rfloor$ ,  $v \leftarrow \lfloor \frac{u - \ell}{w} \rfloor$ ,  $z \leftarrow 2^{2 \lceil \log w \rceil + 2}$

3. – náhodne  $Y \subseteq \{K_{\ell+1}, \dots, K_u\}$ ,  $|Y| = w$  ( $0 \leq j < w : \text{SEL}(\ell + jv + 1, \ell + (j + 1)v, S)$ )

– utriedime(nastavíme 0/1 pre porovnanie splitrov a v kvadratickom počte  $w^2$  procesorov pre  $0 \leq i < w$

pomocou ALLSUM( $\ell + iv + 1, \ell + (i + 1)v, C, D$ )utriedime); v  $D_{\ell+iv+1}$  je rank  $S_{\ell+iv+1}$  v  $Y$

– utriedené presunieme na začiatok Boxu //  $S_{\ell+1}, \dots, S_{\ell+w}$  je utriedené  $Y$

čas  $O(\log(u - \ell))$

PPSORT( $\ell+1, u$ ) cont. - do ktorého boxu  $B^j$  patria jednotlivé  $K_{\ell+1}, \dots, K_u$ ?

$$B^0 = \{K_i \mid \ell + 1 \leq i \leq u, K_i < S_{\ell+1}\}$$

$$B^j = \{K_i \mid \ell + 1 \leq i \leq u, S_{\ell+j} < K_i < S_{\ell+j+1}\}$$

$$B^w = \{K_i \mid \ell + 1 \leq i \leq u, S_{\ell+w} < K_i\}$$

4. paralelne binárnym vyhľadáváním

//  $C_i$  obsahuje index boxu, do ktorého patrí prvok  $K_i$

zistenie veľkostí boxov a relatívneho poradia prvkov v nich...

$$5. [P_i \mid \ell + 1 \leq i \leq u] \quad D_i \leftarrow z^{C_i} \qquad z \leftarrow 2^{2[\log w]+2}$$

$$6. \text{ALLSUM}(\ell + 1, u, D, E)$$

keď počítame v báze  $z$ , koeficient  $\alpha_{j,s}$  v  $E_s = \sum_{i=\ell+1}^s D_i = \sum_{j=0}^w \alpha_{j,s} z^j$  udáva počet prvkov z boxu  $B^j$

$$7. [P_{\ell+1+j} \mid 0 \leq j \leq w] \quad G_{\ell+1+j}^1 \leftarrow \alpha_{j,s} = \lfloor E_u / z^j \rfloor - z \lfloor E_u / z^{j+1} \rfloor$$

$$G_{\ell+1+j}^2 = \sum_{k=0}^j G_{\ell+1+k}^1$$

$\text{ALLSUM}(\ell + 1, \ell + 1 + w, G^1, G^2)$  //z  $G^1, G^2$  vieme počty prvkov v jednotlivých boxoch

$$8. [P_i \mid \ell \leq i \leq u] \quad G_i^3 \leftarrow \alpha_{C_i,i} = \lfloor D_i / z^{C_i} \rfloor - \lfloor D_i / z^{C_i+1} \rfloor$$

$$\text{if } C_i = 0 \text{ then } G_i^4 \leftarrow G_i^3 \text{ else } G_i^4 \leftarrow G_{\ell+C_i}^2 + G_i^3$$

$$K_{\ell+G_i^4} \leftarrow K_i$$

$$9. [P_i \mid \ell + 1 \leq i \leq u]$$

$$\text{if } C_i > 0 \text{ then } L_{\ell+G_i^4} \leftarrow \ell + 1 + G_{\ell+C_i}^2$$

$$U_{\ell+G_i^4} \leftarrow \ell + G_{\ell+1+C_i}^2$$

$$10. \text{PPSORT}(\ell + 1, \ell + G_{\ell+1}^2) \text{ a } \forall 0 < j \leq w \text{PPSORT}(\ell + 1 + G_{\ell+j}^2, \ell + G_{\ell+j+1}^2)$$

analýza času priebeh algoritmu  $\rightsquigarrow$  strom:

- vrchol je box
- synovia boxy, ktoré vznikli rozdelením podľa náhodne vybratých splitrov
- v listoch sú boxy veľkosti  $< \log n$
- váha hrany = čas spotrebovaný na prechod od otca k synovi;
- váha hrany = logaritmus veľkosti otcovského boxu

chceme súčet logaritmov veľkostí boxov na ceste z koreňa do listu je s veľkou pravdepodobnosťou  $O(\log n)$

**veta**  $\forall n$  existuje pravdepodobnostný  $n$ -procesorový PRAM, ktorý triedi  $n$  kľúčov, pričom spraví nanajvýš  $\alpha \log n$  **krokov** s pravdepodobnosťou aspoň  $1 - \exp(-\Omega((\log n)^4))$

fakt  $\forall x \geq 1$

$$\begin{aligned} - \lfloor \sqrt{x} \rfloor &\leq \lfloor x / \lfloor \sqrt{x} \rfloor \rfloor \leq \lfloor \sqrt{x} \rfloor + 2 \\ - 0 &\leq x - \lfloor \sqrt{x} \rfloor \cdot \lfloor x / \lfloor \sqrt{x} \rfloor \rfloor < \lfloor \sqrt{x} \rfloor \end{aligned}$$

Box  $B = K_{\ell+1, \dots, u}$ ,  $w = \lfloor \sqrt{u - \ell} \rfloor$ ,  $v = \lfloor \frac{u - \ell}{w} \rfloor$ ,  $B^0, \dots, B^w$ ,  $b_j = |B^j|$  pre  $0 \leq j \leq w$ .

lema(pokles) Ak  $u - \ell \geq 16$  potom  $\forall \beta \geq 0$

$$Pr[\exists j : b_j \geq 2\beta] \leq (u - \ell) \exp \left( 1 - \frac{\beta}{\sqrt{u - \ell}} \right)$$

krok 2 – splitre ako náhodné prvky v postupnostiach  $\Gamma^0, \dots, \Gamma^{w-1}$  veľkosti  $v$ ,  $\Gamma^w$  veľkosti  $(u - \ell) - vw \leq \sqrt{u - \ell}$ ,  $\Gamma$  sú splitre

$2\beta$  - dĺžka súvislej podpostupnosti  $\Delta$  utriedeného boxu

$$\beta_i = |\Gamma^i \cap \Delta|; \quad \sum_{i=0}^w \beta_i = 2\beta, \quad \beta_w < w;$$

$$\Leftrightarrow Pr[\Gamma \cap \Delta = \emptyset] \leq \max_{\beta_0, \dots, \beta_w} \sum_{i=0}^{w-1} \left( 1 - \frac{\beta_i}{v+2} \right)$$

**lema(SEL)** Nech  $u - \ell \geq 2$ ,  $Q \subseteq K_{\ell+1, \dots, K_u}$ . Pravdepodobnosť, že SEL( $\ell+1, u, S$ ) zvolí prvok z  $Q$  je aspoň  $\frac{|Q|}{(u - \ell + 2)}$

$$Pr[\Gamma \cap \Delta = \emptyset] \leq \max_{\beta_0, \dots, \beta_w} \sum_{i=0}^{w-1} \left(1 - \frac{\beta_i}{v+2}\right)$$

//zlogaritmuje

$$\begin{aligned} \max_{\beta_0, \dots, \beta_w} \sum_{i=0}^{w-1} \ln \left(1 - \frac{\beta_i}{v+2}\right) &\leq \max_{\beta_0, \dots, \beta_w} \sum_{i=0}^{w-1} \left(-\frac{\beta_i}{v+2}\right) \\ &\leq \max_{\beta_0, \dots, \beta_w} -\frac{2\beta}{v+2} + \frac{\beta_w}{v+2} \leq -\frac{2\beta}{\sqrt{u-\ell}+4} + 1 \\ &\leq 1 - \frac{\beta}{\sqrt{u-\ell}} \end{aligned}$$

preto

$$\begin{aligned} Pr[\exists j : b_j > 2\beta] &\leq Pr[\exists \Delta : |\Delta| = 2\beta, \Delta \cap \Gamma = \emptyset] \leq \sum_{\Delta, |\Delta|=2\beta} Pr[\Delta \cap \Gamma = \emptyset] \\ &\leq (u - \ell) \cdot \exp\left(1 - \frac{\beta}{\sqrt{u-\ell}}\right) \end{aligned}$$

□

↔ s veľkou pravdepodobnosťou sú všetky synovské boxy podstatne menšie ako otec

Rekurzia začína s intervalom  $I = [1, n]$

- $\gamma : 1/2 < \gamma < 1$
- $d : 1 < d < 1/\gamma$
- $\forall k, 0 \leq k < M := \lceil \frac{\log \log n - \log \log \log n}{\log(1/\gamma)} \rceil$  definujeme
  - $\tau_k = d^k$
  - $\rho_k = n^{\gamma^k}$
  - $I_k = [\rho_{k+1}, \rho_k]$

$$\frac{\log \log n - \log \log \log n}{\log(1/\gamma)} - 1 \leq M - 1 \leq \frac{\log \log n - \log \log \log n}{\log(1/\gamma)}$$

$$\hookrightarrow \tau_{k-1} < \tau_k, \rho_{k-1} > \rho_k$$

$$\hookrightarrow \frac{1}{d} \left( \frac{\log n}{\log \log n} \right)^{\log d / \log(1/\gamma)} \leq \tau_{M-1} \leq \left( \frac{\log n}{\log \log n} \right)^{\log d / \log(1/\gamma)}$$

$$\hookrightarrow \rho_{M-1} \geq \log n, I_0 = (n^\gamma, n), (1, \log n) \subset I_{M-1}$$

box  $B \rightsquigarrow \alpha(\mathbf{B}) = k$  ak  $|B| \in I_k$

čas na split boxu  $B$  úmerný  $O(\log(\rho_{\alpha(|B|)}))$   $s(B)$  je ten čas

cesta  $\xi$  z koreňa do listu,  $\xi = (B_1, \dots, B_t)$  chceme  $\sum_{j=1}^t \log \rho_{\alpha(B_j)}$

udalosť  $E_\xi$  platí, ak sa v  $\alpha(B_1), \dots, \alpha(B_t)$  žiadna hodnota  $k$  nevyskytuje viac ako  $\tau_k$ -krát //  $1 \leq k \leq c \log \log n$

udalosť  $E_\xi$  platí  $\Rightarrow$  čas na ceste  $\xi$ , je nanajvýš

$$O\left(\log n + \sum_{k=1}^{\infty} \tau_k \gamma^k \log n\right) = O(\log n)$$

$$// \tau_k = d^k, \gamma \cdot d < 1, \log n \sum_{k=1}^{\infty} \tau_k \gamma^k = \log n \sum_{k=1}^{\infty} (d\gamma)^k = O(\log n)$$

Aká je pravdepodobnosť, že udalosť  $E_\xi$  platí?

lema Existuje  $\beta > 1$  tak, že  $E_\xi$  platí s pravdepodobnosťou aspoň  $1 - \exp(-\log^\beta n)$

- ohraničíme pravdepodobnosť, že  $\alpha(B_{j+1}) = \alpha(B_j)$
- spočítame pravdepodobnosť, že pre konkrétne  $k$  sa toto  $k$  vyskytuje v postupnosti  $\alpha(B_1), \dots, \alpha(B_t)$  aspoň  $\tau_k$  krát
- spočítame pravdepodobnosť, že pre  $1 \leq k \leq c \log \log n$  sa  $k$  vyskytuje v postupnosti  $\alpha(B_1), \dots, \alpha(B_t)$  aspoň  $\tau_k$  krát

počet ciest  $\xi$  (resp. listov)  $\leq n$   
veta Existuje konštanta  $b > 0$  tak, že s pravdepodobnosťou aspoň  $1 - \exp(-\log^b n)$  skončí algoritmus BoxSort v  $O(\log n)$  krokoch.

z lemy(pokles)

$$\begin{aligned}
Pr[\alpha(B_{j+1}) = \alpha(B_j) \mid \alpha(B_j) = \lambda] & \\
&\leq |B_j| \cdot \exp\left(1 - \frac{|B_{j+1}|}{2} \frac{1}{\sqrt{|B_j|}}\right) \\
&\leq \rho_\lambda \exp\left(1 - \frac{1}{2} \frac{\rho_{\lambda+1}}{\sqrt{\rho_\lambda}}\right) && |B_j| \leq \rho_\lambda, |B_{j+1}| \geq \rho_{\lambda+1} \\
&= \exp\left(1 + \ln(n^{\gamma^\lambda}) - \frac{1}{2} \frac{n^{\gamma^{\lambda+1}}}{n^{\gamma^\lambda/2}}\right) \\
&= \exp\left(1 + \gamma^\lambda \ln n - \frac{1}{2} \frac{n^{\gamma^{\lambda+1}}}{(n^{\gamma^{\lambda+1}})^{1/2\gamma}}\right) \\
&\leq \exp\left(-\frac{1}{3} \left(n^{\gamma^{\lambda+1}}\right)^{1-1/2\gamma}\right) && n^{\gamma^\lambda} \geq \log n, 1/2\gamma < 1
\end{aligned}$$

Preto

$$\begin{aligned}
Pr[\alpha(B_{j+\tau}) = \alpha(B_{j+\tau-1}) = \dots = \alpha(B_j) \mid \alpha(B_j) = \lambda] & \\
&= \prod_{\ell=j+1}^{j+\tau} Pr[\alpha(B_\ell) = \alpha(B_{\ell-1}) \mid \alpha(B_{\ell-1}) = \dots = \alpha(B_j) = \lambda] \\
&\leq \exp\left(-\frac{\tau}{3} \left(n^{\gamma^{\lambda+1}}\right)^{1-1/2\gamma}\right)
\end{aligned}$$

$$\begin{aligned}
& Pr[\exists 0 \leq k \leq M : \alpha(B_1), \dots, \alpha(B_{t-1}) \text{ obsahuje } k > \tau_k \text{ krát}] \\
& \leq \sum_{k=0}^{M-1} \sum_{j=1}^{t-\tau_k} Pr[\alpha(B_{j+\tau_k}) = \dots = \alpha(B_j) = k] \\
& = \sum_k \sum_j Pr[\alpha(B_{j+\tau_k}) = \dots = \alpha(B_j) \mid \alpha(B_j) = k] \cdot Pr[\alpha(B_j) = k] \\
& \leq \sum_k \frac{n}{\log n} \exp\left(-\frac{\tau_k}{3} \left(n^{\gamma^{k+1}}\right)^{1-1/2\gamma}\right) \quad t \leq n/\log n \\
& k < M
\end{aligned}$$

$$\frac{(\tau_k/3)(n^{\gamma^{k+1}})^{1-1/2\gamma}}{(\tau_{k-1}/3)(n^{\gamma^k})^{1-1/2\gamma}} = d(n^{\gamma^{k+1}-\gamma^k})^{1-1/2\gamma} = d(n^{\gamma^k})^{(\gamma-1)(1-1/2\gamma)} \leq d(\log n)^\epsilon,$$

( ) je klesajúca v  $k$

$$\begin{aligned}
\sum_k \frac{n}{\log n} \exp\left(-\frac{\tau_k}{3} (n^{\gamma^{k+1}})^{1-1/2\gamma}\right) & \leq n \exp\left(-\frac{\tau_{M-1}}{3} (n^{\gamma^{M-1}})^{\gamma-1/2}\right) \\
& \leq n \exp\left(-\frac{1}{3d} \left(\frac{\log n}{\log \log n}\right)^{\log d / \log(1/\gamma)} (\log n)^{\gamma-1/2}\right) \\
& \leq n \exp\left(-\frac{1}{3d} (\log n)^{(\log d / \log(1/\gamma)) + \gamma - 1/2} (\log \log n)^{-\log d / \log(1/\gamma)}\right)
\end{aligned}$$

Máme menej ako  $n$  ciest z koreňa do listu, preto pravdepodobnosť, že  $E_\xi$  neplatí, je nanajvýš

$$1 - n^2 \exp \left( -\frac{1}{3d} (\log n)^{(\log d / \log(1/\gamma)) + \gamma - 1/2} (\log \log n)^{-\log d / \log(1/\gamma)} \right)$$

pre  $\gamma = 5/6, d = 1.19$  platí, že  $\log d / \log(1/\gamma) + \gamma - 1/2 > 1.28$

$$1 - \exp \left( 2 \ln n - \frac{1}{3d} (\log n)^{1.28} (\log \log n)^{-1} \right) \leq 1 - \exp \left( -\Omega((\log n)^4) \right)$$