Rekurzivní funkce

Master theorem

$r(n)$ — rekurzivní fce — a — $n = 1$

$c \cdot n + d\, r\left(\frac{n}{b}\right)$ — $n > 1$ — na kolik to rozdílím — $b = 4$

c: kolik režim části rozdělení na části

d: kolik režim části

$d == b \rightarrow \Theta(n \cdot \log n)$

$d < b \rightarrow \Theta(n)$

$d > b \rightarrow \Theta\left(n^{\log_b d}\right)$ … některé části režim všechno

ad) $d = b$ … jednoduché

0: $c \cdot n + d\, r\left(\frac{n}{b}\right)$

1: $c \cdot n + d\left(c \cdot \frac{n}{b} + d\, r\left(\frac{n}{b^2}\right)\right) = c \cdot n + c \cdot n \frac{d}{b} + d^2 r\left(\frac{n}{b^2}\right) = c \cdot 2n + d^2 r\left(\frac{n}{b^2}\right)$

2: $c \cdot n + d \cdot c\left(\frac{n}{b}\right) + d^2\left(c \frac{n}{b^2} + d\, r\left(\frac{n}{b^3}\right)\right) =$

$= c\, 2n + cn + d^3 r\left(\frac{n}{b^3}\right) = 3cn + d^3 r\left(\frac{n}{b^3}\right)$

k: $k \cdot cn + d^k r\left(\frac{n}{b^k}\right)$

$\sum_{i=1}^{k} \left(i \cdot cn\right) + \left(d^k r\left(\frac{n}{b^k}\right)\right)$

$\frac{n}{b^k} > 1$ … má smysl se množství

$n > b^k$

$\log_b n = k$

$m = \log_b n$

$d^m \cdot a$

m: $cn + \sum_{i=1}^{m-1} c\left(\frac{n}{b^i}\right) \cdot d^i + d^m \cdot \left(r\left(\frac{n}{b^m}\right)\right) = cn + \sum_{i=1}^{m-1} \left(\frac{d}{b}\right)^i \cdot cn + d^m \cdot a = cn + (m-1) \cdot cn + d^m \cdot a$

$n = r\left(\frac{n}{n}\right) = r(1) = a$ (pro $n = 1$)

m-tá složka

a ta je maximální!

Cvi ADT B36 DSA

$$= cn + \underbrace{cn(\log n - 1)}_{\text{toto roste nejvíce } \mathcal{O}(n \log n)} + d^{\log n} \cdot a$$

ostatní

$$cn + \underbrace{cn \sum_{i=1}^{m-1} \left(\frac{d}{b}\right)^i}_{\text{geometrická posloupnost}} + d^m \cdot a$$

$$cn + cn \frac{1 - \left(\frac{d}{b}\right)^{i(?)\, m-1}}{1 - \frac{d}{b}} + d^m \cdot a$$

$d < b$ $\underbrace{c \cdot n + c \cdot n(1 + \dots)}_{\text{je menší } \mathcal{O}(n)} + d^{\log n} \cdot a$

$d > b$ str. 39.

$$\mathcal{O}\left(n^{\log_b d}\right)$$

Př.:

$$T(n) = a + T\left(\frac{n}{2}\right)$$

za 2: $a + a + T\left(\frac{n}{4}\right) = 2a + T\left(\frac{n}{2^2}\right)$

k: $k \cdot a + T\left(\frac{n}{2^k}\right)$

$\frac{n}{2^k} > 1$

$n > 2^k$

$\log_2 n > k$

n: $n \cdot a + T\left(\frac{n}{2^n}\right) = n \cdot a + T(1) = a \cdot \log_2 n + a$

$\mathcal{O}(\log n)$

$\log_2 n = \frac{\log n}{\log 2} \approx \log n$

Rozšíření Master Teorému

brání celých částí

$$r(n) \leq \begin{cases} a, & n = n_0 \\ c \cdot n + d\, r\left(\left\lceil \frac{n}{b} \right\rceil\right) + e & n > n_0 \end{cases}$$

Př 2.8

$$C(n) = \begin{cases} 1, & n = 1 \\ C\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + C\left(\left\lceil \frac{n}{2} \right\rceil\right) + cn, & n > 1 \end{cases}$$

pravidlo oddad

$$\leq 2 \cdot C\left(\left\lceil \frac{n}{2} \right\rceil\right) + c \cdot n \leq$$

podmínka $\left\lceil \frac{n}{b} \right\rceil + e < n$, $\forall n > n_0$

$\left\lceil \frac{2}{2} \right\rceil + 0 = 1 < 2$ funguje

$S(n)$ ... nejbližší větší číslo ve tvaru $b+z \geq n$ str. 40

(nejmenší) -"-

$$\leq$$

$$C(n) \leq cS(n) + d\,R\left(S\left(\left\lceil \frac{n}{b} \right\rceil + e\right)\right)$$

z $\quad$ 0 : hlavní master kterem

e $\quad$ d

z

$d = b^z \Rightarrow 2 = 2 \Rightarrow C(n) = \mathcal{O}(n \cdot \log n)$

Omikron

Zda patří do $\mathcal{O}$ menší jako

jakýkoli násobek $\leq$

Pravděpodobnostní algoritmy

str 17.

Alice (A) — x_A — Bob (B) — x_B

n-bitů

$x_A \bmod p$ — $x_B \bmod p$

$5 \bmod 2$
$4 \bmod 2$ } chyba

k - bitové prvočíslo

k bitů bude mít zbytek

$\frac{n}{k}$ = pravděpodobnost chyby

seznam délky l — a pak pravděp. chyby = $\frac{n/k}{l}$

l = pravděpodobnost $\cdot \frac{n}{k}$

$\frac{2^k}{k}$ ... prvočísel ~~v intervalu~~ počet k bit

$\frac{2^k}{k} \geq l = P \cdot \frac{n}{k}$

pravděpodobnost

$k \geq \log_2(P \cdot n)$

složitost - jaké procento se vybere ze seznamu l počet bitů $= \log_2 l$

- zbytek ... k-bitů

$\log_2 l + k$ ... počet bitů celkem

$$\underbrace{\log_2\left(P \cdot \frac{n}{\log_2(n \cdot P)}\right)}_{l} + \underbrace{\log_2(n \cdot P)}_{k} \approx \log n$$

počet bitů které se přenášejí

ad) pravidlo se tomuto po lince

- po lince jde $k + k = 2 \cdot \log_2(P \cdot n) \approx \log n$
- jednoduchý na generování

Př.] Cvi 2.14 str. 48