Algoritmy a datové struktury I

Jan Hric, KTIML MFF UK
e-mail: Jan.Hric@mff.cuni.cz
http://ktiml.ms.mff.cuni.cz/~hric/vyuka/alg/ads1pr.pdf

21. května 2019

průběžná verze 2019, 8.4. (opravy možné)

Sylabus

- Prostředky pro popis složitosti algoritmů a operací nad datovými strukturami, tzv. asymptotická notace, O-notace
- (Binární stromy,) AVL-stromy, Červenočerné stromy
- B-stromy
- Hašování
- Grafové algoritmy: prohledávaní, topologické třídění, SSK
- Extremální cesty v grafech (a dat.struk. halda)
- Minimální kostra (a dat.struk. Union-Find)
- Metoda Rozděl a panuj
- Třídění: Dolní odhad složitosti (problému) třídění, průměrný případ Quicksortu, randomizace Quicksortu, lineární třídící algoritmy

- Algebraické algoritmy (LUP rozklad)
- (Hladové alg.)

Literatura:

T. H. Cormen, Ch. E. Leiserson, R. L. Rivest, Introduction to Algorithms, MIT Press, 1991

Martin Mareš, Tomáš Valla, Průvodce labyrintem algoritmů, CZ.NIC, z. s. p. o., Praha, 1. vydání, 2017, ISBN 978-80-88168-22-5, http://pruvodce.ucw.cz/, datum přístupu 8.4.2019

A. Koubková, J. Pavelka, Úvod do teoretické informatiky, Matfyzpress, 1998

L. Kučera, Kombinatorické Algoritmy, SNTL, Praha 1983

Měření a porovnávání algoritmů:
- časová složitost
- prostorová (paměťová) složitost
- komunikační složitost (napr. počet paketů)

Používáme funkce závislé na velikosti vstupních dat:
- od konkrétních dat k datům určité velikosti
- porovnáváme funkce

Jak měřit velikost vstupních dat? (i jiných dat)
rigorózně: počet bitů nutných k zapsání vstupních dat

Příklad: vstup jsou (přirozená) čísla $a_1, ..., a_n \in N$ velikost dat D v binárních zápisu je $|D| = \Sigma_{i=1}^{n} \lceil \log_2 a_i \rceil$

Odstranění závislosti na konkrétních datech:
- v nejhorším případě
- v průměrném případě (vzhledem k pravděpodobnostnímu rozložení vstupních dat)

Časová složitost algoritmu: funkce $f : N \to N$ taková, že $f(|D|)$ udává počet kroků algoritmu v závislosti na datech velikosti $|D|$.

Intuitivně: není podstatný přesný průběh funkce f ("až na multiplikativní a aditivní konstanty"), ale to, do jaké "třídy"funkce f patří (lineární, kvadratická, ...)

Co je krok algoritmu:
- teoreticky: operace daného abstraktního stroje (Turingův stroj, stroj RAM)
- zjednodušeně (budeme používat): krok algoritmu = operace proveditelná v konstantním čase (nezávislém na velikosti dat)
- aritmetické operace (+, -, *, ...)
- porovnání dvou hodnot (typicky čísel)
- přiřazení pro jednoduché datové typy (ale ne pro pole)

- tím se zjednoduší i měření velikosti dat (čísla mají pevnou maximální velikost)

Příklad: setřídit čísla $a_1, ..., a_n$: velikost dat $|D| = n$

Toto zjednodušení nevadí při porovnání algoritmů, ale může vést k chybě při zařazování algoritmů do tříd složitosti. (Přesnější měření kroku: cena operace závisí na velikosti zpracovávaných dat, tj. na počtu bitů/buněk)

Proč měřit časovou složitost: (slajd)
- proč někdy nepomůže rychlejší počítač

Asymptotická složitost

- zkoumá chování algoritmu na "velkých"datech (ignoruje konečný počet výjimek)
- zařazuje algoritmy do "kategorií"
- zanedbává multiplikativní a aditivní konstanty

Definice:

- $f(n)$ je asymptoticky menší nebo rovno $g(n)$, značíme $f(n) \in O(g(n))$,
  pokud $\exists c > 0 \exists n_0 \forall n \geq n_0 : 0 \leq f(n) \leq c.g(n)$
- $f(n)$ je asymptoticky větší nebo rovno $g(n)$, značíme $f(n) \in \Omega(g(n))$,
  pokud $\exists c > 0 \exists n_0 \forall n \geq n_0 : 0 \leq c.g(n) \leq f(n)$
- $f(n)$ je asymptoticky stejné jako $g(n)$, značíme $f(n) \in \Theta(g(n))$,
  pokud $\exists c_1, c_2 > 0 \exists n_0 \forall n \geq n_0 : 0 \leq c_1.g(n) \leq f(n) \leq c_2.g(n)$
- $f(n)$ je asymptoticky ostře menší než $g(n)$, značíme $f(n) \in o(g(n))$,
  pokud $\forall c > 0 \exists n_0 \forall n \geq n_0 : 0 \leq f(n) \leq c.g(n)$
- $f(n)$ je asymptoticky ostře větší než $g(n)$, značíme $f(n) \in \omega(g(n))$,
  pokud $\forall c > 0 \exists n_0 \forall n \geq n_0 : 0 \leq c.g(n) \leq f(n)$

Příklady kategorií funkcí: $\Theta(\underline{1})$, $\log(\log n), \log n, \log^2(n)$, $n^{1/2}$, n, $n \log n, n^2$, $n^3, 2^n, 2^{2n}$, $n!, n^n, 2^{2^n}, ...$

Pozn: některé dvojice funkcí nejdou porovnat

DC: (Značení $O(f+g)$) Dokažte: $max(f(n), g(n)) \in \Theta(f(n)+g(n))$.

DC: pro $c_m, c_a > 0$ a $g(n) = c_m.f(n) + c_a$ dokažte $g \in O(f)$ (a $g \in \Theta(f)$)

Příklad tvrzení a důkazu:
Pokud $f \in O(h)$ a $g \in O(h)$, potom $f + g \in O(h)$.
Dk-idea: máme c_f, n_f, c_g, n_g pro c, n_0 z předpokladů o f a g z definice "O". Zvolíme $c = c_f + c_g$, $n_0 = max(n_f, n_g)$, potom pro každé $n \geq n_0$ platí $0 \leq f(n) + g(n) \leq c_f.h(n) + c_g.h(n) = (c_f + c_g).h(n) = c.h(n)$, QED

Aplikace: odhad složitosti sekvence příkazů.

Pozn: nevhodný zápis $f = O(g)$

Pozn: vliv multiplikativní a aditivní konstanty v asymptotické notaci:
Porovnání $n + 100$ a n^2, $2^{100}n$ a n^2
Složitost $f(n) = 10n$ je lepší než $g(n) = 1n \log n$ až pro $n > 2^{10}$
Složitost $f(n) = 5n^{1.9}$ je lepší než $g(n) = 1n^2$ až pro $n > 5^{10}$
Složitost $f(n) = 2^{1000}n$ je lepší než $g(n) = 2^n$ pro $n \geq 1010$
Malá data je někdy vhodné zpracovat jednodušším algoritmem s menší režií, i když má větší asymptotickou složitost.

Dynamické množiny

dynamické - mění se v čase (obsah, velikost, ...)

prvek dynamické množiny je přístupný přes ukazatel (pointer) a obsahuje

1. klíč - typicky z nějaké lineárně uspořádané množiny
2. ukazatel(e) na další prvky (nebo části reprezentující struktury)
3. další (uživatelské) data (!)

Operace na dynamické množině: Nechť S je dynamická množina prvků, k hodnota klíče a x ukazatel na prvek:

- $Find(S, k)$ - vrací ukazatel na prvek s klíčem k v množině S anebo NIL
- $Insert(S, x)$ - do S vloží prvek, na který ukazuje x
- $Delete(S, x)$ - z S odstraní prvek, na který ukazuje x
- $Min(S)$ - vrací ukazatel na prvek v S s minimálním klíčem
- $Max(S)$ - vrací ukazatel na prvek v S s maximálním klíčem
- $Succ(S, x)$ - vrací ukazatel na prvek v S bezprostředně následující (v lineárním uspořádání klíčů) po prvku, na který ukazuje x, anebo vrací NIL
- $Predec(S, x)$ - analogicky pro bezprostředně předcházející prvek k x

Binární vyhledávací stromy (BVS)

Dynamická datová struktura, která podporuje všechny operace na dynamické množině

Binární strom: každý vrchol reprezentuje jeden prvek množiny a obsahuje klíč a 3 pointry na levého syna (levý), pravého syna (pravý) a rodiče (rodič)

- strukturu binárního stromu můžeme použít pro jiné datové struktury, např. pro binární haldu (pro heapsort). V ní je klíč vrcholu menší než oba potomci.

Pro binární vyhledávací strom platí:
pro každý prvek x platí: všechny prvky v levém podstromě prvku x mají menší klíč než x (připouštíme rovnost) a všechny prvky v pravém podstromě prvku x mají vetší klíč než x.

```
Find(x,k) % x je ukazatel na kořen BVS obsahující S
 1 while (x<>NIL) and (k<>klíč(x)) do  % k je pod x
 2   if k < klíč(x)   % zúžení výběru
 3     then x <- levý(x)  % posun doleva
 4     else x <- pravý(x) % posun doprava
 5 return x       % x=NIL or k=klíč(x)
```

Složitost je $O(h)$, kde h je výška BVS. Na každé úrovni stromu spotřebujeme konstantní čas, tj. $O(1)$. Stejná složitost platí i pro ostatní operace.

- další operace (vyhledávací i modifikující):

Min(S): Od kořene doleva, dokud to jde. Prvek, který nemá levého syna, je nejmenší.

Max(S): symetricky.

Succ(S,x): Do pravého syna, pokud existuje, pak opakovaně doleva. Jinak opakovaně přecházíme do rodiče a vracíme prvního rodiče, kde opouštěný syn je vlevo, anebo NIL, pokud dojdeme do kořene.
Lokálně, v levém podstromě hledáme Min(), ale tato operace je zavedena jen pro celou strukturu S.
Pozn. Musíme ošetřit všechny možné případy.

Predec(S,x): symetricky

Insert(S,x): Klesáme podle porovnání doleva nebo doprava. Prvek přidáme místo NIL jako list.

Delete(S,x): Pokud má vypouštěný prvek x 0 nebo 1 syna, vypustíme přímo. Jinak najdeme $s = Succ(S, x)$, kterým nahradíme x (!přelinkováním) a vypouštíme prvek z pozice s.

BVS s n vrcholy:
- nejlepší případ: vyvážený (úplný) strom: výška $\Theta(\log n)$
- nejhorší případ: lineární seznam n vrcholů: výška $\Theta(n)$
- náhodně postavený strom (průměrný případ): výška $\Theta(\log n)$

Chceme zlepšit nejhorší případ: Červeno-černé stromy a AVL stromy pomocí lokálních invariantů a lokálních vyvažovacích operací zaručí výšku $\Theta(\log n)$ v nejhorším případě.

Červeno-černé stromy

- Jsou to binární vyhledávací stromy, které mají navíc obarvené vrcholy: barva je červená nebo černá. (Implementačně: 1 bit)

- Z podmínek na obarvení plyne, že délka cest z kořene do listů se liší nejvíc 2x. Stromy jsou vyvážené v tom smyslu, že nejdelší cesta je logaritmická vůči počtu vrcholů.

Df: BVS je *červeno-černý strom*, pokud splňuje následující vlastnosti:

1. Každý vrchol je červený nebo černý
2. Každý list (Nil, tj. externí vrchol) je černý
3. Pokud je vrchol červený, potom obě děti jsou černé
4. Každá cesta z vrcholu do podřízeného listu obsahuje stejný počet černých vrcholů

Vrcholy, které nejsou externí, jsou vnitřní, tj. interní. Červené vrcholy mají (případně externí) černé syny. Z 3. plyne, že nejsou dva červené vrcholy bezprostředně pod sebou. Následně ze 4. plyne speciálně pro kořen, že při zvolené černé výšce je nejkratší možná cesta z kořene do listu pouze černá a nejdelší jen 2x delší (střídavě červené a černé vrcholy).

Značení: $bh(x)$ je černá výška (black height) - počet černých vrcholů na cestě z x do listů, kromě x. (Podle 4. na volbě listu nezáleží.)

Lemma: Č-č strom s n vnitřními vrcholy má výšku h nejvíc $2\log(n+1)$.

Dk: Indukcí podle výšky podstromů lze dokázat, že podstrom ve vrcholu x má aspoň $2^{bh(x)} - 1$ vnitřních vrcholů.

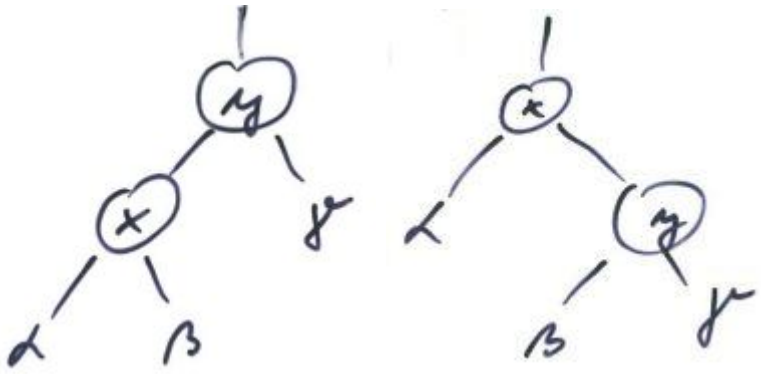
Použijeme pro kořen:
$n \geq 2^{h/2} - 1$, odtud $h \leq 2\log(n+1)$

Pro odstraňování poruchy se používají rotace. Mějme situace:

1. $((\alpha, X, \beta), Y, \gamma)$
2. $(\alpha, X, (\beta, Y, \gamma))$

PraváRotace(Y) převede 1. na 2., LeváRotace(X) převede 2. na 1.

Argument rotace je kořen podstromu, který se mění.



Obrázek 1: Pravá rotace: strom před a po

Pozorování: uspořádání klíčů zůstalo při obou rotacích zachováno.

Pro jednotlivé transformace budeme kontrolovat zachování pořadí klíčů a zachování (lokální) hloubky podstromů.

Hackerská školka: (Neoptimální) implementace rotace (v OOP): Zapamatujeme si nejdřív vše, co budeme potřebovat (pro pravou rot. rodič(y), y, x, kořen(β)), do pomocných proměnných a potom změníme příslušné položky/ukazatele

(6x, pro 3 hrany).

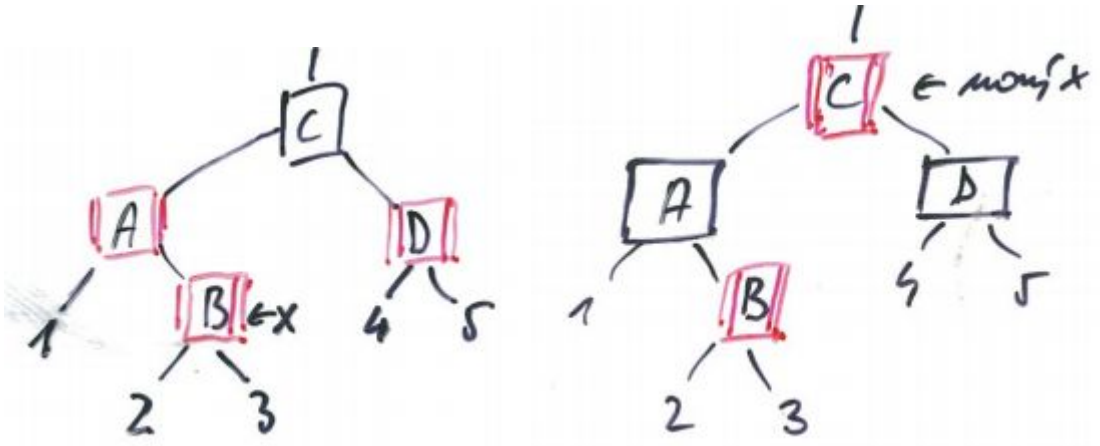
Vkládání: viz Obrázky

Červený kořen můžeme přebarvit na černý bez porušení vlastností Č-Č stromu. Budeme tuto vlastnost udržovat.

Fyzické vložení uzlu: jako v BVS, vložený uzel x obarvíme na červeno.

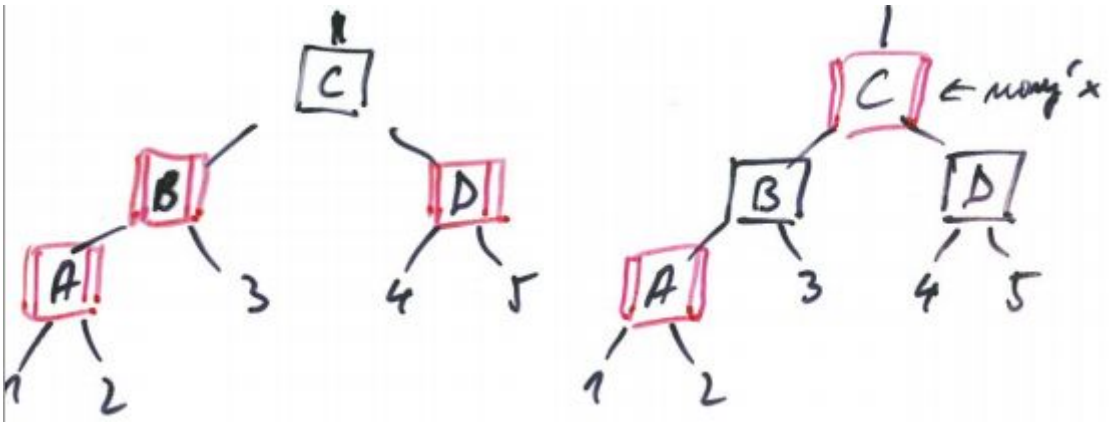
Pak může být porušena pouze vlastnost 3, když vložený uzel x i jeho otec y jsou červené. Pokud tato porucha nastane, y má otce z , který je černý. Jinak končíme, strom je správně utvořený. Bratra y označíme $y2$.

Rozeberme 3 možné případy.

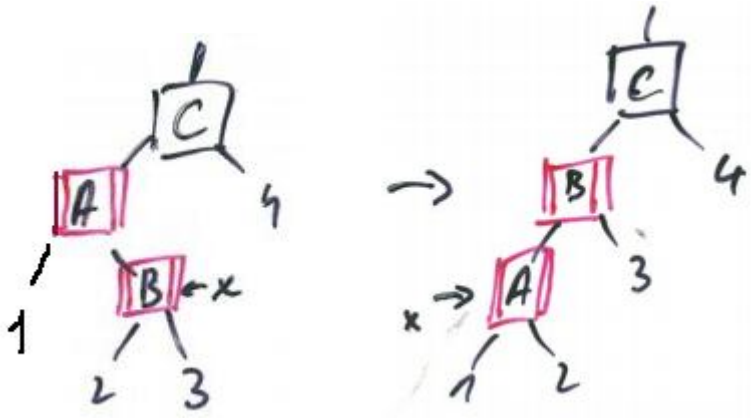


Obrázek 2: Č–Č případ 1a, $x = B$: Strýc D je červený, před a po

1. Zahrnuje 1a, resp. 1b. Bratr $y2 = D$ uzlu $y = A$, resp. $y = B$, tj. strýc x, je červený. Pak y a $y2$ přebarvíme na černo, $z = C$ na červeno. Pokud je z kořen, přebarvíme ho na černo a končíme, pokud má z černého otce, končíme, jinak má z červeného otce, porucha se přesunula výš a iterujeme (rozborem 3 možností). Uzel z je polohou "nový" x.



Obrázek 3: Č–Č případ 1b, $x = A$: Strýc D je červený, před a po

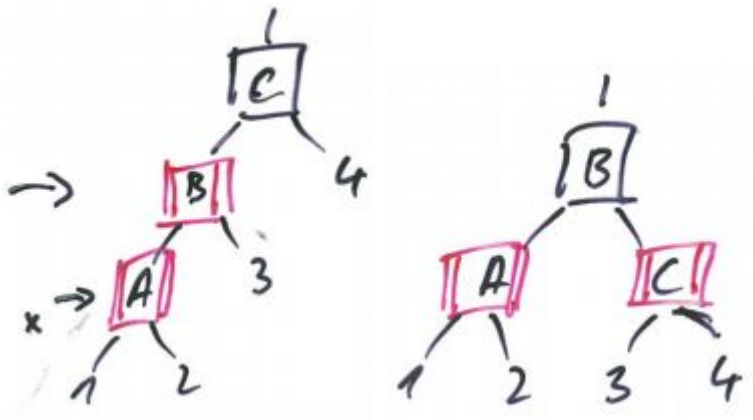


Obrázek 4: Č–Č případ 2: Strýc D je černý, $x = B$ je vnitřní (před a po)

2. Bratr $y2$ uzlu y je černý a x je opačným synem y než y synem z. Pokud je x pravým synem y, tak LeváRotace(y), jinak PraváRotace(y). (Bez přebarvování.) Tím je situace převedena na případ 3.

3. Bratr $y2$ uzlu y je černý a x je stejným synem y než y synem z. Pokud je x levým synem y a y levým synem z, tak PraváRotace(z) a přebarvení y na černo a z na červeno. Tím jsou vlastnosti Č-Č stromu splněny. Opačný případ je symetrický.

Pozn: V případě vkládání dva černé uzly pod sebou tvoří "rezervu", kterou využijeme lokálně a poruchu nemusíme



Obrázek 5: Č–Č případ 3: Strýc D je černý, $x = A$ je vnější (před a po)

propagovat nahoru.

Složitost vkládání je $O(\log n)$.
- vlastní vkládání do BVS $O(\log n)$
- složitost 1. je $O(1)$ (test+rotace+přebarvení), provede se nejvýše $O(\log n)$-krát
- složitost 2. a 3. je $O(1)$, provede se každá nejvýše jednou

Vypouštění:

Prvek odstraníme standardním způsobem z BVS.

Pro vypouštění, červený uzel v lokálním okolí je rezerva, která umožní změnu nepropagovat nahoru.

Skutečně odstraňovaný prvek y má nejvýše jednoho interního syna, nechť je to x. Pokud nemá interní syny, označíme x jednoho z externích synů. (Uzel x se dostane na místo y.)

Pokud je y červený, po jeho vypuštění je strom v pořádku. Pokud je y černý, je po jeho vypuštění porušena vlastnost 4 (kromě případu, když je y kořen), protože cesty vedoucí přes y ztratily 1 ze své černé výšky.

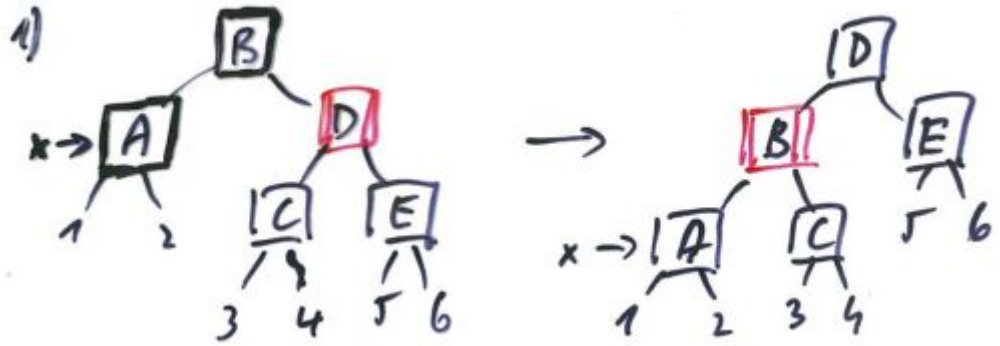
Pokud je x červený , přebarvíme ho na černo a strom je v

pořádku.

Pokud je x černý, označíme ho jako dvojitě černý a tuto (jedinou) poruchu budeme odstraňovat, buď na místě nebo posunem vzhůru.

Pokud je x kořen stromu, tak černou barvu navíc odstraníme a černá výška všech vrcholů klesne o 1. Pokud x není kořen, tak rodič(x), označme ho z, musí mít druhého syna interního, označme ho w, jinak by cesty k listům nesplňovaly podmínky na černou výšku. (Externí uzel má černou výšku 1, tedy menší než x.)

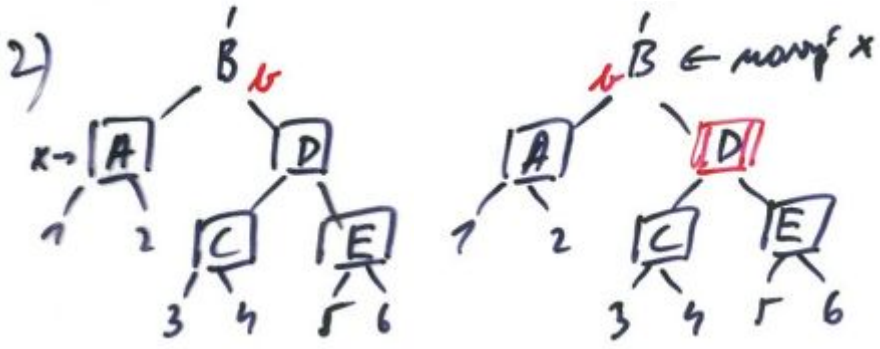
Budeme předpokládat, že x je levým synem rodiče z (opačný případ je symetrický) a rozlišíme čtyři případy podle barvy w a jeho synů.



Obrázek 6: Č–Č případ 1: Bratr D je červený, před a po

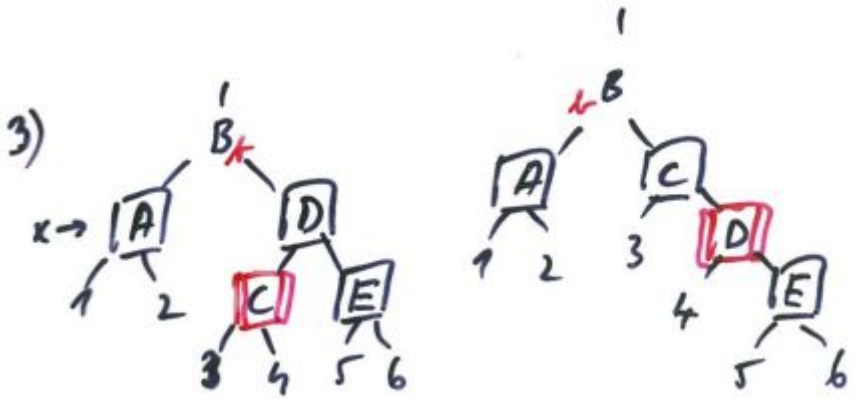
1. uzel w je červený (a tedy má černé syny). Přebarvíme w na černo a z (=rodič(x)=rodič(w)) na červeno a provedeme LeváRotace(z). Tím se situace převede na jednu z dalších 3 možností, tj. x má černého bratra.

2. uzel w je černý a má dva černé syny. Odstraníme jednu černou z x a přebarvíme w na červeno. Jejich otci z



Obrázek 7: Č–Č případ 2: Bratr D, C a E jsou černé, před a po

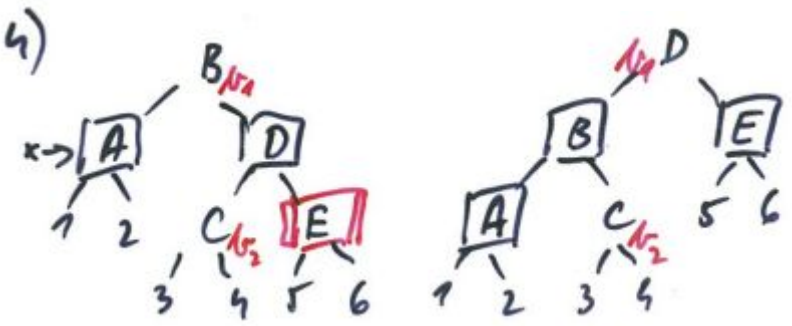
přidáme jednu černou, tj. pokud je červený, přebarvíme na černo a končíme, a pokud je z černý, změníme ho na dvojitě černý. Tím jsme poruchu posunuli ke kořeni a iterujeme. Tento postup dvojitě černé vzhůru se zastaví nejpozději v kořeni, kde jednu černou můžeme odebrat.



Obrázek 8: Č–Č případ 3: Bratr D a vnější syn E černý, vnitřní syn C červený, před a po

3. uzel w je černý, jeho levý ("vnitřní") syn je červený a pravý syn černý. Vyměníme barvy w a jeho levého syna a provedeme PraváRotace(w). Tím převedeme situaci na případ 4.

4. uzel w je černý a jeho pravý syn je červený. Pravého syna uzlu w přebarvíme na černo a odebereme černou z uzlu x. Pokud byl z, tj. rodič x červený, tak ho přebarvíme na



Obrázek 9: Č–Č případ 4: Bratr D je černý, jeho vnější syn E červený, před a po

černo a w na červeno. Provedeme LeváRotace(z).

Pozn: V případě vypouštění červené uzly (případy 3 a 4) tvoří rezervu, kterou můžeme využít lokálně. Pokud máme "v okolí"černé uzly (případ 2), musíme posouvat poruchu výš.

Složitost vypouštění je $O(\log n)$. Vlastní vypouštění (včetně přesunu listu) je $O(\log n)$. Při odstraňování poruchy všechny testy a akce trvají $O(1)$ a případy 1, 3 a 4 se vykonají jednou a případ 2 nejvýš $O(\log n)$-krát.

Pozn.: Popsané změny vykonáváme najednou. Při implementaci můžete samostatně rotovat a přebarvovat, ale pro účely vysvětlování a důkazu používáme pouze zobrazené stavy.

AVL stromy

Df (Adelson-Velskij, Landis): Binární vyhledávací strom je AVL strom (vyvážený AVL), právě když pro každý vrchol x ve stromě platí
$|h(levy(x)) - h(pravy(x))| \leq 1$,
kde $h(x)$ je výška (pod)stromu (počítáme úrovně hran).

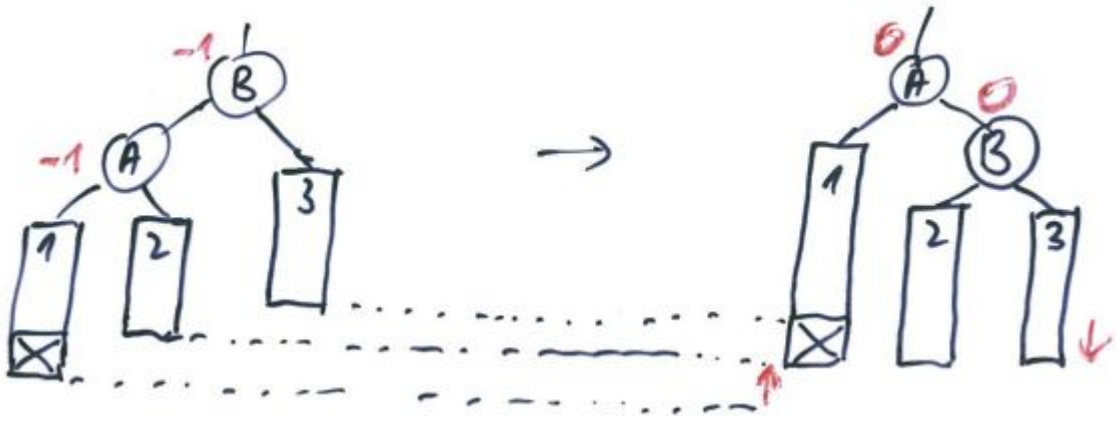
- pro efektivitu operací si pamatujeme explicitně (v položce vrcholu) aktuální vyvážení: v z množiny $\{-1, 0, +1\}$, kde $v = h(pravy) - h(levy)$

Věta: Výška AVL stromu s n vrcholy je $O(\log n)$.
Idea Dk: Konstruujeme nejnevyváženější strom, s nejméně vrcholy při dané výšce: označme p_n počet vrcholů takového stromu T_n s hloubkou n.
$T_0 : p_0 = 1$
$T_1 : p_1 = 2$
$T_n : p_n = p_{n-1} + p_{n-2} + 1 = fibonacci_{n+3} - 1$, (pro $fib_3 = 2$)
Pozn: $fibonacci_n \approx \phi^n = (\frac{1+\sqrt{5}}{2})^n \approx 1.618^n$

Důsledek: Všechny dotazovací operace pro BVS (Find, Min, Max, Succ, Predec) fungují na AVL stromě stejně a mají složitost $O(\log n)$

Zůstávají modifikující operace Insert, Delete.
Operace pracují stejně, po změně upravujeme zdola vyvážení, s případnou propagací změny nahoru (pokud to stačí) a případně použijeme rotace (jednoduchou, dvojitou)
- rotace je časově náročnější než úprava vyvážení (ale pořád $O(1)$)

Jednoduchá rotace: (obrázky na slajdech)



Obrázek 10: AVL: Přidáváme do vnějšího podstromu, před a po

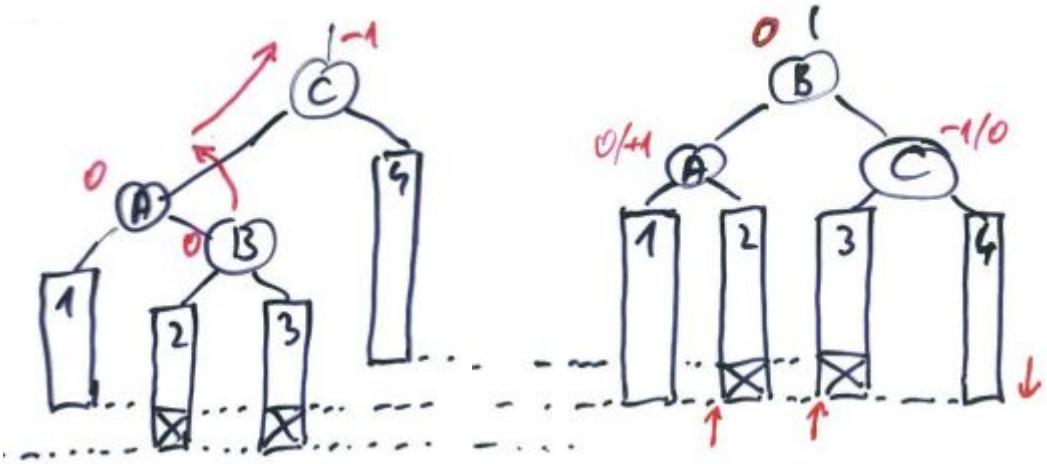
((T1,A/-1,T2),B/-1,T3) → (T1,A/0,(T2,B/0,T3))
- přidáváme prvek do stromu T1 (přesněji: hloubka T1 rostla)
- po rotaci se do předků nového A nešíří změna, protože původní hloubka zůstala zachována
- uspořádání zůstalo: $T1 < A < T2 < B < T3$

- pozn: Jsou programovací jazyky (Prolog, Haskell), které dovolují zapsat (vlastní rotaci, bez testů):

```
RotDoprava( t(t(T1,A,T2),B,T3), t(T1,A,t(T2,B,T3)) ).
RotDoprava (T (T t1 a t2) b t3) = T t1 a (T t2 b t3)
```

Neoptimální implementace rotace: zapamatujeme si ukazatele na "objekty"včetně rodiče B a potom nastavíme nové hodnoty pro jednotlivé změněné položky

Dvojitá rotace: ((T1,A/0,(T2,B/0,T3)),C/-1,T4) → ((T1,A,T2),B/0,(T3,C,T4))
- přidáváme prvek do T2 nebo T3, podle toho určíme vyvážení v A a C po rotaci
- po rotaci se do předků B opět nešíří změna
- uspořádání zůstalo



Obrázek 11: AVL: Přidáváme do vnitřního podstromu, před a po

- dvojitou rotaci bereme jako jeden celek a invarianty popisujeme před a po provedení, ne v mezistavu. Implementačně: lze použít dvě jednoduché rotace

- analogicky symetrické případy

Rozbor případů vyvážení při Insert: (BÚNO, přidávalo se do levého podstromu (tj. zvyšovala se hloubka vlevo))

1) +1 na 0, konec

2) 0 na -1, propagace zvýšení hloubky nahoru

3) -1, přidáváme do levého levého podstromu: jednoduchá rotace, konec

4) -1, přidáváme do pravého levého podstromu: dvojitá rotace, konec

V případech 3) a 4) je nový strom stejně hluboký jako původní, proto nemusíme propagovat změnu nahoru.

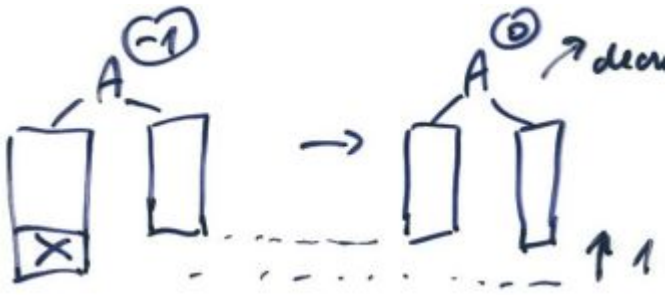
Rezerva pro vkládání je vhodná nevyváženost v kořeni.

Operace Delete, rozbor případů pro předky fyzicky vypouštěného vrcholu:

- ubíráme vrchol, tj. snižujeme výšku, BÚNO vlevo. Při

propagaci nahoru se snížila výška celého stromu a musíme upravovat na cestě ke kořeni.

1) -1 to 0, propagace snižování

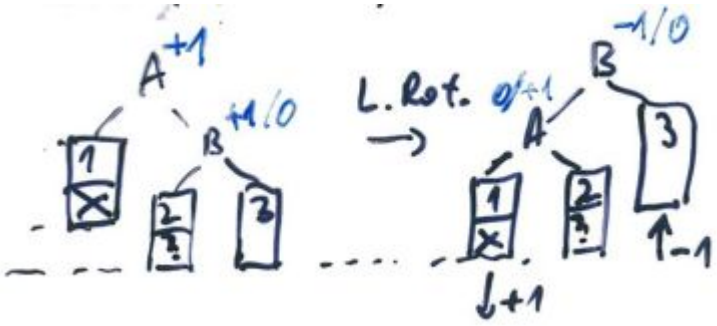


Obrázek 12: AVL: Delete 1: propagace nahoru, před a po

2) 0 to +1, konec

Obrázek 13: AVL: Delete 2: lokální oprava, před a po

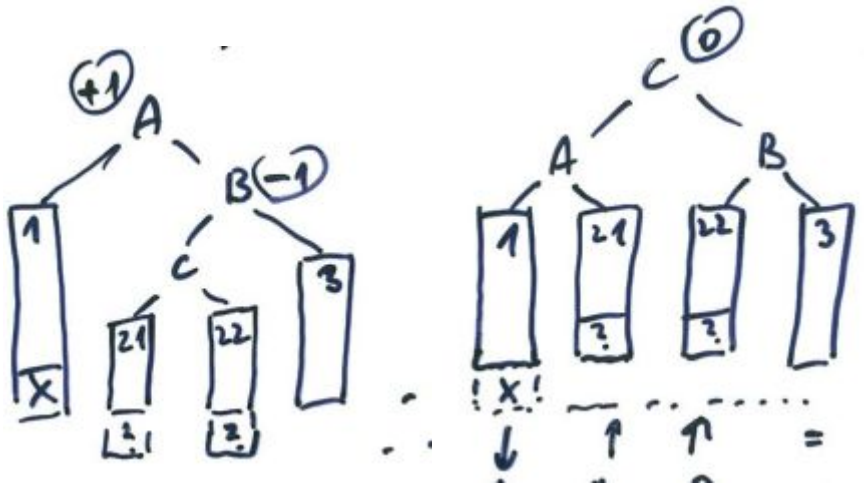
3) -1 v otci, -1 v bratrovi: jednoduchá L-rotace, propagace nahoru



Obrázek 14: AVL: Delete 3,4: před a po

4) -1 v otci, 0 v bratrovi: jednoduchá L-rotace, bez propagace

5) -1 v otci, +1 v bratrovi: dvojitá rotace, propagace nahoru



Obrázek 15: AVL: Delete 5: před a po

- Při Delete nezaručíme O(1) rotací jako v Č-Č stromech.

B-stromy

- B-stromy jsou vyvážené vyhledávací stromy

- jsou s proměnlivým počtem následníků, větším než 2: vrchol x s $n(x)$ klíči má $n(x)+1$ dětí

- aplikace: data na disku, indexové soubory databází

$\rightarrow$ přístup na disk je časově náročnější a diskové stránky se načítají celé, proto chceme menší hloubku za cenu většího počtu dětí a nevyužívání paměti (použitelné i pro bloky cache v operační paměti, obecně paměťovou hierarchii)

$\rightarrow$

B-strom má následující vlastnosti:

1. klíče jsou uloženy v neklesající posloupnosti (zleva doprava)
2. pokud je x vnitřní vrchol s $n(x)$ klíči, pak obsahuje $n(x)+1$ pointrů na děti
3. klíče ve vnitřním vrcholu rozdělují intervaly klíčů v podstromech
4. každý list je ve stejné hloubce
5. pro nějaké pevné t platí, $t \geq 2$ (tzv. minimální stupeň)
   (a) každý vrchol kromě kořene má aspoň $t-1$ klíčů. Každý vnitřní vrchol kromě kořene má aspoň t dětí. Pokud je strom neprázdný, má kořen aspoň 1 klíč.
   (b) každý vrchol má nejvíc $2t-1$ klíčů, teda nejvíc $2t$ dětí.

- pozn. k literatuře: Jsou různé varianty B-stromů. My používáme: s hodnotami ve vnitřních vrcholech (vs. pouze

v listech), s přípravným štěpením a slučováním – tj. počtem dětí p: $t \leq p \leq 2t$ (vs. $t-1 \leq p \leq 2t-1$)

Tvrzení: Pro $n \geq 1$ a každý B-strom T s n klíči, výškou h a minimálním stupněm $t \geq 2$ platí:
$h \leq \log_t \frac{n+1}{2}$
Dk: Pro strom dané výšky h je počet vrcholů minimální, když kořen obsahuje 1 klíč a ostatní vrcholy $t-1$ klíčů. Pak jsou 2 vrcholy v hloubce 1, $2t$ vrcholů v hloubce 2, $2t^2$ vrcholů v hloubce 3 atd., až $2t^{h-1}$ vrcholů v hloubce h.

Počet klíčů n splňuje:

$n \geq 1 + (t-1) \sum_{i=1}^{h} 2t^{i-1}$

$= 1 + 2(t-1)(\frac{t^h-1}{t-1})$

$= 2t^h - 1$

a odtud plyne tvrzení.

Operace na B-stromě:

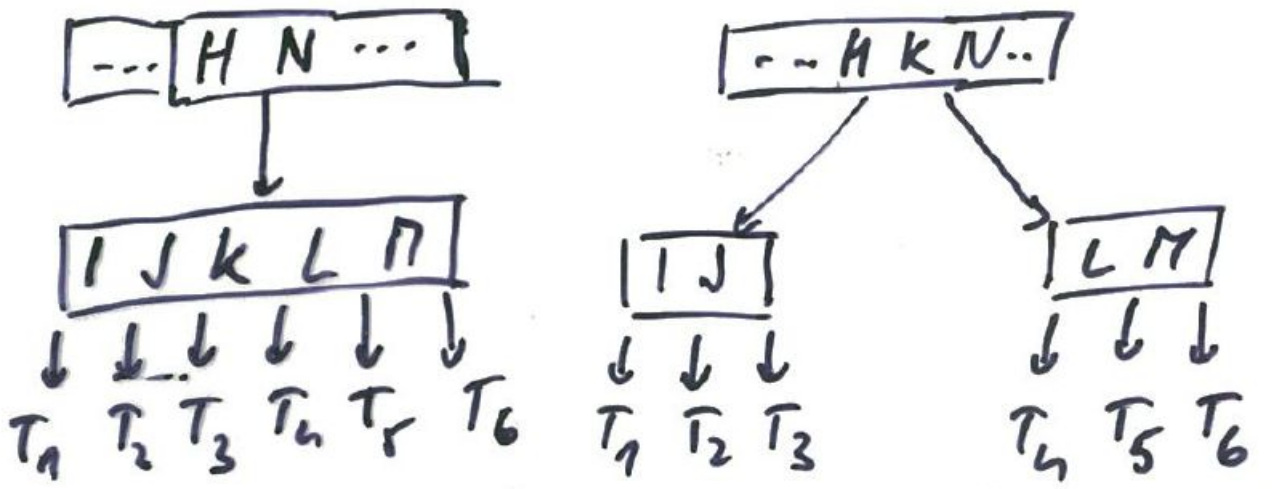
- Create - vytvoření stromu
- Search - nalezení prvku
- Insert - vložení prvku do stromu
- Delete - vypuštění prvku ze stromu

- pomocná operace: rozdělení plného vrcholu: štěpení a slévání

Obrázek 16.

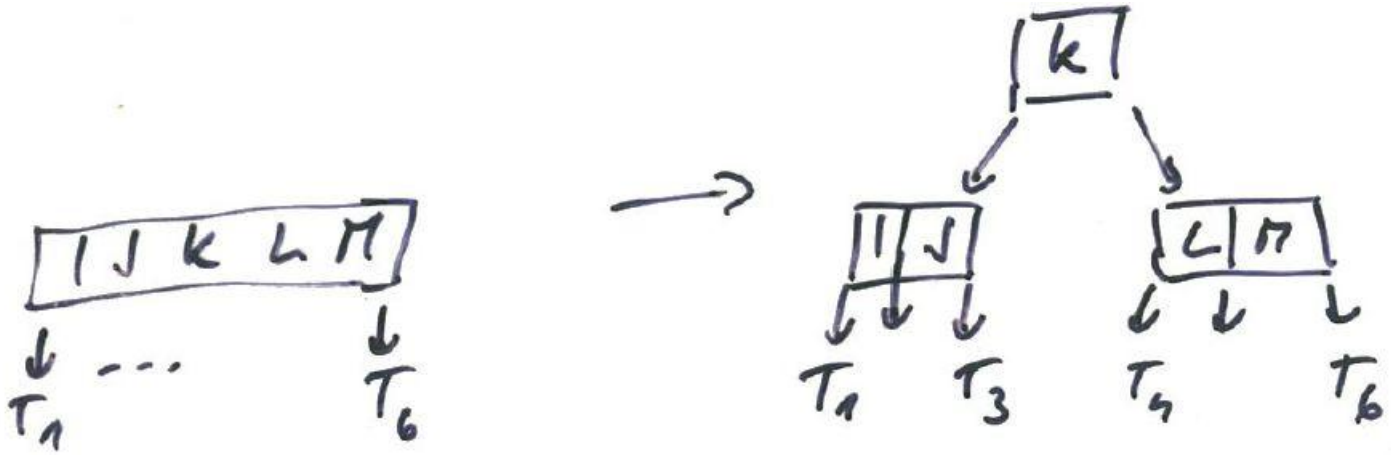
- vkládání do B-stromu výšky h: $O(h)$

- při průchodu dolů (preventivně) štěpíme plné vrcholy
- varianta: štěpíme při navracení, pak si musíme pamatovat



Obrázek 16: B-stromy: štěpení, $t = 3$: před a po

(a zamknout) cestu
- speciálně: dělení kořene způsobí zvýšení výšky o 1
Obrázek 17.



Obrázek 17: B-stromy: štěpení v kořeni, $t = 3$: před a po

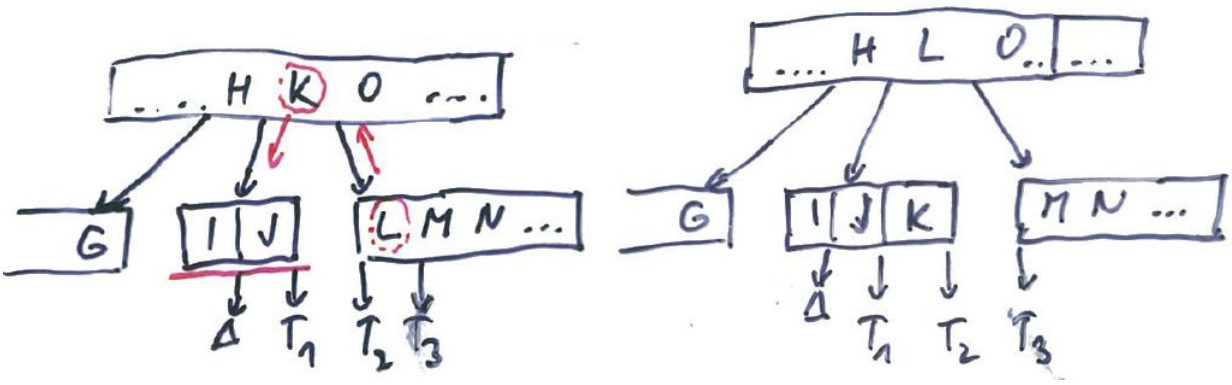
- invariant: vkládáme do neplného vrcholu

Vypouštění z B-stromu
- (rekurzivně) od kořene procházíme stromem, kontrolujeme a vynucujeme invariant: počet klíčů ve vrcholu je aspoň $t \rightarrow$ nejsme na minimu $t - 1$ klíčů
- zabezpečení invariantu: klíč z aktuálního vrcholu se přesune

do syna a nahradí se klíčem ze souseda syna
- speciální případ: kořen (v neprázdném stromě): Pokud kořen nemá žádné klíče a pouze 1 syna, snížíme výšku stromu.

Rozbor případů vypouštění:

1. vypouštíme klíč k z listu x: přímo
2. vypouštíme klíč k z vnitřního vrcholu x
   (a) pokud syn y, který předchází k v x, má aspoň t klíčů: najdi předchůdce k' ke klíči k ve stromě y. Vypusť k' a nahraď k klíčem k' v x. (Nalezení a vypuštění k' v jednom průchodu)
   (b) symetricky, pro následníka z klíče k
   (c) jinak, synové y a z mají $t-1$ klíčů. Slej k a obsah z do y, z vrcholu x vypusť klíč k a ukazatel na z. Syn y má $2t-1$ klíčů a vypustíme k ze syna y.
3. klíč k není ve zkoumaném vrcholu. Určíme odpovídající kořen c_i podstromu s klíčem k. Pokud c_i má pouze $t-1$ klíčů, uprav c_i podle 3a) nebo 3b), aby obsahoval aspoň t klíčů. Pak vypouštěj rekurzivně v odpovídajícím synovi.
   (a) Pokud c_i má $t-1$ klíčů a má souseda s t klíči, přesuň klíč z x do c_i, přesuň klíč z (bezprostředního) souseda do x a přesuň odpovídajícího syna ze souseda do c_i
   (b) Pokud oba sousedé mají $t-1$ klíčů, slej c_i s jedním ze sousedů. Přitom se přesune 1 klíč z vrcholu x do nově vytvářeného vrcholu (jako medián)



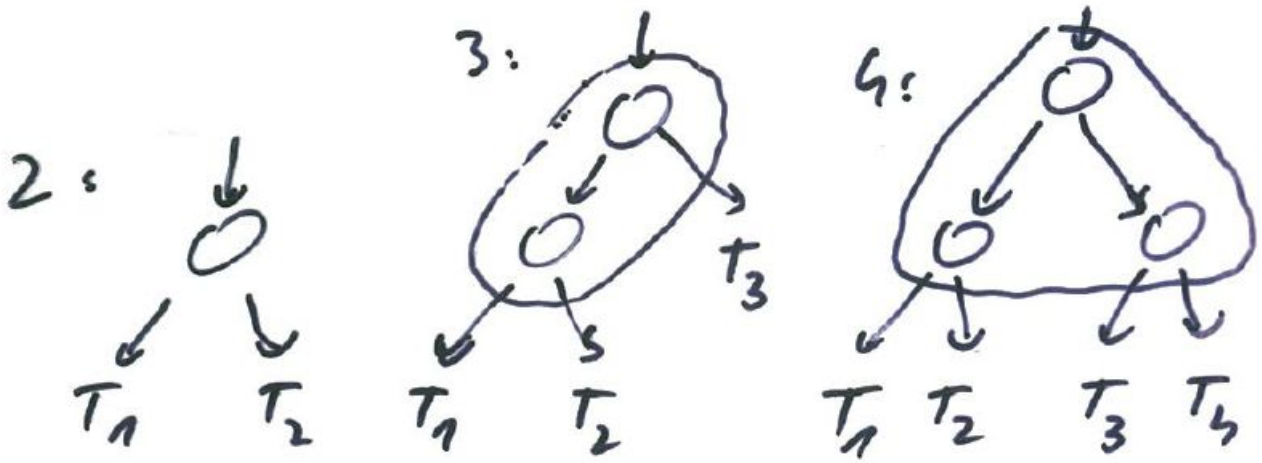
Obrázek 18: B-stromy: vypouštění – přesun: před a po

- složitost vypouštění ze stromu výšky h: máme $O(1)$ diskových přístupů na 1 hladině, proto je $O(h)$ diskových operací celkem

- přesun podrobně, 3a: (obrázek 18)
- uspořádání je zachováno
- hloubka se nemění, tj. neporuší
- nový vrchol IJK má t klíčů, tzn. splňuje invariant
- nový vrchol MN má aspoň $t - 1$ klíčů (po úpravě), tzn. splňuje podm. B-stromu

Souvislosti:

- souvislost s červeno-černými stromy: Pro $t = 2$ má vrchol B-stromu $1-3$ klíče a $2 - 4$ děti, nazývá se $2 - 4$ strom. Vrcholu B-stromu odpovídá černý vrchol s případnými červenými syny.
- varianta: všechna data v listech (tzv. externí reprezentace): výhody: víc B-stromů (indexů) nad stejnými daty, větší štěpení (šetřím pointry na data ve vnitřních vrcholech)
- varianta: počet p klíčů je: $t \leq p \leq 2t$, operace štěpení a slévání se vykonávají po úpravě podstromů, pro $t = 1$ dostaneme $2 - 3$ stromy, zobecnění: $a - b$ stromy



Obrázek 19: B-stromy a Č–Č stromy

- impl: provázané stromy - mají pointry na sousedy; slévání 3 vrcholů na 2; binární hledání pro pevnou délku klíčů; klíče proměnné délky (řetězce)
- statický strom (např. data na CD): vrcholy jsou naplněny, pamětí se neplýtvá

Hašování

- ideově vychází z přímo adresovatelných tabulek, které mají malé univerzum klíčů a prvky nemají stejné klíče.
- operace Insert, Search, Delete v čase $O(1)$
- implementace: pole; hodnoty pole obsahují reprezentované prvky (nebo odkazy na ně) anebo NIL
  - Ale přímo adresovatelné tabulky nevyhovují vždy:
- univerzum klíčů U je velké vzhledem k množině klíčů K, které jsou aktuálně uloženy ve struktuře
- prvky mají stejné klíče
  - idea: adresu budeme z klíče počítat
- hašovací funkce $h : U \to \{0, 1, \ldots, m-1\}$ mapuje univerzum klíčů U do položek hašovací tabulky $T[0..m-1]$
  $\to$ redukce paměti
- problém: vznikají kolize: dva klíče se hašují na stejnou hodnotu
- pozorování: kolizím se nevyhneme, pokud $|U| > m$

Řešení kolizí:
- zřetězením prvků
- otevřená adresace

Pozn: Hašovací funkce mají i jiné aplikace (s jinými požadavky) než pro datové struktury.
- kryptografické hašovací funkce: otisk MD5 (Message Digest 5) nebo SHA2: v kryptografii (např.) pro ověřování neporušenosti zpráv; pro adresaci/identifikaci objektů/souborů v distribuovaných systémech
- hašování pro výrobu signatury: předfiltrování stejných (částí)

klíčů (alg. Rabin-Karp: inkr. změny; Bloomův filtr; "texty"a bioinformatika); databáze: operace join (nerovnoměrné rozdělení dat); transpoziční tabulky v hrách (kolize řešíme přepisováním)

Analýza hašování se zřetězením

Df: Faktor naplnění $\alpha = \frac{n}{m}$ pro tabulku T velikosti m, ve které je uloženo n prvků.
V tabulce se zřetězením může platit $n > m$, teda $\alpha > 1$.

Předpoklady
- jednoduché uniformní hašování: Každý prvek se hašuje do m položek tabulky se stejnou pravděpodobností, nezávisle na jiných prvcích
- hodnota hašovací funkce $h(k)$ se počítá v čase $O(1)$

Analýza hledání prvku:
- úspěšné nalezení
- neúspěšné hledání

Věta: V hašovací tabulce s řešením kolizí pomocí zřetězení neúspěšné vyhledávání trvá průměrně $\Theta(1+\alpha)$, za předpokladu jednoduchého uniformního hašování
Dk: Podle předpokladu se klíč k hašuje se stejnou pravděpodobností do každé z m položek. Neúspěšné hledání klíče k je průměrný čas prohledání jednoho ze seznamů do konce. Průměrná délka seznamů je α. Proto je očekávaný počet navštívených prvků α a celkový čas (včetně výpočtu hašovací funkce $h(k)$) je $\Theta(1 + \alpha)$.

Úspěšné vyhledávání

Věta: V hašovací tabulce s řešením kolizí pomocí zřetězení úspěšné vyhledávání trvá průměrně $\Theta(1+\alpha)$ za předpokladu jednoduchého uniformního hašování.
Dk: Předpokládáme, že vyhledáváme každý z n uložených klíčů se stejnou pravděpodobností. Předpokládáme, že nové prvky se ukládají na konec seznamu.
Očekávaný počet navštívených vrcholů při úspěšném vyhledávání je o 1 větší než při vkládání tohoto prvku. Počítáme průměr přes n prvků v tabulce z 1+ očekávaná délka seznamu, do kterého se přidává i-tý prvek. Očekávaná délka tohoto seznamu je $(i-1)/m$. Dostaneme:

$$\begin{aligned}
\frac{1}{n}\sum_{i=1}^{n}(1+\frac{i-1}{m}) &= 1+\frac{1}{nm}\sum_{i=1}^{n}(i-1) \\
&= 1+\frac{1}{nm}(\frac{(n-1)n}{2}) \\
&= 1+\frac{\alpha}{2}-\frac{1}{2m} \\
&= \Theta(1+\alpha)
\end{aligned}$$

Závěr: Pokud $n = O(m)$, pak $\alpha = n/m = O(m)/m = O(1)$
Po vyhledání, vlastní operace pro přidání, resp. vypuštění prvku v čase $O(1)$.

- pozn: ukládání na konec vs. na začátek (frekventované klíče vs. princip lokality)

Volba Hašovacích funkcí

1) dělením
2) násobením
3) univerzální hašování (samostatně)

Dobrá hašovací funkce splňuje (přibližně) předpoklady jednoduchého uniformního hašování
Pro rozložení pravděpodobností P zvolení klíče k z univerza U chceme:
$\sum_{k:h(k)=j} P(k) = \frac{1}{m}$ pro $j = 0, 1..m-1$
ale: obvykle rozložení pravděpodobností neznáme
- interpretujeme klíče jako (přirozené) čísla, aby se daly používat aritmetické operace

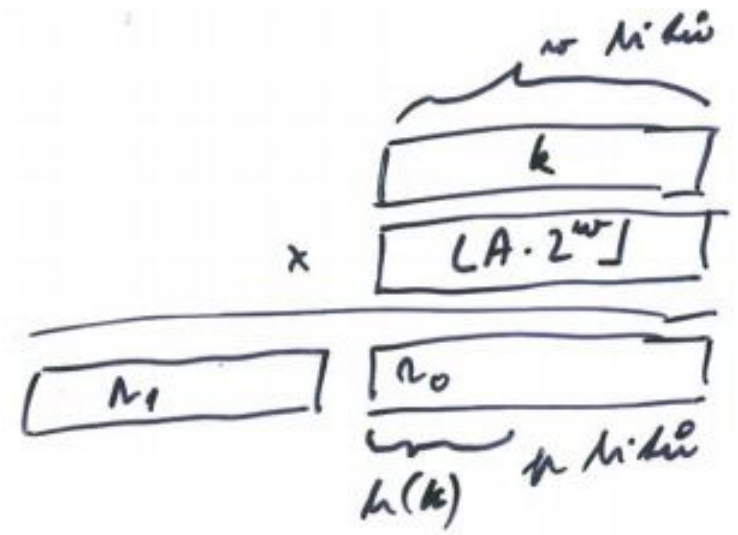
1) Dělení
$h(k) = k \bmod m$ zbytek po dělení
nevhodné pro $m = 2^p, 10^p, 2^p - 1$
vhodné: prvočísla "vzdálené"od mocnin dvojky

2) Násobení
$h(k) = \lfloor m(kA \bmod 1) \rfloor$, pro $k \in [0, 1)$
obvykle pro $m = 2^p$
Knuth doporučuje $A \approx (\sqrt{5}-1)/2 = 0,6180339887$ ... zlatý řez ϕ-1

"Paradox"narozenin (a vztah k hašování): Mezi 23 (a více) lidmi jsou s pravděpodobností větší než 50% aspoň dva se stejnými narozeninami.

Otevřené adresování

- všechny prvky jsou uloženy v tabulce, proto $\alpha < 1$



Obrázek 20: Hašování násobením

- pro řešení kolizí nepotřebujeme pointry, ale počítáme adresy navštívených pozic

$\rightarrow$ ve stejné paměti máme větší tabulku než při zřetězení
- posloupnost zkoušených pozic závisí na klíči a pořadí pokusu: $h : U \times \{0, 1, \ldots, m-1\} \rightarrow \{0, 1, \ldots, m-1\}$
- prohledávání pozic v posl. $\langle h(k,0), h(k,1), \ldots, h(k, m-1)\rangle$

- operace Search, Insert, Delete (pouze někdy)

Předpoklad uniformního hašování: každá permutace pozic $\{0..m-1\}$ je pro každý klíč vybrána stejně pravděpodobně jako posloupnost zkoušených pozic
- je těžké implementovat, používají se metody, které to nesplňují

Otevřené adresování - metody:

1. lineární zkoušení
2. kvadratické zkoušení

3. dvojité hašování

1) Lineární zkoušení, pro hašovací funkci $h' : U \to 0..m-1$ bude
$h(k,i) = (h'(k) + i) \bmod m$
- pouze m různých posloupností zkoušených pozic (a nezáleží na přírůstku)
- problém: primární klastrování: vznikají dlouhé úseky obsazených pozic
Pravděpodobnost obsazení pozice při vkládání závisí na obsazenosti předchozích pozic: pokud je obsazeno i pozic před, je pravděpodobnost obsazení $\frac{i+1}{m}$: speciálně pro $i = 0$, tj. předcházející prázdnou pozici, je pravděpodobnost $1/m$.

Příklad: $\alpha = 0.5$, porovnejte
a) obsazeny sudé pozice
b) obsazena první polovina tabulky
- DC: lze implementovat Delete: následující prvky posuneme, pokud patří na/před uvolňované místo

2) Kvadratické zkoušení:
$h(k,i) = (h'(k) + c_1 i + c_2 i^2) \bmod m$, $c_1 \neq 0$, $c_2 \neq 0$
- aby se prohledala celá tabulka, hodnoty c_1, c_2 a m musí být vhodně zvoleny
- pro stejnou počáteční pozici klíčů x a y (tj. $h(x,0) = h(y,0)$) následuje stejná posloupnost zkoušených pozic
$\to$ problém: druhotné klastrování
- pouze m různých posloupností pozic

3) Dvojité hašování

$h(k,i) = (h_1(k) + i.h_2(k)) \bmod m$, h_1 a h_2 jsou pomocné hašovací funkce
- $h_2(k)$ nesoudělné s m, aby se prošla celá tabulka
možné volby:
a) $m = 2^p$ a $h_2(k)$ je liché
b) m prvočíslo, $0 < h_2(k) < m$

Příklad:
$h_1(k) = k \bmod m$
$h_2(k) = 1 + (k \bmod m')$, kde m' je o trochu menší než m

- máme $\Theta(m^2)$ posloupností zkoušených pozic

- místo Delete používáme Pseudodelete: vypouštěný prvek zneplatníme, odstraníme ho při přehašování tabulky

Analýza hašování s otevřeným adresováním

- "obvyklé"předpoklady: uniformní hašování: Pro každý klíč k je posloupnost zkoušených pozic libovolná permutace $\{0..m-1\}$ se stejnou pravděpodobností.

Věta: V tabulce s otevřeným adresováním s faktorem naplnění $\alpha = n/m < 1$ je očekávaný počet zkoušených pozic při neúspěšném vyhledávání nejvíce $1/(1-\alpha)$, za předpokladu uniformního hašování.

Dk: Všechny zkoušky pozice kromě poslední našly obsazenou pozici.
Definujme $p_i = Pr\{$právě i zkoušek našlo obsazenou pozici$\}$
Očekávaný počet zkoušek je $1 + \sum_{i=0}^{\infty} i \cdot p_i$ (1)
Definujme $q_i = Pr\{$aspoň i zkoušek našlo obsazenou pozici$\}$
Platí $1 + \sum_{i=0}^{\infty} i \cdot p_i = 1 + \sum_{i=1}^{\infty} q_i$, chceme spočítat q_i (!Σ od "1")
První zkouška narazí na obsazenou pozici s pravděpodobností

$n/m = q_1$.
Obecně $q_i = (\frac{n}{m})(\frac{n-1}{m-1})...(\frac{n-i+1}{m-i+1}) \leq (\frac{n}{m})^i = \alpha^i$
Spočítáme (1): $1 + \sum_{i=0}^{\infty} i \cdot p_i = 1 + \sum_{i=1}^{\infty} q_i \leq 1 + \sum_{i=1}^{\infty} \alpha^i = \frac{1}{1-\alpha}$,
QED

Důsledek: vkládání prvku vyžaduje nejvýš $1/(1-\alpha)$ zkoušek, za stejných předpokladů.

Věta: V tabulce s otevřeným adresováním s faktorem naplnění $\alpha = n/m < 1$ je očekávaný počet zkoušek při úspěšném vyhledávání nejvíc

$$\frac{1}{\alpha} \ln \frac{1}{1-\alpha} + \frac{1}{\alpha}$$

za předpokladu uniformního hašování a pokud vyhledáváme každý klíč v tabulce se stejnou pravděpodobností.

Dk: Vyhledávání klíče k zkouší stejnou posloupnost pozic jako při vkládání klíče k. Podle minulého důsledku je vkládání $(i+1)$-ního klíče vykonáno na $1/(1-i/m)$ zkoušek.
Platí $1/(1 - i/m) = m/(m - i)$.
Průměr přes všechny klíče v tabulce je hledaný počet zkoušek: $\frac{1}{n} \sum_{i=0}^{n-1} \frac{m}{m-i} = \frac{m}{n} \sum_{i=0}^{n-1} \frac{1}{m-i} = \frac{1}{\alpha}(H_m - H_{m-n})$ kde $H_i = \sum_{j=1}^{i} \frac{1}{j}$ je i-té harmonické číslo. Platí $\ln i \leq H_i \leq \ln i + 1$, odtud

$$\begin{aligned} \frac{1}{\alpha}(H_m - H_{m-n}) &\leq \frac{1}{\alpha}(\ln m + 1 - \ln(m-n)) \\ &\leq \frac{1}{\alpha} \ln \frac{m}{m-n} + \frac{1}{\alpha} \\ &\leq \frac{1}{\alpha} \ln \frac{1}{1-\alpha} + \frac{1}{\alpha} \end{aligned}$$

QED

Univerzální hašování

Idea: zvolíme hašovací funkce náhodně a nezávisle na klíčích (za běhu, z vhodné množiny funkcí)
- použití randomizace

Df. Nechť H je konečná množina hašovacích funkcí z univerza klíčů U do $\{0..m-1\}$. Množinu H nazveme univerzální, pokud pro každé dva různé klíče $x, y \in U$ je počet hašovacích funkcí $h \in H$, pro které $h(x) = h(y)$, roven $|H|/m$.
- tj. pro náhodně zvolenou funkci h je pravděpodobnost kolize pro x a y, kde $x \neq y$, právě $1/m$. To je stejná pravděpodobnost, jako když jsou hodnoty $h(x)$ a $h(y)$ zvoleny náhodně z množiny $\{0..m-1\}$
- implementace: hašovací funkce závisí na parametrech, které se zvolí za běhu.
$H = \{h_a(x) : U \to \{0..m-1\} | a \in A\}$, kde $h_a(x) = h(a, x)$, a je parametr

Důsledky randomizace:
- žádný konkrétní vstup (konkrétních n klíčů) není apriori špatný
- opakované použití na stejný vstup volá (skoro jistě) různé hašovací funkce

$\rightarrow$ "průměrný případ" nastane pro libovolné rozložení vstupních dat (!); průměr přes možné haš. fce

Věta: Nechť h je náhodně vybraná hašovací funkce z univerzální množiny hašovacích funkcí a nechť je použita k hašování n klíčů do tabulky velikosti m, kde $n \leq m$. Potom očekávaný počet kolizí, kterých se účastní náhodně vybraný konkrétní klíč x je menší než 1.

Dk: Pro každý pár různých klíčů y a z označme c_{yz} náhodnou proměnnou, která nabývá hodnotu 1, pokud $h(y) = h(z)$ a 0 jinak.
Z definice, konkrétní pár klíčů koliduje s pravděpodobností $1/m$, proto očekávaná hodnota $E[c_{yz}] = 1/m$.
Označme C_x celkový počet kolizí klíče x v hašovací tabulce T velikosti m obsahující n klíčů. Pro očekávaný počet kolizí máme:

$$E[C_x] = \sum_{y \in T, y \neq x} E[c_{xy}] = \frac{n-1}{m}$$

Protože $n \leq m$, platí $E[C_x] < 1$.

Pozn: předpoklad $n \leq m$ implikuje, že průměrná délka seznamu klíčů nahašovaných do stejné adresy je menší než 1.

Konstrukce univerzální množiny hašovacích funkcí (jedna z možností).

Zvolíme prvočíslo m jako velikost tabulky. Každý klíč x rozdělíme na $r+1$ částí (např. znaků, hodnota r závisí na velikosti klíčů). Píšeme $x = \langle x_0, x_1 ... x_r \rangle$. Zvolené r splňuje podmínku, že každá část x_i je (ostře) menší než m. Zvolme $a = \langle a_0, a_1 ... a_r \rangle$ posloupnost $(r+1)$ čísel náhodně a nezávisle z množiny $\{0, 1..m-1\}$. Definujeme $h_a \in H$: $h_a(x) = \Sigma_{i=0}^{r} a_i x_i \bmod m$ a $H = \cup_a \{h_a\}$
Platí $|H| = m^{r+1}$, tj. počtu různých vektorů a.

Věta: H je univerzální množina hašovacích funkcí.
Dk: Uvažujme různé klíče x a y. Bez újmy na obecnosti, nech $x_0 \neq y_0$. Pro pevné hodnoty $a_1, a_2 ... a_r$ je právě jedna hodnota a_0, která splňuje $h(x) = h(y)$. Je to řešení rovnice

$$a_0(x_0 - y_0) \equiv -\sum_{i=1}^{r} a_i(x_i - y_i) \bmod m$$

Protože m je prvočíslo, nenulová hodnota $x_0 - y_0$ má jediný inverzní prvek modulo m a teda existuje jediné řešení pro a_0 modulo m. Následně, každý pár klíčů x a y koliduje pro právě m^r hodnot vektoru a, protože kolidují právě jednou pro každou volbu $\langle a_1, a_2 ... a_r \rangle$, tj. pro jedno a_0. Protože je m^{r+1} možností pro a, klíče kolidují s pravděpodobností $m^r/m^{r+1} = 1/m$. Teda H je univerzální. QED

- pozn: a_i vybíráme včetně 0

Příklad randomizace: Zobristovo hašování pro reprezentaci pozic her (v transpozičních tabulkách), používá náhodná čísla pro (jednobitové) rysy/fíčury, používá xor (místo plus a mod), typicky v 32 bitech.
- Pro zjištění úspěchu nalezení se neporovnávají celé klíče, tj.

pozice, ale hodnota sekundární hašovací funkce.

Hašování a rostoucí tabulky (dynamizace h.t.)

Chceme odstranit nevýhody hašování:
- pevná velikost tabulky
- nedokonalá implementace Delete (u některých metod)
při zachování asymptotické ceny operací (tj. průměrně $O(1)$ pro pevné α)

Idea: Periodická reorganizace datové struktury
- při růstu: při dosažení naplnění α zvětšíme tabulku d-krát (např. $d = 2$, z $m = 2^i$ na $m = 2^{i+1}$) a prvky přehašujeme (s novou haš. fcí.)

Dále uvažujme $d = 2$: aspoň $2^{i-1}.\alpha$ operací Insert (od posledního přehašování) zaplatí:

- 1x: přidání $2^{i-1}.\alpha$ prvků do staré tabulky
- 2x: přehašování $2.2^{i-1}.\alpha$ prvků

DC: Kredit operace obecně $\leq \frac{2d-1}{d-1}$

- pozn: vhodné α lze spočítat (z pohledu efektivity budoucích operací s a bez přehašování)

- operace přehašování je amortizována minulými operacemi, které vytvoří dostatečný kredit $\rightarrow$ amortizovaná složitost

Obecné řešení při růstu i zmenšování tabulky: po přehašování je naplnění tabulky $\alpha/4$ až $\alpha/2$, označme $n^* = \alpha.m$.
- tabulku zvětšíme, pokud máme n^* prvků (proběhlo aspoň $n^*/2$ operací Insert)
- tabulku zmenšíme, pokud máme $n^*/8$ prvků (proběhlo aspoň $n^*/8$ operací Delete)

Pozn: Aktuální počet prvků si pamatujeme; pseudovolné místa uvolníme; vytvoření pseudovolného místa potřebuje (aspoň) 2 operace. Přehašování dávkové vs. postupné. Jsou i jiné metody dynamizace dat. struktur.

Haldy ...

Grafové algoritmy

Reprezentace grafu $G = (V, E)$, kde V je množina vrcholů a E je množina hran

1. Matice sousednosti
   $A = (a_{ij})$ typu $|V| \times |V|$
   $a_{ij} = 1$ pokud $(v_i, v_j) \in E$
   $= 0$ jinak

2. Seznamy sousedů
   pole `sousedé` velikosti V
   pro $u \in V$ je `sousedé[u]` hlava seznamu obsahující vrcholy v, pro které platí $(u, v) \in E$
   - paměť: $O(|V| + |E|) = O(\max(|V|, |E|))$
   - lze použít pro varianty:

   (a) neorientovaný graf

   (b) (hranově) ohodnocený graf: cena: $E \to R$

   (c) seznamy sousedů generované dynamicky (šetří paměť)

3. Výpočtem, tj. implicitně zadaný graf: `jeHrana(G,u,v)` vrací *boolean*, `sousedi(G,v)` vrací sousedy (pole/seznam, i líně/iterátorem)

Prohledávání grafů

Dvě metody:

- prohledávání do hloubky (DFS - Depth First Search)
- prohledávání do šířky (BFS - Breadth First Search)

Prohledávání do hloubky

Vstup: graf $G = (V, E)$, zadaný pomocí seznamů sousedů
pomocné datové struktury:

- $\pi(v)$ ... otec vrcholu v ve stromu prohledávání
- $p(v)$ ... pořadí, v němž jsou vrcholy $v \in V$ navštíveny
- pořadí ... globální proměnná, slouží k číslování vrcholů

Algoritmus DFS(G)

```
 1 forall u in V do p(u)<-0, pi(u)<-NIL od
 2 pořadí <- 0
 3 forall u in V do
 4   if  p(u)=0 then Navštiv(u) fi
 5               od

 6 procedura Navštiv(u)
 7 pořadí++; p(u)<-pořadí
 8 forall v in sousedé[u] do
 9   if p(v) = 0 then
10     pi(v) <- u
11     Navštiv(v)
12   fi
13 od.
```

Časová složitost: $O(m + n), n = |V|, m = |E|$
- graf průchodu do hloubky (DFS-les):
$G_\pi = (V, E_\pi)$, kde
$E_\pi = \{(\pi(v), v) | v \in V \wedge \pi(v) \neq NIL\}$

- aplikace DFS:
komponenty grafu
existence kružnice

Df: uzavřený vrchol v: všechny hrany vedoucí z v jsme prohledali

- pro některé aplikace potřebujeme místo časů otevření (tj. pořadí) časy uzavření (nebo obojí).

Klasifikace hran grafu G:

stromová hrana - vede do nového vrcholu

zpětná hrana - vede do už navštíveného (neuzavřeného) vrcholu

dopředná hrana (u, v) - pouze v orientovaném grafu
- vede do uzavřeného vrcholu v, kde pořadí$(u) <$ pořadí(v)

příčná hrana - pouze v orientovaném grafu
- vede do uzavřeného vrcholu v, kde pořadí$(u) >$ pořadí(v)

- pozn: (programování řízené událostmi:) některé algoritmy lze popsat tak, že jednotlivé druhy hran, případně události otevření a uzavření vrcholu, mají své výkonné procedury
- generický alg. a označení vrcholů barvami: černá - uzavřený, tj. prohledaný, šedý - otevřený, tj. prohledávaný, bílá - neotevřený. Udržování invariantu: následnící černého jsou šedí. Pokud projdu všechny šedé vrcholy (a přebarvím je na černo), pak právě všechny dosažitelné vrcholy grafu (ze zvolené šedé počáteční množiny) jsou černé (a nedosažitelné bílé).
- aplikace: garbage collector, serializace dyn. paměti
- impl. (pro implicitní grafy): iterativní prohlubování

Prohledávání do šířky

Vstup: graf $G = (V, E)$, zadaný pomocí seznamů sousedů a vrchol s, ve kterém začíná prohledávání
pomocné datové struktury:

- $\pi(v)$ ... otec vrcholu v ve stromu prohledávání
- $d(v)$ ... vzdálenost z vrcholu s do v
- F ... fronta (neuzavřených vrcholů), operace Přidej, Odeber, funkce Prázdná

Algoritmus BFS(G)

```
 1 forall u in V\{s} do d[u]<- +inf, pi(u)<-NIL od
 2 d[s]<-0; pi[s]<-NIL; Pridej(F,s);
 3 while not Prazdna(F) do
 4   Odeber(F,u);
 5   forall v in sousede(u) do
 6     if d(v) = +inf then
 7       d(v) <- d(u)+1;
 8       pi(v) <- u;
 9       Pridej(F,v);
10     fi
11   od
12 od.
```

Časová složitost: $O(m + n), n = |V|, m = |E|$

- strom průchodu do šířky (BFS-strom):

$G_\pi = (V_\pi, E_\pi)$
$V_\pi = \{v \in V | \pi(v) \neq NIL\} \cup \{s\}$
$E_\pi = \{(\pi(v), v) | v \in V_\pi \setminus \{s\}\}$

- aplikace: nejkratší cesta, $d(v)$ je délka nejkratší cesty z s do v; rekonstrukce cesty (i jinde): pomocí π odzadu

Topologické uspořádání

Df: Posloupnost $v_1, v_2 \dots v_n$ je topologické uspořádání vrcholů orientovaného grafu G, pokud pro každou hranu: $(v_i, v_j) \in E \rightarrow i \leq j$

T: Graf G lze topologicky uspořádat $\leftrightarrow$ G je acyklický (tzv. DAG) $\leftrightarrow$ DFS(G) nenajde zpětnou hranu

- DAG: Directed Acyclic Graph
- pojmy:

- vrchol, poprvé navštívený algoritmem DFS, se nazývá otevřeným
- otevřený vrchol se stane uzavřeným, když je dokončeno zpracování seznamu jeho sousedů

Algoritmus Topologické uspořádání(G)
1. volej DFS(G) a spočítej časy uzavření vrcholů
2. `if` existuje zpětná hrana `then`
3. `return` "G není acyklický";
4. každý vrchol, který je uzavřen, ulož na začátek spojového seznamu S
5. `return` S.

- Časová složitost: $\Theta(|V| + |E|)$, v tom:
- prohledávání do hloubky: $\Theta(|V| + |E|)$
- vkládání vrcholů do výstupního seznamu S: $|V| \cdot O(1)$
- (nevhodná impl: třídění hran podle $k(u)$ v $\Theta(n \log n)$)

Silně souvislé komponenty (SSK)

Df: Orientovaný graf je silně souvislý, pokud pro každé dva vrcholy u, v existuje orientovaná cesta z u do v a současně z v do u.

Silně souvislá komponenta grafu je maximální podgraf, který je silně souvislý.

- pozn: Každý vrchol grafu patří do právě jedné komponenty a ty tvoří rozklad množiny vrcholů

- opačný graf $G^T = (V, E^T)$, kde $E^T = \{(u, v)|(v, u) \in E\}$

- $k(v), v \in V$: pořadí, v jakém jsou vrcholy uzavírány algoritmem DFS

Algoritmus SSK(G)

1. Algoritmem DFS(G) urči časy uzavření $k(v)$ pro všechny $v \in V$
2. Vytvoř G^T
3. Uspořádej vrcholy do klesající posloupnosti podle $k(v)$ a v tomto pořadí je zpracuj algoritmem DFS(G^T)
4. Silně souvislé komponenty grafu G jsou právě podgrafy indukované vrcholovými množinami jednotlivých DFS-stromů z minulého kroku.

Korektnost SSK

Lemma 1. Nechť C, C' jsou dvě různé silně souvislé komponenty grafu G. Pokud existuje cesta v G z C do C', pak neexistuje cesta z C' do C.

Značení: Pro $U \subseteq V(G)$ položme $p(U) = min\{p(u)|u \in U\}$ a $k(U) = max\{k(u)|u \in U\}$, kde
$p(u)$ je čas prvního navštívení vrcholu u (otevření)
$k(u)$ je čas uzavření u

Lemma 2. Nechť C, C' jsou dvě různé silně souvislé komponenty grafu G. Existuje-li hrana z C do C', pak $k(C) > k(C')$.

Věta: Vrcholové množiny DFS-stromů vytvořených algoritmem SSK(G) při průchodu do hloubky grafem G^T odpovídají vrcholovým množinám silně souvislých komponent grafu G.

Dk: Indukcí podle počtu projitých stromů.
- z jednoho (prvního navštíveného) vrcholu u komponenty C projdu celou komponentu v G^T i v G, $k(u) = \max\limits_{v \in C} k(v) (= k(C))$
- pokud se dostanu hranou mimo komponentu (do vrcholu v), je v už uzavřený.

DC: Ukažte, že pokud ve druhém průchodu v algoritmu SSK(G) procházíme graf G (místo G^T) v pořadí rostoucích časů uzavření (místo klesajících), nedostaneme správné komponenty.

Složitost SSK: $\Theta(|V| + |E|)$

Df: Kondenzace grafu: Mějme orientovaný graf $G = (V, E)$ a nechť $V_1 \dots V_k$ jsou množiny vrcholů odpovídající silným komponentám grafu G. Orientovaný graf $C(G)$ se nazývá *kondenzace* grafu G a je definován $C(G) = (\{V_1 \dots V_k\}, E')$, kde $(V_i, V_j) \in E'$, pokud existují vrcholy $x \in V_i$ a $y \in V_j$

takové, že $(x, y) \in E$.

- Kondenzace $C(G)$ grafu G neobsahuje cyklus a teda je DAG.

- DC: další aplikace prohledávání DFS (pomocí lowlink: minimum $p(x)$ konců dosažitelných zp.h.): určení mostů, artikulací, určení reprezentantů SSK, výroba kondenzace

Problém nejkratší cesty

Používáme:
- orientovaný graf $G = (V, E)$
- ohodnocení hran $c : E \to R$
- cena orientované cesty P, $P = v_0, v_1 \ldots v_k$ je

$$c(P) = \sum_{i=1}^{k} c(v_{i-1}, v_i)$$

- Cena nejkratší cesty z u do v

$$\delta(u, v) = \min\{c(P) | P \text{ je cesta z } u \text{ do } v\}$$

- nejkratší cesta z u do v je libovolná cesta P z u do v, pro kterou $c(P) = \delta(u, v)$
- $\delta(u, v) = \infty$ znamená, že (orientovaná) cesta neexistuje
- Zavedeme: $\infty + r = \infty, \infty > r \quad$ pro $\forall r \in R$

Varianty problému Najít nejkratší cestu

1. z u do v, $\quad u, v \in V$ pevné
2. z u do x, $\quad$ pro každé $x \in V$, u pevné
3. z x do y, $\quad$ pro každé $x, y \in V$

Pomocná operace UvolněníHrany(u,v)

```
if d(v) > d(u) + c(u,v)
  then d(v) <- d(u)+ c(u,v)
       pi(v) <- u
fi.
```

Rekonstrukce cesty: (opět) pomocí předchůdců π

Dijkstrův algoritmus (1959) pro cesty z jednoho vrcholu do všech (nebo jednoho konkrétního)

Vstup:
$G = (V, E)$ orientovaný graf
$c : E \to R_0^+$ nezáporné ohodnocení hran
$s \in V$ počáteční vrchol

Výstup:
$d(v), \pi(v)$ pro $\forall v \in V$, tž. $d(v) = \delta(s, v)$
$\pi(v)$ je předchůdce vrcholu v na (nějaké) nejkratší cestě z s do v

Algoritmus

```
01 forall v in V(G) do
02   d(v) <- infty % inicializace
03   pi(v) <- NIL   od
04 d(s) <- 0
05 D <- empty
06 N <- V
07 while N <> empty do
08   u <- OdeberMin(N)
09   D <- D union {u}
10   forall v in Sousede[u] & v in N do
11     UvolněníHrany(u,v)
12   od
13 od.
```

Korektnost Dijkstrova alg.
Lemma 1. Optimální podstruktura

Je-li $v_1 \dots v_k$ nejkratší cesta z v_1 do v_k, potom $v_i \dots v_j$ je nejkratší cesta z v_i do v_j pro $\forall i, j, 1 \leq i < j \leq k$

Lemma 2. Trojúhelníková nerovnost
$\delta(s, v) \leq \delta(s, u) + c(u, v)$ pro každou hranu (u, v)
- po provedení inicializace je ohodnocení vrcholů měněno jen prostřednictvím UvolněníHrany

Lemma 3. Horní mez
$d(v) \geq \delta(s, v)$ pro každý vrchol v a po dosažení hodnoty $\delta(s, v)$ se $d(v)$ už nemění

Lemma 4. Uvolnění cesty
Je-li $v_0 \dots v_k$ nejkratší cesta z $s = v_0$ do v_k, potom po uvolnění hran v pořadí $(v_0, v_1), (v_1, v_2) \dots (v_{k-1}, v_k)$ je $d(v) = \delta(s, v)$

Věta. Pokud Dijkstrův algoritmus provedeme na orientovaném ohodnoceném grafu s nezáporným ohodnocením hran, s počátečním vrcholem s, pak po ukončení algoritmu platí $d(u) = \delta(s, u)$ pro všechny vrcholy $u \in V$
Idea: $d(y) = \delta(s, y)$ pro vrchol vkládaný do D

ad Optimální podstrukt. (Bellmanův princip optimality):
- (platí a) využíva se v hladových alg. a dynamickém progr.
- stačí si pamatovat optimální hodnotu (neoptimální hodnoty a podstruktury se v řešení nevyskytují)
- optimální řešení lze zrekonstruovat (! odzadu; pomocí rovnosti cen)

Pro analýzu složitosti potřebujeme haldy:

Haldy

Datová struktura pro implementaci ADT prioritní fronta (ADT: Abstraktní Datový Typ)
- základní operace pro prioritní frontu:

- Vytvoř() vytvoří prázdnou množinu, tj. reprezentaci
- Přidej(M,x) přidá x do množiny M
- Min(M) vrátí ukazatel na prvek v M s minimálním klíčem
- OdeberMin(M) vrátí ukazatel jako Min(M) a navíc tento prvek odebere z M

- známá implementace: binární halda (v heapsortu)
- reprezentace v poli: vrchol i má syny na adrese $2i$ a $2i + 1$
- reprezentace v binárním stromě: vrchol má menší klíč než (obě) děti

Obrázek.

Další operace pro haldu:

- SníženíKlíče(M,x,k) sníží hodnotu klíče prvku x v M na k
- Vymaž(M,x) odstraní prvek x z M
- Sjednocení($M1$,$M2$) vytvoří novou haldu pro množinu $M1 \cup M2$

- implementace operací (v binární haldě kromě Sjednocení): probubláváním zdola/shora (!při "shora" vyměňuju prvek za *menší* z dětí, používa se pouze v binární haldě (jinak slož. $\omega(\log n)$)

- složitost operací v binární haldě odpovídá hloubce $O(\log n)$ (máme konstantní (tj. shora omezený) počet dětí)
- postupná výroba haldy ("stačí"v heapsortu): $\Theta(n \log n)$, protože přidáváme $n/2$ prvků do hloubky $\Theta(\log n)$
- lépe: "dávková"výroba haldy z n prvků: v $O(n)$. (Odpovídá první fázi heapsortu.) Příklad výhodnosti *líné* implementace datové struktury. Idea: buduju malé haldy zdola.
- (dávkové zrušení haldy v $O(n)$ bez udržování invariantů, resp. přenechám garbage collectoru, např. v min. kostře)
- DC: Dokažte, že celkový počet operací je $O(n)$, teda počet operací na 1 prvek je $O(1)$ (amortizovaná složitost). Počet operací je $\leq \Sigma_{i=1}^{h}\, i \cdot \frac{1}{2^i}$
- DC: udržování vyváženého tvaru (binární) pointrové haldy
- zařadím na správné místo (různé impl.), pak vybublám
- metapozn: Dobrá implementace/optimalizace funguje, i když ji neumíme dokázat (vůbec nebo tesně). (Porovnání vykonaných operací - jsou v jiném pořadí, měření)

(Binomiální stromy, binomiální haldy ...)
- Binomiální stromy: B_0 je jeden vrchol, B_k se skládá ze dvou stromů B_{k-1}, strom s větším kořenem přivěšený pod menší. Číslo k nazýváme řád B_k.
- vlastnosti: B_k má právě 2^k vrcholů, počet synů (šířka) je maximálně $k = \log |B_k|$, hloubka je max. k. Odebráním kořene (tj. OdeberMin) vzniknou binomiální stromy $B_0 ... B_{k-1}$ (v tomto pořadí).
- probubláváme pouze směrem nahoru: SníženíKlíče (DecreaseKey), Vymaž (Delete), čas $O(\log n)$

- Binomiální halda: binomiální stromy v seznamu (nebo poli), každý řád nejvýš jednou - dovoluje lib. počet prvků v haldě
- operace Sjednocení: spojuji stromy stejného řádu v pořadí od nejmenšího, čas $O(\log n)$, lze implementovat líně
- operace Přidej, OdeberMin se převedou na Sjednocení (Fibonacciho halda, idey)
- v DecreaseKey odebírám vrchol (s podstromy) v $O(1)$, protože mám nového kandidáta na minimum, tj. neprobublávám
- z postromu nedovoluju odebrat příliš mnoho vrcholů (vhodným rychlým počítáním), případně snižuju řád, tím zaručuju exponenciální počet vrcholů vzhledem k řádu stromu
- při budování spojuju stromy stejného řádu a zvyšuju řád (jako v binomiálních h.)

- **Dijkstrův alg.: časová složitost:** $n = |V|, m = |E|$

operace:
OdeberMin se vykonává n-krát
SníženíKlíče (v rámci UvolněníHrany) se vykonává m-krát
$\rightarrow T(\text{Dijkstra}) = n.T(\text{OdeberMin}) + m.T(\text{Snížení Klíče})$

	T(OdeberMin)	T(SníženíKlíče)	T(Dijkstra)
pole	$O(n)$	$O(1)$	$O(n^2)$
binární halda (a binomiální)	$O(\log n)$	$O(\log n)$	$O(m.\log n)$
Fibonacciho halda	$O(\log n)$ (amortizovaná)	$O(1)$ (amortizovaná)	$O(n \log n + m)$

Bellman-Fordův algoritmus

Počítá nejkratší cesty z jednoho vrcholu v libovolně ohodnoceném grafu
Vstup: Orientovaný graf $G = (V, E)$
ohodnocení $c : E \to R$
počáteční vrchol $s \in V$

Výstup:
"NE" pokud G obsahuje záporný cyklus dosažitelný z s
"ANO", $d(v)$, $\pi(v)$ pro každé $v \in V$ jinak

Algoritmus:

```
 1 Inicializace(G,s)
 2 for i <- 1 to |V|-1 do  %pevný počet cyklů
 3   forall (u,v) in E do
 4     UvolněníHrany(u,v)
 5   od
 6 od
 7 forall (u,v) in E do  % závěrečná kontrola
 8   if d[v] > d[u] + c(u,v) then return "NE"
 9 od
10 return "ANO" % není záp. cyklus
```

- proč vadí (dosažitelné) záporné cykly, minimální cesta vs. minimální sled
- minimální vs. maximální cesta, pro nejdelší cesty neplatí Bellmanův princip optimality (!při reprezentaci "z u do v" bez mezilehlých vrcholů)
- časová složitost: $O(|V||E|)$

Lemma. Pro graf $G = (V, E)$ s počátečním vrcholem s a cenou $c : E \to R$, ve kterém není záporný cyklus dosažitelný z s, skončí alg. Bellman-Ford tak, že platí $d(v) = \delta(s, v)$ pro všechny vrcholy v dosažitelné z s.

Idea dk: Indukcí podle počtu vnějších cyklů. Po i-tém cyklu jsou minimální cesty délky i správně spočítány.

- pokud je v grafu záporný cyklus, neplatí trojúhelníková nerovnost pro cesty
- impl.: znovuotevírání vrcholů při změně hodnoty, (generický alg. se strategií), expanze pouze otevřených vrcholů

Floyd-Warshallův algoritmus

Řeší verzi 3), nalézt $\delta(u, v)$ pro každé $u, v \in V$
Invariant: $\delta_k(i, j)$ je délka nejkratší cesty z i do j, jejíž všechny vnitřní vrcholy jsou v množině $\{1, 2 \dots k\}$ (pro lib. pevné očíslování vrcholů)

$$\begin{aligned} \delta_k(i,j) &= c(i,j) \quad \text{pro } k = 0 \text{ (pouze přímé hrany)} \\ &= \min\{\delta_{k-1}(i,j), \delta_{k-1}(i,k) + \delta_{k-1}(k,j)\} \text{ pro } k > 0 \end{aligned}$$

- Dokazujeme: 1) na začátku invariant platí, 2) po změně k invariant platí, 3) na konci invariant platí a (!)zahrnuje všechny cesty.

- !Past: k neodpovídá počtu hran budované cesty a indukce nejde podle počtu hran. (Tento "přímočarý"alg. má horší složitost a bude za chvíli)

Vstup:
orientovaný graf $G = (V, E)$
nezáporné ohodnocení hran $c : E \to R_0^+$ (v matici)

Výstup:

matice D, π, kde $D[i,j] = \delta(i,j)$ a $\pi[i,j]$ je předchůdce vrcholu j na nejkratší cestě z i do j

Algoritmus:

```
 1 for i <- 1 to n do
 2   for j <- 1 to n do
 3     pi[i,j] <- NIL
 4     if i=j then D[i,j] <- 0  % "smyčky"
 5       else if not (i,j) in E
 6         then D[i,j] <- infty  % hr. neexistuje
 7         else D[i,j] <- c(i,j) % c. jednohranova
 8              pi[i,j] <- i % posledni vrchol
 9     fi fi
10 od od
11 for k <- 1 to n do % přes mezilehlé v.
12   for i <- 1 to n do   % přes matici
13     for j <- 1 to n do
14       if D[i,k] + D[k,j] < D[i,j] then
15         D[i,j] <- D[i,k] + D[k,j]  % opt.
16         pi[i,j] <- pi[k,j]   % a odp. vrchol
17       fi
18 od od od.
```

- časová složitost: $O(n^3)$, paměťová $O(n^2)$
- implementačně: jedna matice D (místo dvou) pro všechny δ_k; každá hodnota v D má dosvědčující cestu
- adaptace při obecném (tj. i záporném) ohodnocení: dodatečný závěrečný test jako v alg. Bellman-Ford pro detekci záporných cyklů
- záporné cykly se projeví jako záporné číslo na diagonále
- kompaktní reprezentace předchůdců v matici v $O(n^2)$ šetří

paměť (naivně: paměť $O(n^3)$)
- F.-W. alg. je alg. dynamického programování, počítá se iterativně zdola a mezivýsledky se přepisují
- (AG: převod konečného automatu na regulární výraz: pracuje s konečnou reprezentací nekonečně mnoha posloupností (sledů) - nelze postupovat indukcí "podle délky")

Algoritmy „násobení matic“ (pro všechny cesty, v.3)

- postupujeme indukcí podle počtu hran na nejkratší cestě

Definujme d_{ij}^k = minimální cena cesty z i do j s nejvýše k hranami

$d_{ii}^k = 0$

$k = 1$: $d_{ij}^1 = c(i,j)$ pokud hrana (i,j) existuje

$d_{ij}^1 = \infty$ jinak

ind. krok $k-1 \to k$: $d_{ij}^k = \min(d_{ij}^{k-1}, \min_{1\le l\le n}\{d_{il}^{k-1} + c(l,j)\}) = \min_{1\le l\le n}\{d_{il}^{k-1} + c(l,j)\}$ protože $c(j,j) = 0$

Hodnoty d_{ij}^k jsou v matici $D^{(k)}$, hodnoty $c(i,j)$ v matici C (vstupní). Počáteční (nebo koncová :-) podmínka $D^{(1)} = C$.

Potom $D^{(k+1)} = D^{(k)} \otimes C$, kde pro maticové násobení $\otimes$ používáme skalární součin, v němž je:
- násobení nahrazeno sčítáním a
- sčítání nahrazeno minimem

Pokud v G nejsou záporné cykly, potom je každá nejkratší cesta jednoduchá (tj. bez cyklů),
$\to$ každá nejkratší cesta má nejvýše $n-1$ hran
$\to D^{(n-1)} = D^{(n)} = D^{(n+1)} = \ldots = D$

Pomalá verze algoritmu: $n-2$ maticových násobení $\otimes$ matic řádu n

$\rightarrow$ složitost $(n-2).\Theta(n^3) = \Theta(n^4)$

Rychlá verze algoritmu: využijeme asociativitu operace $\otimes$ a počítáme pouze mocniny

$\rightarrow \lceil \log_2(n-2) \rceil$ násobení matic, celková složitost $\Theta(n^3 \log n)$

Pozn: Pro $\otimes$ nelze použít "rychlé"násobení matic (Strassenův alg. v $o(n^3)$)

Algoritmy lze adaptovat na tranzitivní uzávěr grafu.

Pro $G = (V, E)$ je $G^* = (V, E^*)$ *tranzitivní uzávěr* G, kde $E^* = \{(i, j) |$ existuje cesta z i do j v $G\}$.

Konstruovaná matice dosažitelnosti obsahuje boolovské hodnoty (anebo 0/1) a používají se boolovské operace (anebo obvyklý skalární součin).

Impl. triky: počítáme s čísly modulo $n+1$, po fázích převádíme na 0/1, lze použít Strassenův alg.

Algoritmy pro všechny cesty lze získat n-násobným spuštěním algoritmů (pro každý vrchol) pro nejkratší cesty z 1 zdroje (Dijkstra, kritická cesta v DAG)

Extremální cesty v acyklickém grafu

- z jednoho vrcholu do ostatních, verze 2)
- nejkratší cesta v DAG je vždy dobře definovaná, protože i když se vyskytují záporné hrany, neexistují záporné cykly
- Idea: využijeme topologické uspořádání vrcholů

Nejkratší cesta v acyklickém grafu:

Vstup:

acyklický orientovaný graf $G = (V, E)$

$c : E \rightarrow R$ ohodnocení hran

$s \in V$ počáteční vrchol

Výstup
$d(v), \pi(v)$ pro všechna $v \in V$
kde $d(v) = \delta(s, v)$

Algoritmus

1. Topologicky uspořádat vrcholy G
2. Inicializace(G,s)
3. `for` každý vrchol u v pořadí topologického uspořádání
4. `do forall` $v \in$`sousedé[u] do`
5. UvolněníHrany(u,v)
6. `od od`.

- Časová složitost: $\Theta(|V| + |E|)$, protože:
- topologické uspořádání: $\Theta(|V| + |E|)$
- zpracování $|V|$ vrcholů, v cyklu: každý jednou v $O(1)$
- zpracování $|E|$ hran ve vnitřním cyklu: každá jednou, při zpracování poč. vrcholu hrany; vlastní zpracování hrany v $O(1)$ při reprezentaci v poli

- vztah k dynamickému programování: na hledání nejkratší (obecně nejoptimálnější) cesty se lze v případě DAGu dívat jako na algoritmus dynamického programování: pokud mám optimální cesty pro všechny předchůdce, dokážu určit optimální cestu do aktuálního vrcholu. Graf může být zadán implicitně a lze použít obecné optimalizace a varianty algoritmů pro dynamické programování (rekurze s tabelací, převod rekurze na iteraci, průběžné zahazování mezivýsledků).

- v informatice: DAG může sloužit pro popis řídící struktury acyklických výpočtů (např. v dynamickém programování, při transformaci dat, ...) nebo závislostní struktury (tj. návazností) dat (např. podle času, příčinná souvislost)

Aplikace: PERT - Kritická cesta

Problém: Je dána množina *úloh* a délka každé z nich. Některé

dvojice úloh mohou na sobě záviset, tzn. jedna úloha musí skončit dřív, než druhá začne. Cílem je zjistit nejkratší čas, ve kterém mohou všechny úlohy skončit.

- reprezentace: Hrany grafu odpovídají úlohám, ohodnocení hran odpovídá času trvání (vykonávání) úlohy. Pokud hrana (u, v) vstupuje do vrcholu v a hrana (v, x) vystupuje z v, musí být úloha (u, v) ukončena před vykonáváním úlohy (v, x). Graf je DAG.

- cesta reprezentuje úlohy, které se musí vykonat v určitém pořadí.

- *Kritická cesta* je nejdelší cesta v grafu. Odpovídá nejdelšímu času pro vykonávání uspořádané posloupnosti úloh. Cena kritické cesty je dolní odhad pro celkový čas dokončení všech úloh.

Algoritmus nalezení kritické cesty, dvě možnosti.

1. opačné ceny hran a hledání nejkratší cesty
2. hledání *nejdelší* cesty v DAG (změna "∞"na "$-\infty$"v inicializaci a "$<$"na "$>$"v UvolněníHrany)

- proč je hledání nejdelší cesty *v DAG* možné efektivně?: platí princip optimality: libovolná část nejdelší cesty je opět nejdelší mezi příslušnými vrcholy.

- impl: hrany s nulovou cenou pro závislosti (obrázek)

- DC: přirozenější reprezentace: úlohy jsou vrcholy s ohodnocením, hrany odpovídají závislostem: hrana (u, v) znamená, že činnost ve vrcholu u se vykonává před činností v.

- pozn: Činnosti na (nějaké) kritické cestě musí být vykonány včas, jejich zpoždění se projeví celkovým zpožděním

konce. Činnosti mimo kritickou cestu mají rezervu, resp. čas (nejdřívějšího) možného začátku a (nejpozdějšího) nutného konce. Rezerva je rozdíl těchto časů zmenšený o trvání činnosti. Tyto časy lze spočítat pomocí průchodu DAG zepředu, resp. zezadu grafu (pro víc počátečních, resp. koncových vrcholů)

Aplikace: Viterbiho dekódování, zjednodušeno

Hledání cesty v DAG (ze Z do S), která nejpravděpodobněji vygeneruje danou posloupnost písmen P (nad abecedou Σ). Pro zjednodušení, graf je vrstvený, tj. vrcholy lze přiřadit do vrstev a hrany vedou pouze mezi sousedními vrstvami. Hrany jsou ohodnoceny pravděpodobností přechodu mezi vrcholy, vrcholy (kromě Z a S) mají pravděpodobnosti vypsání pro jednotlivá písmena ze Σ. V jednom vrcholu se vypisuje jedno písmeno a pak se pokračuje hranou dál. Pro zjednodušení, pravděpodobnosti jsou nenulové a indukované grafy mezi vrstvami úplné (a teda cesta vždy existuje).

Cílem (algoritmu) je najít takovou cestu ze Z do S, při které se vypíše P s největší možnou pravděpodobností.

(Varianty a zobecnění, aplikace, počítání s log a podtečení, notace argmax ...)

Aplikace Viterbiho dekódování: Převod řeči na text, strojový překlad, hledání podobných genů, ... (Hledání nejpravděpodobnější posloupnosti (skrytých) událostí, která způsobí určitou posloupnost pozorování ve známém (tj. natrénovaném) HMM – Hidden Markov Model)

Minimální kostra grafu

- Vstup: souvislý graf $G = (V, E)$ s hranovým ohodnocením $w : E \to R$

- kostra: podgraf T splňující $V(T) = V$, který je stromem

- minimální kostra: minimalizuje $w(T) = \Sigma_{e \in E(T)}\, w(e)$ mezi všemi kostrami

- první alg.: Otakar Borůvka 1926 (pro různé ceny hran)

Algoritmus: Kruskal 1956

1. uspořádej hrany z E tak, aby $w(e_1) \leq w(e_2) \leq \ldots \leq w(e_m)$
2. $E(T) \leftarrow \emptyset; i \leftarrow 1$
3. `while` $E(T) < |V| - 1$ `do`
4. `if` $E(T) \cup \{e_i\}$ neobsahuje kružnici
5. `then` přidej e_i do $E(T)$ `fi`
6. `i++`
7. `od`

- časová složitost: $(n = |V|, m = |E|)$

- třídění hran v $\Theta(m \log m)$ $(= \Theta(m \log n))$

- zpracování hrany při vhodné reprezentaci $O(\log m)$, pomocí Union-Find struktury, která reprezentuje faktorovou množinu komponent

Datová struktura Union-Find: Ke každé komponentě si pamatujeme reprezentanta (vrchol) – pro všechny vrcholy komponenty vracíme ten samý

implementace, dvě možnosti:

1. v poli velikosti $|V|$: každý vrchol ukazuje přímo na reprezentanta.

Najdi(u) v $O(1)$, $O(m)$-krát
Sjednocení(u,v) v $O(n)$, $O(n)$-krát
celkem: $O(n^2)$

2. pomocí pointrů (v pointrové struktuře nebo poli): Reprezentanti jsou kořeny stromů, pointer vede směrem ke kořeni.
Operace: Sjednocení(u,v): při přidávaní hrany spojujeme komponenty, vykonává se $n-1$-krát, změna d.s. v $O(1)$
implementace:

```
r_u <- najdi(u)
r_v <- najdi(v)
reprezentant(r_u ) <- r_v    (1)
```

operace Najdi(u): projde vrcholy od u nahoru
- při testování hrany zjišťujeme, zda reprezentanti koncových vrcholů hrany jsou stejní (pokud ano, konce jsou ve stejné komponentě a hrana by tvořila cyklus)
- počet volání: 2× pro každou testovanou hranu, tj. $O(m)$
- složitost operace: rovna hloubce stromu reprezentantů
- pokud v (1) připojujeme menší komponentu k větší, dostaneme hloubku $O(\log k)$, kde k ($\leq n$) je velikost kompomenty; široký strom nevadí

$\rightarrow$ celková složitost $O(m \log n)$

- (impl. trik: Nepamatujeme si konkrétní velikost komponent, ale pouze rank r: odpovídá (původní největší) hloubce stromu a zaručuje aspoň 2^r vrcholů, rank zvýšíme o 1, pokud spojujeme komponenty stejného ranku, jinak menší přivěsíme k větší. !Pořadí spojování si nevybíráme, ale směr pointru lze zvolit.)

- (impl: Zkracování cest (při Najdi, několik variant). Vede na "skoro lineární"algoritmus $\Theta(m \cdot f(n))$, kde $f(n)$ je velmi pomalu rostoucí funkce.)

Korektnost. Idea vybírání hran: Postupně přidáváme hrany do množiny $E(T)$ tak, že $E(T)$ je v každém okamžiku podmnožinou nějaké minimální kostry.

Df: Rozklad množiny vrcholů na dvě části $(S, V \setminus S)$ se nazývá řez. Hrana $(u, v) \in E$ *kříží* řez $(S, V \setminus S)$, pokud $|\{u, v\} \cap S| = 1$. Řez respektuje množinu hran A, pokud žádná hrana z A nekříží daný řez. Hrana křížící řez se nazývá *lehká hrana* (pro daný řez), pokud její váha je nejmenší ze všech hran křížících řez.

Df: Nech je množina hran A podmnožinou nějaké minimální kostry . Hrana $e \in E$ se nazývá *bezpečná* pro A, pokud také $A \cup \{e\}$ je podmnožinou nějaké minimální kostry.

Věta: Nech $G = (V, E)$ je souvislý neorientovaný graf s váhovou funkcí $w : E \to R$, nech $A \subseteq E$ je podmnožinou nějaké minimální kostry a nech $(S, V \setminus S)$ je libovolný řez, který respektuje A. Potom pokud je hrana $(u, v) \in E$ lehká pro řez $(S, V \setminus S)$, tak je bezpečná pro A.

Dk: Nech T je min. kostra, která obsahuje A a neobsahuje lehkou (u, v). Zkonstruujme min. kostru T', která obsahuje $A \cup \{(u, v)\}$.

Hrana (u, v) v T uzavírá cyklus. Vrcholy u a v jsou v opačných stranách řezu $(S, V \setminus S)$, proto aspoň jedna hrana v T kříží řez, označme ji (x, y). Platí $(x, y) \notin A$, protože řez respektuje A. Odstranění (x, y) z T kostru rozdělí na

dvě komponenty a přidání (u, v) ji opět spojí a vytvoří $T' = T \setminus \{(x, y)\} \cup \{(u, v)\}$.

Protože (u, v) je lehká pro $(S, V \setminus S)$ a (x, y) kříží tento řez, platí $w(u, v) \leq w(x, y)$, proto $w(T') = w(T) - w(x, y) + w(u, v) \leq w(T)$, odkud T' je min. kostra. Protože $A \cup \{(u, v)\} \subseteq T'$, je (u, v) bezpečná pro A.

Důsl: Nech $G = (V, E)$ je souvislý orientovaný graf s váhovou funkcí $w : E \to R$, nech $A \subseteq E$ je podmnožinou nějaké minimální kostry a nech C je souvislá komponenta (strom) podgrafu zadaného množinou A. Pokud je $(u, v) \in E$ hrana s minimální váhou spojující C s jinými komponentami grafu G_A zadaného množinou A, potom (u, v) je bezpečná pro A.

Dk: Řez $(C, V \setminus C)$ respektuje A a (u, v) je lehká hrana pro tento řez.

- pokud jsou ceny hran různé, je jedna minimální kostra.

Algoritmus: Jarník 1930, Prim 1959

```
 1 Q <- V(G)
 2 forall u in Q
 3   do key[u] <- infty
 4 key[r] <- 0
 5 pi[r] <- NIL
 6 while Q <> 0
 7   do u <- OdeberMin(Q)
 8     forall v in sousede(u)
 9       do if v in Q & w(u,v)<key[v]
10            then pi[v] <- u
```

```
11                  key[v] <- w(u,v) // (A)
12            fi
13    od  od.
```

- časová složitost: $n = |V|$, $m = |E|$
$O(m \log n)$ pro binární haldu
postavení haldy $O(n)$, nebo postupně v $O(n \log n)$
OdeberMin $n.O(\log n)$
SníženíKlíče (A) $m.O(\log n)$
zlepšení: Fibonacciho haldy
SníženíKlíče (A) $m.O(1)$ amortizovane
celkem: $O(m + n \log n)$
reprezentace v poli: $\Theta(n^2)$
OdeberMin $n.\Theta(n)$
SníženíKlíče (A) $m.O(1)$

- Hledání minimální kostry je příklad hladového algoritmu.
- hladový alg.: lokálně optimální rozhodnutí (zde volba bezpečné hrany) vede ke globálnímu optimu
- obecnější metoda než hladový alg. je dynamické programování (platí v něm princip optimality: optimální řešení se skládá pouze z optimálních podřešení)
- tato vlastnost neplatí pro problémy obecně, speciálně NP-těžké problémy (v ADS2): řešení prohledáváním všech možností, typicky backtrakingem
- (řešení pomocí backtrackingu, pro srovnání: najdeme (rekurzivně) optimální řešení se zvolenou hranou a bez ní a z těchto dvou řešení vybereme lepší)
- jiné příklady hlad. alg.: stavba stromu pro Huffmanovo

kódování, rozvrhnutí max. počtu úloh na 1 stroj, problém batohu při dělitelných předmětech ...
- v problému nejdelší cesty (nebo batohu, tj. součtu podmnožiny) lze použít dynamické programování, ale na exponenciálně (tj. nepolynomiálně) větším prostoru stavů
- teorie pro hladové algoritmy: (vážené) matroidy

Metoda Rozděl a panuj (Divide et impera)

- metoda pro návrh (rekurzivních) algoritmů

- Malé (nedělitelné) zadání vyřešíme přímo, jinak
- Úlohu rozdělíme na několik podúloh stejného typu, ale menšího rozsahu (*)
- Vyřešíme podúlohy, rekuzivně
- Sloučíme získaná řešení na řešení původní úlohy

příklady:
- mergesort, binární vyhledávání v utříděném poli
- (*) někdy je potřeba původní úlohu zobecnit: hledání mediánu na hledání k-tého z n prvků (cv.)

Analýza složitosti

$T(n)$ Čas zpracování úlohy velikosti n, pro $n < c$ předpokládáme $T(n) = \Theta(1)$

$D(n)$ čas na rozdělení úlohy velikosti n na a podúloh (stejné) velikosti n/c plus čas na sloučení řešení podúloh

$\rightarrow$ rekurentní rovnice

$T(n) = a.T(n/c) + D(n) \quad pro\ n \geq c$

$T(n) = \Theta(1) \quad pro\ n < c$

příklad: mergesort

```
procedure ms(a[1..n]) % mergesort
(a1[1..n/2],a2[1..n/2]):=rozdel(a[1..n]);
return(merge(ms(a1[1..n/2]),
             ms(a2[1..n/2]) )).
```

- rekurze: dvě ($a = 2$) podúlohy poloviční ($c = 2$) velikosti
- dělení: sudá-lichá $\rightarrow O(n)$, první/druhá polovina (v poli) $\rightarrow O(1)$
- sloučení (merge): $O(n)$, celkem $D(n) = O(n)$, tj. $d = 1$

Vychází rovnice: $T(n) = 2.T(n/2) + O(n)$

Pozn.: "Malé" podproblémy řešíme algoritmem s malou réžií (např. v Quicksortu zatřiďováním). Tato změna neovlivní asymptotickou časovou složitost.

Metody řešení

1. substituční metoda
2. Master Theorem (pomocí "kuchařky")

Master Theorem taky ukazuje, která část řešení je "kritická"

Používáme zjednodušení

- předpoklad $T(n) = \Theta(1)$ pro malá n nepíšeme do rovnice
- zanedbáváme celočíselnost, píšeme pouze $n/2$ místo $\lfloor n/2 \rfloor$ a $\lceil n/2 \rceil$
- řešení nás zajímají pouze asymptoticky $\rightarrow$ používáme asymptotickou notaci už v zápisu rekurentní rovnice

Substituční metoda

- uhádneme asymptoticky správné řešení

- dokážeme, typicky indukcí, správnost odhadu (zvlášť pro dolní a horní odhad)

- - !častá chyba: odhady v indukci musí vyjít se stejnou asymptotickou konstantou jako v ind. předpokladu :-) , nestačí asymptotický odhad s jinou konstantou. (Tak lze chybně indukcí "dokázat" $n^2 \in O(n)$ s využitím $(n+1)^2 = n^2+2n+1$.)

- příklad: mergesort

Pro $T(n) = 2.T(n/2)+b.n$ uhádneme $T(n) = \Theta(n \log n)$. Pro zjednodušení předpokládejme, že funkce $T(n)$ je neklesající.

Dokážeme indukcí horní odhad $T(n) = O(n \log n)$ (pro $n > n_0$). Chceme teda pro vhodnou konstantu c ukázat, že $T(n) \leq cn \log n$, volme $c \geq b$ a tak, aby platili okrajové podmínky pro indukci (tj. $T(n) \leq cn \log n$ pro $n_0/2 \leq n \leq n_0$). Předpokládejme, že tvrzení platí pro $k = n/2$. Potom platí

$T(n) = 2T(n/2) + bn$ (rekurzivní vztah)
$\leq 2c(n/2)\log(n/2) + bn$ (substituce)
$= cn(\log n - \log 2) + bn$ (krácení 2, log)
$= cn(\log n - 1) + bn$ (log)
$= cn \log n - cn + bn$ (distributivita)
$\leq cn \log n$ (volba c), QED

Dolní odhad analogicky.

Ve výše uvedeném příkladě byla náročnost "rekurze" a "režie" vyrovnan

Pro režii $O(n^\alpha)$ je vhodný odhad $O(n^\alpha \log n)$.

- příklad: rychlé násobení dlouhých čísel

Pro $T(n) = 3.T(n/2) + b.n$ uhádneme $T(n) = O(n^{\log_2 3})$. Pro zjednodušení předpokládejme, že funkce $T(n)$ je neklesající.

Dokážeme indukcí horní odhad $T(n) = O(n^{\log_2 3})$ (pro $n > n_0$). Chceme teda pro vhodné konstanty c, d ukázat, že $T(n) \leq cn^{\log_2 3} - dn$ (trik volby), volme $c \geq d$ a tak, aby platili okrajové podmínky pro indukci (tj. $T(n) \leq cn^{\log_2 3} - dn$ pro $n_0/2 \leq n \leq n_0$). Předpokládejme, že tvrzení platí pro $k = n/2$. Hledáme vhodné d a c v závislosti na b (místo uhádnutí v minulém příkladě). Platí

$T(n) = 3T(n/2) + bn$ (rekurzivní vztah)
$\leq 3c(n/2)^{\log_2 3} - 3d(n/2) + bn$ (substituce, ind. předp.)
$= 3cn^{\log_2 3}.(1/2)^{\log_2 3} - (3/2)dn + bn$ (aritmetika)
$= cn^{\log_2 3} + n(-(3/2)d + b)$ (log, vykrácení, upr.)
$? \leq ? cn^{\log_2 3} - dn$ zbývá dokázat

Stačí ukázat $-(3/2)d + b \leq -d$, protože n je kladné.

$-(3/2)d + b \leq -d$ hypotéza
$b \leq -d + (3/2)d = 1/2d$ převedení d, úprava
$2b \leq d$ osamostatnění d
(úpravy byly ekvivalentní, vyjádření d směrem dolu, důkaz (pro zvolené d) směrem nahoru)

Pro tuto volbu $d \geq 2b$ (a následně volbu c) platí poslední nerovnost výše, QED.

Triková volba $cn^\alpha - dn$ umožní dokázat tesnější odhad ($T(n) \in O(n^{\log_2 3})$ místo $T(n) \in O(n^{\log_2 3 + \epsilon})$), protože první člen vyjde z rekurze přesně a druhý člen je rezerva, do kterého

se "schová"režie.

V tomto případě rekurze (tj. # koncových případů) je dominantní, proto vhodná volba odhadu je $T(n) \in O(n^\alpha)$.

Třetí případ je, pokud je dominantní režie. Potom je odhad celkové složitosti roven složitosti režie.

př: hledání mediánu: $T(n) = T(n/5)+T(7n/10)+O(n) \rightarrow T(n) = O(n)$ substituční metodou

Pro $T(n) = T(n/5)+T(7n/10)+O(n)$ uhádneme $T(n) = \Theta(n)$. Pro zjednodušení předpokládejme, že funkce $T(n)$ je neklesající.

Dokážeme indukcí horní odhad $T(n) = O(n)$ (pro $n > n_0$). Chceme teda pro vhodnou konstantu c ukázat, že $T(n) \leq cn$. Zvolíme $c \geq c'$, kde c' je vhodná konstanta, pro kterou platí okrajové podmínky pro indukci (tj. $T(n) \leq cn$ pro $n \leq n_0$). Předpokládejme, že tvrzení platí pro $k < n$. Hledáme vhodné c v závislosti na b. Platí

$T(n) = T(n/5) + T(7n/10) + bn$ (rekurzivní vztah)
$\leq c(n/5) + c(7n/10) + bn$ (substituce, ind. předp.)
$= (9/10)cn + bn$ (aritmetika)
$? \leq ? cn$ zbývá dokázat

Stačí ukázat $9/10c + b \leq c$, protože n je kladné.

$9/10c + b \leq c$ hypotéza
$b \leq c - 9/10c = 1/10c$ převedení c, úprava
$10b \leq c$ osamostatnění c
(úpravy byly ekvivalentní, vyjádření c směrem dolu, důkaz (pro zvolené c) směrem nahoru)

Pro volbu $c \geq \max(10b, c')$ platí poslední nerovnost v

hlavním důkazu výše, QED.

(Hledání k-tého prvku a mediánu)

Master theorem

Nech $a \geq 1, c > 1, d \geq 0$ jsou reálna čísla a nech $T : N \to N$ je neklesající funkce taková, že pro všechna n ve tvaru c^k, pro $k \in N$, platí

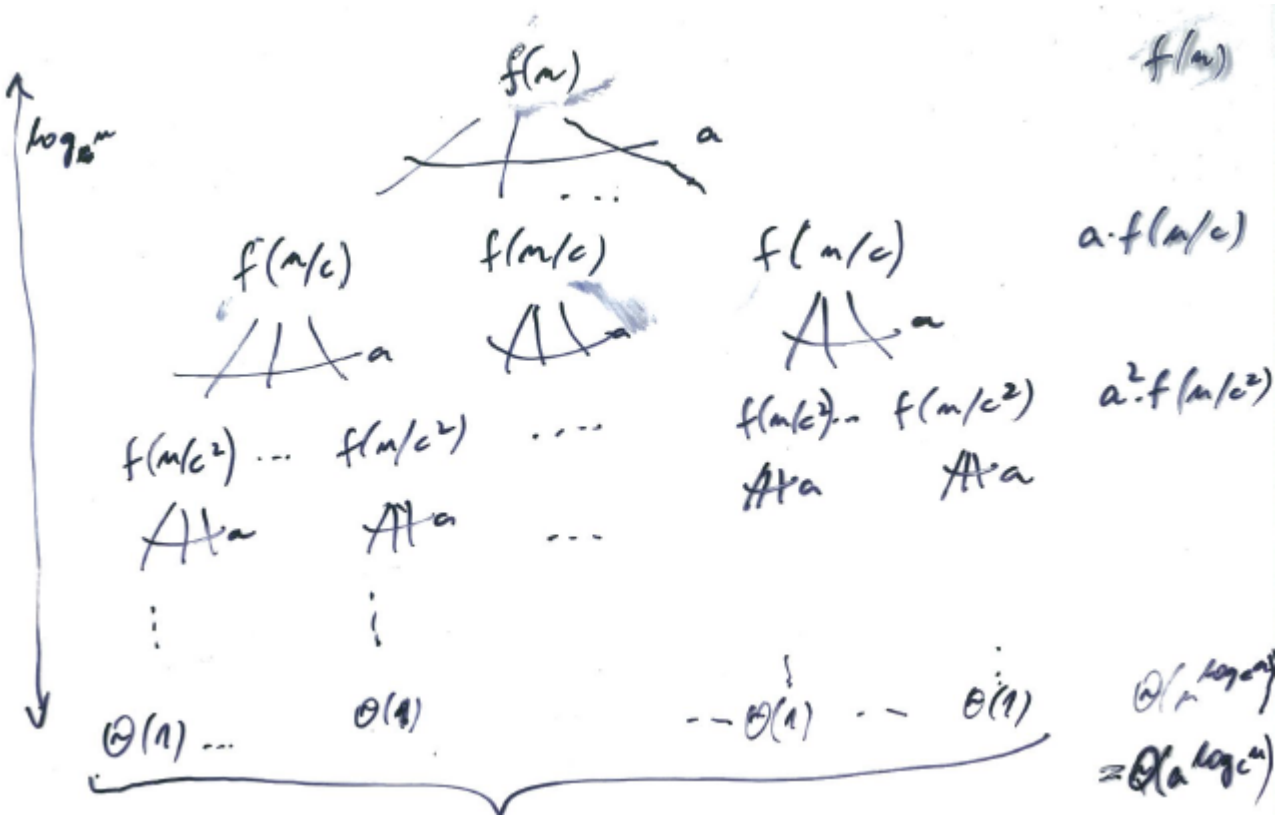
$T(n) = a.T(n/c) + F(n)$

kde pro funkci $F : N \to N$ platí $F(n) = O(n^d)$. Označme $x = \log_c a$. Potom

a) je-li $a < c^d$, tj. $x < d$, potom $T(n) = O(n^d)$

b) je-li $a = c^d$, tj. $x = d$, potom $T(n) = O(n^d \log_c n) = O(n^x \log_c n)$

c) je-li $a > c^d$, tj. $x > d$, potom $T(n) = O(n^x)$



Obrázek 21: Rekurzivní rozdělování

Dk. Protože $F(n) = O(n^d)$, existují n_0 a e taková, že pro každé $n \geq n_0$ platí $F(n) \leq e \cdot n^d$. Zvolme m, tž. $c^m \geq n_0$,

pak pro každé $k \geq m$ platí $F(c^k) \leq e \cdot (c^k)^d$ (tj. platí už bez výjimek).

Zvolme $b = \max\{T(c^m), e \cdot (c^m)^d\}$,

potom pro $k \geq 0$ a $n = c^{m+k} = c^m \cdot c^k$ platí

$$T(n) \leq a \cdot T(n/c) + b \cdot (c^k)^d$$

Indukcí dle k ukážeme, že pro $n = c^{m+k}$ platí

$$T(n) \leq b \cdot \left(a^k + c^{kd} \sum_{i=0}^{k-1} (a/c^d)^i\right)$$

Pro $k = 0$ tvrzení platí.

Předpokládejme, že tvrzení platí pro k, dokažme pro $n = c^{m+k+1}$.

$T(n) \leq a \cdot T(c^{m+k}) + b \cdot (c^{k+1})^d$ z rozpisu

$\leq ab\left(a^k + c^{kd}\, \Sigma_{i=0}^{k-1}(a/c^d)^i\right) + b \cdot (c^{k+1})^d$ subst. z i.p.

$= b\left(a^{k+1} + (c^{k+1})^d)((a/c^d)\, \Sigma_{i=0}^{k-1}(a/c^d)^i\right) + 1)$

$= b\left(a^{k+1} + (c^{k+1})^d)(\Sigma_{i=0}^{k}(a/c^d)^i)\right)$, tím je ind. krok dokončen.

Označme s_k součet prvních k členů geometrické posloupnosti $\{(a/c^d)^i, i = 0, 1, \ldots\}$, t.j.

$$s_k = \frac{(a/c^d)^k - 1}{a/c^d - 1}$$

Rozbor případů:

a) $a < c^d$: geometrická řada s kvocientem a/c^d konverguje a pro libovolné k platí $s_k < s = \frac{c^d}{c^d - a} = konst.$

Odtud (po úpravách) $T(n) \leq T(c^{m+k}) \leq b \cdot (a^k + c^{kd} s_k) < b \cdot (c^{dk} + c^{kd} s_k) \leq konst \cdot c^{kd} = O(n^d)$

Neformálně: Dominující člen je "režie" na jednotlivých úrovních rekurze.

b) $a = c^d$: platí $s_k = k$, protože členy řady jsou rovny 1.

Odtud $T(n) \leq konst \cdot c^{kd} \cdot k = O(n^d \log n)$, protože $k = \Theta(\log n)$

c) $a > c^d$: platí $s_k < \frac{(\frac{a}{c^d})^k}{\frac{a}{c^d}-1} = (\frac{a}{c^d})^k \cdot t$ (Idea: od největšího členu směrem "dolů" je to geometrická řada s kvocientem menším než 1.)

Odtud $T(n) \leq T(c^{m+k}) \leq b \cdot (a^k + c^{kd}(\frac{a}{c^d})^k \cdot t) = b \cdot (a^k + a^k \cdot t) = konst \cdot a^k = konst \cdot c^{(k \cdot \log_c a)} = O(n^{\log_c a})$

Neformálně: Dominující člen je počet (a složitost) koncových případů rekurze.

Příklady

mergesort: $T(n) = 2.T(n/2) + O(n) \rightarrow T(n) = O(n \log n)$

binární vyhl. v utříděném poli: $T(n) = 1.T(n/2) + O(1) \rightarrow T(n) = O(\log n)$

násobení čísel - klasické: $T(n) = 4.T(n/2) + O(n) \rightarrow T(n) = O(n^2)$

násobení čísel - rychlé: $T(n) = 3.T(n/2) + O(n) \rightarrow T(n) = O(n^{\log 3})$

násobení matic - klasické: $T(n) = 8.T(n/2) + O(n^2) \rightarrow T(n) = O(n^3)$

hledání mediánu (k-tého prvku): $T(n) = T(n/5)+T(7n/10)+O(n) \rightarrow T(n) = O(n)$ substituční metodou

kreslení fraktální křivky: $T(n) = 4.T(n/3) + O(1) \rightarrow T(n) = O(n^{\log_3 4})$ (Místo prostřední třetiny úsečky ostatní dvě strany rovnostranného trojúhelníku.)

Násobení čtvercových matic

Úloha: pro dané dvě matice A, B řádu $n \times n$ spočítat $C = A \otimes B$, řádu $n \times n$.

Klasický algoritmus má složitost $O(n^3)$, počítáme n^2 skalárních součinů délky n.

Předpokládejme, že n je mocnina čísla 2, tj. $\exists k, n = 2^k$. Potom vstupní matice můžeme dělit na 4 matice poloviční řádu (až do matic 1 x 1).

Použijeme "rozděl a panuj"(na 4 podmatice)

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \qquad B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \qquad C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

$C_{11} = (A_{11} \otimes B_{11}) \oplus (A_{12} \otimes B_{21})$
$C_{12} = (A_{11} \otimes B_{12}) \oplus (A_{12} \otimes B_{22})$
$C_{21} = (A_{21} \otimes B_{11}) \oplus (A_{22} \otimes B_{21})$
$C_{22} = (A_{21} \otimes B_{12}) \oplus (A_{22} \otimes B_{22})$

- počet maticových operací na maticích řádu $n/2$: 8 násobení $\otimes$ a 4 sčítání $\oplus$ (a pomocné operace)

- počet sčítání reálných čísel v maticovém sčítání: $4(n/2)^2 = n^2$

Vyšla rovnice: $T(n) = 8T(n/2) + O(n^2)$

Master theorem: $a = 8$, $c = 2$, $\log_c a = 3$, $d = 2$, platí $T(n) = O(n^3)$, tj. asymptoticky stejné jako klasický algoritmus

- ke snížení složitosti je potřeba snížit $a = 8$ a zachovat (nebo mírně zvýšit) $d = 2$.

Strassenův alg. násobení matic (1969)

Používá pouze 7 násobení matic řádu $n/2$

$M_1 = (A_{12} \ominus A_{22}) \otimes (B_{21} \oplus B_{22})$

$M_2 = (A_{11} \oplus A_{22}) \otimes (B_{11} \oplus B_{22})$

$M_3 = (A_{11} \ominus A_{21}) \otimes (B_{11} \oplus B_{12})$

$M_4 = (A_{11} \oplus A_{12}) \otimes B_{22}$

$M_5 = A_{11} \otimes (B_{12} \ominus B_{22})$

$M_6 = A_{22} \otimes (B_{21} \ominus B_{11})$

$M_7 = (A_{21} \oplus A_{22}) \otimes B_{11}$

- spočítáme výsledné submatice

$C_{11} = M_1 \oplus M_2 \ominus M_4 \oplus M_6$

$C_{12} = M_4 \oplus M_5$

$C_{21} = M_6 \oplus M_7$

$C_{22} = M_2 \ominus M_3 \oplus M_5 \ominus M_7$

- počet operací nad maticemi řádu $n/2$: 7 násobení $\otimes$ a celkem 18 sčítání $\oplus$ a odčítání $\ominus$

- složitost: $T(n) = 7T(n/2) + O(n^2)$

- Master theorem: $a = 7$, $c = 2$, $\log_c a = \log_2 7 = x$, $d = 2$, teda $T(n) = O(n^x) \doteq O(n^{2.81})$

- praktické použití: husté matice řádu $n > 45$ větší asymptotická konstanta než u klasického násobení

- pozn.: Strassenův algoritmus používá odčítání, tj. inverzní prvky vzhledem ke sčítání $\rightarrow$ pracuje nad (maticí nad) okruhem (s op. plus a krat). Proto nejde použít pro počítání minimálních cest (s min a plus) ani pro boolovské matice (s operacemi or a and). Ale lze ho použít na (vstupní) $0-1$ matice (místo boolovských) pro výpočet tranzitivního uzávěru

grafu. Číslo 0 reprezentuje false, kladné číslo true a počítáme prvky výsledné matice $c_{ij} = \sum\limits_k (a_{ik} b_{kj})$ místo $c_{ij} = \bigvee\limits_k (a_{ik} \wedge b_{kj})$.

Strassenův alg. v obrázcích (A_{ij} po řádcích, B_{ij} po sloupcích):

$$\begin{array}{cc} & \begin{array}{cccc} B_{11} & B_{21} & B_{12} & B_{22} \end{array} \\ C_{11} = \begin{array}{c} A_{11} \\ A_{12} \\ A_{21} \\ A_{22} \end{array} & \begin{pmatrix} + & . & . & . \\ . & + & . & . \\ . & . & . & . \\ . & . & . & . \end{pmatrix} \end{array}$$

$$C_{12} = \begin{pmatrix} . & . & + & . \\ . & . & . & + \\ . & . & . & . \\ . & . & . & . \end{pmatrix} \quad C_{21} = \begin{pmatrix} . & . & . & . \\ . & . & . & . \\ + & . & . & . \\ . & + & . & . \end{pmatrix} \quad C_{22} = \begin{pmatrix} . & . & . & . \\ . & . & . & . \\ . & . & + & . \\ . & . & . & + \end{pmatrix}$$

Matice M:

$$M_1 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & + & \cdot & + \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & - & \cdot & - \end{pmatrix} \quad M_2 = \begin{pmatrix} + & \cdot & \cdot & + \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ + & \cdot & \cdot & + \end{pmatrix} \quad M_3 = \begin{pmatrix} + & \cdot & + & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ - & \cdot & - & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

$$M_4 = \begin{pmatrix} \cdot & \cdot & \cdot & + \\ \cdot & \cdot & \cdot & + \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad M_5 = \begin{pmatrix} \cdot & \cdot & + & - \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \quad M_6 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ - & + & \cdot & \cdot \end{pmatrix}$$

$$M_7 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ + & \cdot & \cdot & \cdot \\ + & \cdot & \cdot & \cdot \end{pmatrix}$$

Součty v závorkách:

$C_{11} = M_1 \oplus (M_2 \ominus M_4 \oplus M_6)$; $C_{22} = (M_2 \oplus M_5 \ominus M_7) \ominus M_3$:

$$M_2 \ominus M_4 \oplus M_6 = \begin{pmatrix} + & \cdot & \cdot & \pm \\ \cdot & \cdot & \cdot & - \\ \cdot & \cdot & \cdot & \cdot \\ \pm & + & \cdot & + \end{pmatrix} \quad (M_2 \oplus M_5 \ominus M_7) = \begin{pmatrix} + & \cdot & + & \pm \\ \cdot & \cdot & \cdot & \cdot \\ - & \cdot & \cdot & \cdot \\ \pm & \cdot & \cdot & + \end{pmatrix}$$

Násobení dlouhých čísel

Úloha: pro dané dvě přirozené čísla x a y o n bitech spočítat součin $s = x * y$. (Analogicky lze počítat v soustavě s jiným základem než 2)

Klasický algoritmus má složitost $O(n^2)$, násobíme každý bit s každým, resp. sčítáme n čísel dlouhých $O(n)$ bitů.

Předpokládejme, že n je mocnina čísla 2. (Případně doplníme nulami zleva.) Označme $m = n \div 2$.

Násobení s rozdělením na poloviny: x a y jsou dvouciferná čísla v soustavě se základem 2^m.

$x = x_1 * 2^m + x_2$

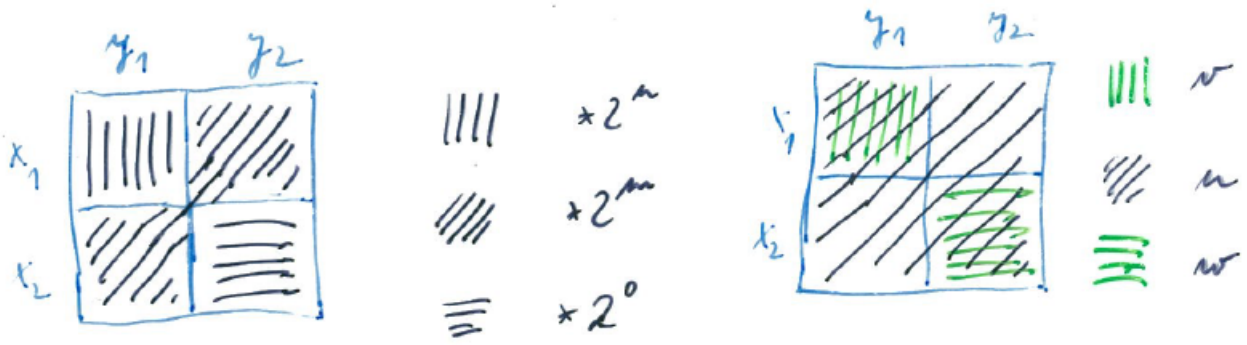
$y = y_1 * 2^m + y_2$

$x * y = x_1 * y_1 * 2^{2m} + (x_1 * y_2 + x_2 * y_1) * 2^m + x_2 * y_2$

- 4 násobení (násobení čísly 2^k jsou shifty), vychází vztah: $T(n) = 4 \cdot T(n/2) + 5n$

odtud: $T(n) = O(n^{\log_2 4}) = O(n^2)$, pro $a = 4, c = 2, d = 1$ (tj. $a > c^d$)

Idea zlepšení (asymptotické složitosti): zmenšit a, tj. ušetřit násobení.



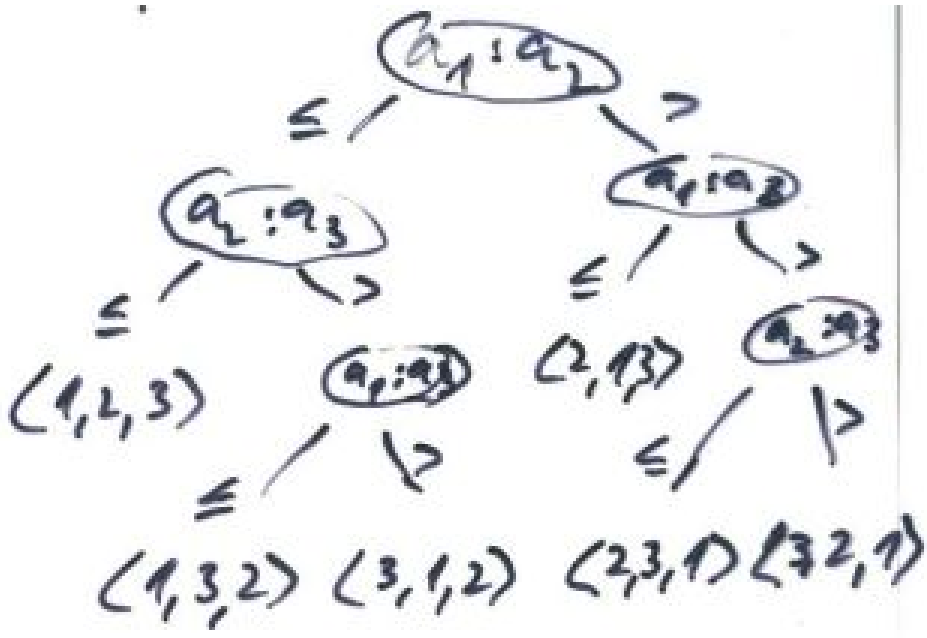
Obrázek 22: Násobení čísel: vlevo klasicky, vpravo lépe

Spočítáme:
$u = (x_1 + x_2) \underline{*} (y_1 + y_2)$
$v = x_1 \underline{*} y_1$
$w = x_2 \underline{*} y_2$
$x * y = v * 2^{2m} + (u - v - w) * 2^m + w$
- 3 násobení: $T(n) = 3 \cdot T(n/2) + O(n)$
odtud: $T(n) = O(n^{\log_2 3}) \doteq O(n^{1.59})$, pro $a = 3, c = 2, d = 1$ (tj. $a > c^d$)

- obecně: Při počítání u mohou být $(x_1 + x_2)$ a $(y_1 + y_2)$ o 1 bit delší než m. To lze ošetřit rozborem případů za cenu dalších (režijních, tj. lineárních) operací. Jiná možnost je využít varianty algoritmu, která počítá $u' = (x_1 - x_2) * (y_1 - y_2)$ a samostatně ošetřuje znaménko u'.

DC: Popište, jak lze vynásobit dvě komplexní čísla pomocí 3 reálných násobení.

Dolní odhad složitosti třídění založeného na porovnávání prvků
- rozhodovací strom: reprezentuje porovnávaní vykonaná při běhu třídícího algoritmu (na vstupu $a_1, a_2, \ldots, a_n$).
- vnitřní uzly jsou označené $a_i : a_j$ a odpovídají testu $a_i \leq a_j$, pro nějaké $1 \leq i, j \leq n$. Vnitřní uzly mají dva podstromy pro dva různé výsledky porovnání. (Hrany označené $\leq$ a $>$)
- listy stromu jsou označené permutací $\langle \pi(1), \pi(2), \ldots, \pi(n) \rangle$, která odpovídá výsledku $a_{\pi(1)} \leq a_{\pi(2)} \leq \ldots \leq a_{\pi(n)}$
- Běh algoritmu odpovídá cestě z kořene do listu. Složitost algoritmu v nejhorším případě je hloubka stromu.



Obrázek 23: Rozhodovací strom (pro třídicí algoritmus)

Pozorování: V listech se musí objevit všech $n!$ permutací, tj. #listů$\geq n!$. Pokud se nějaká permutace neobjeví, jsme schopni na vstup předložit inverzní permutaci a algoritmus ji nedokáže utřídit, tedy *není korektní*.

V: Libovolný rozhodovací strom pro n prvků má výšku $\Omega(n \log n)$.

Dk. Pro strom hloubky h platí $n! \leq 2^h$, protože 2^h je max. počet listů. Odtud zlogaritmováním $\log(n!) \leq h$.

Odhadneme $n!$: $n! \geq n \cdot (n-1) \cdot \ldots \cdot 2 \geq n \cdot (n-1) \cdot \ldots \cdot (\frac{n}{2}) \geq \frac{n}{2}^{\frac{n}{2}}$, odtud $h \geq \log(n!) \geq \log(\frac{n}{2})^{\frac{n}{2}} \geq \frac{n}{2} \log \frac{n}{2} = \frac{1}{2} n(\log n - 1) \in \Omega(n \log n)$

Důsl. Heapsort, Mergesort (a Quicksort v průměrném případě) jsou optimální třídící algoritmy.

Analýza quicksortu

Procedure Quicksort(M)

begin
if $|M| > 1$ then
    pivot := nějaký prvek z M
    $M_1 := \{m | m < pivot\}$
    $M_2 := \{m | m \geq pivot\} \backslash \{pivot\}$
    Quicksort(M_1) – na místě
    Quicksort(M_2) – na místě
end

Analýza složitosti: $T(n)$ je čas zpracování n prvků
T(0) = T(1) = 0
T(n)= 1 +n+T(n-k)+T(k-1), pivot je k-tý

nejlepší případ $k \doteq \frac{n}{2}$
$T(n) = 2 \cdot T(\frac{n}{2}) + O(n) \Rightarrow T(n) = O(n \log n)$

nejhorší případ $k = 1$ nebo $k = n$
$T(n) = 1 + n + T(n-1) \Rightarrow T(n) = O(n^2)$

Potřebujeme předpoklady o pravděpodobnostním rozložení:
na vstupu jsou permutace čísel $1..n$, všechny se stejnou pravděpodobnost
proto: $pivot = k$, pro $\forall k$ se stejnou pravděpodobností
pro vytvořené posloupnosti M_1 a M_2 potřebujeme zaručit
(pro rekurzi), že jsou náhodné permutace: vhodnou volbou
algoritmu

Očekávaná doba výpočtu $ET(n)$:
$ET(0) = ET(1) = 0$
$ET(n) = \Sigma_{k=1}^{n} \frac{1}{n}(n + 1 + ET(k - 1) + ET(n - k))$ pro $n \geq 2$, sloučení sum
$ET(n) = n + 1 + \frac{2}{n} \Sigma_{k=0}^{n-1}(ET(k))$, $(\cdot n)$
$n \cdot ET(n) = n(n + 1) + 2 \Sigma_{k=0}^{n-1}(ET(k))$, (1)
$(n + 1) \cdot ET(n + 1) = (n + 2)(n + 1) + 2 \Sigma_{k=0}^{n}(ET(k))$,
dosadíme n:=n+1 v (1); (2)
Spočteme: (2)-(1):
$(n+1) \cdot ET(n+1) - n \cdot ET(n) = 2(n+1) + 2ET(n))$,
...
$ET(n + 1) = 2 + \frac{(n+2)}{(n+1)} ET(n))$, ...
$ET(n) = \Sigma_{i=2}^{n} 2 \cdot \frac{(n+1)}{(i+1)} = 2(n + 1)(H_{n+1} - 3/2)$
$\leq 2(n + 1) \cdot H_{n+1} \approx 2(n + 1) \cdot \log(n + 1)$
tedy $ET(n) = O(n \log n)$, když použijeme fakt, že n-té harmonické číslo H_i je pro velké n přibližně rovno $\log n$.
$H_n = \Sigma_{i=1}^{n} \frac{1}{i}$

- pivot nemusí být prvek vstupní posloupnosti
- Quicksort jako *schéma* algoritmů podle strategie volby pivota
- pro libovolný pevný způsob výběru pivota existuje (tj. inteligentní nepřítel dokáže zkonstruovat) posloupnost délky n s časem třídění $O(n^2)$

Randomizovaný Quicksort

- randomizovaný: znáhodněný, (pravděpodobnostní)

- problém pevného výběru pivota: určité vstupní posloupnosti se třídí (vždy) v čase $O(n^2)$. Pokud se nevhodné posloupnosti vyskytují na vstupu s větší pravděpodobností, pak očekávaný čas se může blížit $O(n^2)$.

- řešení: volíme pivota náhodně

proto: Pro každou vstupní posloupnost má algoritmus očekávanou složitost $O(n \log n)$. (Počítáme jako průměr časů dosažených při všech volbách dělících bodů.)

Závěr: Pro randomizovaný Quicksort neexistují špatné vstupy, ale pro konkrétní vstup můžeme zvolit špatné pivoty (špatná volba vždy existuje), kdy doba výpočtu je $O(n^2)$. (Randomizovaný Quicksort nevyžaduje rovnoměrné rozdělení vstupů jako deterministický Quicksort.)

Poznámky: (jiný pohled)

Když je pivot vždy vybrán tak, že rozdělí posloupnost v poměru 99 : 1 (nebo lepším)

$T(n) = T(99/100n) + T(n/100) + (n - 1)$

Řešení (subst. metodou): $T(n) = \Theta(n \log n)$

Stejnou složitost dostaneme pro každý konstantní poměr dělení, tj. poměr nezávislý na n (Stačí, když se tento poměr dosáhne aspoň v jedné ze dvou (obecně z pevného počtu k) úrovní.)

Neformálně, pivota mezi 1/4 a 3/4 délky posloupnosti dostaneme s pravděpodobností 1/2. Průměrně se nám taková volba podaří v každé druhé úrovni.

Lineární algoritmy třídění

Radix sort - přihrádkové třídění (původní motivace: třídění děrných štítků)

- třídíme podle jedné cifry (1 sloupce) do p přihrádek ($p = 10$ pro decimální cifry) a skupiny poskládáme za sebe.

- Pozorování: pokud byly přihrádky předem utříděny podle méně významných cifer a použité třídění bylo stabilní, máme utříděnou posloupnost.

pozn: Stabilní třídění zachovává pořadí prvků se stejným klíčem ze vstupu na výstupu.
$\langle a_1, b_1, a_2, c_1, b_2, c_2\rangle \rightsquigarrow \langle a_1, a_2, b_1, b_2, c_1, c_2\rangle$

Alg.: pro d-místná čísla (1. cifra nejnižší, d-tá cifra nejvyšší řád)

```
for i=1 to d do
    utřiď stabilním tříděním podle i-té cifry
```

Složitost: $O(d(n + p))$; d se předpokládá konstantní.

Aplikace: třídění řetězců/slov a strukturovaných klíčů (datum = (rok, měsíc, den)) lexikograficky.

Doplnění/zarovnání:

- Při třídění slov různé délky doplňujeme mezerami zprava
- Při třídění čísel doplňujeme nulami zleva

Counting sort

- omezení: na vstupu I[1..n] čísla v rozsahu 1-k, přirozená.
- pomocná paměť: pole C[1..k]; pole výsledků O[1..n]

Idea alg.:

`for i:=1 to k do C[i]:=0` 0. průchod C: init C

`for i:=1 to n do C[I[i]]++` 1. průchod I: do pole C nasčítáme počet výskytů vstupních čísel z I

`for i:=2 to k do C[i]+=C[i-1]` 2. průchod C: sečtení zdola: C[x] obsahuje počet výskytů menších nebo rovných čísel než x, tj. (konec) umístění výsledků v O

`for i:=n to 1 do O[C[I[i]]]:=I[i]; C[I[i]]--` 3. průchod I, odzadu: uložení vstupního čísla x na C[x]-té místo O, posun pozice dolu

Složitost čas: $O(k+n)$, paměť: $O(k+n)$, předpokládáme $k = O(n)$

Doplňková vlastnost: stabilita třídění, protože ve 3. průchodu jdeme odzadu a indexy `C[x]` po 2.druhém průchodu ukazují na konec úseku s hodnotami `x`.

- pozn.: ve 3. průchodu nestačí vygenerovat příslušný počet indexů `x` do výstupu `O` podle hodnot v `C[x]`, protože nás zajímají i přidružená data v `I`.

DC: Upravte alg. tak, aby 3. průchod byl zepředu (např. streamovaná data z komprese nebo serializace, z mag. pásky `:-)`) a dostali jste stabilní výstup.

LUP dekompozice

Df: Matice je dvourozměrné pole prvků. Matice $A = (a_{ij})$ o rozměrech $m \times n$ má m řádků a n sloupců. Pokud jsou prvky z množiny S, potom množinu matic označujeme $S^{m \times n}$.

příklad matice A: $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

- Transponovaná matice A^T vznikne výměnou sloupců a řádků matice A, tj. matice $A^T = (a_{ji})$.

- Nulová matice má všechny prvky 0. Rozměry matice lze obvykle určit z kontextu.

- Vektory jsou sloupcové matice $n \times 1$. (Řádkové získáme transpozicí.)

- Jednotkový vektor e_i je vektor, který má i-tý prvek 1 a všechny ostatní 0.

- Čtvercová matice $n \times n$ se objevuje často. Speciální prípady čtvercových matic jsou:

- Diagonální matice má $a_{ij} = 0$ pro $i \neq j$.

- Jednotková matice I_n rozměrů $n \times n$ je diagonální matice s jedničkami na uhlopříčce. Sloupce jsou jednotkové vektory e_i. Píšeme I bez indexu, pokud lze rozměry odvodit z kontextu.

- Horní trojuhelníková matice U má $u_{ij} = 0$ pro $i > j$ (hodnoty pod diagonálou jsou 0). Jednotková horní trojúhelníková matice má navíc na diagonále pouze jedničky.

- Dolní trojúhelníková matice L má $l_{ij} = 0$ pro $i < j$ (hodnoty nad diagonálou jsou 0). Jednotková dolní trojúhelníková matice L má navíc na diagonále pouze 1.

- Permutační matice P má právě jednu 1 v každém řádku

a sloupci a 0 jinde. Název permutační pochází z toho, že násobení vektoru x permutační maticí permutuje (přeháže) prvky x.

- Symetrická matice A splňuje $A = A^T$.

- Inverzní matice k $n \times n$ matici A je matice rozměrů $n \times n$, označovaná A^{-1} (pokud existuje), tž. platí $AA^{-1} = I_n = A^{-1}A$. Matice, která nemá inverzní matici, se nazývá singulární (nebo neinvertovatelná), jinak se nazývá nesingulární (nebo invertovatelná). Inverze matice, pokud existuje, je jednoznačná (DC).

Řešení soustav lineárních rovnic, pomocí LUP dekompozice.

Máme soustavu rovnic $Ax = b$, tj. pro $A = (a_{ij})$, $x = (x_j)$ a $b = (b_i)$

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$$
$$\vdots$$
$$a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n$$

Pro dané A a b hledáme řešení x soustavy. Řešení může být i několik (málo určená soustava) nebo žádné (přeurčená soustava).

Pokud je A nesingulární, existuje A^{-1} a $x = A^{-1}b$, protože $x = I_n x = A^{-1}Ax = A^{-1}b$. Řešení x je potom jediné (DC).

Možná metoda řešení: spočítáme A^{-1} a následně x. Ale tento postup je numericky nestabilní, tj. zaokrouhlovací chyby se kumulují při práci s počítačovou *reprezentací* reálných čísel.

(Problémy:
1. Numerická nestabilita. V LUP omezujeme volbou (absolutní hodnotou) velkého pivota s použitím matice P,
2. Špatně podmíněný (ill posed) problém : malá změna vstupních dat (např. zaokrouhlení) způsobí velkou změnu výsledků - "efekt motýlích křídel". (opak je dobře podmíněný, well posed),
3. Testování reálných čísel na 0 (LUP dekompozice: ř. 10). Vlivem zaokrouhlovacích chyb vyjde nenulová hodnota tam, kde měla vyjít 0. Následně: lineárně závislé vektory se stanou lineárně nezávislé, s malou "odchylkou".)

Metoda LUP: pro A najdeme tři matice L, U, P rozměrů $n \times n$, tzv. *LUP dekompozici*, tž. $PA = LU$, kde

- L je jednotková dolní trojúhelníková matice
- U je horní trojúhelníková matice
- P je permutační matice

Soustava $PAx = Pb$ odpovídá přehození rovnic. Použitím dekompozice máme $LUx = Pb$ a řešíme trojúhelníkové soustavy. Označme $y = Ux$. Řešíme $Ly = Pb$ pro neznámý vektor y metodou dopředné substituce a potom pro známé y řešíme $Ux = y$ pro x metodou zpětné substituce. Vektor x je hledané řešení, protože P je invertovatelná a $Ax = P^{-1}LUx = P^{-1}Pb = b$.

Dopředná substituce řeší dolní trojúhelníkovou soustavu v čase $\Theta(n^2)$ pro dané L, P, b.

Označme $c = Pb$ permutaci vektoru b, $c_i = b_{\pi(i)}$. Řešená soustava $Ly = Pb$ je soustava rovnic

$$\begin{aligned}
y_1 &= c_1 \\
l_{21}y_1 + y_2 &= c_2 \\
l_{31}y_1 + l_{32}y_2 + y_3 &= c_3 \\
&\vdots \\
l_{n1}y_1 + l_{n2}y_2 + l_{n3}y_3 + \ldots + y_n &= c_n
\end{aligned}$$

Hodnotu y_1 známe z první rovnice a můžeme ji dosadit do druhé. Dostáváme

$y_2 = c_2 - l_{21}y_1$.

Obecně, dosadíme $y_1, y_2, \ldots, y_{i-1}$ "dopředu"do i-té rovnice a dostaneme y_i:

$y_i = c_i - \sum_{j=1}^{i-1} l_{ij} y_j$

Zpětná substituce je podobná dopředné substituci a řeší horní trojúhelníkovou soustavu v čase $\Theta(n^2)$ pro dané U a y. Soustava má tvar

$$\begin{aligned} u_{11}x_1 + u_{12}x_2 + \ldots + u_{1,n-1}x_{n-1} + u_{1n}x_n &= y_1 \\ u_{22}x_2 + \ldots + u_{2,n-1}x_{n-1} + u_{2n}x_n &= y_2 \\ &\vdots \\ u_{n-1,n-1}x_{n-1} + u_{n-1,n}x_n &= y_{n-1} \\ u_{nn}x_n &= y_n \end{aligned}$$

Řešíme postupně pro $x_n, x_{n-1}, \ldots, x_1$ takto:

$x_n = y_n / u_{nn}$,

$x_{n-1} = (y_{n-1} - u_{n-1,n}x_n)/u_{n-1,n-1}$,

obecně

$x_i = \left(y_i - \sum_{j=i+1}^{n} u_{ij}x_j\right) / u_{ii}$.

Program LUP-solve: přepisem vzorců. Permutační matice P je reprezentována polem $\pi[1..n]$, kde $\pi[i] = j$ znamená, že i-tý řádek P obsahuje 1 v j-tém sloupci.

Složitost LUP-solve: $\Theta(n^2)$ celkem, pro dopřednou i pro zpětnou substituci. V obou případech vnější cyklus probíhá proměnné a vnitřní cyklus počítá sumu, která prochází část řádku.

Výpočet LU dekompozice. Nejprve jednodušší prípad, když matice P chybí (tj. $P = I_n$).

Idea metody: Gaussova eliminace, při které vhodné násobky prvního řádku přičítáme k dalším řádkům tak, abychom odstranili x_1 z dalších rovnic (koeficienty u x_1 v prvním sloupci budou nulové). Potom pokračujeme (rekurzivně) v dalších sloupcích, až vznikne horní trojúhelníková matice, tj. U. Matice L vzniká z koeficientů, kterými jsme násobili řádky.

Z matice A oddělíme první řádek a sloupec, potom matici rozložíme na součin. Matice A' je $(n-1) \times (n-1)$ matice, v sloupcový vektor a w^T řádkový vektor a součin vw^T je také $(n-1) \times (n-1)$ matice.

$$A = \begin{pmatrix} a_{11} & w^T \\ v & A' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v/a_{11} & I_{n-1} \end{pmatrix} \begin{pmatrix} a_{11} & w^T \\ 0 & A' - vw^T/a_{11} \end{pmatrix}$$

Podmatice $A' - vw^T/a_{11}$ rozměrů $(n-1) \times (n-1)$ se nazývá *Schurův komplement* A vzhledem k a_{11}.

Rekurzivně najdeme LU rozklad Schurova komplementu, nech je roven $L'U'$.

S využitím maticových operací odvodíme

$$\begin{aligned} A &= \begin{pmatrix} 1 & 0 \\ v/a_{11} & I_{n-1} \end{pmatrix} \begin{pmatrix} a_{11} & w^T \\ 0 & A' - vw^T/a_{11} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ v/a_{11} & I_{n-1} \end{pmatrix} \begin{pmatrix} a_{11} & w^T \\ 0 & L'U' \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ v/a_{11} & L' \end{pmatrix} \begin{pmatrix} a_{11} & w^T \\ 0 & U' \end{pmatrix} \\ &= LU \end{aligned}$$

Matice L a U jsou jednotková dolní trojúhelníková matice a horní trojúhelníková matice, protože L' a U' jsou požadovaného tvaru.

Program LU dekompozice - přepisem vzorců. (Převádí tail-rekurzivní strukturu na iteraci-cyklus.)

Složitost: $\Theta(n^3)$, protože počítáme n-krát Schurův komplement, který má $\Theta(k^2)$ prvků pro $k = 0..n-1$. Výpočet jedné úrovně rekurze (tj. hlavního cyklu) trvá $\Theta(k^2)$ a celkový čas lze odhadnout $\sum_{k=0}^{n-1} k^2 = \Theta(n^3)$ (DC).

Pokud $a_{11} = 0$, metoda nefunguje, protože se dělí nulou. Prvky, kterými dělíme, nazýváme *pivoty* a jsou na diagonále U. Zavedení matice P nám umožňuje se vyhnout dělení nulou (nebo malými čísly – kvůli zaokrouhlovacím chybám) a vybrat si ve sloupci nenulový prvek. Takový musí existovat, pokud je matice nesingulární.

Implementační poznámky - optimalizace: a) stačí počítat nenulové prvky, b) obě matice můžeme uložit "na místě", pokud ukládáme pouze významné prvky, tj. nenulové a diagonálu U.

Program LUP-dekompozice

```
LUP-dekompozice(A)
 1 n <- rows[A]          % počet řádků
 2 for i <- 1 to n       % P inicializujeme
 3   do pi[i] <- i       %  jako diagonální I_n
 4 for k <- 1 to n-1     % hlavní cyklus
 5   do p <- 0           % nulování pivota
 6      for i <- k to n            % výběr pivota
 7        do if |a[ik]| > p        % test vel. pivota
 8           then p <- |a[ik]|     % bereme maximum
 9                k' <- i          % pozice pivota
10      if p = 0              % test pivota
11        then error "singular matrix" k  % chyba
12      exchange pi[k] <-> pi[k'] % změna P tj. pi[]
13      for i <- 1 to n           % výměna řádků
14        do exchange a[ki] <-> a[k'i]  % matice A
15      for i <- k+1 to n             % přes řádky
16        do a[ik] <- a[ik]/a[kk]  % k-tý sloupec L
17           for j <- k+1 to n     % v řádku i
18             do a[ij]<-a[ij]-a[ik]*a[kj] %změna U
```

Složitost: tři vnořené cykly (18) $\rightarrow \Theta(n^3)$

Počítání inverze pomocí LUP-dekompozice.

Pokud máme LUP rozklad matice A, dokážeme spočítat pro dané b řešení $Ax = b$ v čase $\Theta(n^2)$. LUP rozklad totiž nezávisí na b.

Rovnici $AX = I_n$ můžeme považovat za n různých soustav tvaru $Ax = b$ pro $b = e_i$ a $x = X_i$, kde X_i znamená i-tý sloupec X. Řešení každé soustavy nám dá sloupec matice $X = A^{-1}$.

Složitost: řešíme n soustav rovnic, každou v čase $\Theta(n^2)$. Výpočet LUP dekompozice spotřebuje čas $\Theta(n^3)$, teda celkem inverzi A^{-1} matice A spočítáme v čase $\Theta(n^3)$.

Souvislosti:

Lze ukázat: $T_{inverze}(n) = \Theta(T_{nasobeni}(n))$

Tj. složitost počítání inverze je stejná jako násobení matic.

(Převod maticového násobení na inverzi)

(Redukce inverze na násobení)

...

Pořadí témat 2019, dotace předn.:poř. předn:

- Prostředky pro popis složitosti 0,5:1
- Základní grafové alg. 2:2-3
- Min. cesty 2:4-5
- Min. kostry 1,5: 6-
- Stromové struktury 1,5:7
- Rozděl a panuj 2:8-9
- Třídění 1,5:10+
- Hašování 1:11+
- Lin. Alg. 1:12+
- - Celkem: 13P:...
-
-