Teorie grup: grupoidy, pologrupy, monoidy, grupy. Podgrupy, cyklické grupy a generátory

- množina + operace

$\Rightarrow$ vlastnosti: uzavřenost, asociativita, neutr. prvek, inverze, komutativita

$A+(B+C) = (A+B)+C$ stejný a levý i pravý jedna $A \cdot B = B \cdot A$

$\rightarrow$ libovolná operace

$\rightarrow$ v grupě existuje multiplikativní inverze $\Leftrightarrow$ $bx = c$ má pouze jedno řešení

$\rightarrow$ podgrupa je podmnožina grupy a platí, že stejnou operací je to pořád grupa

N M

$(N,\circ)$ je grupa a $N \subseteq M$, kde $(M,\circ)$ je grupa

$\Rightarrow$ řád grupy = počet prvků grupy, platí, že $a^k = \underbrace{a \circ \dots \circ a}_{k \times}$

$\Rightarrow$ řád podgrupy dělí řád grupy $\Rightarrow$ vezmeme $g_1, g_2 \in G$, provedeme složení s $h \in H$ a $\notin G$, tak dostaneme třídy ekvivalence, díky jednoznačnosti dělení mají všechny tyto třídy rozkladu stejný počet prvků $\Rightarrow k|H| = |G|$

konečný

$\Rightarrow$ nejmenší podgrupu obsahující N, $N \subset M$ nazýváme podgrupu generovanou množinou $N \Leftrightarrow \langle N \rangle$

$\Rightarrow$ grupa je dle cyklická $\Leftrightarrow$ $\exists$ prvek a, který je generátorem ... tedy jedná se o nejmenší grupu, která ji obsahuje $\Leftrightarrow \langle a \rangle = G$

Platí, že: a je gen $\Leftrightarrow$ a^{-1} je gen.

$a^n = \varepsilon$

Počet generátorů v cyklické grupě je $\varphi(n) = n \cdot \prod_i \left(1 - \frac{1}{p_i}\right)$ .. n je řád

Podgrupa cyklické grupy je také cyklická: $G \supseteq H$ ... H je podgrupa

a je gen G $\Longrightarrow$ a^q je nejm. q takové, že $a^q \in H$

$\Rightarrow$ Platí, že $\langle a^q \rangle \subset H$, platí také $H \subset \langle a^q \rangle$?

Najdeme $a^p \in G$ ... $d = \gcd(q,p) = uq + vp \Rightarrow a^d \in G$

$\Rightarrow d \geq q$ a $d \leq q$ $\Rightarrow d = q \Rightarrow q | p$ QED

$\Rightarrow$ Platí malá Fermatova věta

$a^n = \varepsilon$ n je řád a, a je lib. prvek

Grupa Z_p má řád $p-1 = \varphi(n)$

$\Rightarrow a^{p-1} \equiv 1 \mod p \quad | \cdot a$

$a^p \equiv a \mod p$

Cayleyho tabulka: jedna z možností definice zobrazení (TABULKOU)

Abelovská grupa $\Rightarrow$ komutativní grupa $\Leftrightarrow A \cdot B = B \cdot A$

Řád prvku je nejmenší přirozené číslo: $a^n = \underset{\text{neutr. prvek}}{e}$

Když najdeme jeden generátor, máme zároveň všechny.

$\Rightarrow$ řád grupy je n $\Rightarrow g^k$ je generátor $\Leftrightarrow \gcd(k, n) = 1$

<u>Homomorfismus</u>: dvě grupy G a H a zobrazení $\varphi: G \to H$

takové, že pro $g_1, g_2 \in G$ a $h_1, h_2 \in H$: $\varphi(g_1) \overset{\in H}{\circ} \varphi(g_2) = \varphi(g_1 \overset{\in G}{\circ} g_2)$

$\varphi(g_1) = h_1 \quad \varphi(g_2) = h_2$

$\Rightarrow$ zobrazí neutr. prvek na sebe

$\Rightarrow$ jádro jsou všechny prvky (podgrupa), které se zobrazí na e

Izomorfismus = Homomorfismus, který je bijekcí

$\Leftrightarrow$ složení dvou morfismů je zase morfismus?

$\Leftrightarrow$ dvě nekonečné cykl. grupy jsou izomorfní?

$\Rightarrow$ Počet generátorů Z_{23}? $\Rightarrow n = \varphi(23) = 22$

počet generátorů je $\varphi(22) = 22 \cdot (1 - \frac{1}{2})(1 - \frac{1}{11}) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$

Izomorfismus zachovává cykličnost

Počet izomorfismů je počet generátorů $\Rightarrow \varphi(n)$

$\Rightarrow$ např. $Z_8^+ \times Z_{20}^*$

Tělesa a okruhy: Základní definice a vlastnosti. Konečná tělesa. Okruhy polynomů, ireducibilní polynom.

Okruh $(M,+)$ je abel grupa a $(M,\cdot)$ je pologrupa a distributivita $a(b+c) = (b+c)\cdot a$

$\Rightarrow$ řád je počet prvků v $(M,+)$ .. tedy je tam i 0 !

Dělitelé nuly $\Leftrightarrow$ $a \cdot b = 0 \Rightarrow a = \frac{0}{b}$

Obor integrity: komutativní okruh bez dělitelů nuly

Těleso je $(M,+)$ abelovská a $(M,\cdot)$ je grupa a $M \setminus \{0\}$ ... jinde 0 je

Vlastnosti: Triviální těleso je $(\{0,1\},+,\cdot)$

$\forall$ těleso je obor integrity (asi jen pro komut. tělesa)

$\Rightarrow$ součástí jeho mult. grupy ~~prost~~ nesmí být 0

Homomorfismus a izomorfismus fungují stejně... pro jednotlivé grupy

Příklady: Okruh $(\mathbb{Z},+,\cdot)$ není těleso ... v $\{\mathbb{Z} \setminus 0\}$ chybí inverze

$(\mathbb{Q},+,\cdot)$ je těleso

Konečná tělesa: kon. počet prvků : $\mathbb{Z}_p$ $(M,+)$ ... řád je p

$(M,\cdot)$ ... -"- $p-1$ $\Rightarrow$ cyklická

počet generátorů je $\varphi(p-1)$

$\mathbb{Z}_n^\times$ je cyklická pro $n = 2, 4, 2p^k, p^k$ $p \neq 2$

Řád konečného tělesa je vždy p^n

Binární tělesa $GF(p^n)$

: jedná se o polynomy .. K je okruh polynomů a $GF(K)$ se definuje nad ním

polynom je ireducibilní, jestliže $\forall x,y \in K$: $p = xy$ je řád x nebo $y = 0$

$\Rightarrow$ chová se to jako prvočísla

GF .. aditivní grupa ... řád p^n... není cyklická ! ... neutr. je $\overbrace{0 \ldots 0}^{n}$

mult. grupa ... řád $p^n - 1$ .. vždy cyklická ! ... -"- $0 \ldots 01$

Těleso prvočíselného řádu – $GF(p)$

neprvoč. řádu – $GF(p^n)$ $n > 1$ ... zbytek se počítá pomocí zbytku po dělení

Různé algoritmy pro zrychlení inverze a výpočtu – Square And Multiply, EEA

Funkce více proměnných: Základní definice, vlastnosti: Gradient, Hessián, definitnost matic.
Extrémy fcí více proměnných a jejich hledání. Hledání vázaných extrémů. (Rovnostní vazby)

Parciální derivace: $\underbrace{\lim_{k \to \infty} x_k = x_0}_{\text{LIMITA}}$ pokud pak $(\|x_k - x_0\|)_{k=1}^{\infty} = 0$ v normě $\|\cdot\|$

utíkám ve směru $\vec{v}$ od bodu a

Parciální derivace: $\frac{\partial f}{\partial v}(a)$ ve směru v $= \lim_{t \to 0} \frac{f(a + tv) - f(a)}{t}$

Gradient ... parciální derivace ve směrech souřadnicových os $\nabla f = \left(\frac{\partial f}{\partial x_1} \dots \frac{\partial f}{\partial x_n} \right)$

Derivace v bodě → $\frac{\partial f}{\partial v}(a) = v^T \nabla f(a)$ ... v je normalizovaný

Hessián je matice druhé parciální derivace $\nabla^2 f(a) = \begin{pmatrix} \frac{\partial f}{\partial x_1^2} & \cdots & \frac{\partial f}{\partial x_1 \partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f}{\partial x_n x_1} & \cdots & \frac{\partial f}{\partial x_n^2} \end{pmatrix}$ ⇒ rychlost na tak x_1

Jakobián je ~~..~~ rozšíření gradientu na funkci, která zobrazuje do více dimenzí $f: D \to R^m$

Definitnost matic: rozšíření principu pro hledání lokálních extrémů

⇒ lokální max v a ⇔ $\forall x \in H_a$ $f(x) \le f(a)$

-||- min v a ⇔ $\forall x \in H_a$ $f(x) \ge f(a)$

Nutná podmínka lokálního maxima je $\nabla f(a) = 0$ a $\nabla^2(f(a))$ je neg-semidef.
Postačující podmínka -||- negativně definitní ⇒ ∩

Nutná podmínka lokálního minima je $\nabla f(a) = 0$ a $\nabla^2 f(a)$ je pozitivně semidefinitní
Postačující podmínka -||- pozitivně definitní ⇒ ∪

Pozitivně definitní je matice, pokud $\forall x \in \mathbb{R}^n$ $x^T A x > 0$ $x \neq 0$
semidefinitní -||- ≥ 0 a x může být 0

\+ Negativně naopak

Sylvestrovo kritérium: A je pozitivně definitní $\begin{vmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{vmatrix} > 0$ .. kladné subdeterminanty

A je neg. definitní když se subdet. střídají znaménka = - začíná!

$\Leftrightarrow$ Protože platí, že A je pozitivně defi. $\Leftrightarrow$ $-A$ je neg. definitní

Lokální extrémy při omezeních rovností

$\Rightarrow$ bod musí navíc splňovat rovnostní omezení

$\Rightarrow$ zavedeme tzv. Lagrangeovu funkci $L(x,\mu) = \underbrace{f(x)}_{\text{funkce}} + \overbrace{\sum \mu_i g_i(x)}^{\text{omezení}}$

chceme, aby byl její gradient roven 0

$\Rightarrow$ spočteme si $y^T \nabla g_i(a) = 0$ $\Rightarrow$ tj. vektory kolmé na gradienty omezujících rovnic

jak si vezmeme $\nabla^2 L(x,\mu)$

... a testujeme na kolmé vektory, z toho poznáme ty omezení (nebo nepoznáme)

... $y^T \nabla^2 L(x,\mu) y > 0$ ... definitnost

Př.: Najděte lokální maxima a minima fce $f(x,y) = 3x - 4y + 3$ na množině bodů $x^2 + y^2 = 4$

$L(x,y,\mu) = 3x + 4y + \mu(x^2 + y^2 - 4)$

$\nabla L = (3 + 2\mu x,\ 4y + 2\mu y,\ x^2 + y^2 - 4)$

$\nabla L = 0 \Rightarrow$
- $\mu = -\frac{5}{4}$, $x = \frac{6}{5}$, $y = \frac{8}{5}$ a)
- $\mu = \frac{5}{4}$, $x = -\frac{6}{5}$, $y = -\frac{8}{5}$ b)

jen podle přirozené proměnné fa $\Downarrow$

$$\nabla^2 L = \left(\begin{array}{cc|c} 2\mu & 0 & 2x \\ 0 & 4+2\mu & 2y \\ \hline 2x & 2y & 0 \end{array}\right)$$

$\Rightarrow$ Spočteme si vektory kolmé na gradient $y^T \nabla g_i(a) = 0$

$\begin{pmatrix} i \\ j \end{pmatrix} \cdot (2x \ \ 2y) = 0 \Rightarrow xi = -yj$ pro bod

a) $\frac{6}{5} i = -\frac{8}{5} j \Rightarrow i = -\frac{4}{3} j$

b) $-\frac{6}{5} i = +\frac{8}{5} j \Rightarrow i = -\frac{4}{3} j$

$\Rightarrow$ pro a)

$$\Rightarrow \left(-\tfrac{4}{3} j, j\right) \cdot \begin{pmatrix} 2\mu & 0 \\ 0 & 4+2\mu \end{pmatrix} \cdot \begin{pmatrix} -\frac{4}{3} j \\ j \end{pmatrix} = \left[-\tfrac{8}{3} j\mu + 2j(2+\mu)\right] \left(-\tfrac{4}{3} j, j\right) = -\frac{53}{18} j^2 \Rightarrow \underline{\text{neg. definitní}}$$

$\Rightarrow$ maximum

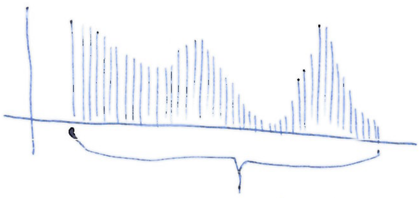
$\Rightarrow$ pro b) to vyjde obráceně $\Rightarrow$ pozitivně definitní $\Rightarrow$ minimum

Integrál funkce více proměnných

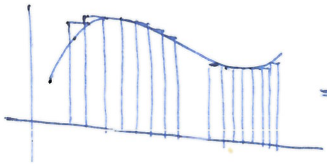
Motivace stejná jako ve 2D, pouze zobecněno!

Máme nějaké ekvidistantní rozdělení intervalu, uděláme součet horní a dolní a pokud se rovnají, pak máme vyhráno.

Platí, že $\int_a^b = -\int_b^a$ $\quad \int_a^a = 0$ $\quad \int_a^b + \int_b^c = \int_a^c$ $\quad \int(a+b) = \int a + \int b$ $\quad c\cdot\int a = \int ca$

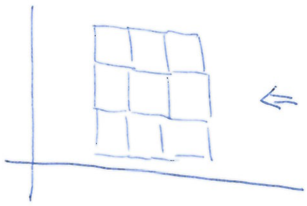


rozdělení intervalu



=> Min x Max rozdělení

Konstrukce na čtverci:



⇐ zezdola => opět stejně, max a min

$R = [a,b]\times[c,d] \subseteq \mathbb{R}^2$ a pokusíme se obdobně úplně analogicky $S(\sigma) = \sum_{\forall x} \sup_{\forall x\in R_i} f(x)\cdot$ plocha R_i

=> lze samozřejmě opět zobecnit na složitější tvary

Další vlastnosti
a) Linearita
b) $\int f'g = fg - \int fg'$
c) $g\circ\phi = \int (f\circ\phi)\cdot\phi'$ .. existuje-li $\int f$, nebo $\int(f\circ\phi)\phi'$
$f: (a,b)$ $\quad \phi:(\alpha,\beta)$ $\quad \phi:(\alpha,\beta)\to(a,b)$
a ϕ je diferenc na (α,β)

=> vlastnosti -> stejně jako pro 2D případ

platí pravidla! Newtonova formule $\int_a^b f = F(b)-F(a)$

a) Per Partes: $\int_a^b f'(x)g(x) = [f(x)g(x)]_a^b - \int_a^b f(x)g'(x)$

b) Substituci $\int_\alpha^\beta f(g(t))g'(t) = \int_{g(\alpha)}^{g(\beta)} f(x)$

PRAM modely a algoritmy

$T_n(n)$ .. časová sl.

$SL(n)$ ... teoret. nejm. složitost, sl. algoritmu

$SV(n)$ .. nejrychl. exist. algoritmus

$T(n,p)$ .. paralelní čas

$S(n,p)$ .. zrychlení $S(n,p) = \cancel{\frac{SV(n)}{T(n,p)}}\ \frac{SV(n)}{T(n,p)}$

$L(n,p)$ .. nejm. možný par. čas $L(n,p) = \frac{SL(n)}{T(n,p)} \leq p$

$C(n,p)$ .. par. cena $C(n,p) = p \cdot T(n,p)$

$C(n,p) \geq SV(n)$

Cenově optimální $C(n,p) = O(SV(n))$

$W(n,p)$ .. práce .. součet práce ve všech procesorech

$SV(n) \leq W(n,p) \leq C(n,p)$

$E(n,p)$ .. efektivita $E(n,p) = \frac{SV(n)}{C(n,p)} = \frac{S(n,p)}{p} = \frac{SV(n)}{\cancel{T(n,p)} \cdot C(n,p) \cdot \cancel{p}}$

RAM – random access machine

- výpočetní model, neomezeně dlouhá páska
- instrukce trvají jednotkový čas (konstanta)
- časová složitost => ~~počet buněk pásky~~ počet provedených instrukcí
- prostorová složitost => počet použitých buněk pásky

PRAM – parallel RAM

- neomezený počet počítačů RAM s vlastní pamětí
- neomezený počet paměťových buněk přístupných v jedn. čase
- $\forall$ procesor zná svůj index P_i a má své registry
- VSTUP: hodnoty v buňkách sdílené paměti
- VÝSTUP: hodnoty v buňkách sdílené paměti
- instrukce jsou prováděny synchronně – READ (R), WRITE (W), LOCAL (L)
- jediný způsob komunikace = READ/WRITE
- P1 má speciální aktivační registr RA ... pro $\forall$ z CPU
- algoritmus končí, až se zastaví P1, (potom ostatní už skončily)
- PRAM mají 2 parametry – p – počet CPU
  – n – počet buněk paměti
- paralelní časová složitost = čas výpočtu na P_1
  - jednotkový model – R, W, L .. trvají čas 1
  - globální model – R, W .. trvají čas d, L .. trvá čas 1

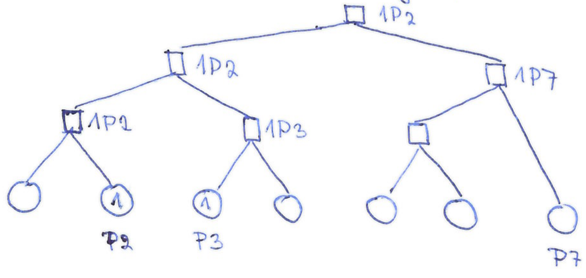
- Význam PRAM - velice silný model, přístup do buněk je konstantní
  - zjednodušený a intuitivní model
  - etalon pro paralelní algoritmy
    => Pokud to nespočítá PRAM, tak to nemá cenu vůbec řešit

- Ošetření konfliktů při přístupech do paměti
  - EREW - exclusive read exclusive write - vůbec není povoleno
  - CREW - exclusive write concurrent read - paralelní čtení
  - CRCW - concurrent read concurrent write - povoleny oba paralelní stavy
    - PRIORITY - pouze CPU s nejv. prioritou
    - RANDOM - náhodné CPU
    - SHODNÝ - algoritmus musí zajistit, aby všechny zapisované hodnoty byly stejné

Výpočetní síla PRAM - výpočetní model A je výp. silnější než B, jestliže pro ∀ algoritmus napsaný pro B, poběží i na A ve stejném paral. čase
- zapisuje se $A \geq B$

Pro CRCW: PRIORITY ≥ ARBITRARY ≥ COMMON ≥ CREW ≥ EREW

Simulace CRCW Priority na EREW => nejsilnější na nejslabším
- CRCW(n,p) na EREW(n·p, p)
- ∀ buňka CRCW je v EREW rozdělena na p buněk
- v těch p buňkách je reprezentován imaginární strom (binární)
- když chce CPU odděleit 10, zapíše svůj index do rodiče
  - nejdříve byl potomek, pak až prvý - ale když už byl zapsal, tak prvý už nezapisuje
  - vždy jeden vítěz - pokud zapisuje => zapíše a stejným způsobem je strom smazán
    - pokud čte => strom opět smazán, ale cestou dolů si ještě předávají čtenou hodnotu
      => všichni vyhrají
      => to trvá vždy $k \cdot \log(p)$



SIMULACE CRCW na EREW (2)

- CRCW priority na EREW $(n+3p, p)$
- ∀ CPU má 3 buňky a ty dohromady tvoří pole
- v ∀ kroku zapíše ∀ CPU do svého pole co ~~chtěj~~ chce číst a co chce zapisovat
  a také zapíše svůj index (nebo zapíše 0)
- pole pak seřadíme v log čase
- sortí se podle paměti čtení/zápisu a až pak podle indexu

=> vedle sebe leží konfliktní IO operace

-> CPU se pak kouká vlevo: CHCI ČÍST/ZÁPIS? NE ×
ANO .. vlevo stejná b ×
ANO .. vlevo jiná b V – VÍTĚZ

: při zápisu musí CPU znát, kdo kam zapisuje V

-> Při čtení čtou i ti, co nevyhráli
– binární distribuce v $\log(n)$ čase

CO ČTU/ZAPISUJU ⇓ VÍTĚZ – 1/0 ⇓

(, ,)

⇑ KDO JSEM

=> složitost $\log(n)$

=> příznak vítěze je 1/0

Přímé ortogonální a řídké hyperkubické a nepřímé vícestupňové propojovací sítě u par. počítače

ORTOGONÁLNÍ SÍTĚ:

HYPERKRYCHLE: Hierarchický rekurzivní ⇒ stupeň je log(n) ⇒ není řídká

Počet automorfismů: $n!\,2^n$

→ tj. překlopení

→ tj. permutace

Velká bisekční šířka, bipartitní a hamiltonovský graf

Počet uzlů ve vzdálenosti i je $\binom{n}{i}$ ⇒ $avg(dist) \doteq \lceil \frac{n}{2} \rceil$

$V(Q_n) = 2^n$

$E(Q_n) = n2^{n-1}$ Průměr: n

$deg(Q_n) = n$ Bisekční šířka: 2^{n-1}

Existuje $k!$ nejkr. cest ve vzdálenosti k ⇒ liší se v k bitech

Symetrická: uzlově i hranově

Nepoužívá se v praxi = něco jako PRAM

MŘÍŽKA dim n

: $M(z_1, z_2 \dots z_n)$ Průměr diam: $\sum(z_i - 1)$

$V(M) = \prod_{\forall i} z_i$

$E(M) = \sum_i (z_i - 1) \cdot \prod_{i \neq j} z_j$

⇒ není regulární ⇒ není uzlově symetrická!

⇒ vzniká aplikací kartézského součinu

– vždy bipartitní

– XY(Z) směrování – vždy podle každé dimenze

TOROID dim n

: $K(z_1 \dots z_n)$

⇒ vzniká jako zabalená mřížka

⇒ platí se vlastnosti mřížky

$diam = \sum \lfloor \frac{z_i}{2} \rfloor$

$deg = \{2n\}$

$b_w = 2 b_w(M)$

⇒ bipartitní ⇔ všechny délky stran jsou sudé

– je regulární, uzlově symetrický

⇒ kartézský součin KRUŽNIC

ŘÍDKÉ HYPERKUBICKÉ SÍTĚ

- odvozeny od hyperkrychle, ale mají konstantní stupeň uzlu
- uzly hyperkrychle se nějakým stejným způsobem rozvinou na více uzlů

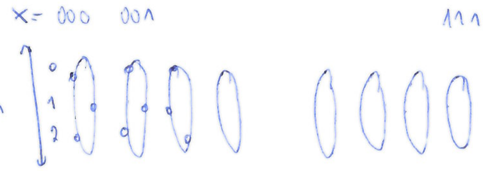
: ZABALENÝ MOTÝLEK - wrapped butterfly

$V = n2^n$

$E = n2^{n+1}$

$diam = n + \lfloor \frac{n}{2} \rfloor$

$b_w = 2^n$



Hrana vede $\langle (i,x);(i \oplus 1, x) \rangle$

$\langle (i,x);(i \oplus 1, neg_i(x)) \rangle$

$\Downarrow$

$i + 1 \mod n$

: OBYČEJNÝ motýlek

⇒ vznikne ze zabaleného tak, že rozpojíme kružnice horizontálně

$V = (n+1)2^n$

$E = n2^{n+1}$

$diam = 2n$

$b_w = 2^n$

Pouze jedna nejkratší cesta ⇒ E-cube směrování

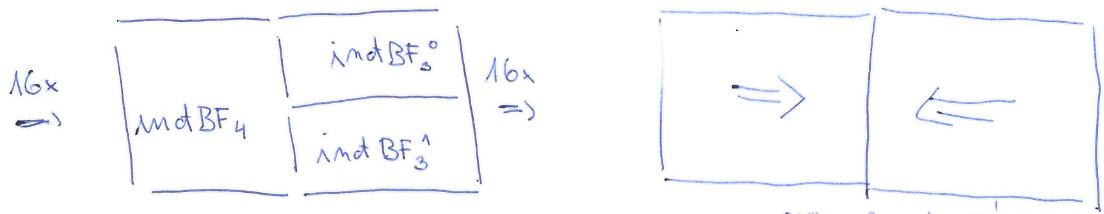
NEPŘÍMÉ SÍTĚ → vícestupňové

- jedna vrstva realizuje permutaci - počet permutací za $\forall$ vrstvu je počet stavů přepínačů na počet přepínačů

$2^{\left(\frac{N}{2}\right)^k}$ N... počet vstupů

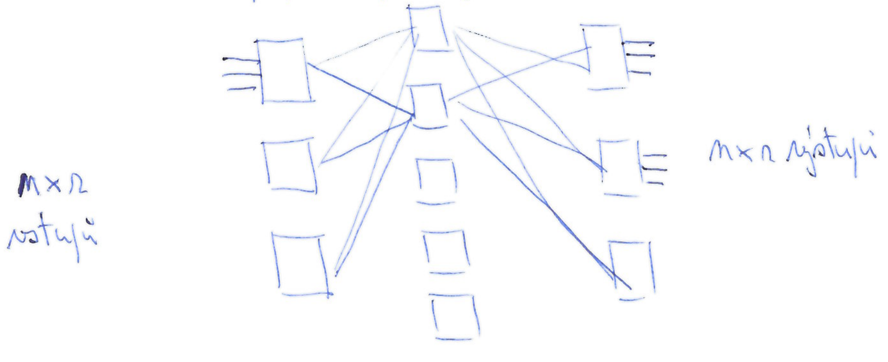
k ... počet vrstev

Benešova síť - back to back motýlek
- dokáže bezblokově realizovat libovolnou permutaci



SYM. 2x MOTÝLEK

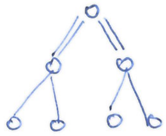
Closova síť - mezi 2 uzly existuje tolik cest, kolik je ve střední vrstvě přepínačů, cesta je pak jednoznačná



⇒ stromové nepřímé sítě

⇒ KOŘEN je komunikační přetížen, navíc má malou bisekční šířku ⇒ malá propustnost

⇒ lze vyřešit hyperstromem, kde existují paralelní hrany



Požadavky na sítě: malý a konstantní stupeň uzlu ⇒ technologicky levné

: malý průměr a malá prům. vzdálenost

: symetrie - zjednodušuje návrh algoritmů

: škálovatelnost - inkrementálně - pokud lze pro libovolné n

: hierarchická rekurzivita - pokud jsou instance nižší dim. podgrafem instancí s dim vyšší

: velká bisekční šířka - propustnost mezi všemi částmi

: měřitelnost : efektivní simulace jiné topologie

Směrování - obousměrné

- jednosměrné

Vícestupňové = sestavené z několika komponent

Měřítka mapování : zobrazení hran a uzlů

- zatížení cílového uzlu (max. zatížení)

- zatížení cílové hrany - (max. zatížení)

- expanze - poměr počtu uzlů obou sítí

- dilatace hrany (na jak dlouhou hranu byla namapována) (max. dilatace)

Quasiisometrické ⇔ existuje mapování s konst. hodnotami měřítek

Výp. ekvivalentní ⇔ pokud lze sítě vzájemně simulovat s konst. zpomalením

Quasiisometrické → výp. ekvivalentní

Obousměrné směrování : výp. uzly jen na jedné straně

⇒ cesta do kořene a zpět ⇒ celkem 2^n cest

M je číslo nejv. bitu, ve kterém se adresy liší

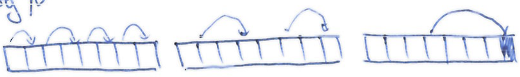
Paralelní redukce a prefixový výpočet nad polem, paralelní konstrukce Eulerovy cesty

PARALELNÍ REDUKCE

- vyžaduje asociativní operaci !
- ideální příklad je binární strom

a) na HYPERKRYCHLI
- e-cube sčítání
- postupně po dimenzích a výsledek zůstane v jednom uzlu

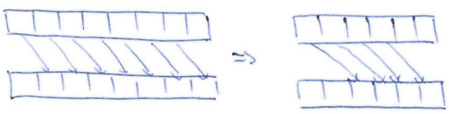
b) na 1D mřížce
- simulace bin. stromu
- $\log\frac{n}{p} + \log p$
- postupně



PREFIXOVÝ SOUČET

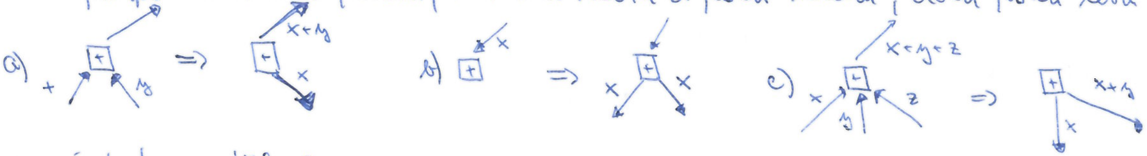
- chceme postupně nasčítat hodnoty v poli

a) nad POLEM
- postupně svůj index zvětšuji 2x a na to místo uložím svou hodnotu
- 1, 2, 4, 8 ...

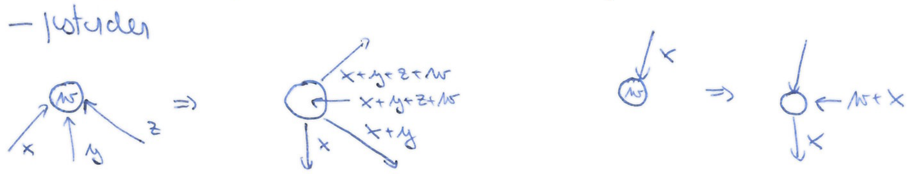


$\Rightarrow \log\frac{n}{p} + \log p$

b) nepřímý strom výpočtu → data pouze v listech
- dokazuje se postupně indukcí
- postupně ve stromech počítám, v uzlu sečtu a pošlu nahoru, dolu pošlu levou část



c) přímý strom výpočtu
- stejný princip je ve vnitřních uzlech počtu ještě
- postorder



d) PPS na KRYCHLI
- 2 hodnoty – TMP a VÝSLEDNÁ
- opět e-cube po dimenzích

- TMP hodnota neustále roste
- VÝSLEDNÁ pouze, pokud dostávám data z nižší dimenze
- na počátku v obou stejná INIT hodnota!
- para data se vymění na obě strany!

KONSTRUKCE EULEROVY CESTY = graf má všechny stupně sudé!

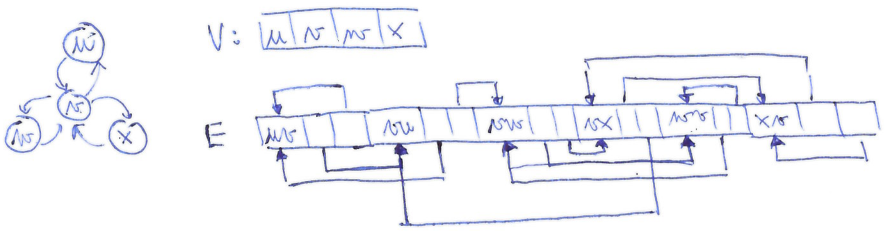
- tah/cesta, který obsahuje každou hranu právě jednou
- tzn. lze nakreslit jedním tahem

Pole uzlů – V, Pole hran – E

↓ ukazatele do pole hran

↓ cyklické podseznamy hran incidujících s uzly

⟹ pole hran je složeno z trojic (uv, ukazatel na opačnou hranu, další hrana tohoto uzlu)



- Využíváme principu pro průchod bludištěm: jdi podle pravé stěny a drž se jí
- EREW_Pram_Eulerian_Tour

for ∀ arc e in E do in parallel: ⟸ Postup po stranu, kde hrany doplníme na antiparalelní!

ET[e] = (E[e].Sib↑).Next

⇑ opačná hrana

ET je pole následníků

4	5	1	2	6	3	← SEM
1	2	3	4	5	6	← ODSUD

PRINCIP ... mám hranu

... vezmu protější

a její následující stranu