

**Teorie grup : Grupoidy, pologrupy, monoidy, grupy.**

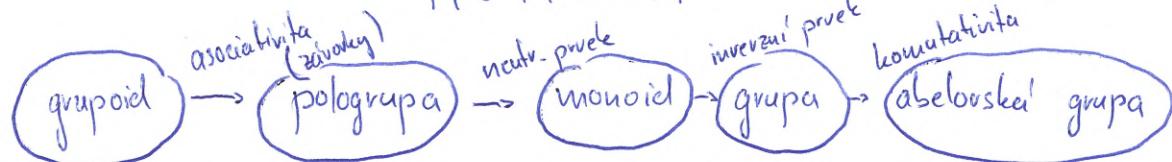
## Podgrupy, cyklicky' grupy a jejich generátory.

- dvojice množina & binární operace  $(M, \circ)$  binární operace na množině  
(konečná či nekonečná)

$$M \neq \emptyset$$

$$M \circ M \rightarrow M$$

musí být uzavřená vůči operaci



$$\text{neutrální prvek} \rightarrow a \circ e = e \circ a = a$$

$$\text{inverzní prvek} \rightarrow a^{-1} \circ a = a \circ a^{-1} = e$$

(musí existovat pro každé a)

$$\begin{aligned} \rightarrow \text{podgrupy} : H &= (N, \circ) && \text{je grupa} \\ &\& N \subseteq M \end{aligned}$$

$$H \subseteq M$$

$(Z, +)$  - množina uzavřená vůči operaci

$$(Q, \circ) \quad a \circ b = \frac{a+b}{2} = \text{grupoid}$$

$$(R^+, \circ) \quad a \circ b = \frac{a \cdot b}{a+b} = \text{pologrupa}$$

$$(R, -) : \text{monoid}$$

- triviální podgrupy:
  - grupa samotná
  - obsahující pouze neutrální prvek
  - existují v každé grupě s alespoň dvěma prvky

◦ vlastnosti

### Rád grupy (podgrupy)

= počet prvků množiny M

- může být nekonečný

- rád podgrupy dělí rád grupy (u konečných) = Lagrangeova věta

(nemusí ho ale dělit naopak) - tj. nemusí pro každý dělitel existovat podgrupa

→ grupa s pravým sítěm má pouze triviální podgrupy

- podgrupa generovaná množinou N  $\rightarrow \langle N \rangle$

- nejménší podgrupa obsahující N

- množina generátorů grupy G  $\langle M \rangle = G$

- grupový obal  $\rightarrow$  získání mocnín všech prvků  $\langle N \rangle$   
(tj. některým všechny prky  $\langle N \rangle$ )
- (- podgrupa  $\langle N \rangle$ ) = průnik všech podgrup obsahujících  $N$ )?

Cyklické grupy - musí existovat prvek  $a$ ;  $\langle a \rangle = G$   
= generátor cyklické grupy

$\mathbb{Z}_n^+$  - generátorem jsou všechna  $k \leq n$  nesoudělná s  $n$   
 $\rightarrow \text{gcd}(k, n) = 1$

$\mathbb{Z}_n^\times$  - když najdu jeden generátor, ostatní najdu umocňováním  
generátoru na mocniny nesoudělné s rádcem

Malá Fermatova Věta :

$$a^{p-1} \equiv 1 \pmod{p}$$

V cyklické grupě je počet generátorů =  $\varphi(m)$  řád grupy  
 $\# X \rightarrow \text{gcd}(x, m) = 1 \quad \forall x \in m$

- vždy platí:  $a^n = e$  (v ~~cyklické~~ grupě)
- podgrupa cyklické grupy je také cyklická

Multiplikativní grupy:  $\mathbb{Z}_n^\times$  řád grupy =  $\varphi(n) = m$

- pro prvočísla  $\varphi(p) = p-1$   
počet ~~generátorů~~ generátorů grupy =  $\varphi(m)$  (platí ~~pro~~ ~~všechny~~ ~~cyklické~~)

- první nejak najdu  $\rightarrow$  další umocňováním na  
číslo nesoudělné s rádcem  $m$

Cyklické jsou pouze pro  $n=2, n=4, n=p^k, n=2p^k$   
 $p$  - liché prvočíslo

Aditivní grupy  $\mathbb{Z}_n^+$  - rad grupy = n

$\Psi(n) = \text{počet generátorů}$

- generátory jsou čísla nesoudělitelná s n

- všechny aditivní grupy  $\mathbb{Z}_n^+$  jsou cyklické

Homomorfismus: dvě grupy G, H a zobrazení  $\varphi: G \rightarrow H$

takový, že  $g_1, g_2 \in G, h_1, h_2 \in H: \varphi(g_1) \stackrel{H}{\circ} \varphi(g_2) =$

$$= \varphi(g_1 \stackrel{G}{\circ} g_2), [\varphi(g_1) = h_1, \varphi(g_2) = h_2]$$

- množství pravý se mapují na sebe

- struktura podgrup musí korespondovat (~~podmnožiny~~)

Isomorfismus: homomorfismus, který je bijekcí

- dvě množiny <sup>cyklické</sup> grupy jsou izomorfní

- izomorfismus zachovává cykличnost

- počet izomorfismů = počet generátorů

dále: v každé grupě lze jednoznačně dítib!

pro libovolny  $a, b \in G$      $a \circ x = b$      $y \circ a = b$     má jedinou řešení

cyklické grupy mají všechny podgrupy kohy cyklické

n-tá mocnina produkta a v grupě

$$a^n = \underbrace{a \circ a \circ \dots \circ a}_{n-\text{krať}} \Rightarrow (\mathbb{Z}, +) \text{ je cyklická všechny pravy lze vygenerovat}$$

$$(-1) \text{ nebo } (1)$$

$$a^0 = e$$

$$a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ a^{-1} \dots \circ a^{-1}}_{n-\text{krať}}$$

Tělesa a okruhy: Základní definice a vlastnosti. Konečná tělesa.

Okruhy polynomů, irreducibilní polynom.

|| Okruh:  $R = (M, +, \cdot)$

pohled:  $(M, +)$  je Abelská grupa (aditivní grupa okruhu)

$(M, \cdot)$  je pologrupa \* (množstevní pologrupa okruhu)

platí levý a pravý distributivní zákon  $a(b+c) = ab+ac$

$\Rightarrow$  rád je počet prvků  $n$   $(M, +)$  (číselní muly)

[ binární okruh:  $(\{0\}, +, \cdot)$  ] - neutrální prvek  $(M, +) =$  nula výsledek  
 → neexistuje hr. 0  
 - násobení 0 musí být 0

množové produkty  $a, b \in M$  lze výv. ře  $a \cdot b = 0 \rightarrow$  dělitelné muly

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

|| Obor Integrity: komutativní okruh bez dělitelné muly

nasobení je komutativní

není nula dělitelná

|| Těleso : okruh, jehož  $(M - \{0\}, \cdot)$  je grupa

binární těleso  $(\{0, 1\}, +, \cdot)$  - nejménší (operace jako XOR, AND)

kvadratické těleso je obor integrity

Homomorfismus & izomorfismus

- funguje pro jednotlivé grupy stejně (aditivní & množstevní)

$(Q, +, \cdot)$  - nejménší číselné těleso

Konečný kříž : koncový počet prvků generátor křížu menšího počtu  
 konkrétní příklad  $\mathbb{Z}_p$  ...  $(M, +)$  - rád p  
 $(M, \cdot)$  - rád  $p-1$  (menší než p)

$(M, \cdot)$  je vždy cyklická,  $q(p-1)$  generátorem

definice:  $\mathbb{Z}_n^*$  je cyklická podskupina  $n = 2, 4, p^k, 2p^k, p^k+2$  ] neplatí  
 - rád konečného kříže je vždy  $p^n$  (charakteristika)

$GF(p^n)$   $P(x) \in K[x]$  ← obraz polynomů

irreducibilní polynom:  $P(x) = A(x) + B(x) \Rightarrow$  stupen  $A(x) = 0 \vee B(x) = 0$

→ chovají se podobně jako prvci

$\left( K \text{ je obr.} \rightarrow K[x] \text{ komutativní obr. polynomů} \right.$   
 $\text{nad oborem } K \left. \right)$

$GF(m^n)$  řídkání definujeme po složkách modulo m

- máme moduluře zadaným irreducibilním polynomem

- aditivní grupa kříže  $GF(p^n)$

- má rád  $p^n$

- neutrální prvek  $0^n$

- menší cyklická

- multiplicativní grupa

- má rád  $p^{n-1}$

- neutrální prvek  $0^{n-1}$

- je vždy cyklická

kříž  $p^n$  pro konkrétní m

$m=1 \rightarrow (\mathbb{Z}_p, +, \cdot)$

$m > 1 \rightarrow$  množina polynomů obrazu

$\mathbb{Z}_p[x]$

(máme najít n-1)

→ řídkání po složkách modulo p

→ máme v oboru  $\mathbb{Z}_p[x]$  mod  
neplatí ied. pol. máme n

operace nad GF( $m^n$ )

$$\sum_{i=0}^n a_i x^i + \sum_{i=0}^n b_i x^i = \sum_{i=0}^n (a_i + b_i) x^i$$

$$\left( \sum_{i=0}^n a_i x^i \right) \cdot \left( \sum_{i=0}^m b_i x^i \right) = \sum_{i=0}^{n+m} \left( \sum_{j+k=i} a_j b_k \right) x^i$$



Funkce více proměnných: gradient, Hessian, definitnost matic, extrémy funkcií více proměnných bez omezení a s rovnostními omezeními

derivace: funkce má v bodě  $a \in \mathbb{R}$  derivaci, jestliže  $f$  definována v okolí bodu  $a$  a existují limity:

$$f'(a) = \lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h} = \lim_{h \rightarrow a} \frac{f(x) - f(a)}{x-a} = \text{derivace funkce } f \text{ v bodě } a$$

Parciální derivace: - derivace funkce  $f$  v bodě  $a$  ve směru  $v$

$$\frac{\partial f}{\partial v}(a) = \Psi_v(a) = \lim_{t \rightarrow 0} \frac{\Psi_v(t) - \Psi_v(0)}{t} = \lim_{t \rightarrow 0} \frac{f(a+tv) - f(a)}{t}$$

- v mřížce byl jazyk holkov množ, nejčastěji se používají směry souřadnicích os

→ gradient  $\nabla f(a) = \left( \frac{\partial f}{\partial x_1}(a), \frac{\partial f}{\partial x_2}(a), \dots, \frac{\partial f}{\partial x_n}(a) \right)$

- matice derivací funkce v bodě  $a$  ve směrech souřadnicích os  
parciálních

- pro lokální extrém platí  $\nabla f(x) = 0$  (místní počívka)

Jacobiova matice: v podstatě více normovaný gradient

- m-násobek skalárních funkcí  $(f_1, \dots, f_m)$  se schodujícím det. oborem

$$J_f = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1} & \dots & \frac{\partial f_m}{\partial x_n} \end{pmatrix} \quad \left[ \begin{array}{l} \text{- pravděpodobně menší souřadnice oblasty} \\ \text{- množina} \end{array} \right]$$

Parciální derivace vyššího řádu

pro funkci  $f(x_1, x_2, \dots, x_n)$ :

$$\nabla^2 f(a) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2}(a) & \frac{\partial^2 f}{\partial x_1 \partial x_2}(a) & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(a) \\ \vdots & \vdots & & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(a) & \frac{\partial^2 f}{\partial x_n \partial x_2}(a) & \dots & \frac{\partial^2 f}{\partial x_n^2}(a) \end{pmatrix}$$

Hessova matice - matice parciální derivací druhého řádu

- pokud je ~~funkce~~ v bodě spojiteľ, musí tam být spojiteľ i funkce  $\frac{\partial^2 f}{\partial x_i \partial x_j}$  a obě parciální derivace se kouzly

→ matice je symetrická  
(pokud jsou spojiteľ všechny)

## Definiteness matic

- matice je pozitivně definitní', pokud pro každý  $\vec{x} \in \mathbb{R}^n - \{\vec{0}\}$  platí  $\vec{x}^T M \vec{x} > 0$ 
    - negativně definitní' - protodi nezmínku
  - pozitivně semidefinitní' :  $\vec{x} \in \mathbb{R}^n \quad \vec{x}^T M \vec{x} \geq 0$  (a zároveň existuje nenule'  $\vec{y} \in \mathbb{R}^n$   $\vec{y}^T M \vec{y} = 0$ )
    - negativn' opět pouze protiargumentu
  - v ostatních případech indefinitní' ( $> i <$  pro některé vektory)
    - $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$

*Sylvestrovo kubovium* - pro symetrické matice  $M \in \mathbb{R}^{n \times n}$

matice  $M_1, M_2, \dots, M_k$  - členové matice  $k \times k$  ktorí v levom hornom rohu majú

- matice je pos. definicí, jehož všechny determinanty jsou kladné  
neg. definicí, ————— || ————— se říkají (obě) a první je rázem

## Extreme funkcií více proměnných

- kritické body ve víc rozměrech  $\nabla f = 0$
  - lokální minimum ( $\forall x \in \Omega_a$ ) ( $f(x) \leq f(a)$ )
  - ~~pochinčka~~ pochinčka pro osobní lokální maximum:
    - $\nabla f = 0$ ,  $\nabla^2 f(a)$  je pozitivně definitní
    - obdobně se dá převést na minimum
  - indefinitní matice - sedlový bod
  - nutná pochinčka pro  $f$  aby měla v bodě  $a \in D$  lokální maximum
  - $\nabla f(a) = 0 \wedge \nabla^2 f(a)$  je negativně semidefinitní
  - posticijní pochinčka pro osobní lokální maximum
  - $\nabla f(a) = 0 \wedge \nabla^2 f(a)$  je negativně definitní

Lokální extrémum při omezeních

funkce  $f$  má v bodě  $a$  obecné lokální minimum při omezeních:

$$\left( \exists H_a \right) \left( \forall x \in H_a \cap \bar{J} = \right) \left( f(x) < f(a) \right)$$

bod musí splňovat konečný počet rovností

$$g_i(a) = 0, \{1, \dots, I\} = \hat{I}, i \in \hat{I}, I \in \mathbb{N}$$



Definujte funkci více proměnných, parciální derivaci, gradient, Hessova, posloup. hledání loc. extrema.

funkce více proměnných:  $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$  zobrazení, kdežto každemu  $x \in \mathbb{R}^n$  přiřadí množství jehož  $a \in \mathbb{R}^m$  ( $f(x) = a$ )

parciální derivace:

$$\text{funkce } \varphi_v(t) = \frac{f(a+tv)}{\|v\|}$$

$v$ : vektor jednotkové délky  $\|v\| = 1$

$a$ : vektor z definičního oboru funkce

derivace funkce  $f$  v bodě  $a$  v směru  $v$ :

$$\frac{\partial f}{\partial v}(a) = \varphi'_v(0) = \lim_{t \rightarrow 0} \frac{\varphi_v(t) - \varphi_v(0)}{t} = \lim_{t \rightarrow 0} \frac{f(a+tv) - f(a)}{t}$$

derivace v bodě 0

-  $v$  je jedním z několika mnoha směrů

→ říkáme ře  $\frac{\partial f}{\partial v}(a)$  je parciální derivace.

Gradient:  $\nabla f(a) = \left( \frac{\partial f}{\partial x_1}(a), \frac{\partial f}{\partial x_2}(a), \dots, \frac{\partial f}{\partial x_n}(a) \right)$  gradient v bodě  $a$

vektor parciálních derivací ve směrech souřadnicích os.

- uvízí směr nejrychlejšího růstu  $f$  v bodě  $a$

$$v_\nabla = \frac{\nabla f(a)}{\|\nabla f(a)\|}$$

Hessova matice: 2. parciální derivace  $f$  v bodě  $a$ :

$$\nabla^2 f(a) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2}(a) & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(a) & \dots & \frac{\partial^2 f}{\partial x_n^2}(a) \end{pmatrix}$$

$$\frac{\partial^2 f}{\partial u \partial v}(a) = \frac{\partial}{\partial u} \frac{\partial f}{\partial v}(a) \quad u \neq v$$

$$\frac{\partial^2 f}{\partial u^2}(a) = \frac{\partial}{\partial u} \frac{\partial f}{\partial u}(a) \quad u = v$$

definice limity řeš posloupnosti vektorů

$$\left\{ \left( x_k \right)_{k=1}^{\infty}, x_k \in \mathbb{R}^n \right\}$$

- konverguje k vektoru  $x_0 \in \mathbb{R}^n$  (tzn.  $x_0$  je její limitou)

$$\boxed{\lim_{k \rightarrow \infty} x_k = x_0}$$

pokud posloupnost čísel  $(\|x_k - x_0\|)_{k=1}^{\infty}$  konverguje k 0

tedy

$$\boxed{\lim_{k \rightarrow \infty} \|x_k - x_0\| = 0}$$

funkce  $f$  má v bodě  $x_0 \in D$  limitu  $y_0 \in \mathbb{R}^m$

pokud:

$$\boxed{\lim_{k \rightarrow \infty} x_k = x_0 \Rightarrow \lim_{k \rightarrow \infty} f(x_k) = y_0}$$

spojitost funkce: (přes limitu)

tedy  $f$  je spojita v bodě  $x_0$  pokud platí

$$\boxed{\lim_{k \rightarrow x_0} f(x) = f(x_0)}$$

okolí:

$$H_a = \{x \in \mathbb{R} \mid \|x - a\| < r\} \text{ pro } r > 0$$

lokální maximum = existuje okolí bodu  $a$   $H_a$  takové,

že pro všechny  $x \in H_a$  platí  $f(x) \leq f(a)$

$$f(x, y) = 3x + 4y \quad g_1 = x^2 + y^2 = 1$$

metoda Lagrangeowych moltiplikatorów:

$$x^2 + y^2 - 1 = 0$$

$$\mathcal{L}(x, y, \lambda) = 3x + 4y + \lambda(x^2 + y^2 - 1)$$

$$\mathcal{L}_x = 3 + 2\lambda x = 0 \quad x = -\frac{3}{2\lambda}$$

$$\mathcal{L}_y = 4 + 2\lambda y = 0 \quad y = -\frac{4}{2\lambda} = -\frac{2}{\lambda}$$

$$\mathcal{L}_\lambda = x^2 + y^2 - 1 = 0 \quad \left(-\frac{3}{2\lambda}\right)^2 + \left(-\frac{2}{\lambda}\right)^2 - 1 = 0$$

$$\left(-\frac{3}{5}, -\frac{4}{5}\right) \Rightarrow \text{lok. min.} \quad \frac{9}{4\lambda^2} + \frac{4}{\lambda^2} - 1 = 0$$

$$\left(\frac{3}{5}, \frac{4}{5}\right) \Rightarrow \text{lok. max.} \quad 9 + \frac{16}{25} = 4\lambda^2$$

$$\nabla^2 f = \begin{pmatrix} 2\lambda & 0 \\ 0 & 2\lambda \end{pmatrix} \quad 25 = 4\lambda^2$$

$$x_{1,2} = -\frac{3}{2\lambda} = \pm \frac{3}{5}$$

$$y_{1,2} = -\frac{4}{2\lambda} = \pm \frac{4}{5}$$

$$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \text{ poz. definitum'}$$

$$\begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix} \text{ negatywne definitum'}$$

$$f(x, y) = x^2 - y^2$$

$$\nabla f(x, y) = \left( 2x, -2y \right)$$

$$2x = 0$$

$$x = 0$$

$$-2y = 0$$

$$y = 0$$

$$\nabla^2 f(x, y) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

- Sylwetkowe kryterium nie mieści się nigdzie

$$(x_1, x_2) \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$(2x_1, -2x_2) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 2x_1^2 - 2x_2^2 \rightarrow \text{indefinitematice}$$

$\rightarrow$  niewiążący bod

# Integral funkcií více proměnných (Riemannova konstrukce)

rozdelení intervalu  $\sigma = \{x_0, x_1, \dots, x_n\}$

$$a = x_0 < x_1 < \dots < x_n = b \rightarrow \text{rozdelení intervalu } [a, b]$$

$\nu(\sigma)$  - norma rozdelení  $\sigma$  = největší interval rozdelení

$f: D \subset \mathbb{R} \rightarrow \mathbb{R}$  → ekvivalentní rozdelení - všechny intervaly jsou stejné  
 $\sigma_{\text{supremum na intervalu}} (\sup_{x \in [x_{i-1}, x_i]} f(x))$

$$S(\sigma) = \sum_{i=1}^n (x_i - x_{i-1}) M_i f(x) - \text{horní součet } f \text{ při rozdelení } \sigma$$

$$s(\sigma) = \sum_{i=1}^n (x_i - x_{i-1}) m_i f(x) - \text{dolní součet}$$

$\leftarrow \text{minimum } (\inf_{x \in [x_{i-1}, x_i]} f(x))$



$$S(\sigma) \geq s(\sigma)$$

o pro  $f$  omezenou na  $[a, b]$ :  $\inf \{S(\sigma) | \sigma \text{ je rozdelení na } [a, b]\}$

→ horní integrální součet  $f$  na  $[a, b]$   $\int_a^b f$

$$\text{... dolní integrální součet } \int_a^b f \quad \boxed{\int_a^b f \leq \int_a^b f}$$

o pokud se integrality rovnají:  $f$  integrálelná na  $[a, b]$

→ nazýváme Riemannův integral  $f$  na  $[a, b]$

vesmírnosti:  $f$  spojka na  $[a, b]$  je integrálelná na  $[a, b]$

pokud  $f(x) = g(x)$  ve každému vnitřním bodě, je  $g$  též integrálelná

additivita v místech:  $\int_a^c f = \int_a^b f + \int_b^c f$  (pokud jsou na intervalu integrálelné)

(+ linearity a monotonicitě funkcií na hodnotách)

- integrování,  $I = D^{-1} \rightarrow$  primitivní funkce (inverzní proces k derivování)

$$\int_a^b f = F(b) - F(a) = [F(x)]_a^b = \text{Newton - Leibnizova formule}$$

$\uparrow$   $\uparrow$   
primitivní funkce

(integral s použitím, substitucí)

$$\int u v = u v - \int u v'$$

→ analogicky se dle definice pro více dimenzi  $R = [a,b] \times [c,d]$

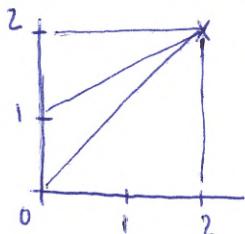
T - rozdělení na pravouhelníky

dvojí integral  $f$  na  $R$  :  $\iint_R f(x,y) dx dy$

- opět platí additivita přes oblast integrací, linearity a monotonicity

$$\iint_R f+g = \iint_R f + \iint_R g, \quad \alpha f = \alpha \iint_R f$$

Dvojí integral nad obecnou oblastí



$$f(x,y) = (x+y)^2$$

$$\left| \begin{array}{l} f(x,y) = x^2 + y^2 \quad D = \langle 0,3 \rangle \times \langle -1,1 \rangle \\ \int_{-1}^1 \int_0^3 x^2 + y^2 dx dy = \int_{-1}^1 \left[ \frac{1}{3}x^3 + xy^2 \right]_0^3 dy = \\ = \int_{-1}^1 9 + 3y^2 dy = \left[ 9y + \frac{3y^3}{3} \right]_{-1}^1 = 10 + 10 = \underline{\underline{20}} \end{array} \right.$$

$$\begin{aligned} \int_0^2 \int_{\varphi(x)}^{\psi(x)} f(x,y) dy dx &= \int_0^2 \int_x^{\frac{x}{2}+1} (x+y)^2 dy dx = \int_0^2 \left[ \frac{1}{3}(x+y)^3 \right]_x^{\frac{x}{2}+1} dx = \frac{1}{3} \int_0^2 \left( x + \frac{x^2}{2} + 1 \right)^3 - (2x)^3 dx = \\ &= \frac{1}{3} \left[ \frac{1}{5} \left( \frac{3x}{2} + 1 \right)^5 - 2x^5 \right]_0^2 = \frac{7}{2} \end{aligned}$$

$$R = [a, b] \times [c, d] \subset \mathbb{R}^2 \quad a < b, c < d$$

$f: D \subset \mathbb{R}^n \rightarrow \mathbb{R}$ ,  $R \subset D$ ,  $f$  je na  $R$  omezená

Kordilní pravouhleho  $R$        $\sigma = \{R_1, R_2, \dots, R_m\}$

- pro  $i = 1 \dots n$   $R_i = [a_i, b_i] \times [c_i, d_i]$   $a_i \leq a_i < b_i \leq b$ ,  $c_i \leq c_i < d_i \leq d$
- rádiu dvou  $R_i, R_j$  nejsou shodné (pozor slabiky!)
- $R_1 \cup \dots \cup R_n = R$

horní součet  $f$  při kordilní  $\sigma$

$$S(\sigma) = \sum_{i=1}^n \sup_{x \in R_i} f(x) \cdot \text{plocha } R_i = \sum_{i=1}^n (b_i - a_i)(d_i - c_i) \sup_{x \in R_i} f(x)$$

dolní součet definovaný stejně s infimum

$$s(\sigma) = \dots$$

úloha  $\inf(S(\sigma))$  je kordilní  $R$ ) horní integrální součet  $f$  na  $R$

$\sup(s(\sigma))$  je kordilní  $R$ ) dolní ————— + —————

Primitivní funkce k funkci  $f$  na intervalu  $(a, b)$  je  $F(x) : \forall x \in (a, b) \quad F'(x) = f(x)$



**Matematika neurčitosti:** vzdálenosti a další mistry podobnosti, fuzzy umozněny a operace s nimi, t-normy a t-konormy, entropie a její souvislost s neurčitostí

podobnost objektů → neurčitá schoda jejich vlastností  
 (objekty, lamy, dokumenty, strukturní dat)

vzdálenost:  $d : X \times X \rightarrow [0, +\infty)$

vlastnosti  $\triangleright$ :  $(\forall x, y \in X) d(x, y) = 0$  právě když  $x = y$

$(\forall x, y \in X) d(x, y) = d(y, x)$

$(\forall x, y, z \in X) d(x, y) \leq d(x, z) + d(z, y)$

mistry podobnosti:  $s : X \times X \rightarrow \mathbb{R}$

$(\exists \mu > 0)(\forall x, y \in X) s(x, y) \leq s(x, x) = \mu$

$(\forall x, y \in X) s(x, y) = s(y, x)$

|| Vzdálenosti číselních vektorů  
 rozšíření na normové vektoru  
 $d(x, y) = \|y - x\|^*$

Minkowského norma (vzdálenost)

$$\|x\|_p = \sqrt[p]{\sum_{i=1}^n |x_i|^p} \quad \text{kde } p \in [1, \infty]$$

○ Eukleidovská norma: ( $p=2$ ):

$$\|x\|_2 = \sqrt{\sum_{i=1}^n |x_i|^2}$$

\* pro normy na prostoru  $\mathbb{R}^n$  platí:

$$\|x\| \geq 0; \|x\| = 0 \Leftrightarrow x = 0; \|ax\| = |a| \|x\|, \|x+y\| \leq \|x\| + \|y\|$$

- manhattanšká norma ( $p=1$ ):

$$\|x\|_1 = \sum_{i=1}^n |x_i|$$

- Čebyševská norma  $p \rightarrow \infty$

|| Vzdáenosť realizácií stejne rozložených vektorov  $X, Y$  (korelační koeficienty)

- sú ich spolu, mají dve spoločné vlastnosti

- maximum pre dve stejne veličiny = 1

- minimum pre nezávisle = 0

Pearson  $\text{corr}(X, Y) = \frac{\text{cov}(X, Y)}{\sqrt{\text{var}(X) \cdot \text{var}(Y)}}$  ← koreancia mezi dvoma veličinami X a Y

Spearman  $\text{rank}(X, Y) = 12 \mathbb{E} (H(X, Y) - F(X)G(Y))$  ← distribučná funkcia jednotlivých veličín

Kendall  $\tau(X, Y) = P[(X_1 - X_2)(Y_1 - Y_2) > 0] - P[(X_1 - X_2)(Y_1 - Y_2) < 0]$

Fuzzy množiny  $A = (U, \mu_A)$  - fuzzy množina,  $\mu_A: U \rightarrow [0, 1]$  - funkcia prísľivnosti

- $\mu_A(x)$  - stupň prísľivnosti  $x \in A$

- $\{x \in U \mid \mu_A(x) > 0\}$  - množina,  $\{x \in U \mid \mu_A(x) = 1\}$  - jadro

příklad:

- $U$  - všechny možné typy vody (hlavně diskrétní)

- $A$  - množina „voda je sladká“

- $\mu_A(x)$  - na kolik typů  $x$  patří do množiny  $A$

Operace nad fuzzy množinami:

- Doplňek -  $A^c: \mu_{A^c}(x) = 1 - \mu_A(x)$

- Průnik -  $A \cap B: \mu_{A \cap B}(x) = \mu_A(x) \wedge \mu_B(x), \wedge: [0, 1]^2 \rightarrow [0, 1] = t\text{-norma}$

- Sježdzení -  $A \cup B: \mu_{A \cup B}(x) = \mu_A(x) \vee \mu_B(x), \vee: [0, 1]^2 \rightarrow [0, 1] = t\text{-konorma}$

I-mormy & konormy

$T$  - množinový součin  
 $\perp$  - množinový součet } mají velmi podobné vlastnosti  
 - rostoucí v  $u, v$ , komutativní a asociační

$$0 \leq u, v \leq 1 \Rightarrow 0 \leq uT v \leq \min(u, v)$$

$$\Rightarrow 1 \geq u \perp v \geq \max(u, v)$$

Gödelova (minimova, maximova)  $T: \min(u, v)$ ,  $\perp: \max(u, v)$

$$\text{socírová} = T: u \cdot v, \perp: u + v - u \cdot v$$

$$\text{Łukasiewiczeva: } T: \max(0, x+y-1) \quad \perp: \min(1, x+y)$$

→ z hledi' mormy mohu dostat konormu pomocí de Morganových vztahů

(Mamdaního metoda - rozdíl mezi dvěma univerzity)

• Kopule a jejich související  $k$ -normamy:  $C: [0,1]^2 \rightarrow [0,1]$

platí:

- $0 \in \{u, v\} \Rightarrow C(u, v) = 0$  dlestejná norma } stejná jako  $k$ -normy
- $1 \in \{u, v\} \Rightarrow C(u, v) = u \perp v \rightarrow C(u, 1) = u, C(1, v) = v$  }
- $C(x_2, y_2) - C(x_2, y_1) - C(x_1, y_2) + C(x_1, y_1) \geq 0$   
 $(\forall (x_1, x_2), (y_1, y_2))$

Skladová věta

- nechť  $X, Y$  jsou náhodné veličiny &  $F, G$  jejich distribuční funkce  $F, G: \mathbb{R} \rightarrow [0, 1]$

-  $H: \mathbb{R}^2 \rightarrow [X, Y] = H$  je skladené rozložení náhodného vektoru  $(X, Y)$  právě

když existuje kopule  $C$  taková, že s plat. 1 platí:

$$H(X, Y) = C(F(X), G(Y))$$

Entropie (viz. PST / KOD)

- role aví chybí brance mezi entropií a fuzzy matematikou  
 (viz. chybí den přehod)

další k fuzzy množinám:

pro k-merný pláti:

$$0 \in \{u, v\}, uT_v = 0$$

$$1 \in \{u, v\}, uT_v = uT_d v$$

$$uT_d v = \begin{cases} v & \text{pokud } u=1 \\ u & \text{pokud } v=1 \\ 0 & \text{jinak} \end{cases}$$

$$\left. \begin{array}{l} uT_v = vT_u \\ ((uT_v)Tw) = (uT(vTw)) \end{array} \right\} \text{pláti i pro komorny}$$

$$0 \in \{u, v\}, uL_v = uL_d v$$

$$1 \in \{u, v\}, uL_v = 1$$

$$uL_d v = \begin{cases} u & \text{pokud } v=0 \\ v & \text{pokud } u=0 \\ 1 & \text{jinak} \end{cases}$$

# MI-SPOL - 6 (MI-PAA)

## Význam tříd NP a NPH pro praktické výpočty

KOMBINATORICKÝ PROBLÉM - uskupení, výsledek, konfigurační proměnné  
+ omezení & optimalizační kritérium  
( konečný a diskrétní )

KONFIGURAČNÍ PROMĚNNÉ - množstvem hranou silou

KONFIGURACE - ohodnocení konfiguračních proměnných

INSTANCE - ohodnocení všech proměnných

ŘEŠENÍ INSTANCE - konfigurace splňující omezení

CERTIFIKÁT - instance, kterou je možné ověřit, zda odpovídá danému správnému

SAT, 3SAT ( kvádruje právě 3 libovoly )

- booleovské formule v CNF ( součet součinů )

STAV ALGORITMU - konfigurační proměnné U vnitřní proměnné algoritmu

STAVOVÝ PROSTOR - ~~číslojce~~  $(S, Q)$  všechny operátory  $\Omega: S \rightarrow S$   $q_j(s_i) \neq s_i$   $\forall q_j, s_i$   
všechny stavů

STRATEGIE POKYBU V PROSTORU - náhodná, systematická ...

→ ROZHODOVACÍ PROBLÉMY existují alespoň 1 řešení ?

→ KONSTRUKTIVNÍ typické jedno řešení

→ ENUMERACNÍ typické všechna řešení

[ → tisk se pouze výsledek, ostatní ji nejdou ]

+ Optimalizační problém ↘ rozlučovací - existuje alespoň tak dobré jako  $\Omega$  ?

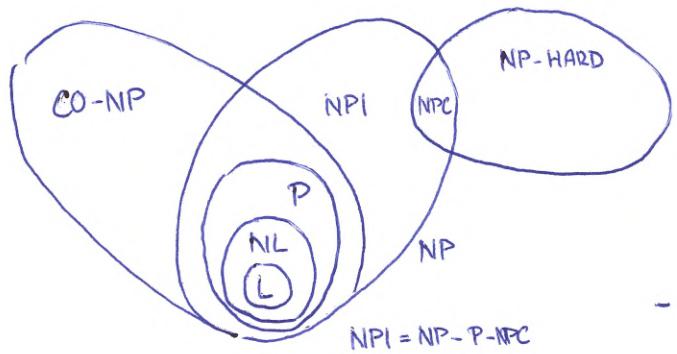
konstrukční  
enumerativní - } co nejlepší

evaluační - najít nejlepší cenu pro danou konfiguraci

Turingův stroj

DETERMINISTICKÝ - další stav je deterministicky ( jednoznačně určený )  
- karetu se nedále poslat kvůli s využitím p polek

NEDETERMINISTICKÝ - v každém kroku se mohou vyskytnout  
→ může přesné kam jít



konečné číslo

P - řešitelné DTS v polynomialním čase  $O(n^k)$

NP - řešitelné NTS v polynomialním čase

[ - Hamiltonovská kružnice ]

- jeho řešení bude v pol. čase ověřit možnost DTS (certifikát)

(D) - NP - pokud jde o dobu  $\bar{X}$  se nachází ve skupině NP

- můžeme ho jednoduše ověřit  $\leftarrow$  neexistuje certifikát
- [ - daná formulace je nesplnitelná ]

Optimalizační PO - patří do NPO a existuje DTS řešitelný hardou instance v pol. čase

- NPO
- velikost instance omezena polynomem
  - v pol. čase lze najít, zda je ~~je~~ kontingenční řešení
  - optimalizační kritérium bude využitelné v pol. čase

NPH - dle něj Turingova redukce převést jednoduché problem z NP v pol. čase  
~~zjednodušit~~

- NPC - patří redukci do NP a NPH [SAT, knoth, ...]
- daje se možnost převést v pol. čase

NPI - není praktická, ale velmi malá

Turingova redukce  $R_1 \leq R_2$  - existuje program pro DTS, který řeší hardou instance  $I_1$  pro problém  $R_1$ , když řeší používá program  $P_2$  pro problém  $R_2$ , jehož podprogram

Karpova redukce  $R_1 \leq K R_2$  - existuje poly. program pro DTS, který  $\neq$  instance A převede na B tak, že výsledky se shodují  $\Rightarrow$  jde o volání polyprogramu

$\Rightarrow$  transitivity & umožňuje využít stejné polynomické ekvivalence

Cochova věta - Existuje NPC - problém (a již SAT)

- pokud je problém NP a lze mu nijí převést SAT, pak je NPC (Karpova redukce)
- $\neq$  problém NP lze převést na SAT

## Experimentální vyhodnocení algoritmů, zejména randomizovaných

- ▷ RANDOMIZOVANÝ ALGORITMUS - vstupuje do něj náhoda
- ▷ PSEUDOPOLYNOMIALNÍ ALGO - závisí ~~na~~ polynomiatně na velikosti instance (počet kroků)
  - + na dalším parametru mimořádně s velikostí instance
- ▷ APPROXIMATIVNÍ ALGO - APR pro daný problém je  $R$ -approximativní ( $\epsilon$ ) pokud každou instanci vyřeší s relativní kvalitou  $R$  (chybou  $\epsilon$ )
  - o polynomiatně čas
- ▷ SAT - CNF : řeší ji pro nějaké ohodnocení pravdivosti
- ▷ MAX SAT : hledá největší klauzuli bee splnit

Řešíme NPO problémy :

Deterministický - variuje chybu v nejhorším případě  
 ( pseudopol., approx )

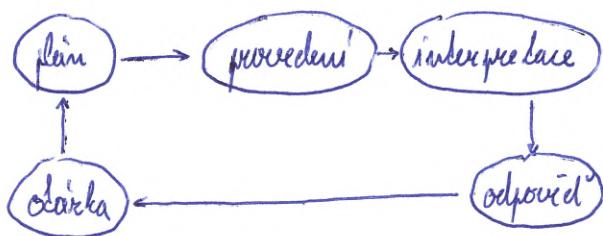
Náhodná a kombinovaná metoda → randomizovaní algoritmy  
 - statistická chyba v průměrném případě

- Monte Carlo - používá čas, náhodnou pravdivost (Miller-Rabinov test pravdivosti)
- Las Vegas - používá pravdivost, náhodný čas  
 (Quick sort a volba pivotu)

výhody : - jednoduchosť  
 - kvalita polynomiatné lepsi' než deterministický  
 - množství opakování → lepsi' kvalita

- poskytuje očekávanou (střední) hodnotu charakteristické veličiny (kvality, času)
- platí pro jakýkoliv rozlož.

## Experimenty



- ▷ je typický algoritmus A nbo B
- ▷ je typické pro praktické instance
- 

## Instance

- metodické generování
- generování s ohledem na experiment
- standardní benchmark

## Hodnotime

- kvalita řešení
  - u známých řešení můžeme absolutně
  - u neznámých pouze relativně
- výpočetní náročnost
  - (- počet testovaných stavů)
  - je-li v něm mnoho externích ovlivů
- měříme nejlepší / nejhorší / průměrný případ

## White box evaluation

- omezení sady instancí, ohled do algoritmu
- detailnější měření
- možnost upravit heuristiky

## Black box evaluation

- plná sada instancí
- ověření kvality výsledků / výkonu

## Parametry

- obecně nejsou známkami / pokud ano, musíme ho respektovat
- případná známkost je nutná očekávat

## Vyhodnocení

- randomizovaná data → řád → množství může mít vliv
  - (?) byl naměřen dostatek dat (instancí)
  - (?) při se data chovají tak, jak se chovají
- využijeme jsou kvalifikativní data  
→ maticovou kohesií verifikují kvalifikativní

PříkladyZaujala procházenka (Walk SAT)

- náhodný maslav všechny ma 0/1 (50%)
- S pravděpodobností  $0 < p < 1$

$p$ : nejdříji náhodnou nesplněnou klauzuli  $\rightarrow$  případ, aby byla splněna

$1-p$ : případ, jehož pravděpodobnost je tak, aby bylo splněno co nejvíce (MAX SAT)

$\rightarrow$  opakuji ( $uvažuju p mezi 0,5 a 0,6$ )

3-sat

- maslav náhodně
- obkroužit všechny obdržené pořadí jedné proměnné, opakuji

Náhodná procházenka

- ji můžu kvalitní odhadovat pravděpodobnost zaujít  $p$



## Princip lokálních heuristik, pojem globálního a lokálního minima, obrana před uvážením v lokálním minimum

globální vs. lokální metody ← dle momentální instance vybíráme půšť  
zadání instance konstruujeme z některého dřívejšího instance

štěstí algoritmu → dřívejší stavu (všechny stavy dosažitelné z tohoto)

→ sousední stavy = patří do dřívejší stavu

( $k$ -dřívejší stavu - dosažitelné až  $k$  krohy)

⇒ graf stavového prostoru      × pravidlo prohledávání

- všechny konfigurace v půdívku sledování  
(i když neplatí)

- ▷ Lokální minimum - všechny sousední stavy mají horší hodnotu optimizačních kritériia
- ▷ Globální minimum - všechny

strategie prohledávání:  
úplná strategie - check everything except worthless  
systematická strategie - nothing more than once

Heuristické funkce: každý stav má hodnotu → preferují by s větší (lepší)

- ~~co~~ nejlípe odhadnutá (může i obecně větší k nejlepšímu)
- používána v praxi, omezení a rychlosť, ...

Greedy heuristika: - always local optimum → hope for global one

↳ konstrukční heuristiky → z kritické konfigurace konstruují řešení

iterativní heuristiky → postupně vyhodnocují řešení z nejakejšího existujícího

& dvojkrokové heuristiky

## Princip lokálních heuristik

- vybíráj stav v ohledu na jednu je lepší, uloží si ho
  - houčeky jsou pod nimi opt. kritéria nebo po čase či počtu houčků
- ▷ výhodná procházka → jehož holič souseď
- neni úplná ani systematická
- ▷ best - only → nejlepší souseď
- neni úplná a je greedy
- ▷ first improvement → první lepší souseď
- neni úplná (a ani greedy!)
- ▷ Kernighan - Lin
- řešení dělají v každém kroku  
více transformací bez ohledu na heuristiku  
či optimalizační funkci

## Únik z lokálního minima

postupy překonání:      jehož holič (neřešenají)  
                                ↳ návratem  
                                jehož cíl (př. simulované ochlazování, tabu search)

- rozšíření prohledávaného okruhu
- stoup k mělkým místním minímum
- návrat ze špatných větví (back-tracking)
- povolení horšího řešení (př. sim. ochlazování)
- resubstiční opatření (tabu search)
- návrat nájednotou (GA)

# MI-SPOL - 9 (MI-PAA)

## Princip genetických algoritmů, význam selekčního kritéria pro jejich funkci

konfigurace - jedinec (fénotyp)

kódování - genotyp, chromozom

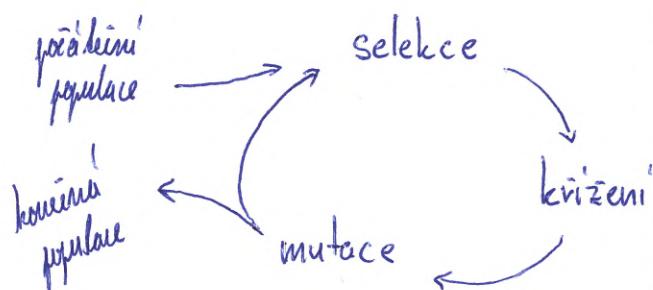
mnожina konfigurací → generace, populace

- binární operátory - mutace, binární operátory - křížení

- optimalizační kritérium - fitness

→ degenerace - uvolnění z lokálního minimu

konvergencie - dosažení kvality populace



Genetický algoritmus - binární řízec  
Genetické programování - rozkladový řízec, vyjádření  
Evoluční programování - autonome řízení  
Evoluční strategie - vzhled R číslo a jejich vlivy na řízení

### 1. selekce

- ovlivňuje selekčním kritérem

↳ konvergencie kritériu

- příčinu množstva selitu jedinců

### 3. mutace

- různé metody

- náhodná invaze jedinců do řízení

- zlepšují průběžné konvergenci

### 2. křížení

- význam informací muri jedinci

- jednotlivci, dvojbolestci, uniformní

(+ permutace)

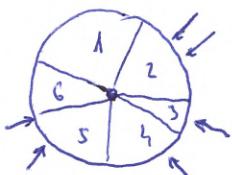
Selektivní tlak - pravděpodobnost výběru nejlepšího jedince

vysoký tlak - nebezpečí degenerace

nízký tlak - pomalá konvergence

- výběr jedinců v další populaci:

▷ Rulebný výběr



- vybereme n pořadí z náhodných čísel  
- mítkaři můžeme i vikend

▷ Universální stochastické výběrování

- kolci jako u ruleby - vyberem náhodný bod  
→ od kohoto bodu n-1krát úhel  $2\pi/m$

→ u obou ji třeba množozad slabším (scaling)

- jinak hrozí degenerace

▷ Turnajový výběr - náhodné r jedinců a z nich nejlepší

→ zahrnuje n kralík až do naplnění populace

- selektivní tlak ovlivňuje velikost turnajů

Řízení populace - uplynutí měsíce

- číslování měsíce

- ustálěna populace - nabízení nej slabších

Elicitivní - nejsilnější výběr první

Ukončení: první počet generací V konvergence

Relaxace - finalizace a připravení řešených řešení

→ oprava řešených řešení

řešení mutace: disaster, gen. náhodných poloh, adaptivní mutace

## Princip simulovaného ochlazování, význam parametrů a způsoby jejich řízení

Řízení smíšení z lokálních minim

- diverzifikace - rozšiřující průzkum pracovního prostoru
  - $\times$                     ← velká chvíla přijetí akci, která vede k horšímu řešení
  - intenzifikace - konvergencie ke finálnímu řešení
- 

- analogie k klasické kavrnině

$\rightarrow$  prohledávání prostoru: rovol náhodného souseda

→ pokud je lepší, přijmeme ho

→ pokud je horší, přijmeme ho na základě zhoršení a kroků

zhoršení  $\rightarrow$  kroků

pravděpodobnost přijeti horšího:  $\text{rand}(0,1) \leq e^{-\delta/T}$

- $\Rightarrow$  1. nejubtí zhoršení přijmu často  $\times$  velké zhoršení
- 2. se stoupající krokůmi zmenší běrovětnejsí

- počítačem slav

vygenerovaný jinou konstruktivní heuristikou  
náhodné řešení

- vysoké krokůy  $\rightarrow$  diverzifikace
- nízké krokůy  $\rightarrow$  intenzifikace

parametry algoritmu:

počítačem kroků

cool ( $T$ )

frozen ( $T$ )

equilibrium (...)

} rozsah ochlazování

cool (T) - určuje rychlosť mixovania telodôby (velkosť roviny)

$$\text{cool}(T) = \alpha T, \quad 0,8 < \alpha < 0,999$$

equilibrium () - počet kroku pred (nuci ochlazovanie)

- prvný počet kroku N
- N pôjazdových a mbo 2N kroku

### Počítačmi teloda

→ nastavime ľubovoľne tak, aby bola pravdepodobnosť minima 0,5

#### - Zjednodušenie riadenia

- vysújeme telodôbu a sledujeme čiernosť pôjazdových krištof
- nastavime tak potrebujeme teloda na 0,5

### frozen() - konec algoritmu

- prvej danej telodôbe mbo ale pôjazdových krištof ci počtu krištof hoci hovorí
- moc vysoké - najem ustálen a pôjazdového sústavu'
- moc nízke - zbytočné prehľadávanie dňa do minimum bez výplní'

### Viacero výpočtu pred ~~equilibrium~~ equilibrium (počet kroku)

- vysoký - zbytočné dňa do prehľadávania
- nízky - nízko výkonnosť a hoci minimum ← užostatkové prehľadávanie prostoru

### Koeficient ochlazovania - počet (a veľkosť!) telodôb krokov

- obvykle číslo v intervale  $\langle 0,8 ; 0,999 \rangle$
- ~~vysoké~~ → "naberajte prehľadové nízkejší farebné"

### Nepôustné kresť

- relaxuje podmienky a pôjazdové nepôustné stavu'
- možno sa napr. opraviť heuristikou

# Výkonnostní měřítka paralelních algoritmů, PRAM model, APRAM model, škálovatelnost

$T_A^K(n)$  - časová složitost seq. algoritmu A, řešícího problem K  
 velikost vstupních dat

$SL(n)$  - spodní mez časové složitosti (kritická dílina velikosti n)

$SU(n)$  - horní mez nejlepšího existujícího algoritmu

$T(n, p)$  - paralelní čas  
 počet procesorů (jader, vláken)

$$\underline{\text{Paralelní rychlémí:}} \quad \boxed{S(n, p) = \frac{SU(n)}{T(n, p)} \leq p}$$

$$\rightarrow \text{lineární pokud } S(n, p) = \Theta(p)$$

- superlineární rychlémí ...

$$\underline{\text{Spodní mez:}} \quad \boxed{L(n, p) = \frac{SL(n)}{p}}$$

$$\underline{\text{Paralelní cena:}} \quad \boxed{C(n, p) = p \cdot T(n, p)} = \Omega(SU(n))$$

$\rightarrow$  cenově optimální algoritmus pokud  $C(n, p) = \Theta(SU(n))$

Paralelní efektivnost:

$$\boxed{E(n, p) = \frac{SU(n)}{C(n, p)} = \frac{S(n, p) \cdot T(n, p)}{p \cdot T(n, p)} = \frac{S(n, p)}{p} \leq 1}$$

- algoritmus je konstantní efektivní

$$E(n, p) \geq E_0 \text{ pro } 0 < E_0 < 1$$

cenová optimalita  $\Leftrightarrow$  lineární rychlémí  $\Leftrightarrow$  konstantní efektivnost

$$T_A(n) = \Theta(SU^K(n)) = \Theta(SL^K(n))$$

"analytický optimální algoritmus"

## PRAM Model

- [ RAM model - Random access machine ]
- instrukce s jednotkovým časem
  - časová složitost = počet provedených instrukcí
  - paměťová složitost - počet použitých buněk největší řady

PRAM: množina p procesorů

- $\forall$  procesor má index a lokální paměť
  - v sdílených paměťových buněk - každý má do jakékoliv access v  $O(1)$   
→ konflikty se musí explicitně řešit
  - typy operací: READ, WRITE, LOCAL
- ↳ jednotkový model: všechny operace trvají 1  
globální model: L trvá 1, R/W konst. čas  $d > 1$

EREW - PRAM - žádne dva procesory nemají R/W do stejné buněky současnou

CREW - PRAM - člení vše majichou je povolen

CRCW - PRAM - i zapis je možný majichou

- common - všechny zapisované hodnoty musí být stejné
- priority - první přidělený priority každému procesoru
- arbitrancy - náhodný pořadí

## APRAM Model

- asynchronní spracování
- je nutná explicitní synchronizace barierou
- není jednotkový čas přístupu do sdílené paměti
- výpočet: posloupnost globálních fází oddělených barierou

Parallelní řešitelnost

- schopnost par. algoritmu obecně parallelní optimality půjčená následkem par.

Silná: jde klesá  $E$  půjčením následkem par., slabá: půjčení p. a následek n.

Ahojatlivý ráhon sítovace parallelace

rozhodnutí nemůže přeslouhovat

$$S(n,p) = \frac{\overbrace{T(n)}^{f_s \cdot T(n) + \frac{1-f_s}{p} \cdot T(n)}}{f_s \cdot T(n) + \frac{1-f_s}{p} \cdot T(n)} = \frac{1}{f_s + \frac{1-f_s}{p}} \leq \frac{1}{f_s}$$

inherenční nákladní podíl úloh → parallelní podíl

př.  $f_s = 10\% \Rightarrow S(n,p) \leq \frac{1}{0,1} = 10$  pro jakékoli  $p$

Gustavsonův ráhon

$$S(n,p) = \frac{t_{seq} + t_{par}(n,1)}{t_{seq} + t_{par}(n,p)}$$

"js. roštuje p. musíme sítovat i velikost problému  $n$ "

- inherenční nákladní část bude  $t_{seq}$  (konstantní)

→ inherenční parallelní část bude lineárně řešitelná

~~MI-SPOL-6~~

(MI-SAA)

~~Vyznam trid NP a NPH~~ ~~pro praktické využity~~

Programový model nad sdílenou pamětí: OpenMP

(paralelní regiony, paralelní vlákna, datový a funkční parallelismus, paměťový model, synchronizační nástroje)

paralelní systém se sdílenou pamětí (Symmetric multiprocessing - SMP), UMA

- komunikace pomocí R/W operací

paralelní systém s distribuovanou pamětí (NUMA)

- komunikace prostřednictvím reprez.

OpenMP - hliníková <sup>pro</sup> programování nad sdílenou pamětí (memuji distribuovanou)

- vybrane režie užívání pro paralelizaci → paralelní regiony

- pomocí fork-join mechanismu jsou růle vytvářena, prováděna a ukončena paralelní vlákna
- mimo existující pouze master vlákno (může využívat pool pro ručení režie)
- programátor je zadováván k thread - safe programu

Model volnéjší konzistence

- vlákna mohou dvěma různými hodnoty aktualizovat a nemusí být konsistentní
- explicitní operace flush()

- paralelní region definován direktivou parallel

- na konci implicitní bariera

if (cond) - podmínka paralelizace

num\_threads - počet vláken v par. regionu

vlastnosti (var) - vlastnosti proměnných

▷ shared - sdílená mezi vlákny

▷ private - lokální ve vlákně (uncle)

▷ firstprivate - lokální ve vlákně s hodnotou, kterou měla v hlavním vlákně

▷ lastprivate - (ugly) - hodnota je staticky poslední iterace ven z par. regionu

▷ default - uvažuje implicitní vlastnost všech proměnných

▷ reduction - reduction (operator: variable)

- statikální proměnné a nepřekrývající operátory

- lineární a logaritmická

## Datový parallelizmus

- direktiva `for` → na konci cyklu je implicitní bariera
- direktiva `schedule`:
  - static - rozděl rovnoměrně mezi vlákna, ↓ chunk-size rozděl po kac velkých kusech
    - rozdělování bloky jsou pro vše jednotné (stejně u všech) ← nejmenší rozdíl, ideální pro stejné veliké kusy
  - dynamic - dynamické rozdělování → velikostí chunk-size mělo 1 ← kolisau' silnou
  - guided - dynamicky přiřazuje max ( $\lceil \# \text{dosaž} \text{ nepřidělených}/p \rceil$ , chunk-size)
  - auto - záleží na komplikaci a OS ← rozdílnou' složitost
- + `collapse()`, `nowait`

## Funkční parallelizmus

- direktiva `task` pro vykárení úloh - vhodné pro D&C algoritmy
- vlákna jsou producenti i konzumenti úloh

`taskwait` - čeká na dokončení úloh z daného par. regionu

`task-if` - podmínka vykárení úloh

`single / master` - kód je proveden pouze jedním město master vláknu

## Synchronizační nástroje

`barrier` - všechna rámce musí dorazit

`master, single`

`critical` - vykárení kritické sekvence provádění pouze jedním vláknu (může být pojmenováno)

`atomic` - atomická paměťová operace

`read, write`

`update` - `read, write and modify`

`capture` - rozšíření update → možnost různám dané proměnné (před město po)

{  
   $my\_ptr = ptr ; ptr + BLOCK\_SIZE$ }

`cancel` - ukončení paralelního regionu a vrak na zadánou barieru  
- ostatní' posírají do same'

Programový model nad distribuovanou pamětí : MPI  
(procesy, komunikátory, 2-bodové a <sup>skupinové</sup> komunikační operace, blokující a neblokující operace a jejich komunikační módy)

## Hybridní MPI + OpenMP model

MPI - Message passing interface → standard rozhraní mezi programy paralelních programů

- pracuje nad distribuovanou pamětí (NUMA)
  - každý proces je vždy součástí atespon jedné skupiny (číslování od 0 do # - 1)
    - v každé skupině obecně jiné číslo

Komunikology - sociální (parametr) kritické komunikační operace

- výměna mezi dvěma procesy probíhá komunikací - MPI\_COMM\_WORLD pro všechny procesy
  - mezi (vnitřní) a mezi (mezi vnitřními)

`MPI_Comm_rank` - číslo procesu v dané skupině

MPI\_Comm\_size - počet procesů dané skupiny

## Kommunikācijas operācijas

- Z jednotek - merí dvěma procesy
  - kolektivní - vstupuje s daným komunikátorem
  - blokující - čeká se na splnění určité podmínky
  - neblokující - hraje chomutík - může odstoupit později

**MPI-Send** (\*buff, count, MPI-Datatype, dest, tag, comm) ↗ library process

**MPI\_Recv** (\*buff, count, MPI\_Datatype, src, tag, comm, &status)

typ daných přemíšťových dat  
[MPI-INT, MPI-DOUBLE, ...]

```

graph TD
    subgraph MPI_ANY_TAG [MPI-ANY-TAG]
        direction TB
        A[od jidi] --> B["lovi proces  
ag, comm"]
        B --> C["tag, comm, & status"]
        C --> D["soubhazejici source  
a tag prijizi reprezov"]
        D --> E["[MPI-STATUS-IGNORE]"]
    end

    subgraph MPI_ANY_SOURCE [MPI-ANY-SOURCE]
        direction TB
        F[od koho muzim prijimat]
        F --> G["[MPI-ANY-SOURCE]"]
    end

```

- reální klasické Mohorjevičovy operace (= buffered nerozvážné synchronizace)

MPI - Bsend - buffered  $\rightarrow$  ulozimí do systémového bufferu (vezávem na cíl)

MPI\_Ssend - synchronous → konieczne kiedyś proces inicjujący przesłanie

MPI - Rsend - ready mode  $\rightarrow$  přijem se může být iniciován, jinak konec s chybou

- všechny operace mají i neblokující variantu (MPI\_Isend, MPI\_Ibsend, ... )
  - musíme explicitně volat blokovací operace
  - buffer do té doby nelze modifikovat
- funkce mají sladcejší parametry MPI\_Request
  - MPI\_Test, MPI\_Wait & ... any, ... all pro hromadné operace
- společná MPI\_Sendrecv
- MPI\_Probe - kontrolouje přítomnost

### Kolektivní komunikaci operace

- 1:N → one-to-all broadcast - MPI\_Bcast (stejný multicast)
- one-to-all scatter - MPI\_Scatter
  - all-to-one gather - MPI\_Gather - shér dle ade všech
    - poslechující dřív se liší počet ve směru, latence jsou stejné

N:N

- all-to-all broadcast
- = all-to-all gather - MPI\_AllGather
- all-to-all scatter - MPI\_Alltoall

### Hybridní model MPI + OpenMP

- v rámci jednoho výpočetního uzel / procesoru běží jenom několik MPI procesů, každý ještě má místní vlákna pomocí OpenMP
- 1. proces má jenom výpočetní uzel → ještě má celý uzel
- 2. proces má každý procesor (tj. socket) → lepší přístup ke sítové paměti
- musíme inicializovat pomocí MPI\_Init\_thread na pořadovou míru polyfunkce
  - MPI\_THREAD\_SINGLE - nedělíme se na vlákna
  - MPI\_THREAD\_FUNNELED - pouze hlavní vlákno může volat MPI funkce
  - MPI\_THREAD\_SERIALIZED - MPI funkce můžou jen jednu chvíli volat jen jedno vlákno
  - MPI\_THREAD\_MULTIPLE - všeobecný model

Právě ortogonální a hyperkubické propojovací sítě paralelních počítaců (definice, vlastnosti, využití)

- $V(G), E(G)$  - množina vrcholů a hrany grafu
- $N = V(G)$  - velikost grafu,  $\langle u, v \rangle$  - hrana grafu
- $\deg_G(u)$  - stupeň vrcholu ( $\#$  sousedů)
  - maximální stupeň grafu  $\Delta(G)$ , minimální stupeň grafu  $\delta(G)$   
→ k regulárnímu grafu:  $\Delta(G) = \delta(G) = k$
- Excentricita vrcholu  $exc(u)$  - vzdáenosť nejvzdálenějšího vrcholu
- Průměr - největší excentricita grafu
- Poloměr - nejmenší excentricita grafu

Topologie  $G_n$  - množina grafů, jejichž velikost a struktura je definována parametrem  $n$   
- hierarchicky rekurencí → instance menších dimenzi jsou podgrafy větších  
(rekurentní / částkově šířkovitelné topologie)

Ridlejši topologie  $|E(G_n)| = O|V(G_n)|$  → stupně vrcholu jsou omezeny konstantou

Hustejši topologie  $|E(G_n)| = \omega|V(G_n)|$  → — " — rozsah  $\propto n$

Konkrétní součin  $G = G_1 \times G_2$

- komutativní a asociativní operace zachovávají symetrii (určovou)

$$V(G) = \{[x, y]; x \in V(G_1), y \in V(G_2)\}$$

$$E(G) = \{\langle [x_1, y_1], [x_2, y_2] \rangle; \langle x_1, x_2 \rangle \in E(G_1)\}$$

$$\cup \{\langle [x_1, y_1], [x_1, y_2] \rangle; \langle y_1, y_2 \rangle \in E(G_2)\}$$

- vrchol symetrický graf:

$$\forall u_1, u_2 \in V(G), \exists \text{ automorfismus } f \text{ takový, že } f(u_1) = u_2$$

- všechny vrcholy symetrické grafy jsou regulární

## Požadavky na PSPP

- Symetrie a hier. rekurenciha (niveli)
- vysoká souvislost, binární říška
- konstantní stupen vrch (cena)
- malý průměr a primární rozdílnost
- možnost jinam

Orbionální sítě - horizontální součin  $\rightarrow$  hierarchický rekurenciha  $Q_n$ : 

□ Binární hyperkrychle dimenze  $n$ ,  $Q_n$

- $|V(Q_n)| = 2^n$  deg =  $n$  - niv. řídká (deg. stupen vrch)
- $|E(Q_n)| = n2^{n-1}$  diam =  $n$  - hierarchický rekurenciha
- $\exists 2^n \times n!$  automorfismů (přezem, permutace) - největší možná binární říška ( $2^{n-1}$ )  $\rightarrow$  D&C
- částečně šikovatelné  $M$  

□  $m$ -normální mřížka rozměru  $m_1, \dots, m_n$   $M(m_1, \dots, m_n)$

$$|V(M)| = \prod_{i=1}^n m_i$$

$$|E(M)| = \sum_{i=1}^n (m_i - 1) \cdot \prod_{j=1, j \neq i}^n m_j$$

-  $M(k, k, \dots, k)$  - k-dim m-krychle

- mříž regulární  $\rightarrow$  mříž určová symetrická

- hierarchický rekurenciha

$$M(m_1, \dots, m_n) = M(m_1) \times M(\dots) \times M(m_n)$$

- topologicky optimální  $\exists$  pro mnoho různých problémů

- hamiltonova kružnice počet alespoň jedna strana je sudá

□  $m$ -normální kroužnice dimenze  $m_1, \dots, m_n$   $K(m_1, \dots, m_n)$

=  $m$ -normální kružnice, základna mřížka

- je určová symetrická

$$|V(K)| = |V(M)|$$

$$\text{deg} = 2m$$

$$- K(m_1, \dots, m_n) = K(m_1) \times \dots \times K(m_n)$$

$$|E(K)| = n \times \prod_{i=1}^n m_i$$

$$\text{diam} = \sum_{i=1}^n \lfloor m_i/2 \rfloor$$

- kompromis mezi MaQ  $\rightarrow$  nejlepší

- polární průměr, diagonální binární říška

## Bílké hyperkubické sítě

- maximální hředlovo ucelu hyperkubické do víc ucelů
  - počet po hraně může měnit všechny dimenze'

□ Zabalený možnosti dimenze n,  $wBF_m$

$$V(wBF_m) = \{(i, x); 0 \leq i \leq n \wedge x \in B^n\} \quad |V| = n2^m$$

$$E(wBF_m) = \{\langle (i, x), (i \oplus_n 1, x) \rangle, \quad |E| = n2^{m+1}$$

má i jednotlivými uceli  $\rightarrow \langle (i, x), (i \oplus_n 1, \text{neg}_i(x)) \rangle \mid (i, x) \in V(wBF_m) \}$

$$\deg = \text{h}, \quad \text{diam} = n + \lfloor \frac{m}{2} \rfloor, \quad bw_e = 2^n$$

- ucelově symetrický, není hierarchicky rekursivní'

□ Obyčejný možnosti dimenze n,  $oBF_m$  (jeden uzel má násobky na dva)

$$V(oBF_m) = \{(i, x); 0 \leq i \leq m \wedge x \in B^n\} \quad |V| = (m+1)2^n$$

$$E(oBF_m) = \{\langle (i, x), (i+1, x) \rangle, \langle (i, x), (i+1, \text{neg}_i(x)) \rangle \mid i \leq n \} \quad |E| = m2^{n+1}$$

$$\deg = \{2, \text{h}\}, \quad \text{diam} = 2n, \quad bw_e = 2^n$$

- není ucelově symetrický, je hierarchicky rekursivní'
- jistina 'reprezentace' cesty  $\rightarrow$  permutací sítě'

(první a naposledy navštívený uzel  $\Rightarrow$  mikrováci sítě')

(douměření možností & hustý strom)

• Lineární pole / kružnice kružnic load = 1    eng = 2  
dil  $\leq 3$

- sestojím hoden grafe a procházím ji DFS  
 $\rightarrow$  uzel umístěn do ucelu v lince uvedený průměrnou naostřit a udej průměrnou poslední'

Vnořování = Embedding problem

$G \rightarrow H$

mínimální kvalita vnořování:

$\varphi: V(G) \rightarrow V(H)$

$\xi: E(G) \rightarrow P(H)$

minimální všechny cesty

load ( $\varphi, \xi$ ) = maximální rážíkum' cílového vrcholu

→ kolik procesů běží na jednom vrcholu

vcnp ( $\varphi, \xi$ ) =  $|V(H)| / |V(G)|$

dil ( $\varphi, \xi$ ) = maximální dilatace → jak daleko jsou od sebe sousední vrcholy

ecng ( $\varphi, \xi$ ) = maximální rážíkum' cílového hrany  
→ rážíkum' cílového kanálu

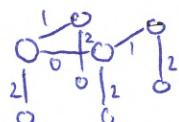
- hranicomebrické grafy - jich má obě strany vnořit s konstantními méněkými
- ⇒ vypočítat ekvivalence (konstantní rozdíl) - neplatí například ~~XX~~

-  $H$  simuluje  $G$  se rozdílem  $\eta$  ještěže jeden krok a  $G$  simulují se  $O(n)$  kroků má  $H$

(průměrný argument)

$$|V(G)| = |V(H)| \wedge \text{load}(\varphi, \xi) - 1 \Rightarrow \text{dil}(\varphi, \xi) \geq \lceil \text{diam}(H) / \text{diam}(G) \rceil$$

### ◦ D&C na hyperkubech (hyper)



- normální hyperkubický algoritmus
- rozděluj a půlku si nech

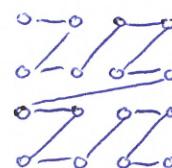
### ◦ $M \leftrightarrow K$ = load = 1, dil = ecng = 2 ( $K \rightarrow M$ )



- opačně binární

### ◦ hyperkubické → mřížky / toroidy

Mortonova kódovka - spojujeme vrcholy v leh pořadí: shidaví x a y



### ◦ 2D toroid do 1D toroidu

$$\text{load} = 1, \text{dil} = \min(m_1, m_2), \text{ecng} = \text{dil} + 2$$

- 2D toroid si představíme jako mřížku
- mapujeme po řádcích / sloupcích

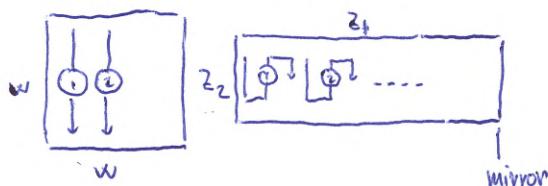
### ◦ obdélník do čtverce

obdélník do čtverce

$$\text{dil} = 1$$

$$\text{load} = \text{ecng} = 2$$

### ◦ čtvercová mřížka do obdélníkové



$$\text{dil} = \lceil \sqrt{z_1 z_2} \rceil \quad \text{load} = 2 \quad \text{ecng} = 1 + \text{dil}$$

Paralelní redukce, prefixový součet, segmentový prefixový součet na PRAM, ortogonálních a hyperkubických sítích, v OpenMP a MPI

### Paralelní redukce

- osoby ji požadují asociativní (a komutativní) operace  $\oplus$
- výstupem globální redukovaná hodnota

$$\text{Paralelní čas: } \alpha \frac{n}{p} + \beta \cdot \log p = T(n, p)$$

$$\text{Dolní mez: } L(n, n) = \Omega(\log n)$$

- normální hyperkubický algoritmus

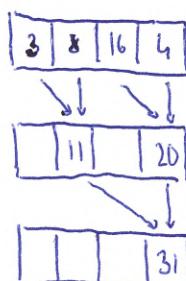
### OpenMP:

#pragma omp reduction (+: result)

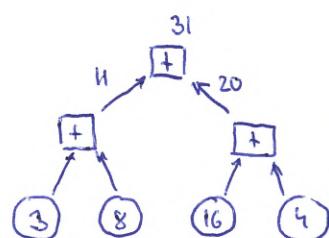
- může se konat rekurencí, nebo ~~rekurencí~~ logaritmicky

$$\hookrightarrow T(n, p) = \alpha \cdot \frac{n}{p} + \beta \cdot p$$

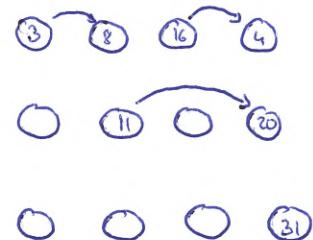
### EREW PRAM:



nejlepší - tj. hodnoty pouze v lince  
uplynou binárním stromem:



### WH 1-D maticha



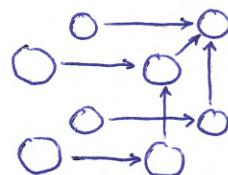
### MPI\_Reduce: - dokládají operace odle všech větších mě

- MPI\_IN\_PLACE - mě se slije souběžně novým bufferem

- MPI\_SUM, MPI\_MAX, ...

(+ MPI\_Allreduce)

### SF Hyperkubické



## Paralelní průchody součet

- asymptoticky jde o redukci, ale více operací

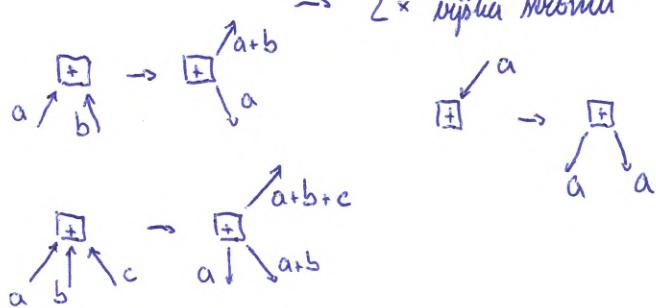
### EREW PRAM:

3	2	4	7
\	\	\	\
3	5	6	11

- možné hodnoty si musí mít identické
- postupně sčítám čísla ve vzdálostech  $2^0, 2^1, 2^n$

### recuprový strom:

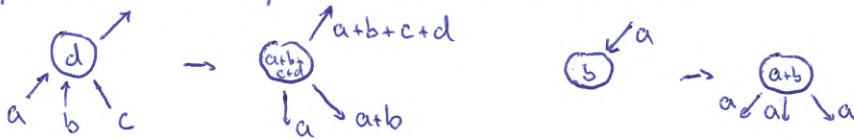
- uplynutí binárního stromu:  $O(\log n)$  kroků
- $2 \times$  výška stromu



### PPS na prvním stromu:

?✓

- procházejeme stromem v postorderovém pořadí (lineárisace)



- lze aplikovat na jakékoli topologie  
→ zhouskávajeme kostry do řady a postorderově ...

### Hyperkyrkule

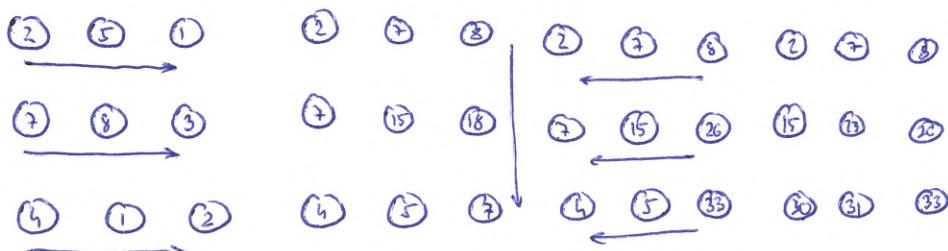
- vrty uspořádání leitografických

- postupně procházím dimenze po dimenzi a dělám uspořádání AAB

- dvě proměnné - v jedné max hodnota, v druhé máj součet  
→ ke moi původním posetům přejde správa z leitografického nízšího vrstu  
→ ke maxu vrstvy, poslední je max

### SF Mřížky

- řádkové leitografické po řádcích



## Škalovatelnost na více CPU

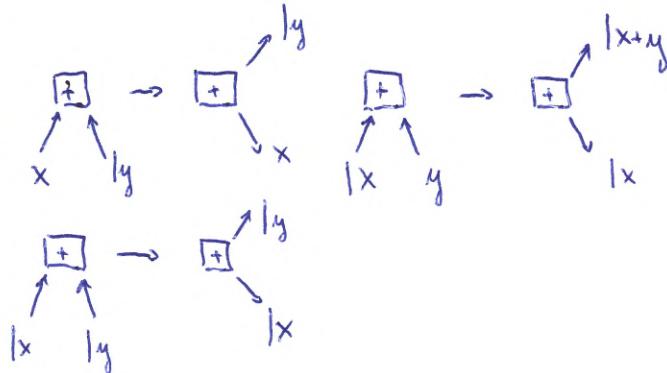
- lokální součty  $\rightarrow$  paralelní globální první součet  
 $\rightarrow$  přechod k lokálním součtem

## Segmentovaný PPS

- PPS musí mít několik segmentů

- upravené operace  $\oplus$

$\bar{\oplus}$	b	$ b$
a	$a \oplus b$	$ b$
$ a$	$ (a \oplus b)$	$ b$



MPI\_Scan - PPS implementace

MPI\_Exscan - exkluzivní (bez možnosti hadnoty)

- funguje jinak stejně jako MPI\_Reduce



Testování statistických hypotéz. T-testy, testy nezávislosti, testy dobré shody.

statistická hypotéza - pohled o měření

~~představitele~~ - <sup>hypotéza</sup> předpady kryjící se hodnoty parametrů rozdělení měř. vel.

✗ neparametrické

→ maximem ověřit a výjádřit o pravdivosti

$H_0$  - nulační hypotéza &  $H_1$  - alternativní ( $H_A$ )

Statistický test = -  $H_0$  racionálně ve prospěch  $H_1$   
-  $H_0$  může racionálně, ale ani pravdivou

Chyba 1. druhu - hypotéza racionálně platí (dvoucestné rozhodnutí)

✗ 2. druhu

		racionálněm $H_0$	racionálněm $H_0$
platí $H_0$	✓ - pravdivost $1-\alpha$	✗ - $\alpha$	
	platí $H_A$	✗ - $\beta$	✓ - pravdivodost $1-\beta$

Testování statistika: funkce měř. veličiny  $X$  ( $T=T(X)$ ) u které při plánosti  $H_0$  může jít rozdílení

Postup měřidelného testu: předpokládám  $H_0$  platí → vymysletím měřidelný počet a co bude výsledkem  
→ stanovitne hladina zpětnivosti  $\alpha$  (pl. chyby 1. druhu)

→ kritický obor  $W$ : tř. část oboru hodnot kamen podle výsledku na plánosti  $H_0$  s počtem  $\alpha$  ( $W_\alpha$ )

→ pokud podle výsledku do kritického oboru, racionálně  $H_0$  má hladinu  $\alpha$

$$p\text{-hodnota} : \hat{p} = \hat{p}(X) = \inf \{\alpha \mid X \in W_\alpha\}$$

Studentovy t-testy = porovnání střední hodnoty  $\mu$  s konstantou  $H_0: \mu = \mu_0$

při racionálném rozptylu  $\sigma^2$   $H_0$  racionálně, pokud  $\mu_0$  patří do intervalu

$$\bar{X}_n = \frac{1}{n} \sum X_i$$

$$\left( \bar{X}_n - z_{\alpha/2} \frac{\sigma}{\sqrt{n}}, \bar{X}_n + z_{\alpha/2} \frac{\sigma}{\sqrt{n}} \right)$$

$$S_n^2 = \frac{1}{n-1} \sum_{i=1}^n (X_i - \bar{X}_n)^2$$

výběrový průměr

kvádrat. hodnoty stand. norm. rozdělení  $N(0,1)$

výběrový rozptyl

pro normální rozptyl:

$$\left( \bar{X}_n - t_{\alpha/2, n-1} \frac{S_n}{\sqrt{n}}, \bar{X}_n + t_{\alpha/2, n-1} \frac{S_n}{\sqrt{n}} \right)$$

směrodatna' odchylnka'

kvádrat. hodnota studentova rozdělení  $t_{n-1}$   
 $\rightarrow n-1$  stupni volnosti

pro jednostranné podobné  $(\bar{X}_n - z_{\alpha} \frac{\sigma}{\sqrt{n}}, +\infty)$  ...

Test:  $H_0: \sigma^2 = \sigma_0^2$  proti alternativě  $H_A: \sigma^2 \neq \sigma_0^2$

$$\left( \frac{(n-1)s_n^2}{\chi^2_{\alpha/2, n-1}}, \frac{(n-1)s_n^2}{\chi^2_{1-\alpha/2, n-1}} \right)$$

kritická hodnota rozdilu  $\chi^2$  s  $n-1$  stupni volnosti na hladině  $\alpha/2$

Testová statistika: reálný rozptyl  $\sigma^2$ : vernátný rozptyl:

$$T = \frac{\bar{X}_n - \mu_0}{\sigma / \sqrt{n}}$$

$$T = \frac{\bar{X}_n - \mu_0}{s_n / \sqrt{n}}$$

Parový t-test - součinné dvojice měření, které majou mezi sebou

- množství výběrů:  $((x_1, y_1), \dots, (x_n, y_n))$

- kritické hodnoty rozdílu  $\mu_1$  a  $\mu_2$  (kritické hodnoty)

$$H_0: \mu_1 - \mu_2 = d \quad X \quad H_A: \mu_1 - \mu_2 \neq d$$

- ~~je~~ pracuje stejně jako jednozávislostní t-test

$$\bar{Z} = \bar{X} - \bar{Y}$$

testová statistika:

$$T = \frac{\bar{Z} - d}{s_Z} \cdot \sqrt{n}$$

Dvouzávislostní t-test - pro dvojice, které jsou nezávislé

- obě veličiny mají stejný (lidově vernátný) rozptyl  $\sigma_1^2 = \sigma_2^2$

$$H_0: \mu_1 - \mu_2 = d \quad X \quad H_A: \mu_1 - \mu_2 \neq d$$

$$T = \frac{\bar{X} - \bar{Y} - d}{\sqrt{\frac{(n-1)s_x^2 + (m-1)s_y^2}{n+m}}} \cdot \sqrt{\frac{m \cdot m \cdot (m+n-2)}{n+m}}$$

vyběrový rozptyl  $\times$  velikost výběru

rozhodujeme, pokud  $|T| > t_{1-\alpha/2}(n+m-2)$

Testy dobrého shody - neparametrický test

- $\chi^2$  - Chi test - rela odhadučka odděluje hodnoty od shutejší je náhoda nebo soubor máloš
- výskytové počty následují s pl:  $p_1, p_2, \dots, p_k$
- $\rightarrow n_1, \dots, n_k$  - četnosti následují po  $n$  nezávislostech počtů

$$H_0: \forall i \in \{1, k\} : p_i = p_i^0 \quad H_A: \exists i \in \{1, k\} : p_i \neq p_i^0$$

$$\chi^2 = \sum_{i=1}^k \frac{(n_i - np_i)^2}{np_i} \quad \text{zamítame, pokud } \chi^2 > \chi^2_{1-\alpha}(k-1)$$

- musí platit pro všechny  $i$ :  $np_i > 5$ , jinak může použít  
(máloš musí být dost, protože je to asymptotický odhad)

Test rozdílosti - mimoře proměnné  $X_1, X_2, \dots, X_n$

- předpokládáme že  $P(X_i = \mu) = 0$
- $$P(X_i > \mu) = P(X_i < \mu) = \frac{1}{2}$$

$N_n = \# míst kde se nepřihodila hodnota  $\mu$  měří experimenty$   
pokud jsou rozdíly platí asymptoticky  $N_n \sim N\left(\frac{n+1}{2}, \frac{n-1}{4}\right)$

$$T = \frac{2N_n - n - 1}{\sqrt{n-1}}$$



## Základy teorie informace a kódování, entropie

Kódování: zobrazení  $C: X \rightarrow D^*$  diskrétní náhodná veličina

$$D^* = \bigcup_{k=1}^{\infty} D^k$$

$D^*$  - množina konečných řetězců symbolů  $\not\in$  - jsou již dány  $D$

obraz  $C(x)$  - kódové slovo  $\rightarrow$  jeho délka  $l(x)$

kódový

Sřední délka ~~čísla~~:  $L(c)$  náhodná veličina  $X \rightarrow p(x)$  rozdělením

$$L(c) = \sum_{x \in X} l(x)p(x) = E l(X)$$

$L(c)$  nemůže být menší než entropie daného textu  $H(X)$

$\rightarrow$  pokud se rovnají, máme optimální kód

### Nesingulární kódy

$\rightarrow$  pokud je zobrazení  $C$  prosté = mohu jednoznačně dekódovat daný kód symbolu  
- nemůže ale platit pro repiky

$$x \neq x' \Rightarrow C(x) \neq C(x')$$

### Jednoznačné dekódovatelné kódy

$$\left[ C^*(x_1, x_2, \dots, x_n) = C(x_1)C(x_2)\dots C(x_n) \right]$$

$\rightarrow$  pokud je  $C^*$  nesingulární

### Instantní (prefixový) kód

$\rightarrow$  rádku kódového slova není prefixem jiného  
 $\rightarrow$  slova reprezentuje kódové slovo, mohu mu dátší

### Huffmanovo kódování

- agreguje vždy nejméně pravděpodobných  $\rightarrow$  rychlé přenášení kódovací
- je optimální: pro Huff. kód  $C^*$  a libovolný unik. dec. kód  $C'$   $L(C^*) \leq L(C')$

## Kraft - McMillan inequality

pro libovolný jednotkový dec. kód musí délky kodových slov splnit nerovnost:

$$\sum_i D^{-l_i} \leq 1$$

|D-čísel abecedy| délky kodových slov

+ pro každou n kici délku splňuje, existuje instanci kód

→ McMillan rozšířil nerovnost i na univ. dekompatibilní

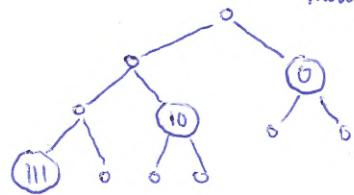
Optimální kódy

$$L(c) \geq H_D(x) \quad \text{entropie} \quad - \text{platí pouze pro instanci (prefiksový kód)}$$

◦ rovnost nastává pokud  $D^{-l_i} = p_i$  pro všechna i

$$H_D(x) = L(c^*) \leq H_D(x) + 1$$

→ optimální kód se vzdálí od dolního meze max o 1



## Entropie - měra neopředstavitelnosti

( pravděpodobnostní funkce  $p(x) \rightarrow \forall x \in \mathbb{R} : p(x) = P(X=x)$  )

$$\text{Entropie } H(x) = \boxed{H(x) = - \sum_{x \in X} p(x) \log_2 p(x)} \quad - \text{ má má min. hodnotu, je na rozdílu, ne na číslných hodnotách}$$

◦ kde  $H_b(x)$  může mít základ logaritmu  $\log_b p(x)$

Entropie je střední hodnota měry neuvěřitelnosti (málo informace)

$$I(x) = -\log_2 p(x) \quad \leftarrow \text{věty neinformační}, \text{ rovná } 0 \text{ u jistých jivů}$$

$$H(x) = \mathbb{E}(I(x))$$

- je nejvyšší pro rovnovážné rozdělení (neobsahuje)

= očekávaná měra neuvěřitelnosti náhodné veličiny H

$$\text{optimální počet binárních složek} = \min H(x) \text{ a } H(x) + 1 \quad (\text{viz optimální kódy})$$

Schurénova entropie  $H(X,Y)$  - entropie souborníku všech měřitelných veličin

$$H(X,Y) = - \sum_{x \in X} \sum_{y \in Y} p(x,y) \log p(x,y)$$

- analogicky se definuje pro měřitelné veličiny

Podmíněná entropie  $H(Y|X)$  - podm. ent. měřitelných veličin  $X, Y$  se schurénovou vlastností

$$H(Y|X) = - \sum_{x \in X} \sum_{y \in Y} p(x,y) \log p(y|x)$$

$p(x,y)$

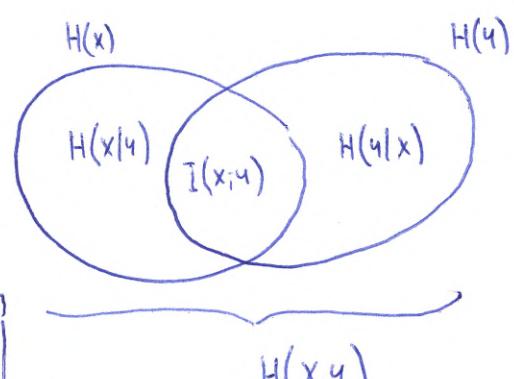
Relativní pravdělo

$$H(X,Y) = H(X) + H(Y|X)$$

$\Rightarrow$  tlerá část informace je v  $Y$  mimo opak  $X$

Relativní entropie (Kullback - Leiblerova vzdálenost)

$$D(p||q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)}$$



Vzájemná informace

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

$$= D(p(x,y) || p(x)p(y))$$

- měra informace, kterou sdílí obě veličiny  $X$  a  $Y$   
 $\rightarrow$  vzdálenost od nezávislosti

$$I(X,Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$$

diferențialul endoscopic ....

## Markovské řetězce s diskrétním časem. Jejich limitní vlastnosti.

Náhodný proces - množina  $\{X_t, t \in T\}$  kde  $X_t$  jsou náhodné veličiny z pravděpodobnostního prostoru  $E = (\Omega, \mathcal{F}, P)$ .

- průběh  $T$  je obvykle indexovaný jako čas
  - diskrétní ( $T$  jsou celá čísla) a spojité ( $T$  je interval  $\mathbb{R}$  či  $\mathbb{N}$ )
  - indexovaná soustava náhodných veličin
  - obecně platí pro  $X(t_1), X(t_2)$  pro některá  $t_1, t_2$  že jsou náhodnosti (= dvě veličiny v některém čase)
  - (realizaci náhodného procesu je funkce nebo řada)
- Homogenní náhodný proces - jeho prav. charakteristiky se s časem nemění  
 → pl. vše se něco stane v příští minuti nezávisí na tom, kolik ji hodin  $P(X_{n+j} = j | X_n = i) = P(X_1 = j | X_0 = i)$
- Číslový proces - bočním událostmi stejněho typu → zajímá nás rozložení v čase  
 platí 1.  $N(t) \geq 0$  2.  $N(t)$  jsou celá čísla 3.  $N(s) \leq N(t)$  pro každý  $s < t$
- Číslový proces bez paměti - nezávisly na historii → např. Poissonův proces

Poissonův proces - každý bod  $t$  máci počítatelný na měřitelný průběh

- počet enších mezi dvěma úseky je nezávislý na ostatních úsecích
- počet reakcí na délku úseku - ne je to ustálené

- jediný parametr procesu je intenzita  $\lambda$

platí: má náhodnosti párnostní

$$N(0) = 0, s < t \Rightarrow N(s) \leq N(t)$$

$$N(s+t) - N(s) \sim \text{Poisson}(\lambda t)$$

= počet událostí v intervalu  $t$  je Poisson. náhodná proměnná se ~~ne~~ svede na hodnotu  $\lambda t$

## Markovské řetězce s diskritním časem

- posloupnost  $X = \{X_0, X_1, \dots, X_n\}$  náhodných veličin se společnou množinou stavů  $S$ , která splňuje Markovskou podmíinku
- je definován: množinou stavů  $S$ , vektorem počátečního rozdělení, matice přechodu  $P$

Irredundantní řetězec - z jakéhokoliv stavu se dostanu do jakéhokoliv jiného

Markovská podmínka: pravděpodobnost budecích stavů je plně určena současným → nezávisí na minulých  
(do menu homogenní vs. nelhomogenní !!)

### o matice přechodu

pravděpodobnost přechodu ze stavu  $i$  do  $j$   $\rightarrow P_{ij} = p(i,j) = P(X_{n+1} = s_j | X_n = s_i)$

→ musíme nastavit matici přechodu

$$P = \begin{matrix} & \begin{matrix} s_j=1 & s_j=n \end{matrix} \\ \begin{matrix} s_i=1 \\ \vdots \\ s_i=n \end{matrix} & \left( \begin{matrix} P_{11} & \dots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{n1} & \dots & P_{nn} \end{matrix} \right) \end{matrix}$$

- matice se dá reprezentovat i diagramem

musi platit:

$$\forall i = 1 \dots n : \sum_{j=1}^n P_{ij} = 1$$

= součet všech řádků je 1 (kazdeho)

o víc-hrokova pravděpodobnost  $P(X_n = s_i | X_0 = s_i) = P_i^n$

- potřebují matice umocnit na  $n$ -hou

Druhy stavů - po opakovaném determinujeme pravděpodobnost naševadlo

$p < 1$  : transitorní stav

$p = 1$  : rekurencní stav

neopustitelný stav = absorbční

Absorbční řetězec = obsahuje mimojíme i absorbční stav (  $P_{ii} > 1$  )

$$\lim_{n \rightarrow \infty} = Q^n = 0 \quad \text{- časem bude určitě počítan}$$

~ transitorní stav

hamiltony kvač matice:

$$P = \begin{matrix} & \begin{matrix} TR & ABS \end{matrix} \\ \begin{matrix} TR \\ ABS \end{matrix} & \left( \begin{matrix} Q & R \\ 0 & 1 \end{matrix} \right) \end{matrix}$$

absorbční stav

jehožkovova matice

$Q_n$  - jst rā po n krocích nebudeme v absorbním stavu

$$P^n = \begin{pmatrix} Q^n & R^n \\ 0 & 1 \end{pmatrix}$$

### Fundamentální matice absorbního řetězce

$$N = (I - Q)^{-1} \leftarrow \text{inverzní matice}$$

↑ jednotková matice

- udává kolikrát proces projde transiente stavy

$$- N_{ij} = E(\text{počet přechodů stavu } j \mid \text{začínáme v } i)$$

### Praostředovnostní matice

- jst rā spadneme do absorbního stavu  $j$  začínáme li v  $i$

$$B_{ij} = P(\text{polohu } s_j \mid \text{začátek } s_i)$$

$$B = N \times R$$

Chapman - Kolmogorova rovnice

matice přechodu

$$\text{platí } 0 \leq m \leq r \in \mathbb{N}_0 \quad P_{(n,r)} = P_{(n,m)} \cdot P_{(m,r)}$$

Stationární rozdělení:

vektor  $\pi$  takový, že:

$$\pi_i \in S \Rightarrow \pi_i \geq 0$$

$$\sum_{i \in S} \pi_i = 1$$

- proces je stationární, pokud jeho horizontální - normální rozdělení invariantní vůči formuli sr čase

$$\& \quad \pi \cdot P = \pi \rightarrow \text{stationární rozdělení řetězce}$$

$$(\pi_1, \pi_2) \begin{pmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{pmatrix} = (\pi_1, \pi_2)$$

- „sr oboustranném horizontu站ární řetězce ve stavu  $j$  průměrné čas  $\pi_j$  (pro všechny  $j$ )“  
„naučíte se počítatím stavu“



Markovské řetězce se spojitym časem. Souvislost s markovskými řetězci s diskrétním časem a s Poissonovým procesem.

- používáme několik malic mimo jeho'

$P_t$  - malice prav. průchozu ze stavu i do stavu j v čase t - časovaný Poissonovým procesem  
 - pruhy malice jsou funkce  $\lambda$  - rádky  $\sum = 1$

$Q$  - malice stokových intenzit

- pruhy malice jsou lambda - intenzity průchozu  $q(i,j)$
- rádky se musí rovnat 0, na diagonále rácky pruhy

Kolmogorovova rovnice

$$\begin{cases} P_t' = Q \cdot P_t \\ P_t' = P_t \cdot Q \end{cases}$$

$U$  - malice diskrétních průchozových pravděpodobností v náhodném čase t  
 - odpovídá průchozové malici  $P$  k diskrétnímu procesu

$$u_{i,j} = (U)_{ij} = \begin{cases} \frac{\lambda_{ij}}{\lambda_{\max}} & \text{pro } i \neq j \\ 1 + \frac{\lambda_{ii}}{\lambda_{\max}} & \text{pro } i = j \end{cases}$$

- rozšiřujeme DMR o to, že můžeme jít dletoho rozstaneme v rámci stavu
  - dan. ráčím dvě řetězce 1, každouho rozlišenou stav (intenzita průchozu)
  - 2, kam půjde (průchozová pravděpodobnost jího u DMR)

Homogenní řetězec:  $\forall t, s \geq 0$

$$P(t, t+s) = P(0, s) = P(s)$$

pro Poissonový proces:

$$Q = \frac{1}{2} \begin{pmatrix} 0 & -\lambda & 0 & 0 & \dots \\ 0 & 0 & -\lambda & 0 & \dots \\ 0 & 0 & 0 & -\lambda & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

~~Kolmogorovova rovnice ...~~

~~4/20~~

## Exponenciální řady (spře datší slánka)

- exponenciální hodiny servisu  $S \sim \text{Exp}(\mu)$   
fronky  $T \sim \text{Exp}(\lambda)$

- řádov řadou v náhodném čase  $\tau = \min(S, T)$

$X_{t+\tau} = n-1$  - když vyhrazí servis  $\times$   $X_{t+\tau} = n+1$  - vyhrazí fronda

$$Z := \min\{T, S\} = \text{Exp}(\mu + \lambda) \quad - \text{pro měření } \mu \& \lambda$$

→ výkaz exp. řádu:

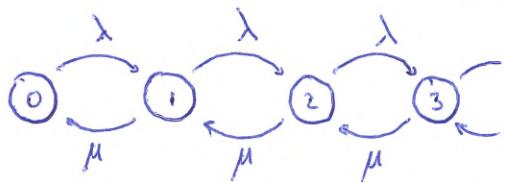
$$P(T < S) = \frac{\lambda}{\lambda + \mu} \quad P(S < T) = \frac{\mu}{\lambda + \mu}$$

- pro měření jazy T ~ Exp(λ) a S ~ Exp(μ) následující platí:

pro  $u \geq 0$  platí, že je  $\{ \min\{T, S\} > u \}$  a  $\{ T < S \}$  jemně měřit

pro systém bronchus oblasty:  $\lambda \rightarrow \boxed{\phantom{0}} \boxed{\phantom{0}} \boxed{\phantom{0}} \boxed{\phantom{0}} \boxed{\phantom{0}} (\mu) \rightarrow$

matice sledovacích  
interválů:  $Q = \begin{pmatrix} 0 & 1 & 2 & 3 & \dots \\ -\lambda & \lambda & 0 & 0 & \dots \\ \mu & -(\lambda + \mu) & \lambda & 0 & \dots \\ 0 & \mu & -(\lambda + \mu) & \mu & \dots \\ \vdots & & & & \end{pmatrix}$



# Systemy hromadné obsluhy a jejich limitní vlastnosti. Souvislost s Markovskými řetězci se spojitym časem.

= teorie front → teorie hromadné obsluhy

volupní řád požadavků → fronta → obsluha → výstupní řád požadavků

Klasifikace = Kendallova notace  $A/B/C/X/Y/Z$

A - rozdílení příchodu jednotek = volupní řád

B - střední počet obslužených jednotek v čase

X - řád paralelních serverů

Y - kapacita fronty (implicitně  $\infty$ )

Z - dočasná fronta (implicitně ~~finite~~)

(+ N - velikost populace (implicitně  $\infty$ ))

$M/M/1$  exponentiální rozdílení  
 - příchozí a čas obsluhy nejsou Pois. procesem s parametry  $\lambda$  a  $\mu$   
 → homogenní Markov řetězec se slouží  $\{0, 1, 2, \dots\}$

$$\lambda_m = \lambda \quad \mu_n = \mu \quad \text{-- proces sítě a záložky}$$

$$Q = \begin{pmatrix} -\lambda & \lambda & 0 & 0 & \dots \\ \mu & -(\mu+\lambda) & \lambda & 0 & \\ 0 & \mu & -(\mu+\lambda) & \lambda & \\ \vdots & & & \ddots & \end{pmatrix}$$

$$\text{stationární rozdílení: } \rho = \lambda / \mu$$

•  $\rho < 1$ : existuje jednoznačně řešení ~~existuje~~ rozdílení  $\pi$  pro všechna  $n$ , platí:

$$P(X_t = n) \rightarrow \pi_n = (1-\rho) \rho^n$$

•  $\rho \geq 1$  stationární rozdílení neexistuje a platí  $\pi_n = 0$

$$P(X_t = n) \rightarrow \pi_n = 0$$

M|M|∞ ...

M|M|c ...

Littleho věta:  $\mathbb{E}N = \lambda \cdot \mathbb{E}T$

počet zákazníků v systému

interválu procesu příchodu

doba stravení v systému

příklad:  $M(\lambda) | M(\mu) | 1$

$$\mathbb{E}N = \mathbb{E}_\pi X_e = \frac{\rho}{1-\rho} = \frac{\frac{\lambda}{\mu}}{1-\frac{\lambda}{\mu}}$$

→ celo výběr platí:  $\mathbb{E}T = \frac{\mathbb{E}N}{\lambda} = \frac{1}{\mu - \lambda}$