1) ČÍSLA

POSLOUPNOSTI A LIMITY

$$\lim_{n\to\infty} n^{\alpha} = \begin{cases} +\infty & \alpha > 0 \\ 1 & \alpha = 0 \\ 0 & \alpha < 0 \end{cases}$$

$$\lim_{n\to\infty} q^{n} = \begin{cases} +\infty & q > 1 \\ 1 & q = 1 \\ 0 & -1 < q < 1 \\ \text{neexistuje} & q \le -1 \end{cases}$$

D: Posloupnost reálných čísel je zobrazení $a: \mathbb{N} \to \mathbb{R}$, zn. $\{a_n\}_{n\in\mathbb{N}}$.

D: Posl. $\{a_n\}$ je omezená, je-li omezená zdola i shora omezená.
ryze monotónní, je-li rostoucí, nebo klesající.
monotónní, je-li neostoucí nebo neklesající.

D: (Limita) Nechť $\{a_n\}$ je posl., $A \in \mathbb{R}$. A je vl. limita posl. $\{a_n\}$, pokud $\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}: \forall n > n_0: |a_n - A| < \varepsilon$.
posl. konverguje
diverguje

V: (O policajtech) Nechť $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}}, \{c_n\}_{n\in\mathbb{N}}$ jsou posl. a platí 1. $\exists n_0 \in \mathbb{N} \cdot \forall n > n_0: a_n \le c_n \le b_n$ 2. $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = A \in \mathbb{R}$ pak $\lim_{n\to\infty} c_n = A$.

V: (Součin mizející a omezené posl.) Nechť $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty}$ posl., $\lim_{n\to\infty} a_n = 0$, $\{b_n\}$ omezená. Pak $\lim_{n\to\infty}(a_n \cdot b_n) = 0$.

D: Nevlastní limita $+\infty$ (resp. $-\infty$) má posl. $\{a_n\}$ pokud $\forall K \in \mathbb{R} \cdot \exists n_0 \in \mathbb{N}: \forall n \ge n_0: a_n \ge K$ (resp. $a_n \le K$).

D: (Podposl.) Nechť $\{a_n\}_{n=1}^{\infty}$ je posl., $\{n_k\}_{k=1}^{\infty}$ rostoucí posl. přirozených čísel. Pak $\{a_{n_k}\}_{k=1}^{\infty}$ je podposl. původní posl. $\{a_n\}_{n=1}^{\infty}$.

D: (Limes superior, limes inferior) Nechť $\{a_n\}_{n=1}^{\infty}$ je posl. Pak definujeme

$$\limsup a_n := \begin{cases} \lim_{n\to\infty} \sup\{a_k, k \ge n\} & \text{pro } a_n \text{ shora omez.} \\ \infty & \text{pro } a_n \text{ shora neomez.} \end{cases}$$

$$\liminf a_n := \begin{cases} \lim_{n\to\infty} \inf\{a_k, k \ge n\} & \text{pro } a_n \text{ zdola omez.} \\ \infty & \text{neomez.} \end{cases}$$

D: (Hromadný bod/hodnota) Nechť $\{a_n\}_{n=1}^{\infty}$ je reálná posl. Pak $A \in \mathbb{R}^*$ je hromadný bod $\exists$ podposl. $\{a_{n_k}\}: \lim_{k\to\infty} a_{n_k} = A$. zn. $H(\{a_n\})$

D: (Cauchyovská posl.) je posl. $\{a_n\}_{n=1}^{\infty}$ pokud splňuje: $\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}: m, n \in \mathbb{N}\ m, n > n_0: |a_n - a_m| < \varepsilon$.

V: (Bolzano-Weierstrassova v.) Každá omezená posl. reálných čísel má konvergentní podposloupnost.

V: (Bolzano-Cauchyova v.) $\{a_n\}$ má limitu $\iff$ $\{a_n\}$ je cauchyovská

ŘADY REÁLNÝCH ČÍSEL $\sum_{n=1}^{\infty} a_n = a_1 + a_2 + \dots = \lim_{n\to\infty} s_n$

D: (částečný součet) n-tý částečný součet řady je součet jejích prvních n členů, $s_n = a_1 + a_2 + \dots + a_n$

Pokud $\exists \lim_{n\to\infty} s_n = L$ pak říkáme, že řada konverguje a její součet je L. Pokud neexistuje nebo je nevlastní, řada diverguje.

geometrická řada
$$\sum_{n=0}^{\infty} q^n = \begin{cases} \frac{1}{1-q} & -1 < q < 1 \\ +\infty & q \ge 1 \\ \text{neexistuje} & q \le -1 \end{cases}$$
harmonická řada $\sum_{n=1}^{\infty} \frac{1}{n}$

V: (podmínka konvergence řady) Nechť $\sum_{n=1}^{\infty} a_n$ je nekonečná řada reálných čísel. Platí:
1. Pokud konverguje $\Rightarrow \lim_{n\to\infty} a_n = 0$ cauchyovost $\{s_n\}$
2. Konverguje $\iff$ splňuje Cauchyovu podm. pro řady: $\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N} \cdot m > n > n_0 \Rightarrow |a_{n+1} + a_{n+2} + \dots + a_m| < \varepsilon$.

D: Řada $\sum a_n$ konverguje absolutně, pokud konverguje řada absolutních hodnot jejích členů $\sum |a_n|$. abs. konvergující řada $\Rightarrow$ konverguje

V: (Leibnizovo kritérium) Nechť $\{a_n\} \subset \mathbb{R}$ splňuje $a_1 \ge a_2 \ge \dots \ge 0 \wedge \lim a_n = 0$. Pak $\sum (-1)^{n+1} a_n = a_1 - a_2 + a_3 - a_4 \dots$ konverguje

V: Nechť $\alpha, \beta \in \mathbb{R}$. Pokud řady $\sum a_n, \sum b_n$ konvergují, konverguje i $\sum(\alpha a_n + \beta b_n)$ a platí $= \alpha \sum a_n + \beta \sum b_n$

KRITÉRIA KONVERGENCE ŘAD

(Srovnávací kritéria konvergence řad) Nechť $\sum a_n, \sum b_n$ jsou řady s nezáp. členy.
1. Nechť $\exists n_0 \in \mathbb{N}$ t.ž. $n > n_0 \Rightarrow a_n \le b_n$. Pak: $\sum b_n$ konverguje $\Rightarrow \sum a_n$ konverguje
2. Nechť $\lim \frac{a_n}{b_n} = K \in \mathbb{R}^*$, patrně $K \ge 0$. Pak: $0 < K < +\infty \Rightarrow \sum a_n$ konv. $\iff \sum b_n$ konv.
$K = 0 \Rightarrow \sum b_n$ konv. $\Rightarrow \sum a_n$ konv.
$K = +\infty \Rightarrow \sum a_n$ konv. $\Rightarrow \sum b_n$ konv.

V: (Cauchyovo odmocninové krit.) Nechť $\sum a_n$ je řada s nezáp. členy.
1. Předpokládejme, že $\exists q \in \mathbb{R}, 0 < q < 1, n_0: n > n_0 \Rightarrow a_n^{\frac{1}{n}} < q$. Pak řada konverguje
2. Když $\limsup a_n^{\frac{1}{n}} < 1 \Rightarrow$ řada konv.
3. Když $\lim a_n^{\frac{1}{n}} < 1 \Rightarrow$ řada konv.
4. $\limsup > 1 \Rightarrow$ diverguje
5. $\lim > 1 \Rightarrow$ diverguje

Body 1., 2., 3., 5. jen se výmění $a_n^{\frac{1}{n}} \rightleftarrows \frac{a_{n+1}}{a_n}$

V: (d'Alembertovo podílové krit.) Nechť $\sum a_n$ je řada s nezáp. členy.

V: (Cauchyovo krit.) Nechť posl. $\{a_n\} \subset \mathbb{R}$ splňuje $a_1 \ge a_2 \ge a_3 \ge \dots \ge 0$. Pak $\sum a_n$ konv. $\iff$ konv. $\sum 2^k a_{2^k} = a_1 + 2a_2 + 4a_4 + 8a_8 + \dots$

V: (Abelovo a Dirichletovo krit.) Nechť $\{a_n\}, \{b_n\} \subset \mathbb{R}$ jsou posl., $a_1 \ge a_2 \ge \dots \ge 0$.
1. (Abelovo) $\sum b_n$ konv. $\Rightarrow \sum a_n b_n$ konv.
2. (Dirichlet) $\lim a_n = 0 \wedge$ posl. čs. $\{s_n\}$ součtů řady $\sum b_n$ je omezená $\Rightarrow \sum a_n b_n$ konverguje

Násobení řad

$\{a_n\}, \{b_n\}$ abs. konv. Pak $(\sum a_n) \cdot (\sum b_n)$ součin

$$\sum_{n=1}^{\infty} a_n \sum_{k=1}^{\infty} b_k = \sum_{n,k=1}^{\infty} a_n b_k$$

$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ $\exp(x)\exp(y) = \exp(x+y)$

POSLOUPNOSTI

konstantní posl.

$\lim_{n\to\infty} a = a$

mocniny a odmocniny

$a>0$: $\lim_{n\to\infty} \frac{1}{n^a} = 0$ resp $\lim_{n\to\infty} \frac{1}{n} = 0$

$a>0$: $\lim_{n\to\infty} n^a = \infty$

$a<0$: $\lim_{n\to\infty} n^a = 0$

$\lim_{n\to\infty} \sqrt[n]{n} = 1$

$a \geq 1$: $\lim_{n\to\infty} \sqrt[n]{a} = 1$

$0<a<1$: $\lim_{n\to\infty} \sqrt[n]{a} = 0$

g. posl. $\lim_{n\to\infty} q^n = \begin{cases} \infty & \text{pro } q>1 \\ 1 & \text{pro } q=1 \\ 0 & \text{pro } |q|<1 \\ \nexists & \text{pro } q \leq -1 \end{cases}$

$\lim_{n\to\infty} \left(\frac{n}{\sqrt[n]{n!}}\right) = e$ ... objevuje se u odmocninového krit(Σ)

exponenciála

$\lim_{n\to\infty} \left(1+\frac{k}{n}\right)^n = e^k$ ... objevuje se u podílového krit(Σ)

$1{,}65 = \sqrt{e}$

resp $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e$

$\lim_{n\to\infty} \sqrt[n]{n!} = +\infty$

$\lim_{n\to\infty} \frac{q^n}{n!} = 0$ resp. $\lim \frac{k^n}{n!} = 0$

$q>1$: $\lim_{n\to\infty} \frac{q^n}{n^k} = \infty$

$|q|<1$: $\lim_{n\to\infty} q^n n^k = 0$

Alternující a oscilující posl.

$\lim_{n\to\infty} \frac{(-1)^n}{n} = 0$

např. $\nexists$:

$\lim_{n\to\infty} (-1)^n$, $\lim_{n\to\infty} \sin(n)$, $\lim_{n\to\infty} \cos(n)$

Průběh fce:

asymptoty

$\lim_{x\to\pm\infty} \frac{f(x)}{x} = a$ $\lim_{x\to\pm\infty} (f(x)-ax) = b$

Lim složené fce

$\lim_{x\to a} f(g(x)) = \lim_{x\to b} f(b)$

$\lim_{x\to a} g(x) = b$

$\forall f$ spojitá nebo $g(x) \neq k$, $x \in (k-\delta, k+\delta)$

L'Hopital

„$\frac{0}{0}$“, „$\frac{\text{cokoli}}{\infty}$“

Limity fcí

V. o složené fci

$\lim_{x\to 0} \frac{\sin x}{x} = 1$ $\lim_{x\to 0} \frac{\arcsin x}{x} = 1$

$\lim_{x\to 0} \frac{e^x-1}{x} = 1$

$\lim_{x\to 0} \frac{1-\cos x}{x^2} = \frac{1}{2}$ $\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1$

$\lim_{x\to 1} \frac{\ln x}{x-1} = \lim_{h\to 0} \frac{\ln(1+h)}{h} = 1$

---

① Aritmetika limit

a) HPSS 1) $\lim_{n\to\infty} (a_n+b_n) = A+B$

2) $\lim_{n\to\infty} a_n \cdot b_n = A\cdot B$

3) $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{A}{B}$

b) vytáhnu největší nekonečno a ignoruju zbytek

c) nedef. výrazy $\frac{\infty}{\infty}$, $\frac{\text{cokoli}}{0}$, $0\cdot\infty$, $\infty-\infty$, 0^0

$\frac{0}{\infty} = 0$ $1^\infty = e^{\infty \cdot \ln 1}$

• V. o lim. (omezená · mizející) = 0

• V. lim „$\frac{1}{+0}$“

$\forall a_n > 0 \wedge \lim a_n = 0$

$\lim \frac{1}{a_n} = \infty$

• V. Bolzano-Weierstrassova

z každé omezené posl. lze vybrat konvergentní posl.

② V. o sevřené posloupnosti

③ Rekurentně zadané posl.

a) V. o vybrané posl.

1) $a_{n+1} = \bigcirc + a_n$

$\left.\begin{array}{l}\lim_{n\to\infty} a_{n+1} = a \\ \lim_{n\to\infty} a_n = a\end{array}\right\} \Rightarrow a = \bigcirc + a \Rightarrow a = \_\_$

$\Rightarrow$ kandidáti na limitu např. $a = \{\pm 2\}$

$A \in \mathbb{R}$

$a \in \{\pm\infty\}$

$a \nexists$ $\longrightarrow$ tato možnost odpadá pokud a_n je monotónní

2) $\lim_{n\to\infty} a_{n_k} \neq \lim_{n\to\infty} a_{n_l} \Rightarrow \lim a_n \nexists$

• Def. f'

• Průběh fce

b) V. o monotónní posl. každá monot. posl. má lim.

1) $a_{n+1} - a_n > 0 \Rightarrow$ rostoucí; $< 0 \Rightarrow$ klesající

2) $\frac{a_{n+1}}{a_n} > 1 \Rightarrow$ rostoucí; $< 1 \Rightarrow$ klesající

$(a+b)^2 = a^2+2ab+b^2$

$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$

$a^2-b^2 = (a-b)(a+b)$

$a^3 \pm b^3 = (a\pm b)(a^2 \mp ab + b^2)$

RADY $\quad \sum a_n$

$e = 2{,}71\ldots$

řady s nezáp. členy

① Nutná podmínka konvergence $\quad \sum \text{konv.} \Rightarrow \lim\limits_{n\to\infty} a_n = 0$

$\lim\limits_{n\to\infty} a_n \neq 0 \Rightarrow \sum$ diverguje (v osciluje)

② Srovnávací krit ($\{a_n\}, \{b_n\}$ mají nezáp. členy)

$\forall n \quad a_n > b_n$: $\quad b_n$ div. $\Rightarrow a_n$ div.

a_n kon. $\Rightarrow b_n$ konv.

③ Limitní srovnávací krit. (pro nezáp. členy)

$$\lim_{n\to\infty} \frac{a_n}{b_n} = A$$

$A \in \mathbb{R} \Rightarrow a_n, b_n$ se chovají stejně

$A = 0 \Rightarrow \sum b_n$ kon $\Rightarrow \sum a_n$ konv $\qquad b_n > a_n$

$A = \infty \Rightarrow a_n > b_n \qquad \sum a_n$ konv $\Rightarrow \sum b_n$ konv

$\sum \frac{1}{n^\alpha} \begin{cases} \alpha > 1 & \sum \text{konv.} \\ \alpha \leq 1 & \sum \text{div.} \end{cases} \qquad \frac{\ldots n^{\beta_1} \ldots}{\ldots n^{\beta_2}} \Rightarrow \alpha = \beta_1 - \beta_2$

$\sum \frac{1}{n}$ div

$\sum q^n \quad |q| < 1 \Leftrightarrow \sum$ konv. $\left(\wedge \sum q^n = \frac{1}{1-q}\right)$

$|q| > 1 \Leftrightarrow \sum q^n$ div.

$\sum\limits_0^\infty \frac{x^n}{n!} = e^x \quad, x \in \mathbb{R} \Rightarrow$ diverguje

$\sum \frac{n!}{x^n} = \frac{1}{e} \quad$ konv.

$\sum \ln\left(1 + \frac{1}{n^2}\right) \sim \frac{1}{n^2}$

④ Odmocninové a podílové krit.

a) $\lim \sqrt[n]{a_n} = A$ (Cauchyovo krit.)

b) $\lim \frac{a_{n+1}}{a_n} = A$ (d'Alambertovo)

$\left.\right\}$ $A < 1 \Rightarrow \sum$ konv.

$A > 1 \Rightarrow \sum$ div

$A = 1 \Rightarrow$ nevím nic

Alternující řady

člen mění znaménko

⑤ Absolutní konvergence

$\sum |a_n|$ konv. $\Rightarrow \sum a_n$ konv. absolutně (i neabsolutně)

$\sum |a_n|$ div. $\Rightarrow$ nevím nic

④ a) $\lim \sqrt[n]{|a_n|}$ b) $\lim \left|\frac{a_{n+1}}{a_n}\right| = A$ $\quad > 1 \Rightarrow \sum |a_n|$ div $\Rightarrow \sum a_n$ div $\quad$ } neboť $\lim a_n \neq 0$!

$\Rightarrow \sum |a_n|$ div $\Rightarrow \sum a_n$ konv i takto $\sum a_n$ div

$< 1 \Rightarrow \sum$ konv. absolutně

⑥ Leibnitzovo krit

$\sum\limits_1^\infty (-1)^n a_n$: $\lim a_n = 0 \Leftrightarrow \sum$ konverguje (neabsolutně)

↳ a_n nerostoucí $\quad$ → můžu vzít fci a zderivovat

↳ $\forall n: a_n \geq 0$

Nezapomenout napsat odpověď!

Derivace fcí

1. $(c)' = 0$
2. $(x^n)' = n \cdot x^{n-1}$
3. $(a^x)' = a^x \ln a$
4. $(e^x)' = e^x$
5. $(\log_a x)' = \frac{1}{x \ln a}$
6. $(\ln x)' = \frac{1}{x}$

7. $(\sin x)' = \cos x$
8. $(\cos x)' = -\sin x$
9. $(\mathrm{tg}\, x)' = \frac{1}{\cos^2 x}$
10. $(\mathrm{cotg}\, x)' = -\frac{1}{\sin^2 x}$

11. $(\arcsin x)' = \frac{1}{\sqrt{1-x^2}} \quad x \in$
12. $(\arccos x)' = -\frac{1}{\sqrt{1-x^2}}$
13. $(\mathrm{arctg}\, x)' = \frac{1}{1+x^2}$
14. $(\mathrm{arccotg}\, x)' = -\frac{1}{1+x^2}$

15. $(|x|)' = \mathrm{sgn}\, x$

$u, v: \mathbb{R} \to \mathbb{R}, c \in \mathbb{R}$

1. $[u(x) \pm v(x)]' = u'(x) \pm v'(x)$
2. $[c\,u(x)]' = c\,u'(x)$
3. $[u(x) \cdot v(x)]' = u'(x) \cdot v(x) + u(x) \cdot v'(x)$
4. $\left[\frac{u(x)}{v(x)}\right]' = \frac{u'(x)v(x) - u(x)v'(x)}{v^2(x)}$
5. složená fce der. vnější · der. vnitřní $\quad [f(g(x))]' = f'(g(x)) \cdot g'(x)$
6. inverzní fce $(f^{-1})'(x_0) = \frac{1}{f'(f^{-1}(x_0))}$

6.A Funkce

Fce je $Z: \mathbb{R} \to \mathbb{R}$, ~~tedy~~ $f \subseteq \mathbb{R} \times \mathbb{R}$

Def: $D(f) = \{x \in \mathbb{R} : \exists! y \in \mathbb{R}, y = f(x)\}$ ... definiční obor

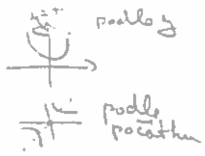
$H(f) = \{y \in \mathbb{R} : \exists x \in \mathbb{R} ; y = f(x)\}$ ... obor hodnot

Def: Graf fce je množina bodů $X[x, f(x)]$, $x \in D(f)$, $\in E_2$.

Def: Sudá, resp. lichá fce: 1) $\forall x \in D(f)$: $(-x) \in D(f)$

2) $\forall x \in D(f)$: $f(x) = f(x)$, – sudá

resp. $f(-x) = -f(x)$ – lichá



Def: Fce je prostá $\iff$ $\forall x_1, x_2 \in D(f)$: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

Def: f je na M a) rostoucí $\iff$ $\forall x_1, x_2 \in M$: $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$

b) klesající $\iff$ — // — $\Rightarrow f(x_1) > f(x_2)$ } ryze monotónní

c) nerostoucí $\iff$ — // — $\Rightarrow f(x_1) \geq f(x_2)$

d) neklesající $\iff$ — // — $\Rightarrow f(x_1) \leq f(x_2)$ } monotónní fce

Def: f je na $M \subseteq D(f)$ a) shora omezená $\iff$ $\exists k \in \mathbb{R}$: $\forall x \in M$: $f(x) \leq k$

b) zdola omezená $\iff$ $\exists k \in \mathbb{R}$: $\forall x \in M$: $f(x) \geq k$

c) omezená $\iff$ f je shora $\wedge$ zdola omezená

Def: Maximum na $\forall x \in M$: $f(x) \leq f(a)$

Minimum na b $\forall x \in M$: $f(x) \geq f(b)$

Ostré max., resp. min. na m $\forall x \in M$: $f(x) < f(m)$, resp. $f(x) > f(m)$

Def: f je periodická $\iff$ $\exists p \in \mathbb{R}^+$ $\forall x \in D(f)$: 1) $x \in D(f) \Rightarrow x \pm kp \in D(f)$

2) $f(x) = f(x \pm kp)$

p je perioda

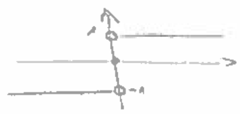
Def: p_0 je nejmenší perioda $\iff$ $\forall p > p_0$

Dirichletova fce

$$\chi(x) \begin{cases} 1 & \text{pro } x \in \mathbb{Q} \\ 0 & \text{pro } x \in \mathbb{Q}'_{\mathbb{R}} \end{cases}$$

Fce signum

$$\operatorname{sgn}(x) = \begin{cases} -1 & \text{pro } \forall x \in \mathbb{R}^- \\ 0 & x = 0 \\ 1 & \forall x \in \mathbb{R}^+ \end{cases}$$

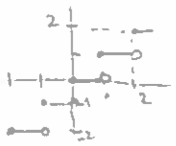


Celá část čísla

dolní celá část: $x \in \mathbb{R}$: $\exists!$ dvojice z, a $z \in \mathbb{Z}, a \in \langle 0, 1)$: $x = z + a$

$[x] = z$

$\lfloor x \rfloor = z$



Spojitá funkce $\iff$ $\lim\limits_{x \to x_0} f(x) = f(x)$

Derivace fce

Fce konvexní - nad tečnou

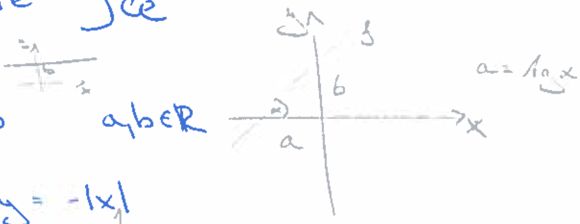
konkávní - pod tečnou

Fce primitivní: taková, že $d f(x) = f(x)$

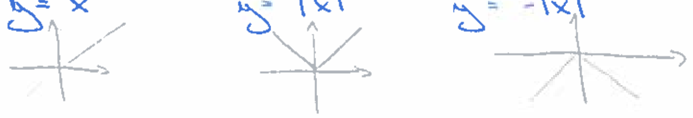
Def: Nechť f je prostá. Relaci f^{-1} nazýváme inverzní funkcí.

Polynomické ~~a~~ racionální lomené fce a mocninné fce

- konstantní $f: y = b$
- lineární: $f: y = ax + b \quad a, b \in \mathbb{R}$



$y = x \qquad y = |x| \qquad y = -|x|$



|| zobrazit pod $\underline{x}$ podle $\underline{x}$ nahoru

(−) zobrazí y podle osy x

$y = |3 - x| = |x - 3| \qquad y = 3 - |x| \qquad y = 2 - |x + 1|$

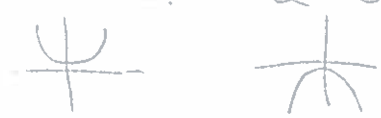
přičítá v závorce posouvá po $\underline{x}$, posouvá o −1

- kvadratická fce $f: y = ax^2 + bx + c \quad a \neq 0, a, b, c \in \mathbb{R}$

posun po ose y

posun po $\underline{x}$ a y

$a > 0 \qquad a < 0$



sudá a zároveň prostá

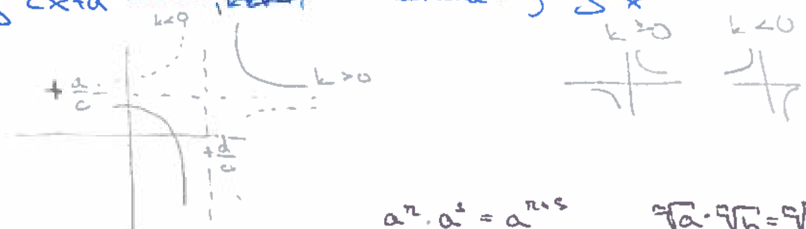
- lineární lomená fce $f: y = \frac{ax+b}{cx+d}$ ~~ad ≠ bc~~

lomená: $f: y = \frac{k}{x} \quad k \in \mathbb{R} \setminus \{0\}$

$y = \frac{ax+b}{cx+d} = \frac{a}{c} + \frac{k}{x - \frac{-d}{c}}$

po y posun po x

$k > 0 \qquad k < 0$



Př: $y = \frac{-2}{x-1} + 3$

$a^r \cdot a^s = a^{r+s}$

$a^r : a^s = a^{r-s}$

$a^{r^s} = a^{r \cdot s}$

$(a \cdot b)^r = a^r \cdot b^r$

$\left(\frac{a}{b}\right)^r = \frac{a^r}{b^r}$

$\boxed{a^0 = 1}$

$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{a \cdot b}$

$\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$

$\sqrt[n]{a^m} = (\sqrt[n]{a})^m$

$\sqrt[m]{\sqrt[n]{a}} = \sqrt[m \cdot n]{a}$

$\sqrt[n]{a} = \sqrt[m \cdot n]{a^p}$

$\sqrt[q]{a^p} = a^{\frac{p}{q}}$

- mocninná $y = x^n$

$n \in \mathbb{N}$

n sudé → sudá $\qquad n$ liché → lichá

$n \in \mathbb{N}, x \neq 0 \qquad y = x^{-n} = \frac{1}{x^n}$

sudá $\qquad$ lichá

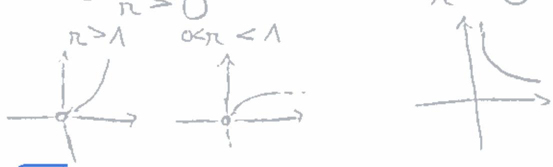
− s racionálním exponentem $\frac{p}{q} \in \mathbb{Q}$

$f: y = x^{\frac{p}{q}} = \sqrt[q]{x^p} \qquad x \in \mathbb{R}^+$

$f: y = x^r$

$r > 0 \qquad r < 0$

$r > 1 \qquad 0 < r < 1$



− odmocnina

$n \in \mathbb{N}, n \geq 2, x \geq 0 \qquad f: y = x^n \qquad f^{-1}: y = \sqrt[n]{x}$

teorie 2/2 (6.A)

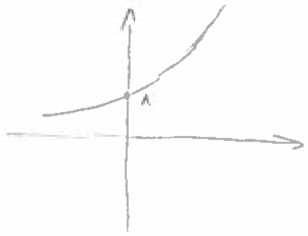
- exponenciální fce

$a \in \mathbb{R}^+ \setminus \{1\}$

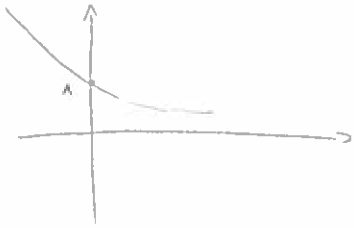
$$f: y = a^x$$

(a … základ)

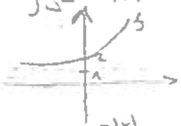
$a > 1$



$0 < a < 1$

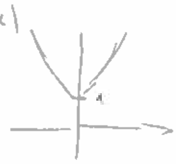


Př: $f: y = 2^x + 1$



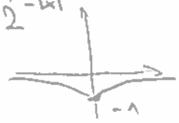
$f: y = 2^{(x+1)}$

$f: y = 2^{|x|}$



$y = 2^{-|x|}$

$y = -2^{-|x|}$



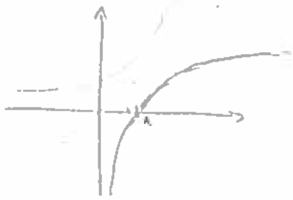
- logaritmická fce = inverzní k exponenciální $x \in \mathbb{R}^+$

$a \in \mathbb{R}^+ \setminus \{1\}$

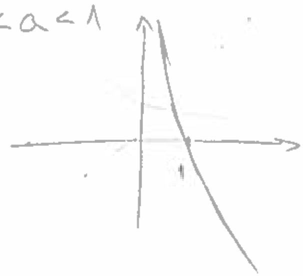
$$f: y = \log_a x$$

(a → základ)

$a > 1$



$0 < a < 1$



$$\log_a b = c \Leftrightarrow a^c = b$$

$\log_a x = \text{moc} \Leftrightarrow a^{\text{moc}} = x$

$\log_b n = \dfrac{\log_a n}{\log_a b}$

$a^{\log_a x} = x$

$\log_a a^x = x$

$\log_a b \cdot \log_b c = \log_a c$

$\log_a b \cdot \log_b a = 1$

$\log_{\frac{1}{a}} x = -\log_a x$

$\log_a \frac{1}{x} = -\log_a x$

$\log_a (x \cdot y) = \log_a x + \log_a y$

$\log_a \left(\frac{x}{y}\right) = \log_a x - \log_a y$

$\log_a x^r = r \cdot \log_a x$

$\frac{1}{2} \log x^2 = \log |x|$

dekadický logaritmus … $\log_{10} x = \log x$

přirozený logaritmus … $\log_e x = \ln x$ $e = 2{,}718\ldots$

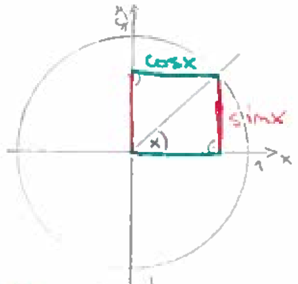
$f: y = \ln x$ - rostoucí

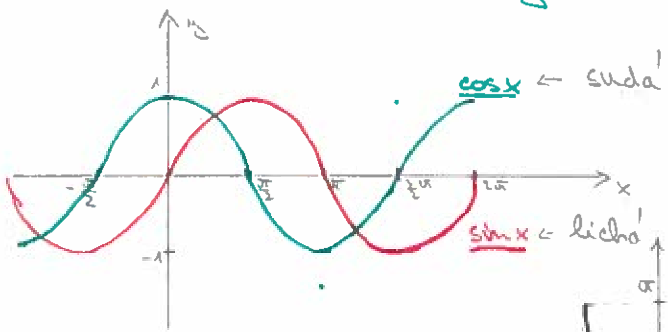
$\ln x = \dfrac{\log x}{\log e}$ $\log e = 0{,}434294$

$\log x = \dfrac{\ln x}{\ln 10}$ $\ln 10 = 2{,}302585$

3/14. GONIOMETRICKÉ A CYKLOMETRICKÉ FUNKCE

$\sin x, \cos x, \mathrm{tg}\,x, \mathrm{cotg}\,x$ | $\arcsin x, \arccos x, \mathrm{arctg}\,x, \mathrm{arccotg}\,x$





$\frac{\pi}{2} \doteq 1{,}6$

sin x ← lichá

cos x ← sudá

perioda 2π

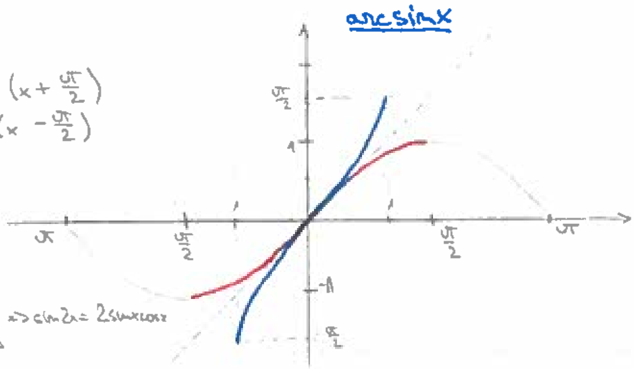
$\forall x \in \mathbb{R}$: $\sin x = \cos\left(x - \frac{\pi}{2}\right) = -\cos\left(x + \frac{\pi}{2}\right)$

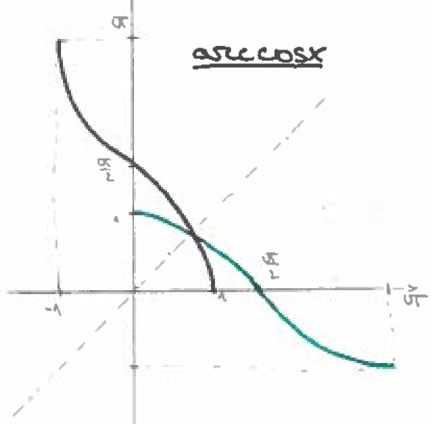
$\cos x = \sin\left(x + \frac{\pi}{2}\right) = -\sin\left(x - \frac{\pi}{2}\right)$

$\boxed{\sin^2 x + \cos^2 x = 1}$

$\sin x = \cos\left(\frac{\pi}{2} - x\right)$

$\cos x = \sin\left(\frac{\pi}{2} - x\right)$





SOUČTOVÉ VZORCE

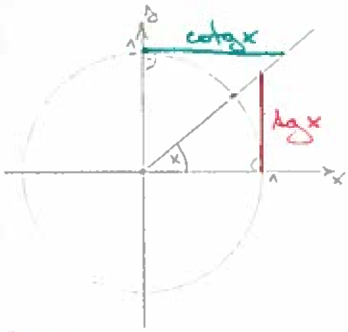
$\sin(x+y) = \sin x \cos y + \cos x \sin y \Rightarrow \sin 2x = 2 \sin x \cos x$

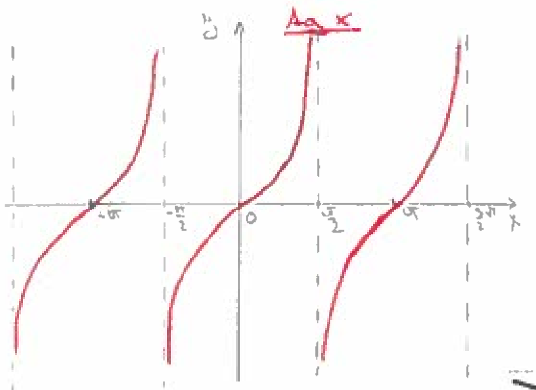
$\sin(x-y) = \sin x \cos y - \cos x \sin y$

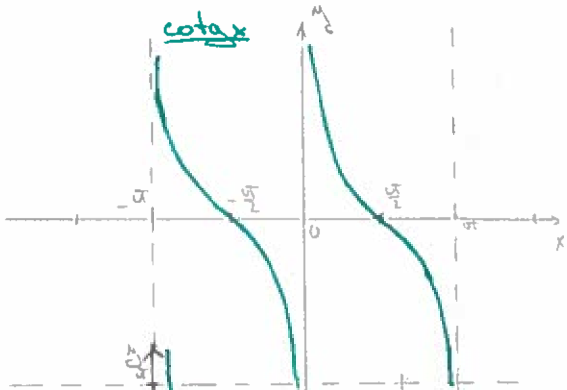
$\cos(x+y) = \cos x \cos y - \sin x \sin y \Rightarrow \cos 2x = \cos^2 x - \sin^2 x$

$\cos(x-y) = \cos x \cos y + \sin x \sin y$

x	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
sin x	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	0	−1	0
cos x	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	−1	0	1







tg x, cotg x } liché, perioda π

$\forall x \in \mathbb{R} \setminus \bigcup \{k \cdot \frac{\pi}{2}\}$; $k \in \mathbb{Z}$

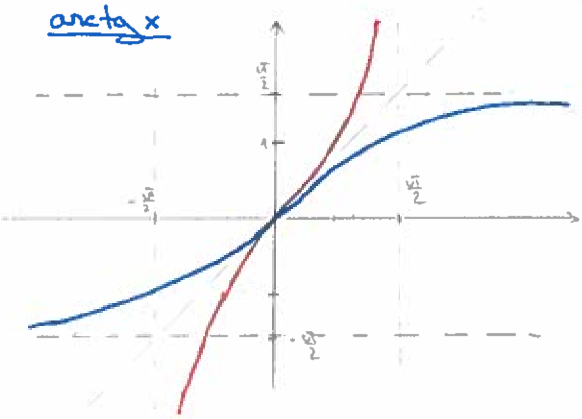
$\mathrm{tg}\,x = -\mathrm{cotg}\left(x \pm \frac{\pi}{2}\right)$

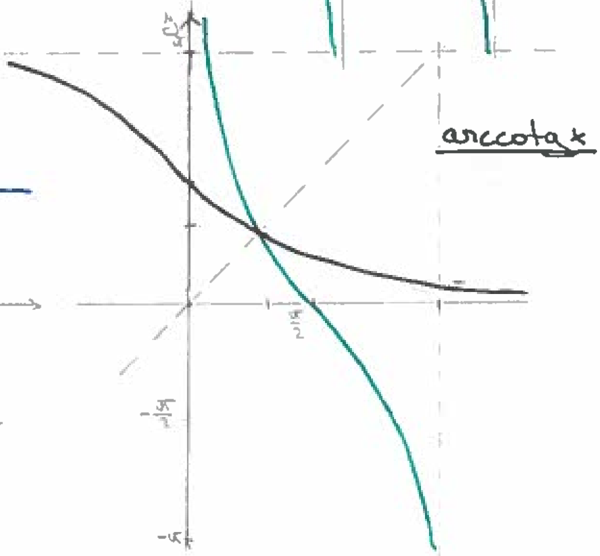
$\mathrm{cotg}\,x = -\mathrm{tg}\left(x \pm \frac{\pi}{2}\right)$

$\boxed{\mathrm{tg}\,x \cdot \mathrm{cotg}\,x = 1}$

$\mathrm{tg}\,x = \mathrm{cotg}\left(\frac{\pi}{2} - x\right)$

$\mathrm{cotg}\,x = \mathrm{tg}\left(\frac{\pi}{2} - x\right)$

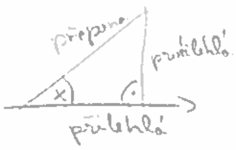




x	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
tg x	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	—	0	—	0
cotg x	—	$\sqrt{3}$	1	$\frac{\sqrt{3}}{3}$	0	—	0	—

Vyjádření goniometrických fcí pomocí jiné g. fce

$x \in (0, \frac{\pi}{2})$	$\sin x$	$\cos x$	$\mathrm{tg}\, x$	$\mathrm{cotg}\, x$
$\sin x$	—	$\sqrt{1-\cos^2 x}$	$\frac{\mathrm{tg}\, x}{\sqrt{1+\mathrm{tg}^2 x}}$	$\frac{1}{\sqrt{1+\mathrm{cotg}^2 x}}$
$\cos x$	$\sqrt{1-\sin^2 x}$	—	$\frac{1}{\sqrt{1+\mathrm{tg}^2 x}}$	$\frac{\mathrm{cotg}\, x}{\sqrt{1+\mathrm{cotg}^2 x}}$
$\mathrm{tg}\, x$	$\frac{\sin x}{\sqrt{1-\sin^2 x}}$	$\frac{\sqrt{1-\cos^2 x}}{\cos x}$	—	$\frac{1}{\mathrm{cotg}\, x}$
$\mathrm{cotg}\, x$	$\frac{\sqrt{1-\sin^2 x}}{\sin x}$	$\frac{\cos x}{\sqrt{1-\cos^2 x}}$	$\frac{1}{\mathrm{tg}\, x}$	—



$$\sin x = \frac{\text{protilehlá}}{\text{přepona}}$$

$$\cos x = \frac{\text{přilehlá}}{\text{přepona}}$$

$$\mathrm{tg}(x) = \frac{\text{protilehlá}}{\text{přilehlá}}$$

$$\mathrm{cotg}(x) = \frac{\text{přilehlá}}{\text{protilehlá}}$$

obor konvergence

$(3\cos x)' = 0\cdot\cos x - 3\cdot(-\sin x) = 3\cdot(-\sin x) = 3\cdot(\cos x)'$

Vzorce pro derivování.

1. $(c)' = 0$
2. $(x^n)' = nx^{n-1}$

---

3. $(a^x)' = a^x \ln a$
4. $(e^x)' = e^x$

---

5. $(\log_a x)' = \dfrac{1}{x \ln a}$
6. $(\ln x)' = \dfrac{1}{x}$

---

7. $(\sin x)' = \cos x$
8. $(\cos x)' = -\sin x$
9. $(\operatorname{tg} x)' = \dfrac{1}{\cos^2 x}$
10. $(\operatorname{cotg} x)' = -\dfrac{1}{\sin^2 x}$

---

11. $(\arcsin x)' = \dfrac{1}{\sqrt{1-x^2}}$ $x \in (-1,1)$
12. $(\arccos x)' = -\dfrac{1}{\sqrt{1-x^2}}$
13. $(\operatorname{arctg} x)' = \dfrac{1}{1+x^2}$
14. $(\operatorname{arccotg} x)' = -\dfrac{1}{1+x^2}$

Pravidla pro počítání.

$u, v : \mathbb{R} \to \mathbb{R}$, $c \in \mathbb{R}$,

1. $(u(x) \pm v(x))' = u'(x) \pm v'(x)$
2. $(cu(x))' = cu'(x)$ pro násobení
3. $(u(x)v(x))' = u'(x)v(x) + u(x)v'(x)$
4. $\left(\dfrac{u(x)}{v(x)}\right)' = \dfrac{u'(x)v(x) - u(x)v'(x)}{v^2(x)}$

5. Derivace složené fce = derivace vnější · derivace vnitřní

6. inverzní fce

Vzorce pro integrování.

1. $\int dx = x + c$ na $(-\infty, \infty)$

$\int 0\,dx = c$

2. $\int x^n\,dx = \dfrac{x^{n+1}}{n+1} + c$ $(n \neq -1)$ na $(0,\infty)$ (na $\mathbb{R}$ nebo...)

$\int \frac{dx}{x} = \ln|x| + c$

3. $\int \dfrac{1}{x}\,dx = \ln|x| + c$ $(-\infty, 0) \cup (0, \infty)$

---

4. $\int a^x\,dx = \dfrac{a^x}{\ln a} + c$ $(a > 0,\ a \neq 0)$ na $(-\infty, \infty)$
5. $\int e^x\,dx = e^x + c$ na $(-\infty, \infty)$

---

6. $\int \sin x\,dx = -\cos x + c$ na $(-\infty, \infty)$
7. $\int \cos x\,dx = \sin x + c$ —//—
8. $\int \dfrac{1}{\cos^2 x}\,dx = \operatorname{tg} x + c$ $(-\frac{\pi}{2} + k\pi, \frac{\pi}{2} + k\pi)$ $k \in \mathbb{Z}$
9. $\int \dfrac{1}{\sin^2 x}\,dx = -\operatorname{cotg} x + c$ na $(k\pi, \pi + k\pi)$ $k \in \mathbb{Z}$

---

10. $\int \dfrac{1}{\sqrt{A^2 - x^2}}\,dx = \arcsin \dfrac{x}{A} + c$
11. $\int \dfrac{1}{\sqrt{x^2 \pm B}}\,dx = \ln|x + \sqrt{x^2 \pm B}| + c$

---

12. $\int \dfrac{1}{A^2 + x^2}\,dx = \dfrac{1}{A} \operatorname{arctg} \dfrac{x}{A} + c$ $(-\infty, \infty)$
13. $\int \dfrac{1}{A^2 - x^2}\,dx = \dfrac{1}{2A} \ln \left|\dfrac{A+x}{A-x}\right| + c$

Základní integrační metody.

per-partés, rozklad na parciální zlomky, substituční metoda

$\int \frac{f'(x)}{f(x)}\,dx = \ln|f(x)| + c$

(4) FCE VÍCE PROMĚNNÝCH

V. o vázaných extrémech a implicitní fci viz Šánal MA II, 7 př

D: <u>Fci n (reálných) proměnných</u> rozumíme zobrazení $f: M \to \mathbb{R}$, kde $M \subseteq \mathbb{R}^n$.

D: Nechť $G \subseteq \mathbb{R}^n$ je otevřená mn., $i \in \{1, \dots, n\}$, $f: G \to \mathbb{R}$, $x \in G$. <u>Parciální derivací</u> fce f v bodě $\underline{x}$ podle i-té proměnné nazveme $\frac{\partial f}{\partial x_i}(x) = \lim_{h \to 0} \frac{f(x_1, \dots, x_i + h, \dots, x_n) - f(x_1, \dots, x_i, \dots, x_n)}{h}$, pokud lim. $\exists$.

D: Nechť f má na otv. mn. $G \subseteq \mathbb{R}^n$ parc. derivaci $\frac{\partial f}{\partial x_i}$, $i \in \{1, \dots, n\}$. Pak definujeme pro $a \in G$, $j \in \{1, \dots, n\}$ <u>druhou parc. derivaci</u> $\frac{\partial^2}{\partial x_i \partial x_j} f(a) := \frac{\partial}{\partial x_j}\left(\frac{\partial f}{\partial x_i}\right)(a)$ pokud se $i \neq j$ nazývá se též smíšená derivace

D: Nechť $G \subseteq \mathbb{R}^n$ je otev., $f: G \to \mathbb{R}$, $x \in G$. Lin. zob. $df(x): \mathbb{R}^n \to \mathbb{R}$ je <u>"totální diferenciál"</u> („derivace fce více proměnných") fce f v bodě $\underline{x}$ jestliže (existuje) platí $\lim_{h \to 0} \frac{f(x+h) - f(x) - df(x)h}{\|h\|} = 0$. $\|h\| = \sqrt{\sum h_i^2}$ Eukl. norma

<u>gradient fce</u> f v bodě $\underline{x}$ $\nabla f(x) = \left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right)$ (udává směr největšího přírustku)
totální diferenciál je pak $df = \nabla f(x) \cdot \underline{dx} = \frac{\partial f}{\partial x_1} dx_1 + \dots + \frac{\partial f}{\partial x_n} dx_n$ = tečná nadrovina k f v bodě $\underline{x}$
skalární součin ↳ vektor změn jednotlivých prom. $dx = (dx_1, \dots, dx_n)$

D: Hessián je matice druhých parciálních derivací fce f $G \to \mathbb{R}$, $G \subseteq \mathbb{R}^n$ v bodě $\underline{a}$. Matice je $n \times n$.

$$D^2 f = \left(\frac{\partial^2 f(a)}{\partial x_i \partial x_j}\right)_{i,j=1}^{n}$$

V: (Postačující podmínka pro lok. extrém) Nechť $G \subseteq \mathbb{R}^n$ je otev. mn. $a \in G$, $f \in C^2(G)$ (má na G spojité 2. parc. derivace), $df(a) = 0$.
- je-li $D^2 f(a)$ pozitivně definitní $\Rightarrow$ v $\underline{a}$ je lok. min.
- negativně definitní $\Rightarrow$ lok. min.
- indefinitní $\Rightarrow$ v a není extrém

V: (O přírůstku fce víc proměnných „o střední hodnotě") Nechť f má vl. parc. derivace v ~~[illegible]~~ $\forall$ bodě $[a,b] \subset \mathbb{R}^m$.
Pak $\exists$ body $c_1, c_2, \dots, c_m \in [a,b]$ $f(b) - f(a) = \sum_{i=1}^{m} \frac{\partial f}{\partial x_i}(c_i)\,(b_i - a_i)$

5 METRICKÉ PROSTORY

viz Šámal MA II

D: (Metrický prostor) je dvojice (M, d), kde M je mn. bodů a $d: M \times M \to \mathbb{R}$ je zob. zvané metrika a splňující:
1. $d(x,y) = 0 \iff x = y$ — „silná antisymetrie"
2. $d(x,y) = d(y,x)$ — symetrie
3. $d(x,y) \leq d(x,z) + d(z,y)$ — Δ-nerovnost

Metriky:
- součtová $d_1(x,y) = \sum_{i=1}^{m} |x_i - y_i|$ = Manhattanská = newyorská, odpovídá čtvercové síti, pošťácká
- Euklidovská $d_2(x,y) = \sum_{i=1}^{m} \sqrt{(x_i - y_i)^2}$ $\to$ Euklidovský prostor $(\mathbb{R}^n, d_2)$
- maximová $d_\infty(x,y) = \max_i |x_i - y_i|$
- diskrétní pro lib. mn. P: $d(x,x) = 0$ pro $x \in P$, $d(x,y) = 1$ pro $x \neq y$
- supremová $d(f,g) = \sup_{x \in X} |f(x) - g(x)|$, X je mn. $f, g: X \to \mathbb{R}$ omezené

D: Nechť (M,d) je metrický prostor, $x \in M$, $r > 0$. Otevřená koule se středem x a poloměrem r je mn.
$B(x,r) = \{y \in M \mid d(x,y) < r\}$
Uzavřená koule $\overline{B}(x,r) = \{y \in M \mid d(x,y) \leq r\}$
$G \subseteq M$ je otevřená množina v M když $\forall x \in G \; \exists r > 0 : B(x,r) \subseteq G$. $\to$ př: $\emptyset, M$
$F \subseteq M$ je uzavřená množina, pokud její doplněk $M \setminus F$ je otevřená.

V: Vlastnosti otevřených mn.
1. $M, \emptyset$ jsou otevřené
2. $\bigcap$ konečně mnoha otev. mn. je otevřená mn.
3. $\bigcup$ lib. mnoha otev. mn. je otevřená mn.

uzavřených mn.
1. $M, \emptyset$ jsou uzavřené
2. $\bigcap$ lib. mnoha uzav. mn. je uzavřená mn.
3. $\bigcup$ kon. mnoha uzav. mn. je uzavřená mn.

D: Buď (M,d) metrický podprostor, $A \subseteq M$ neprázdná. Pak $(A, d|_{A \times A})$ je ~~p~~podprostor prostoru (M,d)

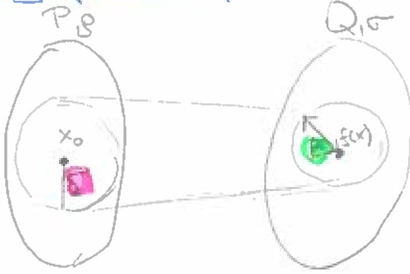
D: Nechť (M,d) je m. prostor. Řekneme, že X je kompaktní prostor, jestliže z každé posloupnosti prvků z X lze vybrat konvergentní podposloupnost. Řekneme, že množina je kompaktní $A \subseteq X$ jestliže je prostor $(A, d|_{A \times A})$ kompaktní.
z: Tedy A mn. je kompaktní, pokud z každé posl. jejích prvků lze vybrat podposl. konvergující k bodu v A

V: Podmn. $\mathbb{R}^m$ je kompaktní $\iff$ je omezená $\wedge$ uzavřená
↳ tj. podprostor euklidovského prostoru E_m

D: Podmn. M metrického prostoru (X, ρ) je omezená, pokud $\exists K$ konečné: $\forall x,y \in M \Rightarrow \rho(x,y) < K$.

„spojité zob. mezi metrickými prostory"
D: Nechť (P, ρ), (Q, σ) jsou metrické prostory, $f: P \to Q$, $x_0 \in P$.
f je spojitá v bodě x_0, když $\forall \varepsilon > 0 \; \exists \delta > 0 \; \forall x \in B_\rho(x_0, \delta) : f(x) \in B_\sigma(f(x_0), \varepsilon)$
Řekneme, že f je spojitá na P, je-li spojitá v každém bodě P.

D: Buď X mn., $G \subseteq P(X)$. Dvojice (X, G) je topologický prostor, pokud:
- $\emptyset, X \in G$
- $G_1, \dots, G_m \in G \Rightarrow G_1 \cap \dots \cap G_m \in G$
- $\forall a \in A: G_a \in G \Rightarrow \bigcup_{a \in A} G_a \in G$



6 ALGEBRA

př.: $\mathbb{Z}(+,-,1)$

D: **Grupa** je mn. G s asociativní bin. operací vůči, kt. zde $\exists$ neutrální prvek a všechny prvky z G jsou invertibilní. $G(\cdot)$ resp. $G(\cdot, ^{-1}, 1)$

arita operací na R

D: Nechť máme množinu s operacemi, tj. algebru $R(+,\cdot,-,0,1)$ typu $(2,2,1,0,0)$. Je to

- **okruh**, pokud
  - $R(+)$ je komut. grupa tj. $+$ je asociativní, $\exists$ neutr. prvek, $\exists$ inverzy to zajišťuje $-$
  - $R(\cdot)$ je monoid tj. $\cdot$ je asociativní s $\exists$ neutr. prvkem 1
  - platí distributivita tj. $\forall a,b,c \in R$ $a\cdot(b+c) = a\cdot b + a\cdot c$, $(a+b)\cdot c = a\cdot c + b\cdot c$
- **těleso**
  - $R(+,\cdot,-,0,1)$ je okruh
  - všechny prvky krom 0 jsou vůči $\cdot$ invertibilní

Těleso je mn. R s aspoň 2 prvky $0, 1$ a operacemi splňující
- $R(+,-,0)$ je komutativní grupa
- $R\setminus\{0\}(\cdot, ^{-1}, 1)$ je grupa
- platí distributivní zákony

$\alpha_i : A^{\Omega(i)} \to A$

D: Nechť $\alpha_i : A^n \to A$ n-ární operace, I mn. indexů (operací), $\Omega : I \to \mathbb{N}_0$ typ. Pak pro neprázdnou mn. A je $A(\alpha_i \mid i \in I)$ **algebra** typu Ω, α_i je $\Omega(i)$-ární operace

D: **Kongruence** je ekvivalence ϱ slučitelná se $\forall$ operacemi algebry, tj. $(a_i, b_i) \in \varrho$ $\forall i \in [n] \Rightarrow (\alpha(a_1,\dots,a_n), \alpha(b_1,\dots,b_n)) \in \varrho$

D: **Podalgebra** je podmnožina uzavřená na $\forall$ operace. $H \leq G$

D: **Podgrupa** je podmnožina uzavřená na danou bin. operaci a na inverzy vůči té operaci.

Normální podgrupa splňuje navíc $H \trianglelefteq G$: $\forall g \in G$ $\forall h \in H$ $g^{-1} h g \in H$.

D: **Faktor mn. A** podle ekvivalence ϱ je mn. rozkladových tříd ekvivalence ϱ. $A/_\varrho = \{[a]_\varrho \mid a \in A\}$ (s konečnými) ↳ mn. prvků ekvivalentních s a

D: (Faktorgrupa) Pro grupu $(G, \cdot, ^{-1}, e)$ a její normální podgrup N je **faktorgrupa** $G/N = \{g \cdot n \mid g \in G, n \in N\}$.

Levá (resp. pravá) rozkladová třída podle $H \trianglelefteq G$ je $G/_H = g \cdot H := \{g\} \cdot H$ resp. $(= Hg)$

mají stejné operace

D: **Homomorfismus** mezi algebrami stejného typu je zob. slučitelné se $\forall$ operacemi.

Izomorfismus algeber je bijektivní homomorfismus, tj. zob. prosté, na, slučitelné s operacemi.

D: $\mathcal{R} = (R, +, \cdot, -, 0, 1)$ buď okruh, $I \subseteq R$. I je pravý (resp. levý) ideál pokud
- I je podgrupa $R(+)$
- $\forall i \in I, \forall r \in R$: $i \cdot r \in I$ (resp $r \cdot i \in I$) $\forall r \in R$ $Ir \in I$

I je ideál, pokud je pravý a zároveň levý ideál.

Homomorfismus = zob. $f(a \cdot b) = f(a) \cdot f(b)$

kongruence = ekvivalence $a \sim b \Leftrightarrow \alpha(a) \sim \alpha(b)$

obojí to musí být slučitelné se $\forall$ operacemi

ALGEBRA I DEFINICE

1. PŘEDMĚTY ZKOUMÁNÍ

D: Pro každé celé $n \geq 0$ nazveme *n-ární operací* na mn. A každé zob. $A^n \to A$, číslo n budeme nazývat *aritou* nebo *četností* operace.

D: Máme-li bin. op $*$ na mn. A, nějakou $U \subseteq A$, $\circ$ bin op. na B. Řekneme, že U je *uzav.* na op. $*$ jestliže $\forall x,y \in U: x*y \in U$. Zob. $f: A \to B$ nazveme *slučitelné* s operacemi $*$ a $\circ$ je-li $\forall x,y \in A$ $f(x*y) = f(x) \circ f(y)$.

D: *Relací* na mn. A rozumíme lib. podmn. $A \times A$. Nechť ρ je relace na A, označme:
- *opačná relace*: $\rho^{-1} = \{(b,a) \mid (a,b) \in \rho\}$
- *tranzitivní obal*: $\rho^{+} = \{(a,b) \mid \exists a=a_0, a_1, \dots, a_{m-1}, a_m = b \in A; (a_i, a_{i+1}) \in \rho\}$
- *identita*: $id = \{(a,a) \mid a \in A\}$

Řekneme, že ρ je
- *symetrická*, jestliže $\rho^{-1} \subseteq \rho$
- *reflexivní*, jestliže $id \subseteq \rho$
- *tranzitivní*, jestliže $\rho^{+} \subseteq \rho$
- *ekvivalence*, jestliže ρ je symetrická, reflexivní, tranzitivní.

D. Je-li ρ ekvivalence na A, *faktorem množiny* A (= *kvocientem*) podle ekvivalence ρ je mn. $A/\rho = \{[a]_\rho \mid a \in A\}$, kde $[a]_\rho = \{b \in A \mid (a,b) \in \rho\}$ jsou *rozkladové třídy* (= *kosety*), tedy A/ρ tvoří *rozklad množiny* A. Naopak máme-li $\{B_i \mid i \in I\}$ rozklad mn. A, pak relace ρ určená podmínkou $(a,b) \in \rho \Leftrightarrow \exists i \in I: a,b \in B_i$ je ekvivalencí a $A/\rho = \{B_i \mid i \in I\}$.

D: *Jádro zobrazení* f je $\ker f = \{(x,y) \in A \times A \mid f(x) = f(y)\}$. $f: A^2 \to B$
homomorfismu φ je $Ker(\varphi) = \{a \in G \mid \varphi(a) = 1\}$

2. ZÁKLADY ELEMENTÁRNÍ TEORIE ČÍSEL

D: Dělitelnost $v\ \mathbb{Z}$, $a,b,c \in \mathbb{Z}$, $d \in \mathbb{N}_0$
- a *dělí* b $(a \mid b) \overset{def.}{\equiv} \exists c: b = a \cdot c$

greatest common divisor
- $c = GCD(a,b) \in \mathbb{N}_0$ je *největší spol. dělitel*, jestliže $(c \mid a \wedge c \mid b)$ & $d: d \mid a \wedge d \mid b \Rightarrow d \mid c$

least common multiple $lcm(a,b)$ nejmenší spol. násobek
- $p \in \mathbb{N} \setminus \{1\}$ je *prvočíslo*, jestliže $p = a\,b \Rightarrow a = \pm 1 \vee b = \pm 1$.

je ekvivalence → D: Na $\mathbb{Z}$ pro $m \in \mathbb{N}, m \geq 2$ definujeme *kongruenci* $\equiv \pmod m$ předpisem $a \equiv b \pmod m \Leftrightarrow m \mid (a-b)$.

D: Uvažujme na mn. A bin op. $*$ a ekvivalenci $\sim$. Řekneme, že $\sim$ je slučitelná s op. $*$, jestliže $\forall a_1, a_2, b_1, b_2 \in A: a_1 \sim b_1 \wedge a_2 \sim b_2 \Rightarrow (a_1 * a_2) \sim (b_1 * b_2)$. $k < m$, $k \in \{0,1,\dots,m-1\}$

D: *Eulerovou fcí* nazveme zob. $\varphi: \mathbb{N} \to \mathbb{N}$ dané předpisem $\varphi(m) = |\{k \in \mathbb{Z}_m \mid GCD(k,m) = 1\}|$

3. ASOCIATIVNÍ BINÁRNÍ OPERACE

D: Bin. op. $*$ na mn. A je *asociativní* pokud $\forall a,b,c \in A$: $a*(b*c) = (a*b)*c$,
resp. *komutativní* pokud $\forall a,b \in A$: $a*b = b*a$

D: Buď $*$ bin. op na A. *Neutrálním prvkem* $e \in A$ op. $*$ ~~rozum~~ splňuje $\forall a \in A$: $e*a = a*e = a$.

D: Nechť $\cdot$ je bin. op na A a 1 je neutr. prvek vzhledem k $\cdot$. Řekneme, že $a \in A$ je *invertibilní* pokud $\exists a^{-1} \in A: a^{-1} \cdot a = a \cdot a^{-1} = 1$. Prvek a^{-1} nazveme *inverzním prvkem* k prvku a.

D: Je-li G množina s bin. op. $\cdot$
- *grupoid* je $G(\cdot)$
- *pologrupa*: $\cdot$ asociativní $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *monoid*: pologrupa s neutr. prvkem $\exists e \in G$ $g \in G$: $g \cdot e = e \cdot g = g$
- *grupa*: monoid, kde $\forall g \in G: \exists g^{-1}$ $\forall g \in G$ jsou invertibilní
- *komutativní (abelovská) grupa*: grupa, kde $\cdot$ je komut. $a \cdot b = b \cdot a$ $\forall a,b \in G$

Restrikce operace $\cdot$ na mn. H zn. $\cdot|_H$

Pro monoid $S(\cdot)$ bude mn. invertibilních prvků značena S^*.

4. GRUPY A PODGRUPY

D: *Podgrupou* grupy $G(\cdot)$ budeme rozumět každou $H \subseteq G$, kt. je uzav. na $\cdot$, obsahuje neutr. prvek $1 \in H$ a pro $\forall h \in H$ platí $h^{-1} \in H$ (zn. $H \leq G$). H je *normální podgrupa* grupy $G(\cdot)$

norm podgrupy (zn. $H \trianglelefteq G$) je-li H podgrupa G a navíc $\forall g \in G, \forall h \in H: g \cdot h \cdot g^{-1} \in H$. resp. $g^{-1} \cdot h \cdot g \in H$

rmod = lmod D: Buď $H \leq G$, $G(\cdot)$ grupa. Definujme relaci rmod H, lmod H. $a,b \in G$

$(a,b) \in r\bmod H \Leftrightarrow a \cdot b^{-1} \in H \Leftrightarrow b^{-1} \cdot a \in H$

$(a,b) \in l\bmod H \Leftrightarrow a^{-1} \cdot b \in H \Leftrightarrow b \cdot a^{-1} \in H$

D: $G(\cdot)$ grupa, $H \leq G$, $K \leq G$, $a \in G$. Označme $H \cdot K = \{h \cdot k \mid h \in H, k \in K\}$, $aH = \{a\}H$, $Ha = H\{a\}$. $hk = h \cdot k$, $HK = H \cdot K$

D: Buď $H \leq G(\cdot)$, $G(\cdot)$ grupa. Potom číslu $[G:H] = |G/r\bmod H| = |G/l\bmod H|$ říkáme **index podgrupy** H v grupě G. Velikost $|G|$ mn. G nazýváme **řád grupy** G.

5. HOMOMORFISMY A IZOMORFISMY GRUP

slučitelnost $G(\cdot), H(*)$ $f(g_1) \cdot f(g_2) = f(g_1 * g_2)$ $\in H$? ?

D: Zob. $f: G \to H$ grup $G(\cdot)$ a $H(\cdot)$ slučitelné s jejich bin. operacemi se nazývá (grupový) **homomorfismus**. Bijektivní homomorfismus budeme nazývat **izomorfismus**.
Podmnožině $\mathrm{Ker} f := \{g \in G \mid f(g) = 1\}$
i relaci $\ker f := \{(g_1, g_2) \in G \times G \mid f(g_1) = f(g_2)\}$ budeme říkat **jádro** homomorfismu.
Že G_1 a G_2 grupy jsou izomorfní (tj. $\exists$ mezi nimi izomorfismus) značíme $G_1 \cong G_2$.

D: Buď $G(\cdot)$ grupa ρ ekvivalence na G. Pak **přirozená projekce** na faktorovou mn. G/ρ je zob. $\pi_\rho: G \to G/\rho$ daná podmínkou $\pi_\rho(g) = [g]_\rho$, kde $g \in G$.

D: Grupě zavedenou na faktorové množině budeme nazývat **faktorovou grupou**.
Každé ekv. ρ slučitelné s bin. op. na grupě jednoznačně odpovídá normální podgrupa $H = [1]_\rho$, to nám umožňuje faktorovou množinu zapisovat ve tvaru G/H, tedy $G/H := G/r\bmod H$.
$G/\rho(\cdot) = G/H(\cdot)$, kde $H = [1]_\rho$ & $[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho$
přiroz. projekce $G \to G/H$ značíme π_H a místo $[a]_\rho$ píšeme $[a]_H = aH = Ha$

6. CYKLICKÉ GRUPY

D: Buď $G(\cdot)$ grupa a $X \subseteq G$. Podgrupu $\langle X \rangle$ nazveme **podgrupou $G(\cdot)$ generovanou množinou X**,
$\langle X \rangle := \bigcap \{H$ je podgrupa $G(\cdot) \mid X \subseteq H\}$ = nejmenší podgrupa obsahující prvky X
Řekneme, že $G(\cdot)$ je **cyklická grupa**, jestliže $\exists g \in G$: $\langle g \rangle = G$. $\langle \{g\} \rangle$

D: Značení: $G(\cdot)$ grupa, $g \in G$, $z \in \mathbb{Z}$ mocnění $z > 0$: $g^z = \underbrace{g \cdots g}_{z\times}$, $z = 0$: $g^z = g^0 = 1$, $z < 0$, $g^z = (g^{-1})^{-z}$ $\quad z > 0$: $g^z = g^{z-1} \cdot g$

4. EULEROVA VĚTA A PROTOKOL RSA

D: $G(\cdot)$ grupa, $g \in G$. **Řád prvku** g je $m = |\langle g \rangle|$. Alternativně nejmenší $m \geq 1$ t.ž. $g^m = 1$ pokud $\exists$
Exponent prvku g je lib. m: $g^m = 1$.

8. UNIVERZÁLNÍ POHLED: POJEM ALGEBRY

D: Je-li I mn., budeme říkat zobrazení $\Omega: I \to \mathbb{N}_0$ **typ**. Řekneme, že $A(\alpha_i \mid i \in I)$ je **algebra** typu Ω, je-li A neprázdná a pro $\forall i \in I$ je α_i právě $\Omega(i)$-ární operací na A. $\alpha_i: A^{\Omega(i)} \to A$

D: Buď α n-ární op. na A. Řekneme, že $B \subseteq A$ je **uzavřená na operaci** α, jestliže $\alpha(a_1, \dots, a_m) \in B$ pro $\forall a_1, \dots, a_m \in B$. Řekneme, že B je **podalgebrou** algebry $A(\alpha_i \mid i \in I)$, je-li B uzav. na $\forall$ operaci α_i, $i \in I$.
Označíme-li $\beta_i = \alpha_i|_{B^n}$ restrikci n-ární operace α_i na B^n, potom pro podalgebru B leží $\forall$ hodnoty zob. β_i opět v B. Zobrazení β_i lze tedy chápat jako operace na mn. B a tak dostáváme strukturu algebry $B(\beta_i \mid i \in I)$ na každé podalgebře B.

D: Nechť α označuje m-ární op. na A i B. Řekneme, že **zob** $f: A \to B$ je **slučitelné s op. α**, jestliže $f(\alpha(a_1, \dots, a_m)) = \alpha(f(a_1), \dots, f(a_m))$.
Zob. $f: A \to B$ mezi dvěma algebrami $A(\alpha_i \mid i \in I)$, $B(\alpha_i \mid i \in I)$ stejného typu Ω budeme říkat **homomorfismus**, je-li sluč. se všemi operacemi α_i, $i \in I$. Bijektivní homomorfismus budeme nazývat **izomorfismus**. Jestliže $\exists$ izomorfismus mezi algebrami $A(\alpha_i \mid i \in I)$ a $B(\alpha_i \mid i \in I)$, říkáme, že A a B **jsou izomorfní** (zn. $A \cong B$).

D: Nechť ρ je ekvivalence a α je m-ární op. na mn. A. Řekneme, že ρ je **slučitelná s α**, jestliže pro každý systém prvků $a_1, \dots, a_m, b_1, \dots, b_m \in A$ pro které $(a_i, b_i) \in \rho$ $i = 1, \dots, n$ platí, že $(\alpha(a_1, \dots, a_m), \alpha(b_1, \dots, b_m)) \in \rho$. Je-li $A(\alpha_i \mid i \in I)$ algebra a ρ ekvivalence na A, pak ρ nazveme **kongruencí**, je-li ρ sluč. se $\forall$ op. α_i, $i \in I$.

D: Nechť ρ je ekvivalence a α m-ární op. na A. Je-li ρ sluč. s α, definujeme **op. α na faktoru** A/ρ předpisem $\alpha([a_1]_\rho, \dots, [a_m]_\rho) = [\alpha(a_1, \dots, a_m)]_\rho$. Je-li ρ kongruencí na algebře A, pak tímto zp. definujeme na A/ρ strukturu algebry stejného typu.

D: Nechť $\rho \subseteq \sigma$ jsou dvě ekv. na A. Definujme relaci σ/ρ na A/ρ následovně:
$([a]_\rho, [b]_\rho) \in \sigma/\rho \Leftrightarrow (a, b) \in \sigma$.

9. IZOMORFISMY ALGEBER

D: Buď A algebra $X \subseteq A$. Potom podalgebra $\langle X \rangle$ algebry A, kt. dostaneme jako průnik $\forall$ podalgeber A obsahujících mn. X nazveme **podalgebra generovaná X**. (tj. X generuje podalgebru $\langle X \rangle$).

10. OKRUHY A IDEÁLY

D: Nechť $\mathcal{R} = R(+,\cdot,-,0,1)$ je algebra typu $(2,2,1,0,0)$.
Řekneme, že jde o:

- <u>okruh</u>, jestliže
  - $R(+)$ je komutativní grupa s $-$ (op. opačného prvku), 0 (neutr. prvek)
  - $R(\cdot)$ je monoid s 1 (neutr. prvek)
  - $\forall a,b,c \in R$: $a\cdot(b+c) = a b + a\cdot c$, $(a+b)\cdot c = a\cdot c + b\cdot c$ — distributivita

Podokruhem okruhu $\mathcal{R}$ je každá podalgebra algebry $\mathcal{R}$.

- <u>komutativní okruh</u>, je-li $\mathcal{R}$ okruh a $\cdot$ je komutativní
- <u>obor</u> (integrity), je-li $\mathcal{R}$ komutativní okruh a $\forall a,b \in R \quad a\cdot b = 0 \Rightarrow a = 0 \vee b = 0$
- <u>těleso</u>, jestliže $\mathcal{R}$ je okruh a $R^* = R - \{0\}$ (tj. ∀ prvky $\neq 0$ jsou v $R(\cdot)$ invertibilní) $0 \neq 1$
- <u>komutativní těleso</u>, je-li $\mathcal{R}$ těleso a $\cdot$ je komutativní.

Prvek okruhu $\mathcal{R}$ je invertibilní jedná-li se o invertibilní prvek monoidu $R(\cdot)$

D: $\mathcal{R} = R(+,\cdot,-,0,1)$ buď okruh, $I \subseteq R$. Řekneme, že I je <u>pravý</u> (resp. <u>levý</u>) <u>ideál</u>, jestliže:
- I je podgrupa $R(+)$
- $\forall i \in I \ \forall r \in R$: $i \cdot r \in I$ (resp. $r \cdot i \in I$).

I je <u>ideál</u>, je-li pravý a zároveň levý ideál.
<u>Homomorfismus</u> (<u>izomorfismus</u>) <u>okruhů</u> je homom. (resp. izomorf.) příslušných algeber.
triviální ideály $\{0\}$, R hlavní ideály aR, resp. $Ra = \{r\cdot a \mid r \in R\}$ $a \in R$

D: O (levém, pravém) <u>ideálu</u> I okruhu $R(+,\cdot,-,0,1)$ řekneme, že je <u>vlastní</u>, jestliže $I \neq \{0\}$ a $I \neq R$ a, ~~že je maximální, jestliže $I \neq R$~~ a neexistuje žádný (levý, pravý) ~~ideál J splňující $I \subseteq J \subset R$ a $I \neq J \neq R$.~~

D: <u>Okruh</u> je <u>jednoduchý</u> pokud neobsahuje žádné vlastní (oboustranné) ideály a zároveň se nejedná o těleso.

D: Uvážíme-li ideál I okruhu $R(+,\cdot,-,0,1)$ pak I je podgrupa grupy $R(+)$, tedy můžeme pracovat s ekvivalencí <u>$r \bmod I$</u> danou podmínkou
$(a,b) \in r \bmod I \Leftrightarrow a-b = a+(-b) \in I$.

D: Je-li I ideál okruhu $R(+,\cdot,-,0,1)$, potom faktorovou algebru $R/I(+,\cdot,-,[0]_I,[1]_I)$ nazýváme faktorový okruh (= <u>faktorokruh</u>) okruhu R podle ideálu I.

D: Buď okruh. Položme $R[x] = \{p : \mathbb{N}_0 \to R \mid \{m \mid p(m) \neq 0\}$ je konečná$\}$. Prvek $p \in R[x]$ budeme zapisovat také ve tvaru $p = \sum_{m\in\mathbb{N}_0} p_m x^m$, kde $p_m = p(m)$, tedy $R[x]$ obsahuje právě všechny formální nekonečné sumy s konečným nosičem. Na $R[x]$ definujeme bin. operace $+$ a $\cdot$, unární op. $-$ a nulární operace $\mathbf{0}$ a $\mathbf{1}$ pro
pro $p = \sum_{m\in\mathbb{N}_0} p_m x^m$ a $q = \sum_{m\in\mathbb{N}_0} q_m x^m$:

$$p+q = \sum_{m\in\mathbb{N}_0} (p_m+q_m) x^m$$
$$p\cdot q = \sum_{m\in\mathbb{N}_0} \Big(\sum_{i=0}^{m} p_i \cdot q_{m-i}\Big) x^m$$
$$-p = \sum_{m\in\mathbb{N}_0} -p_m x^m$$
$$\mathbf{0} = \sum_{m\in\mathbb{N}_0} 0 x^m$$
$$\mathbf{1} = 1x^0 + \sum_{m\in\mathbb{N}} 0 x^m \quad (m>0)$$

Je-li $p \neq \mathbf{0}$, budeme největší takové $m \in \mathbb{N}_0$, že $p_m \neq 0$, nazývat <u>stupeň polynomu</u> p. (zn. st p)
Stupeň polynomu $\mathbf{0}$ položíme roven -1.
Okruh $R[x](+,\cdot,-,\mathbf{0},\mathbf{1})$ nazýváme <u>okruhem polynomů</u> jedné neurčité a jeho prvky <u>polynomy</u>.

11. KONSTRUKCE TĚLES

D: Nechť $\mathcal{R} = R(+,\cdot,-,0,1)$ je komutativní okruh. Řekneme, že <u>ideál</u> I okruhu $\mathcal{R}$ je <u>maximální</u> pokud $I \neq R$ a kdykoliv existuje ideál J takový že $I \subseteq J$ potom buď $J = I$ nebo $J = R$.

Jestliže $a,b \in R$, definujeme $a \mid b$, <u>a dělí b</u>, standardním vztahem $(\exists c \in R)\ ac = b$.
O neinvertibilním nenulovém prvku $p \in R$ řekneme, že je <u>ireducibilní</u>, pokud pro každý rozklad $p = a\cdot b$ platí, že je a nebo b invertibilní.

F je konečné těleso $|F| = p^n$, $p \in \mathbb{P}$, $n \in \mathbb{N}$

D: $R(+,\cdot,-,0,1)$ obor, definujme algebru $F(+,\cdot,-,0,1)$, kde $F = R \times R \setminus \{0\}$ s operacemi

$(a,b)\cdot(c,d) = (a\cdot c,\ b\cdot d)$ $\qquad 0 = (0,1)$
$(a,b) + (c,d) = (a\cdot d + b\cdot c,\ b\cdot d)$ $\qquad 1 = (1,1)$
$-(a,b) = (-a, b)$

Na algebře $F(+,\cdot,-,0,1)$ definujeme relaci $\sim$ předpisem $(a,b) \sim (c,d) \Leftrightarrow a\cdot d = b\cdot c$

D: Komutativní těleso $F/_\sim$ budeme nazývat podílovým tělesem okruhu R a jeho prvky ozn. $\frac{a}{b} = [(a,b)]_\sim$

12. SVAZY

D: Relaci $\leq$ na mn. M budeme říkat ~~uspořádání~~, je-li reflexivní a tranzitivní a splňuje podmínku $a \leq b$ && $b \leq a \Rightarrow a = b$ pro $\forall a, b \in M$ (tj. jde o slabě antisymetrickou relaci). Dvojice $(M, \leq)$ se nazývá uspořádaná množina.

D: Nechť $\leq$ je uspořádání na mn. M, $A \subseteq M$. Řekneme, že $m \in M$ je nejmenší (resp. největší) prvek mn. A jestliže $m \leq a$ (resp. $a \leq m$) pro $\forall a \in A$.

Supremem (resp. infimem) mn. A je nejmenší prvek mn. $\{m \in M \mid \forall a \in A : a \leq m\}$ zn. $\sup_{\leq}$.
(resp. největší prvek mn. $\{m \in M \mid \forall a \in A : m \leq a\}$) zn. $\inf_{\leq}$.

Dvojici $(M, \leq)$ budeme říkat svaz, pokud pro každé dva prvky $a, b \in A$ existuje supremum a infimum mn. $\{a, b\}$. Svaz $(M, \leq)$ je úplným svazem, existuje-li supremum a infimum každé podmnožiny M.

Zn.: $\forall m, n \in M$ značíme $m \vee n = \sup_{\leq}(m, n)$ ↑, $m \wedge n = \inf_{\leq}(m, n)$ ↓

Bin. operaci $\vee$ nazveme spojení a op. $\wedge$ průsek.

D: Nechť $f: A \to B$ je zob. a $(A, \leq)$, $(B, \leq)$ jsou svazy. Řekneme, že f je homomorfismus (izomorfismus) jde-li o homomorfismus (izomorfismus) algeber $A(\wedge, \vee)$ a $B(\wedge, \vee)$. A f nazveme monotónním zob. platí-li implikace $a_1 \leq a_2 \Rightarrow f(a_1) \leq f(a_2)$. Podsvazem svazu $A(\wedge, \vee)$ budeme rozumět podalgebru algebry $A(\wedge, \vee)$

D: Nechť A je mn., $C \subseteq \mathcal{P}(A)$ je nějaký systém podmnožin mn. A. Řekneme, že C je uzávěrovým systémem nad A, pokud: 1) $A \in C$
2) pro $\forall$ podsystém $\{B_i \mid i \in I\} \subseteq C$, je $\bigcap \{B_i \mid i \in I\} \in C$.

13. BOOLEOVY ALGEBRY

D: O svazu $S(\wedge, \vee)$ řekneme, že je modulární, jestliže pro $\forall a, b, c \in S$ takovou, že $a \leq c$, platí rovnost $a \vee (b \wedge c) = (a \vee b) \wedge c$. Svaz je distributivní platí-li pro $\forall a, b, c \in S$ rovnost $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

D: Nechť svaz $S(\wedge, \vee)$ má nejmenší prvek 0 a největší prvek 1. Prvek $a \in S$ nazveme atomem (resp. koatomem), jestliže a pokrývá 0 (resp. 1 pokrývá a).
Komplementem prvku $a \in S$ nazveme takový prvek $a' \in S$, že $a \vee a' = 1$ a $a \wedge a' = 0$.

D: Nechť $(M, \leq)$ je usp. mn., $a, b, c \in M$. Řekneme, že prvek b pokrývá prvek a (píšeme $a \prec b$), jestliže ($a \leq b$, $a \neq b$, & $a \leq c \leq b$) $\Rightarrow$ ($c = a$ nebo $c = b$). Hasseovým diagramem uspořádané mn. $(M, \leq)$ rozumíme orientovaný graf, jehož vrcholy tvoří prvky mn. M a a je s b spojen takovou hranou, že b se nachází výše než a právě když b pokrývá a.

D: Booleovou algebrou nazveme takovou algebru $S(\vee, \wedge, 0, 1, ')$, že $S(\wedge, \vee)$ je distributivní svaz s největším prvkem 1 a nejmenším prvkem 0 a unární operace $'$ přiřadí každému prvku jeho komplement. Homomorfismem (izomorfismem) Booleových algeber v obvyklém smyslu.

ALGEBRA I
POJMY

Relace ϱ na mn. X

- reflexivní $\Longleftrightarrow$ $\forall x \in X$: $x \varrho x$ - - - - - $id \subseteq \varrho$
- symetrická $\Longleftrightarrow$ $\forall x,y \in X$: $x \varrho y \Rightarrow y \varrho x$ - - - - - $\varrho^{-1} \subseteq \varrho$
- tranzitivní $\Longleftrightarrow$ $\forall x,y,z \in X$: $x \varrho y \wedge y \varrho z \Rightarrow x \varrho z$ - - - - - $\varrho^{+} \subseteq \varrho$
- (slabě) antisymetrická $\Longleftrightarrow$ $\forall x,y \in X$, $x \neq y$: $x \varrho y \Rightarrow \neg y \varrho x$ tj. $\Leftrightarrow x \varrho y \wedge y \varrho x \Rightarrow x = y$ $\varrho \cap \varrho^{-1} \subseteq id$
- silně antisymetrická $\Longleftrightarrow$ $\forall x,y \in X$: $x \varrho y \Rightarrow \neg y \varrho x$ - - - - - $\varrho \cap \varrho^{-1} = \emptyset$
- antireflexivní $\Longleftrightarrow$ $\forall x \in X$: $\neg (x \varrho x)$ - - - - - $\varrho \cap id = \emptyset$

- ekvivalence • reflexivní $\wedge$ symetrická $\wedge$ tranzitivní
- (neostré) uspořádání • reflexivní $\wedge$ antisymetrická $\wedge$ tranzitivní
- ostré • antireflexivní $\wedge$ tranzitivní
- kvaziuspořádání • reflexivní $\wedge$ tranzitivní Př: dělitelnost

$m\mathbb{Z} = \{m \cdot z \mid z \in \mathbb{Z}\}$

$f_m: \mathbb{Z} \to m\mathbb{Z}$ $\qquad\qquad$ $F_m: \mathbb{Z} \to \mathbb{Z}_m$

$f_m(k) = m \cdot k$ $\qquad\qquad$ $a \to (a) \bmod m$

- Buď A mn. s bin. operací $*$
  $U \subseteq A$
  B mn. s bin. operací $\circ$.

U je uzavřená na operaci $*$, jestliže $\forall a,b \in U: a * b \in U$.

Zob. $f: A \to B$ je slučitelné s operacemi $*$ a $\circ$, jestliže $\forall a,b \in A: f(a*b) = f(a) \circ f(b)$.

- Značení - relace

$\varrho^{-1} = \{(b,a) \mid (a,b) \in \varrho\}$

$\varrho^{+} = \{(a,b) \mid \exists\, a = a_0, a_1, \dots, a_{n-1}, a_n = b \in A;\ (a_i, a_{i+1}) \in \varrho\} = \bigcup_{n \geq 1} \varrho^n$ tranzitivní obal

$id = \{(a,a) \mid a \in A\}$ identita

$\varrho^2 = \varrho \circ \varrho = \{(x,z) \mid \exists y: x \varrho y \wedge y \varrho z\}$

$\varrho^n = \{(x,y) : \exists x_1, \dots, x_{n-1}: x \varrho x_1 \varrho x_2 \dots x_{n-1} \varrho y\}$

když už je dán ϱ^2 tak jsou tam v mocnině

Základní v. aritmetiky: Každé ~~číslo~~ přirozené číslo > 1 má až na pořadí jednoznačný rozklad

- kongruence (mod m) $\quad a \equiv b \pmod m \overset{def.}{\equiv} m \mid a - b \quad$ (na $\mathbb{Z}$, $m \in \mathbb{N}, m \geq 1$).
  ↳ ekvivalence

Buď $a,b,c,d \in \mathbb{Z}$, $m,k \in \mathbb{N}$, $m \geq 1$

- $a \equiv b \pmod m \wedge c \equiv d \pmod m \Rightarrow$
  $a + c \equiv b + d \pmod m$
  $a \cdot c \equiv b \cdot d \pmod m$
  $a - c \equiv b - d \pmod m$
  $a^k \equiv b^k \pmod m$
- $c > 0$ $\quad a \equiv b \pmod m \Leftrightarrow$
  $\Leftrightarrow a \cdot c \equiv b \cdot c \pmod{c \cdot m}$
- $c > 0: GCD(c,m) = 1$: $\quad a \equiv b \pmod m$
  $\Leftrightarrow ac \equiv bc \pmod m$

- Buď A mn., $*$ bin. op. na A
  $\sim$ ekvivalence na A.

Pak $\sim$ je slučitelná s $*$, jestliže $a \sim b$, $c \sim d \Rightarrow a * c \sim b * d$, $\forall a,b,c,d \in A$.

- Eulerova fce je $\varphi: \mathbb{N} \to \mathbb{N}$, $\varphi(n) = |\{k \in \mathbb{Z} \mid GCD(k,n) = 1, k \leq n\}|$.

- faktor množiny (= kvocient) rozklad A podle ekv. ϱ je $A/\varrho = \{[a]_\varrho \mid a \in A\}$, kde
  $[a]_\varrho = \{b \in A \mid (a,b) \in \varrho\}$ jsou rozkladové třídy (= kosety)
- Jádro zobrazení $f: X \to Y$ je i) $\ker f := \{(x,y) \mid f(x) = f(y)\}$

- Lemma: p prvočíslo 1) $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$
2) $p \mid a_1 a_2 \ldots a_k \Rightarrow \exists i : p \mid a_i$

- $G : \mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}_{m_i}$ $a \in \mathbb{Z}$

$G(a) = ((a) \bmod m_1, (a) \bmod m_2, \ldots, (a) \bmod m_k)$

$H : \mathbb{Z}_m \to \prod_{i=1}^{k} \mathbb{Z}_{m_i}$ $a \in \mathbb{Z}_m$ tedy $a \in \{0, \ldots, m-1\}$

$H(a) = ((a) \bmod m_1, (a) \bmod m_2, \ldots, (a) \bmod m_k)$

Čínská v. o zbytcích: $m_1, \ldots, m_k \in \mathbb{N} \setminus \{1\}$, $m = \prod_{i=1}^{k} m_i$, zobrazení $H : \mathbb{Z}_m \to \prod_{i=1}^{k} \mathbb{Z}_{m_i}$ je slučitelné s $+, \cdot$.

H je bijekce $\Leftrightarrow \forall i \neq j \;\; GCD(m_i, m_j) = 1$

Malá Fermatova věta: p prvočíslo, $a \in \mathbb{Z}$, $GCD(a, p) = 1$:
Platí: $a^{p-1} \equiv 1 \pmod{p}$
$\Updownarrow$
$a^p \equiv a \pmod{p}$ to znamená $p \mid a^p - a$

Zobecnění: $a^{\varphi(p)} \equiv 1 \pmod{p}$

Věta: Buď $p_1 < p_2 < \ldots < p_k$ prvočísla, $r_1, r_2, \ldots, r_k$ kladná celá čísla. Potom

$$\varphi\left(\prod_{i=1}^{k} p_i^{r_i}\right) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1}$$

- Eulerova fce $\varphi : \mathbb{N}^+ \to \mathbb{N}^+$

$\varphi(1) = 1$

$\varphi(p) = p - 1$ $p \in \mathbb{P}$

$\varphi(p^m) = (p-1) \cdot p^{m-1}$; $p \in \mathbb{P}, m \in \mathbb{Z}^+$

$x, y \in \mathbb{Z}^+, GCD(x, y) = 1$: $\varphi(xy) = \varphi(x) \cdot \varphi(y)$

Bin. operace

- je-li $*$ bin. op. na A, $e \in A$ splňující $e * a = a * e = a, \forall a \in A$ se nazývá neutr. prvek.
- je-li $\cdot$ bin. op. na A, 1 neutr. prvek k $\cdot$. Pak $a^{-1} \in A$ nazveme inverzní prvek k $a \in A$, pokud platí: $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Pro monoid $A(\cdot)$ značíme mn. všech invertibilních prvků A^*
- Každá bin. op má nejvýše 1 neutr. prvek
- $s \in S$ je invertibilní, pokud $\exists\, s^{-1} \in S$: $s^{-1} s = s^{-1} s = 1$. Prvek s^{-1} je inverz k s.

- je-li G mn. s bin. op. $\cdot$
  - $G(\cdot)$ je grupoid
  - pologrupa : $\cdot$ asociativní
  - monoid : pologrupa s neutr. prvkem
  - grupa : monoid, kde $\forall g \in G : \exists g^{-1}$
  - komutativní (abelovská) grupa : grupa, kde $\cdot$ je komut. $a \cdot b = b \cdot a$

- Restrikce operace $\cdot$ na mn. H značíme $\cdot|_H$

průnik podgrup je grupa
$K \cap H = \langle K \cap H \rangle$
spojení $K \vee H := \langle K \cup H \rangle$
součin $K \cdot H := \{h \cdot k : h \in H, k \in K\}$

Def. $G(\cdot)$ je <u>grupa</u>, jestliže $G(\cdot)$ je monoid splňující $\forall g \in G\ \exists g^{-1}: g \cdot g^{-1} = g^{-1} \cdot g = 1$
↳ • uzavřenost
• asociativita

Def. Je-li $G(\cdot)$ grupa a $H \subseteq G$, pak H je <u>podgrupa</u> grupy $G(\cdot)$ jestliže je H uzav. na $\cdot$, dále $1 \in H$, a pro $\forall h \in H$ platí $h^{-1} \in H$. Zn. $H \leq G$

Def. H je <u>normální podgrupa</u> grupy $G(\cdot)$, je-li H podgrupa a $\forall g \in G: \forall h \in H: g^{-1} h g \in H$. popř. $g h g^{-1} \in H$

Def. $H \leq G$, $G(\cdot)$ grupa, definujme relaci $r \bmod H$ a $l \bmod H$ $\quad a, b \in G$

$(a,b) \in r \bmod H \overset{def}{\equiv} a \cdot b^{-1} \in H \Leftrightarrow b^{-1} a \in H$
$(a,b) \in l \bmod H \overset{def}{\equiv} a^{-1} \cdot b \in H \Leftrightarrow b a^{-1} \in H$

Def. Buď H podgrupa $G(\cdot)$ grupy. Potom číslo $[G:H] = |G/r \bmod H| = |G/l \bmod H|$ (tj. # ekviv. tříd) říkáme <u>index podgrupy</u> H v grupě G.
Velikost $|G|$ množiny G nazýváme <u>řád grupy</u> G.

V: (<u>Lagrange</u>) Je-li $H \leq G(\cdot) \Rightarrow |G| = [G:H] \cdot |H|$.
Důsl.: Je-li $G(\cdot)$ konečná $\Rightarrow \forall H \leq G: |H|$ dělí $|G|$

slučitelnost zob. s operacemi
$G(\cdot)\ H(*)\quad f(g_1) \cdot f(g_2) = f(g_1 * g_2)$

Def. Zob. $f: G \to H$, $G(\cdot)$ a $H(\cdot)$ grupy, slučitelné s jejich bin. operacemi se nazývá (grupový) <u>homomorfismus</u>.
Bijektivní homomorfismus budeme nazývat <u>izomorfismem</u>.
Podmnožině $\operatorname{Ker} f = \{g \in G \mid f(g) = 1\}$ ← neutrální prvek
i relaci $\ker f = \{(g_1, g_2) \in G \times G \mid f(g_1) = f(g_2)\}$ budeme říkat <u>jádro homomorfismu</u>.
Že G_1 a G_2 jsou izomorfní (tj. $\exists$ mezi nimi izomorfismus) značíme $G_1 \cong G_2$

Def. Buď $G(\cdot)$ grupa, ρ ekvivalence na G. Pak <u>přirozená projekce</u> na faktorovou množinu G/ρ je zob. $\pi_\rho: G \to G/\rho$ dané podmínkou $\pi_\rho(g) = [g]_\rho$, kde $g \in G$. $\ker \pi_\rho = \rho$?

V5.5: Nechť $f: G_1 \to G_2$ je homomorfismus grup G_1 a G_2.
(1) (<u>Věta o homomorfismu</u>)
Je-li H normální podgrupa $G_1(\cdot)$, pak
($\exists$ homomorfismus $g: G_1/H \to G_2$ splňující: $g \pi_H = f$) $\Leftrightarrow H \subseteq \operatorname{Ker} f$
(tj. $r \bmod H \subseteq r \bmod \operatorname{Ker} f$)

Navíc, jestliže g existuje, je g izomorfismus $\Leftrightarrow$ f je <u>na</u> a $\operatorname{Ker} f = H$.

(2) (<u>1. věta o izomorfismu</u>)
$f(G_1)$ je podgrupa G_2 a $G_1/\operatorname{Ker} f(\cdot)$ je izomorfní $f(G_1)(\cdot)$.

V5.6: (<u>2. věta o izomorfismu</u>)
Nechť $G(\cdot)$ je grupa a H, K její normální podgrupy. Jestliže $H \subseteq K$, pak K/H je normální podgrupa grupy $G/H(\cdot)$ a faktorová grupa $G/K(\cdot)$ je izomorfní grupě $(G/H)/(K/H)(\cdot)$.

Def: Buď $G(\cdot)$ grupa a $X \subseteq G$. Podgrupu $\langle X \rangle$ nazveme <u>podgrupou</u> $G(\cdot)$ <u>generovanou množinou</u> X.
$\langle X \rangle := \bigcap \{H \text{ podgrupa } G(\cdot) \mid X \subseteq H\}$ $\quad \langle \{g\} \rangle$
Řekneme, že $G(\cdot)$ je <u>cyklická grupa</u>, jestliže $\exists g \in G: \langle g \rangle = G$.

Def: $G(\cdot)$ grupa, $g_1, g_2 \in G$. Řekneme, že g_1 a g_2 jsou <u>konjugované</u> v G pokud $\exists h \in G: h g_1 h^{-1} = g_2$
Permutace σ a τ jsou konjugované pokud $\exists$ permutace $\pi: \pi \sigma \pi^{-1} = \tau$
<u>Typ permutace</u> π = počet a délka nezávislých cyklů v rozkladu π.
Pro permutace platí: $\pi \overbrace{(p_1\ p_2\ p_3 \dots p_m)}^{cyklus} \pi^{-1} = (\pi(p_1)\ \pi(p_2) \dots \pi(p_m))$
Nalezení π pro σ, τ: $\quad \sigma = (1)\ (2)\ (5\ 8\ 3\ 4)\ (6\ 9\ 7)$
$\tau = (3)\ (4)\ (9\ 1\ 5\ 6)\ (2\ 7\ 8)$ ⤳ $\pi \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 5 & 6 & 9 & 2 & 8 & 1 & 3 \end{pmatrix} = (1\,7\,8)(2\,4\,6)(3\,5\,9)$
součin nezávislých cyklů

? cyklus $(p_1\ p_2\ p_3 \dots p_m) = (p_1\ p_2) \circ (p_2\ p_3) \circ (p_3\ p_4) \dots \circ (p_{m-1}\ p_m)$ ← součin transpozic

Def. $G(\cdot)$ grupa, $g \in G$. <u>Řád prvku</u> g je $m = |\langle g \rangle|$. alternativně nejmenší $m \geq 1$ takové, že $g^m = 1$ pokud $\exists$
<u>Exponent prvku</u> g je libovolné <u>m</u>: $g^m = 1$
Pozn: řád m-cyklu je m

V4.7: Nechť $G(\cdot)$ je grupa, ρ relace na G. Pak ρ je ekvivalence slučitelná s $\cdot$ právě tehdy když $H=[1]_\rho$ je normální podgrupa $G(\cdot)$ a $\rho = r\bmod H$ (= $l \bmod H$).

Poz 5.1: Nechť $G_1(\cdot), G_2(\cdot), G_3(\cdot)$ jsou grupy a $f: G_1 \to G_2$, $g: G_2 \to G_3$ homomorfismy.

Poz 4.4. ~~Nechť~~

$[a]_{r \bmod H} = Ha$

(Dú 6)

$G(\cdot)$ grupa. Pro $g,h \in G$ definujeme komutátor $[g,h] := ghg^{-1}h^{-1}$

komutant $G' := [G,G] := \langle \{[g,h] : g,h \in G\} \rangle$

↳ podgrupa generovaná komutátory

Platí $G' \trianglelefteq G$

7 VEKTOROVÉ PROSTORY

Def: Grupa je dvojice $(G,\circ)$, kde G je mn., $\circ$ je bin operace na G, $\circ: G^2 \to G$, a platí:

1. asociativita $\quad \forall a,b,c \in G: \; a\circ(b\circ c) = (a\circ b)\circ c$
2. $\exists$ neutrální prvek $\quad \exists e \in G \; \forall a \in G: \; a\circ e = e\circ a = a$
3. $\exists$ inverze $\quad \forall a \in G \; \exists a^{-1} \in G: \; a\circ a^{-1} = a^{-1}\circ a = e$

Př (neabelovské grupy) (zob. na mn., skládání) př (rotace $\mathbb{R}^n$ podle 0) (permutace, $\circ$) maticová grupa (reg. matice, $\cdot$)

Pro Abelovu (komutativní grupu) navíc → Př: $(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+), (\mathbb{C},+), (\mathbb{R}^{m\times n},+), (\mathbb{Z}_n,+), (\mathbb{Q}\setminus\{0\},\cdot), (\mathbb{R}\setminus\{0\},\cdot)$

4. komutativita $\quad \forall a,b \in G: \; a\circ b = b\circ a$ (reál. polynomy: prom x, +)

⚠ Grupy nejsou: $(\mathbb{N},+), (\mathbb{Z},-), (\mathbb{R}\setminus\{0\},:), \dots$

Vlastnosti v grupě $(G,\circ)$

1. krácení $\quad a\circ c = b\circ c \Rightarrow a = b$
2. jednoznačnost e (neutr. prvku)
3. jednoznačnost inverzu $\quad \forall a \in G: \exists! \, a^{-1}$
4. pro $\forall a,b \in G \; \exists!$ řešení rce $a\circ x = b$
5. $(a^{-1})^{-1} = a$
6. $(a\circ b)^{-1} = b^{-1}\circ a^{-1}$

(symetrická) grupa permutací $\pi: [n] \to [n]$ (bijekce) zn. $(S_n,\circ)$
- není komutativní
- Def: π se skládá z k cyklů: $\operatorname{sgn}(\pi) = (-1)^{n-k}$ < $1 \Rightarrow \pi$ sudá; $-1 \Rightarrow \pi$ lichá (↳ transpozice)
- inverze (i,j): $i<j \wedge \pi(i) > \pi(j)$
- $\operatorname{sgn}(\pi\circ\sigma) = \operatorname{sgn}(\pi)\cdot\operatorname{sgn}(\sigma)$
- $(-1)^{\#\text{inverzí}} = \operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$
- $= \operatorname{sgn}(\pi) = (-1)^t$, kde t je počet transpozic v rozkladu

Def: Podgrupa $(H,\circ) \le (G,\circ)$ když $H \subseteq G \wedge (H,\circ)$ je grupa. ← $e \in H$; $\circ$ uzavřená na H $(\forall a,b \in H: a\circ b \in H)$; $\forall a \in H: a^{-1} \in H$

triviální podgrupy $(G,\circ)$, $(\{e\},\circ)$ $\quad (\mathbb{N},+) \not\le (\mathbb{Z},+) \le (\mathbb{Q},+) \le (\mathbb{R},+) \le (\mathbb{C},+)$

Každá grupa je izomorfní nějaké symetrické grupě. // maticové podgrupě.

Def: Těleso $\mathbb{T} = (T,+,\cdot)$, T mn., $+$, $\cdot$ komutativní bin. operace splňující
(// pole; // komutativní těleso; krát komutativita násobení)

1. $(T,+)$ komutativní grupa, 0 neutrální, $-a$ inverz
2. $(T\setminus\{0\},\cdot)$ komutativní grupa, 1 neutrální, a^{-1} inverz
3. distributivita $\quad \forall a,b,c \in T: \; a\cdot(b+c) = ab + ac$

Galois field zn. $GF(p^n)$
- $p \in \mathbb{P}$
- mn. polynomů st. $\le n-1$ s koeficienty v $\mathbb{Z}_p$
- + sčítání normální
- $\cdot$ % ireducibilní polynom stupně n (ireducibilní = nerozložitelný!)

Vlastnosti v tělese $(T,+,\cdot)$
1. $0\cdot a = 0$
2. $ab = 0 \Rightarrow a = 0 \vee b = 0$
3. $-a = (-1)a$

Př: tělesa $(\mathbb{Z}_2,+,\cdot), (\mathbb{Z}_3,+,\cdot)$
⚠ není těleso $(\mathbb{Z}_4,+,\cdot)$ $\nexists\, 2^{-1}$
$(\mathbb{Z}_n,+,\cdot)$ je těleso $\Leftrightarrow$ n prvočíslo

Každé kon. těleso velikosti p^n je izomorfní $GF(p^n)$.

Def: Charakteristika tělesa je 0, nebo nejmenší n t. že $\underbrace{1+1+\dots+1}_{n} = 0$ → je to vždy prvočíslo ($1 \neq 0$ a jinak by nebylo nejmenší)

(Malá Fermatova věta) Buď p prvočíslo, $a \in \mathbb{Z}_p$, $a \neq 0$. Pak v $\mathbb{Z}_p$ platí $a^{p-1} = 1$

Def: (Vektorový prostor) Buď $\mathbb{T} = (T,+,\cdot,^{-1},0,1)$ těleso. Vektorový prostor (= lineární prostor) nad tělesem $\mathbb{T}$ je mn. V s operacemi $+: V^2 \to V$
$\cdot: T\times V \to V$ splňující pro každé $\alpha,\beta \in T$, $u,v \in V$:

1. $(V,+)$ komutativní grupa, neutr. prvek o, inverz k v je $-v$
2. asociativita $\quad \alpha(\beta v) = (\alpha\beta)v$
3. $1\cdot v = v$
4. distributivita $\quad (\alpha+\beta)v = \alpha v + \beta v$
5. distributivita $\quad \alpha(u+v) = \alpha u + \alpha v$

Př: $\cdot\, \mathbb{R}^n$ nad $\mathbb{R}$ $\quad \cdot\, \mathbb{R}^{m\times n}$ nad $\mathbb{R}$
$\cdot\, \mathbb{T}^n$ nad $\mathbb{T}$ $\quad \cdot\, \mathbb{T}^{m\times n}$ nad $\mathbb{T}$
zn. $\mathcal{P}$ ... prostor $\forall$ reál. polynomů 1 prom
dim $= n+1$ ← $\mathcal{P}^n$ ... // st. $\le n$
$\mathcal{F}$ ... prostor reálných fcí

Vlastnosti vektorů v prostoru V nad $\mathbb{T}$
1. $\forall v \in V: \; 0\cdot v = o$
2. $\forall \alpha \in \mathbb{T}: \; \alpha o = o$
3. $\forall v \in V\, \alpha \in \mathbb{T}: \; \alpha v = o \Rightarrow \alpha = 0 \vee v = o$
4. $\forall v \in V: \; (-1)v = -v$

$\mathcal{P}^n \Subset \mathcal{P} \Subset \mathcal{F}$
osa x $\Subset$ $\mathbb{R}^n$ nad $\mathbb{R}$
sym. matice $\Subset \mathbb{R}^{n\times n}$
$U \Subset W \wedge V \Subset W: \; U \subseteq V \Rightarrow U \Subset V$

Def: (Podprostor) Nechť V je v.p. nad $\mathbb{T}$. Pak $U \subseteq V$ je podprostor V zn $U \Subset V$ pokud U je v.p. nad $\mathbb{T}$.
← obsahuje o; uzavřenost +; uzavřenost $\cdot$

⚠ $\cup$ podprostorů nemusí být podprostor

Průnik podprostorů je podprostor.

Def: Lineární obal podprostoru $U = \{u_1,\dots,u_n\}$, $\operatorname{span}(U) = \bigcap_{W:\, U \subseteq W \Subset V} W$ $= \{\sum_{i=1}^{n} \alpha_i v_i, \alpha_j \in \mathbb{T}\}$, tj. co do inkluze nejmenší podprostor V obsahující celé U.

Mn. U generuje $\operatorname{span}(U)$, tento prostor je kon. generovaný jestliže U je konečná!

Def: Buď V kon. generovaný v.p. nad $\mathbb{T}$. Báze V je lib. nezávislý systém generátorů V, tj. lin. nezáv. mn.

- Lin. kombinace vektorů $v_1, \dots, v_m \in V$ nad T je $\sum_{i=1}^{m} \alpha_i v_i$, $\alpha_i \in T$.
- Vektory $v_1, \dots, v_m$ jsou lin. nezávislé pokud $\sum_{i=1}^{m} \alpha_i v_i = o \Leftrightarrow \alpha_1 = \dots = \alpha_m = 0$ jinak jsou závislé.
- Kanonická báze $e_1, \dots, e_n$ — e_i má samé nuly a na pozici i jedničku
  báze P^n: $1, x, x^2, \dots, x^n$
- Nechť B je báze prostoru $u \in V$, $B = \{v_1, \dots, v_m\}$ pak u má jednoznačné souřadnice
  zn. $[u]_B = (\alpha_1, \dots, \alpha_m)^T$ $\quad u = \sum_{i=1}^{n} \alpha_i v_i$

$$\begin{pmatrix} | & | & & | \\ v_1 & v_2 & \dots & v_n \\ | & | & & | \end{pmatrix} \begin{pmatrix} | \\ u \\ | \end{pmatrix} \qquad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = [u]_e \qquad B \cdot [u]_B = u$$

Steinitzova v. o výměně = LN mn. vektorů jde doplnit na mn. generující celý prostor

Buď V vektorový prostor, $x_1, \dots, x_m$ lin. nezáv. systém ve V, $y_1, \dots, y_n$ generátory V. Pak platí:

1. $m \leq n$
2. existují indexy $k_1, \dots, k_{n-m}$ t.ž. $x_1, \dots, x_m, y_{k_1}, \dots, y_{k_{n-m}}$ jsou generátory V.

▼ indukcí podle m. ▲

Def (spojení podprostorů) $U, V \subseteq W$. Spojení $U + V := \{u + v;\ u \in U, v \in V\} = \mathrm{span}(U \cup V)$

V: $\dim(U + V) + \dim(U \cap V) = \dim U + \dim V$

Def: Maticové prostory. Buď $A \in \mathbb{R}^{m \times n}$.
- sloupcový prostor $\mathcal{S}(A) := \mathrm{span}\{A_{*1}, \dots, A_{*n}\} = \{Ax;\ x \in \mathbb{R}^n\}$
- řádkový prostor $\mathcal{R}(A) := \mathrm{span}$ řádků $= \mathcal{S}(A^T) = \{A^T y;\ y \in \mathbb{R}^m\}$
- jádro $\mathrm{Ker}(A) := \{x \in \mathbb{R}^n;\ Ax = o\}$

Def: (Lineární zobrazení = homomorfismus) Nechť U, V jsou v.p. nad tělesem T. Zob. $f: U \to V$ je lineární zob. pokud je slučitelné s $+, \cdot$. Tj. $\forall x, y \in U, \alpha \in T$: $f(x + y) = f(x) + f(y)$
$f(\alpha x) = \alpha f(x)$

izomorfismus je lin. zob., kt. je prosté a na. Tj. vzájemně jednoznačné lin. zob.

- každé lin. zob. lze zapsat $f(x) = Ax$
  $\mathrm{Ker}(A) = \mathrm{Ker}(f)$
- Následující tvrzení jsou ekvivalentní
  1. f je prosté $\quad x \neq y \Rightarrow f(x) \neq f(y)$
  2. $\mathrm{Ker}(f) = \{o\}$
  3. obraz $\forall$ lin. nezáv. mn. je lin. nezáv. mn.

Def. matice zobrazení $f: U \to V$
báze $B_1 = \{u_1, u_2, \dots, u_n\} \longrightarrow B_2 = \{v_1, \dots, v_m\}$ $\quad f(u_j) = \sum_{i=1}^{m} a_{ij} v_i$

$$A = {}_{B_2}[f]_{B_1} := \text{matice s prvky } a_{ij}, \quad A \in T^{m \times n}$$

$$= \begin{pmatrix} | & | & & | \\ f(u_1) & f(u_2) & \dots & f(u_n) \\ | & | & & | \end{pmatrix}$$

Matice přechodu od B_1 k B_2 je ${}_{B_2}[id]_{B_1}$

získám ji $(B_2 \mid B_1) \rightsquigarrow (I_n \mid {}_{B_2}[id]_{B_1})$
ve sloupcích

Když chci vektor x z B_1 do B_2 spočítám ${}_{B_2}[id]_{B_1} \cdot x$

Mám vektor v a bázi $B = \{b_1, b_2, b_3\}$ vektor v vyjádřím v B

$$\left(\begin{array}{ccc|c} | & | & | & v_1 \\ b_1 & b_2 & b_3 & v_2 \\ | & | & | & v_3 \end{array}\right) \rightsquigarrow (x_1, x_2, x_3) = [v]_B$$

Př: $f: U \to V$ → báze neznáhodná
daná báze $\{b_1, b_2, b_3\}$
$f(b_1) = y_1$
$f(b_2) = y_2$ $\quad \rightsquigarrow [f]_B = (y_1\ y_2 \dots$
$f(b_3) = y_3$

báze $X = \{x_1, x_2, x_3\}$ $\quad [v]_X = (v_1, v_2, v_3)$
báze Y: $\{x_1, x_1 + x_2, x_2 + 3x_3\}$ $\quad [v]_Y = ?$

${}_{kan}[f]_{kan} = {}_{kan}[f]_{B_2} \, {}_{B_2}[id]_{kan}$
$(B \mid I) \rightsquigarrow (I \mid \dots)$

$x_1 v_1 + x_2 v_2 + x_3 v_3 = x_1 \alpha_1 + (x_1 + x_2)\alpha_2 + (x_2 + 3x_3)\alpha_3$
$x_1(\alpha_2) + x_2(\alpha_2 + \alpha_3) + x_3(\alpha_1 + \frac{1}{3}\alpha_3)$

8 SKALÁRNÍ SOUČIN

Def: Buď V v. prostor nad $\mathbb{R}$, skalární součin je bin. operace $\langle \cdot,\cdot \rangle : V^2 \to \mathbb{R}$

nezápornost 1.) $\langle x,x \rangle \geq 0 \quad \forall x \in V$, $\langle x,x \rangle = 0$ když $x = o$

linearita 2. $\langle x+y,z \rangle = \langle x,z \rangle + \langle y,z \rangle \quad \forall x,y,z \in V$

3. $\langle \alpha x,y \rangle = \alpha \langle x,y \rangle \quad \forall x,y \in V, \alpha \in \mathbb{R}$

symetrie 4. $\langle x,y \rangle = \langle y,x \rangle \quad \forall x,y \in V$

standardní S.S.: v $\mathbb{R}^n$ $\langle x,y \rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot (y_1 \dots y_n)$

v $\mathbb{C}^n$ $\langle x,y \rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot (\overline{y_1} \dots \overline{y_n})$

v $\mathbb{R}^{m \times n}$ součin matic

Buď V vekt. prostor nad $\mathbb{C}$, skalární součin je bin. op. $\langle \cdot,\cdot \rangle : V^2 \to \mathbb{C}$

1. $\langle x,x \rangle \geq 0 \quad \forall x \in V$, rovnost pouze pro $x = o$
2. $\langle x+y,z \rangle = \langle x,z \rangle + \langle y,z \rangle \quad \forall x,y,z \in V$
3. $\langle \alpha x,y \rangle = \alpha \langle x,y \rangle \quad \forall x,y \in V, \alpha \in \mathbb{C}$
4. $\langle x,y \rangle = \overline{\langle y,x \rangle} \quad \forall x,y \in V$

↳ je to vždy reálné číslo $\Rightarrow \langle x,x \rangle = \overline{\langle x,x \rangle}$

fce spojité na intervalu $C_{[a,b]}$ $\quad \langle f,g \rangle = \int_a^b f(x) \cdot g(x)\, dx$

Norma $\|\cdot\| : V \to \mathbb{R}$ nad $\mathbb{R}$ nebo $\mathbb{C}$ splňuje nezáp., násobení skalárem, Δ ner.

1. $\|x\| \geq 0 \quad \forall x \in V$, $\|x\| = 0$ jen pro $x = o$
2. $\|\alpha x\| = |\alpha| \cdot \|x\|$
3. $\|x+y\| \leq \|x\| + \|y\|$

Def: Norma indukovaná skal. součinem $\|x\| := \sqrt{\langle x,x \rangle}$.

$x,y \in V$ jsou kolmé pokud $\langle x,y \rangle = 0$

v $\mathbb{R}^n$ $\sqrt{\sum x_i^2}$

geometricky $\langle x,y \rangle = \|x\| \cdot \|y\| \cdot \cos\varphi$

(Cauchy-Schwarzova nerovnost) pro $\forall x,y \in V$ platí $|\langle x,y \rangle| \leq \|x\| \cdot \|y\|$

$y \neq o \quad f(\lambda) = \langle x+\lambda y, x+\lambda y \rangle$

nezáp kvadr. fce $\leadsto$ diskriminant $\leadsto$ odmocnění $\blacktriangle$

Δ-nerovnost $\forall x,y \in V$: $\|x+y\| \leq \|x\| + \|y\|$

Př. normy $\|x\|_p = \sqrt[p]{\sum |x_i|^p}$ $\quad \|x\|_2$ eukleidovská

$\|x_1\|_1$ součtová $= \sum |x_i|$ Manhattonská

Ortonormální báze • vektory jsou kolmé

• mají jednotkovou velikost

Gramova-Schmidtova ortogonalizace

Def: Ortogonální doplněk $M^\perp$ ve V je ($M \subseteq V$)

$M^\perp := \{ x \in V : \langle x,y \rangle = 0, \forall y \in M \}$

Vlastnosti:

- $M^\perp$ je podprostor V
- $M \subseteq N \Rightarrow M^\perp \supseteq N^\perp$
- $M^\perp = \mathrm{span}(M)^\perp$
- $U \Subset V$ $\quad$ U báze $b_1, \dots, b_m$

  V báze $\quad$ —"— $\quad$ $, b_{m+1}, \dots, b_n$

  $U^\perp$ má bázi $\quad b_{m+1}, \dots, b_n$
- $\dim V = \dim U + \dim U^\perp$
- $V = U + U^\perp$
- $(U^\perp)^\perp = U$
- $U \cap U^\perp = \{ o \}$

- $\mathcal{R}(A)^\perp = \mathrm{Ker}(A)$ $\to$ hledání doplňku k mn. vektorů
  1. napíšu je do řádků
  2. najdu kernel matice
  tj. řeším $(A \mid o)$
- $\mathrm{Ker}(A^TA) = \mathrm{Ker}(A)$
- $\mathcal{R}(A^TA) = \mathcal{R}(A)$
- $\mathrm{rank}(A^TA) = \mathrm{rank}(A)$

Ortogonální projekce (je lin. zobr.) do $U \Subset V$ $\quad$ ortonormální $b_1, \dots, b_m$ báze U

$x \in V \leadsto x_U = \sum_{i=1}^{m} \langle x, b_i \rangle b_i$ $\quad$ to splňuje $\|x - x_U\| = \min_{y \in U} \|x - y\|$

~~Postup~~ matice projekce do $S(A)$ je $P := A(A^TA)^{-1}A^T$

↳ symetrická, $P^2 = P$

$\Rightarrow$ Metoda nejmenších čtverců $\quad \min_{x \in \mathbb{R}^n} \|Ax - b\|$

$Ax = b \quad | \cdot A^T$

$A^TAx = A^Tb \quad | \cdot (A^TA)^{-1}$

$x = (A^TA)^{-1}A^Tb$

Ortogonální matice $Q \in \mathbb{R}^{n \times n}$ splňuje $Q^TQ = I \iff$ reg. $\wedge$ $Q^{-1} = Q^T \iff$ sloupce i řádky jsou ortonormální báze $\mathbb{R}^n$

Unitární m. $\quad Q \in \mathbb{C}^{n \times n}$ $\quad (\overline{Q})^TQ = I$

$\to$ zobrazení definované ortogon. maticí nemění úhly

$\det(Q) = \pm 1$

Řešení homogenní soustavy je ortog. doplněk řádků

$\{ x \mid Ax = o \} = \{ A_{1*}, A_{2*}, \dots, A_{m*} \}^\perp$

⑨ ŘEŠENÍ SOUSTAV LIN. ROVNIC

$Ax = b$ $\qquad {}_m\begin{pmatrix} & A & \end{pmatrix}^{n} \cdot \begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} b \end{pmatrix}$

$\bigcap$ afinních prostorů je afinní prostor

- $\operatorname{rank}(A) > \operatorname{rank}(A|b) \Rightarrow$ 0 řešení
  b není lin. kombinací sloupců A
- $\operatorname{rank}(A) = \operatorname{rank}(A|b) \Rightarrow$ 1 řešení $\Leftrightarrow$ A je reg.
  bod v $\mathbb{R}^n$
- $\operatorname{rank}(A) < \operatorname{rank}(A|b) \Rightarrow$ nekonečně mnoho řešení
  afinní podprostor $\mathbb{R}^n$
  podle # volných proměnných přímka/rovina/…/nadrov.

Gaussova eliminace $\rightsquigarrow$ odstupňovaný tvar $\rightarrow$ REF

Gauss-Jordanova el. $\rightsquigarrow$ redukovaný odst. tvar

RREF = pivoti jsou jedničky a nad i pod nimi jsou nuly

$e_i = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \leftarrow i$

Buď $U \subset\subset V$, $a \in V$

Afinní podprostor prostoru V nad $\mathbb{T}$ je jakákoliv mn. $M \subseteq V$ tvaru $M = U + a = \{v + a ; v \in U\}$

Frobeniova věta $\quad (A|b)$ má (aspoň jedno) řešení $\Leftrightarrow \operatorname{rank}(A) = \operatorname{rank}(A|b)$.

10 MATICE

Regulární matice $A \in \mathbb{R}^{n\times n}$ ← vždy čtvercová, když $Ax = 0$ má 1 řešení $x = 0$.
jinak je singulární

$$I_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} \in \mathbb{R}^{n\times n}$$

- $\operatorname{rank} A = n$
- $\operatorname{RREF}(A) = I$
- $\exists b \in \mathbb{R}^n : \exists! x \quad Ax = b$
- $\forall b \in \mathbb{R}^n : \quad \exists! x \quad Ax = b$
- $\det(A) \neq 0$
- $\exists! A^{-1} : \quad A^{-1}A = AA^{-1} = I$
- 0 není vl. číslo A

- A reg $\Rightarrow$ A^T je reg.
- A, B reg $\Rightarrow$ $A \cdot B$ reg

Inverzní matice $\quad A^{-1}A = AA^{-1} = I$

– výpočet $\quad (A \mid I_n) \xrightarrow{\text{RREF}} (I_n \mid A^{-1})$

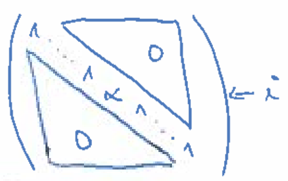
- $(A^{-1})^{-1} = A$
- $(A^{-1})^T = (A^T)^{-1}$
- $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1} \quad \alpha \neq 0$
- $(AB)^{-1} = B^{-1}A^{-1}$

pro $Ax = b \qquad x = A^{-1}b$

Elementární úpravy – násobení E zleva $\qquad A' = E \cdot A$

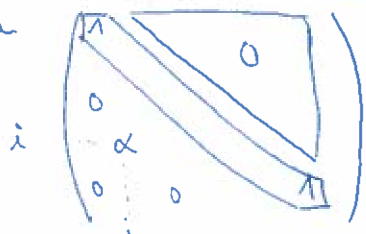
1. $\alpha \cdot$ i-tý řádek $\quad \alpha \neq 0$

$E_i(\alpha) = I + (\alpha - 1) e_i e_i^T =$ ← ta jednička se přičte



2. přičtení α-násobku i-tého k j-tému

$E_{ij}(\alpha) = I + \alpha e_i e_j^T$



3. výměna i-tého s j-tým

$E_{ij} = I + (e_j - e_i)\cdot(e_i - e_j)^T =$

‖ v I prohodím i-tý řádek s j-tým

– matice úprav jsou regulární ⇒ nemění řešení soustavy

TODO rozklady matic ?

Def: Buď $A \in \mathbb{R}^{n \times n}$ symetrická. Pak A je pozitivně semidefinitní pokud $x^T A x \geq 0 \ \forall x \in \mathbb{R}^n$
pozitivně definitní pokud $x^T A x > 0 \ \forall x \neq 0$

$\Updownarrow$

vl. čísla jsou > 0

$\Updownarrow$

$\exists U \in \mathbb{R}^{m \times n} : \text{rank}(U) = n : A = U^T U$

Vlastnosti poz. def. matic

1. $A, B \in \mathbb{R}^n$ poz. def $\Rightarrow A + B$ poz. def.
2. A poz. def. $\alpha > 0 \Rightarrow \alpha A$ poz. def.
3. A poz. def. $\Rightarrow A^{-1}$ poz. def.

testování A poz. def $\Leftrightarrow \alpha > 0 \wedge \tilde{A} - \alpha a a^T$ je poz. def.

$$A = \left(\begin{array}{c|c} \alpha & a^T \\ \hline a & \tilde{A} \end{array}\right)$$

Choleského rozklad

Pro $\forall$ poz. def. $A \in \mathbb{R}^{n \times n}$ $\exists!$ L dolní $\triangle$ z $\mathbb{R}^{n \times n}$ s kladnou diagonálou, t.ž.

$$A = L \cdot L^T = \cdot$$

11 DETERMINANTY

Def: $A \in T^{m\times m}$. $\det(A) = \sum_{p\in S_m} \operatorname{sgn}(p) \prod_{i=1}^{m} a_{i,p(i)} = \sum_{p\in S_m} \operatorname{sgn}(p)\, a_{1,p(1)} \cdot \ldots \cdot a_{m,p(m)}$

Elem. úpravy $A \rightsquigarrow A'$

1. vynásobení řádku α — $\det(A') = \alpha \det(A)$
2. výměna 2 řádků — $\det(A') = -\det(A)$
3. přičtení α-násobku řádku k jinému — $\det(A') = \det(A)$

Platí: $\det A^T = \det A$

$\det(\text{trojúhelníková}) = \prod$ prvků na diagonále

linearita determinantu $\quad \triangle \; \det(A+B) \neq \det(A) + \det(B)$

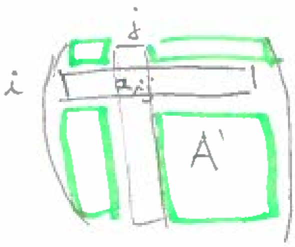
$$\det\begin{pmatrix} & A_1 & \\ a_{i1}+b_1 & \cdots & a_{im}+b_m \\ & A_2 & \end{pmatrix} = \det\begin{pmatrix} & A_1 & \\ a_{i1} & \cdots & a_{im} \\ & A_2 & \end{pmatrix} + \det\begin{pmatrix} & A_1 & \\ b_1 & \cdots & b_m \\ & A_2 & \end{pmatrix}$$

$\det(A\cdot B) = \det A \cdot \det B = \det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$

$\det(A^{-1}) = \det(A)^{-1} \implies \det(A^{-1}) = \dfrac{1}{\det(A)}$

Laplaceův rozvoj

$\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{ij} \det(A')$ — bez i-sloupu, j-řádku



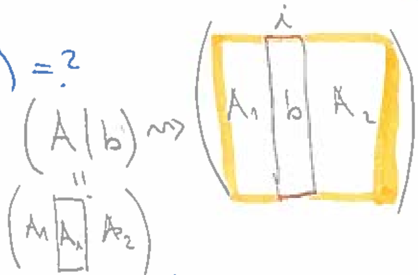
Cramerovo pravidlo

$Ax = b$

$x = (x_1, \ldots, x_n) = ?$

$x_i = \dfrac{\det A'}{\det A}$

$(A|b) \rightsquigarrow$

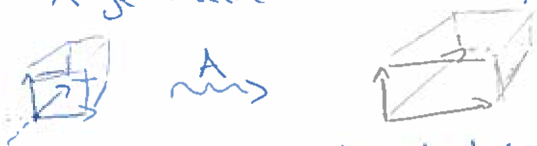


Každá čtvercová matice je regulární $\iff \det(A) \neq 0$

Geometrický význam determinantu

změna objemu

nechť A je matice zobrazení Aj. $x \to Ax$



$V = 1 \qquad V' = \det(A) = V \cdot \det(A)$

- \# koster grafu $= \det$ (redukovaná Laplaceova matice grafu)
  - $\hookrightarrow a_{ii} = \deg v_i$
  - $a_{ij} = \begin{cases} -1 & v_i \text{ sousedí s } v_j \\ 0 & \text{jinak} \end{cases}$
  - $\to$ vyškrtnu 1 řádek a 1 sloupec $\Rightarrow$ redukovaná Lap. matice

Minor = subdeterminant matice (viz A' u Laplaceova rozvoje)

inverzní matice A^{-1} k A splňuje $A^{-1}A = A^{-1}A = I_n$.

12 VLASTNÍ ČÍSLA A HODNOTY

Def: Buď $A \in \mathbb{C}^{n\times n}$. Pak $\lambda \in \mathbb{C}$ je <u>vlastní číslo</u> matice A a $x \in \mathbb{C}^n$ jemu příslušný <u>vlastní vektor</u> pokud platí $Ax = \lambda x$, $x \neq o$.
↳ není jednoznačný, můžu ho vynásobit $\alpha \in \mathbb{C}$

- Geometrický význam • vl. vektor je směr, kt. se zobrazí sám na sebe
  • vl. číslo je škálování v tomto směru

Věta: (Charakteristika vl. čísel a vektorů) Buď $A \in \mathbb{C}^{n\times n}$. Pak
1. $\lambda \in \mathbb{C}$ je vl. č. $\iff \det(A - \lambda I) = 0$ λ_j vl. č. jsou kořeny char. polynomu

   ▼ λ je vl. č. $\iff$ $Ax = \lambda x$
   $Ax = \lambda I x$
   $Ax - \lambda I x = 0$ → $(A - \lambda I)x = 0$ protože $x \neq o \Rightarrow A - \lambda I$ je sing. $\iff \det = 0$
   $\det(A - \lambda I) = 0$ ▲

2. $x \in \mathbb{C}^n$ je vl. v. $\iff$ $x \in \operatorname{Ker}(A - \lambda I)$

• vl. čísel je n
• Δ matice má vl. č. na diagonále
• sym matice má reálná vl. č.

Def: <u>Charakteristický polynom</u> matice $A \in \mathbb{C}^{n\times n}$ vzhledem k proměnné λ je $p_A(\lambda) = \det(A - \lambda I)$.

$$p_A(\lambda) = \det(A - \lambda I_n) \overset{?}{=} (-1)^n \lambda^n + \underset{(-1)^{n-1}(a_{11} + \dots + a_{nn})}{a_{n-1}\lambda^{n-1}} + \dots + a_1\lambda + \underset{\lambda = 0 \Rightarrow \det(A)}{a_0}$$

$$p_A(\lambda) \overset{?}{=} (-1)^n (\lambda - \lambda_1) \cdot \ldots \cdot (\lambda - \lambda_n)$$

Věta: (Součin a součet vl. čísel) Buď $A \in \mathbb{C}^{n\times n}$ s vl. č. $\lambda_1, \dots, \lambda_n$. Pak
1. $\det(A) = \lambda_1 \cdot \ldots \cdot \lambda_n$

   ▼ $\det(A - \lambda I_n) = (-1)^n (\lambda - \lambda_1) \cdot \ldots (\lambda - \lambda_n)$
   $\lambda = 0$
   $\det(A) = (-1)^n (-\lambda_1) \ldots (-\lambda_n) = \lambda_1 \cdot \ldots \cdot \lambda_n$ ▲

2. $a_{11} + \ldots + a_{nn} = \lambda_1 + \ldots + \lambda_n$

   ▼ $\det(A - \lambda I)$ koeficienty u λ^{n-1}:
   $(a_{11} - \lambda) \ldots (a_{nn} - \lambda)$ → $(-1)^{n-1}(a_{11} + \ldots + a_{nn})$
   $(-1)^n(-\lambda_1 - \ldots - \lambda_n)$
   $\Rightarrow (-1)^{n-1}(a_{11} + \ldots + a_{nn}) = (-1)^n(-\lambda_1 - \ldots - \lambda_n)$
   $a_{11} + \ldots + a_{nn} = \lambda_1 + \ldots + \lambda_n$ ▲

Vlastnosti vl. č. A má vl. č. $\lambda_1, \dots, \lambda_n$ a vl. vektory $x_1, \dots, x_n$
1. A reg $\iff$ 0 není vl. č.
2. A reg. $\Rightarrow$ A^{-1} má vl. č. $\lambda_1^{-1}, \dots, \lambda_n^{-1}$, vl. v. $x_1, \dots, x_n$
3. A^2 má vl. č. $\lambda_1^2, \dots, \lambda_n^2$ vl. vektory $x_1, \dots, x_n$
4. αA — // — $\alpha\lambda_1, \dots, \alpha\lambda_n$ — // —
5. $A + \alpha I_n$ — // — $\lambda_1 + \alpha, \dots, \lambda_n + \alpha$ — // —
6. A^T má vl. č. $\lambda_1, \dots, \lambda_n$, ale vl. v. obecně jiné

Věta: Je-li λ vl. č. $A \in \mathbb{C}^{n\times n}$ $\Rightarrow$ $\overline{\lambda}$ je vl. č. A.

Věta (Cayley-Hamiltonova) Buď $A \in \mathbb{C}^{n\times n}$, její char. p. $p_A(\lambda) = (-1)^n \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0$. Pak
$$(-1)^n A^n + a_{n-1}A^{n-1} + \ldots + a_1 A + a_0 I_n = 0$$
= A je kořenem svého char. polynomu.

Def: $A, B \in \mathbb{C}^{n\times n}$ jsou podobné, zn. $A \sim B$, pokud $\exists S \in \mathbb{C}^{n\times n}$: $A = SBS^{-1}$
$A \sim B \iff \exists S$ reg : $AS = SB$

Věta: $A \sim B \Rightarrow$ mají stejná vl. čísla.

Def: Matice $A \in \mathbb{C}^{n\times n}$ je diagonalizovatelná pokud $A \sim D$ ($A = SDS^{-1}$), & D je diagonální. $\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$

Věta: A je diagonalizovatelná $\iff$ A má n lin. nezávislých vl. vektorů.
$\lambda_1, \lambda_2, \dots, \lambda_k$ různá vl. λ $x_1, \dots, x_n$ LN $\Rightarrow$ A je diagonalizovatelná

JORDANOVA NORM FORMA

Def: Buď $\lambda \in \mathbb{C}$, $k \in \mathbb{N}$. Jordanova buňka $J_k(\lambda) \in \mathbb{C}^{k\times k}$ je matice $\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$ λ je k-násobné vl. č.

Matice $J \in \mathbb{C}^{n\times n}$ je v Jordanově normální formě, pokud je v blokově diagonálním tvaru

$$J = \begin{pmatrix} J_{k_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{k_m}(\lambda_m) \end{pmatrix}$$

Věta: Každá $A \in \mathbb{C}^{n\times n}$ je podobná matici v J. normální formě. Ta je až na pořadí bloků jednoznačná.

Věta: Sym. matici lze rozložit $A = Q \Lambda Q^T$, kde Q ortogonální, Λ diagonální

$A = Q \Lambda Q^{-1}$ ↳ má ve sloupcích vl. vektory a ty jsou ortogonální

V: Gerschgorinovy disky

$\forall$ vl. č. λ matice $A \in \mathbb{C}^{n\times n}$ leží v kruhu $k\left(\overset{\text{střed}}{a_{ii}}, \overset{\text{poloměr}}{\sum_{i\neq j} |a_{ij}|}\right)$ pro nějaké $i \in [n]$

$\forall \lambda$ leží v kruhu $r = \max \Sigma$ řádku

$$\begin{pmatrix} a_{11} & 3 & 7 \\ 1 & a_{22} & 1 \\ 4 & 5 & a_{33} \end{pmatrix} \quad \begin{matrix} r_1 = 10 \\ r_2 = 2 \\ r_3 = 9 \end{matrix}$$

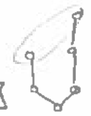
(13) DISKRÉTNÍ MATEMATIKA

Def (částečné uspořádání) Relace $\leq$ je částečné uspořádání pokud je
- reflexivní
- tranzitivní
- (slabě) antisymetrické

Př.: $\leq$, $|$ dělení, $=$

(ČUM) Množina X je částečně uspořádaná mn. s relací částečného usp. $\leq$ definovaného na X.

Def. Maximální prvek $m \in X$: $\forall x \in X: \ x \geq m \Rightarrow x = m$.
Největší prvek $\mathcal{M} \in X$: $\forall x \in X: \ \mathcal{M} \geq x$ … největší ze všech, nemusí $\exists$



Minimální prvek $m \in X$: $\forall x \in X: \ x \leq m \Rightarrow x = m$
Nejmenší $\mathcal{M} \in X$: $\forall x \in X: \ \mathcal{M} \leq x$ … nemusí $\exists$

Př.: $(\mathbb{N}, =)$ každý x je maximální, $\nexists$ největší

Def. řetězec je posl. různých prvků pokud $x_1 \leq x_2 \leq \dots \leq x_k$
výška je max. délka řetězce, zn. $\omega(X, \leq)$
antiřetězec (nezáv. mn.) pokud žádné dva prvky nejsou porovnatelné
šířka je max. velikost antiřetězce, zn.: $\alpha(X, \leq)$

Věta (o dlouhém a širokém) Pro $\forall (X, \leq)$ ČUM: $\omega \cdot \alpha \geq |X|$

$\blacktriangledown$ rozdělím X na vrstvy X_k

$$|X| = \sum_{i=1}^{k} |X_k| \leq \omega \cdot \alpha \quad \blacktriangle$$

Kombinační čísla

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \qquad \binom{n}{0} = \binom{n}{n} = 1 \qquad \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Binomická věta $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$, $n \in \mathbb{N}$ $\triangledown$ indukcí $\triangle$ (na znásobením)

Důsl.: $(x+y)^n = \sum_{k=1}^{n} x^k y^{n-k}$

Dirichletův princip Nechť $A_1, A_2, \dots, A_k$ jsou kon. mn. Pak $\exists i \in [k]: |A_i| \geq \dfrac{\left|\bigcup_{j=1}^{k} A_j\right|}{k}$

$\triangledown$ sporem $\triangle$

$$|A_i| \geq \frac{\sum_{j=1}^{k} |A_j|}{k}$$

Princip inkluze a exkluze Nechť $A_1, \dots, A_n$ konečné mn.

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \in \binom{\{1,\dots,n\}}{k}} \left|\bigcap_{j \in I} A_j\right| = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ I \neq \emptyset}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

Šatnářka

$š(n) = |\{\pi \in S_n : \forall i: \pi(i) \neq i\}| = ?$

$F_i = \{\pi \in S_n : \pi(i) = i\}$

$$š(n) = n! - \left|\bigcup_{i=1}^{n} F_i\right| = n! - \sum_{k=1}^{n} (-1)^{k+1} \underbrace{\sum_{I \in \binom{\{1,\dots,n\}}{k}}}_{\binom{n}{k}} \overbrace{\left|\bigcap_{i \in I} F_i\right|}^{(n-k)!} = n! - \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! = n! + \sum_{k=1}^{n} (-1)^k \frac{n!}{k!\,\cancel{(n-k)!}} \cdot \cancel{(n-k)!}$$

$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

ve chápat i jako „multimnožinu"

Množinový systém $(X, \mathcal{S})$: $\mathcal{S} \subseteq 2^X$, X nosná mn.

Systém různých reprezentantů (SRR) je prostá fce $f: \mathcal{S} \to X$ t. ž. $\forall A \in \mathcal{S}: f(A) \in A$

Hallova věta

Množinový systém $(X, \mathcal{S})$ má SRR $\iff \underbrace{\forall \mathcal{J} \subseteq \mathcal{S}: |\bigcup \mathcal{J}| \geq |\mathcal{J}|}_{\text{Hallova podmínka}}$

∇ indukcí podle $|\mathcal{S}|$ Δ

Párování v grafu $G(V,E)$ je $P \subseteq E$ t. že $\forall e, f \in P, e \neq f: e \cap f = \emptyset$

Maximální párování (co do inkluze) nejde zvětšit. / (co do velikosti) má největší # hran co může mít nějaké párování

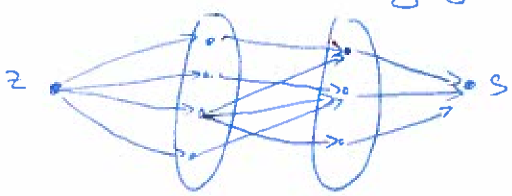
Perfektní párování pokrývá všechny vrcholy

Hallova věta $\Rightarrow$ k-regulární bipartitní graf má k navzájem disjunktních perf. párování

$\Rightarrow$ částečně (po celých řádcích) vyplněný latinský čtverec lze vždy doplnit na celý

„v ∀ řádku i sloupci je permutace $[n]$" A $n \times n$

Hledání PP v bipartitních grafech



$c(e) = 1$

$f :=$ celočíselný max. tok

$|f| = |M|$

↳ maximální párování

↳ mn. hran s kladným tokem

Birkhoffova: Bistochastická matice je konvexní kombinace permutačních matic

nezáporná, ∀ řádek i sloupec má sumu 1

↳ v ∀ řádku 1 jednička, —//— sloupci —//—, jinak 0

VP Vrcholové pokrytí = podmnožina vrcholů incidentní se ∀ hranami $|M| \leq$ max pokrytí co do velikosti

HP Hranové pokrytí = $M \subseteq E$: $\bigcup_{e \in M} e = V$ $|M| \geq$ —//—

Königova v.: Pro bipartitní graf je velikost maximálního párování rovna velikosti minimálního VP.

Kombinatorické počítání

- počet podmnožin $\{1, \dots, n\}$ je 2^n t.j. $2^{|M|}$
- počet k-prvkových podmn. $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$
- # zobr. $\{A\} \to B$ $|B|^{|A|}$

  prostých $|A| \leq |B|$ $|B| \cdot (|B|-1) \cdot \ldots \cdot (|B|-|A|+1) = \frac{|B|!}{|A|!}$
- # permutací $\{1, \dots, n\}$ je $n!$

1 → 1
1 1 → 2
1 2 1 = 4
1 3 3 1 → 8
1 4 6 4 1 → 16

DISKRÉTKA

RELACE, USPOŘÁDÁNÍ, KOMBINATORIKA

Binární relace $R \subseteq X \times Y = \{(x,y) \mid x \in X, y \in Y\}$

~~obor~~ **nosič** $D(R) = \{x \in X \mid \exists y \in Y: (x,y) \in R\}$ = „definiční obor"

obor hodnot $R(R) = \{y \in Y \mid \exists x \in X: (x,y) \in R\}$ = „obor hodnot"

složení relací $R \subseteq X \times Y, S \subseteq Y \times Z$; $R \circ S \subseteq X \times Z = \{(x,z) \mid x \in X, z \in Z, \exists y \in Y: (x,y) \in R \wedge (y,z) \in S\}$

funkce $R \subseteq X \times Y$; Pokud $\forall x \in X: \exists! y \in Y: (x,y) \in R$ pak R je fce (zobrazení)

- prostá (injektivní) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
- na (surjektivní) $\forall y \in Y: \exists x \in X: f(x) = y$ (tedy $R(f) = Y$)
- vzájemně jednoznačná (bijektivní) = prostá + na

relace $R \subseteq X \times X$

- reflexivní $\forall x \in X: (x,x) \in R$
- symetrická $\forall x,y \in X: (x,y) \in R \Rightarrow (y,x) \in R$
- antisymetrická $\forall x,y \in X: (x,y) \in R \wedge (y,x) \in R \Rightarrow x = y$
- tranzitivní $\forall x,y,z \in X: (x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$

diagonála $\Delta_X = \{(x,x) \mid x \in X\}$

inverzní relace $R \subseteq X \times Y$; $R^{-1} \subseteq Y \times X = \{(y,x) \mid (x,y) \in R\}$

ekvivalence $R \subseteq X \times X$ je $R \wedge S \wedge T$

částečné uspořádání R je $R \wedge AS \wedge T$

↳ ČUM = částečně uspořádaná mn.

třídy prvku vzhledem k ekvivalenci $R[x] = \{y \in X \mid (x,y) \in R\}$

V1.1. $R \subseteq X \times X$ ekvivalence; 1) $\forall x \in X: R[x] \neq \emptyset$ 2) $\forall x,y \in X: R[x] = R[y] \vee R[x] \cap R[y] = \emptyset$

~~Dk~~ ? 3) rozkladové třídy jednoznačně určují ekvivalenci

lineární usp. $(X, \leq)$ je ČUM; ČUM je lin. usp. pokud $\forall x,y \in X$: buď $x \leq y$ nebo $y \leq x$

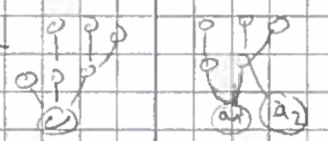
Hasseho diagram

minimální prvek uspořádání $(X, \leq)$ $a \in X$; $\forall x \in X: x \leq a \Rightarrow x = a$

maximální prvek usp. $b \in X$; $\forall x \in X: x \geq b \Rightarrow x = b$

nejmenší prvek usp. $c \in X: \forall x \in X: c \leq x$

největší prvek usp. $d \in X: \forall x \in X: d \geq x$



V každé ČU na konečné X lze doplnit na lin. uspořádání $R \subseteq X \times X: \exists$ lin. usp. $R' \subseteq X \times X: R \subseteq R'$

L v každé ČU na konečné X ~~…~~ $\exists$ alespoň jeden minimální prvek. Mat Indukce

?! **Boolovské usp.**

? **vnoření usp.** $(X, \leq), (X', \leq')$; $f: X \to X'$ pokud 1) f prosté zob. 2) $\forall x,y \in X: x \leq y \Leftrightarrow f(x) \leq' f(y)$

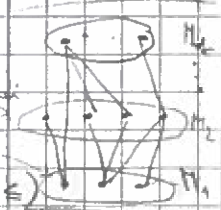
V Ať $(X, \leq)$ je ČUM, X konečná; Pak $(X, \leq)$ lze vnořit do B_n, $n = |X|$.

řetězec ČUM $x_1, \ldots, x_k$; $x_i \neq x_j \wedge x_i \leq x_j$ (resp. $x_1 < x_2 < \ldots < x_k$)

výška ČUM $\omega(X, \leq)$ délka max. řetězce

šířka ČUM $\alpha(X, \leq)$ velikost max. antiřetězce

antiřetězec (nezávislá mn.)



V. O Dlouhém a Širokém $(X, \leq)$ konečná ČUM Pak $|X| \leq \omega(X, \leq) \cdot \alpha(X, \leq)$

Lemma Erdös-Szekeres: Pro posl. délky n^2+1 $\exists$ monot. vybr. podposl. délky $n+1$

V 2.1 Jsou-li X, Y konečné mn., Pak # $\forall$ zobrazení X do Y je $|Y|^{|X|}$

V 2.2 # $\forall$ prostých zob. z X do Y je $|Y| \cdot (|Y|-1) \cdot \ldots \cdot (|Y|-|X|+1)$

permutace mn X je bijekce $X \to X$

$|X| = n$ # $\forall$ permutací je $n!$

$0! = 1$

T Je-li X konečná mn. pak $|2^X| = 2^{|X|}$

T ? → X konečná; # $\forall$ podmn. se sud. počtem prvků je $2^{|X|-1}$

T počet k-prvkových podmnožin

kombinační číslo

Kombinační čísla

V Binomická věta $n \in \mathbb{N}$: $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ → INDUKCÍ

Důsledek $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

V Multinomická věta

T Dirichletův princip $\exists i \in \{1, \ldots, k\}: |A_i| \geq \frac{|\bigcup_{j=1}^{k} A_j|}{k}$

V Princip inkluze a exkluze $|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} \sum_{I \in \binom{\{1,\ldots,n\}}{k}} (-1)^{k+1} |\bigcap_{i \in I} A_i|$

Problém šatnářky

PRAVDĚPODOBNOST

pravděpodobnostní prostor $(\Omega, 2^{\Omega}, p)$

elementární jevy ω … prvky Ω

pravděpodobnost fce $p: 2^{\Omega} \to \langle 0, 1 \rangle$

axiomy pravděpodobnosti
- $\sum_{\omega \in \Omega} p(\{\omega\}) = 1 = p(\Omega)$
- $\forall A \subseteq \Omega: p(A) = \sum_{\omega \in A} p(\{\omega\})$

$A_1, \dots, A_n \subseteq \Omega$ $\quad p\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} p(A_i)$

součin pravděpodobnostních prostorů $(\Omega_1 \times \Omega_2, 2^{\Omega_1 \times \Omega_2}, p)$ $\quad p = p_1(\{\omega_1\}) \cdot p_2(\{\omega_2\})$

podmíněná pрst $P(A|B) = \frac{P(A \cap B)}{P(B)}$

V O úplné prsti $B_1 \dot\cup \dots \dot\cup B_m = \Omega$, $A \subseteq \Omega$; $p(A) = \sum_{i=1}^{m} p(A|B_i) \cdot p(B_i)$

V Bayesova v. $p(B_i|A) = \frac{p(A|B_i) \cdot p(B_i)}{\sum_{j=1} p(A|B_j) \cdot p(B_j)}$

nezávislé jevy $\forall I \subseteq \{1, \dots, m\}: p\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} p(A_i)$ $\quad P(A \cap B) = p(A) \cdot p(B)$

náhodné veličiny (proměnné) $X: \Omega \to \mathbb{R}$ (hodnota, kterou nabývá jev)

střední hodnota $E(X) = \sum_{\omega \in \Omega} X(\omega) \cdot p(\{\omega\})$ součet (hodnot, kt. nabývá experiment, vynásobený její prstí)

$p(X = k)$ prst, že náhodná veličina nabývá hodnoty k $= p(\{\omega \in \Omega : X(\omega) = k\})$

V O linearitě střední hodnoty $\alpha \in \mathbb{R}$; $E(\alpha X) = \alpha E(X)$, $E(X+Y) = E(X) + E(Y)$

V Markovova nerovnost X nezáporná, $E(X) > 0$, $A \geq 1$
↳ střední hodnota $P(X \geq A \cdot EX) \leq \frac{1}{A}$

V Čebyševova nerovnost
↳ rozptyl $P(|X - EX| \geq a) \leq \frac{Var(X)}{a^2}$ pro $a \geq \sqrt{Var(X)}$

indikátor ✓

nezávislé náhodné veličiny $X, Y \iff P(X \geq a), P(Y \geq b)$ nezávislé na hodně jevy pro $a, b \in \mathbb{R}$

rozptyl náhodné veličiny $Var(X) = E(X - EX)^2$

distribuční fce

alternativní rozdělení

binomické rozdělení

rovnoměrné rozdělení

pascalovo rozdělení

hypergeometrické rozdělení

GRAFY

Matice sousednosti

Graf
Izomorfizmus grafů
Podgraf
Indukovaný podgraf
E_n
K_n
$\bar{G}$
cesta + délka cesty $(P_n) = n-1$ .. neopakují se vrcholy (=> ani hrany)
kružnice
bipartitní graf
T: G bipartitní $\Leftrightarrow \nexists C_n : C \subseteq G \wedge n = 2k+1$
T 1) ? ∃ různých grafů na V vrcholech 2) neizomorfních grafů na V
úplný bipartitní graf $K_{m,n}$
Operace na grafech odebrání v/e, přidání v/e, podrozdělení e, kontrakce e
tah neopakují se hrany
sled obecná posl. vrcholů a hran (můžu opak. v i e)
∃ sled z x do y => ∃ cesta z x do y
vzdálenost
relace ~ ∃ hrany mezi x, y
~ je ekvivalence
komponenty souvislosti
souvislý graf
T vlastnosti vzdálenosti nezáporná ($x = y \Leftrightarrow$ je 0), symetrická, △ nerovnost
okolí vrcholu
stupeň vrcholu
iterované okolí $v \in V$
otevřené iterované okolí $v \in V$
T Princip sudosti $\sum_{v \in V} deg(v) = 2|E|$ $p = \#(v, e)$

Stromy
strom
les
list
L: G strom $|V| \geq 2$ => G má aspoň 2 listy
L: G strom <=> (G − v) strom, v je list
Důsl.: G strom => $|E| = |V| - 1$
V ekvivalentní podmínky 1) G je strom

Kostry = spanning tree
kostra
Každý souvislý G má kostru
skóre grafu
V: O skóre (Havel–Hakimi)

Rovinné grafy
oblouk
rovinné nakreslení
rovinný graf
body rovinného nakreslení
stěna rovinného nakreslení
V Jordanova v. o kružnici Topologická kružnice dělí rovinu na 2 části
V Eulerova formule G rovinný souvislý $|V| - |E| + s = 2$
V Max # hran rov. grafu $|V| \geq 3$ $|E| \leq 3n - 6$ if $C_3 \not\subseteq G$ => $|E| \leq 2n - 4$
Důsl. $K_5 \wedge K_{3,3}$ nejsou rovinné
operace dělení hrany neovlivňuje rovinnost grafu
V Kuratowski G rovinný <=> neobsahuje dělení K_5 ani $K_{3,3}$ jako podgraf

duální graf
multigraf se smyčkami
Platónská tělesa

Barevnost grafů

dobré k-obarvení G $c: V \to \{1, \dots, k\}$
barevnost grafu $\chi(G)$
Ö $\chi(G) \leq |V(G)|$
klikovost grafu $\omega(G)$
nezávislost grafu $\alpha(G)$
Ö $\forall G: \omega(G) \leq \chi(G)$
L: $\chi(G) \geq 2 \iff G$ je bipartitní
T $G=(V,E)$: 1) $\chi(G) + \alpha(G) \leq |V|+1$
2) $\chi(G) \cdot \alpha(G) \geq |V|$
d-degenerovaný graf
degenerovanost (= coloring number) $col(G) = d+1$
min/max stupeň grafu $\delta(G) / \Delta(G)$
Ö $\delta(G)+1 \leq col(G) \leq \Delta(G)+1$
Ö G d-degenerovaný $\Rightarrow$ $G' \subseteq G$ je také d-degenerovaný
Důsl.: $G' \subseteq G \Rightarrow col(G') \leq col(G)$
problém 4 barev
T: G rov. $\to \chi(G) \leq 6$
V O 5 barvách
V $\forall k \in \mathbb{N}: \exists G_k = (V_k, E_k)$ bez C_3 (tedy $\omega(G_k) \leq 2$) t.že $\chi(G_k) = k$

Eulerovské grafy

uzavřený tah
eulerovský tah
eulerovský graf
V Eulerova: G bez izolovaných vrcholů, pak G eulerovský $\iff$ G souvislý $\wedge$ $\forall$ deg(v) sudé

Orientované grafy

orientovaný graf $\vec{G}(V, \vec{E})$, $V \neq \emptyset \wedge \vec{E} \subseteq V \times V$
podkladový g.
smyčky
protisměrné hrany
orientovaná cesta/tah/sled
vstupní stupeň v $\deg_{in}(v) = |\{e \in E \mid \exists x \in V: (x,v) = e\}|$
výstupní stupeň v $\deg_{out}(v) = |\{e \in E \mid \exists y \in V: (v,y) = e\}|$
souvislost • silná $\forall u,v \in V: \exists$ orientovaná cesta z u do v
• slabá – podkladový graf je souvislý
V $\exists$ orientovaný eulerovský tah v $\vec{G}$ $\iff$ $\vec{G}$ slabě souvislý $\wedge$ $\forall v \in V: \deg_{in}(v) = \deg_{out}(v)$
je i silně souvislý

Maticová reprezentace

matice incidence
matice sousednosti
T mocnění matice sousednosti $\to$ počet sledů délky k

Věty o pevném bodě

V

L Spernerovo lemma (pro Δ)
 triangulaci $\to$ $\exists$ Δ obarvený barvami 1,2,3
V Brouwerova věta o pevném bodě pro Δ
Každá spojitá fce $f: \Delta \to \Delta$ má pevný bod

(14) TEORIE GRAFŮ

Def: Graf $G(V,E)$ je usp dvojice, V kon. neprázdná mn. vrcholů, $E \subseteq \binom{V}{2}$ hrany.
Podgraf $G_1 \subseteq G_2$ pokud $V_1 \subseteq V_2 \wedge E_1 \subseteq E_2$
Indukovaný podgraf ~~...~~ vrcholy jsou podmn. + $\forall$ hrany na těchto vrcholech.
Doplněk (komplement) $\overline{G} = (V, \binom{V}{2} - E)$
Izomorfismus grafu je bijekce mezi grafy slučitelná s relací sousedení.
Poz: Prázdný graf $E_n(V, \emptyset)$ úplný $K_n(V, \binom{\{1,\dots,n\}}{2})$ úplný bipartitní $K_{n,m}$
Def: Bipartitní graf $\exists A, B \subseteq V: A \cap B = \emptyset, A \cup B = V \wedge \forall e \in E: |A \cap e| = 1$
V: G je bipartitní $\Leftrightarrow$ G neobsahuje kružnici liché délky
V: 1. na n vrcholech $\exists\ 2^{\binom{n}{2}}$ různých grafů
2. —— // —— $\exists$ aspoň $2^{\binom{n}{2}}/n!$ neizomorfních grafů
- Operace $G \setminus e$, $G \setminus v$, $G + e$, $G + v$
• podrozdělení hrany $G \% e$
• kontrakce hrany $G \cdot e$

Def: Sled - lib. posl. vrcholů (a hran mezi nimi)
Tah - neopakuje hrany $\qquad \exists$ sled $\Rightarrow \exists$ cesta
Cesta - neopakuje vrcholy
Vzdálenost vrcholů $d(x,y) = \begin{cases} \text{délka nejkratší cesty } x \to y \\ \infty \end{cases}$ (je nezáp., symetrická, △ nerovnost)
Komponenta souvislosti
Souvislý graf
Def: okolí vrcholu $N(v)$
stupeň vrcholu $\deg(v) = |N(v)|$
iterované okolí
otevřené okolí $N_r'(v) = \{x \in V \mid d(v,x) \le r\}$
Princip sudosti $\sum_V \deg(v) = 2|E|$

Strom 1. souvislý acyklický graf
2. $\forall u, v \in V: \exists!$ cesta $u \to v$
3. min. souvislý
4. max acyklický
5. souvislý a $|E| = |V| - 1$
6. bez kružnic a $|E| = |V| - 1$

$\kappa(G) = \kappa(G-e) + \kappa(G \cdot e)$, redukovaná Laplaceova matice
Kostra podgraf na V vrcholech, kt. je strom. # koster $\kappa(G)$ $\quad \kappa(G) = |Q_{ij}|$ $\quad q_{ii} = \deg(i)$, $q_{ij} = \begin{cases} -1 & \{i,j\} \in E \\ 0 & \notin E \end{cases}$
Skóre grafu „neklesající vzestupná" posl. stupňů vrcholů
V. o skóre $\exists$ skóre grafu $D = (d_1, \dots, d_n) \Leftrightarrow D'$ je skóre grafu $D' = (d_1', \dots, d_{n-1}')$ $\quad d_i' = \begin{cases} d_i & i < n - d_n \\ d_i - 1 & i \ge n - d_n \end{cases}$ „utrhnu vrchol s max stupněm"

Rovinný graf je G pokud $\exists$ nějaké jeho rovinné nakreslení.
Rovinné nakreslení 1. prosté $f_1: V \to \mathbb{R}^2$
2. $f_2: E \to$ ... je spojité prosté
• $f_2(e) = \varphi_e \quad \varphi: \langle 0,1 \rangle \to \mathbb{R}^2$ spoj. prosté = oblouk
$\varphi_e(0) = f_1(u) \quad \varphi_e(1) = f_1(v) \quad e = \{u, v\}$
• Pokud mají 2 hrany společný bod je to jejich společný vrchol.
Stěna nakreslení = komponenta $\mathbb{R}^2 \setminus$ body rov. nakreslení.
Jordanova v. o kružnici: Topologická kružnice dělí rovinu na 2 části.
Eulerova formule: s ... # stěn $\quad |V| - |E| + s = 2 \quad$ pro $\forall G$ rovinný.
V: Max # hran rov. g.: Buď $|V| \ge 3$. $\quad |E| \le 3n - 6$
Důsl: K_5 a K_{33} nejsou rov.
Kuratowski: G rovinný $\Leftrightarrow$ neobsahuje dělení K_5 ani K_{33}
Duální graf
Multigraf
Smyčka
Platonské těleso ($\exists$ jich 5: čtyřstěn, krychle $\leftrightarrow$ 8-stěn, 12-stěn $\leftrightarrow$ 20-stěn) - rovinný graf $\forall$ vrcholy stejný stupeň & stěny k-úhly

Dobré k-obarvení $c: V \to \{1, \dots, k\}$ pokud $\forall$ sousední vrcholy mají různou barvu.
Barevnost (chromatické číslo) $\chi(G) = \min \{k \in \mathbb{N} \mid G$ má dobré k-obarvení$\}$.
Klikovost $\omega(G) = \max \{k \in \mathbb{N} \mid K_k \subseteq G\}$
Nezávislost $\alpha(G) = \omega(\overline{G})$ ... vel. max nezáv. mn.

$\omega(G) \leq \chi(G)$
$\chi(G) + \alpha(G) \leq |V| + 1$
$\chi(G) \cdot \alpha(G) \geq |V|$

d-degenerovaný graf = každý jeho podgraf má vrcholy $\deg(v) \leq d$ — d-deg graf jde obarvit $d+1$ barvami
$col(G) = \min\{d \mid G$ je d-deg.$\} + 1$ ... tj. # barev kt. lze obarvit d-deg graf
$\delta(G)$ = nejmenší st. grafu
$\Delta(G)$ = největší st. grafu
$\delta(G) + 1 \leq col(G) \leq \Delta(G) + 1$

Věta: O 5 barvách: $\forall$ rovinný graf jde (vrcholově) obarvit 5 barvami. tj. $\chi(G) \leq 5$

Uzavřený tah
Eulerovský tah = uzav. $\wedge$ přes $\forall$ hrany
Eulerovský graf = bez izolovaných vrcholů a $\exists$ zde E. tah.
V: Eulerova: G je eulerovský $\iff$ G souvislý $\wedge$ $\forall v \in V$ $\deg(v)$ sudý

Orientovaný graf $\vec{G}$
vstupní stupeň $\deg_{in}$
výstupní stupeň $\deg_{out}$
souvislost • silná
• slabá = podkladový neor. g. je souvislý

V: $\vec{G} = (V, \vec{E})$ má eulerovský orientovaný tah $\iff$ souvislý $\wedge$ $\deg_{in} = \deg_{out}$ pro $\forall v \in V$

Matice incidence $I_G\,(i)_{V \times E}$ $\quad i_{ve} = \begin{cases} 1 & v \in e \\ 0 & v \notin e \end{cases}$ resp. -1 pro $\vec{G}$

Matice sousednosti $A_G\,(a)_{V \times V}$ $\quad a_{uv} = \begin{cases} 1 & \{u,v\} \in E \\ 0 & \notin E \end{cases}$

V: k-tá mocnina matice sousednosti má na a_{ij} # sledů z v_i do v_j délky k.

Toky
Síť je $(\vec{G}(V,E), z, s, c)$ kde $\vec{G}$ je orient. graf, $z, s \in V$ jsou zdroj a stok, $c: E \to \mathbb{R}^+_0$ kapacita
Tok je $f: E \to \mathbb{R}^+_0$ v síti splňující: • $\forall e \in E: f(e) \leq c(e)$
• $\forall v \in V \setminus \{z, s\}$: $\sum_{(x,v) \in E} f(x,v) = \sum_{(v,x) \in E} f(v,x)$

Velikost toku $|f| = \sum_{(x,s) \in E} f(x,s) - \sum_{(s,x) \in E} f(s,x)$
z-s-řez je $R \subseteq E$ t.ž. z, s jsou v jiných komponentách souvislosti $G'(V, E \setminus R)$
velikost řezu $|R| = \sum_{e \in R} c(e)$

Dualita toku a řezu
velikost max toku = velikost min. řezu
Graf k-e-souvislý $\iff |R_E(G)| \geq k$ — R_E hranový
k-v-souvislý $\iff |R_V(G)| \geq k$ — R_V vrcholový řez

Mengerovy věty: G je graf
• G ~~souvislý~~ k-e-souv. $\iff$ $\exists$ aspoň k e-disjunktních cest $v \to u$, $\forall u, v \in V, \{v,u\} \notin E$
k-v-souv. $\iff$ v-disjunktních

Ušaté lema: $|V| \geq 3$. G 2-souvislý $\iff$ $\exists$ rozklad $(C, U_1, \dots, U_e)$ t.že G se vytvoří z C postupným přilepováním uší (na různé vrcholy)

Artikulace
most

15 PAST

- Náhodný jev = výsledek náh. pokusu. Pravděpodobnostní prostor je trojice $(\Omega, \mathcal{A}, P)$ — prostor, σ-algebra, $P: \mathcal{A} \to \langle 0,1 \rangle$
- Podmíněná prst $P(A|B) = \frac{P(A \cap B)}{P(B)}$, $P(B) > 0$
- Nezávislost náhodných jevů $A_1, A_2, \ldots$: $\forall M \subseteq \{A_1, A_2, \ldots\}: P\left(\bigcap_{A_i \in M} A_i\right) = \prod_{M} P(A_i)$

  spec. $P(A \cap B) = P(A) \cdot P(B)$
- Def: Náhodná veličina je zobrazení $X: \Omega \to \mathbb{R}$ (resp. $X: (\Omega, \mathcal{A}, P) \to (\mathbb{R}, \mathcal{B})$), kt. je měřitelné.

  Střední hodnota: diskrétní X $EX = \sum_i x_i \cdot P(X = x_i)$ spojitá $EX = \int_{-\infty}^{\infty} x \cdot f(x)\,dx$
- rozdělení • rovnoměrné X nabývá $x_1, x_2, \ldots, x_n$: $P(x_i) = \frac{1}{n}$.

JXS KŘETKA

Pravděpodobnost

Pravděpodobnostní prostor ~~...~~

Ω ... všechny možné jevy

Prvky Ω nazýváme elementární jevy ω

$(\Omega, 2^{\Omega}, p)$

$p: \Omega \to \langle 0,1\rangle \qquad \sum_{\omega\in\Omega} p(\omega) = 1$ pravděpodobnost

$p: 2^{\Omega} \to \langle 0,1\rangle \qquad A \subseteq \Omega: p(A) = \sum_{\omega\in A} p(\omega)$

$A_1, \dots, A_m \subseteq \Omega \qquad p\left(\bigcup_{i=1}^{m} A_i\right) \le \sum_{i=1}^{m} p(A_i)$

Př: Kostka

$\Omega = \{1,2,3,4,5,6\}$

$i = 1 \dots 6$

$p(\{i\}) = \frac{1}{6}$

Mince

$\Omega = \{R, L\}$

$p(\{R\}) = p(\{L\}) = \frac{1}{2}$

Opakovaný hod mincí ($n \in \mathbb{N}$) $\qquad n = 2$: RR, LL, RL, LR

$\Omega = \{R, L\}^n$

$\omega \in \Omega: p(\{\omega\}) = \frac{1}{2^n}$

Součin pravděpodobnostních prostorů $(\Omega_1, 2^{\Omega_1}, p_1), (\Omega_2, 2^{\Omega_2}, p_2)$

je $(\Omega_1 \times \Omega_2, 2^{\Omega_1\times\Omega_2}, p)$

$p(\{(\omega_1, \omega_2)\}) = p_1(\{\omega_1\}) \cdot p_2(\{\omega_2\})$

Podmíněná pravděpodobnost: $A, B \subseteq \Omega$

$$P(A|B) = \frac{p(A\cap B)}{p(B)} \quad (\text{pro } p(B) > 0)$$

A pokud nastane B

Věta: O úplné pravděpodobnosti

$A, B_1, \dots, B_m \subseteq \Omega$ t. že $\bigcup_{i=1}^{m} B_i = \Omega$, pro $i \neq j$ je $B_i \cap B_j \neq \emptyset$

Potom $p(A) = \sum_{i=1}^{m} p(A|B_i)\cdot p(B_i)$

[Dk: $A_i = A \cap B_i \Rightarrow \bigcup A_i = A$, A_i disjunktní.

$$\left.\begin{array}{l} p(A) = \sum_1^m p(A_i) = \sum_1^m p(A \cap B_i) \\ p(A|B_i)\cdot p(B_i) = p(A\cap B_i) \end{array}\right\} p(A) = \sum_{i=1}^{m} p(A|B_i)\, p(B_i) \quad]$$

Př: Choroba

$p(HIV) = \frac{1}{10^3}$

test (pst, že je správný) $\quad p(T+|HIV) = 0{,}95$

$p(T-|\overline{HIV}) = 0{,}95$

$p(HIV|T+) = ?$

$$p(HIV|T+) = \frac{p(HIV\cap T+)}{p(T+)} = \frac{\frac{19}{20\,000}}{\frac{1018}{20\,000}} = \frac{19}{1018} < \frac{20}{1000} \approx 2\,\%$$

$p(HIV \cap T+) = p(T+|HIV)\cdot p(HIV) = \frac{19}{20}\cdot\frac{1}{1000}$

$\dots \frac{19}{\dots} \cdot \frac{999\,000}{\dots} \; 10^{-18}$

V **Bayesova v.**

$A, B_1, \dots, B_m \subseteq \Omega$, $\bigcup_{i=1}^{m} B_i = \Omega$, B_i disjunktní

$$p(B_i \mid A) = \frac{p(A \mid B_i)\cdot p(B_i)}{\sum_{j=1}^{m} p(A \mid B_j)\cdot p(B_j)}$$

Def: ~~jevy~~ $A, B \subseteq \Omega$ jsou nezávislé, pokud $p(A \cap B) = p(A)\cdot p(B)$

$A_1, \dots, A_m \subseteq \Omega$ — // — , pokud $\forall I \subseteq \{1, \dots, m\}: p(\bigcap_{i\in I} A_i) = \prod_{i \in I} p(A_i)$

Př. $\Omega = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$

A_i = i-té číslo je 1

A_1 a A_2 ... nezávislé

$p(A_1) = p(A_2) = p(A_3) = \frac{1}{2}$

$p(A_1 \cap A_2) = p(A_1 \cap A_3) = p(A_2 \cap A_3) = \frac{1}{4}$

A_1, A_2, A_3 nejsou nezávislé

Def: Náhodné veličiny (= náhodné proměnné)
(čísla přiřazená na určitým jevům)

Reálná náhodná veličina na konečném pstním prostoru $(\Omega, 2^{\Omega}, p)$ je $X: \Omega \to \mathbb{R}$.

součet hodnot, kt. nabývá experiment, vynásobených jejich prstí

Def: Střední hodnota náhodné proměnné X je $EX = \sum_{\omega\in\Omega} p(\{\omega\})\cdot X(\omega)$

$p(X=k) = p(\{\omega \in \Omega \mid X(\omega)=k\}) = \sum_{\omega \in} p(\omega)$

prst že náhodná veličina nabývá hodnoty k

$\mathcal{R}(X) = \{\underbrace{k_1, k_2, \dots, k_n}_{\text{hodnoty kt. může nabývat } X}\}$ $\quad EX = \sum_{i=1}^{n} \underbrace{p(X=k_i)}_{\text{prst, že } X = k_i}\cdot k_i$? třída ekvivalence $\mathcal{R}(X)$

indikátor jevu

Př: Kolik padne rubů?
rub ... 1
líc ... 0

$\Omega =$	X	
000	0	
100	1	$p(X=1)=\frac{3}{8}$
010	1	
001	1	
011	2	
101	2	$p(X=2)=\frac{3}{8}$
110	2	
111	3	$p(X=3)=\frac{1}{8}$

$EX = \frac{1}{8}(0+1+1+1+2+2+2+3) = \frac{12}{8} = \frac{3}{2}$

$EX = 0\cdot\frac{1}{8} + 1\cdot\frac{3}{8} + 2\cdot\frac{3}{8} + 3\cdot\frac{1}{8} = \dots = \frac{3}{2}$

X_i = počet 1 na i-té pozici $\in \{0,1\}$

$p(X_i = 1) = p(X_i = 0) = \frac{1}{2}$

$X = X_1 + X_2 + X_3$

$EX = EX_1 + EX_2 + EX_3$

V **O linearitě střední hodnoty**

pstní prostor $(\Omega, 2^{\Omega}, p)$, X, Y náhodné veličiny, $\alpha \in \mathbb{R}$.

Potom $E(\alpha X) = \alpha EX$, $\quad E(X+Y) = EX + EY$

Dk: $E(\alpha X) = \sum_{\omega\in\Omega} p(\{\omega\})\cdot(\alpha X(\omega)) = \alpha \sum_{\omega\in\Omega} p(\{\omega\})\cdot X(\omega) = \alpha \cdot EX$

$E(X+Y) = \sum_{\omega\in\Omega} p(\{\omega\})(X(\omega)+Y(\omega)) = \sum_{\omega\in\Omega} p(\{\omega\})X(\omega) + \sum_{\omega\in\Omega} p(\{\omega\})Y(\omega) = EX + EY$

Důsledek: $E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y)$

$E\left(\sum_{i}^{m} \alpha_i X_i\right) = \sum_{i}^{m} \alpha_i EX_i$

Indikátor $A \subseteq \Omega$: $I_A : \Omega \to \{0,1\}$

$$I_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A \end{cases}$$

$$EI_A = \sum_{\omega \in \Omega} P(\{\omega\}) \cdot I_A(\omega) = P(I_A = 1) = P(A)$$

↳ střední hodnota indikátoru

11. 11. 13

Př: Mince rub padá s pstí $p \in \langle 0,1 \rangle$
X = počet R při n hodech

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$$

$$EX = \sum_{k=0}^{n} k \cdot P(X=k) = \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k} = \dots$$

$i = 1, \dots, n$ $\quad I_i$ ... identifikátor „je R při i-tém hodu"

potom $X = \sum_{i=1}^{n} I_i$ $\qquad EI_i = P(I_i = 1) = p$

$$EX = \sum_{i=1}^{n} EI_i = \sum_{i=1}^{n} p = n \cdot p$$

Př: n lovců zajíců, každý 1x zastřelí zajíce
Jaká je prům. hodnota kolik zajíců uteče

X = # živých zajíců po střelbě
I_i = indikátor, že i-tý zajíc přežije

$$X = \sum_{i=1}^{n} I_i$$

$$EI_i = P(I_i = 1) = \left(1 - \frac{1}{n}\right)^n$$

$$EX = \sum_{i=1}^{n} P(I_i = 1) = n \cdot \left(1 - \frac{1}{n}\right)^n \longrightarrow \frac{n}{e}$$

nezávislé jevy $\quad P(A \cap B) = P(A) \cdot P(B)$

~~nezávislé náhodné~~

Def Nezávislé náhodné veličiny $X, Y \iff$
$\iff P(X \geq a) P(Y \geq b)$ nezávislé náhodné jevy pro $\forall a, b \in \mathbb{R}$

Def: Rozptyl náhodné veličiny X: $\quad Var(X) = E(X - EX)^2$
variance

Zk? limit

Markovova nerovnost:

X nezáporná náhodná veličina, $EX > 0$, $\lambda \geq 1$

$$P(X \geq \lambda \cdot EX) \leq \frac{1}{\lambda}$$

[Dk: $\underline{EX \geq a \cdot P(X \geq a)}$ pro $a > 0$

$A = \{\omega \in \Omega \mid X(\omega) \geq a\}$

$$\underline{EX} = \sum_{\omega \in \Omega} X(\omega) \cdot P(\{\omega\}) = \sum_{\omega \in A} X(\omega) \cdot P(\{\omega\}) + \underbrace{\sum_{\omega \in \Omega \setminus A} \overbrace{X(\omega)}^{\geq 0} \cdot P(\{\omega\})}_{\geq 0} \geq$$

$$\geq \sum_{\omega \in A} X(\omega) P(\{\omega\}) \geq \sum_{\omega \in A} a \cdot P(\{\omega\})$$

$$\geq a \sum_{\omega \in A} P(\{\omega\}) = a \cdot P(A) = \underline{a \cdot P(X \geq a)}$$

Dosadíme $a = \lambda EX$

$$EX \geq \lambda EX \cdot P(X \geq \lambda EX)$$

$$\underline{\frac{1}{\lambda} \geq P(X \geq \lambda EX)}$$

]

se střední hodnotou / s rozptylem

Zk? limit

Čebyševova nerovnost

$$P(|X - EX| \geq a) \leq \frac{Var(X)}{a^2} \qquad \text{pro } a \geq \sqrt{Var(X)}$$

nová náhodná veličina

[Dk: $Y = (X - EX)^2$ ... nezáporná

$$\underline{P(|X - EX| \geq a)} = P((X - EX)^2 \geq a^2) = P(Y \geq a^2) = P\left(Y \geq \underbrace{\frac{a^2}{EY}}_{\geq \lambda} EY\right) \leq$$

$$\overset{\text{Markov. ner. 1}}{\leq} \frac{1}{\frac{a^2}{EY}} = \frac{EY}{a^2} = \frac{Var(X)}{a^2}$$

$$EY = E(X - EX)^2 = Var X$$

$$\underline{P(|X - EX|) \geq a) \leq \frac{Var X}{a^2}}$$

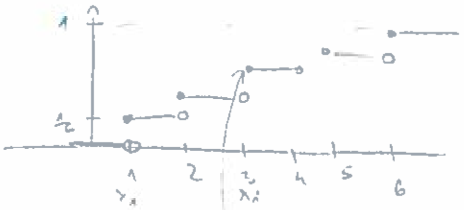
]

Distribuční funkce

$F: \mathbb{R} \to \langle 0, 1 \rangle$ $\qquad F(z) = P(\{\omega \in \Omega \mid X(\omega) \leq z\})$

prst, že náhodná veličina bude mít prst $\leq z$

Př: házení kostkou



$P(X = x_i)$ prst, že náh. hodnota nabývá hodnoty x_i

Alternativní rozdělení (indikátory)

s pravděpodobností p nabývá 1, $p \in \langle 0, 1 \rangle$, 0 v opačném případě

$$X \begin{cases} 1 & p \\ 0 & 1-p \end{cases} \qquad P(X = 0) = 1 - p, \; P(X = 1) = p$$

$$EX = p, \quad Var X = p(1-p)$$

Binomické rozdělení

$(m \in \mathbb{N}, p \in \langle 0, 1 \rangle)$ „Bernoulliho rozdělení"

$$P(X = k) = \binom{m}{k} \cdot p^k (1-p)^{m-k} \quad \text{pro } k = 0, 1, \ldots, m$$

$$EX = p \cdot m, \quad Var X = m \cdot p(1-p)$$

Provádíme-li $\underline{m}$ nezávislých pokusů, kde prst úspěšného pokusu je p, pak pro prst toho, že právě $\underline{k}$ pokusů bude úspěšných platí možností

Rovnoměrné rozdělení $(n \in \mathbb{N})$! ⚀ — příkostka

$$P(X=k) = \frac{1}{n} \quad \text{pro } k = 1, 2, \dots, n$$

$$EX = \sum_{k=1}^{n} \frac{1}{n} \cdot k = \frac{1}{n} \cdot \frac{n(n+1)}{2} = \frac{n+1}{2}$$

Pascalovo rozdělení: $n \in \mathbb{N}$, $p \in \langle 0, 1 \rangle$

Jak dlouho musím čekat na n-tý úspěch

$n = 1$ ... Geometrické rozdělení

$$P(X=k) = (1-p)^{k-1} \cdot p \qquad k = 1, 2, \dots$$

n obecné

$$P(X=k) = \binom{k-1}{n-1} p^{n-1} (1-p)^{(k-1)-(n-1)} \cdot p =$$

$$= \binom{k-1}{n-1} p^n (1-p)^{k-n} \qquad k \geq n$$

$$EX = n\left(\frac{1-p}{p} + 1\right)$$

Hypergeometrické rozdělení (počet kuliček v osudí; M jich má požadovanou vlastnost; kolik vylosuju; N, M počáteční hodnoty, $n \in \mathbb{N}$, $M < N$, $n < N$)

$$P(X=k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}} \quad \text{pro } k = \max(0, M-N+n)$$

N M

$n - (N-M) = M - N + n$

Normální rozdělení

↳ Gaussovka

GRAFY

Def <u>Graf</u> $G=(V,E)$ uspořádaná dvojice
V … konečná neprázdná mn. vrcholů
$E \subseteq \binom{V}{2}$ … hrany

Př: $G=(\{a,b,c,d,e\},\{\{a,b\},\{b,c\},\{c,d\},\{d,e\},\{a,e\},\{a,c\}\})$

Def: <u>Izomorfizmus grafů</u>
$f: V_1 \to V_2$ t. že f je bijekce $\forall u,v \in V_1: \{u,v\} \in E_1 \Leftrightarrow$
$\Leftrightarrow \{f(u), f(v)\} \in E_2$
$G_i = (V_i, E_i)$ $i=1,2$

přečíslování vrcholů slučitelné s operací u,v sousedí $(u,v) \in E$

Def: <u>Podgraf</u> $G_1 \subseteq G_2$ pokud $V_1 \subseteq V_2 \wedge E_1 \subseteq E_2$

Def: <u>Indukovaný podgraf</u> $G_1 \leq G_2$: $V_1 \subseteq V_2$ ~~&~~ $E_1 = E_2 \cap \binom{V_1}{2}$
zachovám $\forall$ hrany t. vedoucí mezi vrcholy V_1 v grafu G_2

<u>Speciální typy grafů</u>

Prázdný graf $E_n = (\{1,\dots,n\}, \emptyset)$

Úplný graf $K_n = \left(\{1,\dots,n\}, \binom{\{1,\dots,n\}}{2}\right)$ — $\forall$ dvojice z mn $\{\dots\}$

Komplement / ~~Doplněk~~: Graf $G=(V,E)$, doplněk $\overline{G} = (V, \binom{V}{2} - E)$

👁 $\overline{G} \cong G$

úplný graf jehož $\forall v \in V: \deg(v) \leq 2 \wedge$ právě 2 vrcholy mají stupeň 1

Def: <u>Cesta</u> $P_n = (\{1,\dots,n\}, \{\{i,i+1\}, i=1,\dots,n-1\})$ — neopakuju vrcholy

Def: <u>Kružnice</u> $C_n = (\{1,\dots,n\}, \{\{i,i+1\}, i=1,\dots,n-1\} \cup \{\{1,n\}\})$ $n \geq 3$
souvislý graf t. že $\forall v \in V: \deg(v) = 2$
délka$(P_n) = n-1$

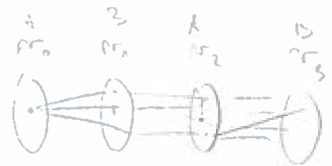
Def: $G=(V,E)$ je <u>bipartitní graf</u>, pokud $\exists A,B \subseteq V$ t. ž.
$A \cap B = \emptyset$, $A \cup B = V$ a $\forall e \in E: |A \cap e| = 1$ $(\Rightarrow |B \cap e| = 1)$.

👁 Kružnice C_n je bipartitní $\Leftrightarrow$ n je sudé

Tvrzení: G je bipartitní $\Leftrightarrow$ G neobsahuje žádnou kružnici liché délky jako podgraf

[Dk: Procházení grafu do šířky: $G=(V,E)$, $v_0 \in V$
v_1 = sousedé v_0
v_2 = nenavštívené vrcholy, dosažitelné z v_1
v_3 = ——— // ——— v_2
⋮

žádná hrana uvnitř v_i $\Rightarrow$ $\left.\begin{array}{l} A = v_0 \cup v_2 \cup \dots \\ B = v_1 \cup v_3 \cup \dots \end{array}\right\}$ G je bipartitní



16 LOGIKA

VÝROKOVÁ LOGIKA

Jazyk nad neprázdnou mn. výrokových proměnných $\mathbb{P}$ (prvovýroků) je mn. těchto proměnných společně s logickými symboly.

Zn. pravda $\top$ je zkratka za $p \vee \neg p$
spor $\perp$ je zkratka za $p \wedge \neg p$

Formule (výrok) nad $\mathbb{P}$ jsou
1. proměnné z $\mathbb{P}$ je ~~atom~~ formule
2. φ, ψ jsou formule, pak formule jsou $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$
3. každá formule vznikne konečným použitím 1, 2

Zn. mn. všech formulí $VF_{\mathbb{P}}$
mn. proměnných s výskytem ve φ $var(\varphi)$

vytvořující strom $(p \vee q) \rightarrow r$
$p \vee q$ r

Sémantika – přiřazení významu výroku, pravdivost
- prvovýrok je 0, nebo 1
- sémantika logických spojek – pravdivostní tabulka

p	q	p → q	¬p	p ∧ q	p ∨ q	p ↔ q
0	0	1	1	0	0	1
0	1	1	1	0	1	0
1	0	0	0	0	1	0
1	1	1	0	1	1	1

priorita spojek
1. $\rightarrow, \leftrightarrow$
2. $\wedge, \vee$
3. $\neg$

Převod výroku do CNF
1. tabulka pravdivostních hodnot
2. vezmu $\forall$ splňujících ohodnocení a hodnoty proměnných spojím díky $\wedge$, mezi ohodnocení $\vee$
3. $\Rightarrow$ DNF zneguju $\Rightarrow$ CNF

Tautologie je formule, která je splněna pro všechna možná ohodnocení (platí v každém modelu) zn. $\models \varphi$
↳ tzn. formule je pravdivá = Pravdivost

Splnitelnost (tzn. platí) pokud $\exists$ splnitelné ohodnocení v.
↳ výrok φ platí / je splněn pro ohodnocení v, když $v \models \varphi$, tj $\bar{v}(\varphi) = 1$
↳ výrok φ platí pokud pro něj $\exists$ model (= ohodnocení)
↳ ohodnocení v splňuje formuli

Dokazatelnost – formule φ je dokazatelná z teorie T, pokud $\exists$ důkaz φ z T, zn. $T \vdash \varphi$.
Důkaz je konečný objekt vycházející z axiomů dané Teorie a pravidel odvozování.

Teorie = mn. formulí
Model teorie = ohodnocení proměnných v němž teorie platí ($\forall$ formule jsou splněné ~~pravdivé~~)
- sporná = je v ní dokazatelný spor $\perp$ (výrok $p \wedge \neg p$, resp $p \vee \neg p$
- bezesporná = není sporná
- kompletní = není sporná & každá formule je v ní dokazatelná či vyvratitelná

Důkaz tablo metodou
Dáno teorie $T = \{A_1, \dots, A_i, \dots, A_n\}$
Formule φ
Chci dokázat φ v T, tj. $T \models \varphi$

1. do kořene dám $F(\varphi)$
2. budu rozvíjet tablo
3. když mám $\forall$ rozvinuté na konci $\{$všech nesporných větví dám $T(A_1)$
4. opakuju 2. a pak přidám všude $T(A_2)$ ....
5. Pokud jsou $\forall$ větve sporné $\otimes$ φ je dokázaná je pravdivá v T.

př: $T = \{\varphi, \varphi \rightarrow \psi\}$
$T \vdash \psi$?

$F(\psi)$
$T\varphi$
$T(\varphi \rightarrow \psi)$
$F\varphi$ $T\psi$ – $\otimes$

ψ je dokazatelné v T

Věta o úplnosti: Nechť T je teorie, φ formule. Je-li φ pravdivá v T, pak je tablo dokazatelná.
Tj $T \models \varphi \Rightarrow T \vdash \varphi$

▼ Věta říká, že každé tablo s kořenem $F\varphi$ je sporné.
sporem: mějme tablo s kořenem $F\varphi$ a nespornou větví, dle této větve lze sestrojit ohodnocení proměnných v, kt. splňuje $F(\varphi)$ a zároveň splňuje $\forall$ axiomy $T = \{A_1, \dots, A_n\}$ (ty jsou totiž na větvi všechny jako $T(A_i)$) $\Rightarrow$ $\exists$ model pro nějž neplatí φ $\Rightarrow$ spor že φ je pravdivá = φ je splněna ve $\forall$ modelech ▲

Věta o kompaktnosti: Teorie má model $\Leftrightarrow$ každá její kon. část má model.
▼ „$\Rightarrow$" zřejmá
„$\Leftarrow$" obměna $\neg B \Rightarrow \neg A$: T nemá model, tj. je sporná, lze z ní systematickým tablem dokázat spor.
Tablo důkaz je vždy konečný, použije tedy jen kon. podmn $T' \subseteq T$ a tato konečná část T' tedy nemá model. ▲

LOGIKA

elementární ekvivalence

Zákl. pojmy

Třída – je definovaná množinovou vlastností $\varphi(x)$, zn. $\{x \mid \varphi(x)\}$
– vlastní třída – je třída, kt. není množinou (př. $\{x \mid x = x\}$)

zn. $x \notin y$ tj. $\neg(x \in y)$, $x \neq y$ tj. $\neg(x = y)$

zn. $\{x_0, \dots, x_{n-1}\}$ je mn. s prvky $x_0, \dots, x_{n-1}$

singleton = jednoprvková mn., zn. $\{x\}$

neusp. dvojice = zn. $\{x, y\}$

zn. $\emptyset, \cup, \cap, \setminus, \triangle$ tj. prázd. mn., sjednocení, průnik, rozdíl, sym. rozdíl

zn. $x \cap y = \emptyset$ tj. jsou **disjunktní**

$x \subseteq y$ tj. x je podmn. y

Potenční mn. (**potence**) x je $\mathcal{P}(x) = \{y \mid y \subseteq x\}$ mn. $\forall$ podmnožin x

sjednocení (suma) – x je $\bigcup x = \{z \mid \exists y (z \in y \wedge y \in x)\}$

pokrytí mn. x je mn. $y \subseteq \mathcal{P}(x) \setminus \{\emptyset\}$ s $\bigcup y = x$ (tj. mn. množin jejichž sjednocení je celá M) nějaké
– je rozklad pokud platí navíc, že každé dvě různé mn. v y jsou disjunktní

Relace

usp. dvojice – je $(x, y) = \{x, \{x, y\}\}$, tedy $(x, x) = \{x, \{x\}\}$

usp. n-tice – je $(x_0, \dots, x_{n-1}) = ((x_0, \dots, x_{n-2}), x_{n-1})$ pro $n > 2$

kartézský součin = $a \times b = \{(x, y) \mid x \in a, y \in b\}$

kartézská mocnina
$x^0 = \{\emptyset\}$
$x^1 = x$
$x^n = x^{n-1} \times x$ pro $n > 1$

disjunktní sjednocení $x \uplus y = (\{\emptyset\} \times x) \cup (\{\{\emptyset\}\} \times y)$

relace = mn. uspořádaných dvojic zn. $R(x, y)$ ~~...~~ $(x, y) \in R$ xRy

doména (definiční obor) $\mathrm{dom}(R) = \{x \mid \exists y\, (x, y) \in R\}$ zn. D_R

obor hodnot $\mathrm{rng}(R) = \{y \mid \exists x\, (x, y) \in R\}$

rozšíření **extenze** – prvku x v R je $R[x] = \{y \mid (x, y) \in R\}$

inverzní relace – k R je $R^{-1} = \{(y, x) \mid (x, y) \in R\}$

zúžení **restrikce** – R na mn. z je $R \restriction z = \{(x, y) \in R \mid x \in z\}$

složení relací R a S je $R \circ S = \{(x, z) \mid \exists y ((x, y) \in R \wedge (y, z) \in S)\}$

identita na mn. Z je relace $Id_Z = \{(x, x) \mid x \in Z\}$

ekvivalence je relace na mn. X, kde $\forall x, y, z \in X$ platí:
- reflexivita $R(x, x)$
- symetrie $R(x, y) \to R(y, x)$
- tranzitivita $R(x, y) \wedge R(y, z) \to R(x, z)$

třída ekvivalence (faktor) – prvku x dle R je $R[x]$, zn. též $[x]_R$

faktorizace mn. X dle R je ~~...~~ $X/R = \{R[x] \mid x \in X\}$
mn. ∀ tříd ekvivalence platí, že X/R je rozklad X, neboť třídy jsou disjunktní a pokrývají X)
(rozklad X určuje ekvivalenci na mn. X)

Uspořádání

Nechť $\leq$ je relace na mn. X. Pak $\leq$ je:

částečné usp. – pokud $\forall x, y, z \in X$ platí
- $x \leq x$ reflexivita
- $x \leq y \wedge y \leq x \to x = y$ antisymetrie
- $x \leq y \wedge y \leq z \to x \leq z$ tranzitivita

lineární (totální) usp. – pokud navíc $\forall x, y \in X$: $x \leq y \vee y \leq x$ dichotomie každé 2 prvky jsou porovnatelné

dobré usp. – pokud navíc každá neprázdná mn. obsahuje nejmenší prvek

~~...~~

husté usp. – Buď $x < y$ za $x \leq y \wedge x \neq y$. Lin. usp. $<$ na X je husté, pokud X není singleton a pro $\forall x, y \in X$: $x < y \to \exists z (x < z \wedge z < y)$ ...hustota

Fce

fce f je relace pro niž platí: $\forall x \in \mathrm{dom}(f)\ \exists!\, y : (x, y) \in f$, zn. $f : X \to Y$, $\mathrm{dom}(f) = X$, $\mathrm{rng}(f) \subseteq Y$

hodnota – fce f v bodě x je y, zn. $f(x) = y$

surjektivní (na) – pokud $\mathrm{rng}(f) = Y$

prostá (injektivní) – pokud $\forall x, y \in \mathrm{dom}(f)$: $x \neq y \to f(x) \neq f(y)$

bijekce – je-li prostá a na

inverzní fce $f^{-1} = \{(y, x) \mid (x, y) \in f\}$ pokud f je prostá

obraz mn. A přes f je $f[A] = \{y \mid (x, y) \in f$ pro nějaké $x \in A\}$

složení $(f \circ g)(x) = g(f(x))$

Čísla

přirozená čísla
$m = \{0, \dots, m-1\}$, $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$, ...

$\mathbb{N}$ je nejmenší mn. obsahující $\emptyset$ uzavřená na $S(x) := x \cup \{x\}$ (následník).

$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, kde $\sim$ je ekvivalence def. $(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$

$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\approx$, kde $\approx$ je : $(a,b) \approx (c,d) \Leftrightarrow a \cdot d = b \cdot c$

$\mathbb{R}$ je mn. řezů racionálních čísel, tj. netriviálních, dolů uzavřených podmn. $\mathbb{Q}$ bez největšího prvku ($A \subset \mathbb{Q}$ je dolů uzav., pokud $y < x \in A \Rightarrow y \in A$)

Velikosti mn.

$(x \preccurlyeq y) \equiv |x| \leq |y|$ (x je subvalentní y) pokud $\exists$ prostá $f: x \to y$

$(x \approx y) \equiv |x| = |y|$ pokud $\exists f$ bijekce $x \to y$

$(x \prec y) \equiv |x| < |y|$ pokud $x \preccurlyeq y$ a není $x \approx y$

? kardinální číslo κ pro x je $x \approx \kappa$ zn. $|x| = \kappa$

konečná x pokud $|x| = n$, $n \in \mathbb{N}$

spočetná pokud $|x| = |\mathbb{N}| = \omega$

nespočetná není-li ani konečná

mohutnost kontinua $|x| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}$

n-ární relace a fce

Arita (četnost) - relace je číslo $n \in \mathbb{N}$, relace $R \subseteq X^n$ zn. $ar(R)$ — nulární, unární, binární, n-ární

Při $n=0$: $R = \emptyset = 0$ nebo $R = \{\emptyset\} = 1$

$n=1$: $R \subseteq X$

- (částečné) fce ~~$f: X^n \to Y$~~ zn. $ar(f)$

$f: X^n \to Y$

je-li $Y = X$ pak f je operace na X

konstantní fce $f: A^n \to B$ pokud $rng(f) = \{y\}$ pro nějaké $y \in Y$, pro $n=0$ je $f \{(\emptyset, y)\}$

a f ztotožňujeme s konstantou y.

Stromy

Strom je mn. T s částečným usp $<_T$ ve kt. existuje (jediný) nejmenší prvek kořen,

a ~~mn.~~ předků lib. prvku je dobře uspořádaná.

Větev stromu T je maximální lineárně usp. podmn. T.

- větev v kon. stromu je cesta ~~od~~ z kořene do listu

konečně větvící se strom - ~~vrcholu~~

otec - bezprostřední předek

n-tá úroveň stromu, $n \in \mathbb{N}$, obsahuje syny $(n-1)$-ní úrovně,

0-tá obsahuje kořen

hloubka stromu T je maximální ~~n~~ neprázdná úroveň

~~prázdná~~ pro T s nekonečnou větví je hloubka nekonečná či ω

uspořádaný strom T kt. má lin. usp. synů každého vrcholu (pravolevé) $<_L$

(stromové) $<_T$

značkový strom je strom T s lib. fcí (značící fce), kt. každému vrcholu T

přiřazuje nějaký objekt (značku)

II

prvovýrok = výroková proměnná (mimologický symbol)

$\mathbb{P}$ = mn. prvovýroků (neprázdná), většinou nejvýše spočetná ($\Rightarrow$ formule mají ~~spočetnou~~ konečnou délku)

Jazyk ~~VL~~ VL je určen $\mathbb{P}$ a symboly • výrokové prom.

• spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ } logické symboly

• závorky $(,), [,], \{, \}$

$\top$ pravda, $\bot$ spor tj. $p \vee \neg p$, resp. $p \wedge \neg p$

Výroky (výrokové formule) jsou i) $\forall$ výroková prom $\in \mathbb{P}$

ii) je-li φ, ψ výrok pak i: $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow$

iii) výrok vzniklý konečným použitím pravidel i), ii)

řetězec je konečná posl. symbolů jazyka

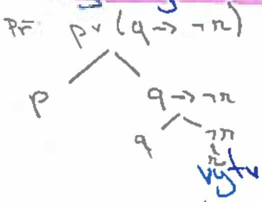
podformule (podvýrok) je výroková formule, kt. je součástí nějaké jiné formule φ

$VF_{\mathbb{P}}$ ... mn. $\forall$ výrokových formulí

$var(\varphi)$ ... mn. $\forall$ výrokový prom. s výskytem ve φ

asociativita $\vee, \wedge$: $(p \vee q) \vee r \equiv p \vee (q \vee r) \equiv p \vee q \vee r$

Vytvořující strom je kon. usp. strom jehož vrcholy jsou označeny výroky dle násl. pravidel:



1) listy (a jen listy) jsou označeny prvovýroky
2) je-li vrchol označen $(\neg\varphi)$, má jediného syna φ
3) je-li vrchol označen $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ nebo $(\varphi \leftrightarrow \psi)$ má 2 syny, přičemž levý je φ a pravý je ψ

výtv. strom výroku φ je výtv. strom s kořenem označeným φ

pravdivostní tabulka

Booleovské fce jsou n-ární operace na $2 = \{0,1\}$

ohodnocení prvovýroků je fce $v : \mathbb{P} \to \{0,1\}$, tj. $v \in {}^{\mathbb{P}}2$

hodnota výroku φ je $\bar{v}(\varphi)$ při ohodnocení v daná induktivně

$\bar{v}(p) = v(p)$ pokud $p \in \mathbb{P}$ $\qquad \bar{v}(\neg\varphi) = -_1(\bar{v}(\varphi))$

$\bar{v}(\varphi \wedge \psi) = \wedge_1(\bar{v}(\varphi), \bar{v}(\psi))$ $\qquad \bar{v}(\varphi \vee \psi) = \vee_1(\bar{v}(\varphi), \bar{v}(\psi))$

$\bar{v}(\varphi \to \psi) = \to_1(\bar{v}(\varphi), \bar{v}(\psi))$ $\qquad \bar{v}(\varphi \leftrightarrow \psi) = \leftrightarrow_1(\bar{v}(\varphi), \bar{v}(\psi))$

kde $-_1, \wedge_1, \vee_1, \to_1, \leftrightarrow_1$ jsou B. fce dané tabulkami.

Poz: $\bar{v} : VF_{\mathbb{P}} \to 2$ je jednoznačná extenze fce v.

Výrok φ nad $\mathbb{P}$ je ($v \in {}^{\mathbb{P}}2$ ohodnocení):

platí (~~splněný~~) při ohodnocení v pokud $\bar{v}(\varphi) = 1$
pak $\bar{v}$ je splňující ohodnocení, zn. $v \models \varphi$

pravdivý (logicky platí, tautologie) pokud $\bar{v}(\varphi) = 1$ pro $\forall v \in {}^{\mathbb{P}}2$, zn. $\models \varphi$
~~platí~~ platí v $\forall$ ohodnocení

lživý (sporný) pokud $\bar{v}(\varphi) = 0$ pro $\forall v \in {}^{\mathbb{P}}2$, tj. $\neg\varphi$ je pravdivý.

nezávislý pokud $\bar{v}_1(\varphi) = 0$ a $\bar{v}_2(\varphi) = 1$ pro nějaká $v_1, v_2 \in {}^{\mathbb{P}}2$
tj. není ani pravdivý ani lživý

splnitelný pokud $\bar{v}(\varphi) = 1$ pro nějaké ~~φ~~ $v \in {}^{\mathbb{P}}2$, tj. není lživý

Výroky φ a ψ jsou (logicky) **ekvivalentní** pokud $\bar{v}(\varphi) = \bar{v}(\psi)$ pro $\forall v \in {}^{\mathbb{P}}2$
tj. výrok $\varphi \leftrightarrow \psi$ je pravdivý, zn. $\varphi \sim \psi$

Modely

- **Model jazyka** -nad $\mathbb{P}$ je $v \in {}^{\mathbb{P}}2$ (tj. ohodnocení $v : \mathbb{P} \to \{0,1\}$)
- **Třída $\forall$ modelů jazyka** -nad $\mathbb{P}$ je mn. $\forall$ modelů jazyka (tj. $M(\mathbb{P}) = \{v \mid v \in {}^{\mathbb{P}}2\}$
zn. $M(\mathbb{P})$, $M(\mathbb{P}) = {}^{\mathbb{P}}2$ fakt ~~?~~ jo ~~$M(\mathbb{P}) = 2^{2^{\mathbb{P}}}$~~

- Výrok φ nad $\mathbb{P}$ (je)
  - **platí** v modelu $v \in M(\mathbb{P})$, pokud $\bar{v}(\varphi) = 1$
    ↳ pak $\bar{v}$ je **model výroku** φ, zn. $v \models \varphi$
    ↳ **třída modelů** φ je $M^{\mathbb{P}}(\varphi) = \{v \in M(\mathbb{P}) \mid v \models \varphi\}$
  - **pravdivý** (logicky) ~~platí, tautologie~~ pokud platí v každém modelu (jazyka), zn. $\models \varphi$
  - **lživý** (sporný), pokud nemá model
  - **nezávislý**, pokud platí v nějakém modelu a neplatí v jiném
  - **splnitelný**, pokud má model tj. $\exists$ model
- **Výroky** φ a ψ jsou (logicky) **ekvivalentní**, pokud mají stejné modely, zn. $\varphi \sim \psi$

Spojky

- NOR = Peirceova spojka ~~...~~; zn. $p \downarrow q$
- NAND = Shefferova spojka, zn. $p \uparrow q$
- **Mn. spojek** je **univerzální**, pokud lze každou Booleovskou fci reprezentovat nějakým z nich (dobře) vytvořeným výrokem.

CNF a DNF

- **literál** je prvovýrok nebo jeho negace $\neg p$ buď p^0; p buď p^1
- **opačný literál** k literálu ℓ značíme $\bar{\ell}$
- **klauzule** je disjunkce literálů
  ↳ prázdnou klauzulí rozumíme $\perp$
- Výrok je v konjunktivní normálním tvaru (**CNF**), je-li konjunkcí klauzulí
  ↳ prázdným výrokem v CNF rozumíme $\top$
- **Elementární konjunkce** je konjunkce literálů
  ↳ prázdná konjunkce je $\top$
- Výrok je v disjunktivní normálním tvaru (**DNF**), je-li disjunkcí elem. konjunkcí.
  ↳ prázdným výrokem v DNF rozumíme $\perp$

formule ke pro všechny volné prom. z φ dám před φ ∀ pro každou takovou prom.

in ... sentence
Thm ... P, ∀ sentence ... nemá volné výskyty

4

- **k-CNF** je tvar výroku v CNF, kde každá klauzule má nejvýše k literálů.
- **k-SAT** je problém: Je výrok φ v k-CNF splnitelný?

- Orientovaný graf G je silně souvislý, pokud $\forall u, v \in V: \exists$ orientovaná cesta $u \leadsto v$ a $v \leadsto u$
- Silně souvislá komponenta grafu G je maximální silně souvislý podgraf G.
- **Implikační graf** výroku φ v 2-CNF je orientovaný g. G_φ, v němž:
  1) vrcholy jsou prvenné výroku φ nebo jejich negace
  2) klauzuli $l_1 \vee l_2$ reprezentujeme dvojicí hran $\overline{l_1} \to l_2$, $\overline{l_2} \to l_1$
  3) klauzuli l_1 reprezentujeme hranou $\overline{l_1} \to l_1$
- $\vec{G}$ je acyklický neobsahuje-li orientovaný cyklus
- lin. usp. < vrcholů G je topologické, pokud $p < q$ pro každou hranu z p do q

Horn-SAT

- **jednotková klauzule** je klauzule obsahující jediný literál.
- **Hornova klauzule** je klauzule obsahující nejvýše 1 pozitivní literál. $\neg p_1 \vee \ldots \vee \neg p_n \vee q \sim (p_1 \wedge \ldots \wedge p_n \to q)$
- **Hornova formule** je konjunkce hornových klauzulí.
- **Horn-SAT** je problém splnitelnosti daného Hornova výroku.
- **jednotková propagace** - ∃ jednotková klauzule l, nastav l na 1, odstraň ∀ klauzule obsahující l, odstraň ze ∀ klauzulí $\overline{l}$

Teorie

- **Výroková teorie** nad jazykem $\mathbb{P}$ je lib. mn. T výroků z $VF_{\mathbb{P}}$
  Výrokům z teorie T říkáme **axiomy** teorie T.
- **Model teorie** T nad $\mathbb{P}$ je ohodnocení $v \in M(\mathbb{P})$ (tj. model jazyka), ve kt. platí ∀ axiomy z T, zn. $v \models T$
- **Třída modelů T** je $M^{\mathbb{P}}(T) = \{v \in M(\mathbb{P}) \mid v \models \varphi \text{ pro } \forall \varphi \in T\}$.
- Je-li teorie T konečná, lze ji nahradit konjunkcí jejích axiomů.
- zn. $M(T, \varphi)$ je $M(T \cup \{\varphi\})$

Sémantika vzhledem k teorii

Nechť T je teorie nad $\mathbb{P}$. Výrok φ nad $\mathbb{P}$ je
- **pravdivý** v T (platí v T), pokud platí v ∀ modelu T, zn. $T \models \varphi$.
  ↳ říkáme též, že φ je důsledkem teorie T.
- **lživý** v T (sporný v T), pokud neplatí v žádném modelu T
- **nezávislý** v T, pokud platí v nějakém modelu T a neplatí v jiném.
- **splnitelný** v T (konzistentní s T), pokud platí v nějakém modelu T
- výroky φ a ψ jsou **ekvivalentní**, pokud ∀ model T je model φ ⟺ je model ψ
- **Důsledek teorie** T nad $\mathbb{P}$ je množina $\theta^{\mathbb{P}}(T) = \{\varphi \in VF_{\mathbb{P}} \mid T \models \varphi\}$, tj. mn. ∀ pravdivých výroků v T.

Vl. teorií

- Výroková teorie T nad $\mathbb{P}$ je (sémanticky)
  - **sporná**, jestliže v ní platí spor, jinak je **bezesporná** (splnitelná). → má model
  - **kompletní**, jestliže není sporná a každý výrok je v ní pravdivý, či lživý, tj. žádný výrok v ní není nezávislý

!! model

  - **extenze** teorie T' nad $\mathbb{P}'$, $\mathbb{P}' \subseteq \mathbb{P}$ ∧ $\theta^{\mathbb{P}'}(T') \subseteq \theta^{\mathbb{P}}(T)$
    extenze T je **jednoduchá**, pokud $\mathbb{P}' = \mathbb{P}$
    extenze T je **konzervativní**, pokud $\theta^{\mathbb{P}'}(T') = \theta^{\mathbb{P}}(T) \cap VF_{\mathbb{P}'}$

$M^{\mathbb{P}}(T) \subseteq M^{\mathbb{P}}(T')$

v extenzi neplatí nic navíc
∀ co platí v extenzi a omezím se na původní jazyk nesmí toho být víc než v původní teorii

  - **ekvivalentní** s T', jestliže T je extenzí T' a T' je extenzí T.

$M^{\mathbb{P}}(T) = M^{\mathbb{P}}(T')$

- Nechť T je bezesporná teorie nad $\mathbb{P}$. Na množině $VF_{\mathbb{P}}/\sim_T$ lze zadefinovat operace $\neg, \wedge, \vee, \bot, \top$ (korektně) pomocí reprezentantů, např. $[\varphi]_{\sim_T} \wedge [\psi]_{\sim_T} = [\varphi \wedge \psi]_{\sim_T}$
  Pak $AV^{\mathbb{P}}(T) = \langle VF_{\mathbb{P}}/\sim_T, \neg, \wedge, \vee, \bot, \top \rangle$ je algebra výroků T.
  Jelikož $\varphi \sim_T \psi \Leftrightarrow M(T, \varphi) = M(T, \psi)$, je $h([\varphi]_{\sim_T}) = M(T, \varphi)$ korektně definovaná prostá fce $h: VF_{\mathbb{P}}/\sim_T \to \mathcal{P}(M(T))$ a platí:

$$h(\neg[\varphi]_{\sim_T}) = M(T) \setminus M(T, \varphi)$$
$$h([\varphi]_{\sim_T} \wedge [\psi]_{\sim_T}) = M(T, \varphi) \cap M(T, \psi)$$
$$h([\varphi]_{\sim_T} \vee [\psi]_{\sim_T}) = M(T, \varphi) \cup M(T, \psi)$$
$$h([\bot]_{\sim_T}) = \emptyset$$
$$h([\top]_{\sim_T}) = M(T)$$

navíc h je na pokud M(T) je konečná

Formální dokazovací systémy (= kalkul)

- Důkaz je konečný objekt, může vycházet z axiomů dané teorie.
- φ je dokazatelná z T zn. $T \vdash \varphi$
- korektní form. dokazovací systém = každá formule φ dokazatelná z T je v T pravdivá
- úplný f. dok. systém = každá formule φ pravdivá v T je z T dokazatelná

Příkaldy: tablo metody, Hilbertovské systémy, ...

Tablo Nechť $\mathbb{P}$ je nejvýše spočetný jazyk ($\Rightarrow \forall T$ nad $\mathbb{P}$ jsou nejvýše spočetné)

Atomické tablo je jeden z následujících (položkami ~~s~~ značkovaných) stromů, kde $p \in \mathbb{P}$ je lib. prom. a φ, ψ jsou lib. výrokové formule.

$T(\neg\varphi)$ — $F\varphi$; $F(\neg\varphi)$ — $T\varphi$; Tp; Fp; $T(\varphi\wedge\psi)$ — $T\varphi$ — $T\psi$; $F(\varphi\wedge\psi)$ — $F\varphi$ | $F\psi$; $T(\varphi\vee\psi)$ — $T\varphi$ | $T\psi$; $F(\varphi\vee\psi)$ — $F\varphi$ — $F\psi$; $F(\varphi\to\psi)$ — $T\varphi$ — $F\psi$; $F(\varphi\to\psi)$ — $F\varphi$ | $T\psi$

$F(\varphi\leftrightarrow\psi)$ — $T\varphi$, $F\psi$ | $F\varphi$, $T\psi$; $T(\varphi\leftrightarrow\psi)$ — $T\varphi$, $T\psi$ | $F\varphi$, $F\psi$

- Konečné tablo je bin. položkami značkovaný strom daný ~~pravidly~~ předpisem
  - i) každé atomické tablo je kon. tablo
  - ii) je-li P položka na větvi V koneč. tabla τ a τ' vznikne z τ připojením atom. tabla pro P na konec větve V, je τ' rovněž konečné tablo
  - iii) každé kon. tablo vznikne konečným užitím pravidel i), ii)
- Tablo je ~~kon~~ posl. $\tau_0, \tau_1, \dots, \tau_n, \dots$ (kon. i nekon.) konečných tabel takových, že τ_{n+1} vznikne z τ_n pomocí pravidla ~~i)~~ ii), formálně $\tau = \bigcup \tau_n$
- položka je formule s příznakem T nebo F, kt. reprezentuje předpoklad, že formule v nějakém modelu platí nebo neplatí

Tablo důkaz

Nechť P je položka na větvi V tabla τ. Řekneme, že

- položka P je redukovaná na V, pokud se na V vyskytuje jako kořen atomického tabla, tj. při konstrukci τ již došlo k jejímu rozvoji na V,
- větev V je sporná, obsahuje-li položky $T\varphi$ a $F\varphi$ pro nějakou formuli φ, jinak je bezesporná
- větev V je dokončená, je-li sporná nebo je každá její položka redukovaná na V.
- tablo τ je dokončené, pokud je každá jeho větev dokončená
- tablo τ je sporné pokud každá jeho větev je sporná
- Tablo důkaz (důkaz tablem) výrokové formule φ je sporné tablo s položkou $F\varphi$ v kořeni
- φ je (tablo) dokazatelná má-li tablo důkaz, zn. $\vdash \varphi$.
- analogicky vyvrácení formule φ tablem je sporné tablo s položkou $T\varphi$ v kořeni.
- φ je (tablo) vyvratitelná, má-li vyvrácení tablem, tj. $\vdash \neg\varphi$

Tablo z teorie

- Konečné tablo z teorie T je zobecnění konečného tabla přidáním pravidla
  - iii)' je-li V větev kon. tabla a $\varphi \in T$, pak připojením $T\varphi$ na konec V vznikne také konečné tablo z T.
- tablo z teorie T je posl. $\tau_0, \tau_1, \dots, \tau_n, \dots$ kon. tabel z T takových, že τ_{n+1} vznikne pomocí ii) nebo iii)', formálně $\tau = \bigcup \tau_n$
- tablo dk. formule φ z teorie T je sporné tablo z T s $F\varphi$ v kořeni,
  - má-li φ tablo dk. z T, je (tablo) dokazatelná z T, píšeme $T \vdash \varphi$
- vyvrácení formule φ tablem z teorie T je sporné tablo z T s $T\varphi$ v kořeni.
- u tabla z teorie je větev V dokončená, pokud je sporná, nebo je každá její položka redukovaná na V a navíc obsahuje $T\varphi$ pro $\forall \varphi \in T$

Tablo dk z teorie Nechť P je položka na větvi V tabla τ z teorie T. Řekneme, že

- položka P je redukovaná na V, pokud se na V vyskytuje jako kořen atom. tabla, tj. při konstrukci τ došlo k jejímu rozvoji na V
- větev V je sporná, obsahuje-li položky $T\varphi$ a $F\varphi$ pro nějakou formuli φ
- větev V je dokončená, je-li sporná, nebo je každá její položka redukovaná na V a navíc obsahuje $T\varphi$ pro každé $\varphi \in T$.
- tablo τ je dokončené, pokud je každá jeho větev dokončená; tablo τ je sporné pokud je každá jeho větev sporná
- tablo důkaz formule φ z teorie T je sporné tablo z T s $F\varphi$ v kořeni; φ je tablo dokazatelná z T, má-li tablo dk. z T, $T \vdash \varphi$
- vyvrácení formule φ tablem z teorie T je sporné tablo s $T\varphi$ v kořeni; φ je tablo vyvratitelná z T, má-li vyvrácení ~~tablem~~ z T.

Tablo Krok

Systematické tablo

- Systematické tablo ~~ze~~ z teorie T pro položku R je výsledkem následující konstrukce, tj. $\tau = \bigcup \tau_m$
- Systematická konstrukce vedoucí vždy k dokončenému tablu:
  Nechť R je položka a $T = \{\varphi_0, \varphi_1, \dots\}$ je teorie (kon. či nekon.).
  (1) Za τ_0 vezmi atom. tablo pro R. ~~Dokud~~ to lze aplikuj následující kroky.
  (2) Nechť P je nejlevější položka v co nejmenší úrovni již daného tabla τ_m, která není redukovaná na nějaké bezesporné větvi procházející skrze P.
  (3) Za τ_m' vezmi tablo vzniklé z τ_m přidáním atom. tabla pro P na $\forall$ bezespornou větev skrze P. (Neexistuje-li P, vezmi $\tau_m' = \tau_m$)
  (4) Za τ_{m+1} vezmi tablo vzniklé z τ_m' přidáním $T\varphi_m$ na každou bezespornou větev ~~do~~ neobsahující $T\varphi_m$. (Neexistuje-li φ_m, vezmi $\tau_{m+1} = \tau_m'$)
- Řekneme, že položka P se shoduje s ohodnocením v, pokud P je $T\varphi$ a $v(\varphi)=1$ nebo pokud P je $F\varphi$ a $v(\varphi)=0$.
- ~~Větev~~ Větev V tabla se shoduje s v, shoduje-li se s v každá položka na V.

Vl. teorií (syntakticky)

- Nechť T je teorie nad $\mathbb{P}$. Je-li φ dokazatelná z T, řekneme, že φ je věta (teorém) teorie T.
  Mn. vět teorie ~~T~~ T označíme $\mathrm{Thm}^{\mathbb{P}}(T) = \{\varphi \in VF_{\mathbb{P}} \mid T \vdash \varphi\}$
- Řekneme, že T je
  - sporná, jestliže je v T dokazatelný $\perp$ (spor),
    jinak je bezesporná
  - kompletní, jestliže není sporná a každá formule je v ní dokazatelná či vyvratitelná, tj. $T \vdash \varphi$ či $T \vdash \neg\varphi$ ~~pro~~ $\forall \varphi \in VF_{\mathbb{P}}$
  - extenze ~~T~~ teorie T' nad $\mathbb{P}'$, jestliže $\mathbb{P}' \subseteq \mathbb{P} \wedge \mathrm{Thm}^{\mathbb{P}'}(T') \subseteq \mathrm{Thm}^{\mathbb{P}}(T)$
    extenze T teorie T' ~~...~~ je jednoduchá, pokud $\mathbb{P} = \mathbb{P}'$
    extenze T ~~je~~ teorie T' je konzervativní, pokud $\mathrm{Thm}^{\mathbb{P}'}(T') = \mathrm{Thm}^{\mathbb{P}}(T) \cap VF_{\mathbb{P}'}$
  - ekvivalentní s teorií T', jestliže T je extenzí T' a T' je extenzí T.

(Graf G (V,E) je k-obarvitelný, pokud $\exists c: V \to k$ takové, že $\forall \{u,v\} \in E: c(u) \neq c(v)$)

Množinová reprezentace (formulí v $\boxed{CNF}$)

Př: $(\neg p \vee q) \wedge (\neg p \vee \neg q \vee r)$ ..... $\{\{\neg p, q\}, \{\neg p, \neg q, r\}\}$

~~...~~

- klauzule C je kon. mn. literálů („tvořících disjunkci").
  ↳ Prázdná klauzule není nikdy splněna, zn. $\square$
- formule S je mn. (i nekon.) klauzulí („tvořících konjunkci")
  ↳ Prázdná formule je vždy splněna, zn. $\emptyset$
- (částečné) ohodnocení v je lib. konzistentní mn. literálů;
- konzistentní mn. literálů L je taková mn., kt. neobsahuje dvojici opačných literálů
- ohodnocení v je totální, obsahuje-li pozitivní či negativní literál od každé výrokové proměnné
- ohodnocení v splňuje formuli S, pokud $C \cap v \neq \emptyset$, pro $\forall C \in S$, zn. $v \models S$

LOGIKA – VĚTY

Cantorova věta

$x \prec P(x)$ pro každou množinu x.

▼ $f(y) = \{y\}$ pro $y \in x$ je prostá fce $f : x \to P(x)$, tedy $x \preceq P(x)$.
P.s.p.: $\exists$ prostá $g : P(x) \to x$
Definujme $y = \{g(z) \mid z \subseteq x \wedge g(z) \notin z\}$
Dle definice, $g(y) \in y \Leftrightarrow g(y) \notin y$ … spor ▲

Königovo lemma

Každý nekonečný, konečně se větvící strom T obsahuje nekonečnou větev.

▼ Hledání nekonečné větve začneme v kořeni. Jelikož má jen kon. mnoho synů, $\exists$ syn s nekonečně mnoha potomky. Vyberme ho a stejně pokračujme v jeho podstromě. Takto získáme nekonečnou větev. ▲

Horn-SAT

$(p \vee \neg q) \wedge (\neg r \vee \neg q)$

Problém: Je splnitelný Hornův výrok? → konjunkce klauzulí s nejvýše 1 pozitivním literálem

Alg.: (1) obsahuje-li φ dvojici jednotkových klauzulí ℓ a $\bar{\ell}$, není splnitelný
(2) obsahuje-li φ jednotkovou klauzuli ℓ, nastav ℓ na 1, odstraň $\forall$ klauzule obsahující ℓ, odstraň ze $\forall$ klauzulí $\bar{\ell}$ a opakuj od začátku
(3) neobsahuje-li φ jednotkovou klauzuli je splnitelný ohodnocením 0 všech zbývajících ~~kterého~~ proměnných

▼ Algoritmus řešící Horn-SAT je korektní.

V. o kompaktnosti a její důsledky
dokazatelnost, konečnost dk., korektnost, úplnost
Tablo metoda ve VL

korektnost 1. kroku je zřejmá!
2. kroku plyne z ÄÄ Nechť φ' je výraz získaný z φ jednotkovou propagací. Pak φ' je splnitelný $\Leftrightarrow$ φ je splnitelný.
3. kroku díky Hornově tvaru, neboť v každé zbývající klauzuli je negativní literál ▲

2-SAT

Problém: Je splnitelný výrok v 2-CNF tvaru?

Alg.:
- vytvoření implikačního grafu
- nalezení silně souvislých komponent grafu
  ~~ohodnocení proměnných~~
- kontrakcí silně souv. komponent vytvoř G^*
- najdi topologické uspořádání v G^* „<"
- ohodnoť: Pro každou komponentu v rostoucím pořadí dle <, nejsou-li její literály dosud ohodnocené, nastav ~~•~~ je na 0 a literály v opačné komponentě na 1

Tablo metoda ve VL - syst. tablo

Dokončenost:

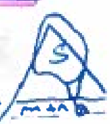
Tvrzení: Pro každou teorii T a položku R je syst. tablo τ dokončené.

▼ Nechť $\tau = \bigcup \tau_n$ je syst. tablo z $T = \{\varphi_0, \varphi_1, \dots\}$ s R v kořeni.

- Je-li větev v τ bezesporná, je i každý její prefix v τ_n bezesporný.
- Je-li položka P neredukovaná na větvi ~~V~~ v τ, je neredukovaná na každém jejím prefixu v τ_n (na němž leží).
- Do úrovně každé položky P (včetně její) je v τ jen konečně položek.
- Kdyby P byla neredukovaná na nějaké bezesporné větvi τ, přišla by na ni řada v nějakém kroku (2) tablo metody a byla by zredukována krokem (3).
- Každá $\varphi_n \in T$ bude dle (4) nejpozději v τ_{n+1} na každé bezesporné větvi.
- Tedy systematické tablo τ obsahuje pouze dokončené větve ▲

Konečnost dk

Tvrzení: Je-li $\tau = \bigcup \tau_n$ sporné tablo, je τ_n sporné konečné tablo pro nějaké n.



▼ Nechť S je mn. vrcholů stromu τ, jenž nad sebou neobsahují spor, tj. mezi předky nemají dvojici $T\varphi$ a $F\varphi$ pro žádné φ.

- Kdyby S byla nekonečná, dle Königova lemmatu by podstrom τ na vrcholech S obsahoval nekonečnou větev, tedy by τ nebylo sporné.
- Jelikož je S konečná, všechny vrcholy z S leží do úrovně m pro nějaké m.
- tedy každý vrchol v úrovni $m+1$ má nad sebou spor
- Zvolme n takové, že τ_n se shoduje s τ do úrovně $m+1$ včetně.
- Pak každá větev v τ_n je sporná. ▲

KOREKTNOST $T \vdash \varphi$ (kořen) $\Rightarrow \exists$ větev, kt. to dokazuje, shoduje se s modelem $\mathcal{V}$

Lemma: Nechť $\mathcal{V}$ je model teorie T, kt. se shoduje s položkou v kořeni tabla $\tau = \bigcup \tau_n$ z T. Pak v tablu τ $\exists$ větev shodující se s $\mathcal{V}$.

▼ Indukcí nalezneme posl. $V_0, V_1, \dots$ takovou, že pro $\forall n$ je V_n větev v τ_n shodující se s $\mathcal{V}$ a V_n je obsažena ve V_{n+1}.

- ověřením atomických tabel snadno zjistíme, že základ indukce platí.
- Pokud τ_{n+1} vznikne z τ_n bez prodloužení V_n, položme $V_{n+1} = V_n$
- Vznikne-li τ_{n+1} z τ_n připojením $T\varphi$ k V_n pro nějaké $\varphi \in T$, nechť V_{n+1} je tato větev. Jelikož $\mathcal{V}$ je modelem φ, shoduje se V_{n+1} s $\mathcal{V}$.
- Jinak τ_{n+1} vznikne z τ_n prodloužením V_n o atom. tablo nějaké položky P na V_n. Jelikož se P shoduje s $\mathcal{V}$ a tvrzení platí pro atom. tabla, lze požadovanou větev V_{n+1} v τ_{n+1} nalézt. ▲

Věta (o korektnosti): Pro každou teorii T a formuli φ platí $T \vdash \varphi \Rightarrow T \models \varphi$.

(je-li φ dokazatelná z T $\Rightarrow$ je pravdivá v T)

▼
- Nechť φ je tablo dokazatelná z T, tj. $\exists$ sporné tablo τ s $F\varphi$ v kořeni.
- Pro spor předpokládejme, že φ není pravdivá v T, tj. $\exists$ model $\mathcal{V}$ teorie T, ve kt. φ neplatí (protipříklad).
- Jelikož se položka $F\varphi$ shoduje s $\mathcal{V}$, dle předchozího lemmatu v tablu τ $\exists$ větev shodující se s $\mathcal{V}$.
- To ale není možné, neboť každá větev tabla τ je sporná, tj. obsahuje dvojici $T\psi, F\psi$ pro nějaké ψ. ▲

ÚPLNOST → Bezesporná větev dává protipříklad

Lemma: Nechť V je bezesporná větev dokončeného tabla τ. Pro následující ohodnocení $\overline{v}$ výrokových proměnných platí, že V se shoduje s $\overline{v}$.

$$\overline{v}(p) = \begin{cases} 1 & \text{pokud } Tp \text{ se vyskytuje na } V \\ 0 & \text{jinak} \end{cases}$$

▼ Indukcí dle struktury formule v položce vyskytující se na V

- Je-li položka Tp na V, kde p je prvovýrok, je $\overline{v}(p)=1$ dle definice $\overline{v}$.
- Je-li položka Fp na V, není Tp na V, jinak by V byla sporná, tedy $\overline{v}(p)=0$, dle definice $\overline{v}$.

rozbor spojek

Je-li $T(\varphi \wedge \psi)$ na V, je $T\varphi$ a $T\psi$ na V, neboť τ je dokončené. Dle ind. předpokladu je $\overline{v}(\varphi) = \overline{v}(\psi) = 1$, tedy $\overline{v}(\varphi \wedge \psi) = 1$.

Je-li $F(\varphi \wedge \psi)$ na V, je $F\varphi$ nebo $F\psi$ na V, neboť τ je dokončené. Dle ind. př. je $\overline{v}(\varphi) = 0$ nebo $\overline{v}(\psi) = 0$, tedy $\overline{v}(\varphi \wedge \psi) = 0$.

- Pro ostatní spojky obdobně jako v předchozích dvou případech. ◢

Věta: Pro každou teorii T a formuli φ, je-li φ pravdivá v T, je φ tablo dokazatelná z T, tj. $T \models \varphi \Rightarrow T \vdash \varphi$.

▼ Nechť φ je pravdivá v T. Ukážeme, že lib. dokončené tablo τ z teorie T s položkou $F\varphi$ v kořeni je sporné.

Sporem:

- Nechť V je nějaká bezesporná větev τ.
- Dle předchozího lemmatu $\exists$ ohodnocení $\overline{v}$ prvovýroků takové, že V se shoduje s $\overline{v}$, speciálně s $F\varphi$, tj. $\overline{v}(\varphi) = 0$
- Jelikož V je dokončená, obsahuje $T\psi$ pro které $\psi \in T$.
- Tedy $\overline{v}$ je modelem teorie T (neboť V se shoduje s $\overline{v}$).
- To je ale ve sporu s tím, že φ platí v každém modelu T ⇒ v kořeni je $F\varphi$

Tedy tablo τ je důkazem φ z T. ◢

$\tau = \tau_n$

(Výroková logika)

V. o kompaktnosti:
Teorie má model $\Longleftrightarrow$ každá její konečná část má model

i) ▼ „$\Rightarrow$" zřejmá

„$\Leftarrow$" Sporem: pokud teorie T nemá model, je sporná; tj. je z ní dokazatelný $\perp$ systematickým tablem τ. Jelikož je τ konečné, je $\perp$ dokazatelný z nějaké konečné ~~části~~ $T' \subseteq T$, tj. T' nemá model. ▲

ii) ▼

Nechť $T = \{\varphi_i \mid i \in \mathbb{N}\}$.
Uvažme strom S na konečných bin. posloupnostech σ uspořádaných prodloužením. Přičemž $\sigma \in S$ právě když $\exists v$ ohodnocení prodlužující σ takové, že $v \models \varphi_i$, pro $\forall i \leq lth(\sigma)$ ▲

length

S má nekonečnou větev $\Longleftrightarrow$ T má model.
▽ Jelikož $\{\varphi_i \mid i \in n\} \subseteq T$ má model pro každé $n \in \mathbb{N}$, bude každá úroveň v S neprázdná. Tedy S je nekonečný, navíc binární a dle Königova lemmatu obsahuje nekonečnou větev △

REZOLUCE

- Korektnost
  Je-li S rezolucí zamítnutelná, je S nesplnitelná. ... formule v CNF v množinové reprezentaci
- Úplnost
  Je-li konečná S nesplnitelná, je rezolucí vyvratitelná, tj. $S \vdash_R \square$
- LI-rezoluce pro Hornovy formule - úplnost
  Je-li Hornova formule T splnitelná a $T \cup \{G\}$ nesplnitelná pro cíl G, lze $\square$ odvodit LI-rezolucí z $T \cup \{G\}$ začínající G.

SÉMANTIKA PL

- V. o konstantách
  Nechť φ je formule jazyka L s volnými proměnnými $x_1, \dots, x_n$ a T je teorie jazyka L. Označme L' rozšíření L o nové konstantní symboly $c_1, \dots, c_n$ a T' teorii nad jazykem L'. Pak $T \models \varphi \iff T' \models \varphi(x_1/c_1, \dots, x_n/c_n)$.
- vlastnosti otevřených teorií
  - $\nexists T \vdash \bot \implies$ T je sporná, jinak bezesporná
  - $(\forall \varphi$ sentence : $T \vdash \varphi$ či $T \vdash \neg\varphi) \wedge$ není sporná $\implies$ T kompletní
  - Buď T' jazyka L'.
    $L' \subseteq L \wedge \mathrm{Thm}^{L'}(T') \subseteq \mathrm{Thm}^{L}(T) \implies$ T je extenze T'
    $L = L' \implies$ jednoduchá
    $\mathrm{Thm}^{L'}(T') = \mathrm{Thm}^{L}(T) \cap \mathrm{Fm}_{L'} \implies$ konzervativní
  - T extenze T' $\wedge$ T' extenze T $\implies$ T je ekvivalentní s T'
- V. o dedukci
  $T, \varphi \vdash \psi \iff T \vdash \varphi \rightarrow \psi$

TABLO METODA V PL

- Dokončenost syst. tabla
  Pro každou teorii T a položku R je systematické tablo τ dokončené.
- Konečnost
  Je-li systematické tablo τ důkazem (z teorie T), je τ konečné.
- význam axiomů rovnosti
  Axiomy: i) $x = x$
  ii) $x_1 = y_1 \wedge \dots \wedge x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$ pro $\forall$ n-ární fční symbol jazyka L
  iii) $x_1 = y_1 \wedge \dots \wedge x_n = y_n \rightarrow R(x_1, \dots, x_n) = R(y_1, \dots, y_n)$ pro $\forall$ n-ární rční symbol jazyka L včetně =

  Vlastnosti: Nechť $\mathcal{A}$ struktura pro jazyk L, ve kt. je rovnost interpretována jako $=^{A}$ splňující axiomy rovnosti.
  1) Z axiomů (i) a (iii) plyne, že relace $=^{A}$ je ekvivalence na A
  2) Axiomy (ii) a (iii) vyjadřují, že relace $=^{A}$ je kongruence pro každou fci ~~a~~ relaci v $\mathcal{A}$
  3) Je-li $\mathcal{A} \models T^*$, je i $(\mathcal{A}/=^{A}) \models T^*$,
  kde $\mathcal{A}/=^{A}$ je faktorstruktura struktury $\mathcal{A}$ dle $=^{A}$, přičemž rovnost je v $\mathcal{A}/=^{A}$ interpretovaná jako identita,

TABLO METODA V PL

- Korektnost
  Pro každou teorii T a sentenci φ, je-li φ tablodokazatelná z T je φ pravdivá v T, tj. $T \vdash \varphi \implies T \models \varphi$.
  Lemma: Nechť $\mathcal{A}$ je model teorie T jazyka L, kt. se shoduje s položkou R v kořeni tabla $\tau = \bigcup \tau_n$ z T. Pak $\mathcal{A}$ lze expandovat do jazyka L_C tak, že se shoduje s nějakou větví V v tablu τ.
- Úplnost
  Pro každou teorii T a sentenci φ, je-li φ pravdivá v T, je φ tablodokazatelná z T, tj. $T \models \varphi \implies T \vdash \varphi$
  Lemma: kanonický model $\mathcal{A}$ z bezesporné dok. větve V se shoduje s V.

TABLO METODA PL

- Kanonický model s rovností
  Kanonický model s rovností z větve V je faktorstruktura $\mathcal{A}/=^A$.
  - Kanonický model
    Nechť V je bezesporná větev dokončeného tabla z teorie T jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$. Kanonický model z větve V je L_c-struktura $\mathcal{A} = \langle A, \mathcal{F}^A, \mathcal{R}^A \rangle$, kde:
    (1) A je mn. ∀ konstantních ~~termů~~ L_c
    (2) ~~...~~ $f^A(t_{i_1}, \dots t_{i_n}) = f(t_{i_1}, \dots, t_{i_n})$
    pro každý n-ární fční symbol $f \in \mathcal{F} \cup (L_c/L)$ a $t_{i_1}, \dots, t_{i_n} \in A$
    (3) $R^A(t_{i_1}, \dots, t_{i_n}) \Leftrightarrow TR(t_{i_1}, \dots, t_{i_n})$ je položka na V
    pro každý n-ární relační symbol $R \in \mathcal{R}$ či rovnost a $t_{i_1}, \dots t_{i_n} \in A$

- Löwenheim-Skolemova v.
  Každá bezesporná teorie T nejvýše spočetného jazyka L bez rovnosti má model, který je spočetný.
- V. o kompaktnosti
  Teorie má model $\Longleftrightarrow$ každá její konečná část má model.
  + důsledky

- Extenze o definice
  - Nechť T je teorie jazyka L, $\psi(x_1, \dots, x_n)$ je formule jazyka L ve volných proměnných $x_1, \dots, x_n$ a L' je rozšíření L o nový relační symbol R.
    Extenze teorie T o definici R formulí ψ je teorie T' vzniklá přidáním axiomu
    $$R(x_1, \dots, x_n) \leftrightarrow \psi(x_1, \dots, x_n)$$
    ÄÄ každý model T lze jednoznačně expandovat na model T'.
    Důsledek: T' je konzervativní extenze T.
    Tvrzení: Pro každou formuli φ' nad L' $\exists \varphi$ nad L, t.ž. $T' \models \varphi' \leftrightarrow \varphi$.
  - Nechť T je teorie jazyka L a pro formuli $\psi(x_1, \dots x_n, y)$ jazyka L volných prom. $x_1, \dots, x_n, y$ platí: $T \models (\exists y)\, \psi(x_1, \dots, x_n, y)$ (existence)
    $T \models (\psi(x_1, \dots, x_n, y) \wedge \psi(x_1, \dots, x_n, z)) \rightarrow y = z$ (jednoznačnost)
    označme L' rozšíření jazyka L o nový n-ární fční symbol f.
    Extenze teorie T o definici f formulí ψ je teorie T' vzniklá přidáním axiomu: $f(x_1, \dots, x_n) = y \leftrightarrow \psi(x_1, \dots, x_n, y)$
    –||–

  - ~~Extenze~~ Teorie T' jazyka L' je extenze T jazyka L o definice, pokud vznikla z T postupnou extenzí o definici relačního a fčního symbolu

  Důsledky:
  - pro každou formuli φ' nad L' $\exists \varphi$ nad L takové, že $T' \models \varphi' \leftrightarrow \varphi$
- Skolemova v.
  Každá teorie T má otevřenou konzervativní extenzi T*.
- Herbrandova v.
  Nechť T je otevřená teorie jazyka L bez rovnosti a s alespoň jedním konstantním symbolem. Pak:
  a) T má Herbrandův model, anebo
  b) ∃ konečně mnoho základních instancí axiomů z T, jejichž konjunkce je nesplnitelná, a tedy T nemá model

REZOLUCE V PL

- Korektnost
  Je-li formule S rezolucí zamítnutelná, je S nesplnitelná.
- Úplnost
  Je-li formule S nesplnitelná, je $S \vdash_R \square$.
  - Lifting lemma
    Nechť $C_1^* = C_1\tau_1$, $C_2^* = C_2\tau_2$ jsou základní instance klauzulí C_1, C_2 neobsahující stejnou proměnnou a C^* je rezolventa C_1^* a C_2^*. Pak existuje rezolventa C klauzulí C_1 a C_2 taková, že $C^* = C\tau_1\tau_2$ je základní instance C.

- Elementární ekvivalence
  ~~Struktury~~ $\mathcal{A}$ a $\mathcal{B}$ jazyka L jsou elementárně ekvivalentní, zn. $\mathcal{A} \equiv \mathcal{B}$, pokud v nich platí stejné formule (jazyka L), tj. $Th(\mathcal{A}) = Th(\mathcal{B})$.

  ? důsledky L.-S. věty ?

- Izomorfismus a sémantika
  Nechť $\mathcal{A}, \mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$. Bijekce $h: A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$ právě když platí zároveň:
  (i) $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[he]$ pro $\forall$ term t a $e: Var \to A$
  (ii) $\mathcal{A} \models \varphi[e] \iff \mathcal{B} \models \varphi[he]$ pro $\forall$ formuli φ a $e: Var \to A$

- ω-kategoričnost
  Nechť jazyk L je nejvýše spočetný.
  i) Je-li teorie T jazyka L bez rovnosti ω-kategorická, je kompletní.
  ii) Je-li teorie T jazyka L s rovností ω-kategorická a bez konečného modelu, je kompletní.
  ∇ Každý model teorie T je elementárně ekvivalentní s nějakým spočetným modelem T, ale ten je až na izomorfismus jediný. Tedy všechny modely T jsou elementárně ekvivalentní, tj. T je kompletní. Δ

- Podmínky pro axiomatizovatelnost
  Nechť $K \subseteq M(L)$ je třída struktur jazyka L. Řekneme, že K je
  - axiomatizovatelná, pokud $\exists$ teorie T jazyka L s $M(T) = K$
  - konečně axiomatizovatelná, pokud je axiomatizovatelná konečnou teorií
  - otevřeně ——— " ——— otevřenou teorií
  - teorie T je konečně (otevřeně) axiomatizovatelná, pokud $M(T)$ je ~~axi~~ konečně (resp. otevřeně) axiomatizovatelná

3 DATABÁZE

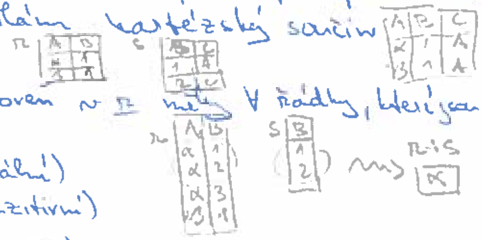
Vrstvy
- konceptuální (ER, UML) – pohled reálného světa
- logická – reprezentace konceptuálních částí v databázi a její struktura (relace, XML, graf, …)
- fyzická – implementace (datové soubory, indexové soubory)

Relační Algebra

- tabulka: Tab_jm(Atribut$_1$: typ, Atribut$_2$: typ, …)
- nadklíč = skupina atributů jednoznačně ~~určující~~ identifikující řádek
  - klíč = minimální nadklíč

nadklíč = super klíč, klíč = kandidátní klíč

- cizí klíč – skupina atributů, kt. v jiné referenční tabulce tvoří klíč (nadřazená tabulka)
  ↳ referenční integrita (odkazování se mezi tabulkami)
- primární klíč = identifikuje řádek tabulky, nesmí být NULL, musí být jednoznačný
- přirozené spojení (natural join) – relace profiltruji přes podmínku $r \cap s$, a to přes společné atributy!
  $r = (a_1, a_2, a_3)$ řádky $r(a_3) = s(a_3)$ nechám – a na tom co mi zbylo udělám kartézský součin
  $s = (a_3, a_4, a_5)$ zbytek řádků smažu ⇝ r', s' ⇝ $r' \times s'$
- dělení $r \div s$ = jen ty atributy r kt. nejsou v s a zároveň v r mají ∀ řádky, které jsou v s



- Armstrongova pravidla
  1. $Y \subseteq X \Rightarrow X \to Y$ (triviální)
  2. $X \to Y \wedge Y \to Z \Rightarrow X \to Z$ (tranzitivní)
  3. $X \to Y \wedge X \to Z \Rightarrow X \to YZ$ (kompozice)
  4. $X \to YZ \Rightarrow X \to Y \wedge X \to Z$ (dekompozice)
- • Funkční závislosti
  $R(A,F)$ $F = \{a \to b\}$ $A = \{a, b\}$
  - fční uzávěr = mn. všech fčních závislostí zn. F^+
  - redundantní fční závislost f = F^+ bez ní je stejná
  - uzávěr mn. atributů A^+ = jen ∀ atributy odvoditelné pomocí F
  - redundantní atribut a = $X \to Y \wedge a \in X \wedge Y \subseteq (X - a)^+$.
- klíč vždy generuje ∀ atributy tj. $K \to A$

1. NORMÁLNÍ FORMA (=plochost databáze) Každý atribut schématu relace je elementárního typu a je nestrukturovaný
- ✔ Osoba(Id: integer, Jm: string)
- ✗ Zamestnanci (Id: integer, Podřízení: Osoba[], Nadřízený: Osoba)
  ↳ vnořená tabulka ⇝ strukturovaný typ

2. NORMÁLNÍ FORMA Neexistuje částečná závislost neklíčových atributů na lib. klíči.
↳ porušení vede k redundanci

✗

JM	Bydliště	Cosi
Petr	Praha	123
Petr	Praha	45
Pavel	Brno	45
Pavel	Brno	17

dekompozice ⇝

JM	Cosi
Petr	123
Petr	45
Pavel	15
Pavel	17

JM	Bydliště
Petr	Praha
Pavel	Brno

✔

3. NORMÁLNÍ FORMA Žádný neklíčový atribut není tranzitivně závislý na klíči

⇅ $\forall a \in A : X \subseteq A : X \to a$ platí alespoň 1 z:
- závislost je triviální
- X je nadklíč
- a je část klíče

BCNF (Boyce-Coddova normal forma) ∀ atribut je netriviálně závislý na klíči.
⇅ pro $X \to a$ platí alespoň 1 z:
- závislost je triviální
- X je nadklíč

✗ 

SELECT [DISTINC] výraz | * | slupec | hodnota | COUNT([DISTINCT] * / sloupec) | MAX | MIN (výraz) | SUM | AVG ([DISTINCT] výraz) — FROM — tabulka — WHERE — podmínka — GROUP BY — sloupec — HAVING — podmínka — ORDER BY — sloupec ;

tabulka.sloupec

tabulka 1 AS t1

JOIN tabulek

výraz =, <>, <, >, <=, >= výraz / ANY (dotaz)

AND, OR

IS [NOT] NULL

EXISTS ( ) – vnitřní dotaz

IN ( )

[NOT] LIKE "string" – lib. řetězec %, lib. znak _

[NOT] BETWEEN (expr1 AND expr2)

SELECT – UNION / INTERSECT / EXCEPT – SELECT

- vyhodnocení: FROM → WHERE → GROUP BY → HAVING → projekce SELECT → ORDER BY

T1 CROSS JOIN T2 = kartézský součin

T1 NATURAL JOIN T2

T1 INNER JOIN T2 ON podmínka

T1 UNION JOIN T2 = vrací řádky T1 s NULL atributy z T2 a řádky T2 s NULL atributy T1

T1 LEFT / RIGHT / FULL OUTER JOIN T2 ON podmínka

obsahuje celou levou tabulku (pokud není v T2 řádek se doplní NULL ami)

CREATE TABLE jm_tabulky(jm typ, ... id INTEGER, jm VARCHAR(128), cena DECIMAL(6,2), dat DATE, je_tu BIT DEFAULT TRUE, ... FLOAT)

jm Typ CONSTRAINT ~~pk~~ PRIMARY KEY / UNIQUE / NOT NULL / REFERENCES tab2(atribut) / CHECK podmínka (FOREIGN)

ALTER TABLE tabulka ADD sloupec / DROP sloupec / constraint podmínka

DROP TABLE jm_tabulky – smaže vše včetně schématu

DELETE FROM tabulka WHERE podmínka – smaže řádky

INSERT INTO tabulka (sloupec1, sl2, ...) VALUES ('hodnota1', 'hodnota2', TRUE, ...)

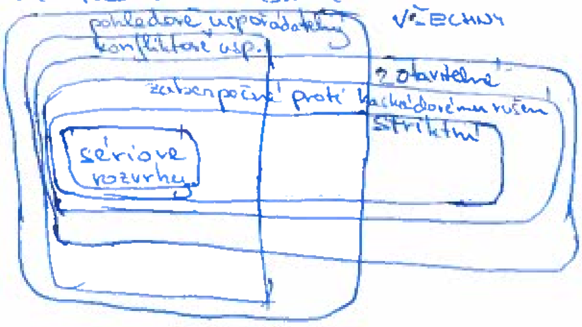
UPDATE tabulka SET cena = '155' WHERE id = '3'

TRANSAKCE

aplikace ⟷ manažer transakcí ⟷ rozvrhovač transakcí (scheduler) — manažer DB — DB

- ACID vlastnosti
  - Atomicita
  - Consistency (konzistence)
  - Isolation – vzájemně se neovlivňují
  - Durability – provedené operace jsou v DB

Operace
- ukončení – úspěšné – COMMIT / neúspěšné ABORT, ROLL-BACK
- další ob. operace: READ(), WRITE()
- transakce = posl. operací
- serializovatelný rozvrh = uspořádatelný tak aby po vykonání byla DB v konzistentním stavu
- konflikty R-W, W-R, W-W na 1 objektu
- konfliktová uspořádatelnost ⟺ precedenční graf je acyklický (transakce vrcholy, hrany orientované konflikty)
- zotavitelný rozvrh – každá transakce T je potvrzena až jsou ∀ ostatní co použily data předtím
- kaskádové rušení transakcí



Uzamykání
- zámek
  - exkluzivní – má ho jen 1 transakce
  - sdílené – zamčení pro zápis (více transakcí čtení – lze číst, nelze zapisovat)
- lock manager
- 2PL – dvoufázový uzamykací protokol – pravidla:
  1.) pokud chci číst (resp. W) musím zamknout sdílený (resp. exkluzivní) zámek
  2.) nemůžu si zamknout nic dalšího pokud už jsem něco odemkla
  ↳ zajistí acyklicitu precedenčního grafu
- Striktní 2PL
  1) stejný
  2.) ∀ zámky jsou uvolněny na konci transakce

Deadlock = cyklicky na sebe čekají transakce
- tj. cyklus ve wait-for grafu, vrcholy = aktivní transakce, hrany T1 → T2 ... T2 má zámek, kt. chce T1
- řešení
  - při dlouhém čekání zrušíme transakci (asi vrazda)
  - zrušíme 1 transakci z wait-for cyklu podle
    - a) má nejméně zámků
    - b) zatím udělala nejméně operací
    - c) má nejdál k dokončení
- prevence
  - každá transakce má časové razítko (čím starší tím větší priorita)
  - konzervativní 2PL – všechny zámky si transakce zamkne před začátkem provádění operací – nepoužitelné

Fantom – jedna transakce mění entitu pod rukama jiné
=> nekonzistence databáze
- prevence
  - zamykání víc věcí
  - indexové zamykání (hlídá se změna indexu nad entitou)

Log – záznam úprav a transakcí

6 SÍTĚ

TAXONOMIE POČÍTAČOVÝCH SÍTÍ

velikost/dosah
- LAN (Local Area Network) = lokální síť
- WAN (Wide Area Network) = rozlehlá síť
- MAN (Metropolitan A.N.) = „rozsah města" př: PASNET pražské vysoké školy, Praguenet (pražský magistrát)
- GAN (Global A.N.) = „větší než rozlehlá" př: Internet
- PAN (Personal A.N.)

- internet (internetwork) = jakákoliv soustava propojených počítačových sítí (bez ohledu na rozsáhlost)
- Internet = konkrétní internetová síť vzniklá z ARPANETu v USA, dnes je již globální sítí
  tj. Internet je zároveň internetem

vztah k uživatelům
- PDN (Public Data Network) = VDS Veřejná Datová síť (je určena pro ∀ a pro přenos dat)
- Privátní datová síť = totéž co ↑ akorát uživatel sítě je přímo její vlastník
- Neveřejná/Poloprivátní síť = může to být privátní síť s rezervní kapacitou, která je pronajímána nebo třeba veřejná síť omezená na konkrétní skupinu uživatelů
- VPDN (Virtual Private Data Network) = virtuální privátní datová síť
  VPN – sw-ové řešení sloužící např. k větší bezpečnosti (autentizace)
  site-to-site VPN – propojení 2 více lokalit přes veřejný internet (řeší to směrovače)
  remote access VPN – slouží ke vzdálenému připojení k (firemní) síti (řeší to u klient)
- VAN (Value Added Network) = síť s přidanou hodnotou, poskytuje kromě přenosových služeb navíc nějaké přidané služby (VAS – Value Added Services) např. elektronickou poštu, přístup do databáze

- podle přenosového média: datové sítě, optické, bezdrátové
- způsob použití: intranet, extranet (vzdálený přístup do vnitřní sítě = intranetu)
- původ: telekomunikační, počítačové, terminálové sítě
- způsobu fungování: přepojované vs. distribuční sítě (přepojování okruhů/paketů)
- účel: páteřní sítě (transparentní), přístupové
- topologie: se systematickou topologií (strom, kruh, sternice, …), nesystematickou top., ad-hoc sítě (decentralizovaná)
- podle architektury: TCP/IP, ISO/OSI, sítě SNA, …

MODELY

definuje protokoly · Protocolar Data Unit

referenční model ISO/OSI	síťová architektura TCP/IP	protokoly rodiny TCP/IP	bloky dat = PDU (hlavička, tělo)
7 aplikační	aplikační	FTP, HTTP, DNS (překlad jmen na adresy), NFS, XDR, RPS (vlastním vzhled)	zpráva (message) → segmentace (proměnná velikost)
6 prezentační			
5 relační			
4 transportní	transportní (spolehlivé spojované)	TCP, UDP, ICMP (chybové hlášení ping, zjištění MTU)	segment, datagram (nespojovaný přenos)
3 síťová	síťová	IP (nespojovaný, nespolehlivý), ARP	fragmentace paket (packet), datagram
2 linková	síťové rozhraní	Ethernet, FDDI, ATM, WiFi, SLIP, PPP, …	buňka (cell) (pevná velikost), rámec (frame) (proměnná velikost)
1 fyzická			přenos bitů (někdy po blocích)

end-to-end komunikace mezi koncovými uzly
(ne)spojovaný, (ne)spolehlivý přenos, Best Effort/QoS

- směrování (routing) mezi sítěmi (jaká bude cesta)
- forwarding ručené předávání po cestě
} router (směrovač)

Směrování algoritmy

směrovač vždy vybalí paket z rámce (z jedné sítě), rozhodne kam ho poslat, zabalí do nového rámce a pošle do jiné sítě

- statické / dynamické (ada. reagují na změny sítě)
- izolované (každý směrovač se rozhoduje podle sebe)
- distribuované (vzájemně směrovače spolupracují)
- hierarchické (v jednotlivých částech soustavy se směrování řeší samostatně)

⇒ směrovací tabulka – obsah: Cílová síť, Síťová maska, Brána (Next hop), Rozhraní (kudy to vysílá), Metrika
routing = hledání cesty

⇒ forwardovací tabulka – vzniká ze směrovací – obsah: Cílová síť, Next hop IP
forwarding = předávání
– rychlá, vybraná optimální cesta

– H
1969 ARPANET
1974 Internet
- RFC (Request for Comments) – standardy, informace, návrhy
- Protokoly • normy – musí
  • standardy – měly by

- Adresování služeb URL ⊆ URI : ftp://unsite.mff.cuni.cz/NET/RFC.
  protokol / schéma, autorita, [cesta]
  http://www.cuni.cz:1080/q?ID=123#Local
  mailto: forst@cuni.cz
  [dotaz] [fragment]

- počítačů
  - MAC adresa (př. ethernetová 8:0:20:ae:6:1f)
    ↳ v lokální síti ; linková vrstva
  - IP adresa (př. IPv4 194.50.16.71, IPv6 ::1)
    desítkové části 32b=4B; šestnáctkové části 128b=16B
    ↳ podle topologie sítě, síťová vrstva
  - doménová adresa (př. whois.cuni.cz)
    ↳ podle organizační struktury, aplikační vrstva
    nejvyšší doména (Top Level Domény) cz, NTC
    ↳ kód země

CIDR - maska / prefixová maska udává délku síťového prefixu 24b
192.168.0.0/24
resp. 225.225.225.0

- rozhraní vs. protokol - v rozhraní se předávají ~~pakety~~ datové bloky mezi jednotlivými vrstvami aby odpovídaly protokolům

- port = 16b číslo identifikující jeden konec spojení (aplikaci/proces)
  destination-port - ten musí znát klient (well-known services)
  source-port (>1024) navazovatel

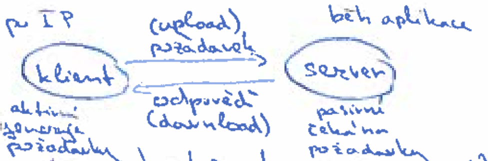
- socket - <IP adresa, port> - jeden konec komunikace

- FTP (File Transfer Protocol) - jeden z nejstarších protokolů,
  - správa souborů

- SMTP - protokol pro elektronickou poštu stejně jako POP a IMAP

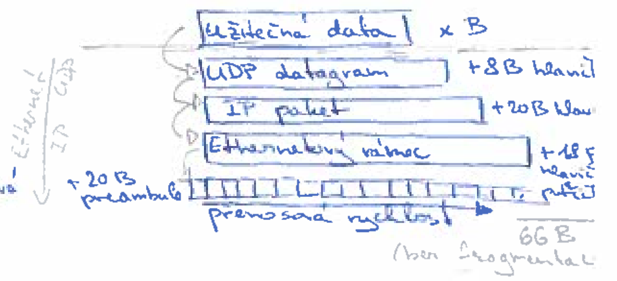
- VoIP (Voice over IP) = technologie pro přenos hlasu po IP

- Model klient/server = centralizovaný model
  peer-to-peer - symetrické řešení
  - každý uzel server (poskytuje své zdroje), klient (využívá cizí)



- šířka přenosového pásma = rozsah frekvencí, kt. lze využít pro přenos signálu [Hz]

- přenosová rychlost = #bitů / s
- přenosový výkon = efektivní přenosová rychlost
  tj. bez režijních dat (=> nižší než přenosová pokud se nepoužije komprese)

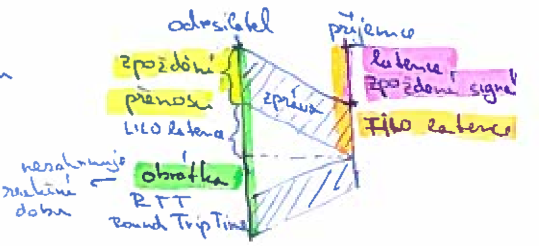


- Multiplex = více přenosů používá 1 cestu
- Demultiplex = opak

- modulace = vložení dat do posílané nosné (sinusovky), tj. změna signálu
  - amplitudová
  - frekvenční
  - fázová (posun) - nejlepší na detekci změn (ostré)

  $y = A \sin(\omega t + \varphi)$

  - modulační rychlost = # změn signálu za 1 s [Bd] BAUD
  - digitální modulace = vkládání digitálních dat



jitter - pravidelnost doručování

Best Effort — QoS
všem stejně — prioritní princip — garantované služby

8 DISKRÉTNÍ MODELY A STRUKTURY
(Teorie množin & Kombinatorika a grafy II)

KOMBAGRA II

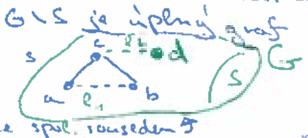
(Tutteova v.) - o perf. párování: Pro $\forall G=(V,E)$ platí: G má PP $\Leftrightarrow$ $\underbrace{\forall S\subseteq V \cdot odd(V\setminus S)\leq |S|}_{\text{Tutteova podm.}}$ # lichých komponent

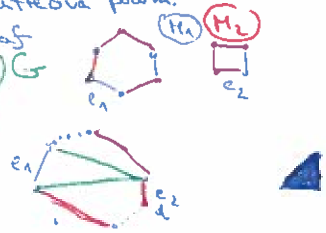
„$\Rightarrow$" obměna je snadným pozorováním

„$\Leftarrow$" indukcí přes # nehran ① každá komponenta $G\setminus S$ je úplný graf

pro víc jak ① nehran najdu PP ② jinak $\exists$ komponenta

Lemma: souv. ú̇plný G obsahuje 2 nesousedy se spol. sousedem

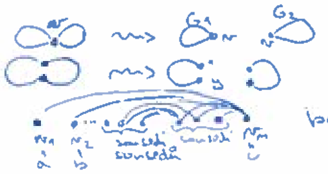




- Barvení grafů

(Brooks) Pro každý souvislý G, kt. není izomorfní liché kružnici, nebo K_n platí: $\chi(G) \leq \Delta(G)$ vrcholová barevnost

$\Delta(G)\leq 2$; $\Delta(G)>2$: má řez vel. 1; — // — 2; je vrcholově 3-souv.



barvím zleva a, b mají stejnou barvu

hranová barevnost

(Vizing) $\forall G: \chi_e(G) \leq \Delta(G)+1$

Vezmu největší podgraf G splňující větu (H má všech vrcholech, míň hran) $\chi_e(H)\leq\Delta(G)+1 \Rightarrow$ mám obarvenou

spor Pro $\forall$ vrchol mám nepoužitou barvu — nepoužitou hranu můžu obarvit posunutím barev po vějíři:
→ spor s maximalitou
najdu co nejdelší dvoubarevnou cestu, na ní prohodím barvy a dostanu první případ

- Extremální kombinatorika

(Ramseyova v. - pro grafy) Pro každé k, l existuje N takové, že kterýkoliv graf na N vrcholech obsahuje kliku velikosti k nebo nezávislou mn. velikosti l.
tj. když obarvím hrany K_N vždy najdu monochromatickou kliku dané velikosti

Def: Nejmenší takové N pro dané k, l se nazývá Ramseyovo číslo (zn. R(k,l)).

$$R(k,l)\leq\binom{k+l-2}{k-1}\leq 2^{k+l-2} \qquad R(k,k) \text{ roste exponenciálně.}$$

(Ramseyova vícebarevná) Pro každé k, t existuje N t.,že pro každou fci $c:\binom{[m]}{2}\to[t], m\geq N$ existuje mn. $A\in\binom{[m]}{k}$, pro niž fce c na $\binom{A}{2}$ je konstantní.

↳ tj. v grafu na m vrcholech lze najít kliku velikosti k indukovanou množinou A, hrany grafu barvím c pomocí t barev a klika je pak jednobarevná

k konečné se dělá přes nekonečnou

(Nekonečná Ramseyova) Pro $\forall$ každé t a každou fci $c:\binom{\mathbb{N}}{2}\to[t]$ existuje nekonečná mn. $A\subseteq\mathbb{N}$ pro niž je fce c na $\binom{A}{2}$ konstantní.

přes princip holubníku vyberu si mn. kde se opakuje nějaká barva nekonečněkrát $\triangle$

Do teď jsme barvily hrany, tj. dvojice, nyní to zobecníme na p-tice:

(Ramseyova pro p-tice) Pro $\forall p,t,k$ existuje N t.,že pro každou fci $c:\binom{[m]}{p}\to[t], m\geq N$ existuje mn. $A\in\binom{[m]}{k}$, pro níž je c na $\binom{A}{p}$ konstantní.

(Nekonečná R. pro p-tice) Pro $\forall p,t,k$ existuje N t.,že pro každou fci $c:\binom{\mathbb{N}}{p}\to[t]$ existuje mn. $A\subseteq\mathbb{N}$, pro niž je c na $\binom{A}{p}$ konstantní.

(Erdős-Ko-Rado) $\forall k,m\in\mathbb{N}, m\geq 2k$. Maximální velikost množinového systému k-tic na m-prvkové mn. je rovna $\binom{m-1}{k-1}$. $M=\{M_1,M_2,\dots,M_t\}$, $M_i\subseteq\binom{[m]}{k}$, v němž se každé 2 k-tice protínají

$f(k,m):=\max|M|=\binom{m-1}{k-1}$

$\triangledown$ $M=\{M_i\in\binom{[m]}{k}, 1\in M_i\}$ má velikost $\binom{m-1}{k-1}$ a každé 2 M_i se protínají.

maximální $|M|\leq\binom{m-1}{k-1} \Leftrightarrow \frac{|M|}{|\binom{[m]}{k}|}\leq\frac{\binom{m-1}{k}}{\binom{m}{k}}=\frac{k}{m}$

M obsahuje nejvýš k cyklických intervalů → Def je to mn. tvaru $\{j,j+1,\dots,j+k-1\}$ čítání je modulo m ⇒ $\exists$ m cyklických intervalů

$\mathcal{D}=\{(\pi,M_i), \pi$ je permutace, $M_i\in M$, π zobrazí M_i na nějaký cyklický interval$\}$

Počítání 2 zp. 1. $|\mathcal{D}|\leq m!\cdot k$
2. $|\mathcal{D}|=|M|\cdot m\cdot k!(m-k)!$ $\Big\}$ $|M|\cdot m\cdot k!(m-k)!\leq m!\,k$

$\Rightarrow |M|\leq\binom{m-1}{k-1}$ $\triangle$

TAHÁK

Zobrazení { • surjekce = na
bijekce { • injekce = prosté

Implikace

A	B	A ⇒ B
1	1	1
1	0	0
0	1	1
0	0	1

negace $A \wedge \neg B$

obměna $\neg B \Rightarrow \neg A$

$A \to B \iff \neg A \vee B$

Asociativita – uzávorkování $x+(y+z)=(x+y)+z$

Komutativita $x+y=y+x$

Distributivita – roznásobování $(x+y)\cdot z = x\cdot z + y\cdot z$

Relace
- reflexivita aRa
- silná antisymetrie $aRb \Rightarrow \neg(bRa)$
- slabá antisymetrie $(aRb \wedge bRa) \Rightarrow a=b$

Δ-nerovnost $|a+b| \le |a| + |b|$

Relace • ekvivalence • reflexivní, • symetrická • tranzitivní
• uspořádání • reflexivní • tranzitivní • slabě antisym.

$\pi = 3{,}14\ldots$

$e = 2{,}71\ldots$

$(a\mp b)^2 = a^2 \mp 2ab + b^2$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$(a^2 - b^2) = (a-b)(a+b)$

$(a^3 \pm b^3) = (a\pm b)(a^2 \mp ab + b^2)$

$0^n = 0$ $\quad (-\infty)\cdot(+\infty) = -\infty$

$(\text{cokoli})^0 = 1$

$\forall a \in \mathbb{R}: -\infty < a < \infty$

$\forall a \in \mathbb{R}^*$ $a \neq -\infty$: $a + (\infty) = \infty + a = \infty$

$\forall a \in \mathbb{R}^*$ $a \neq \infty$: $a + (-\infty) = (-\infty) + a = -\infty$

$\forall a \in \mathbb{R}^*$ $a > 0$: $a(\pm\infty) = (\pm\infty)\cdot a = \pm\infty$

< 0: $a(\pm\infty) = (\pm\infty)\cdot a = \mp\infty$

$\forall a \in \mathbb{R}: \dfrac{a}{\pm\infty} = 0$

neurčité výrazy: $\infty - \infty$, $-\infty + \infty$, $0\cdot(\pm\infty)$, $(\pm\infty)\cdot 0$, $\dfrac{\pm\infty}{\pm\infty}$

pro $a \in \mathbb{R}^*$ $\dfrac{a}{0}$ spec. i $\dfrac{0}{0}$

geom. řada $-1 < q < 1$ $\sum_{n=0}^{\infty} \dfrac{1}{1-q}$

Derivace	Integrály
$(c)' = 0$	$\int 1\,dx = x + c$ $\quad \int 0\,dx = c$ $\quad (-\infty,\infty)$
$(x^n)' = n\cdot x^{n-1}$	$\int x^n dx = \frac{x^{n+1}}{n+1} + c$ $\quad n \neq -1$ na $(0,\infty)$ (resp. na $\mathbb{R}$ / $\mathbb{R}\setminus\{0\}$)
$(a^x)' = a^x \ln a$	$\int a^x dx = \frac{a^x}{\ln a} + c$ $\quad a>0$ na $(-\infty,\infty)$
$(e^x)' = e^x$	$\int e^x dx = e^x + c$ $\quad$ na $(-\infty,\infty)$
$(\log_a x)' = \frac{1}{x \ln a}$	
$(\ln x)' = \frac{1}{x}$	$\int \frac{1}{x} dx = \ln\lvert x\rvert + c$ $\quad (-\infty,0)\cup(0,\infty)$
$(\sin x)' = \cos x$	$\int \sin x\, dx = -\cos x + c$ $\quad$ na $\mathbb{R}$
$(\cos x)' = -\sin x$	$\int \cos x\, dx = \sin x + c$ $\quad$ na $\mathbb{R}$
$(\mathrm{tg}\, x)' = \frac{1}{\cos^2 x}$	$\int \frac{1}{\cos^2 x} dx = \mathrm{tg}\, x + c$ $\quad k\in\mathbb{Z}$ $(-\frac{\pi}{2}+k\pi, \frac{\pi}{2}+k\pi)$
$(\mathrm{cotg}\, x)' = -\frac{1}{\sin^2 x}$	$\int \frac{1}{\sin^2 x} dx = -\mathrm{cotg}\, x + c$ $\quad (k\pi, \pi + k\pi)$
$(\arcsin x)' = \frac{1}{\sqrt{1-x^2}}$	$\int \frac{1}{\sqrt{A^2 - x^2}} dx = \arcsin\frac{x}{A} + c$
$(\arccos x)' = -\frac{1}{\sqrt{1-x^2}}$	$\int \frac{1}{\sqrt{x^2 \pm B}} dx = \ln\lvert x + \sqrt{x^2 \pm B}\rvert + c$
$(\mathrm{arctg}\, x)' = \frac{1}{1+x^2}$	$\int \frac{1}{A^2 + x^2} dx = \frac{1}{A}\mathrm{arctg}\frac{x}{A} + c$ $\quad \mathbb{R}$
$(\mathrm{arccotg}\, x)' = -\frac{1}{1+x^2}$	$\int \frac{1}{A^2 - x^2} dx = \frac{1}{2A}\ln\left\lvert\frac{A+x}{A-x}\right\rvert + c$

Pravidla: $f, g: \mathbb{R} \to \mathbb{R}$, $c \in \mathbb{R}$

$(f(x) \pm g(x))' = f'(x) \pm g'(x)$

$(c\cdot f(x))' = c\cdot f'(x)$

$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

$\left(\dfrac{f(x)}{g(x)}\right)' = \dfrac{f'(x)g(x) - f(x)g'(x)}{g^2(x)}$

$(f(g(x)))' = f'(g(x))\cdot g'(x)$

Integrační pravidla:

Per partes $\int f(x)g'(x)\,dx = f(x)g(x) - \int f'(x)g(x)\,dx$

integrál	f	g'
$\int P(x)e^{ax}dx$	$P(x)$	e^{ax}
$\int P(x)\sin(ax)dx$	$P(x)$	$\sin ax$
$\int P(x)\cos(ax)dx$	$P(x)$	$\cos ax$

} použijeme tolikrát, co je st. polynomu

$\int e^{ax}\sin(bx)dx$, $\int e^{ax}\cos(bx)dx$ } opakujeme 2x; 1. volba lib., 2. stejná jak 1. ⇒ rce s neznámou integrál

$\int P(x)\ln x\,dx$ $\quad \ln x$ $\quad P(x)$

Substituční metoda $[F(\varphi(x))]' = F'(\varphi(x))\cdot\varphi'(x) = f(\varphi(x))\cdot\varphi'(x)$

1. $\int f(\varphi(x))\cdot\varphi'(x)\,dx = F(\varphi(x)) + c$
2. $\int f(x)\,dx = \int f(\varphi(t))\cdot\varphi'(t)\,dt$

typ $\int \dfrac{f'(x)}{f(x)}dx = \left| \begin{matrix} t = f(x) \\ dt = f'(x)\,dx \end{matrix} \right| = \int \dfrac{dt}{t} = \ln\lvert t\rvert + c = \ln\lvert f(x)\rvert + c$

Rozklad na parc. zlomky – integrace $\dfrac{P(x)}{Q(x)}$
- s $\mathbb{R}$ kořeny
- s $\mathbb{C}$ kořeny

Newtonův integrál

$\int_a^b f(x)\,dx = [F(x)]_a^b = F(b) - F(a)$

$P(A|B) = \dfrac{P(A\cap B)}{P(B)}$

nezáv. jevy: $P(A\cap B) = P(A)\cdot P(B)$

$ax^2 + bx + c = 0$

$x_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

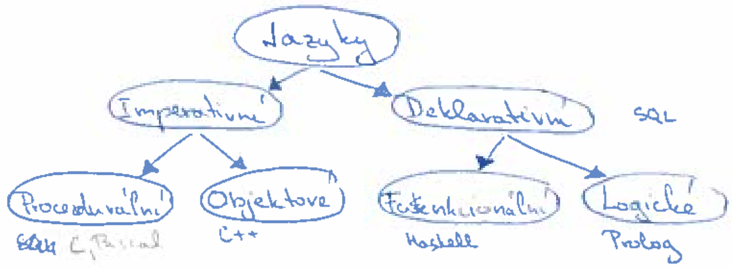
$(x-2)(x+3) = x^2 + 1x - 6$

$G=(V,E)$ $|V|=n$ $E \subseteq \binom{\{1,\dots,n\}}{2}$

- # G na n vrcholech $2^{\binom{n}{2}}$ ← max # hran
  ← každá tam je / není
- # neizomorfních G na n vrcholech $\geq \frac{2^{\binom{n}{2}}}{n!}$ ← počet bijekcí na G

Sled – opakuje vrcholy
Tah – neopakuje hrany
Cesta – neopakuje (ani) vrcholy
$K_{m,n}$ – úplný bipartitní graf 
Skóre grafu = posloupnost stupňů vrcholů, vzestupná

PARADIGMATA PROGRAMOVACÍCH JAZYKŮ



Imperativní = procedurální = krok za krokem popisuje co má počítač dělat
„jak se to dělá"
C, Pascal, Java, PHP, Rust

Deklarativní = popis toho co se má udělat (ne jak) - to řeší interpret)
„co se dělá"
SQL, Prolog, Scheme

imperativní → strukturované - dělení programu na dílčí úlohy, funkce či procedury, řídící struktury cykly apod.
→ nestrukturované (BASIC, COBOL, FORTRAN) - návěští a skoky

Objektově orientované = struktura objektů s metodami

- objekty = entity seskupující data a další prvky
- abstrakce = objekty jsou takové černé skříňky, není ~~[illegible]~~
- zapouzdření = nelze šahat na cizí vnitřnosti, přístup pouze přes rozhraní
- kompozice = objekt může obsahovat jiné objekty
- delegování = objekt může ~~využít~~ požádat o provedení operace nějaký jiný objekt
- dědičnost =
- polymorfismus = metody se chovají různě podle toho jaké třídy je objekt instancí (tj. stejné rozhraní pro různé objekty)

Program je parciálně korektní pokud pro ∀ vstup pro kt. skončí dá správný výsledek.