1 Základy

Axiom je výchozí tvrzení dané teorie, které se nedokazuje, jejich platnost se předpokládá.

Důsledek je tvrzení odvozené dedukcí z axiomů.

Bezespornost – vyvozené důsledky nesmějí obsahovat dané tvrzení a zároveň jeho negaci.

Symboly tvoří abecedu teorií, spojením vznikají slova – **formule**

2 Výroková logika

Prvotní formule $p, q, \ldots$ jsou jednoduché výroky, které dále neanalyzujeme. Složitější výroky konstruujeme pomocí spojek $\neg$, $\&$, $\vee$, $\rightarrow$, $\equiv$ a závorek.

Výrokové formule jsou všechny prvotní formule a všechny formule vzniklé aplikací spojek a závorek.

Pravdivostní ohodnocení formulí je zobrazení do množiny $\{0, 1\}$, kde 1 znamená pravdivé ohodnocení.

Tautologie jsou formule, které jsou pravdivé při libovolném ohodnocení, píšeme $\models$, např.:

- **zákon vyloučení třetího:** $A \vee \neg A$
- **zákon dvojí negace:** $\neg\neg A \equiv A$
- **vyloučení sporu:** $\neg(A \& \neg A)$

Logicky ekvivalentní formule mají stejné pravdivostní ohodnocení při libovolném ohodnocení jejich částí.

3 Formální axiomatický systém logiky Hilbertova typu

Abeceda obsahuje množinu prvotních formulí P, závorky a spojky $\neg$ a $\rightarrow$.

Axiomy: $A \rightarrow (B \rightarrow A)$, $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$, $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$

Odvozovací pravidlo modus ponens: z formulí A,$A \rightarrow B$ (*předpoklady*) se odvodí formule B (*závěr*).

Důkaz je libovolná konečná posloupnost formulí $A_1 \ldots A_n$ takových, že A_i je buď axiom nebo důsledek MP (předpoklady jsou v posloupnosti před A_i).

A **je dokazatelná**, pokud existuje důkaz, jehož poslední formulí je A, píšeme $\vdash A$. A je pak *tautologií.*

Dedukce: T je množina formulí. $T \vdash A \rightarrow B$ ($A \rightarrow B$ je dokazatelná pomocí T), právě když $T \cup \{A\} \vdash B$, píšeme $T, A \vdash B$.

Neutrální formule neovlivňuje důkaz, tedy $T, A \vdash B$ a také $T, \neg A \vdash B$. Pak platí $T \vdash B$.

Postova věta o úplnosti: Dokazatelné formule jsou tautologiemi ($\vdash A \Leftrightarrow \models A$).

4 Predikátová logika

Proměnné označují libovolný prvek z daného oboru objektů.

Konstanty označují jediný objekt (většinou něčím význačný).

Funkční symboly označují operace nad objekty. Mají *aritu* (četnost) – celé číslo, počet argumentů (konstanta je nulární funkce).

Termy jsou tvrzení sestavená pomocí proměnných a funkčních symbolů.

Predikátové symboly označují vlastnosti objektů (predikáty) a vztahy mezi nimi (je menší než, rovná se, . . .), také maji aritu.

Atomické formule jsou tvrzení sestavená pomocí termů a predikátovýh symbolů.

Logické spojky a pomocné symboly jsou definovány stejně jako ve výrokové logice.

Kvantifikátory označují platnost pro *všechny* objekty oboru, popř. *existenci* požadovaného objektu (v dalším textu označuje symbol Q predikáty $\forall$ nebo $\exists$).

Formule jsou trvzení sestavená pomocí atomických formulí, logických spojek a kvantifikátorů.

Predikátová logika 1. řádu umožňuje kvantifikovat pouze proměnné pro individua, ne množiny nebo relace ($\forall_{n=0}^{\infty} x$).

Vázaný výskyt proměnné x ve formuli φ znamená, že proměnná x se nachází v podformuli φ tvaru $\forall x\varphi$ nebo $\exists x\varphi$. Pak se φ nazývá *obor kvantifikátoru*, jinak je proměnná x *volnou proměnnou.*

Uzavřená formule = výrok, neobsahuje žádnou volnou proměnnou.

5 Sémantika predikátové logiky

Realizací jazyka L je algebraická struktura $\mathcal{M}$, složená z:

- univerzum M – neprázdná množina objektů
- funkční zobrazení $f_{\mathcal{M}}: M^n \to M$ pro každý funkční symbol
- predikátová relace $p_{\mathcal{M}} \subseteq M^n$

Ohodnocení proměnných je libovolné zobrazení e všech proměnných do M.

Formule φ **je splněna v realizaci** $\mathcal{M}$, pokud je pravdivá při každém ohodnocení e. Píšeme $\mathcal{M} \models \varphi$ Je-li φ uzavřená, pak říkáme, že φ je pravdivá v $\mathcal{M}$.

Formule φ **je logicky platná**, pokud pro každou realizaci $\mathcal{M}$ platí $M \models \varphi$.

Formule φ **a** ψ **jsou logicky ekvivalentní**, pokud při libovolné realizaci $\mathcal{M}$ a libovolném ohodnocení e je $\mathcal{M} \models \varphi[e]$ právě když $\mathcal{M} \models \psi[e]$.

Každá formule φ je ekvivalentní nějaké formuli ψ, ve které se nevyskytuje jeden kvantifikátor, popř. takové, ve které se vyskytují pouze spojky $\neg$ a $\to$ a kvantifikátor $\forall$.

Substituce termů za proměnné: Pokud v termu t dosadíme za proměnné další termy, t zůstává termem. Dosazením termů za proměnné ve formuli vytvoří opět formuli. Ne vždy je to vhodné, proměnná musí být *substituovatelná*.

Substituovatelná proměnná x je taková, že žádný její volný výskyt neleží v oboru kvantifikátoru proměnné y, která je obsažená v substituovaném termu. Např. $S(y)$ není substituovatelný za x ve formuli $x \to \exists y(x = S(y))$.

6 Axiomy predikátové logiky

Axiomy lze definovat pouze za použití spojek $\neg$ a $\to$ a kvantifikátoru $\forall$. $\exists x\varphi$ znamená $\neg(\forall x(\neg\varphi))$.

Výrokové axiomy: $\varphi \to (\psi \to \varphi)$, $(\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta))$, $((\neg\psi) \to (\neg\varphi)) \to (\varphi \to \psi)$

Axiom kvantifikátoru: $(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x\psi))$, x *nemá* volný výskyt v φ.

Axiom substituce: $(\forall x\varphi) \to \varphi_x[t]$, kde t je term substituovatelný za x

Axiomy rovnosti: $x_1 = y_1 \to (x_2 = y_2 \to (\ldots(x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))\ldots))$, obdobně pro predikáty.

Pravidlo odloučení (MP): z formulí $\varphi, \varphi \to \psi$ lze odvodit ψ

Pravidlo zobecnění: pro libovolnou proměnnou x z φ lze odvodit $\forall x(\varphi)$

Dedukce: pokud $T \vdash \varphi \to \psi$, pak také $T, \varphi \vdash \psi$.

7 Věta o úplnosti, kompaktnosti

Teorie T je libovolná množina formulí daného jazyka L a má svou realizaci $\mathcal{M}$.

$\mathcal{M}$ **je modelem teorie** T, pokud $\mathcal{M} \models \varphi$ pro každou $\varphi \in T$. Pak píšeme $\mathcal{M} \models T$.

φ **je důsledkem teorie** T, pokud pro každý model $\mathcal{M}$ je $\mathcal{M} \models \varphi$. Pak píšeme $T \models \varphi$.

Má-li teorie nějaký model, pak je *bezesporná*.

Teorie T **je úplná**, pokud je bezesporná a pro každou uzavřenou formuli platí buď $T \models \varphi$ nebo $T \models \neg\varphi$.

Věta o kompaktnosti: Nechť T je množina formulí jazyka L. Pak teorie T má nějaký model právě když každá její konečná podmnožina $Q \subseteq T$ má model.

8 Normální tvar formulí

Pořadí kvantifikátorů neovlivňuje význam formule.

$\vdash \varphi$, právě když $\vdash \forall x_1 \ldots \forall x_n \varphi$, kde $x_1, \ldots, x_n$ jsou všechny volné proměnné ve formuli φ.

Nahrazením podformulí ve formuli φ za ekvivalentní formule vytvoříme formuli ψ, která je ekvivalentní s formulí φ.

Pokud x není volná ve φ a $\circ$ je některá z binárních spojek, pak platí:

- $\vdash \forall x(\varphi \circ \psi) \Leftrightarrow (\varphi \circ \forall x\psi)$
- $\vdash \exists x(\varphi \circ \psi) \Leftrightarrow (\varphi \circ \exists x\psi)$
- $\vdash \forall x(\psi \rightarrow \varphi) \Leftrightarrow (\exists x\psi \rightarrow \varphi)$
- $\vdash \exists x(\psi \rightarrow \varphi) \Leftrightarrow (\forall x\psi \rightarrow \varphi)$

Varianta formule φ, φ' vznikne postupným nahrazením podformulí $Qx\psi$ podformulemi $Qy\psi_x[y]$, kde y se nevyskytuje v ψ. φ a φ' jsou *ekvivalentní*.

9 Prenexní tvar formulí

Prenexní forma formule: $Q_1x_1 \dots Q_nx_n\varphi$, kde φ neobsahuje kvantifikátory a $x_1, \dots, x_n$ jsou rozdílné proměnné.

Ke *každé* formuli lze sestrojit ekvivalentní formuli v prenexním tvaru:

1. Vyloučení zbytečných kvantifikátorů – vypuštění $Qx\varphi$, pokud x není ve φ volná.
2. Přejmenování proměnných – pokud pro proměnnou x existuje více kvantifikátorů Qx, nahradíme od duplicity dále proměnnou za x', která se liší od všech ostatních proměnných ve formuli.
3. Eliminace spojky $\Leftrightarrow$ – $\varphi \Leftrightarrow \psi$ je ekvivalentní s $(\varphi \rightarrow \psi)\&(\psi \rightarrow \varphi)$.
4. Přesun negace dovnitř – $\neg(\neg\varphi) \dots \varphi$, $\neg(\varphi\&\psi) \dots \neg\varphi \vee \neg\psi$, $\neg(\varphi \vee \psi) \dots \neg\varphi\&\neg\psi$, $\neg(Qx\varphi) \dots \bar{Q}x(\neg\varphi)$
5. Přesun kvantifikátorů doleva – pro ψ, ve kterých se nevyskytuje x provádíme převody:
   - $(Qx\varphi) \vee \psi$ na $Qx(\varphi \vee \psi)$ nebo $(Qx\varphi)\&\psi$ na $Qx(\varphi\&\psi)$
   - $(Qx\varphi) \rightarrow \psi$ na $\bar{Q}x(\varphi \rightarrow \psi)$
   - $\psi \rightarrow (Qx\varphi)$ na $Qx(\psi \rightarrow \varphi)$

   Někdy je možné použít substituci a kvantifikátor vynechat:

   - $(\exists x\varphi) \vee (\exists y\psi)$ na $\exists x(\varphi \vee \psi_y[x])$
   - $(\forall x\varphi)\&(\forall y\psi)$ na $\exists x(\varphi\&\psi_y[x])$

10 Univerzální algebry

Operace je zobrazení ω na množině A daná předpisem $\omega: A^n \rightarrow A$, kde n je četnost (arita) operace. Zapisujeme $\omega x_1, \dots, x_n$. Pro binární operace píšeme $x_1\omega x_2$ a pro nulární (konstanty) ω.

Příklady operací: $-$ je unární operace na $\mathbb{C}$, $+$ je binární operace $\mathbb{R}$, apod.

Parciální operace je operace daná předpisem $\omega: D \rightarrow A$, kde $D \subset A^n$, např. $-$ na $\mathbb{N}$, / na $\mathbb{Z}$, apod.

Univerzální algebra je dvojice $\mathfrak{A} = (A, \Omega)$, kde A je *nosná množina* a Ω je *soubor operací*.

Příklady algeber: $(\mathbb{Z}, +, -, 0)$ je algebra typu $(2, 1, 0)$

Neutrální prvek e vzhledem k binární operaci $\circ$ je prvek, který je *pravým* i *levým neutrálním prvkem*. Existuje nejvýše jeden.

Levý neutrální prvek – $\forall x \in A: e \circ x = x$

Pravý neutrální prvek – $\forall x \in A: x \circ e = x$

Zákony jsou rovnice tvaru $t_1(\vec{x}) = t_2(\vec{x})$ s vhodnými termy t_1,t_2 a musejí být splněny pro všechny prvky nosné množiny ($\forall x \in A : e \circ x = x$).

V případě multiplikativního značení se používá termín *jednotkový prvek* a v případě aditivního, *nulový prvek*.

Inverzní prvek x^{-1} vzhledem k binární operaci $\circ$ je prvek, který je levým i pravým inverzním prvkem.

Levý inverzní prvek – $\forall x \in A :\ x^{-1} \circ x = e$

Pravý inverzní prvek – $\forall x \in A :\ x \circ x^{-1} = e$

Inverzibilní prvek je prvek s inverzním prvkem.

Asociativní operace je binární operace, kde platí $\forall x, y, z \in A :\ (x \circ y) \circ z = x \circ (y \circ z)$ (asociativní zákon).

Pro asociativní binární operace je pravý a levý inverzní prvek totožný. Pro aditivní operace je častější zápis $-x$.

Komutativní operace je binární operace, kde platí $\forall x, y \in A :\ x \circ y = y \circ x$ (komutativní zákon)

$\cdot$ **je distributivní operace** nad $+$, pokud $\cdot$ a $+$ jsou binární a platí $\forall x, y, z \in A :\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (levý distributivní zákon) a $\forall x, y, z \in A :\ (y + z) \cdot x = (y \cdot x) + (z \cdot x)$ (pravý distributivní zákon).

11 Klasifikace algeber

Grupoid je algebra $(A, \cdot)$ typu (2), operace musí být *uzavřena* na nosné množině.

Pologrupa je grupoid s *asociativní* operací $\cdot$.

Monoid je pologrupa s *neutrálním prvkem* $e \ldots (A, \cdot, e)$.

Grupa je monoid se všemi prvky *invertibilními* $\ldots (A, \cdot, e, ^{-1})$.

Komutativní (abelovská) grupa je grupa jejíž operace $\cdot$ je komutativní.

Okruh je algebra $(A, +, 0, -, \cdot)$ typu $(2, 0, 1, 2)$, pokud $(A, +, 0, -)$ je abelovská grupa, $(A, \cdot)$ je pologrupa a $\cdot$ je distributivní nad $+$.

Komutativní okruh je okruh, jehož operace $\cdot$ je komutativní.

Okruh s jednotkovým prvkem k operaci $\cdot$ značíme $(A, +, 0, -, \cdot, 1)$.

Obor integrity je komutativní okruh s jednotkovým prvkem, kde platí, že $0 \neq 1$ a neexistují dělitelné nuly ($x \neq 0 \land y \neq 0 \rightarrow xy \neq 0$).

Těleso je okruh s jednotkovým prvkem, kde platí, že $0 \neq 1$ a $(A - \{0\}, \cdot)$ je grupa.

Pole je komutativní těleso.

Svaz je algebra $(A, \cap, \cup)$ typu $(2, 2)$, kde platí, že $\cap$ i $\cup$ jsou komutativní a asociativní a platí absorbční zákony $X \cap (X \cup Y) = X$, $X \cup (X \cap Y) = X$.

Distributivní svaz je svaz, ve kterém platí distributivní zákony.

Ohraničený svaz je algebra $(A, \cap, \cup, 0, 1)$ typu $(2, 2, 0, 0)$, kde $(A, \cap, \cup)$ je svaz, 0 je nulový a 1 je jednotkový prvek svazu.

Komplementární svaz je ohraničený svaz, kde platí $\forall a \in A\ \exists a' \in A:\ a \cap a' = 0 \wedge a \cup a' = 1$.

Booleův svaz je distributivní a komplementární svaz.

Booleova algebra je algebra $(A, \cap, \cup, 0, 1,')$ typu $(2, 2, 0, 0, 1)$, kde $(A, \cap, \cup, 0, 1)$ je Booleův svaz.

12 Vlastnosti grup

Řád prvku $a \in A$, kde A je nosná množina grupy, je kardinální číslo
$o(a) = |\{a^0, a^1, a^{-1}, \ldots\}| = |\{a^k | k \in \mathbb{Z}\}|$ pak $o(a) \in \mathbb{N}$ nebo $o(a) = |\mathbb{Z}| = |\mathbb{N}| = \aleph_0$

Řád grupy $|G| \geq o(a)$ pro všechny prvky $a \in A$.

13 Podalgebry

Uzavřená množina – T je uzavřená vzhledem k operaci ω na nosné množině $A^n \to A$, pokud $\omega(T^n) \subseteq T$.

Podalgebra – (T, Ω) je podalgebrou (A, Ω), pokud je T uzavřena vzhledem ke všem operacím z Ω (a $T \subseteq A$).

Průnik podalgeber dané algebry A je také podalgebra algebry A.

Podalgebra generovaná množinou – Mějme algebru (A, Ω). Množina $S \subseteq A$ je *množina generátorů*. Algebra $\langle S \rangle = \bigcap\{T \mid S \subseteq T, T\ \textit{je podalgebra}\ (A, \Omega)\}$ je *nejmenší podalgebrou, která S obsahuje* (podalgebra generovaná množinou S).

Podgrupa generovaná prvkem – Buď $(A, \cdot, e,^{-1})$ grupa, $x \in A$, $S = \{x\}$. Pak
$\langle x \rangle = \langle S \rangle = \{x^k \mid k \in \mathbb{Z}\}$ je podgrupa grupy A generovaná prvkem x.

Pro abelovské grupy platí $\langle \{x_1, \ldots, x_n\} \rangle = \{x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \mid k_i \in \mathbb{Z}\}$ popř. $\langle \{x_1, \ldots, x_n\} \rangle = \{k_1 x_1 + \ldots + k_n x_n \mid k_i \in \mathbb{Z}\}$

Cyklická grupa je grupa, kde platí $\exists x \in A:\ \langle x \rangle = A$. Prvek x se pak nazývá *generátor*.

1. $o(x) = \infty$, pak A je také nekonečná, $A = \{e, x, x^{-1}, x^2, x^{-2}, \ldots\}$. Např.: $(\mathbb{Z}, +, 0, -)$, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$
2. $o(x) = n \in \mathbb{N}$, pak $|A| = n$ a $A = \{e, x, x^2, \ldots, x^{n-1}\}$. Např: $(\mathbb{Z}_m, +, 0, -)$, $\mathbb{Z}_m = \langle 1 \rangle = \langle k \rangle$, kde $NSD(m, k) = 1$

14 Relace ekvivalence a rozklad na třídy ekvivalence

Relace R na množině M je podmnožina kartézského součinu – binární relace $R \subseteq M \times M$. U binárních relací místo $(x, y) \in R$ píšeme xRy.

Univerzální relace: $\alpha_M = M \times M$.

Identická relace: $\imath_M = \{(x, x) \mid x \in M\}$ (relace rovnosti).

Reflexivní relace: $\forall x \in M:\ xRx$

Symetrická relace: $\forall x, y \in M:\ xRy \Rightarrow yRx$

Antisymterická relace: $\forall x, y \in M:\ xRy \wedge yRx \Rightarrow x = y$

Tranzitivní relace: $\forall x, y, z \in M: \; xRy \wedge yRz \Rightarrow xRz$

Relace ekvivalence je reflexivní, symetrická a tranzitivní.

Relace částečného uspořádání je reflexivní, antisymetrická a tranzitivní.

Rozklad M na třídy ekvivalence je množina $\mathcal{P} \subseteq 2^M$, pro níž platí: $\emptyset \notin \mathcal{P}$, $\bigcup \mathcal{P} = M$ a množiny v $\mathcal{P}$ jsou po dvou rozdílné.

Třída ekvivalence prvku $a \in M$ je definována jako $[a]_\pi = \{b \in M \mid b\pi a\}$, kde π je relace ekvivalence na M.

Faktorová množina množiny M podle π je definována jako $M/\pi = \{[a]_\pi \mid a \in M\}$. ($M/\pi$ je rozklad na třídy ekvivalence)

15 Homomorfismy

Mějme algebry $\mathfrak{A} = (A, \Omega)$ a $\mathfrak{A}^* = (A^*, \Omega^*)$ téhož typu. Zobrazení $f: \; A \rightarrow A^*$ se nazývá *homomorfismus* algebry $\mathfrak{A}$ do algebry $\mathfrak{A}^*$, pokud $\forall \omega \in \Omega$ a $\forall \omega^* \in \Omega^*$ platí: $\forall x_1, \dots, x_n \in A: \; f(\omega x_1 \dots x_n) = \omega^* f(x_1) \dots f(x_n)$

Typy homomorfismu:

- *epimorfismus* – f je surjektivní (pokrývá cílovou množinu)
- *monomorfismus* – f je injektivní (mapuje jeden prvek pouze na jeden prvek)
- *izomorfismus* – f je bijektivní (injektivní i surjektivní)
- *endomorfismus* – $\mathfrak{A} = \mathfrak{A}^*$
- *automorfismus* – izomorfní a endomorfní zároveň

16 Relace kongruence a faktorové algebry

Relace kongruence je relace π na algebře $\mathfrak{A} = (A, \Omega)$ taková, že pro všechny operace $\omega \in \Omega$ platí: $\forall a_1, \dots, a_n, b_1, \dots, b_n$: $a_1 \pi b_1 \wedge \dots \wedge a_n \pi b_n \Rightarrow \omega a_1 \dots a_n \pi \omega b_1 \dots b_n$.

Faktorová algebra algebry $\mathfrak{A}$ podle kongruence π – $\mathfrak{A}/\pi = (A/\pi, \Omega^*)$ Často klademe $\Omega = \Omega^*$.

Příklad: $\mathfrak{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$, $\pi: \; a\pi b \Leftrightarrow \exists c: \; a - b = cn$, tedy $a \equiv b$ mod n pro dané $n \in \mathbb{N}$.
Při $n = 5$ pak např. $1\pi 6$.
Faktorová algebra $\mathfrak{A}/\pi = (\mathbb{Z}_n, +^*, 0^*, -^*, \cdot^*, 1^*)$. Nové operace definujeme pomocí reprezentantů tříd: $[a] +^* [b] = [a + b]$ atd. Symboly * se většinou vynechávají.

17 Přímé součiny algeber

Mějme soubor algeber $\mathfrak{A}_k = (A_k, \Omega_k)$. Množina A je kartézským součinem množin A_k a operace $\omega \in \Omega$ je definována jako $\omega a_{k_1} \dots a_{k_n} = (\omega_1 a_{k_1} \dots a_{k_n}, \dots, \omega_n a_{k_1} \dots a_{k_n})$. Pak *přímý součin* algeber $\mathfrak{A}_k$ značíme $\Pi \mathfrak{A}_k = (A, \Omega)$.

Příklad: $\mathfrak{A}_1 = (A_1, \cdot, e, ^{-1})$, $\mathfrak{A}_2 = (A_2, +, 0, -)$, pak $\mathfrak{A}_1 \times \mathfrak{A}_2 = (A_1 \times A_2, \circ, (e, 0), ')$.
Operace $\circ: \; (a_1, b_1) \circ (a_2, b_2) = (a_1 \cdot a_2, b_1 + b_2)$. Operace $': \; (a, b)' = (a^{-1}, -b)$.

Přímé součiny pologrup (grup, vektorových prostorů, okruhů, Booleových algeber) jsou opět pologrupy (grupy, vektorové prostory, okruhy, Booleovy algebry).

18 Metrické prostory

Metrický prostor $\mathcal{X} = (X, \varrho)$ je libovolná množina X (jejíž prvky značíme *body*), ve které je dána tzv. *vzdálenost*.

Vzdálenost je jednoznačná nezáporná reálná funkce $\varrho(x, y)$, která je definována pro $\forall x, y \in X$ a která splňuje:

1. $\varrho(x, y) = 0 \Leftrightarrow x = y$
2. $\forall x, y: \ \varrho(x, y) = \varrho(y, x)$ (symetrie)
3. $\forall x, y, z: \ \varrho(x, y) + \varrho(y, z) \geq \varrho(x, z)$ (trojúhelníková nerovnost)

Příklady metrických prostorů:

Prostor izolovaných bodů – $\varrho(x, y) = 0$, pokud $x = y$ nebo 1 jinak.
Metrický prostor R^1 – $\varrho(x, y) = |x - y|$.
Metrický prostor R^n – $\varrho(x, y) = \sqrt{\sum\limits_{k=1}^{n} (y_k - x_k)^2}$ (euklidovský prostor).

Otevřená koule $S(x_0, r)$ v metrickém prostoru $\mathcal{X}$ je množina bodů $x \in \mathcal{X}$, pro které platí $\varrho(x, x_0) < r$. Pevný bod x_0 se nazývá *střed* a r *poloměr* koule.

Uzavřená koule je definována analogicky, pouze $\varrho(x, x_0) \leq r$.

ε**-okolí** bodu x_0 je otevřená koule $O_\varepsilon(x_0) = S(x_0, \varepsilon)$, kde ε uvažujeme jako nekonečně malé číslo.

Bod uzávěru množiny M je takový bod x, jehož ε-okolí obsahuje alespoň jeden bod z množiny M. Množina všech bodů uzávěru se nazývá *uzávěr množiny* (značíme $\overline{M}$). Platí, že $M \subseteq \overline{M}$.

Uzavřená množina je taková, že platí $M = \overline{M}$. Analogicky pro otevřenou množinu.

Vnitřní bod množiny je takový bod, jehož ε-okolí je celé obsaženo v dané množině. Množina s pouze vniřními body je *otevřená*.

Vztahy: $\overline{\overline{M}} = \overline{M}$, $M_1 \subseteq M \Rightarrow \overline{M_1} \subseteq \overline{M}$, $\overline{M \cup N} = \overline{M} \cup \overline{N}$.

Hromadný bod množiny M je takový bod, jehož okolí obsahuje nekonečně mnoho bodů z M. Hromadný bod může a nemusí náležet M.

Izolovaný bod $x \in M$ množiny M, pokud jeho okolí neobsahuje body z M, kromě x.

Každý bod uzávěru je buď hromadný nebo izolovaný.

Limita posloupnosti $x_1, \ldots, x_n$ je takové číslo x, pro jehož jakékoli okolí $O_\varepsilon(x) \mid \varepsilon > 0$ lze nalézt takové číslo m, že všechny body $x_m, \ldots, x_n \in O_\varepsilon(x)$. Posloupnost tedy *konverguje* k x.

Množina A je **hustá** v B, pokud $B \subseteq \overline{A}$. A je **všude hustá**, pokud $\overline{A} = \mathcal{X}$.

Separabilní metrický prostor obsahuje všude hustou spočetnou množinu.

Spojité zobrazení je takové zobrazení $f: \ \mathcal{X} = (X, \varrho) \to \mathcal{Y} = (Y, \varrho^*)$, které je spojité ve všech bodech.

Zobrazení spojité v bodě $x_0 \in \mathcal{X}$ je takové, že k libovolnému $\varepsilon > 0$ lze najít $\delta > 0$ tak, aby platilo $\forall x$: $\varrho^*(f(x), f(x_0)) < \varepsilon \Rightarrow \varrho(x, x_0) < \delta$

Zobrazení na: každý bod z Y má alespoň jeden vzor v X

Homeomorfní prostory jsou takové, že mezi nimi existuje *homeomorfní zobrazení*, tedy vzájemně jednoznačné a vzájemně spojité.

Izometrické prostory jsou takové, že mezi nimi existuje *izometrické zobrazení*, tedy platí $\varrho(x_1, x_2) = \varrho^*(f(x_1), f(x_2))$.

Úplný metrický prostor je takový, že libovolná v něm obsažená cauchyovská posloupnost konverguje.

Cauchyovská posloupnost je taková, že pro libovolné ε lze nalézt takové číslo $N(\varepsilon)$, že platí $\varrho(x_m, x_n) < \varepsilon \ \forall x_m, x_n \geq N(\varepsilon)$ (každá konvergentní posloupnost je také cauchyovská).

19 Normované prostory

Dále uváděný termín "těleso" znamená těleso reálných nebo komplexních čísel.

Lineární (vektorový) prostor $\mathcal{L}$ je taková množina, že platí:

1. $(\mathcal{L}, +, \theta, -)$ je komutativní grupa
2. Ke každému číslu α nějakého tělesa T a každému prvku $x \in \mathcal{L}$ je jednoznačně přiřazen prvek $\alpha x \in \mathcal{L}$ tak, že platí: $\alpha(\beta x) = (\alpha\beta)x$ a $1 \cdot x = x$, kde $1 \in T$.
3. Výše uvedené násobení prvku číslem je distributivní nad operací $+$.

Normovaný lineární prostor je takový lineární prostor, ve kterém existuje *norma*.

Norma je reálné nezáporné číslo $||x||$, které je přiřazeno každému prvku x, kde platí:

1. $||x|| = 0 \Leftrightarrow x = \theta$
2. $||\alpha x|| = |\alpha| \cdot ||x||$
3. $||x + y|| \leq ||x|| + ||y||$

Každý lineární normovaný prostor je metrickým prostorem (stačí položit $\varrho(x, y) = ||x - y||$).

Banachův prostor (B-prostor) je *úplný* lineární normovaný prostor.

Příklady normovaných prostorů:

Číselné těleso s normou absolutní hodnota ($\mathbb{R}^1$ – reálná osa)
Množina všech uspořádancýh n-tic čísel (n-rozměrný prostor)
Množina všech spojitých reálných funkcí na intervalu $\langle a, b\rangle$

20 Unitární prostory

Unitární prostor je takový lineární prostor, v němž je definován *skalární součin.*

Skalární součin je reálná funkce v reálném lineárním prostoru $\mathcal{R}$, kde $\lambda \in \mathbb{R}$ a platí:

1. $(x, y) = (y, x)$
2. $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$
3. $(\lambda x, y) = \lambda(x, y)$
4. $(x, x) \geq 0$, $(x, x) = 0 \Leftrightarrow x = \theta$

Norma v unitárním prostoru: $||x|| = \sqrt{(x, x)}$

Příklady unitárních prostorů:

Konečně rozměrný prostor $\mathbb{R}^2$, jehož prvky jsou všechny n-tice reálných čísel $x = (x_1, \ldots, x_n)$ s obvyklými operacemi sčítání a násobení n-tic a skalárním součinem $(x, y) = \sum_{i=1}^{n} x_i y_i$

21 Obyčejné grafy

Obyčejný graf je dvojice $G = (U, H)$, kde U je konečná množina uzlů (vrcholů) a $H = \{\{u, v\} \mid u, v \in U \wedge u \neq v\}$ je konečná množina hran. Hrana $\{u, v\}$ je *incidentní* s uzly u a v.

Orientovaný graf je dvojice $G = (U, H)$, kde $H = \{(u, v) \mid u, v \in U\}$ je konečná množina orientovaných hran.

Obecný graf je trojice $G = (U, H, \epsilon)$, kde ϵ je zobrazení, které přiřazuje každé hraně dvojici různých uzlů: $\epsilon : H \rightarrow \{\{u, v\} \mid u, v \in U \wedge u \neq v\}$. Mezi dvěma uzly může být více hran.

Sled mezi uzly u, v o délce n je posloupnost $(u = w_0, h_1, w_1, h_2, \ldots, w_{n-1}, h_n, w_n = v)$, kde $w_k \in U$, $h_k \in H$ a $h_i = \{w_{i-1}, w_i\}$, popř. (w_{i-1}, w_1) pro orientovaný graf.

Sled mezi uzly u a v o délce n je posloupnost, ve které se střídají uzly a hrany, začínající uzlem u, končící uzlem v a mající n hran. Sousední uzly v posloupnosti jsou spojeny mezi nimi ležící hranou.

Ve sledu se mohou opakovat jak uzly tak i hrany.

Tah mezi uzly u a v o délce n je sled $(u = w_0, h_1, w_1, h_2, \ldots, w_{n-1}, h_n, w_n = v)$ takový, že platí $i \neq j \Rightarrow h_i \neq h_j$.

V tahu se mohou opakovat uzly, ale všechny hrany jsou různé.

Cesta mezi uzly u a v o délce n je sled $(u = w_0, h_1, w_1, h_2, \ldots, w_{n-1}, h_n, w_n = v)$ takový, že platí $i \neq j \Rightarrow w_i \neq w_h \wedge h_i \neq h_j$.

Cesta obsahuje všechny uzly a hrany maximálně jednou.

Kružnice v grafu G o délce n je sled $(w_0, h_1, w_1, h_2, \ldots, w_{n-1}, h_n, w_n)$ takový, že platí $i \neq j \Rightarrow w_i \neq w_j \wedge w_0 = w_n$.

Kružnice obsahuje každou hranu maximálně jednou a všechny uzly až na první a poslední jsou různé.

Pokud graf obsahuje dvě kružice se společnou hranou, pak graf také obsahuje třetí kružnici, která vznikne spojením těchto dvou kružnic, ale neobsahuje společnou hranu.

Souvislý graf obsahuje pro libovolnou dvojici uzlů nějaký sled.

Podgraf grafu – Graf $G' = (U', H')$ je podgrafem grafu $G = (U, H)$, pokud $U' \subseteq U$ a $H' \subseteq H$.

Faktor grafu je takový podgraf, kde platí $(u, v \in U' \wedge \{u, v\} \in H) \Rightarrow \{u, v\} \in H'$.

Komponenta grafu – Graf $G' = (U', H')$ je komponentou grafu $G = (U, H)$, pokud G' je souvislým faktorem G a při odebrání uzlu již graf není souvislý.

Komponenta je uzlově maximální souvislý faktor grafu.

Most je hrana, jejíž odebráním zvýšíme počet komponent grafu.

Stupeň vrcholu je číslo $deg(u)$ definované jako počet hran incidentních s uzlem u.

Pro obyčejný graf platí: $\sum_{u \in U} deg(u) = 2m$, kde $m = |H|$

22 Stromy

Les je obyčejný graf, který neobsahuje kružnici.

Strom je obyčejný *souvislý* graf, který neobsahuje kružnici (souvislý les).

Pro les s alespoň jednou hranou platí: $\exists u, v \in U: \ deg(u) = deg(v) = 1$

Pro strom platí: $|H| = |U| - 1$, každá hrana je mostem, mezi každou dvojicí uzlů existuje jediná cesta, přidáním libovolné hrany vznikne kružnice.

23 Kostry

Kostra je takový podgraf grafu, že je stromem a obsahuje všechny uzly – $K = (U, H')$.

Obyčejný graf je souvislý právě když má kostru.

Tětiva kostry – Pokud $K = (U, H')$ je kostra grafu $G = (U, H)$, pak hrany z množiny $H - H'$ jsou tětivy kostry.

Základní kružnice kostry – Máme-li kostru K a tětivu $t = (u, v)$, pak v kostře existuje jediná cesta mezi u a v. Tato cesta spolu s tětivou t tvoří základní kružnici kostry vytvořenou tětivou t, značíme $C^K(t)$.

Rozpojující množina je podmnožina hran, jejíž odebráním se graf stane nesouvislým.

Řez grafu je minimální rozpojující množina grafu.

Každá hrana kostry je řezem. Odstraněním jakékoli hrany z kostry grafu vznikne nesouvislý graf o dvou podstromech.

24 Minimální kostra

Oceněný graf je trojice $G = (U, H, c)$, kde (U, H) je obyčejný graf a c je zobrazení $c: \ H \to \mathbb{R}$, které každé hraně přiřazuje cenu $c(h)$. $c(G)$ je cena grafu $c(G) = \sum\limits_{h \in H} c(h)$.

Minimální kostra je kostra K oceněného grafu G taková, že $c(K) \leq c(L)$ pro všechny kostry L grafu G.

Kruskalův algoritmus hledání minimální kostry oceněného grafu $G = (U, H, c)$:

1. Seřadíme hrany do posloupnosti $S = (h_1, \ldots, h_n)$ tak, že platí $c(h_i) \leq c(h_{i+1})$.
2. Odstraníme první hranu z S a vytvoříme pomocí této hrany kostru K_1.
3. Dokud jsou v S hrany, bereme nejnižší a pokud by přidáním do kostry vznikla kružnice, hranu přeskočíme. Jinak ji přidáme do kostry.

Primův algoritmus hledání minimální kostry:

1. Vybereme libovolný výchozí uzel.
2. Vybereme hranu s nejnižším hodnocením jdoucí z výchozího uzlu a sestrojíme kostru K_1.
3. Procházíme všechny uzly v kostře a přidáme vždy hranu s nejnižším hodnocením vycházející z některého z uzlů. Pokud by vznikla kružnice, hranu přeskočíme.

Maticová varianta Primova algoritmu:

1. Vyplníme matici tak, že na souřadnici i, j je cena hrany mezi uzly u_i a u_j.
2. Vyškrtneme první sloupec a první řádek vybereme.
3. Pokud ve vybraném řádku jsou všechny prvky již označeny, algoritmus končí a označené prvky matice označují hrany minimální kostry. Jinak vybereme nejmenší neoznačený prvek.
4. Vybraný prvek c_{ij} označíme a vybere se j-tý řádek. Neoznačené prvky j-tého sloupce se vymažou a pokračuje se krokem 3.

25 Orientované grafy

Orientovaný graf je trojice $G = (U, H, \epsilon)$, kde U je konečná množina uzlů (vrcholů), H je konečná množina orientovaných hran a ϵ je zobrazení $\epsilon :\ H \to \{(u, v) \mid u, v \in U\} \cup \{u \mid u \in U\}$ které každé hraně přiřadí dvojici uzlů nebo jeden uzel (vznikne smyčka).

Výstupní stupeň uzlu je počet hran, které z uzlu vystupují, $deg_-(u)$. Pokud $deg_-(u) = 0$, jedná se o tzv. *koncový uzel*.

Vstupní stupeň uzlu je počet hran, které do uzlu vstupují, $deg_+(u)$. Pokud $deg_+(u) = 0$, jedná se o tzv. *počáteční uzel*.

Orientovaný sled, tah, cesta a kružnice jsou definovány analogicky k obyčejným.

Symetrická orientace grafu je nahrazení hran v obyčejném grafu dvěma orientovanými hranami opačného směru. Vytvoří se tak jediný orientovaný graf.

Orientace grafu je nahrazení hran v obyčejném grafu jedinou orientovanou hranou. Na rozdíl od symetrické orientace je takto možno vytvořit více orientovaných grafů.

Symetrizace grafu je nahrazení všech hran spojujících dané dva uzly jedinou neorientovanou hranou. Vytvoří se tak jediný obyčejný graf.

Souvislost – Orientovaný graf je souvislý, pokud symetrizací vznikne souvislý obyčejný graf.

Silná souvislost – Orientovaný graf je silně souvislý, pokud pro libovolné dva uzly existuje orientovaná cesta.

Turnaj je orientovaný graf, kde kmezi každými dvěma různými uzly existuje právě jedna orientovaná hrana.

Eulerovský graf je orientovaný graf, kde existuje uzavřený *tah*, který obsahuje všechny jeho orientované hrany.

Souvislý orientovaný graf je Eulerovský, pokud platí: $\forall u \in U :\ deg_+(u) = deg_-(u)$

26 Délky hran a cest – orientované grafy

Délka hrany je reálné číslo $l(h)$ přiřazené ke každé hraně grafu.

Délka cesty je součet všech délek hran v dané cestě.

Minimální délka cesty je nejmenší možná délka cesty mezi uzly u a v, značíme $d(u, v)$, pokud cesta neexistuje, pak $d(u, v) = \infty$.

27 Dijkstrův algoritmus pro nalezení minimální cesty

Počáteční uzel s je uzel, od kterého se délky cesty počítají.

Horní odhad vzdálenosti z uzlu s do uzlu v je číslo $D(v) \geq d(s,v)$, které je horním uzávěrem všech délek možných cest.

Předchozí uzel $\pi(v)$ je uzel, který uzlu v bezprostředně předchází na aktuálně počítané cestě. Pro zatím neexistující cestu platí $\pi(v) = \emptyset$.

Následné uzly jsou množina uzlů $N(v) = \{w \in U \mid (v,w) \in H\}$, tedy uzlů, které jsou přímo spojeny hranou počínající v uzlu v.

Další pojmy: $p(s,v)$ – aktuální cesta, $d(s.v)$ – délka aktuální cesty, $S \subseteq U$ – množina uzlů, pro které již cesta je spočítána, $Q = U - S$.

Algoritmus:

1. Inicializace – $\forall u \in U: \ \pi(u) = \emptyset, D(s) = 0, D(u) = \infty, S = \emptyset$
2. Test konce – Pokud $S = U$, přechod na 5.
3. Nalezení uzlu s definitivní cestou – Z Q přesuneme do S uzel v s nejnižší hodnotou $D(v)$. Pokud pro všechny $u \in Q$ platí $D(u) = \infty$, přechod na 5.
4. Zlepšení horních odhadů – $\forall w \in N(v) \cap Q$ takový, že $D(w) > D(v) + l((v,w))$, položíme $D(w) = D(v) + l((v,w))$ a $\pi(w) = v$, přechod na 2.
5. Konstrukce výstupu – Do uzlů, které zůstaly ve Q žádná cesta z s neexistuje. Pro ostatní uzly položíme $d(s,v) = D(v)$ a cestu minimální délky sestrojíme obrácením cesty $v \to \pi(v) \to \pi(\pi(v)) \to \ldots \to s$.

Dijkstrův algoritmus nefunguje, pokud v grafu jsou hrany se zápornou délkou.

28 Floyd-Warshallův algoritmus pro nalezení minimální cesty

Tento algoritmus funguje i se zápornými hranami. Při nalezení kružnice záporné délky tuto odhalí (diagonální prvek matice bude záporný).

Vstup (délky hran) je zadán maticí A (sloupec a řádek označuje počáteční/koncový uzel hrany).

Dále máme matici posloupností P, na počátku obsahuje každý prvek pouze číslo svého sloupce.

Postupnými iteracemi (n iterací, kde $n = |U|$) se vypočítávají další kroky matic až se dojde do koncového tvaru a matice vzdáleností obsahuje minimální vzdálenosti.

V každé iteraci se prvky matic A^i přepočítají:

$a^j_{ik} = a^{j-1}_{ik}, p^j_{ik} = p^{j-1}_{ik}$ pokud $a^{j-1}_{ik} \leq a^{j-1}_{ij} + a^{j-1}_{jk}$
$a^j_{ik} = a^{j-1}_{ij} + a^{j-1}_{jk}, p^j_{ik} = p^{j-1}_{ij}$ pokud $a^{j-1}_{ik} > a^{j-1}_{ij} + a^{j-1}_{jk}$

Česky: Pro iteraci j sledujeme matici A^{j-1} a to *pouze* její j-tý řádek a j-tý sloupec (tedy takový kříž). Pro všechny prvky z A^{j-1} porovnáváme jejich hodnotu s *průmětem* na tento kříž (tedy se součtem s odpovídajícími prvky na stejném řádku a sloupci v kříži). Pokud je součet větší než hodnota prvku, opíšeme hodnoty obou matic. Pokud je součet menší, v matici A^j zapíšeme součet a v matici P^j zapíšeme hodnotu $j-1$.