KATEDRA INFORMATIKY
PŘÍRODOVĚDECKÁ FAKULTA
UNIVERZITA PALACKÉHO

DISKRÉTNÍ MATEMATIKA PRO INFORMATIKY II

RADIM BĚLOHLÁVEK, VILÉM VYCHODIL

VÝVOJ TOHOTO UČEBNÍHO TEXTU JE SPOLUFINANCOVÁN
EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY

Olomouc 2006

Abstrakt

Text je úvodem do vybraných partií diskrétní matematiky a souvisejících oblastí. Postupně seznamuje čtenáře s úvodem do logiky, množin, relací a funkcí, kombinatorikou, teorií grafů a vybranými pokročilejšími partiemi z teorie relací a logiky. Text je psán matematickým stylem, tj. nové pojmy jsou definovány, o definovaných pojmech jsou vyslovována tvrzení a ta jsou pak dokazována. Důraz je kladen na motivaci pro zavedení nových pojmů a jejich vysvětlení. Text předpokládá jen základní středoškolské znalosti matematiky.

Cílová skupina

Text je určen pro studenty oboru Aplikovaná informatika uskutečňovaného v kombinované formě na Přírodovědecké fakultě Univerzity Palackého v Olomouci. Může být užitečný i studentům jiných informatických a matematických oborů a těm, kteří se chtějí seznámit se se základy diskrétní matematiky.

Obsah

4 Grafy a stromy

Studijní cíle: Po prostudování kapitol 4.1, 4.2, 4.3 a 4.4 by student měl rozumět základním pojmům teorie grafů. Měl by dále znát základní tvrzení, která pro probírané pojmy platí. K vybraným úlohám teorie grafů by student měl znát algoritmy pro jejich řešení.

Klíčová slova: orientovaný graf, neorientovaný graf, vrchol, hrana, izomorfismus grafů, podgraf, sled,délka sledu, uzavřený sled, tah, cesta, kružnice, vzdálenost vrcholů, ohodnocený graf, souvislost, komponenta, hledání cest, stupeň vrcholu, skóre, eulerovský tah

Potřebný čas: 180 minut.

4.1 Co a k čemu jsou grafy

V životě se často setkáváme se situacemi, ve kterých jsou dána určitá místa a spojení mezi nimi. Některá místa jsou spojena s jinými, některá nejsou. Tak například místy mohou být křižovatky ve městě, spojeními pak ulice mezi jednotlivými křižovatkami. Někdy přitom na orientaci spojení nezáleží (tj. je jedno, jestli vede spojení z místa A do místa B nebo vede-li spojení z místa B do místa A), někdy na orientaci záleží (může se stát, že vede spojení z A do B ale neexistuje spojení z B do A). Např. v situaci s křižovatkami a ulicemi pro chodce na orientaci spojení nezáleží. Jsou-li totiž křižovatky A a B spojeny ulicí, která je lemována chodníkem, chodec o orientaci spojení neuvažuje, protože může jít z A do B i z B do A. Pro chodce je tedy důležité, že A a B jsou spojena. Na druhou stranu, pro řidiče na orientaci záleží. Místa A a B mohou být totiž spojena jednosměrkou a pak je důležité, jestli spojení vede z A do B nebo z B do A. Jiným příkladem podobné situace je každý náčrtek, kde jsou body spojené čarami (např. schema elektrického obvodu, vývojový diagram, schema hierarchické struktury ve firmě).

Uvedenými situacemi se zabývá tzv. teorie grafů. Místa se nazývají vrcholy, spojení pak hrany. Graf je dán množinou vrcholů a množinou hran mezi nimi. Nezáleží-li na orientaci hran, nazývá se graf neorientovaný, v opačném případě se nazývá orientovaný.

Grafy mají řadu zajímavých aplikací. Např. ve městě může být pekařská firma, která má každé ráno do prodejen pečiva rozvést zboží. Majiteli firmy přitom záleží na tom, aby se zbytečně neplýtvalo pohonnými hmotami, tj. aby byl při ranním rozvozu počet ujetých kilometrů co nejmenší. Z pohledu teorie grafů jde o úlohu najít cestu, která vychází z pekařství, prochází v libovolném pořadí všemi prodejnami pečiva a končí opět v pekařství. Přitom hledáme cestu, která je ze všech takových nejkratší. Podobný příklad: Cestující vlakem chce najít co nejrychlejší spojení ze jedné stanice do druhé. Může ji najít vyhledávacím programem na internetu. Samotný program vlastně hledá nejkratší cestu v grafu, který představuje železniční síť.

4.2 Neorientované a orientované grafy: základní pojmy

Definice 4.1 (neorientovaný a orientovaný graf). *Neorientovaný graf* je dvojice $G = \langle V, E\rangle$, kde V je neprázdná množina tzv. *vrcholů* (někdy také *uzlů*) a $E \subseteq \{\{u, v\} \mid u, v \in V,\ u \neq v\}$ je množina dvouprvkových množin vrcholů, tzv. *(neorientovaných) hran*.

Orientovaný graf je dvojice $G = \langle V, E\rangle$, kde V je neprázdná množina tzv. *vrcholů* (*uzlů*) a $E \subseteq V \times V$ je množina uspořádaných dvojic vrcholů, tzv. *(orientovaných) hran*.

Hrana se tedy u neorientovaných grafů chápe jako dvouprvková množina $\{u, v\}$ vrcholů $u, v \in V$. Pak říkáme, že hrana $\{u, v\}$ vede mezi u a v, popř. spojuje u a v. To odpovídá záměru: Graf je neorientovaný, tj. na pořadí vrcholů u hrany nezáleží. U orientovaných grafů se hrana chápe jako uspořádaná dvojice $\langle u, v\rangle$ vrcholů u a v. Pak říkáme, že hrana vede z u do v. I to odpovídá záměru: Graf je orientovaný, tj. na pořadí vrcholů u hrany záleží. Hrana $\langle u, v\rangle$ je tedy něco

Obrázek 4: Neorientovaný (vlevo) a orientovaný (vpravo) graf.

jiného než hrana $\langle v, u\rangle$. *Koncové vrcholy* hrany jsou u neorientované hrany $\{u, v\}$ vrcholy u a v, u orientované hrany $\langle u, v\rangle$ také vrcholy u a v.

Příklad 4.2. Uvažujme množinu vrcholů $V = \{u, v, w, x, y\}$. Uvažujme množinu neorientovaných hran $E_1 = \{\{u, v\}, \{u, w\}, \{u, x\}, \{v, w\}\}$. $G_1 = \langle V, E_1\rangle$ je neorientovaný graf a vidíme ho znázorněný na Obr. **??** vlevo. Uvažujme teď množinu orientovaných hran $E_2 = \{\langle u, v\rangle, \langle v, w\rangle, \langle w, u\rangle, \langle w, v\rangle, \langle x, u\rangle\}$. Pak $G_2 = \langle V, E_2\rangle$ je orientovaný graf a vidíme ho znázorněný na Obr. **??** vpravo.

Pro (neorientovaný nebo orientovaný) graf $G = \langle V, E\rangle$ se V a E nazývají množina vrcholů a množina hran grafu G a značí se $V(G)$ a $E(G)$. Bude-li z kontextu jasné, jde-li o graf orientovaný nebo neorientovaný, budeme psát jen "graf". Graf můžeme zadat přímo jeho obrázkem. Např. řekneme-li "uvažujme graf z Obr. 4 vlevo", lze z tohoto obrázku určit jak množinu V vrcholů, tak množinu E hran. Znázornění grafu obrázkem je přitom přehlednější než jeho popis jakožto struktury $G = \langle V, E\rangle$.

K orientovanému grafu je třeba někdy uvažovat graf, který vznikne zanedbáním orientace hran. Říká se mu symetrizace orientovaného grafu.

Definice 4.3 (symetrizace). *Symetrizace* orientovaného grafu $G = \langle V, E\rangle$ je neorientovaný graf $G' = \langle V, E'\rangle$, kde

$$\{u, v\} \in E' \quad \text{právě když} \quad \langle u, v\rangle \in E \text{ nebo } \langle v, u\rangle \in E.$$

Například na Obr. 4 je graf vlevo symetrizací grafu vpravo. Grafy, které se liší jen přejmenováním vrcholů, se nazývají izomorfní.

Definice 4.4 (izomorfní grafy). Neorientované grafy $G_1 = \langle V_1, E_1\rangle$ a $G_2 = \langle V_2, E_2\rangle$ se nazývají *izomorfní*, právě když existuje bijekce $h : V_1 \to V_2$ (říká se jí izomorfismus), pro kterou

$$\{u, v\} \in E_1 \quad \text{právě když} \quad \{h(u), h(v)\} \in E_2.$$

Orientované grafy $G_1 = \langle V_1, E_1\rangle$ a $G_2 = \langle V_2, E_2\rangle$ se nazývají *izomorfní*, právě když existuje bijekce $h : V_1 \to V_2$, pro kterou

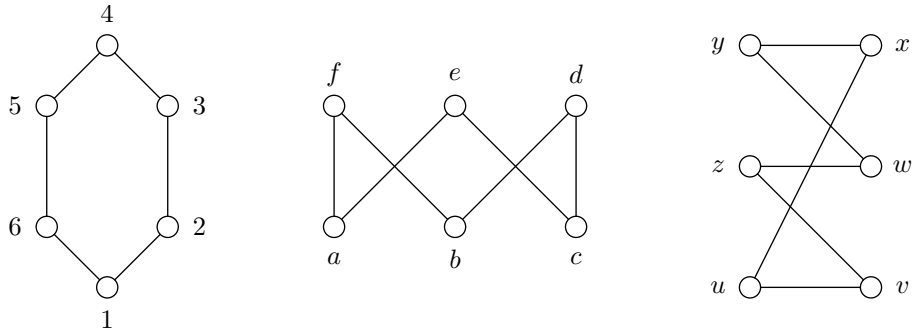
$$\langle u, v\rangle \in E_1 \quad \text{právě když} \quad \langle h(u), h(v)\rangle \in E_2.$$

Jsou-li G_1 a G_2 izomorfní, píšeme $G_1 \cong G_2$.

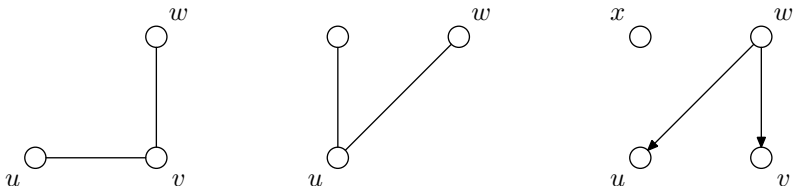
Příklad 4.5. Všechny grafy z Obr. 5 jsou po dvou izomorfní. Např. bijekce h, pro kterou $h(1) = a$, $h(2) = e$, $h(3) = c$, $h(4) = d$, $h(5) = b$, $h(6) = f$, je izomorfismus mezi prvním a druhým grafem.

Části grafů se nazývají podgrafy.

Definice 4.6 (podgrafy). (Orientovaný nebo neorientovaný) graf $\langle V_1, E_1\rangle$ je *podgrafem* grafu $\langle V_2, E_2\rangle$, právě když $V_1 \subseteq V_2$ a $E_1 \subseteq E_2$. Podgraf $\langle V_1, E_1\rangle$ grafu $\langle V_2, E_2\rangle$ se nazývá *indukovaný*, právě když E_1 obsahuje každou hranu z E_2, jejíž oba koncové vrcholy patří do V_1.



Obrázek 5: Izomorfní neorientované grafy.



Obrázek 6: Podgrafy.

Např. první dva grafy na Obr. 6 jsou podgrafy grafu z Obr. 4 vlevo, přitom první z nich není indukovaný (není v něm hrana $\{u, w\}$), druhý ano. Třetí graf na Obr. 6 je podgrafem grafu z Obr. 4 vpravo.

Důležitou oblastí je tzv. cestování v grafech. Je motivováno skutečným cestováním, představíme-li si vrcholy grafu jako místa a hrany jako spojnice, po kterých lze z míst do míst přecházet. Základním pojmem pro cestování v grafech je pojem cesty. Cesta odpovídá postupnému průchodu místy po existujících spojnicích. Přitom praktické úlohy vedou na různé doplňující požadavky, např. aby se při průchodu žádné místo nenavštívilo dvakrát, aby se po žádné spojnici nešlo dvakrát apod. Ukažme teď základní pojmy.

Definice 4.7 (cestování). *Sled* v (neorientovaném nebo orientovaném) grafu[5] $G = \langle V, E \rangle$ je posloupnost

$$v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n,$$

kde $v_i \in V$ jsou vrcholy, $e_j \in E$ jsou hrany a platí, že

- $e_i = \{v_{i-1}, v_i\}$ pro $i = 1, \ldots, n$, je-li G neorientovaný,
- $e_i = \langle v_{i-1}, v_i \rangle$ pro $i = 1, \ldots, n$, je-li G orientovaný.

Číslo n se nazývá *délka sledu*. Sled $v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$, se nazývá

- *uzavřený*, je-li $v_0 = v_1$,
- *tah*, neopakuje-li se v něm žádná hrana (tj. pro $i \neq j$ je $e_i \neq e_j$),
- *cesta*, neopakuje-li se v něm žádný vrchol (tj. pro $i \neq j$ je $v_i \neq v_j$),
- *kružnice*, je-li $v_0 = v_n$ a s výjimkou vrcholů v_0 a v_1 jsou každé dva vrcholy různé.

Vzdálenost z vrcholu u do vrcholu v je délka cesty z u do v, která má ze všech cest z u do v délku nejmenší.

[5] Názvosloví je tady nejednotné. Tedy to, co my budeme nazývat sled, tah a cesta, se v jiné literatuře může nazývat jinak.

Říkáme také, že sled $v_0, e_1, \ldots, v_n$ vede z v_0 do v_n. Z definice máme, že každý tah je sledem. Každá cesta je tahem, neboť neopakují-li se ve sledu vrcholy, nemohou se opakovat ani hrany. Kružnice nemůže být cestou, protože se v ní opakují vrcholy (první a poslední).

Uvažujme graf na Obr. 4 vlevo. $u, \{u,w\}, w, \{w,v\}, v, \{v,u\}, u, \{u,w\}, w$ je sled, který není tahem (a tedy ani cestou), protože se v něm opakuje hrana $\{u,w\}$. $u, \{u,w\}, w, \{w,v\}, v, \{v,u\}, u, \{u,x\}, x$ je tah, který není cestou, protože se v něm opakuje vrchol u. Sled $x, \{x,u\}, u, \{u,w\}, w, \{w,v\}, v, \{v,u\}, u, \{u,x\}, x$ je sice uzavřený, ale není to kružnice, protože se v něm opakuje vrchol u. Sled $u, \{u,w\}, w, \{w,v\}, v, \{v,u\}, u$, je kružnice.

Existují tedy sledy, které nejsou cestami. Následující věta ukazuje, že pokud nám jde o dosažitelnost z vrcholu do vrcholu, vystačíme s cestami.

Věta 4.8. *Existuje-li v grafu sled z vrcholu u do vrcholu v, existuje také cesta z u do v.*

Důkaz. Důkaz je jednoduchý. Opakuje-li se ve sledu $u, \ldots, v$ nějaký vrchol w, tj. má-li sled tvar $u, \ldots, w, \ldots, w, \ldots v$, vynecháme posloupnost $w, \ldots,$. Dostaneme $u, \ldots, w, \ldots v$, což je také sled z u do v. Pokud je už cestou, jsme hotovi. Pokud ne, opět vynecháme podúsek mezi opakujícími se vrcholy. Protože je sled konečný, po konečném počtu kroků takto skončíme u cesty z u do v. □

Jaký význam mají pojmy z Definice 4.7? Sled odpovídá putování bez omezení: Vyjdeme z nějakého místa, po libovolné hraně z něho přejdeme do jiného místa, atd., až dojdeme do koncového místa. Najít vhodný tah se bude snažit např. poštovní doručovatelka. Kdyby šla po hraně (tj. po ulici) vícekrát, zbytečně se nachodí. Hledáním vhodných cest se zabývají např. ve spedičních firmách při rozvozu zboží: Projet vrcholem (místem, kde se vyloží část zboží) vícekrát je příznakem nehospodárného naplánování rozvozu.

Ulice, kterou v grafu reprezentujeme hranou, má ve skutečnosti nějakou délku, popř. propustnost. Stejně tak sklad, reprezentovaný v grafu pomocí vrcholu, může mít určitou kapacitu. V grafech se takovým doplňujícím informacím říká ohodnocení.

Definice 4.9 (ohodnocení). *Hranové ohodnocení* grafu $\langle V, E\rangle$ s množinou hodnot D je funkce $w : E \to D$. *Vrcholové ohodnocení* grafu $\langle V, E\rangle$ s množinou hodnot D je funkce $w : V \to D$.

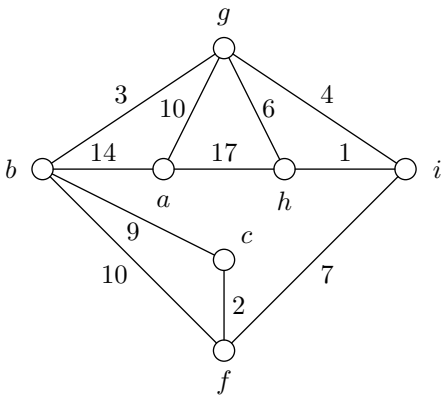
Je-li jasné, o jaké ohodnocení jde, říkáme jen ohodnocení. Grafu spolu s ohodnocením(i) říkáme také hranově, popř. vrcholově ohodnocený graf, popř. jen ohodnocený graf. Množinou hodnot D je většinou nějaká množina čísel (to budeme automaticky předpokládat). Hodnota $w(e) \in D$ přiřazená funkcí w hraně $e \in E$ představuje např. délku hrany (vzdálenost mezi místy), její kapacitu (propustnost informačního nebo dopravního spojení) apod. Hodnota $w(u) \in D$ přiřazená funkcí w vrcholu $u \in V$ představuje např. propustnost uzlu, do kterého něco přichází a něco odchází, apod. Množina hodnot D může obsahovat libovolné prvky, např. názvy ulic nebo datové struktury obsahující strukturovanou informaci o dané hraně či vrcholu.

Příklad 4.10. Na Obr. 7 je ohodnocený (hranově i vrcholově) graf. Hranové ohodnocení w_E je dáno předpisem $w_E(\{a,b\}) = 14, w_E(\{a,g\}) = 10, \ldots, w_E(\{h,i\}) = 1$. Vrcholové ohodnocení w_V je dáno předpisem $w_V(a) = 17, \ldots, w_V(i) = 3$.

Představuje-li hranové ohodnocení délky jednotlivých hran, je přirozené zavést pojem délky sledu, který zohledňuje toto ohodnocení. *Délka sledu $v_0, e_1, \ldots, e_n, v_n$ v hranově ohodnoceném grafu* je číslo

$$w(e_1) + \cdots + w(e_n),$$

je to tedy součet délek všech hran, které se ve sledu vyskytují. Např. délka sledu $b, \{b,f\}, f, \{f,i\}, i, \{i,h\}, h$ v grafu na Obr. 7 je 18. Podobně jako v neohodnoceném grafu definujeme vzdálenost z u do v jako délku nejkratší cesty (délka se uvažuje vzhledem k ohodnocení). Uvědomte si, že přiřazuje-li hranové ohodnocení w každé hraně číslo 1, je délka sledu v takto ohodnoceném grafu rovna délce sledu v neohodnoceném grafu (viz Definice 4.7).



Obrázek 7: Hranově a vrcholově ohodnocený graf.

Následující pojmy zavedeme pro neorientované grafy. Pro orientované najdete návod v úkolech k textu.

Definice 4.11 (souvislost a komponenty). Neorientovaný graf $G = \langle V, E\rangle$ se nazývá *souvislý*, právě když pro každé dva vrcholy $u, v \in V$ existuje sled z u do v. *Komponenta* neorientovaného grafu je každý jeho maximální souvislý podgraf.

Komponenta grafu $G = \langle V, E\rangle$ je tedy podgraf indukovaný množinou vrcholů $V' \subseteq V$ takovou, že každé dva vrcholy z V' lze spojit tahem a že k V' není možné přidat další vrchol, aby to stále platilo. Např. graf na Obr. 4 není souvislý (vrcholy x a y nejsou spojeny sledem). Jeho podgraf indukovaný vrcholy u, v a w je souvislý, ale není to komponenta, protože není maximální souvislý. Komponenty v tomto grafu jsou dvě. První je podgraf indukovaný vrcholy u, v, w, x, druhá je podgraf indukovaný vrcholem y. I obecně platí, že komponenty tvoří „rozklad grafu".

Komponenty tvoří rozklad grafu.

Věta 4.12. *Nechť $G_1 = \langle V_1, E_1\rangle, \ldots, G_n = \langle V_n, E_n\rangle$ jsou všechny komponenty grafu $G = \langle V, E\rangle$. Pak každý vrchol $v \in V$ patří právě do jedné V_i a každá hrana $e \in E$ patří právě do jedné E_i.*

Důkaz. Vezměme vrchol $v \in V$. Podgraf indukovaný $\{v\}$ je zřejmě souvislý. Proto je podgrafem nějakého maximálního souvislého podgrafu grafu G, tj. komponenty G_i. Proto $v \in V_i$, tj. v patří aspoň do jedné z množin $V_1, \ldots, V_n$. Ukažme, že v nemůže patřit do dvou různých $V_i \neq V_j$. Kdyby $v \in V_i \cap V_j$, pak uvažujme nějaký $v_i \in V_i - V_j$ (takový existuje, protože G_i a G_j jsou komponenty, a tedy $V_i \not\subseteq V_j$ a $V_j \not\subseteq V_i$). Protože G_i je souvislý, existuje sled $v_i, e_1, u_1, \ldots, v$. Uvažujme množinu vrcholů V', která vznikne z V_j přidáním všech vrcholů sledu $v_i, e_1, u_1, \ldots, v$. Pak $V_j \subseteq V'$ a podgraf indukovaný množinou V' je souvislý (vezmeme-li $v_1, v_2 \in V'$, pak existuje sled z v_1 do v i sled z v do v_2 a složením těchto sledů dostaneme sled z v_1 do v_2). Tedy G_j by nebyl maximální souvislý podgraf, tj. nebyl by komponetou, což je spor s předpokladem.

Že každá hrana $e \in E$ patří právě do jedné E_i dostaneme podobnou úvahou, když si uvědomíme, že pro $e = \{u, v\}$ je podgraf indukovaný množinou vrcholů $\{u, v\}$ je souvislý. □

4.3 Hledání cest

Předpokládejme, že máme síť měst se známými vzdálenostmi mezi sousedními měst (tj. některé dvojice měst jsou spojeny silnicemi a my známe délky těchto spojujících silnic). Zajímá nás, jak se co nejkratším způsobem dostat z města A do města B (tj. tak, abychom ujeli co nejméně kilometrů). Jak to zjistit?

Z hlediska teorie grafů jde o problém hledání nejkratší cesty. Představme si následující neorientovaný graf. Ke každému městu bude v grafu existovat vrchol (pro různá města různé vrcholy).

Jsou-li města spojena silnicí, bude mezi jim odpovídajícími vrcholy v grafu hrana. Tento graf hranově ohodnotíme tak, že hodnota hrany bude rovna délce jí odpovídající silnice. Otázka, jak se co nejkratším způsobem dostat z A do B, pak skutečně znamená najít nejkratší cestu (ve smyslu teorie grafů) která vede z uzlu odpovídajícího městu A do uzlu odpovídajícího B.

V následujícím uvedeme jeden z nejznáměnších algoritmů hledání nejkratší cesty, tzv. Dijkstrův[6] algoritmus.

Algoritmus pracuje následovně. Na vstupu je neorientovaný graf $G = \langle V, E\rangle$, jeho hranové ohodnocení $w : E \to \mathbb{R}^+$ (každé hraně je přiřazeno kladné reálné číslo), a vrchol $s \in V$. Výstupem algoritmu je pro každý vrchol $v \in V$ číslo $d(v)$, které je vzdáleností z s do v. Algoritmus používá proměnné A, N, d, m, přitom hodnotami A, N jsou množiny vrcholů, hodnotou d je funkce přiřazující vrcholům kladná reálná čísla, hodnotou m je nezáporné reálné číslo. V každém kroku algoritmu je pro vrchol $v \in V$ hodnota $d(v)$ rovna délce nejkratší zatím nalezené vzdálenosti z s do v. Na začátku se nastaví $d(s) = 0$ a $d(v) = \infty$ pro ostatní vrcholy $v \neq s$. V průběhu výpočtu je $d(v)$ délka nejkratší zatím nalezené cesty z s do v. Množina se na začátku nastaví na $A = V$. Během výpočtu obsahuje A vrcholy v, pro něž zatím nebyla stanovena definitivní $d(v)$ (tj. $d(v)$ byla stanovena, ale v dalším výpočtu se ještě může změnit). Algoritmus je iterační, opakuje následující krok: Z množiny A vyjme všechny vrcholy v, pro které je $d(v)$ nejmenší, tj. v se přesune z A do N, právě když

$$d(v) = \min\{d(u) \mid u \in A\}.$$

Každý vrchol v z N je kandidátem na to, že přes něj vede do nějakého vrcholu w z A, který s ním sousedí, kratší cesta než byla dosud nalezena. Algoritmus tedy pro každý $v \in N$ a pro každý $u \in A$, pro který $\{v, u\} \in E$ (v a u sousedí), porovná $d(v) + w(\{v, u\})$ (délka možné cesty z s do u, která vede přes v) a $d(u)$ (délka dosud nejkratší nalezené cesty z s do u). Je-li $d(v) + w(\{v, u\}) < d(u)$ (tj. cesta přes v je kratší), změní se hodnota $d(u)$ na $d(u) := d(v) + w(\{v, u\})$. Tento krok se opakuje, dokud není $d(v) = \infty$ pro každý $v \in A$ (této podmínce vyhovuje i stav $A = \emptyset$). Vrcholy, které po skončení výpočtu zůstaly v A, jsou právě ty, do kterých nevede z s cesta.

Poznamenejme, že pro praktickou implementaci volíme místo ∞ nějakou velkou hodnotu, které nemůže být jinak dosaženo, např. součet délek všech hran zvětšený o 1. Následuje stručný popis algoritmu.

Algoritmus 4.13 (nalezení nejkratších cest z daného vrcholu).
Vstup: graf $G = \langle V, E\rangle$, hranové ohodnocení $w : E \to \mathbb{R}^+$, vrchol $s \in S$
Výstup: hodnota $d(v)$ pro každý $v \in V$, $d(v)$ je délka nejkratší cesty z s do v
Proměnné: funkce $d : V \to \mathbb{R}^+$, číslo $m \in \mathbb{R}^+$, množiny $A, N \subseteq V$

1. $A := V$; $d(s) := 0$; pro $v \in V - \{s\}$: $d(v) := \infty$;
2. pokud neexistuje $v \in A$ takový, že $d(v) \neq \infty$, skonči.
3. $m := \min\{d(v) \mid v \in A\}$; $N := \{v \in A \mid d(v) = m\}$; $A := A - N$;
4. pro všechny $v \in N$, $u \in A$ takové, že $\{v, e\} \in E$: jestliže $d(v) + e(\{v, u\}) < d(u)$, pak $d(u) := d(v) + e(\{v, u\})$; pokračuj krokem 2.

Ukažme si činnost algoritmu na jednoduchém příkladě. Uvažujme graf na Obr. 7. Nechť je dále $s = h$. Kroku 1: Nastaví se $A := \{a, b, c, f, g, h, i\}$, $d(a) = \infty$, $d(b) = \infty$, $d(c) = \infty$, $d(f) = \infty$, $d(g) = \infty$, $d(h) = 0$, $d(i) = \infty$. Krok 2: Pokračuje se dál (protože podmínka ukončení není splněna). Krok 3: Nastaví se $m := 0$, $N = \{h\}$, $A := \{a, b, c, f, g, i\}$. Krok 4: Upraví se $d(a) = d(h) + d(\{h, a\}) = 0 + 17 = 17$, $d(g) = d(h) + d(\{h, g\}) = 0 + 6 = 6$,

[6] Edsger W. Dijkstra [dajkstra] (1930–).

$d(i) = d(h) + d(\{h, i\}) = 0 + 1 = 1$, tedy pro $v \in A$ je $d(a) = 17$, $d(b) = \infty$, $d(c) = \infty$, $d(f) = \infty$, $d(g) = 6$, $d(i) = 1$. Krok 2: Pokračuje se dál. Krok 3: Nastaví se $m := 1$, $N = \{i\}$, $A := \{a, b, c, f, g\}$. Krok 4: Upraví se $d(f) = d(i) + d(\{i, f\}) = 1 + 7 = 8$, $d(g) = d(i) + d(\{i, g\}) = 1 + 4 = 5$, tedy pro $v \in A$ je $d(a) = 17$, $d(b) = \infty$, $d(c) = \infty$, $d(f) = 8$, $d(g) = 5$. Krok 2: Pokračuje se dál. Krok 3: Nastaví se $m := 5$, $N = \{g\}$, $A := \{a, b, c, f\}$. Krok 4: Upraví se $d(a) = 15$, $d(b) = 8$, tedy pro $v \in A$ je $d(a) = 15$, $d(b) = 8$, $d(c) = \infty$, $d(f) = 8$. Krok 2: Pokračuje se dál. Krok 3: Nastaví se $m := 8$, $N = \{b, f\}$, $A := \{a, c\}$. Krok 4: Upraví se $d(c) = 17$, tedy pro $v \in A$ je $d(a) = 15$, $d(c) = 17$. Krok 2: Pokračuje se dál. Krok 3: Nastaví se $m := 15$, $N = \{a\}$, $A := \{c\}$. Krok 4: d se neupravuje, tedy pro $v \in A$ je $d(c) = 17$. Krok 2: Pokračuje se dál. Krok 3: Nastaví se $m := 17$, $N = \{c\}$, $A := \emptyset$. Krok 4: d se neupravuje. Krok 2: Výpočet se ukončí. Vzdálenosti $d(v)$ z h do v jsou tedy $d(a) = 15$, $d(b) = 8$, $d(c) = 17$, $d(f) = 8$, $d(g) = 5$, $d(h) = 0$, $d(i) = 1$.

K navrženému algoritmu musíme provést důkaz jeho správnosti.

Ručním ověřením zjistíme, že vypočítané vzdálenosti jsou správné. Musí tomu tak být vždy? Tedy, je algoritmus správný v tom smyslu, že pro každý ohodnocený graf a jeho vrchol s budou po skončení výpočtu $d(v)$ délky nejkratších cest z s do v? To je zásadní otázka pro každý navržený algoritmus (ať řeší cokoli). Měli bychom tedy provést důkaz jeho správnosti.

Průvodce studiem

Ke každému navrženému algoritmu je třeba provést důkaz jeho správnosti. Nestačí zjistit, že algoritmus pracuje správně na několika příkladech. Na jiných by mohl dávat nesprávné výsledky. Důkaz správnosti je ověření, že pro jakékoli přípustné hodnoty vstupů algoritmus vypočítá správné výstupy.

Například Algoritmus 4.13 vychází z intuice, že hledáme-li nejkratší cestu lokálně, tj. z navštíveného vrcholu se snažíme jít do nejbližšího vrcholu, najdeme cestu, která je nejlepší i globálně. To ovšem není zřejmé a je třeba to ověřit. K tomu slouží důkaz správnosti.

Pro $u, v \in V$ označme $\delta(u, v)$ délku nejkratší cesty z u do v. Předpokládejme, že $d(v)$ jsou hodnoty vypočítané algoritmem pro daný graf $\langle V, E\rangle$, ohodnocení w a vrchol s. Máme dokázat, že pro každý vrchol $v \in V$ je $d(v) = \delta(s, v)$. Dokážeme $d(v) \leq \delta(s, v)$ a $\delta(s, v) \leq d(v)$. Při tom budeme dokazovat indukcí podle počtu průchodů „cyklu“ sestávajícího z kroků 2., 3., 4. Tím se rozumí následující: Výpočet probíhá tak, že je proveden krok 1., pak pak se buď skončí, nebo se provedou kroky 2., 3., 4. (první průchod cyklem), pak pak se buď skončí, nebo se provedou kroky 2., 3., 4. (druhý průchod cyklem), atd. Provede-li se cyklus celkem n-krát, můžeme mluvit o 1., 2., . . . , n-tém průchodu a o hodnotách proměnných v těchto průchodech. Hodnoty proměnných po i-tém průchodu cyklu 2., 3., 4. budeme značit d_i, m_i, A_i a N_i (tj. např. $A_i = N_i - A_{i-1}$ apod.).

Nejdříve dokážeme

$$\delta(s, v) \leq d(v). \tag{4.1}$$

Protože $d(v) = d_j(v)$ pro nějaké j, stačí dokázat $\delta(s, v) \leq d_i(v)$. To dokážeme indukcí podle i. Pro $i = 0$ (tj. před prvním průchodem) je to zřejmé. Je totiž $\delta(s, s) = 0 = d_0(s)$ a pro ostatní v je jistě $\delta(s, v) \leq d_0(v) = \infty$. Předpokládejme, že platí $\delta(s, v) \leq d_i(v)$ a dokažme $\delta(s, v) \leq d_{i+1}(v)$. Pro vrchol v jsou dvě možnosti. Buď při $(i + 1)$-tém průchodu cyklem v kroku 4 nedojde ke změně, tj. $d_{i+1}(v) = d_i(v)$, a pak je $\delta(s, v) \leq d_{i+1}(v)$ podle indukčního předpokladu. Nebo ke změně dojde, tj. $d_{i+1}(v) = d_i(u) + w(\{u, v\})$ pro nějaký u. Pak ale z indukčního předpokladu máme $\delta(s, u) + w(\{u, v\}) \leq d_i(u) + w(\{u, v\})$, a protože jistě platí $\delta(s, v) \leq \delta(s, u) + w(\{u, v\})$, máme $\delta(s, v) \leq d_i(u) + w(\{u, v\}) = d_{i+1}(v)$. (4.1) je dokázáno.

Označme nyní $D_1, \ldots, D_k$ všechny od sebe různé vzdálenosti vrcholů grafu od vrcholu s tak, že $0 = D_1 < D_2 < \cdots < D_k$ (tj. $D_1 = 0$ je vzdálenost s od s, D_k je vzdálenost nejvzdálenějšího

vrcholu od s). Označme dále $V_i = \{v \in V \mid d(s,v) = D_i\}$ pro $i = 1, \ldots, k$, tj. V_i obsahuje právě vrcholy se vzdáleností D_i od s. Indukcí podle i dokážeme, že $D_i = m_i$ a $V_i = N_i$ pro každý provedený průchod i cyklem 2., 3., 4. Z tohoto tvrzení už plyne požadovaná rovnost $d(v) = \delta(s,v)$: Za prvé, každý $v \in V$, do kterého existuje cesta z s, patří do nějaké $V_i = N_i$ (pro ostatní je $d_i(v) = \infty$). Za druhé, pro vrcholy v z N_i je $d_i(v) = m_i$ a výsledná vypočtená hodnota $d(v)$ je $d(v) = d_i(v)$ (v se odstraní z A a dál se s nimi nepracuje). Tedy pro každý vrchol v, do kterého existuje z s cesta, je $d(v) = d_i(v) = m_i = d(s,v)$.

Dokažme tedy $D_i = m_i$ a $V_i = N_i$. Pro $i = 1$ je to zřejmé: $D_1 = 0 = m_1$, $N_1 = \{s\} = V_1$. Předpokládejme, že tvrzení platí pro všechna $j < i$ a dokažme ho pro i: Vezměme libovolný $v \in V_i$. Pak podle definice V_i má nejkratší cesta $s, \ldots, u, e, v$ délku D_i. Cesta $s, \ldots, u$ je pak nejkratší cestou z s do u (jinak by $s, \ldots, u, e, v$ nebyla nejkratší z s do v, rozmyslete). Její délka je tedy některou z $D_j < D_i = D_j + w(\{u,v\})$. Podle indukčního předpokladu je $u \in V_j = N_j$, a proto $d_j(v) = D_i$ (podrobněji: kdyby $d_j(v) < D_i$, pak z $d(v) \leq d_j(v)$ je $d(v) < D_j = \delta(s,v)$, spor s (4.1); na druhou stranu se hodnota D_i se do $d_j(v)$ dostane v j-tém cyklu přiřazením $d_j(v) := d_j(u) + w(\{u,v\})$ nebo už bylo $d_{j-1}(v) = D_i$). Proto i $d_i(v) = D_i$ (pro $j < k \leq i$ nemůže být $d_k(v) < d_j(v)$, pak by opět $d(v) < \delta(s,v)$). Tedy pro všechny $v \in V_i$ je $d_i(v) = D_i$.

Ukážeme teď $D_i = m_i$, tj. $D_i = \min\{d_i(u) \mid u \in A_{i-1}\}$. Kdyby existoval $u \in A_{i-1}$ tak, že $d_i(u) < D_i$, pak je $u \notin V_i$ (neboť jsme ukázali, že pro $u \in V_i$ je $d_i(u) = D_i$). Tedy buď existuje $j < i$ a $u \in V_j = N_j$, což nelze (protože $N_j \cap A_{i-1} = \emptyset$), nebo existuje $j > i$ a $u \in V_j$, což také nelze, protože pak by $d(s,u) = D_j > D_i > d_i(u) \geq d(u)$, a to je spor s (4.1). Máme tedy $D_i = m_i$. Podle definice N_i je tedy $V_i \subseteq N_i$ (protože pro $u \in V_i$ je $d_i(u) = D_i = m_i$). Ale žádný jiný u z A_{i-1} do N_i nepatří. Pak by totiž musel $u \in V_j$ pro $j > i$, tedy by $d(s,u) = D_j > D_i = d_i(u) \geq d(u)$, což je spor s (4.1). Tedy je $V_i = N_i$. Důkaz správnosti Algoritmu 4.13 je hotov. □

4.4 Stupně vrcholů

Jednou ze základních a snadno zjistitelných informací o grafu je, kolik hran vchází a vychází do jednotlivých vrcholů. Je to informace, kterou dobře vnímáme i pohledem na obrázek grafu. V této kapitole ukážeme několik základních úvah založených na počtech hran jednotlivých vrcholů.

Definice 4.14 (stupeň vrcholu). *Stupeň vrcholu* $v \in V$ grafu $\langle V, E \rangle$ je počet hran, jejichž jedním z koncových vrcholů je v, a značí se $\deg(v)$.

U orientovaných grafů se někdy zavádí vstupní a výstupní stupeň vrcholu jako počet hran, které do přicházejí, a počet hran, které z něj vycházejí. Stupeň vrcholu je pak součet vstupního a výstupního stupně. Pro graf na Obr. 4 vlevo je $\deg(u) = 3$, $\deg(v) = 2$, $\deg(w) = 2$, $\deg(x) = 1$, $\deg(y) = 0$. Pro graf vpravo je $\deg(u) = 3$, $\deg(v) = 3$, $\deg(w) = 3$, $\deg(x) = 1$, $\deg(y) = 0$. . Protože orientace hran v naší definici stupně vrcholu nehraje roli, budeme v této kapitole předpokládat, že grafy, se kterými se zabýváme, jsou neorientované.

Věta 4.15. *V grafu* $G = \langle V, E \rangle$ *je* $\sum_{v \in V} \deg(v) = 2|E|$.

Důkaz. Máme dokázat, že součet stupňů všech vrcholů grafu je roven dvojnásobku počtu hran. Tvrzení je téměř zřejmé, uvědomíme-li si následující. Každá hrana $e \in E$ má dva vrcholy, u a v. Hrana e přispívá jedničkou do $\deg(u)$ (je jednou z hran, jejichž počet je roven $\deg(u)$), jedničkou do $\deg(v)$ a do stupně žádného jiného vrcholu nepřispívá. Hrana e tedy přispívá právě počtem 2 do $\sum_{v \in V} \deg(v)$. To platí pro každou hranu. Proto $\sum_{v \in V} \deg(v) = 2|E|$. □

Důsledek 4.16. *Počet vrcholů lichého stupně je v libovolném grafu sudý.*

Důkaz. Označme S a L množiny vrcholů, které mají sudý a lichý stupeň. Protože každý vrchol patří buď do S, nebo do L, je $\sum_{v\in V}\deg(v) = \sum_{v\in S}\deg(v) + \sum_{v\in L}\deg(v)$. Je jasné, že $\sum_{v\in S}\deg(v)$ je sudé číslo. Podle Věty 4.15 je $\sum_{v\in V}\deg(v) = 2|E|$, tedy $\sum_{v\in V}\deg(v)$ je sudé číslo. Proto i $\sum_{v\in L}\deg(v)$ musí být sudé číslo. Kdyby byl počet vrcholů s lichým stupněm lichý, byl by $\sum_{v\in L}\deg(v)$ součet lichého počtu lichých čísel, a tedy by $\sum_{v\in L}\deg(v)$ bylo liché číslo, což není možné. Počet vrcholů s lichým stupněm je tedy sudý. □

Uvedená tvrzení představují základní podmínky, které stupně každého grafu splňují. Představme si, že o grafu s vrcholy $v_1, \ldots, v_n$ nevíme nic víc než stupně jeho vrcholů, tj. známe posloupnost $\deg(v_1), \ldots, \deg(v_n)$ stupňů jeho vrcholů. Tato posloupnost se nazývá *skóre grafu* (někdy grafová posloupnost). Přitom dvě skóre považujeme za stejná, liší-li se jen permutací (seřazením) členů. Určuje skóre graf jednoznačným způsobem (až na izomorfismus)? Vezměme např. posloupnost $1, 1, 1, 1, 1, 1$. Jednoduchou úvahou dojdeme k tomu, že každé dva grafy, jejichž skóre je $1, 1, 1, 1, 1, 1$ jsou izomorfní. Jsou to grafy izomorfní s grafem $\langle V, E\rangle$, kde $V = \{a, b, c, d, e, f\}$ a $E = \{\{a, b\}, \{c, d\}, \{e, f\}\}$. Skóre $2, 2, 2, 2, 2, 2$ však graf jednoznačným způsobem neurčuje. Na množině vrcholů $V = \{a, b, c, d, e, f\}$ totiž můžeme mít dva grafy, které nejsou izomorfní, a přesto je $2, 2, 2, 2, 2, 2$ skóre každého z nich. První je dán množinou hran $\{\{a, b\}, \{b, c\}, \{a, c\}, \{d, e\}, \{e, f\}, \{d, f\}\}$ (dva trojúhelníky), druhý množinou $\{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{a, f\}\}$ (šestiúhelník). Grafy si nakreslete a zdůvodněte si to.

Jak víme, ne každá posloupnost čísel je skóre nějakého grafu. Např. $3, 4, 2, 0$ není skóre grafu. Zkuste takový graf nakreslit a uvidíte, že to nejde! Můžeme to ale zjistit i bez kreslení. Stačí použít Důsledek 4.16: Graf, jehož skóre je $3, 4, 2, 0$ by měl právě jeden vrchol lichého stupně, což není možné. Posloupnost $6, 2, 2, 0$ ale podmínce z Důsledku 4.16 vyhovuje, ale graf se skóre $6, 2, 2, 0$ také neexistuje (zkuste nakreslit). Vidíme, že podmínka z Důsledku 4.16 je sice nutná, ale není postačující. Otázkou je, jestli existuje jednoduchá podmínka, kterou posloupnost nezáporných celých čísel splňuje, právě když je to skóre nějakého grafu. Ukážeme, že ano a že to, zda platí, dokonce lze ověřit jednoduchým algoritmem.

Věta 4.17. *Nechť $d_1 \geq d_2 \geq d_3 \geq \cdots \geq d_n$ jsou nezáporná celá čísla a $1 \leq d_1 \leq n-1$. Pak*

$$d_1, d_2, d_3, \ldots, d_n$$

je skóre nějakého grafu, právě když

$$d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$$

je skóre nějakého grafu.

Důkaz. Uvědomme si nejdříve tohle. Posloupnost $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ má $n-1$ prvků. Přitom její část $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1$ má d_1 prvků a dostaneme ji odečtením jedničky z prvních d_1 prvků posloupnosti $d_2, d_3, \ldots, d_n$. Část $d_{d_1+2}, \ldots, d_n$ má $n - d_1$ prvků a je to posledních $n - d_1$ prvků prvků posloupnosti $d_2, d_3, \ldots, d_n$.

Ukážeme nejdříve, že když $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ je skóre, pak i $d_1, d_2, d_3, \ldots, d_n$ je skóre. Když je $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ skóre grafu $G = \langle V, E\rangle$, má G $n-1$ vrcholů (označme je $v_2, \ldots, v_n$), které mají po řadě stupně $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, \ldots, d_{d_1+2}, \ldots, d_n$. Vytvořme z G nový graf $G' = \langle V', E'\rangle$ přidáním vrcholu v_1, tj.

$$V' = \{v_1, v_2, \ldots, v_n\},$$

a ke každému z vrcholů $v_2, \ldots, v_{d_1+1}$ přidejme hranu k vrcholu v_1, tj.

$$E' = E \cup \{\{v_1, v_j\} \mid j = 2, \ldots, d_1 + 1\}.$$

V grafu G' vede z vrcholu v_1 právě d_1 hran (tolik jsme jich přidali) a stupeň každého z vrcholů $v_2, \ldots, v_{d_1+1}$ se o 1 zvýšil. Stupně ostatních vrcholů se nezměnily (hrany jsme k nim

nepřidávali). Skóre grafu G' je tedy $\deg(v_1), (d_2 - 1) + 1, (d_3 - 1) + 1, \ldots, (d_{d_1+1} - 1) + 1, d_{d_1+2}, \ldots, d_n$, což je právě $d_1, d_2, d_3, \ldots, d_n$. Dokázali jsme, že $d_1, d_2, d_3, \ldots, d_n$ je skóre grafu.

Ukažme teď naopak, že když $d_1, d_2, d_3, \ldots, d_n$ je skóre, je i $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ skóre. Je-li $d_1, d_2, d_3, \ldots, d_n$, uvažujme příslušný graf G s vrcholy $v_1, \ldots, v_n$ tak, že $\deg(v_i) = d_i$. Rozlišíme dva případy.

První případ: Vrchol v_1 stupně d_1 je hranami spojen s vrcholy $v_2, dots, v_{d_1+1}$. Pak graf, který vznikne z G odstraněním vrcholu v_1 a hran, které z něj vycházejí (to jsou právě hrany $\{v_1, v_2\}, dots, \{v_1, v_{d_1+1}\}$), má právě skóre $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$, tedy posloupnost $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ je skóre grafu.

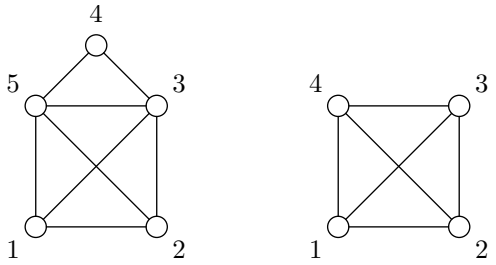
Druhý případ: Vrchol v_1 stupně d_1 spojený hranami s vrcholy $v_2, dots, v_{d_1+1}$ neexistuje. Pak tedy existuje vrchol v_i ($2 \leq i \leq d_1 + 1$), který není spojen s v_1, a vrchol v_j ($d_1 + 1 < j \leq n$), který je spojen s v_1. Protože $d_i \geq d_j$, existuje vrchol v_k různý od v_j, který je spojen s v_i, ale ne s v_j (kdyby v_k jiný než v_j neexistoval, nemohlo by být $d_i \geq d_j$). Vytvořme graf G', který vznikne z G odstraněním hran $\{v_1, v_j\}$ a $\{v_i, v_k\}$ a přidáním hran $\{v_1, v_i\}$ a $\{v_j, v_k\}$. Skóre grafu G' je opět $d_1, d_2, d_3, \ldots, d_n$. Záměnou jsme dosáhli toho, že z posloupnosti $v_2, \ldots, v_{d_1+1}$ je hranou spojeno s vrcholem v_1 více vrcholů v novém grafu G' než v původním G. Na graf G' je teď buď možné použít první případ, nebo ho lze postupným opakováním právě provedené úpravy převést na graf, na který první případ už použít lze. □

Věta 4.17 je základem pro následující algoritmus.

Algoritmus 4.18 (test skóre).
Vstup: $n \in \mathbb{N}$, $\langle d_1, \ldots, d_n \rangle$, kde $d_1 \geq \cdots \geq d_n \geq 0$ jsou celá čísla;
Výstup: ANO, pokud $\langle d_1, \ldots, d_n \rangle$ je skóre, NE v opačném případě;

1. je-li $n = 1$ a $d_1 = 0$, odpověz ANO a skonči;
2. je-li $n = 1$ a $d_1 \neq 0$, odpověz NE a skonči;
3. je-li $d_1 > n - 1$, odpověz NE a skonči;
4. vypočítej novou posloupnost
   $\langle d'_1, \ldots, d'_{n-1} \rangle = \langle d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n \rangle$;
5. je-li některé d'_i záporné, odpověz NE a skonči;
6. uspořádej $d'_1, \ldots, d'_{n-1}$ sestupně, přiřaď takto uspořádané hodnoty do $d_1, \ldots, d_{n-1}$, sniž n o 1 (tj. $n := n - 1$) a pokračuj bodem 1.

Ukažme, že algoritmus pracuje správně. Skončí-li algoritmus v bodě 1., je to správně, protože jednoprvková posloupnost 0 je skóre grafu (o jednom vrcholu a žádné hraně). Skončí-li algoritmus v bodě 2., je to správně, neboť pro $n > 0$ jednoprvková posloupnost n skóre samozřejmě není. Skončí-li algoritmus v bodě 3., je to správně, neboť stupeň žádného vrcholu nemůže být větší než počet vrcholů minus jedna. Pokud má aktuální posloupnost více než 1 člen, v bodě 4. se vypočítá nová posloupnost, která je dle Věty 4.17 skóre grafu, právě když je původní posloupnost skóre grafu. Na základě Věty 4.17 se tedy v tomto kroku testování redukuje na testování posloupnosti, která je o 1 člen kratší. Pokud se při výpočtu nové posloupnosti objeví záporné číslo, algoritmus skončí s odpovědí NE (stupeň vrcholu nemůže být záporný). Jinak algoritmus novou posloupnost sestupně setřídí a pokračuje znovu bodem 1. Je zřejmé, že algoritmus vždy skončí, neboť posloupnosti se vždy o 1 zkracují. Pro vstupní posloupnost délky n algoritmus skončí nejvýše po $n - 1$ výpočtech nové posloupnosti. Algoritmus bychom mohli urychlit o krok, ve kterém by se testovaná posloupnost zkrátila o koncové nuly (zdůvodněte si to).



Obrázek 8: Nakreslete obrázky jedním tahem.

Příklad 4.19. Algoritmus 4.18 použijeme ke zjištění, jestli jsou posloupnosti $6,6,5,4,3,3,3,3,2,1,0$ a $4,3,2,1,1$. Test posloupnosti $6,6,5,4,3,3,3,3,2,1,0$ vede postupně na testy posloupností $5,4,3,3,2,2,2,2,1,0$, pak $3,2,2,2,2,1,1,1,0$, pak $2,1,1,1,1,1,1,0$, pak $1,1,1,1,0,0,0$, pak $1,1,0,0,0,0$, pak $0,0,0,0,0,0,0,0,0,0$, pak $0,0,0$, pak $0,0$, pak 0 a skončí odpovědí ANO v bodě 1. Test $4,3,2,1,1$ vede postupně na $2,1,0,0$, pak se v bodě 4. vypočítá posloupnost $1,-1,0$ a algoritmus skončí s odpovědí NE. To, že $4,3,2,1,1$ není skóre můžeme poznat také přímo podle Důsledku 4.16, protože $4,3,2,1,1$ má lichý počet lichých stupňů.

Se stupni vrcholů souvisí známá úloha nakreslit jedním tahem zadaný obrázek.

Průvodce studiem

Úloha o kreslení jedním tahem: Nakreslete obrázek, viz např. Obr. 8, jedním tahem. Přitom žádnou hranu není povoleno projít dvakrát a při kreslení není povoleno zvednout tužku od papíru.

S touto úlohou se asi každý setkal na základní škole. Ukážeme si, že rozhodnout, zda obrázek lze nakreslit jedním tahem, popř. zda je i možné přitom začít i skončit v jednom místě, jde jednoduše podle stupňu vrcholů. Na kreslení jednotažek navíc existuje algoritmus.

Na Obr. 8 jsou dva obrázky. Úkolem je nakreslit obrázek jedním tahem s tím, že žádnou hranu nesmíme nakreslit dvakrát a nesmíme zvednout tužku z papíru. U levého obrázku to jde (např. $1,2,3,5,1,3,4,5,2$), u pravého ne (zkuste zdůvodnit).

Definice 4.20 (eulerovský tah). Eulerovský[7] **tah** je tah, který obsahuje všechny vrcholy grafu a ve kterém se každá hrana vyskytuje právě jednou. Je-li navíc uzavřený, nazývá se **uzavřený eulerovský tah**.

Eulerovský tah představuje kreslení "jedním tahem". Chceme-li navíc při kreslení vyjít i skončit v jednom místě, musíme najít uzavřený eulerovský tah. Následující věta ukazuje, jak jednoduše poznat, zda eulerovký tah vůbec existuje.

Jestli graf má (uzavřený) eulerovský tah, lze jednoduše poznat ze stupňů jeho vrcholů.

Věta 4.21.
- *V neorientovaném grafu existuje uzavřený eulerovský tah, právě když je souvislý a každý vrchol má sudý stupeň.*
- *V neorientovaném grafu existuje neuzavřený eulerovský tah, právě když je souvislý a má právě dva vrcholy lichého stupně.*

Důkaz. Dokážeme nejdříve tvrzení pro uzavřené eulerovské tahy. Mějme graf $G = \langle V, E\rangle$.

Předpokládejme nejdřív, že v G existuje uzavřený eulerovský tah $v, e, \ldots, v$. Je jasné, že G je souvislý. Uvažujme libovolný vrchol $u \in V$ a množinu E_u všech hran, jichž je u koncovým vrcholem. Jejich počet je stupeň u, tj. $\deg(u) = |E_u|$. Pro $u \neq v$ je libovolný výskyt u v tahu

[7] Leonhard Euler (1707–1783), jeden z nejvýznamnějších matematiků.

$v, e, \ldots, v$ tvaru $\ldots, e, u, e', \ldots$, kde $e, e' \in E_u$, tj. každý výskyt u je doprovázen výskytem dvou hran z E_u (jednou z nich se do u vstoupí, druhou se vystoupí). Protože se v tahu každá hrana vyskytuje právě jednou, je jasné, že hran z E_u je sudý počet. Pro $u = v$ to platí s výjimkou prvního (tam hrana z v pouze vychází) a posledního výskytu (tam hrana do v pouze vchází). Každý z nich je doprovázen výskytem jedné hrany z E_u a proto je počet hran v E_u opět sudé číslo.

Předpokládejme teď, že G je souvislý a že každý jeho vrchol má sudý stupeň. Uvažujme tah $v_0, e_1, \ldots, e_n, v_n$ (označme ho t) v G, který má největší možnou délku (to můžeme: tah nemůže být delší než počet všech hran rafu G, tahů s největší délkou ale může být více). Všimněme si nejdřív, že musí být $v_0 = v_n$. Jinak by vrchol v_0 byl koncovým vrcholem lichého počtu hran (hrana z něj vychází a pak vždy vchází a vychází). Protože má v_0 sudý stupeň, existuje hrana $e = \{v, v_0\}$, která není obsažena v tahu t. Pak je ale $v, e, v_0, e_1, \ldots, e_n, v_n$ tah, který je delší než t, a to je spor s tím, že t má největší možnou délku. Tedy musí být $v_0 = v_n$. Abychom tvrzení dokázali, stačí ukázat, že $\{e_1, \ldots, e_n\} = E$ (hrany tahu t jsou právě všechny hrany grafu). Uvažujme graf $G' = \langle V', E' \rangle$, který má za vrcholy všechny vrcholy tahu t a za hrany všechny hrany tahu t. Kdyby $V' \neq V$, tj. existuje $u \in V - V'$, plyne ze souvislosti G, že pro nějaký $v_i \in V'$ existuje hrana $e = \{u, v_i\}$. Pak by ale

$$v_i, e_{i+1}, \ldots, e_n, v_n, e_1, \ldots, e_i, v_i, e, u$$

byl tah a byl by delší než tah t, což je spor. Tedy musí být $V' = V$. Kdyby $E' \neq E$, existuje hrana $e = \{v_i, v_j\} \in E \notin E'$. Pak by ale

$$v_i, e_{i+1}, \ldots, e_n, v_n, e_1, \ldots, e_i, v_i, e, v_j$$

byl opět tah delší než tah t, což je opět spor. Vidíme tedy, že t je eulerovský tah.

Část tvrzení, která se týká eulerovských tahů, se provede podobně (viz seznam úloh k textu). □

Průvodce studiem

Úloze rozhodnout, zda v grafu existuje uzavřený eulerovský tah, je podobná úloha tzv. hamiltonovské[8] kružnice. Hamiltonovská kružnice je kružnice, která obsahuje všechny vrcholy grafu. Připomeňme, že uzavřený eulerovský tah obsahuje všechny hrany grafu. Zatímco zjistit, zda v grafu existuje uzavřený eulerovský tah, je velmi snadné (podle Věty 4.21 stačí ověřit, že kařdý vrchol má sudý stupeň), není znám rychlý algoritmus, který by zjistil, zda graf má hamiltonovskou kružnici. Navíc je pravděpodobné, že takový algoritmus ani neexistuje (zjistit existenci hamiltonovské kružnice je totiž tzv. NP-úplný problém).

Shrnutí

Graf je tvořen množinou vrcholů a hran spojujících některé vrcholy. Graf může být orientovaný nebo neorientovaný, podle toho, jestli rozlišujeme, zda orientace hran hraje roli. Posloupnost vrcholů a hran, která odpovídá možnému průchodu grafem, se nazývá sled. Rolišujeme několik typů sledů. Mezi důležité úlohy patří různé úlohy o cestování v grafech.

Pojmy k zapamatování

- orientovaný graf, neorientovaný graf, vrchol, hrana,
- izomorfismus grafů, podgraf,
- sled, délka sledu, uzavřený sled, tah, cesta, kružnice, vzdálenost vrcholů,
- ohodnocený graf,

- souvislost, komponenta, hledání cest,
- stupeň vrcholu, skóre, eulerovský tah.

Kontrolní otázky

1. *Vysvětlete rozdíl mezi pojmy orientovaný graf a neorientovaný graf.*
2. *Je-li graf G izomorfní s grafem G', je jeho podgrafem?*
3. *Jaký je rozdíl mezi pojmy sled, tah, cesta?*
4. *Může mít souvislý graf po odstranění jedné hrany tři komponenty?*
5. *Existuje graf, který má skóre $7, 3, 1$?*

Cvičení

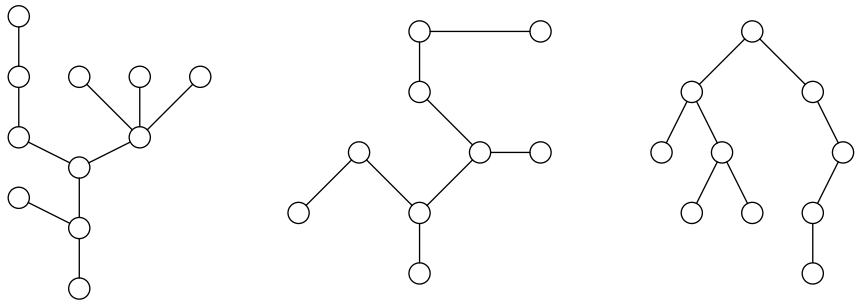
1. Je-li graf G izomorfní s grafem G', je každý podgraf grafu G izomorfní nějakému podgrafu grafu G'. Dokažte.
2. Nechť jsou dány grafy G s vrcholy $v_1, \ldots, v_n$ a G' s vrcholy $v'_1, \ldots, v'_n$ takové, že $\deg(v_i) = \deg(v'_i)$. Musí být G a G' izomorfní?
3. Jaký je největší možný součet stupňů vrcholů neorientovaného grafu s n vrcholy?
4. Určete (např. pomocí Algoritmu 4.18), zda jsou skóre posloupnosti
   (a) $6, 6, 6, 6, 5, 4, 3$,
   (b) $5, 5, 5, 5, 5, 4, 3$,
   (c) $4, 4, 4, 4, 3, 3, 2$.
   Nakreslete příslušné grafy.

Úkoly k textu

1. Dokončete důkaz Věty 4.12, tj. ukažte, že každá hrana grafu je hranou právě jedné jeho komponenty.
2. Dokončete důkaz Věty 4.21, tj. dokažte, že v neorientovaném grafu existuje neuzavřený eulerovský tah, právě když je souvislý a má právě dva vrcholy lichého stupně. Návod: Postupujte podobně jako pro uzavřené eulerovské tahy. Sečtením hran v eulerovském tahu dojdete k tomu, že když neuzavřený eulerovský tah existuje, mají právě dva vrcholy lichý stupeň. Naopak, když je graf souvislý a právě dva vrcholy, u a v, mají lichý stupeň, uvažujte opět nejdelší tah. O něm nejdříve dokažte, že jeho krajní vrcholy jsou u a v. Pak postupujte podobně jako u důkazu pro uzavřený eulerovský tah, tj. ukažte, že obsahuje všechny vrcholy i všechny hrany grafu.
3. Navrhněte algoritmus pro hledání uzavřeného eulerovského tahu a algoritmus pro hledání eulerovského tahu. Proveďte důkazy správnosti těchto algoritmů.
4. Upravte Algoritmus 4.13 tak, aby fungoval i pro orientované grafy. Tj. vstupem bude ohodnocený orientovaný graf a jeho vrchol s. Výstupem budou čísla $d(v)$, kde $d(v)$ je délka nejkratší cesty z s do v. Proveďte důkaz správnosti.

Řešení

1. Snadné.
2. Ne. Uvažujme $n = 6$ a $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_1\}\}$ a $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_1\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_6, v_4\}\}$.
3. $n \cdot (n - 1)$.



Obrázek 9: Stromy.

4. 1. ne, 2. ano, 3. ano.

Studijní cíle: Po prostudování kapitoly 4.5 by student měl rozumět speciálním grafům nazývaným stromy. Měl by znát základní vlastnosti stromů a algoritmy pro jejich procházení.

Klíčová slova: strom, list, kostra, kořenový strom, úroveň vrcholu, hloubka stromu, vyvážený strom, m-ární strom, uspořádaný kořenový strom, preorder, postorder, inorder

Potřebný čas: 180 minut.

4.5 Stromy

Průvodce studiem

Stromy jsou speciální grafy, které dostaly název podle toho, že vypadají podobně jako stromy, popř. keře v přírodě. Typický strom-graf vypadá jako strom v přírodě. Má svůj kořen (speciální vrchol), ve kterém se větví (vedou z něj hrany) do míst (vrcholů), ve kterých se opět větví atd. Stromy jsou grafy, které mají nejčastější použití. Setkáváme se s nimi v běžném životě (různá členění, např. členění knihy na kapitoly, podkapitoly atd., mají stromovou strukturu), jako uživatelé počítačů (stromová struktura adresářů) i jako informatici (rozhodovací stromy, vyhledávací stromy).

4.5.1 Definice a základní vlastnosti

Pojem strom lze zavést několika způsoby. Jako definici vezmeme následující.

Definice 4.22. *Strom* je neorientovaný souvislý graf bez kružnic.

Někdy se zavádí i pojem strom pro orientované grafy. My se tím ale zabývat nebudeme. Příklady stromů vidíme na Obr. 9.

Vrchol grafu se stupněm 1 se nazývá *koncový*. Koncový vrchol stromu se nazývá *list*. Následující tvrzení ukazují, že stromy vznikají přidáváním listů.

Věta 4.23. *V každém stromu s alespoň dvěma vrcholy existují aspoň dva listy.*

Důkaz. Uvažujme cestu $v_0, e_1, \ldots, v_n$, která má maximální délku. Tvrdíme, že v_0 i v_n jsou listy. Kdyby např. v_0 nebyl list, pak by existovala hrana $e = \{v, v_0\}$, která na cestě neleží (jinak by to musela být hrana e_1). Kdyby $v = v_i$ pro nějaké $i = 2, \ldots, n$, pak by $v, e, v_0, \ldots, v_i$ byla kružnice, což je spor s tím, že G je strom. Pak ale $v, e, v_0, e_1, \ldots, v_n$ je cesta, která je delší než $v_0, e_1, \ldots, v_n$, což je opět spor. Podobně se ukáže, že v_n je list. □

Věta 4.24. *Pro graf G a jeho koncový vrchol v jsou následující tvrzení ekvivalentní.*

1. *G je strom.*

2. *$G - v$ je strom.*

Důkaz. Poznamenejme, že $G - v$ vznikne z G vymazáním v a hrany, která do něho vede. Tvrzení je téměř zřejmé (viz úkoly k textu). □

Zde jsou další možná zavedení pojmu strom.

Věta 4.25. *Pro neorientovaný graf $G = \langle V, E \rangle$ jsou následující tvrzení ekvivalentní.*

1. *G je strom.*

2. *Mezi každými dvěma vrholy existuje právě jedna cesta.*

3. *G je souvislý a vynecháním libovolné hrany vznikne nesouvislý graf.*

4. *G neobsahuje kružnice, ale přidáním jakékoli hrany vznikne graf s kružnicí.*

5. *G neobsahuje kružnice a $|V| = |E| + 1$.*

6. *G je souvislý a $|V| = |E| + 1$.*

Důkaz. „1. $\Rightarrow$ 2.“: Předpokládejme, že G je strom. Protože G je podle definice souvislý, existuje mezi každými dvěma vrcholy cesta. Kdyby mezi nějakými vrcholy u a v existovaly dvě různé cesty, znamenalo by to, že v G je kružnice. Totiž, jsou-li ty cesty $u, e_1, v_1, \ldots, e_n, v$ a $u, e'_1, v'_1, \ldots, e'_m, v$, pak jejich spojením je uzavřený sled $s = u, e_1, v_1, \ldots, e_n, v, e'_m, \ldots, v'_1, e'_1, u$. Pokud ten ještě není kružnicí, opakuje se v něm nějaký vrchol $w \neq u$, tj. exsituje v něm úsek $w, \ldots, w$. Nahrazením tohoto úseku jen uzlem w toto opakování odstraníme. Pokud se ve zbylém uzavřeném s' úseku už žádný vrchol neopakuje, je s' hledanou kružnicí. Pokud ano, můžeme v něm opět nahradit nějakou část $w', \ldots, w'$ uzlem w'. Tak postupně dostaneme kružnici. To je ale spor s tím, že G je strom.

„2. $\Rightarrow$ 3.“: Vynechme hranu $e = \{u, v\} \in E$ stromu G, dostaneme tak graf G'. Kdyby byl G' souvislý, existovala by v něm cesta $u, e_1, \ldots, v$ mezi u a v. To by ale znamenalo, že v G existují dvě cesty z u do v: jednou je $u, e_1, \ldots, v$, druhou je u, e, v. To je spor s tím, že mezi každými dvěma vrcholy je v G právě jedna cesta.

„3. $\Rightarrow$ 4.“: Kdyby G obsahoval kružnici, pak odstraněním jedné její hrany dostaneme opět souvislý graf, což je spor s předpokladem 3. Kdyby po přidání hrany $e = \{u, v\}$ nevznikla kružnice, v G by neexistovala cesta mezi u a v (kdyby ano, přidáním e k této cestě dostaneme kružnici), a tedy G by nebyl souvislý, což je spor s 3.

„1. $\Rightarrow$ 5.“: Máme ukázat, že ve stromu je $|V| = |E| + 1$. Dokažme to indukcí podle počtu vrcholů. Pro $n = 1$ vrchol to zřejmě platí (pak je totiž $|E| = 0$). Předpokládejme, že to platí pro každý strom o n vrcholech. Má-li G $n + 1$ vrcholů, odstraňme z něj nějaký list. Výsledný graf $\langle V', E' \rangle$ je podle Věty 4.24 opět strom, má n vrcholů, a tedy podle předpokladu platí $|V'| = |E'| + 1$. Protože však $|V| = |V'| + 1$ a $|E| = |E'| + 1$, platí i $|V| = |E| + 1$.

„5. $\Rightarrow$ 6.“: Nechť k je po5et komponent grafu G. Vyberme z každé komponenty po jednom vrcholu a označme tyto vrcholy $v_1, \ldots, v_k$. Přidejme $r-1$ hran $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{k-1}, v_k\}$ ke grafu G. Takto vzniklý graf $G' = \langle V, E' \rangle$ je strom (je souvislý a nemá kružnice, protože G neměl kružnice). Z výše dokázaného „1. $\Rightarrow$ 5.“ plyne, že $|V| = |E'| + 1$. Podle předpokladu je ale $|V| = |E| + 1$. Tedy $|E| = |E'|$. Protože $|E'| = |E| + r - 1$, je $r = 1$, tedy G má právě jednu komponentu, tj. je souvislý.

„6. $\Rightarrow$ 1.“: Dokážeme indukcí podle počtu vrcholů. Má-li G jeden vrchol, je tvrzení zřejmé. Předpokládejme, že tvrzení platí pro každý graf s n vrcholy a že G má $n + 1$ vrcholů a splňuje $|V| = |E| + 1$. Součet stupňů jeho vrcholů je $2|E| = 2|V| - 2$. Ze souvislosti plyne, že každý vrchol má stupeň aspoň 1. Kdyby měl každý vrchol stupeň aspoň 2, byl by součet stupňů všech

vrcholů aspoň $2|V|$, ale ten součet je $2|V| - 2 < 2|V|$. Tedy musí existovat vrchol v stupně právě 1, tj. list. Jeho odstraněním dostaneme graf $G' = \langle V', E' \rangle = G - v$, který je zřejmě souvislý, n vrcholů a platí pro něj $|V'| = |V| - 1$, $|E'| = |E| - 1$. G' tedy splňuje $|V'| = |E'| + 1$ a z indukčního předpokladu plyne, že je to strom. Proto je i G strom (viz Větu 4.24). □

4.5.2 Hledání minimální kostry grafu

Definice 4.26. *Kostra* neorientovaného grafu G je jeho podgraf, který je stromem a obsahuje všechny vrcholy grafu G.

Věta 4.27. *Graf má kostru, právě když je souvislý.*

Důkaz. Snadné, zkuste sami. □

4.5.3 Kořenové stromy

Definice 4.28. *Kořenový strom* je dvojice $\langle G, r \rangle$, kde $G = \langle V, E \rangle$ je strom a $r \in V$ je vrchol, tzv. *kořen*.

Kořenový strom je tedy strom, ve kterém je vybrán jeden vrchol (kořen). Může to být kterýkoliv vrchol. Bývá to ale vrchol, který je v nějakém smysly na vrcholu hierarchie objektů, která je stromem reprezentována.

To, že je v kořenovém stromu jeden vrchol pevně zvolený a že ve stromu exsituje mezi vrcholy jediná cesta, umožňuje ve kořenovém stromu zavádět uspořádání vrcholů. Na základě tohoto uspořádání se stromy kreslí. Základem je následující definice.

Definice 4.29 (kořenový strom–další pojmy). Nechť $\langle G, r \rangle$ je kořenový strom.

- Vrchol v se nazývá *potomek* vrcholu u (u se nazývá *rodič* vrcholu v), právě když cesta z kořene r do v má tvar $r, \ldots, u, e, v$.
- *Úroveň* vrcholu v je délka cesty od kořene r do v.
- *Hloubka* stromu $\langle G, r \rangle$ je největší z úrovní jeho listů.

Kořenový strom hloubky h se nazývá *vyvážený*, právě když každý jeho list má úroveň h nebo $h - 1$.

Vrchol může mít několik potomků, ale má právě jednoho rodiče (ukažte, viz úkoly k textu). Hloubku lze také definovat jako délku nejdelší cesty, která vychází z kořene (ukažte).

Na základě pojmů rodič-potomek a úroveň se kořenové stromy kreslí: Nejvýše se nakreslí kořen, pod něj se nakreslí jeho potomci, tj. vrcholy, které mají úroveň 1. Vrcholy úrovně $l + 1$ přitom kreslíme pod vrcholy úrovně l tak, aby se hrany na obrázku nekřížily. Toho lze zřejmě dosáhnout tak, že všechny potomky $v_1, \ldots, v_n$ vrcholu v nakreslíme pod vrchol v tak, že mezi libovolnými dvěma potomky v_i a v_j vrcholu v buď není žádný vrchol, nebo opět potomek vrcholu v. Příklad stromu nakresleného tímto způsobem vidíme na Obr. **??**. Vrchol TADY je kořenem (tj. jediným vrcholem úrovně 0), TADY jsou vrcholy úrovně 1, TADY jsou vrcholy úrovně 2, TADY jsou vrcholy úrovně 3. Strom má hloubku 3. Není to vyvážený strom, protože vrchol TADY má úroveň 1 (což není ani hloubka, ani hloubka minus 1).

Zvolíme-li v kořenovém stromu libovolný vrchol v, pak vrcholy, které se nacházejí „pod ním“, indukují podgraf, který se nazývá *podstrom indukovaný* vrcholem v (viz cvičení). Např. na Obr. **??** obsahuje podstrom indukovaný vrcholem TADY vrcholy TADY.

Definice 4.30 (m-ární stromy). Kořenový strom se nazývá *m-ární*, právě když každý jeho vrchol má nejvýše m potomků. 2-ární strom se nazývá *binární*. Kořenový strom se nazývá *úplný m-ární*, právě když každý jeho vrchol nemá buď žádného nebo má právě m potomků.

Strom na Obr. **??** je tedy 3-ární (tj. ternární) kořenový strom. Není to ale úplný 3-ární strom, protože vrchol TADY má 1 potomka. Příklad úplného binárního stromu je na Obr. **??** Tento strom je vyvážený.

Při analýze různých problémů (např. při odhadu časové složitosti algoritmů) jsou užitečné různé vztahy mezi hloubkou stromu a počtem jeho listů. Ukážeme některé základní. Nejdříve připomeňme, že pro reálné číslo x je $\lceil x \rceil$ nejmenší celé číslo, které je větší nebo rovno x, tj.

$$\lceil x \rceil = \min\{m \in \mathbb{Z} \mid x \leq m\}.$$

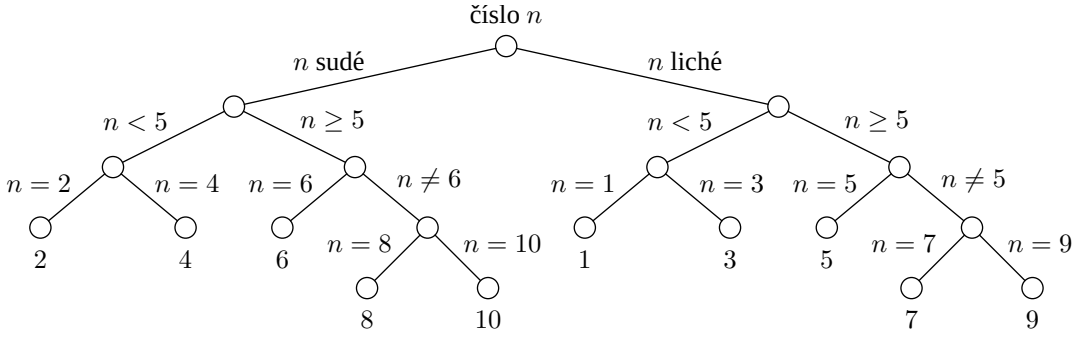
Například $\lceil 1.2 \rceil = 2$, $\lceil 5.8 \rceil = 6$, $\lceil 3 \rceil = 3$.

Věta 4.31. *Necht' $G = \langle V, E \rangle$ je úplný m-ární strom s l listy, který má hloubku h. Pak*

- *$l \leq m^h$ a $h \geq \lceil \log_m l \rceil$,*
- *je-li G vyvážený, je $h = \lceil \log_m l \rceil$.*

Důkaz. Ukažme nejdřív $l \leq m^h$. Máme tedy ukázat, že úplný m-ární strom hloubky h nemůže obsahovat více než m^h listů. Představme si tedy takový strom, který má listů nejvíce (je nejplnější). Je jasné, že bude vypadat takto: Má kořen. Ten má právě m potomků, tj. v úrovni 1 je m vrcholů. Každý z nich má opět m potomků, tj. v úrovni 2 je $m \cdot m = m^2$ vrcholů. Každý z těchto m^2 vrcholů v úrovni 2 má opět m potomků, tj. v úrovni 3 je $m^2 \cdot m = 3$ potomků. Pokračováním dojdeme k tomu, že v úrovni h je právě m^h vrcholů, a to jsou právě listy. Tedy listů je nejvýše m^h, tj. $l \leq m^h$. Zlogaritmujme nyní tuto nerovnost při základu m. Protože logaritmus je rostoucí funkce (tj. z $x < y$ plyne $\log_m(x) < \log_m(y)$), dostáváme $\log_m l \leq h$. Protože pro $x \leq y$ je $\lceil x \rceil \leq \lceil y \rceil$ a pro celé číslo x je $\lceil x \rceil = x$, máme $\lceil \log_m l \rceil \leq \lceil h \rceil = h$.

Předpokládejme nyní, že strom G je navíc vyvážený. Takový strom hloubky h vypadá buď jako ten, který jsme si představili výše, tj. každý z m^{h-1} vrcholů z úrovně $h-1$ má právě m potomků (a strom má tedy v úrovni h právě m^h listů a žádné jiné listy nemá), nebo právě jeden z m^{h-1} vrcholů z úrovně $h-1$ nemá potomky a ostatní mají právě m potomků (a strom má tedy v úrovni h právě $m^h - m$ listů a na úrovni $h-1$ má 1 list), nebo právě dva z m^{h-1} vrcholů z úrovně $h-1$ nemají potomky a ostatní mají právě m potomků(a strom má tedy v úrovni h právě $m^h - 2m$ listů a na úrovni $h-1$ má 2 listy), nebo ... nebo právě $m^{h-1} - 1$ z m^{h-1} vrcholů z úrovně $h-1$ nemá potomky a zbývající vrchol má právě m potomků (a strom má tedy v úrovni h právě $m^h - (m^{h-1} - 1)m$ listů a na úrovni $h-1$ má $m^{h-1} - 1$ listů). Jiné možnosti nejsou. Strom má totiž hloubku h, a tedy aspoň jeden z vrcholů úrovně $h-1$ musí mít potomky. Na druhou stranu, protože je strom vyvážený, má úroveň $h-1$ „plný počet" vrcholů, tj. m^{h-1}. Vidíme tedy, že počet listů stromu G je buď m^h, nebo $m^h - m + 1$ listů, nebo $m^h - 2m + 2$ listů, nebo ... nebo $m^h - (m^{h-1} - 1)m + (m^{h-1} - 1)$ listů. Tedy, G může mít obecně $l = m^h - k \cdot (m-1)$ listů, kde k nabývá hodnot $0, 1, 2, \ldots, m^{h-1} - 1$. Máme dokázat, že pro každou takovou hodnotu k je $h = \lceil \log_m l \rceil$. Protože $\log_m$ je rostoucí funkce, stačí to dokázat pro krajní hodnoty $k = 0$ a pro $k = m^{h-1} - 1$. Pro $k = 0$ máme $l = m^h$, a tedy $\lceil \log_m l \rceil = \lceil \log_m m^h \rceil = \lceil h \rceil = h$ (h je celé číslo). Pro $k = m^{h-1} - 1$ je $l = m^{h-1} + m - 1$. Protože $\log_m m^h = h$ a $\log_m m^{h-1} = h - 1$ (neboť h i $h-1$ jsou celá) a protože $m^h > l = m^{h-1} + m - 1 > m^{h-1}$, dostáváme $h = \log_m m^h > \log_m l > \log_m m^{h-1} = h - 1$. Je tedy jasné, že nejmenší celé číslo větší než $\log_m l$ je právě h, tj. $\lceil \log_m l \rceil = h$, což jsme měli dokázat. □



Obrázek 10: Strom pro hádání čísla z $1, \ldots, 10$.

Průvodce studiem

Promyslete si důkladně Větu 4.31. Úvaha, která vede k $\lceil \log_m \rceil$, se v informatice (ale i v běžném životě) používá velmi často. Předpokládejme, že máme pomocí otázek typu Ano/Ne uhodnout kartu z balíčku 32 karet. Pro jednoduchost očíslujme karty čísly $1, \ldots, 32$, a předpokládejme tedy, že máme uhodnout číslo mezi 1 a 32. Jedna možnost (optimální) je první otázkou rozdělit čísla na dvě stejné části (např. otázka „Je číslo menší než 17?“, tj. části po 16 kartách. Další položená otázka, např. „Je číslo sudé?“ zbylých 16 karet opět rozdělí na dvě poloviny. Atd. až dojdeme k jednomu číslu, a to je to, které hádáme. Např. pro číslo 7 může být posloupnost dotazů kladených hadačem a posloupnost odpovědí následující. Dotaz: „Je číslo menší než 17?“ Odpověď: „Ano.“ Zbývají $1, \ldots, 16$. D: „Je číslo sudé?“ O: „Ne.“ Zbývají 1, 3, 5, 7, 9, 11, 13, 15. D: „Je číslo menší než 9?“ O: „Ano.“ Zbývají 1, 3, 5, 7. D: „Je číslo menší než 5?“ O: „Ne.“ Zbývají 5, 7. D: „Je to číslo 5?“ O: „Ne.“ Zbývá 7 a to je číslo, které hádáme. Strateie volit otázky tak, abychom vždy zredukovali počet možností (pokud možno) na polovinu se nazývá *metoda půlení*. Důležité je, že existuje-li l možností, metodou půlení se dobereme správné možnosti nejpozději v $\lceil \log_2 l \rceil$ krocích. Strom, který odpovídá naší situaci, je totiž vyvážený úplný binární strom o l listech. Výška stromu je právě počet otázek, které musíme v nejhorším případě položit. Na Obr. 10 je strom, odpovídající situaci, kdy hádáme čísla z $1, \ldots, 10$.

Při kreslení stromu po úrovních není uspořádání potomků uzlu zleva doprava jednoznačné.

Definice 4.32. Kořenový strom se nazývá *uspořádaný*, je-li ke každému vrcholu, který není listem, zadáno lineární uspořádání jeho potomků.

Formálněji, uspořádaný kořenový strom je struktura $\langle \langle V, E \rangle, r, \{\leq_v \mid v \in V\} \rangle$, kde $\langle \langle V, E \rangle, r \rangle$ je kořenový strom a pro vrchol $v \in V$ je $\leq_v$ lineární uspořádání na množině $P_v = \{v_1, \ldots, v_n\}$ všech potomků vrcholu v, pokud v není list, a $\leq_v = \emptyset$, pokud je v list. Jsou-li potomkové vrcholu v uspořádáni $v_1 \leq_v \cdots \leq_v v_n$, říkáme, že v_1 je první potomek v atd. V tomto pořadí je také kreslíme po vrchol v.

Např. strom na Obr. TADY je nakreslen jako uspořádaný kořenový strom za předpokladu, že potomci vrcholu TADY jsou uspořádány pořadím TADY, potomci TADY.

Častým úkolem spojeným se stromy je projít všechny vrcholy stromu a v každém provést nějakou akci. Ve vrcholech stromů mohou být například uloženy nějaké informace. Náš úkol může úkol může být vypsat všechny tyto informace (tj. projít všechny vrcholy a pro každý vrchol vypsat informaci, která je v něm uložena). Jiný úkol může být zjistit, zda ve stromu existuje vrchol, který obsahuje zadanou informaci. Máme tedy za úkol pro každý vrchol provést operaci `zpracuj(v)`. Přitom `zpracuj(v)` může znamenat „vypiš informaci uloženou ve v“ apod.

Ukážeme si teď dva způsoby procházení kořenového stromu, tzv. *preorder* a *postorder*. Popíšeme je jako procedury `preorder(v)` a `postorder(v)`, které pracují následovně. `v` je

vstupní parametr, za který můžeme dosadit libovolný vrchol stromu. Je-li pak `u` konkrétní vrchol stromu, znamená `preorder(u)` „vyvolání“ procedury `preorder` pro vrchol `u`. Stejně je to pro `postorder(u)`. Procedury mají tvar

Algoritmus 4.33 (průchod preorder).
Vstup: kořenový strom $\langle\langle V, E\rangle, r\rangle$
Výstup: hodnota $d(v)$ pro každý $v \in V$, $d(v)$ je délka nejkratší cesty z s do v
Proměnné: funkce $d : V \to \mathbb{R}^+$, číslo $m \in \mathbb{R}^+$, množiny $A, N \subseteq V$

1. $A := V$; $d(s) := 0$; pro $v \in V - \{s\}$: $d(v) := \infty$;
2. pokud neexistuje $v \in A$ takový, že $d(v) \neq \infty$, skonči.
3. $m := \min\{d(v) \mid v \in A\}$; $N := \{v \in A \mid d(v) = m\}$; $A := A - N$;
4. pro všechny $v \in N$, $u \in A$ takové, že $\{v, e\} \in E$: jestliže $d(v) + e(\{v, u\}) < d(u)$, pak $d(u) := d(v) + e(\{v, u\})$; pokračuj krokem 2.

```
preorder(v)
{
 zpracuj(v);
 jsou-li v1,...,vn potomci v v jejich usporadani, proved
   zpracuj(v1),...,zpracuj(vn).
}
```

a

```
postorder(v)
{
 jsou-li v1,...,vn potomci v v jejich usporadani, proved
   zpracuj(v1),...,zpracuj(vn);
 zpracuj(v).
}
```

Pro uspořádaný kořenový strom $\langle R, r\rangle$ způsobí `preorder(r)` průchod a zpracování stromu metodou preorder, `postorder(r)` způsobí průchod a zpracování metodou postorder. Tedy např. u metody preorder se nejprve zpracuje kořen r (`zpracuj(v)`) a má-li r potomky $v_1, \ldots, v_n$ (takto uspořádané), vyvolá se průchod metodou preorder ve vrcholu v_1 (`preorder(v1)`), po dokončení tohoto průchodu se se vyvolá průchod ve vrcholu v_2 (`preorder(v2)`) atd. až po průchod ve vrcholu v_n (`preorder(vn)`). Přitom průchod `preorder(v1)` ve v_1 probíhá tak, že se zpracuje v_1, tj. proběhne `zpracuj(v1)`, a pak dojde k vyvolání průchodů v případných potomcích vrcholu v_1.

Uvažujme kořenový strom na Obr. TADY. Předpokládejme, že `zpracuj(v)` provede vypsání uvedeného u vrcholu v. Při průchodu preorder budou čísla vypsána v pořadí TADY, při průchodu postorder pak v pořadí TADY. Podrobněji, při vyvolání `preorder(1)` TADY ...

U binárních uspořádaných stromů se někdy používá průchod metodou *inorder*.

```
inorder(v)
{
 je-li v1 prvni potomek vrcholu v, zpracuj(v1);
 zpracuj(v);
 je-li v1 prvni potomek vrcholu v, zpracuj(v2).
}
```

Vráťme se k Obr. TADY. Při průchodu inorder budou postupně vypsána čísla TADY.

Shrnutí

Stromy jsou speciální grafy, které lze definovat několika ekvivalentními způsoby, např. jako grafy bez kružnic. Stromy mají četné aplikace v informatice. Speciálními případy stromů jsou m-ární stromy, kořenové stromy, uspořádané kořenové stromy. Pro stromy jsou odvozeny užitečné vztahy mezi jejich charakteristikami.

Pojmy k zapamatování

- strom, list, kostra,
- kořenový strom, úroveň vrcholu, hloubka stromu, vyvážený strom,
- m-ární strom, uspořádaný kořenový strom, preorder, postorder, inorder.

Kontrolní otázky

1. *Co je to strom? Uveďte několik definic. Je strom totéž co kostra?*
2. *Proč se pojmy úrověň vrcholu a hloubka stromu zavádějí až pro kořenové stromy. Jaká je největší možná hloubka kořenového stromu s n vrcholy?*
3. *Je každý m-ární strom vyvážený?*

Cvičení

1. Nechť $\langle\langle V, E\rangle, r\rangle$ je kořenový strom a $v \in V$. Ukažte, že podgraf G_v indukovaný množinou $V_v = \{u \in V \mid$ cesta z u do r prochází vrcholem $v\}$ je strom (tzv. podstrom indukovaný vrcholem v). Ukažte také, že $u \in V_v$, právě když úroveň vrcholu u je větší nebo rovna úrovni vrcholu v a existuje cesta z u do v, která neprochází kořenem r.
2. Ukažte, že v úplném n-árním stromu, který má n vrcholů, l listů a i vnitřních vrcholů (ty, které nejsou listy) platí (a) $n = mi + 1$, (b) $l = (m-1)i + 1$, (c) $i = (l-1)/(m-1)$.
3. Jaký je nejmenší počet listů úplného m-árního stromu výšky h? Jaký je nejmenší počet vrcholů úplného m-árního stromu výšky h?

Úkoly k textu

1. Dokažte podrobně Větu 4.24.
2. Dokažte, že v kořenovém stromu má každý vrchol právě jednoho rodiče.

Řešení

1. G_v neobsahuje kružnici, protože je to podgraf stromu, a ten neobsahuje kružnici. Zbývá ukázat, že G_v je souvislý. Když $u, w \in V_v$, pak dle definice cesta ta je ve stromu jediná) z u do r i cesta z w do r prochází vrcholem v. Vezmeme-li úseky z u do v (z první cesty) a z v do w (z druhé cesty), jejich spojením dostaneme cestu z u do w. Tedy G_v je souvislý, a tedy je to strom. Vezměme $u \in V_v$. Pak existuje cesta z u do r, která prochází v, tedy dle definice je úroveň u je větší nebo rovna úrovni v a existuje cesta z u do v, která neprochází kořenem r. Když je úroveň u je větší nebo rovna úrovni v a existuje cesta z u do v, která neprochází kořenem r, uvažujme cestu z u do r. Ta musí obsahovat v. Jinak by by hloubka u byla menší než hloubka v nebo by cesta vzniklá spojením cesty z u do r a cesty z r do v byla cestou z u do v, která obsahuje r (podrobně rozeberte).
2. Snadné, plyne téměř přímo z definic a základních vztahů.
3. Představte si, jak vypadá takový strom s nejméně vrcholy. Obsahuje kořen a v každé z následujících h úrovní má právě m vrcholů. Má tedy $1 + h \cdot m$ vrcholů (1 kořen plus m vrcholů v každé z h úrovní) a $(m-1)(h-1) + m$ listů (v 1. až $(h-1)$. úrovni po $m-1$ listech, v poslední úrovni m listů).

5 Relace (znovu u relací)

Studijní cíle: Po prostudování kapitoly by student měl znát běžné vlastnosti binárních relací na množině, jejich vzájemné vztahy a měl by mít představu o elementárních technikách, jak tyto vztahy rozpoznat. Dále by měl bých schopen k dané relaci najít její reflexivní, symetrický a tranzitivní uzávěr.

Klíčová slova: antisymetrie, asymetrie, irreflexivita, mocnina relace, reflexivita, relace, symetrie, tranzitivita, uzávěr (reflexivní, symetrický, tranzitivní), úplnost

Potřebný čas: 90 minut.

5.1 Binární relace na množině

V kapitole 2.3 jsme zavedli pojem *relace* jakožto matematický protějšek běžně používaného pojmu *vztah.* Nyní se zaměříme na další vlastnosti a práci s relacemi, konkrétně s binárními relacemi na množině. Zopakujme, že binární relace R na množině $X \neq \emptyset$ je podmnožina kartézského součinu $X \times X$, to jest $R \subseteq X \times X$. Binární relace na množině jsou tedy matematickým protějškem vztahů mezi dvěma prvky množiny, například „x je menší než y“, „x má stejnou barvu jako y“, „x nezávisí na y“, ... Speciálními relacemi jsou *prázdná relace* $\emptyset$, *relace identity* $\omega_X = \{\langle x, x\rangle | \, x \in X\}$, a *kartézský čtverec* $\iota_X = X \times X$.

Mnohé binární relace mají podobné vlastnosti a to i přesto, že jsou definovány na různých nosičích. Vezměme například množinu přirozených čísel $\mathbb{N}$ a definujme binární relaci R na $\mathbb{N}$:

$$R = \{\langle m, n\rangle | \, m \text{ má stejný počet cifer jako } n\} .$$

Dále uvažujme, že X označuje množinu všech lidí (z daného regionu) a definujme binární relaci R' na X následujícím předpisem

$$R' = \{\langle x, y\rangle | \, \text{rozdíl měsíčních příjmů } x \text{ a } y \text{ je menší než 10 000 Kč}\} .$$

Různé relace mohou mít analogické vlastnosti.

I když mají relace R, R' odlišené (námi přisouzené) interpretace, mají několik společných vlastností. Platí například, $\langle n, n\rangle \in R$ („n má stejný počet cifer jako n“) pro každé číslo $n \in \mathbb{N}$, analogicky $\langle x, x\rangle \in R'$ („rozdíl příjmů x a x je menší než 10 000 Kč“) pro každého člověka $x \in X$. Pro obě relace R, R' dále platí: pokud $\langle m, n\rangle \in R$, pak i $\langle n, m\rangle \in R$; pokud $\langle x, y\rangle \in R'$, pak i $\langle y, x\rangle \in R'$. V následující definici zavedeme vlastnosti binárních relací na množině.

Definice 5.1. Nechť R je binární relace na X. Řekneme, že R je

(i) *reflexivní,* pokud pro každé $x \in X$ platí $\langle x, x\rangle \in R$,
(ii) *irreflexivní,* pokud pro každé $x \in X$ platí $\langle x, x\rangle \notin R$,
(iii) *symetrická,* pokud pro každé $x, y \in X$ platí $\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \in R$,
(iv) *asymetrická,* pokud pro každé $x, y \in X$ platí $\langle x, y\rangle \in R \Rightarrow \langle y, x\rangle \notin R$,
(v) *antisymetrická,* pokud pro každé $x, y \in X$ platí $(\langle x, y\rangle \in R \wedge \langle y, x\rangle \in R) \Rightarrow x = y$,
(vi) *úplná,* pokud pro každé $x, y \in X$ platí $\langle x, y\rangle \in R \vee \langle y, x\rangle \in R$,
(vii) *tranzitivní,* pokud pro každé $x, y, z \in X$ platí $(\langle x, z\rangle \in R \wedge \langle z, y\rangle \in R) \Rightarrow \langle x, y\rangle \in R$.

Vlastnosti relací uvedené v definici 5.1 mají přirozenou interpretaci a u konečných binárních relací je lze vyčíst z jejich maticové a grafové reprezentace. Předpokládejme, že máme dánu binární relaci R na X.

- *Reflexivita* relace R vyjadřuje, že každý prvek $x \in X$ je v relaci R „sám ze sebou“. Relace R je reflexivní, právě když má binární matice $\mathbf{M}^R$ na diagonále samé jedničky, což je právě když je v orientovaném grafu $\langle X, R\rangle$ relace R u každého vrcholu „smyčka“.

- *Irreflexivita* relace R vyjadřuje, že *žádný* prvek $x \in X$ není v relaci R „sám se sebou“. Relace R je irreflexivní, právě když má binární matice $\mathbf{M}^R$ na diagonále samé nuly, což je právě když u žádného vrcholu orientovaného grafu $\langle X, R\rangle$ není „smyčka“. Relace nemůže být zároveň reflexivní a irreflexivní, nemusí mít ale ani jednu vlastnost z těchto dvou.
- *Symetrie* relace R vyjadřuje, že $\langle x, y\rangle \in R$, právě když $\langle y, x\rangle \in R$. To jest relace je symetrická pokud pro každé $x, y \in X$ máme buď současně $\langle x, y\rangle \in R$ a $\langle y, x\rangle \in R$, nebo současně $\langle x, y\rangle \notin R$ a $\langle y, x\rangle \notin R$. Relace R je symetrická, právě když její binární matice $\mathbf{M}^R$ je *symetrická podle diagonály,* to jest právě když je transponovaná matice $(\mathbf{M}^R)^T$ shodná s $\mathbf{M}^R$. V grafu relace se symetrie projevuje tak, že mezi vrcholy x, y buď není žádná hrana, nebo vede hrana z x do y i z y do x.
- *Asymetrie* relace R vyjadřuje, že do R nepadnou $\langle x, y\rangle$ a $\langle y, x\rangle$ současně. To jest relace je asymetrická pokud pro každé $x, y \in X$ máme buď současně $\langle x, y\rangle \notin R$ a $\langle y, x\rangle \notin R$, nebo do R padne právě jedna z dvojic $\langle x, y\rangle$ a $\langle y, x\rangle$. Z asymetrie přímo plyne irreflexivita, tím pádem asymetrie vylučuje reflexivitu. Pokud je relace R symetrická a asymetrická současně, pak $R = \emptyset$.
- *Antisymetrie* relace R vyjadřuje, že pro každé dva *různé* prvky $x, y \in X$ neplatí současně $\langle x, y\rangle \in R$ a $\langle y, x\rangle \in R$. R je antisymetrická, právě když každá dvě různá pole matice $\mathbf{M}^R$, která jsou souměrná podle diagonály, neobsahují dvě jedničky. V grafu relace se antisymetrie projevuje tak, že mezi dvěma různými vrcholy x, y je buď jedna hrana, nebo žádná. Z asymetrie plyne antisymetrie (obráceně obecně neplatí). Je-li R současně symetrická i antisymetrická, pak platí $R \subseteq \omega_X$.
- *Úplnost* relace R vyjadřuje, že pro každé dva $x, y \in X$ aspoň jedna z dvojic $\langle x, y\rangle, \langle y, x\rangle$ padne do R. Úplnost implikuje reflexivitu, to jest irreflexivita vylučuje úplnost, tím pádem i asymetrie vylučuje úplnost. R je úplná, právě když každá dvě pole matice $\mathbf{M}^R$, která jsou souměrná podle diagonály, obsahují aspoň jednu jedničku. V grafu $\langle X, R\rangle$ lze úplnost poznat tak, že mezi každými dvěma vrcholy vede aspoň jedna hrana.
- *Tranzitivita* relace R vyjadřuje, že pokud $\langle x, y\rangle \in R$ a pokud $\langle y, z\rangle \in R$, pak také $\langle x, z\rangle \in R$, to jest neformálně: pokud je x ve vztahu R s y (v grafu $\langle X, R\rangle$ vede hrana z x do y) a pokud je y ve vztahu R se z (v grafu $\langle X, R\rangle$ vede hrana z y do z), pak je i x ve vztahu R se z (v grafu $\langle X, R\rangle$ vede hrana z x do z). Řečeno ještě jinak, pokud v grafu $\langle X, R\rangle$ můžeme přejít z vrcholu x do vrcholu y po dvou hranách přes vrchol z, pak lze přejít x do y přímo (z x do y vede hrana).

Vlastnosti konečných relací je možné testovat zcela mechanicky prostě tím, že ověříme, zda-li platí definiční podmínky dané vlastnosti. Uvědomte si, že k prokázání, že daná vlastnost neplatí stačí najít jen jednu n-tici prvků, pro kterou definiční předpis neplatí – taková n-tice prvků nám slouží jako *protipříklad.* Například k tomu abychom zjistili, že relace R na X není symetrická stačí najít $x, y \in X$ tak, že $\langle x, y\rangle \in R$, ale $\langle y, x\rangle \notin R$. Pokud chceme ukázat, že vlastnost pro danou R platí, musíme provést test pro všechny prvky. Problém testování vlastností relací nastává v případě, kdy X je nekonečná množina – zde již mechanické testování „přes všechny prvky“ obecně nelze použít. V tomto případě lze obecně doporučit snažit se vysledovat vlastnosti relací z jejich popisu (definice) a poté je dokázat nebo vyvrátit protipříkladem. Někdy pomáhá představit si pouze konečnou podmnožinu X, vysledovat vlastnosti R zúžené na tuto konečnou podmnožinu a pak se je snažit dokázat obecně.

Příklad 5.2. (1) Nejprve si uvědomme vlastnosti speciálních relací $\emptyset, \omega_X$ a ι_X. $\emptyset$ je irreflexivní, symetrická, asymetrická, antisymetrická a tranzitivní, evidentně však není úplná ani reflexivní. ω_X je reflexivní, symetrická, antisymetrická a tranzitivní, není irreflexivní a není asymetrická. ω_X je úplná, právě když $|X| = 1$. ι_X je reflexivní, symetrická, tranzitivní a úplná, není irreflexivní, není asymetrická. ι_X je antisymetrická, právě když $|X| = 1$.

(2) Mějme dánu množinu $X = \{a, b, c, d\}$ a binární relaci R na X, kde

$$R = \{\langle a,a\rangle, \langle a,d\rangle, \langle b,b\rangle, \langle b,d\rangle, \langle c,a\rangle, \langle c,b\rangle, \langle c,c\rangle, \langle c,d\rangle, \langle d,d\rangle\}\,.$$

R je reflexivní, antisymetrická a tranzitivní (ostatní vlastnosti uvedené v definici 5.1 nemá).

(3) Vrátíme-li se nyní k motivačním příkladům z úvodu kapitoly, pak pro

$$R = \{\langle m,n\rangle \mid m \text{ má stejný počet cifer jako } n\}\,.$$

definovanou na množině celých čísel platí, že R je reflexivní, symetrická, tranzitivní (ostatní vlastnosti nemá). Relace

$$R' = \{\langle x,y\rangle \mid \text{rozdíl měsíčních příjmů } x \text{ a } y \text{ je menší než } 10\,000 \text{ Kč}\}\,.$$

je reflexivní a symetrická, ale obecně nemusí být tranzitivní (pokuste se vymyslet protipříklad).

(4) Mějme relaci R na množině celých čísel danou $R = \{\langle m,n\rangle \mid m - 2 \leq n\}$. R je reflexivní, protože $m - 2 \leq m$. R není tranzitivní, protože $4 - 2 \leq 2$, $2 - 2 \leq 0$, ale $4 - 2 \not\leq 0$, to jest $\langle 4,2\rangle \in R$, $\langle 2,0\rangle \in R$, ale $\langle 4,0\rangle \notin R$. R je úplná, protože pro libovolná $m, n \in \mathbb{Z}$ máme buď $m \leq n$ (potom tím spíš $m - 2 \leq n$, tedy $\langle m,n\rangle \in R$), nebo $n \leq m$ (potom $\langle n,m\rangle \in R$). R není symetrická, protože třeba $\langle 5,2\rangle \notin R$ a $\langle 2,5\rangle \in R$. R není asymetrická, protože je reflexivní. R není antisymetrická, protože $\langle 1,2\rangle \in R$ a $\langle 2,1\rangle \in R$.

(5) Uvažujme libovolnou množinu U, dále zavedeme binární relaci R na 2^U následujícím předpisem: $R = \{\langle A,B\rangle \mid A, B \in 2^U \text{ a } A \text{ je podmnožina } B\}$. Relace R je reflexivní, antisymetrická a tranzitivní. Tuto relaci jsme si zavedli již v kapitole 2.2.3 na straně 26 jako množinovou inkluzi a fakt $\langle A,B\rangle \in R$ jsme zapisovali $A \subseteq B$. Analogicky bychom mohli chápat množinovou rovnost $A = B$ jako vyjádření příslušnosti $\langle A,B\rangle$ k průniku $R \cap R^{-1} = \omega_{2^U}$ (zdůvodněte proč).

Průvodce studiem

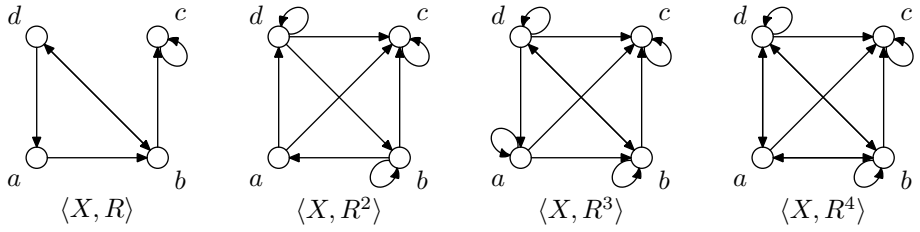
Asymetrii a antisymetrii nelze zaměňovat. Každá asymetrická relace je antisymetrická, ale obecně to neplatí obráceně. Například relace ω_X je antisymetrická, ale není asymetrická. Volně řečeno, antisymetrie vyjadřuje „téměř totéž co asymetrie“, až na prvky vyskytující se na diagonále. Platí, že antisymetrická relace je asymetrická, právě když je irreflexivní.

Věta 5.3. *Nechť R je binární relace na X. Pak*

(i) *R je reflexivní, právě když $\omega_X \subseteq R$,*
(ii) *R je irreflexivní, právě když $\omega_X \cap R = \emptyset$,*
(iii) *R je symetrická, právě když $R = R^{-1}$,*
(iv) *R je asymetrická, právě když $R \cap R^{-1} = \emptyset$,*
(v) *R je antisymetrická, právě když $R \cap R^{-1} \subseteq \omega_X$,*
(vi) *R je úplná, právě když $R \cup R^{-1} = \iota_X$,*
(vii) *R je tranzitivní, právě když $R \circ R \subseteq R$.*

Důkaz. Tvrzení (i), (ii), (iii), (iv) a (vi) jsou zřejmá.
(v): Nechť R je antisymetrická a nechť $\langle x,y\rangle \in R \cap R^{-1}$. Pak $\langle x,y\rangle \in R$ a $\langle x,y\rangle \in R^{-1}$, tedy $\langle y,x\rangle \in R$. Odtud $x = y$, tedy $\langle x,y\rangle \in \omega_X$. Obráceně, předpokládejme $R \cap R^{-1} \subseteq \omega_X$. Pro $\langle x,y\rangle \in R$ a $\langle y,x\rangle \in R$ máme $\langle x,y\rangle \in R^{-1}$, tedy $\langle x,y\rangle \in R \cap R^{-1} \subseteq \omega_X$, z čehož $x = y$. Relace R je tedy antisymetrická.
(vii): Nechť R je tranzitivní a nechť $\langle x,y\rangle \in R \circ R$. Pak existuje $z \in X$ takové, že $\langle x,z\rangle \in R$ a $\langle z,y\rangle \in R$, tedy z tranzitivity $\langle x,y\rangle \in R$, to jest $R \circ R \subseteq R$. Obráceně, nechť platí $R \circ R \subseteq R$, pak pokud $\langle x,z\rangle \in R$ a $\langle z,y\rangle \in R$, pak $\langle x,y\rangle \in R \circ R \subseteq R$, tedy R je tranzitivní. □

Nyní zavedeme n-tou mocninu relace pomocí skládání relací.



Obrázek 11: n-tá mocnina relace

Definice 5.4. Nechť R je binární relace na X. Pro každé $n \in \mathbb{N}$ definujeme binární relaci R^n na X:

n-tou mocninu relace zavádíme pomocí skládání relací.

$$R^n = \begin{cases} R & \text{pokud } n = 1, \\ R \circ R^{n-1} & \text{jinak.} \end{cases}$$

R^n se nazývá *n-tá mocnina R.*

Dle definice 5.4 máme $R^1 = R$, $R^2 = R \circ R^1 = R \circ R$, $R^3 = R \circ R^2 = R \circ (R \circ R) \ldots$ Podle věty 2.19 na straně 36 navíc platí, že $R^3 = R \circ (R \circ R) = (R \circ R) \circ R$, bez újmy tedy můžeme vynechávat závorky a psát pouze $R^3 = R \circ R \circ R$ a podobně. n-tou mocninu relace R na X lze vyjádřit následujícím způsobem: $\langle x, y\rangle \in R^n$ pokud existují $z_1, \ldots, z_{n-1} \in X$ tak, že

$$\langle x, z_1\rangle \in R, \langle z_1, z_2\rangle \in R, \ldots, \langle z_{n-2}, z_{n-1}\rangle \in R, \langle z_{n-1}, y\rangle \in R. \tag{5.1}$$

Tedy například pro $n = 2$ přejde (5.1) v

$$\langle x, z_1\rangle \in R, \langle z_1, y\rangle \in R,$$

pro $n = 3$:

$$\langle x, z_1\rangle \in R, \langle z_1, z_2\rangle \in R, \langle z_2, y\rangle \in R$$

a tak dále. Význam R^n si pro konečnou X nejlépe uvědomíme na orientovaných grafech příslušných R a R^n. Neformálně řečeno: v grafu R^n vede hrana z x do y (to jest $\langle x, y\rangle \in R^n$), právě když se v grafu R lze dostat z x do y po orientovaných hranách tak, že počet hran, přes které při tom přejdeme je roven n. Vše si demonstrujme na následujícím příkladu.

Příklad 5.5. Mějme binární relaci $R = \{\langle a, b\rangle, \langle b, c\rangle, \langle b, d\rangle, \langle c, c\rangle, \langle d, a\rangle, \langle d, b\rangle\}$ na čtyřprvkové množině $X = \{a, b, c, d\}$. Na obrázku 11 jsou zobrazeny orientované grafy odpovídající relacím $R = R^1$, R^2, R^3 a R^4, matice těchto relací vypadají následovně:

$$\mathbf{M}^R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \mathbf{M}^{R^2} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \mathbf{M}^{R^3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \mathbf{M}^{R^4} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Například $\langle a, b\rangle \in R$, $\langle b, d\rangle \in R$ a $\langle d, a\rangle \in R$, máme tedy $\langle a, a\rangle \in R^3$ – neformálně řečeno, z a jsme se dostali do a cestou přes tři hrany: $\langle a, b\rangle$, $\langle b, d\rangle$ a $\langle d, a\rangle$. Na druhou stranu ale třeba $\langle a, a\rangle \notin R^4$, protože neexistuje žádná „cesta z a do a“ přes čtyři hrany. Na tomto příkladu si dále všimněte, že obecně neplatí $R^n \subseteq R^{n+1}$, zde konkrétně $R^3 \nsubseteq R^4$.

V následujícím tvrzení si uvedeme některé další vlastnosti skládání a mocnění relací.

Věta 5.6. *Nechť R, S, T jsou binární relace na X, kde $S \subseteq T$. Pak*

(i) $S^{-1} \subseteq T^{-1}$,
(ii) $R \circ S \subseteq R \circ T$ *a* $S \circ R \subseteq T \circ R$,
(iii) *pokud je R tranzitivní, pak $R^n \subseteq R$ pro každé $n \in \mathbb{N}$,*
(iv) $R^m \circ R^n = R^{m+n} = R^n \circ R^m$ *pro každé $m, n \in \mathbb{N}$,*
(v) *pokud $|X| \leq n$ a $\langle x, y\rangle \in R^{n+1}$, pak $\langle x, y\rangle \in R^m$ pro nějaké $m \in \mathbb{N}$ splňující $m \leq n$.*

Důkaz. (i) je zřejmé.
(ii): Dokážeme $R \circ S \subseteq R \circ T$, druhý vztah se dokazuje analogicky. Nechť $\langle x, y\rangle \in R \circ S$, pak tedy existuje $z \in X$ tak, že $\langle x, z\rangle \in R$ a $\langle z, y\rangle \in S$. Jelikož ale $S \subseteq T$, dostáváme $\langle z, y\rangle \in T$, tedy $\langle x, y\rangle \in R \circ T$. Tím jsme dokázali $R \circ S \subseteq R \circ T$.
(iii): Triviálně $R^1 \subseteq R$. Indukcí ukážeme, že pokud tvrzení $R^n \subseteq R$ platí pro $n \in \mathbb{N}$, pak platí i pro $n + 1$. Nechť tedy $R^n \subseteq R$. Jelikož je R tranzitivní relace, pak dle (ii) věty 5.6 a dle (vii) věty 5.3 dostáváme $R^{n+1} = R \circ R^n \subseteq R \circ R \subseteq R$.
(iv) plyne z definice a užitím věty 2.19 na straně 36.
(v): Mějme $|X| \leq n$, to jest X je nejvýš n-prvková množina a nechť $\langle x, y\rangle \in R^{n+1}$. Dle definice 5.4 tedy existují elementy $z_1, \ldots, z_n \in X$ takové, že

$$\langle x, z_1\rangle \in R, \langle z_1, z_2\rangle \in R, \ldots, \langle z_{n-1}, z_n\rangle \in R, \langle z_n, y\rangle \in R.$$

Označíme-li $z_0 = x$, pak má posloupnost $z_0, \ldots, z_n$ právě $n + 1$ prvků, což vzhledem k počtu prvků množiny X (předpokládáme $|X| \leq n$) znamená, že musí existovat indexy $i, j \in \{0, \ldots, n\}$ takové, že $i < j$ a $z_i = z_j$. Vezmeme-li nyní posloupnost dvojic

$$\langle z_0, z_1\rangle \in R, \langle z_1, z_2\rangle \in R, \ldots, \langle z_{i-1}, z_i\rangle \in R, \langle z_j, z_{j+1}\rangle \in R, \ldots, \langle z_{n-1}, z_n\rangle \in R, \langle z_n, y\rangle \in R,$$

kterou jsme získali vyjmutím $(j - i)$ dvojic $\langle z_k, z_{k+1}\rangle$ $(i \leq k < j)$ z výchozí posloupnosti, pak zřejmě dostáváme $\langle x, y\rangle \in R^{n+1-(j-i)}$. Hledané $m \in \mathbb{N}$ je tedy například $m = n + 1 - (j - i)$. □

5.2 Uzávěry relací

Binární relace se často používají k popisu stavů systému a jejich návaznosti. Mějme množinu stavů X, ve kterých se může nacházet nějaký systém (například přístroj se může nacházet ve stavech „zapnut“, „v pohotovosti“, „v činnosti“, „vypnut“, . . . ; tržní ekonomika se může nacházet ve stavu „konjunktury“, „inflace“, „deflace“, „stagflace“, „recese“, „deprese“, . . .). Předpokládejme, že R je binární relace na X s významem: $\langle x, y\rangle \in R$, právě když „systém může (v jednom kroku) přejít ze stavu x do stavu y“. Relace R (tak zvaná *přechodová relace*) nemusí být obecně tranzitivní: těžko si lze představit, že například ekonomika přejde přímo z „deprese“ do „konjunktury“. Kdybychom navíc na X definovali další binární relaci R' jakožto relaci *dosažitelnosti stavů* v obecně více krocích, pak by R' byla přirozeně *tranzitivní* a měla by navíc úzký vztah k přechodové relaci R: R by byla obsažena v R' a R' by byla nejmenší (ve smyslu množinové inkluze $\subseteq$) ze všech tranzitivních relací na X obsahujících R. Tento a podobné typy vztahů mezi relacemi si nyní zavedeme přesně.

Definice 5.7. Pro binární relaci R na X definujeme binární relace $\mathrm{Ref}(R), \mathrm{Sym}(R), \mathrm{Tra}(R)$ na X tak, že $\mathrm{Ref}(R)$ ($\mathrm{Sym}(R)$, případně $\mathrm{Tra}(R)$) je reflexivní (symetrická, případně tranzitivní) relace obsahující R a pro každou reflexivní (symetrickou, případně tranzitivní) relaci R' na X, kde $R \subseteq R'$, máme $\mathrm{Ref}(R) \subseteq R'$ ($\mathrm{Sym}(R) \subseteq R'$, případně $\mathrm{Tra}(R) \subseteq R'$). $\mathrm{Ref}(R)$ se nazývá *reflexivní uzávěr* R, $\mathrm{Sym}(R)$ se nazývá *symetrický uzávěr* R, $\mathrm{Tra}(R)$ se nazývá *tranzitivní uzávěr* R.

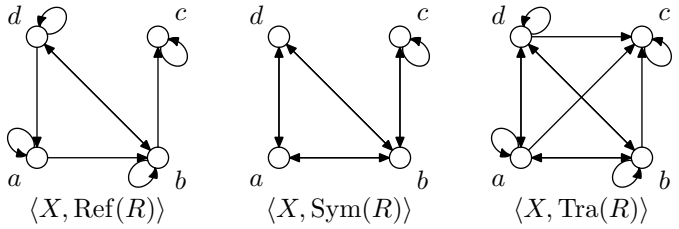
Předchozí definice je nekonstruktivní, neříká nic o tom, jak relace $\mathrm{Ref}(R)$, $\mathrm{Sym}(R)$ a $\mathrm{Tra}(R)$ vypadají a dokonce z ní ani přímo neplyne, zda takové relace existují pro každou R. V následující větě si ukážeme, že všechny výše uvedené uzávěry existují vždy ke každé binární relaci na libovolné množině a lze je konstruktivně popsat.

Věta 5.8. *Nechť R je binární relace na X. Pak*

$$\mathrm{Ref}(R) = R \cup \omega_X, \tag{5.2}$$

$$\mathrm{Sym}(R) = R \cup R^{-1}, \tag{5.3}$$

$$\mathrm{Tra}(R) = \textstyle\bigcup_{n=1}^{\infty} R^n. \tag{5.4}$$



Obrázek 12: Reflexivní, symetrický a tranzitivní uzávěr relace

Důkaz. Tvrzení pro $\mathrm{Ref}(R)$ je zřejmé.
Položme $S = R \cup R^{-1}$. Nyní prokážeme, že $\mathrm{Sym}(R) = S$. Platí $S^{-1} = (R \cup R^{-1})^{-1} = R^{-1} \cup (R^{-1})^{-1} = R^{-1} \cup R = S$. To jest S je symetrická dle bodu (iii) věty 5.3 a evidentně $R \subseteq S$. Mějme symetrickou relaci S' na X takovou, že $R \subseteq S'$. Nechť $\langle x, y\rangle \in S = R \cup R^{-1}$. Pokud $\langle x, y\rangle \in R$, pak triviálně $\langle x, y\rangle \in S'$. Pokud $\langle x, y\rangle \notin R$, pak $\langle x, y\rangle \in R^{-1}$, tedy $\langle y, x\rangle \in R$, to jest $\langle y, x\rangle \in S'$. Jelikož je S' symetrická, dostáváme odtud $\langle x, y\rangle \in S'$. Prokázali jsme tedy $S \subseteq S'$ a dohromady $\mathrm{Sym}(R) = R \cup R^{-1}$.
Položme $T = \bigcup_{n=1}^{\infty} R^n$, to jest $T = R^1 \cup R^2 \cup R^3 \cup \cdots$. Evidentně $R \subseteq T$. Ověříme tranzitivitu T: nechť $\langle x, z\rangle \in T$ a $\langle z, y\rangle \in T$. Z definice T plyne, že existují $m, n \in \mathbb{N}$ taková, že $\langle x, z\rangle \in R^m$ a $\langle z, y\rangle \in R^n$. Tedy $\langle x, y\rangle \in R^m \circ R^n = R^{m+n} \subseteq T$. Mějme tranzitivní relaci T' na X takovou, že $R \subseteq T'$. Pak dle bodů (ii) a (iii) věty 5.6 platí $R^n \subseteq (T')^n \subseteq T$ pro každé $n \in \mathbb{N}$. Odtud máme $T \subseteq T'$, tedy $\mathrm{Tra}(R) = \bigcup_{n=1}^{\infty} R^n$. □

Vztahu (5.4) je třeba rozumět tak, že výsledný tranzitivní uzávěr $\mathrm{Tra}(R)$ dostaneme tím, že sjednotíme nekonečně mnoho relací $R^1 \cup R^2 \cup R^3 \cup \cdots \cup R^n \cup R^{n+1} \cup \cdots$. Z pohledu informatika je toto vyjádření tranzitivního uzávěru pořád nekonstruktivní, protože pro vstupní relaci R nedává předpis pro algoritmus, který by vždy po *konečně mnoha krocích výpočtu* stanovil relaci $\mathrm{Tra}(R)$. Pokud je ale R definovaná na konečné množině X, pak jako důsledek bodu (v) věty 5.6 dostáváme, že $R^k \subseteq \bigcup_{i=1}^{n} R^i$ pro každé $k \in \mathbb{N}$, kde $k > n = |X|$. To jest máme

Důsledek 5.9. *Nechť R je binární relace na X, kde $|X| = n$. Pak* $\mathrm{Tra}(R) = \bigcup_{i=1}^{n} R^i$. □

Příklad 5.10. (1) Vezměme relaci R z příkladu 5.5. Na obrázku 12 jsou zobrazeny orientované grafy odpovídající reflexivnímu, symetrickému a tranzitivnímu uzávěru R, matice těchto relací vypadají následovně (pro přehlednost jsou nově přidané prvky zvýrazněny barevně):

$$\mathbf{M}^{\mathrm{Ref}(R)} = \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 \\ 0 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & \mathbf{1} \end{pmatrix}, \quad \mathbf{M}^{\mathrm{Sym}(R)} = \begin{pmatrix} 0 & 1 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 1 & 1 \\ 0 & \mathbf{1} & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{M}^{\mathrm{Tra}(R)} = \begin{pmatrix} \mathbf{1} & 1 & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & \mathbf{1} & \mathbf{1} \end{pmatrix}.$$

(2) Mějme binární relaci R na množině přirozených čísel $\mathbb{N}$ definovánu $R = \{\langle m, n\rangle \mid m + 1 = n\}$. Relace R je irreflexivní, asymetrická, antisymetrická a není tranzitivní. Fakt $\langle m, n\rangle \in R$ lze intuitivně chápat jako „m je bezprostřední předchůdce n v množině přirozených čísel“. Pro $\mathrm{Tra}(R)$ máme $\langle m, n\rangle \in \mathrm{Tra}(R)$, právě když $m < n$. Na tomto příkladu je dobré uvědomit si, že v případě relací na nekonečných množinách můžeme mít $\bigcup_{i=1}^{n} R^i \subset \mathrm{Tra}(R)$ pro každé $n \in \mathbb{N}$. V tomto konkrétním případě: pro libovolné $n \in \mathbb{N}$ máme $\langle 1, n+2\rangle \in \mathrm{Tra}(R)$, ale $\langle 1, n+2\rangle \notin \bigcup_{i=1}^{n} R^i$. To jest důsledek 5.9 obecně nelze rozšířit pro relace na nekonečných množinách.

Průvodce studiem

Pokud binární relaci R na X interpretujeme jako přechodovou relaci, pak tranzitivní uzávěr $\mathrm{Tra}(R)$ relace R má přirozenou interpretaci jako relace dosažitelnosti. Tranzitivní uzávěry relací se často používají v informatice, například v teorii automatů: pokud R popisuje

možnost změny stavu (elementární krok výpočtu) nějakého abstraktního výpočetního stroje, pak $\mathrm{Tra}(R)$ lze chápat jako relaci, která určuje „výpočet“, to jest $\langle x, y\rangle \in \mathrm{Tra}(R)$, pokud stroj během výpočtu začínajícího ve stavu x dojde do stavu y.

Shrnutí

Binární relace na dané množině lze chápat jako matematický protějšek vztahů mezi dvěma objekty dané množiny. Při zkoumání vlastností binárních relací na množině zavádíme abstraktní vlastnosti relací a zkoumáme jejich vzájemné vztahy. Mezi nejčastěji uvažované vlastnosti patří reflexivita, symetrie, antisymetrie, tranzitivita a úplnost. Ke každé relaci můžeme navíc stanovit její reflexivní, symetrický nebo tranzitivní uzávěr, to jest nejmenší reflexivní, symetrickou nebo tranzitivní relaci na dané množině, která obsahuje výchozí relaci.

Pojmy k zapamatování

- reflexivita, irreflexivita,
- symetrie, asymetrie, antisymetrie,
- úplnost,
- tranzitivita,
- mocnina relace,
- reflexivní uzávěr, symetrický uzávěr, tranzitivní uzávěr

Kontrolní otázky

1. *Existuje úplná a symetrická relace na X různá od ι_X?*
2. *Jaký je vztah mezi asymetrickými a antisymetrickými relacemi?*
3. *Platí, že relace je irreflexivní, právě když není reflexivní?*
4. *Jaký význam má tranzitivní uzávěr relace a jak jej lze najít?*

Cvičení

1. Zjistěte, jaké vlastnosti mají následující relace R na X.
   (a) $X = \mathbb{Z}$, $R = \{\langle m, n\rangle \mid m$ dělí n beze zbytku$\}$.
   (b) $X = \{a, b, c, d\}$, $R = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle b, c\rangle\}$.
   (c) $X = \mathbb{Z} \times \mathbb{Z}$, $R = \{\langle\langle m, m'\rangle, \langle n, n'\rangle\rangle \mid m \leq n$ a $m' \leq n'\}$.
   (d) $X = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $R = \{\langle m, n\rangle \mid m - n \leq 2\}$.
2. Najděte relaci R na $X = \{a, b, c, d\}$, tak aby
   (a) R byla reflexivní, tranzitivní, úplná a nebyla ani symetrická, ani antisymetrická,
   (b) R byla reflexivní, antisymetrická a nebyla tranzitivní,
   (c) R byla tranzitivní a asymetrická a zároveň $R \cup \omega_X$ byla úplná,
   (d) $\mathrm{Sym}(\mathrm{Tra}(R))$ nebyla tranzitivní.
3. Mějme relaci $R = \{\langle a, d\rangle, \langle c, d\rangle, \langle d, a\rangle\}$ na množině $X = \{a, b, c, d, e, f\}$.
   Stanovte $\mathrm{Ref}(R)$, $\mathrm{Sym}(R)$, $\mathrm{Tra}(R)$, $\mathrm{Sym}(\mathrm{Tra}(R))$, $\mathrm{Tra}(\mathrm{Sym}(R))$, $\mathrm{Tra}(\mathrm{Sym}(\mathrm{Ref}(R)))$.

Úkoly k textu

1. Mějme reflexivní relaci R na X, kde $|X| = n$. Dokažte, že $\mathrm{Tra}(R) = R^n$.

Řešení

1. Relace mají právě tyto vlastnosti
   (a) reflexivita, tranzitivita, (nesplňuje: irreflexivita, symetrie, asymetrie, antisymetrie, úplnost),
   (b) nesplňuje ani jednu vlastnost z definice 5.1,
   (c) reflexivita, tranzitivita, antisymetrie, (nesplňuje: irreflexivita, symetrie, asymetrie, úplnost),
   (d) reflexivita, úplnost, (nesplňuje: irreflexivita, symetrie, asymetrie, antisymetrie, tranzitivita).
2. Relace mají například následující tvar:
   (a) $R = \iota_X - \{\langle a,b\rangle, \langle a,c\rangle, \langle a,d\rangle\}$,
   (b) $R = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,b\rangle, \langle b,c\rangle, \langle c,c\rangle, \langle d,d\rangle\}$,
   (c) $R = \{\langle a,b\rangle, \langle a,c\rangle, \langle a,d\rangle, \langle b,c\rangle, \langle b,d\rangle, \langle c,d\rangle\}$,
   (d) $R = \{\langle a,b\rangle\}$.
3. Relace mají následující tvar:

$$\begin{aligned}
\mathrm{Ref}(R) &= \{\langle a,a\rangle, \langle a,d\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,d\rangle, \langle e,e\rangle, \langle f,f\rangle\}\,,\\
\mathrm{Sym}(R) &= \{\langle a,d\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,c\rangle\}\,,\\
\mathrm{Tra}(R) &= \{\langle a,a\rangle, \langle a,d\rangle, \langle c,a\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,d\rangle\}\,,\\
\mathrm{Sym}(\mathrm{Tra}(R)) &= \{\langle a,a\rangle, \langle a,c\rangle, \langle a,d\rangle, \langle c,a\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,c\rangle, \langle d,d\rangle\}\,,\\
\mathrm{Tra}(\mathrm{Sym}(R)) &= \{\langle a,a\rangle, \langle a,c\rangle, \langle a,d\rangle, \langle c,a\rangle, \langle c,c\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,c\rangle, \langle d,d\rangle\}\,,\\
\mathrm{Tra}(\mathrm{Sym}(\mathrm{Ref}(R))) &= \mathrm{Tra}(\mathrm{Sym}(R)) \cup \{\langle b,b\rangle, \langle e,e\rangle, \langle f,f\rangle\}\,.
\end{aligned}$$

Studijní cíle: Po prostudování kapitoly by student měl být seznámen s vlastnostmi nejčastěji používaných binárních relacích na množinách. Student by měl mít přehled o relaci ekvivalence a jejím vztahu k rozkladu na množině a k surjektivním obrazům. Dále by měl být seznámen se základními vlastnostmi a typy uspořádaných množin.

Klíčová slova: antiřetězec, ekvivalence (indukovaná zobrazením / příslušná rozkladu), ekvivalence, faktorová množina, Hasseův diagram, infimum, kužel (dolní, horní), kvaziuspořádání, lineární uspořádání, pokrytí, polosvaz (průsekový, spojový), princip duality, (minimální / nejmenší / maximální / největší) prvek, přirozené zobrazení, rozklad na množině, rozklad příslušný ekvivalenci, řetězec, supremum, svaz, třída ekvivalence / rozkladu, uspořádaná množina, uspořádání

Potřebný čas: 120 minut.

5.3 Ekvivalence

V této podkapitole se budeme zabývat binárními relacemi, které lze interpretovat jako matematické protějšky *nerozlišitelnosti.* Motivace pro zkoumání tohoto fenoménu je v celku jasná. Pokud množina X reprezentuje velkou kolekci prvků, třeba nekonečnou, v některých případech můžeme chtít *ztotožnit* ty prvky z X, které jsou vzájemně nerozlišitelné některou svou vlastností a získat tak „zjednodušený náhled“ na X. Ztotožněním nerozlišitelných prvků můžeme získat množinu „reprezentantů“, která může být výrazně menší než výchozí množina X.

Ztotožněním nerozlišitelných prvků získáme „náhled“ na množinu.

V úvodu kapitoly si nejprve definujeme speciální relaci, která je matematickým protějškem nerozlišitelnosti prvků. Jaké vlastnosti by tato relace měla mít? Určitě by měla být reflexivní, protože každé $x \in X$ je totožné s x, to jest „x nelze rozlišit od x“. Dále by relace měla být i symetrická: „pokud x nelze rozlišit od y, pak i y nelze rozlišit od x“. Další vlastností nerozlišitelnost je tranzitivita: „pokud x nelze rozlišit od y a y nelze rozlišit od z, pak x nelze rozlišit od z“. Uvědomte si, že kdybychom hledali matematický protějšek vlastnosti „být podobný“, pak by již automatické přijetí tranzitivity bylo přinejmenším diskutabilní. Nyní zavedeme relaci ekvivalence jako matematický protějšek nerozlišitelnosti.

Definice 5.11. Reflexivní a symetrická binární relace na množině se nazývá *tolerance*. Tranzitivní tolerance se nazývá *ekvivalence*. Pro ekvivalenci E na množině X definujeme pro každý $x \in X$ množinu $[x]_E = \{y \in X \mid \langle x, y\rangle \in E\}$, kterou nazýváme *třída ekvivalence prvku* x.

Ekvivalence je matematický protějšek nerozlišitelnosti.

Je-li E ekvivalence na X, pak vztah $\langle x, y\rangle \in E$ někdy čteme „x je E-ekvivalentní y“. Vzhledem k tomu, že E je symetrická, můžeme $\langle x, y\rangle \in E$ číst „x a y jsou E-ekvivalentní“. Třída ekvivalence $[x]_E$ je dle definice množina těch prvků $y \in X$, které jsou E-ekvivalentní x. Jinými slovy, $[x]_E$ obsahuje právě ty prvky z X, které nelze od x rozlišit ekvivalencí E.

Příklad 5.12. (1) ω_X a ι_X jsou ekvivalence na X, které navíc mají mezi všemi ekvivalencemi na X výsadní postavení. Relace ω_X musí být dle (i) věty 5.3 obsažena v každé ekvivalenci na X, to jest ω_X je nejmenší ekvivalence na X ve smyslu množinové inkluze $\subseteq$. Pro každý prvek $x \in X$ máme $[x]_{\omega_X} = \{x\}$. Naopak relace ι_X je evidentně největší ekvivalence na X. Pro každý prvek $x \in X$ máme $[x]_{\iota_X} = X$.

(2) Na $X = \{a, b, c\}$ existuje pět vzájemně různých ekvivalencí:

$$\begin{aligned}
\omega_X &= \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle\},\\
E_1 &= \{\langle a,a\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle b,b\rangle, \langle c,c\rangle\},\\
E_2 &= \{\langle a,a\rangle, \langle b,b\rangle, \langle b,c\rangle, \langle c,b\rangle, \langle c,c\rangle\},\\
E_3 &= \{\langle a,a\rangle, \langle a,c\rangle, \langle b,b\rangle, \langle c,a\rangle, \langle c,c\rangle\},\\
\iota_X &= \{\langle a,a\rangle, \langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle b,b\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle c,b\rangle, \langle c,c\rangle\}.
\end{aligned}$$

(3) Uvažujme množinu celých čísel $\mathbb{Z}$ a $m \in \mathbb{N}$ a uvažujme binární relaci $\mathbb{Z}_m \subseteq \mathbb{Z} \times \mathbb{Z}$ definovanou

$$\mathbb{Z}_m = \{\langle a, b\rangle \mid a = b + t \cdot m \text{ pro nějaké } t \in \mathbb{Z}\}\,. \tag{5.5}$$

Snadno lze ukázat, že relace $\mathbb{Z}_m$ je ekvivalence na $\mathbb{Z}$. Podrobně, $\mathbb{Z}_m$ je zcela jistě reflexivní, platí $a = a + 0 \cdot m$, odtud plyne $\langle a, a\rangle \in \mathbb{Z}_m$. Pokud $\langle a, b\rangle \in \mathbb{Z}_m$, pak lze psát $a = b + t \cdot m$ pro nějaké $t \in \mathbb{Z}$. Tento výraz lze upravit na $a - t \cdot m = b$. Z vlastností součtu a součinu plyne $b = a + (-t) \cdot m$, to jest $\langle b, a\rangle \in \mathbb{Z}_m$ – relace je symetrická. Zbývá ověřit tranzitivitu: uvažujme $\langle a, b\rangle \in \mathbb{Z}_m$, $\langle b, c\rangle \in \mathbb{Z}_m$. Existují tedy $s, t \in \mathbb{Z}$, kde $a = b + s \cdot m$, $b = c + t \cdot m$. Dosazením za b dostáváme $a = c + t \cdot m + s \cdot m$, to jest $a = c + (t + s) \cdot m$. Relace $\mathbb{Z}_m$ se nazývá *ekvivalence modulo* m. O číslech $a, b \in \mathbb{Z}$ splňujících $\langle a, b\rangle \in \mathbb{Z}_m$ říkáme, že a *je ekvivalentní* b *modulo* m.

(4) Na $\mathbb{Q}$ můžeme uvažovat binární relaci $R = \{\langle x, y\rangle \mid x, y \in \mathbb{Q},\ |x| = |y|\}$, to jest $\langle x, y\rangle \in R$, právě když mají x a y tutéž absolutní hodnotu. Zcela evidentně jde o ekvivalencí na $\mathbb{Q}$, přitom pro každé $x \in \mathbb{Q}$ máme $[x]_E = \{x, -x\}$. Speciálně máme $[0]_E = \{0\}$.

Další přirozený způsob zachycení informace o nerozlišitelnosti prvků množiny X je jejich „shlukování“ do podmnožin vzájemně nerozlišitelných prvků. Zřejmě každý prvek $x \in X$ je nerozlišitelný sám se sebou, takže ke každému $x \in X$ lze uvažovat neprázdnou podmnožinu $Y_x \subseteq X$ obsahující všechny prvky, které jsou od x nerozlišitelné. Zřejmě máme $X = \bigcup_{x \in X} Y_x$ a intuice také říká, že pokud lze x od x' rozlišit, pak neexistuje žádný prvek $z \in X$, který by byl zároveň nerozlišitelný od x i od x'. Následující definice shrnuje předchozí pozorování:

Definice 5.13. Nechť $X \neq \emptyset$ je množina. Systém množin $\Pi \subseteq 2^X$ splňující

(i) $Y \neq \emptyset$ pro každou $Y \in \Pi$,

(ii) pro každé $Y_1, Y_2 \in \Pi$ platí: pokud $Y_1 \cap Y_2 \neq \emptyset$, pak $Y_1 = Y_2$,

(iii) $\bigcup \Pi = X$,

se nazývá *rozklad na množině* X. Množiny $Y \in \Pi$ nazýváme *třídy rozkladu* Π. Pro prvek $x \in X$ označíme $[x]_\Pi$ tu třídu rozkladu Π, která obsahuje x.

Rozklad na množině je matematický protějšek shluků nerozlišitelných prvků.

Poznámka 5.14. Rozeberme nyní definici 5.13. Rozklad Π na X je systém neprázdných podmnožin X, přitom dle bodu (ii) požadujeme, aby každé dvě různé množiny $Y_1, Y_2 \in \Pi, Y_1 \neq Y_2$ byly disjunktní, to jest $Y_1 \cap Y_2 = \emptyset$, a konečně chceme, aby sjednocení všech množin z Π bylo rovno množině X – někdy proto říkáme, že rozklad na X je *disjunktní pokrytí množiny* X. Mějme například množinu $X = \{1, 2, 3, 4, 5, 6\}$. Například $\Pi_1 = \{\{1, 2\}, \{3, 4\}, \{5\}\}$ není rozklad na X, protože nesplňuje podmínku (iii) definice 5.13 ($6 \notin \bigcup \Pi_1$), stejně tak $\Pi_2 = \{\{1, 2, 3\}, \{3, 4\}, \{5, 6\}\}$ není rozklad na X, protože nesplňuje podmínku (ii) definice 5.13 ($\{1, 2, 3\} \cap \{3, 4\} \neq \emptyset$), na druhou stranu třeba $\{\{1, 5, 3\}, \{4\}, \{2, 6\}\}$ je rozklad na X.

Příklad 5.15. (1) Na množině X existují dva mezní rozklady. První z nich je rozklad Π, kde $[x]_\Pi = \{x\}$ pro každé $x \in X$, to jest všechny třídy rozkladu Π jsou jednoprvkové. Druhým mezním případem je rozklad $\Pi = \{X\}$, to jest Π obsahuje jedinou třídu, která je rovna celé X, tím pádem $[x]_\Pi = X$ pro každé $x \in X$.

(2) Mějme $X = \{a, b, c, d\}$. Na X existuje patnáct vzájemně různých rozkladů:

$$\begin{array}{llll} \{\{a\},\{b\},\{c\},\{d\}\}, & \{\{a,b\},\{c\},\{d\}\}, & \{\{b\},\{a,c\},\{d\}\}, & \{\{b\},\{c\},\{a,d\}\}, \\ \{\{a\},\{b,c\},\{d\}\}, & \{\{a,b,c\},\{d\}\}, & \{\{b,c\},\{a,d\}\}, & \{\{a\},\{c\},\{b,d\}\}, \\ \{\{a,c\},\{b,d\}\}, & \{\{c\},\{a,b,d\}\}, & \{\{a\},\{b\},\{c,d\}\}, & \{\{a,b\},\{c,d\}\}, \\ \{\{b\},\{a,c,d\}\}, & \{\{a\},\{b,c,d\}\}, & \{\{a,b,c,d\}\}. & \end{array}$$

(3) Uvažujme rozklad $\Pi_7 = \{Z_0, Z_1, \ldots, Z_6\}$ na množině celých čísel $\mathbb{Z}$ takový, že každá třída Z_i rozkladu Π_7 obsahuje právě ta celá čísla, která jsou dělitelná číslem 7 se zbytkem i. To jest máme $Z_0 = \{0, 7, -7, 14, -14, \ldots\}$, $Z_1 = \{1, -1, 8, -8, 15, -15, \ldots\}$ a tak dále. Analogicky bychom mohli uvažovat rozklad Π_n pro každé $n \in \mathbb{N}$. Π_n se nazývá *systém zbytkových tříd modulo* n.

(4) Na množině racionálních čísel $\mathbb{Q}$ můžeme uvažovat rozklad Π takový, že pro každé $q \in \mathbb{Q}$ máme $[q]_\Pi = \{q, -q\}$. Jiným rozkladem na $\mathbb{Q}$ může být například systém $\Pi = \{Z, \{0\}, K\}$, kde $Z = \{x \in \mathbb{Q} \mid x < 0\}$, $K = \{x \in \mathbb{Q} \mid x > 0\}$.

Rozklady a ekvivalence vyjadřují de facto totéž.

Pozorný čtenář si jistě všiml, že ukázky rozkladů v předchozím příkladu byly analogické příkladům ekvivalencí z příkladu 5.12. Například je vidět, že v bodu (4) předchozího příkladu jsme uvedli ukázky rozkladů, které odpovídají třídám ekvivalence uvedených v bodu (4) příkladu 5.12. Vskutku, ekvivalence na množině popisují „totéž“ jako rozklady na množině o čemž se přesvědčíme ve zbytku kapitoly.

Věta 5.16. *Nechť* Π *je rozklad na* X. *Pak binární relace* E_Π *na* X *definovaná*

$$\langle x, y\rangle \in E_\Pi, \ \textit{právě když} \ [x]_\Pi = [y]_\Pi \tag{5.6}$$

je ekvivalence.

Důkaz. Pro každý $x \in X$ platí $[x]_\Pi = [x]_\Pi$ triviálně, to jest $\langle x, x\rangle \in E_\Pi$, čímž jsme prokázali reflexivitu E_Π. Nechť $\langle x, y\rangle \in E_\Pi$, tedy $[x]_\Pi = [y]_\Pi$, odtud zřejmě $[y]_\Pi = [x]_\Pi$, tedy $\langle y, x\rangle \in E_\Pi$. Nechť $\langle x, y\rangle \in E_\Pi$ a $\langle y, z\rangle \in E_\Pi$, pak $[x]_\Pi = [y]_\Pi = [z]_\Pi$, to jest $\langle x, z\rangle \in E_\Pi$. □

Definice 5.17. Ekvivalence E_Π definovaná (5.6) se nazývá *ekvivalence příslušná rozkladu* Π.

Nyní víme, že každému rozkladu přísluší ekvivalence. Dále prokážeme, že ke každé ekvivalenci přísluší rozklad a navíc, že rozklady a ekvivalence jsou ve vzájemně jednoznačné korespondenci. Nejprve si však dokážeme některé základní vlastnosti tříd ekvivalence.

Lemma 5.18. *Nechť* E *je ekvivalence na* X. *Pak platí*

(i) $x \in [x]_E$,
(ii) $y \in [x]_E$, *právě když* $\langle y, x\rangle \in E$,
(iii) $x \in [y]_E$, *právě když* $y \in [x]_E$,
(iv) $[x]_E = [y]_E$, *právě když* $y \in [x]_E$.

Důkaz. (i) plyne z reflexivity E, (ii) plyne ze symetrie E, (iii) je důsledek bodu (ii).
(iv): Pokud $[x]_E = [y]_E$, pak dle (i) máme $y \in [y]_E = [x]_E$. Předpokládejme tedy $y \in [x]_E$, to jest $\langle x, y\rangle \in E$. Pokud $z \in [x]_E$, pak $\langle z, x\rangle \in E$ dle (ii), z tranzitivity potom $\langle z, y\rangle \in E$, odtud $z \in [y]_E$ dle (ii). Prokázali jsme $[x]_E \subseteq [y]_E$. Opačná inkluze se prokazuje analogicky. Dohromady $[x]_E = [y]_E$. □

Věta 5.19. *Nechť E je ekvivalence na X. Pak systém množin $\Pi_E \subseteq 2^X$ definovaný*

$$\Pi_E = \{[x]_E \mid x \in X\} \tag{5.7}$$

je rozklad na množině X.

Důkaz. Postupně pro Π_E ověříme podmínky (i)–(iii) definice 5.13.
(i): Nechť $Y \in \Pi_E$, pak dle (5.7) existuje $x \in X$ tak, že $Y = [x]_E$. To jest $x \in [x]_E = Y \neq \emptyset$.
(ii): Předpokládejme, že $[x]_E \cap [y]_E \neq \emptyset$. Pak existuje $z \in X$, kde $z \in [x]_E$ a $z \in [y]_E$. To jest máme $\langle x, z\rangle \in E$ a $\langle z, y\rangle \in E$, dále užitím tranzitivity $\langle x, y\rangle \in E$, což znamená $y \in [x]_E$, odtud $[x]_E = [y]_E$ dle bodu (iv) lemmy 5.18.
(iii): Jelikož $x \in [x]_E$ pro každý $x \in X$, máme $X \subseteq \bigcup_{x\in X}[x]_E = \bigcup \Pi_E$. $\bigcup \Pi_E \subseteq X$ platí triviálně, to jest $\bigcup \Pi_E = X$. □

Definice 5.20. Rozklad Π_E definovaný (5.7) se nazývá *rozklad příslušný ekvivalenci E.*

Rozklady a ekvivalence jsou ve vzájemně jednoznačné korespondenci.

Mějme ekvivalenci E a příslušný rozklad Π_E. Pokud uvažujeme ekvivalenci E_{Π_E} příslušnou Π_E, pak zřejmě $\langle x, y\rangle \in E$, právě když $[x]_{\Pi_E} = [y]_{\Pi_E}$, to je právě když $\langle x, y\rangle \in E_{\Pi_E}$. Dostáváme tak vztah $E = E_{\Pi_E}$. Analogické tvrzení lze ukázat pro rozklady, což dohromady shrnuje následující

Důsledek 5.21. *Pro ekvivalenci E na X a pro rozklad Π na X máme $E_{\Pi_E} = E$, $\Pi_{E_\Pi} = \Pi$.* □

Rozklad na množině X příslušný ekvivalenci E označujeme běžně X/E místo Π_E a někdy jej nazýváme *faktorová množina X podle E*. Jelikož $[x]_E = [x]_{\Pi_E}$, říkáme, že $[x]_E$ *je třída rozkladu množiny X podle E*. Uvažujeme-li o vztahu množiny X a rozkladu X/E, pak víme, že každému $x \in X$ přísluší třída rozkladu $[x]_E$, pro kterou $x \in [x]_E$. Pro ekvivalenci E na X tedy můžeme uvažovat zobrazení $f_E \colon X \to X/E$, kde

$$f_E(x) = [x]_E \tag{5.8}$$

Přirozené zobrazení je vždy surjektivní.

pro každý $x \in X$, a nazýváme jej *přirozené* (*kanonické*) *zobrazení*. Zcela očividně platí, že každé přirozené zobrazení f_E je surjektivní, protože každá třída $Y \in X/E$ je neprázdná, existuje tedy $y \in Y$, odtud $f_E(y) = [y]_E = Y$. Dále je vidět, že f_E je injektivní (a tím pádem bijekce), právě když $[x]_E = \{x\}$ pro každé $x \in X$, což je právě když $E = \omega_X$.

Průvodce studiem

Faktorová množina X/E představuje „zjednodušující pohled“ na výchozí množinu X, při kterém jsme ztotožnili ty prvky X, které od sebe nebyly rozlišitelné ekvivalencí E. Pro konečnou X a $E \neq \omega_X$ navíc platí, že faktorová množina X/E je ostře menší než výchozí množina X, to jest platí $|X/E| < |X|$. Faktorizace jako obecná metoda zmenšení výchozí množiny (třeba souboru dat) má aplikace v informatice například při analýze dat a shlukování.

Přirozené zobrazení lze chápat jako *zobrazení indukované ekvivalencí*. Nyní se budeme věnovat opačnému fenoménu, to jest budeme se snažit definovat ekvivalenci pro dané zobrazení. Nejprve si však řekněme, že kromě ekvivalencí a rozkladů existují další přirozené pohledy na to „jak

zjednodušit nazírání“ na výchozí množinu. Jedním z nich je *surjektivní zobrazení*. Pokud je zobrazení $f\colon X \to Y$ surjektivní, pak lze obraz $f(x)$ prvku x chápat jako vyjádření: „prvek x nahradíme (zjednodušíme) prvkem $f(x)$“, neboli „$f(x)$ je zjednodušeným pohledem na x“. Surjektivita f zaručuje, že každý prvek z Y je „zjednodušeným pohledem“ na nějaký $x \in X$. Opět lze ukázat, že surjektivní zobrazení a ekvivalence mají zvláštní vztah. Pro zobrazení $f\colon X \to Y$ definujeme binární relaci E_f na X předpisem

$$\langle x, y\rangle \in E_f, \text{ právě když } f(x) = f(y). \tag{5.9}$$

E_f je ekvivalence o čemž se můžete snadno přesvědčit. Ekvivalence E_f definovaná vztahem (5.9) se nazývá *ekvivalence indukovaná zobrazením f*. Nyní můžeme prokázat následující větu.

Věta 5.22 (o přirozeném zobrazení). *Necht' $g\colon X \to Y$ je zobrazení. Pak existuje injektivní zobrazení $h\colon X/E_g \to Y$ takové, že $g = f_{E_g} \circ h$. Pokud je navíc g surjektivní, pak je h bijekce.*

Důkaz. Nejprve si uvědomme, že hledané h je zobrazení z faktorové množiny X/E_g, kde E_g je ekvivalence indukovaná zobrazením g, do množiny Y. Můžeme tedy položit $h([x]_{E_g}) = g(x)$ pro každé $x \in X$. Zobrazení h je zavedeno jednoznačně – hodnota $h([x]_{E_g})$ nezávisí na výběru prvku z třídy rozkladu $[x]_{E_g}$. Vskutku, pro $x' \in [x]_{E_g}$ máme $\langle x, x'\rangle \in E_g$, to jest $g(x) = g(x')$, odtud

$$h([x]_{E_g}) = g(x) = g(x') = h([x']_{E_g}).$$

Máme-li $g(x) = g(x')$, pak $\langle x, x'\rangle \in E_g$, to jest $[x]_{E_g} = [x']_{E_g}$, tedy zobrazení h je injektivní. Pro přirozené zobrazení $f_{E_g}\colon X \to X/E_g$ navíc platí $f_{E_g}(x) = [x]_{E_g}$, to jest

$$g(x) = h([x]_{E_g}) = h(f_{E_g}(x)) = (f_{E_g} \circ h)(x)$$

pro každé $x \in X$, což dokazuje $g = f_{E_g} \circ h$. Pokud je navíc g surjektivní, pak pro každé $y \in Y$ existuje $x \in X$ tak, že $y = g(x) = h([x]_{E_g})$, tedy i h je surjektivní, to jest h je bijekce. □

Poznámka 5.23. Podle předchozí věty tedy platí, že pokud je $g\colon X \to Y$ surjektivní zobrazení, to jest zobrazení nahrazující prvky z X jejich zjednodušenými protějšky z Y, pak Y je stejně mohutná množina jako faktorová množina X/E_g, kterou získáme rozkladem výchozí množiny X ekvivalencí indukovanou zobrazením g. V tomto smyslu lze tedy „zjednodušení“ dané surjektivním zobrazením g nahradit faktorovou množinou X/E_g. Opačně, pro faktorovou množinu X/E lze uvažovat přirozené (surjektivní) zobrazení $f_E\colon X \to X/E$. Ve smyslu „zjednodušení pohledu“ a „nerozlišitelnost“ jsou tedy ekvivalence a surjektivní zobrazení vzájemně nahraditelné.

Příklad 5.24. Vezměme surjektivní zobrazení $g\colon \mathbb{Z} \to \{-1, 0, 1\}$, které každému celému číslu $z \in \mathbb{Z}$ přiřazuje prvek z $\{-1, 0, 1\}$ předpisem

$$g(z) = \begin{cases} -1 & \text{pokud } z < 0, \\ 1 & \text{pokud } z > 0, \\ 0 & \text{jinak.} \end{cases}$$

Zobrazení g tedy reprezentuje funkci *signum*. Faktorová množina X/E_g se skládá ze tří tříd rozkladu: $\{x \in \mathbb{Z} \mid x < 0\}$, $\{0\}$ a $\{x \in \mathbb{Z} \mid x > 0\}$. Z intuitivního pohledu g i X/E_g reprezentují zjednodušení množiny celých čísel, které jsme získali „odhlédnutím od konkrétní číselné hodnoty a soustředěním se pouze na znaménko“. Poznamenejme, že i na úrovni konečné množiny X/E_g lze dělat řadu úvah o vlastnostech celé množiny $\mathbb{Z}$.

5.4 Uspořádání

Relace uspořádání je dalším typem speciální binární relace na množině. Uspořádání má mnoho interpretací. Na jednu stranu se na něj lze dívat jako na abstraktní relaci, jejíž speciální případy

jsou relace „srovnávání čísel“, které dobře známe. Na druhou stranu ale uspořádání mohou mít rysy, které nemají přímou analogii při prostém porovnávání čísel. V některých případech je uspořádání interpretovatelné jako relace určující „hierarchii“, případně „závislosti“. Abychom hned na začátku předešli nedorozuměním, upozorněme na to, že uspořádání, kterému se budeme ve zbytku kapitoly věnovat, *nemá nic společného* se „škatulkováním“ – to jest kategorizací (prvků jisté množiny) podle nějakých jejich vlastností.

Uspořádání je v informatice pojem zcela zásadní ačkoliv si to někdy neuvědomujeme. Mezi základní výbavu každého informatika patří znalost *problému třídění* a typických *třídících algoritmů.* Problém třídění jako takový však de facto nemá smysl uvažovat pokud bychom na množině klíčů, podle kterých třídíme, nezavedli nějakou smysluplnou relaci uspořádání – – obvykle ji však chápeme jako „určenou daným kontextem“ a explicitně ji nezdůrazňujeme. Uspořádání množin může výrazně zvýšit efektivitu některých algoritmů, například vyhledávání a podobně.

Definice 5.25. Reflexivní a tranzitivní binární relace R na X se nazývá *kvaziuspořádání.* Antisymetrické kvaziuspořádání se nazývá *uspořádání.* Úplné uspořádání se nazývá *lineární uspořádání* neboli *řetězec.* Pokud je R uspořádání na X, pak se $\langle X, R\rangle$ nazývá *uspořádaná množina.*

Relaci uspořádání na X obvykle značíme $\leq$ v souladu s intuitivním chápáním uspořádání a místo $\langle x, y\rangle \in \leq$ píšeme $x \leq y$. Zdůrazněme ale, že označení $\leq$ v tuto chvíli nemá (obecně) nic společného se srovnáváním čísel, na které jsme zvyklí. Pro uspořádání dále přijímáme značení $x \geq y$ jako zkratku za $x \leq y$. Pro vyjádření faktu $x \leq y$ a $x \neq y$ budeme používat stručný zápis $x < y$ a analogicky $x > y$.

Kvaziuspořádání obecně není antisymetrické, to jest je-li $\leq$ kvaziuspořádání na X, pak mohou existovat prvky $x, y \in X$, kde $x \leq y$, $y \leq x$ a $x \neq y$. Pokud je $\leq$ uspořádání, pak tato situace nastat nemůže, protože z $x \leq y$ a $y \leq x$ plyne $x = y$. Z předchozí definice je také patrný vztah mezi kvaziuspořádáním, uspořádáním a ekvivalencí:

- *symetrické kvaziuspořádání je ekvivalence,*
- *antisymetrické kvaziuspořádání je uspořádání.*

Uspořádání pořád ještě není formálním protějškem „uspořádání“ na které jsme zvyklí při porovnávání čísel. Je-li $\langle X, \leq\rangle$ uspořádaná množina, pak mohou existovat $x, y \in X$ (definice to nevylučuje), pro které neplatí ani $x \leq y$ ani $x \geq y$. V tomto případě říkáme, že prvky $x, y \in X$ jsou *nesrovnatelné,* což někdy značíme $x \parallel y$. V opačném případě (buď $x \leq y$ nebo $y \leq x$) řekneme, že prvky $x, y \in X$ jsou *srovnatelné.* Je-li $\leq$ lineární uspořádání na X, pak je $\leq$ úplná relace, což znamená, že každé dva prvky jsou srovnatelné. Lineární uspořádání tedy lze chápat jako matematický protějšek „tradičního srovnávání čísel“.

V řetězci jsou každé dva prvky srovnatelné.

Každá relace identity ω_X je uspořádání, které nazýváme *antiřetězec.* Je-li $\leq$ na X antiřetězec (jinými slovy: $\leq = \omega_X$), pak pro každé dva různé $x, y \in X$ máme $x \parallel y$. Antiřetězce jsou v jistém smyslu nejmenší uspořádání, protože každé uspořádání $\leq$ na X obsahuje ω_X.

Příklad 5.26. (1) Příkladem kvaziuspořádání, které není ani ekvivalence ani uspořádání je například relace $R = \{\langle a, a\rangle, \langle a, b\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle c, a\rangle, \langle c, b\rangle, \langle c, c\rangle\}$ na množině $X = \{a, b, c\}$.

(2) Následující relace R jsou uspořádání na $X = \{x \mid \langle x, x\rangle \in R\}$:

(a) $R = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$,
(b) $R = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, a\rangle, \langle c, b\rangle, \langle c, c\rangle, \langle d, a\rangle, \langle d, b\rangle, \langle d, c\rangle, \langle d, d\rangle\}$,
(c) $R = \{\langle a, a\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle c, a\rangle, \langle c, b\rangle, \langle c, c\rangle\}$,
(d) $R = \{\langle a, a\rangle, \langle b, a\rangle, \langle b, b\rangle, \langle c, a\rangle, \langle c, c\rangle, \langle d, a\rangle, \langle d, b\rangle, \langle d, d\rangle, \langle e, a\rangle, \langle e, b\rangle, \langle e, c\rangle, \langle e, d\rangle, \langle e, e\rangle\}$,
(e) $R = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, a\rangle, \langle c, b\rangle, \langle c, c\rangle, \langle d, a\rangle, \langle d, b\rangle, \langle d, d\rangle\}$.

(3) Číselné množiny $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ... jsme běžně zvyklí uspořádávat relací „menší rovno“, přitom tato relace je zjevně reflexivní, antisymetrická, tranzitivní i úplná – jedná se tedy o lineární

uspořádání, kterému budeme dál říkat *přirozené uspořádání čísel* (přirozených, celých, racionálních, . . .). Uvědomme si však, že přirozené uspořádání čísel není jediné možné uspořádání číselných množin! Vezměme si například množinu $\mathbb{N}$ a pro $x, y \in \mathbb{N}$ položme $x \leq y$, právě když x dělí y beze zbytku. Pak například $2 \leq 4$, ale $2 \not\leq 3$, protože 2 dělí 3 se zbytkem 1. Snadno nahlédneme, že takto zavedené $\leq$ je rovněž uspořádání na $\mathbb{N}$, které není lineární (například $2 \parallel 3$). Na $\mathbb{N}$ ale existují i lineární uspořádání různá od přirozeného uspořádání, dokonce je jich nekonečně mnoho. Označíme-li například $\leq$ přirozené uspořádání $\mathbb{N}$, pak $R = (\leq - \{\langle 1, 2\rangle\}) \cup \{\langle 2, 1\rangle\}$ je lineární uspořádání, ve kterém jsme oproti $\leq$ „zaměnili dvojku za jedničku“, to jest $2 < 1 < 3 < 4 < \cdots$.

Přirozené uspořádání množiny čísel není jediné možné.

(4) Uvažujme nyní množinu pravdivostních hodnot $X = \{0, 1\}$, které jsme zavedli v kapitole 1.2.2. Pro $x, y \in X$ položíme $x \leq y$, právě když $x \to y = 1$. Z vlastností logické operace $\to$ plyne, že $\leq$ je lineární uspořádání na X, pro které platí $0 \leq 1$, to jest slovně: „nepravda je menší než pravda“.

(5) Relace R z bodu (5) příkladu 5.2 na straně 87 je uspořádání, které značíme $\subseteq$ a nazýváme jej množinová inkluze. Pro obecná U není $\subseteq$ lineární uspořádání. Analogicky bychom mohli zavést uspořádání $\supseteq$: pro $A, B \in 2^U$ klademe $A \supseteq B$, právě když B je podmnožina A. Obě dvě relaci mají zřejmý vztah, jedná se o vzájemně inverzní relace.

Pozorování z bodu (5) předchozího příkladu zobecňuje následující zřejmý princip.

Věta 5.27 (princip duality).
Nechť $\leq$ je uspořádání na X. Pak $\leq^{-1}$ je uspořádání na X, které označujeme $\geq$. □

Nyní si řekněme něco o znázorňování konečných uspořádaných množin. Konečné uspořádání $\leq$ na X je relace, tím pádem ji můžeme reprezentovat binární maticí $\mathbf{M}^{\leq}$ nebo příslušným orientovaným grafem $\langle X, \leq\rangle$. Díky speciálním vlastnostem konečných uspořádání je však můžeme znázorňovat mnohem přehledněji pomocí speciálních diagramů. Ke každému uspořádání $\leq$ na X lze uvažovat odvozenou relaci $\prec$ definovanou předpisem

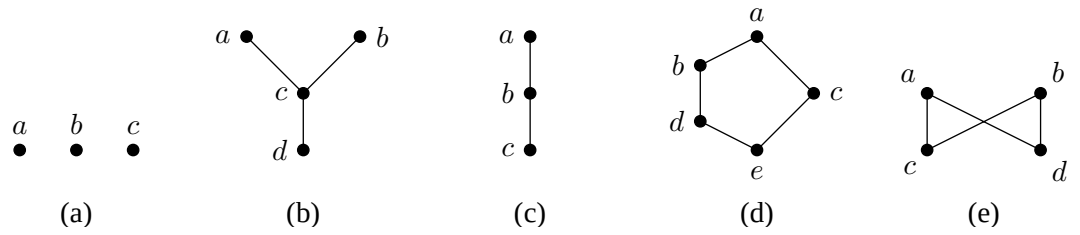
$$x \prec y, \text{ právě když } x < y \text{ a pro každé } z \in X \text{ platí: pokud } x \leq z \leq y \text{ pak } z \in \{x, y\}\,. \quad (5.10)$$

Relaci $\prec$ nazýváme *pokrytí* příslušné $\leq$, výraz $x \prec y$ čteme „x je pokryt y“ nebo „y pokrývá x“. Zřejmě máme $\prec \subseteq \leq$, to jest relace $\prec$ je obsažena v uspořádání $\leq$. Relace pokrytí je dle definice irreflexivní, asymetrická (plyne z vlastností $<$) a obecně není tranzitivní. Význam pokrytí příslušného uspořádané množině $\langle X, \leq\rangle$ je následující: $x \prec y$ znamená, že $x < y$ a zároveň neexistuje žádný prvek $z \in X$, který by se nacházel „mezi x a y“ vzhledem k uspořádání $\leq$. Relace $\prec$ tedy zachycuje informaci o prvcích, které se „bezprostředně pokrývají“. Pro uspořádání $\leq$ na konečné množině zřejmě máme $\leq = \mathrm{Tra}(\mathrm{Ref}(\prec))$, obecně to však neplatí. Uvažujme například množinu racionálních čísel $\mathbb{Q}$ a její přirozené uspořádání $\leq$. V tomto případě máme $\prec = \emptyset$, protože mezi každými dvěma různými racionálními čísly $x, y \in \mathbb{Q}$, $x < y$ existuje $z \in \mathbb{Q}$ tak, že $x < z < y$. Zřejmě tedy $\leq \neq \mathrm{Tra}(\mathrm{Ref}(\prec)) = \omega_{\mathbb{Q}}$.

Na relaci pokrytí je založena jedna z metod jak znázornit konečnou uspořádanou množinu, tak zvané *Hasseovy diagramy uspořádaných množin*. Diagramy jsou složeny z uzlů reprezentujících prvky množiny X a hran, které vyznačují relaci pokrytí $\prec$ příslušnou danému uspořádání $\leq$ na X. Podrobněji, prvky množiny X znázorníme jako uzly (to jest „body“) v rovině tak, aby v případě, kdy $x < y$, ležel bod x níže než bod y. Dva body $x, y \in X$ spojíme v diagramu hranou (úsečkou), právě když $x \prec y$. Horizontální umístění bodů je vhodné volit tak, aby pokud možno nedocházelo ke křížení hran.

Konečné uspořádané množiny znázorňujeme Hasseovými diagramy.

Příklad 5.28. Na obrázku 13 jsou zobrazeny Hasseovy diagramy relací uvedených v bodu (2) příkladu 5.26, v diagramech jsou pro přehlednost vyznačeny odpovídající uzly. Všimněte si, že obrázek (a) odpovídá tříprvkovému antiřetězci a obrázek (c) odpovídá tříprvkovému řetězci. Hasseův diagram dané uspořádané množiny má obecně mnoho možných nakreslení.



Obrázek 13: Hasseovy diagramy uspořádaných množin

Nyní se budeme zabývat existencí speciálních prvků v uspořádaných množinách a jejich vzájemnému vztahu. Například vezmeme-li přirozené uspořádání $\leq$ na množině $\mathbb{N}$, pak o číslu 1 říkáme, že je „nejmenší“. Správně bychom ale měli říkat „nejmenší vzhledem k uspořádání $\leq$“, protože vlastnosti jako jsou „být nejmenší“, „být minimální“ a podobně, jsou těsně vázány k uvažovanému uspořádání. Nyní si tyto a analogické speciální prvky uspořádaných množin přesně zavedeme.

Definice 5.29. Nechť $\langle X, \leq \rangle$ je uspořádaná množina. Prvek $x \in X$ se nazývá

- *minimální,* jestliže pro každý $y \in X$ platí: pokud $y \leq x$, pak $x = y$,
- *nejmenší,* jestliže $x \leq y$ pro každý $y \in X$,
- *maximální,* jestliže pro každý $y \in X$ platí: pokud $y \geq x$, pak $x = y$,
- *největší,* jestliže $x \geq y$ pro každý $y \in X$.

Poznámka 5.30. V definici minimálního a nejmenšího prvku je podstatný rozdíl, i když to na první pohled možná není zřejmé. Prvek $x \in X$ je nejmenší, právě když je $x \in X$ menší (ve smyslu $\leq$) než všechny ostatní prvky z X. Minimalita prvku $x \in X$ znamená, že neexistuje žádný prvek, který by byl ostře menší (ve smyslu $<$) než x. Je téměř zřejmé, že pokud je x nejmenší, pak je také minimální, ale obráceně to již platit nemusí. Analogická situace nastává pro největší a maximální prvky. Nejprve si vztahy prvků ukážeme na příkladech.

Příklad 5.31. (1) Budeme-li uvažovat číselnou množinu $\mathbb{N}$ a její přirozené uspořádání $\leq$, pak číslo 1 je nejmenším a zároveň minimálním prvkem v $\langle \mathbb{N}, \leq \rangle$. Žádný největší ani maximální prvek v $\langle \mathbb{N}, \leq \rangle$ neexistuje. Pokud bychom uvažovali množinu $\mathbb{N} - \{1\}$, to jest množinu přirozených čísel bez jedničky, a pokud bychom na ní zavedli uspořádání $\leq$ předpisem: $x \leq y$, právě když x dělí y beze zbytku, pak by $\langle \mathbb{N} - \{1\}, \leq \rangle$ měla nekonečně mnoho minimálních prvků, kterými by byla právě všechna prvočísla. Na druhou stranu $\langle \mathbb{N} - \{1\}, \leq \rangle$ by neměla žádný nejmenší prvek, ani žádný největší či maximální prvek. Například $\mathbb{Q}$ uspořádaná přirozeným uspořádáním nemá žádný ze speciálních prvků uvedených v definici 5.29.

(2) Uvažujme uspořádané množiny dané diagramy na obrázku 13. Ad (a): prvky a, b, c jsou všechny zároveň maximální i minimální, žádný největší ani nejmenší prvek neexistuje. Ad (b): prvek d ne nejmenší a zároveň minimální, prvky a, b jsou maximální, žádný největší prvek neexistuje. Ad (c): a je největší a maximální, c je nejmenší a minimální. Ad (d): a je největší a maximální, e je nejmenší a minimální. Ad (e): a, b jsou maximální, c, d jsou minimální, žádné největší ani nejmenší prvky neexistují. Všimněte si, že v Hasseově diagramu jsou maximální prvky reprezentovány těmi uzly, které nemají žádné pokrytí – neexistuje žádný výše zakreslený uzel, se kterým by byl tento uzel spojen čarou. Největší prvek poznáme z Hasseova diagramu tak, že pod ním leží všechny ostatní prvky – je tedy zakreslen v diagramu nejvýš a do každého prvku se z něj lze dostat obecně přes několik hran. Analogicky pro minimální a nejmenší prvky.

(3) Potenční množina 2^U uspořádaná množinovou inkluzí $\subseteq$ má nejmenší a zároveň minimální prvek, kterým je $\emptyset$ a dále má i největší a zároveň maximální prvek, kterým je množina U.

V předchozím příkladu jsme mohli vypozorovat vztahy speciálních prvků z definice 5.29. Některé z nich si nyní prokážeme. V důkazu následující věty vhodně využijeme *principu duality* uvedeného ve větě 5.27. Přímo z definice 5.29 totiž pro každé $x \in X$ plyne, že x je

největší (maximální / nejmenší / minimální) prvek v uspořádané množině $\langle X, \leq\rangle$, právě když je x nejmenší (minimální / největší / maximální) prvek v $\langle X, \geq\rangle$.

Věta 5.32. *Nechť $\langle X, \leq\rangle$ je uspořádaná množina. Pak platí*

(i) *v $\langle X, \leq\rangle$ existuje nejvýš jeden největší a jeden nejmenší prvek;*

(ii) *je-li $x \in X$ největší (nejmenší) prvek, pak je také maximální (minimální) a žádné další maximální (minimální) prvky se v X nevyskytují;*

(iii) *pokud je $\leq$ lineární uspořádání, pak je $x \in X$ největší (nejmenší) prvek, právě když je maximální (minimální).*

Důkaz. (i): Nechť $x \in X$ je největší prvek. Ukážeme, že pokud $y \in Y$ splňuje definiční podmínky největšího prvku, pak máme $x = y$. Pokud pro $y \in X$ platí: $z \leq y$ pro každé $z \in X$, pak máme i $x \leq y$. Jelikož je x největší prvek, máme $y \leq x$. To jest z antisymetrie dostáváme $x = y$. Tvrzení pro nejmenší prvek dostaneme užitím principu duality.
(ii): Nechť $x \in X$ je největší prvek a nechť $y \geq x$, pak máme rovněž $y \leq x$, odtud z antisymetrie $x = y$, to jest x je maximální. Pokud je $y \in X$ maximální prvek, pak $y \leq x$ implikuje $x = y$. Zbytek tvrzení plyne z principu duality.
(iii): Nechť $\leq$ je lineární uspořádání. Vzhledem k bodu (ii) stačí ukázat, že pokud je $x \in X$ maximální, pak je největší. Nechť je tedy x maximální a nechť $y \in X$. Jelikož je $\leq$ úplná relace, máme buď $x \leq y$ nebo $y \leq x$. Pokud $y \leq x$, jsme hotovi. Pokud $x \leq y$, pak z maximality plyne $y = x \leq x$. To jest x je největší prvek. Zbytek plyne z principu duality. □

Teď obrátíme naši pozornost k prvkům uspořádané množiny $\langle X \leq\rangle$, které mají speciální význam vzhledem k některým podmnožinám X. Uvažujeme-li například podmnožinu $Y \subseteq X$, můžeme se ptát, zda-li v X existuje nějaký prvek, který je větší (menší) než všechny prvky z Y. Pokud prvek těchto vlastností existuje, můžeme jej chápat jako „horní (dolní) mez“ množiny Y.

Definice 5.33. Nechť $\langle X, \leq\rangle$ je uspořádaná množina a nechť $Y \subseteq X$. Definujeme množiny,

$$\mathrm{L}(Y) = \{x \in X \mid x \leq y \text{ platí pro každé } y \in Y\}, \tag{5.11}$$

$$\mathrm{U}(Y) = \{x \in X \mid x \geq y \text{ platí pro každé } y \in Y\}. \tag{5.12}$$

$\mathrm{L}(Y)$ se nazývá *dolní kužel množiny Y v $\langle X, \leq\rangle$*. $\mathrm{U}(Y)$ se nazývá *horní kužel množiny Y v $\langle X, \leq\rangle$*.

Jinak řečeno, dolní kužel Y v $\langle X, \leq\rangle$ obsahuje právě ty prvky z X, které jsou menší nebo rovny všem prvkům obsaženým v Y, analogicky pro horní kužel. Definice nám okamžitě říká, jak dolní (horní) kužel nalézt, viz následující příklady.

Příklad 5.34. (1) Mějme uspořádanou množinu $\langle X, \leq\rangle$. Pro $Y = \emptyset$ máme $\mathrm{L}(\emptyset) = X = \mathrm{U}(\emptyset)$. Podrobněji, pro každý $x \in X$ je předpoklad $y \in \emptyset$ nepravdivý, to jest z vlastnosti implikace víme, že tvrzení „pokud $y \in \emptyset$, pak $x \leq y$ (případně $x \geq y$)“ platí triviálně pro každé $x \in X$.

(2) Vezmeme-li $\mathbb{Z}$ a její přirozené uspořádání, pak například máme $\mathrm{L}(\mathbb{N}) = \{x \in \mathbb{Z} \mid x \leq 1\}$, $\mathrm{U}(\{0\}) = \mathbb{N} \cup \{0\}$, $\mathrm{U}(\{x \in \mathbb{N} \mid x \text{ je sudé číslo}\}) = \emptyset$. Pro $\mathbb{Q}$ a její přirozené uspořádání máme například $\mathrm{L}(\{\frac{1}{n} \mid n \in \mathbb{N}\}) = \mathrm{L}(\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}) = \{q \in \mathbb{Q} \mid q \leq 0\}$.

(3) Uvažujme uspořádané množiny dané diagramy na obrázku 13. Uvedeme si některé zajímavé horní a dolní kužely. Ad (a): Máme $\mathrm{U}(\{x\}) = \{x\} = \mathrm{L}(\{x\})$ pro libovolný $x \in X$. Ad (b): $\mathrm{U}(\{a, b\}) = \emptyset$, $\mathrm{L}(\{a, b\}) = \{c, d\}$. Ad (c): $\mathrm{U}(\{a, b, c\}) = \{a\}$, $\mathrm{L}(\{a, b, c\}) = \{c\}$. Ad (d): $\mathrm{U}(\{b, c\}) = \mathrm{U}(\{c, d\}) = \{a\}$, $\mathrm{L}(\{b, c\}) = \mathrm{L}(\{c, d\}) = \{e\}$. Ad (e): $\mathrm{U}(\{a, b\}) = \emptyset$, $\mathrm{L}(\{a, b\}) = \{c, d\}$, $\mathrm{U}(\{c, d\}) = \{a, b\}$, $\mathrm{L}(\{c, d\}) = \emptyset$.

Řekli jsme, že horní a dolní kužel $Y \subseteq X$ je možné interpretovat jako množiny, které danou podmnožinu Y omezují shora a zdola. Platí navíc, že $\langle \mathrm{U}(Y), \leq_{\mathrm{U}(Y)}\rangle$, kde $\leq_{\mathrm{U}(Y)}$ je relace vzniklá ze $\leq$ zúžením na množinu $\mathrm{U}(Y)$, je opět uspořádaná množina. Duálně $\langle \mathrm{L}(Y), \leq_{\mathrm{L}(Y)}\rangle$

je uspořádaná množina. Můžeme tedy bez újmy zkoumat kužely coby uspořádané množiny. Obzvláště zajímavé pro nás je, pokud horní kužel $\mathrm{U}(Y)$ obsahuje nejmenší prvek, protože tento prvek lze interpretovat jako nejmenší horní mez podmnožiny Y v $\langle X, \leq\rangle$. Duálně k tomu, největší prvek dolního kuželu $\mathrm{L}(Y)$ lze interpretovat (pokud existuje) jako největší dolní mez podmnožiny Y v $\langle X, \leq\rangle$. Tyto speciální prvky nyní zavedeme jako supremum a infimum:

Definice 5.35. Nechť $\langle X, \leq\rangle$ je uspořádaná množina a nechť $Y \subseteq X$. Pokud má $\mathrm{L}(Y)$ největší prvek, pak se nazývá *infimum* Y a označuje se $\inf(Y)$. Pokud má $\mathrm{U}(Y)$ nejmenší prvek, pak se nazývá *supremum* Y a označuje se $\sup(Y)$.

Speciálně pro $\{x, y\} \subseteq X$ píšeme $\inf(x, y)$ místo $\inf(\{x, y\})$, stejně tak pro supremum. Supremum a infimum dané množiny obecně nemusí existovat. Ukažme si nejprve některé příklady.

Příklad 5.36. (1) Vezměme $\mathbb{N}$ uspořádanou přirozeným uspořádáním $\leq$. Pak zřejmě pro každé $x, y \in \mathbb{N}$ máme $\inf(x, y) = \min(x, y)$ a $\sup(x, y) = \max(x, y)$. V tomto případě tedy infimum i supremum existuje pro každé dva prvky. Dále zřejmě máme $\mathrm{L}(\mathbb{N}) = \{1\}$, tedy $\inf(\mathbb{N}) = 1$. Například ale $\mathrm{U}(\mathbb{N}) = \emptyset$, to jest $\sup(\mathbb{N})$ neexistuje. Zde vidíme, že i když supremum existuje ke každým dvěma prvkům z $\mathbb{N}$, nemusí nutně existovat k libovolné podmnožině $\mathbb{N}$.

(2) Vezměme $\mathbb{N} - \{1\}$ a položme $x \leq y$, právě když x dělí y beze zbytku. Pak například pro čísla 8 a 12 máme $\mathrm{L}(8, 12) = \{2, 4\}$, to jest $\inf(8, 12) = 4$. Analogicky $\mathrm{U}(8, 12) = \{24, 48, 72, 96, \dots\}$, tedy $\sup(8, 12) = 24$. Například ale $\inf(2, 3)$ neexistuje, protože $\mathrm{L}(2, 3) = \emptyset$. Supremum existuje ke každým dvěma prvkům a $\sup(x, y)$ je nejmenším společným násobkem x a y. Infimum existuje ke každým dvěma soudělným číslům a je rovno jejich největšímu společnému děliteli.

(3) Uvažujme uspořádané množiny dané diagramy na obrázku 13, uvedeme si infima a suprema některých podmnožin. Ad (a): $\inf(x, y)$ a $\sup(x, y)$ existuje, právě když $x = y$. Ad (b): $\inf(a, b) = c$, $\sup(a, b)$ neexistuje, $\inf(x, d) = d$ pro každé $x \in \{a, b, c, d\}$. Ad (c): Infimum a supremum existuje k libovolné podmnožině. Ad (d): $\sup(b, c) = \sup(c, d) = a$, $\inf(b, c) = \inf(c, d) = e$. Ad (e): $\sup(a, b)$ neexistuje (zde je $\mathrm{U}(\{a, b\}) = \emptyset$), $\inf(a, b)$ neexistuje (zde je sice $\mathrm{L}(\{a, b\}) = \{c, d\} \neq \emptyset$, ale $c \parallel d$, to jest $\mathrm{L}(\{a, b\})$ nemá největší prvek), analogicky $\sup(c, d)$ neexistuje ani $\inf(c, d)$ neexistuje.

Na základě existence infima či suprema ke každým dvěma prvkům definujeme speciální uspořádané množiny zvané polosvazy a svazy.

Definice 5.37. Nechť $\langle X, \leq\rangle$ je uspořádaná množina. Pokud pro každé $x, y \in X$ existuje $\inf(x, y)$, pak $\langle X, \leq\rangle$ nazveme *průsekový polosvaz.* Pokud pro každé $x, y \in X$ existuje $\sup(x, y)$, pak $\langle X, \leq\rangle$ nazveme *spojový polosvaz.* Je-li $\langle X, \leq\rangle$ průsekový i spojový polosvaz, pak $\langle X, \leq\rangle$ nazveme *svaz.*

Ve svazu existuje ke každým dvěma prvků infimum a supremum.

Svaz je tedy uspořádaná množina, kde ke každým dvěma prvkům existuje jejich infimum i supremum. Nosiče svazu značíme obvykle L místo X, to jest svaz značíme $\langle L, \leq\rangle$. Dalším zřejmým pozorováním, které plyne z principu duality je fakt, že $\langle X, \leq\rangle$ je průsekový (spojový) polosvaz, právě když je $\langle X, \geq\rangle$ spojový (průsekový) polosvaz.

Příklad 5.38. (1) Každá lineárně uspořádaná množina $\langle X, \leq\rangle$ je svaz, protože pro každé dva prvky $x, y \in X$ máme buď $x \leq y$, v tom případě $\inf(x, y) = x$ a $\sup(x, y) = y$, nebo platí $y \leq x$, v tom případě $\inf(x, y) = y$ a $\sup(x, y) = x$. Speciálně tedy číselné množiny $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ uspořádané přirozeným uspořádáním jsou svazy, ve kterých infima a suprema odpovídají minimu a maximu z obou prvků. Obecně v nich ale neexistují infima a suprema nekonečných podmnožin.

(2) $\mathbb{N} - \{1\}$ z bodu (2) příkladu 5.36 je spojový polosvaz, ale nejedná se o průsekový polosvaz. Kdybychom však dělitelností uspořádali celou množinu $\mathbb{N}$, pak by se jednalo i o průsekový polosvaz a tudíž o svaz.

(3) Uvažujme uspořádané množiny dané diagramy na obrázku 13, pak (a) není polosvaz (ani průsekový, ani spojový), (b) je průsekový polosvaz, ale nejedná se o spojový polosvaz, (c) a (d) jsou svazy, (e) není polosvaz (ani průsekový, ani spojový).

Na závěr podotkněme, že indukcí se lze snadno přesvědčit, že pokud je $\langle L, \leq \rangle$ svaz, pak v něm existuje supremum i infimum pro libovolnou konečnou a neprázdnou podmnožinu L o čemž se lze snadno přesvědčit matematickou indukcí: pro $x \in L$ máme triviálně $\inf(\{x\}) = x$; nechť infimum existuje pro každou $n-1$ prvkovou podmnožinu L, pak zřejmě

$$\inf(\{x_1, \ldots, x_n\}) = \inf(\{x_1, \ldots, x_{n-1}\}, x_n).$$

Každý konečný svaz má největší a nejmenší prvek.

Tvrzení lze prokázat duálně pro suprema. Toto pozorování má následující důsledek. Pokud je $\langle L, \leq \rangle$ konečný svaz, to jest L je konečná množina, pak existuje $\inf(L)$ a $\sup(L)$, což dle definice infima a suprema znamená, že v $\langle L, \leq \rangle$ je $\inf(L)$ nejmenší prvek a $\sup(L)$ je největší prvek. Jinými slovy, každý konečný svaz má nejmenší prvek (značený 0) a největší prvek (značený 1). U nekonečných svazů to obecně neplatí, viz příklad 5.38.

Shrnutí

Relace ekvivalence reprezentují matematický protějšek nerozlišitelnosti, jedná se o reflexivní, symetrické a tranzitivní relace. Ekvivalence jsou ve vzájemně jednoznačné korespondenci s rozklady na množině, to jest s disjunktními pokrytími množiny. Ekvivalence mají rovněž vztah k surjektivním zobrazením.
Kvaziuspořádání je reflexivní a tranzitivní relace. Relace uspořádání je reflexivní, antisymetrická a tranzitivní relace. Lineární uspořádání je reflexivní, antisymetrická, tranzitivní a úplná relace. V uspořádaných množinách se mohou nacházet speciální prvky (největší, maximální, nejmenší, minimální). Dalšími speciálními prvky uspořádaných množin vzhledem k jistým podmnožinám jsou infimum a supremum. Průsekový polosvaz je uspořádaná množina, ve které ke každým dvěma prvkům existuje jejich infimum, spojový polosvaz je uspořádaná množina, ve které ke každým dvěma prvkům existuje jejich supremum. Svaz je uspořádaná množina, ve které ke každým dvěma prvkům existuje jejich infimum i supremum.

Pojmy k zapamatování

- ekvivalence, třída ekvivalence, rozklad na množině, třída rozkladu,
- ekvivalence příslušná rozkladu, rozklad příslušný ekvivalenci, faktorová množina,
- přirozené zobrazení, ekvivalence indukovaná zobrazením,
- kvaziuspořádání, uspořádání, uspořádaná množina, lineární uspořádání, řetězec, antiřetězec,
- princip duality, pokrytí, Hasseův diagram,
- minimální prvek, nejmenší prvek, maximální prvek, největší prvek,
- dolní kužel, horní kužel, infimum, supremum,
- spojový polosvaz, průsekový polosvaz, svaz

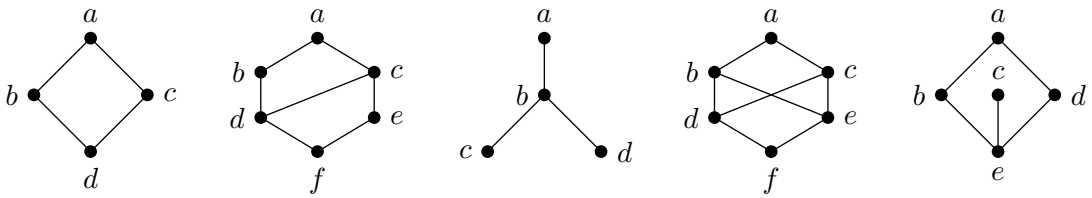
Kontrolní otázky

1. *Co víte o intuitivním významu ekvivalence?*
2. *Jaký je vztah rozkladu k ekvivalenci?*
3. *Proč je každá ekvivalenční třída neprázdná?*
4. *Jak vypadá nejmenší a největší ekvivalence na dané množině?*
5. *Jaký je rozdíl mezi kvaziuspořádáním, uspořádáním a ekvivalencí?*
6. *Co říká princip duality a jaký má intuitivní význam?*
7. *Která ekvivalence je zároveň uspořádání?*

8. *Mohou existovat v lineárně uspořádané množině dva různé maximální prvky?*

Cvičení

1. Rozhodněte, které z následujících relací R jsou ekvivalence. Proveďte diskusi.
   (a) $X = \{0,1,2,3\}, R = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 3,3\rangle\}$,
   (b) $X = 2^U$, $R = \{\langle A,B\rangle \mid A,B \in X,\ |A| = |B|\}$,
   (c) $X = 2^U$, $R = \{\langle A,B\rangle \mid A,B \in X,\ A \cap B \neq \emptyset\}$,
   (d) $R = S \cap S^{-1}$, kde S je reflexivní a tranzitivní relace na X.
2. K následujícím rozkladům Π nalezněte ekvivalence E_Π.
   (a) $\Pi = \{\{a,b,c\},\{d\},\{e,f\},\{g\}\}$,
   (b) $X = 2^{\{a,b\}}$, $\Pi = \{\{\{a\},\{a,b\}\},\{\emptyset,\{b\}\}\}$,
   (c) $X = \mathbb{N}$, $\Pi = \{\{0,2,4,\dots\},\{1\},\{3\},\{5\},\dots\}$.
3. K následujícím ekvivalencím E na X nalezněte rozklady Π_E.
   (a) $X = \{0,\dots,4\}$, $E = \{\langle 0,2\rangle, \langle 0,4\rangle, \langle 2,0\rangle, \langle 2,4\rangle, \langle 4,0\rangle, \langle 4,2\rangle\} \cup \omega_X$,
   (b) $X = \{0,1,2,3,4,5,6,7,8,9\}$, $E = \{\langle x,y\rangle \mid$ rozdíl $x - y$ je dělitelné třemi beze zbytku$\}$,
   (c) $X = \mathbb{N} \times \mathbb{N}$, $E = \{\langle\langle m,n\rangle,\langle p,q\rangle\rangle \mid m,n,p,q \in \mathbb{N},\ m+n = p+q\}$.
4. Určete, které z následujících relací R na X jsou kvaziuspořádání, uspořádání, případně řetězce.
   (a) $X = \{1,2,3,4\}$, $R = \{\langle 1,1\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,2\rangle, \langle 3,4\rangle, \langle 4,4\rangle\}$,
   (b) $X = \mathbb{Z}$, $\langle x,y\rangle \in R$, právě když buď $|x| = |y|$ a $x \geq y$, nebo $|x| < |y|$,
   (c) $X = \mathbb{Q}$, $R = \{\langle x,y\rangle \mid x,y \in \mathbb{Q},\ x^2 \leq y^2\}$,
   (d) $X = \mathbb{N} \times \mathbb{N}$, $R = \{\langle\langle m,n\rangle,\langle p,q\rangle\rangle \mid m,n,p,q \in \mathbb{N},\ m \leq p$ a $n \leq q\}$.
5. Uspořádané množiny zobrazené na následujících diagramech zapište binárními maticemi.



6. Vraťte se k předchozímu příkladu a určete nejmenší, minimální, největší a maximální prvky.
7. Vraťte se k předchozímu příkladu a rozhodněte, které z diagramů reprezentují průsekové případně spojové polosvazy či svazy.

Úkoly k textu

1. Nechť R je binární relace na X. Dokažte, že relace $E = \mathrm{Tra}(\mathrm{Sym}(\mathrm{Ref}(R)))$ je ekvivalence na X obsahující R a pro každou ekvivalenci E' na X obsahující R platí $E \subseteq E'$.

2. Pro každou množinu X označme $E(X)$ systém všech ekvivalencí na X. To jest například pro $X = \{a,b,c\}$ máme $E(X) = \{\omega_X, E_1, E_2, E_3, \iota_X\}$, kde E_1, E_2 a E_3 jsou ekvivalence z bodu (2) příkladu 5.12 na straně 94. Dokažte následující tvrzení.
   (a) Pro každé $E_1, E_2 \in E(X)$ platí $E_1 \cap E_2 \in E(X)$.
   (b) $\langle E(X), \subseteq\rangle$ je průsekový polosvaz, kde $\inf(E_1,E_2) = E_1 \cap E_2$.
   (c) Existuje X a $E_1, E_2 \in E(X)$ tak, že $E_1 \cup E_2$ není tranzitivní.
   (d) Pro každé $E_1, E_2 \in E(X)$ platí $\mathrm{Tra}(E_1,E_2) \in E(X)$.
   (e) $\langle E(X), \subseteq\rangle$ je spojový polosvaz, kde $\sup(E_1,E_2) = \mathrm{Tra}(E_1 \cup E_2)$.
   (f) $\langle E(X), \subseteq\rangle$ je svaz s nejmenším prvkem ω_X a největším prvkem ι_X.

   Předchozí tvrzení dokazujte postupně a vhodně využijte již prokázaných tvrzení.

Řešení

1. (a) není ekvivalence, protože není symetrická; (b) je ekvivalence; (c) pro $|X| = 1$ je ekvivalence, pro $|X| \geq 2$ není tranzitivní; (d) je ekvivalence: reflexivita a tranzitivita plyne z reflexivity a tranzitivity S a S^{-1}, symetrie plyne ze vztahu S a S^{-1}.
2. Ekvivalence mají následující tvar:
   (a) $\{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle c,b\rangle, \langle e,f\rangle, \langle f,e\rangle\} \cup \omega_{\{a,b,c,d,e,f,g\}}$,
   (b) $\{\langle\emptyset,\emptyset\rangle,\langle\emptyset,\{b\}\rangle,\langle\{b\},\emptyset\rangle,\langle\{b\},\{b\}\rangle,\langle\{a\},\{a\}\rangle,\langle\{a\},\{a,b\}\rangle,\langle\{a,b\},\{a\}\rangle,\langle\{a,b\},\{a,b\}\rangle\}$,
   (c) $\{\langle x,y\rangle \mid x,y \in \mathbb{N},\ x,y$ jsou obě sudá, nebo $x = y\}$.
3. Rozklady mají následující tvar:
   (a) $\{\{0,2,4\},\{1\},\{3\}\}$,
   (b) $\{\{0,3,6,9\},\{1,4,7\},\{2,5,8\}\}$,
   (c) $\{\{\langle 1,1\rangle\},\{\langle 1,2\rangle,\langle 2,1\rangle\},\{\langle 1,3\rangle,\langle 2,2\rangle,\langle 3,1\rangle\},\{\langle 1,4\rangle,\langle 2,3\rangle,\langle 3,2\rangle,\langle 4,1\rangle\},\dots\}$.
4. (a) není reflexivní, (b) řetězec, (c) kvaziuspořádání (není antisymetrické), (d) uspořádání.
5. Matice jsou uvedeny zleva doprava, pořadí sloupců a řádků dle abecedy.

$$\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{pmatrix},\quad \begin{pmatrix}1&0&0&0&0&0\\1&1&0&0&0&0\\1&0&1&0&0&0\\1&1&1&1&0&0\\1&0&1&0&1&0\\1&1&1&1&1&1\end{pmatrix},\quad \begin{pmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&1&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0&0&0\\1&1&0&0&0&0\\1&0&1&0&0&0\\1&1&1&1&0&0\\1&1&1&0&1&0\\1&1&1&1&1&1\end{pmatrix},\quad \begin{pmatrix}1&0&0&0&0\\1&1&0&0&0\\0&0&1&0&0\\1&0&0&1&0\\1&1&1&1&1\end{pmatrix}.$$

6. Zleva doprava: a je největší a maximální, d je nejmenší a minimální; a je největší a maximální, f je nejmenší a minimální; a je největší a maximální, c, d jsou minimální; a je největší a maximální, f je nejmenší a minimální; a, c jsou maximální, e je nejmenší a minimální.
7. Zleva doprava: svaz, svaz, spojový polosvaz, —, průsekový polosvaz.

6 Logika (znovu u logiky)

Studijní cíle: Po prostudování kapitoly by student měl rozumět rozdílu mezi sémantickým vyplýváním a syntaktickým vyplýváním ve výrokové logice a jejich vzájemnému vztahu. Student by měl mít představu o formalizaci důkazu ve výrokové logice a o základních vlastnostech důkazů.

Klíčová slova: axiom, axiomatický systém, axiomové schéma, bezespornost, dokazatelnost, důkaz, instance schéma, korektnost, modus ponens, monotonie dokazatelnosti, nesplnitelnost, odvozovací pravidlo, pravidlo odloučení, předpoklady, splnitelnost, spornost, syntaktické vyplývání, systém formulí, tranzitivita implikace, úplnost, věta o dedukci

Potřebný čas: 120 minut.

6.1 Dokazatelnost ve výrokové logice

V úvodní kapitole o výrokové logice jsme zavedli pojem *sémantické vyplývání.* Problém ověření, zda-li je formule φ sémantickým důsledkem formulí $\chi_1, \ldots, \chi_k$ lze snadno vyřešit tabelací. Máme tedy k dispozici „mechanický potup“, jak o sémantickém vyplývání z $\chi_1, \ldots, \chi_k$ rozhodnout. Problémem je, že velikost tabulky, kterou při tabelaci vytváříme, je v exponenciální závislosti na počtu výrokových symbolů ve formulích $\chi_1, \ldots, \chi_k$. Pokud by například $\chi_1, \ldots, \chi_k$ obsahovaly celkem 100 různých výrokových symbolů, což je při popisu reálných systémů vcelku zanedbatelné množství, pak bychom museli při tabelaci zkoumat 2^{100} pravdivostních ohodnocení – to je z časových důvodů hluboko za hranicemi našich možností i za hranicemi možností nejen soudobých, ale i budoucích počítačů. Nabízí se tedy otázka, zda-li není možné o sémantickém vyplývání rozhodnout jinak než tabelací. Na tuto otázku se budeme snažit najít odpověď v této kapitole.

Tabelace je neúnosná při velkém množství výrokových symbolů.

Nejprve si zavedeme nový pojem vyplývání, který nebude založen na pojmu pravdivostní ohodnocení, ale pouze na manipulaci s formulemi na úrovni jejich tvaru. Základní pojem, na kterém je tento typ vyplývání založen je *odvozovací pravidlo* – předpis, pomocí nějž ze vstupních formulí odvozujeme další formule. Odvozovací pravidla formalizují elementární úsudky. Pro účely dalšího výkladu bude postačovat pouze jediné odvozovací pravidlo, tak zvané *pravidlo odloučení* neboli *modus ponens* (MP), které lze schématicky vyjádřit

Odvozovací pravidla formalizují úsudky.

$$MP\colon \quad \frac{\varphi,\ \varphi \Rightarrow \psi}{\psi}$$

a jehož význam je: „z formulí φ a $\varphi \Rightarrow \psi$ odvodíme formuli ψ“. O formuli ψ říkáme, že *vzniká použitím modus ponens* z formulí φ a $\varphi \Rightarrow \psi$. Formulím φ a $\varphi \Rightarrow \psi$ někdy říkáme *předpoklady.* Například formule $\neg q$ vzniká použitím modus ponens z formulí $p \Rightarrow r$ a $(p \Rightarrow r) \Rightarrow \neg q$. Pokud se nyní vrátíme zpět k našemu úvodu do formální logiky, tak zjistíme, že pravidlo modus ponens jsme již (neformálně) použili při odvození tvrzení „Silnice jsou mokré“ z předpokladů „Jestliže prší, pak jsou silnice mokré“ a „Prší“. Stejný způsobem bylo odvozeno tvrzení „Petr spí“ z předpokladů „Pokud je Petr unavený, pak spí“ a „Petr je unavený“. Odvozování formulí z jiných pouze na základě jejich formy (tvaru) bez úvah o jejich pravdivosti tedy není nikterak umělé.

Při odvozování nových formulí budeme vždy používat *množinu výchozích formulí* (*předpokladů*), kterou budeme značit podle potřeby $T, T', S, \ldots$ a budeme ji nazývat *systém formulí.* Použití označení „systém formulí“ místo možná přímočařejšího „množina formulí“ je více méně věcí vkusu. My se podržíme označení „systém formulí“ abychom předešli nedorozuměním během dalšího výkladu, například totiž pojem „sporná množina formulí“, by mohl intuitivně svádět k představě, že „spornost“ je nějaká obecná vlastnost *množin,* což není.

Systém formulí označuje množinu výchozích předpokladů.

Při odvozování formulí budeme dále používat *axiomy,* což jsou formule, které automaticky přijímáme jako „platné“. Axiomy popisují vlastnosti logických spojek a jejich vzájemný vztah. Pro

jednoduchost budeme ve zbytku kapitoly pracovat s jazykem výrokové logiky, který obsahuje pouze symboly spojek $\Rightarrow$ a $\neg$, ostatní spojky budeme vyjadřovat pomocí nich. Připomeňme, že v kapitole 1.2.2 jsme uvedli, že negace spolu s implikací postačují k vyjádření ostatních logických spojek. Axiomy si definujeme pomocí tří *axiomových schémat:*

$$\begin{aligned}
&\text{V1:}\quad \varphi \Rightarrow (\psi \Rightarrow \varphi),\\
&\text{V2:}\quad (\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi)),\\
&\text{V3:}\quad (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi).
\end{aligned}$$

Každý axiom je instancí některého axiomového schéma.

Jakákoliv formule, která je ve tvaru jednoho ze schémat V1–V3 se nazývá *axiom.* Axiomová schémata jsou jinými slovy „předpisy“, kterými definujeme všechny axiomy. Ačkoliv budeme používat pouze tři axiomová schémata, axiomů jako takových je nekonečně mnoho. Pokud budeme potřebovat upřesnit, v jakém ze tvarů V1–V3 daný axiom je, budeme říkat, že *axiom je instancí daného schéma* nebo že *jistá formule je axiomem dle daného schéma.* Například formule $p \Rightarrow (\neg q \Rightarrow p)$ je axiom, který je instancí schéma V1, konkrétně vznikne, pokud φ a ψ nahradíme po řadě formulemi p a $\neg q$. Dále například $(\neg\neg\neg p \Rightarrow \neg\neg(p \Rightarrow p)) \Rightarrow (\neg(p \Rightarrow p) \Rightarrow \neg\neg p)$ je instance V3, která vznikne nahrazením φ a ψ po řadě formulemi $\neg(p \Rightarrow p)$ a $\neg\neg p$. Například $p \Rightarrow (r \Rightarrow q)$ a $(\neg p \Rightarrow q) \Rightarrow (q \Rightarrow p)$ nejsou axiomy.

Průvodce studiem

V tomto okamžiku je možná již jasné, proč je výhodné za základní symboly spojek přijmout pouze $\Rightarrow$ a $\neg$ a všechny ostatní vyjadřovat pomocí nich. Kdybychom v jazyku VL pracovali i se spojkami $\wedge, \vee, \Leftrightarrow$, vedlo by to minimálně k nárůstu axiomových schémat, protože bychom museli pomocí vhodných axiomů popsat vlastnosti spojek. V další části textu také uvidíme, že by se tím dál zbytečně zkomplikovala řada důkazů.

Odvozovací pravidla a axiomy tvoří axiomatický systém.

Množinu axiomů a odvozovacích pravidel, která používáme, souhrnně nazýváme *axiomatický systém.* Výše představený axiomatický systém se v literatuře obvykle nazývá *axiomatický systém klasické výrokové logiky Hilbertova typu.* Pod pojmem „důkaz“ je intuitivně myšlen záznam odvozování, provedený tak, že za sebe napíšeme tvrzení, ke kterým se postupně dobíráme tak, že začneme předpoklady a pokračujeme tvrzeními, které z předchozích tvrzení plynou pomocí elementárních úsudkových kroků. Nyní zavedeme přesný pojem důkazu v našem axiomatickém systému – neformální pojem důkazu tak převedeme z úrovně intuice na přesnou formální úroveň.

Definice 6.1. *Důkaz* formule φ ze systému formulí T je libovolná posloupnost formulí $\varphi_1, \ldots, \varphi_n$, pro kterou platí, že $\varphi_n = \varphi$ a každá φ_i $(i = 1, \ldots, n)$

- je axiomem,
- nebo $\varphi_i \in T$,
- nebo vzniká z předchozích formulí důkazu pomocí odvozovacího pravidla modus ponens, to jest existují indexy $j, k < i$ tak, že φ_k je formule ve tvaru $\varphi_j \Rightarrow \varphi_i$.

Formule φ je *dokazatelná z* T (zapisujeme $T \vdash \varphi$), pokud existuje důkaz formule φ z T. Pokud $\vdash \varphi$, pak říkáme, že φ *je dokazatelná* (*z prázdného systému předpokladů*).

Každý axiom je dokazatelný.

Dokazatelnosti budeme také dále říkat *syntaktické vyplývání,* abychom tím zdůraznili, že jde o protějšek sémantického vyplývání. Fakt $T \vdash \varphi$ lze tedy číst: „φ syntakticky plyne z T“, případně „φ je syntaktickým důsledkem T“. Dále si uvědomme triviální fakt, že $\vdash \varphi$ platí pro každý axiom φ, protože jednoprvková posloupnost φ je důkazem φ z prázdného systému předpokladů. Pro libovolnou φ máme, že φ je dokazatelná ze „sebe sama“, to jest přesněji: $\{\varphi\} \vdash \varphi$, protože φ je jednoprvkový důkaz formule φ z předpokladů $\{\varphi\}$. Pro zpřehlednění zápisu zavedeme

Označení 6.2. Místo $T \cup \{\varphi_1, \ldots, \varphi_k\} \vdash \psi$ píšeme $T, \varphi_1, \ldots, \varphi_k \vdash \psi$.

Příklad 6.3. Prokážeme, že pro každou formuli φ platí $\vdash \varphi \Rightarrow \varphi$. Máme tedy ukázat, že existuje důkaz (z prázdného systému T), jehož posledním prvkem je $\varphi \Rightarrow \varphi$. Například posloupnost

1. $\varphi \Rightarrow ((\varphi \Rightarrow \varphi) \Rightarrow \varphi)$	*axiom dle V1,*
2. $(\varphi \Rightarrow ((\varphi \Rightarrow \varphi) \Rightarrow \varphi)) \Rightarrow ((\varphi \Rightarrow (\varphi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi))$	*axiom dle V2,*
3. $(\varphi \Rightarrow (\varphi \Rightarrow \varphi)) \Rightarrow (\varphi \Rightarrow \varphi)$	*užitím MP na 1. a 2.,*
4. $\varphi \Rightarrow (\varphi \Rightarrow \varphi)$	*axiom dle V1,*
5. $\varphi \Rightarrow \varphi$	*užitím MP na 3. a 4.*

je důkazem formule $\varphi \Rightarrow \varphi$. Fakt $\vdash \varphi \Rightarrow \varphi$ budeme dále používat.

V příkladu 6.3 jsme sestrojili důkaz, který je konečnou posloupností formulí. Je patrné, že hledání důkazů v tomto tvaru je obecně dost těžké a vyžaduje jistou představivost a cvik. Naším cílem ale není zkoumat konkrétní důkazy jakožto konečné posloupnosti formulí, nýbrž zkoumat vlastnosti syntaktického vyplývání. Podstatný je tedy pro nás fakt $T \vdash \varphi$, to jest že nějaká formule φ je dokazatelná z jistého systému formulí T, tvar konkrétního důkazu pro nás zajímavý není. Jinými slovy, nezajímají nás ani tak konkrétní důkazy, jako spíš fakt, že „něco je z něčeho dokazatelné“.

Zkoumáme vlastnosti $\vdash$, nikoliv konkrétní důkazy.

Průvodce studiem

Všimněte si, že nyní používáme pojem *důkaz* dvojím způsobem. Prvním pojem je důkaz jakožto konečná posloupnost formulí tak, jak jsme jej zavedli v definice 6.1. Druhý pojem „důkaz“ používáme, když dokazujeme tvrzení, například na straně 15 jsme uvedli důkaz lemmy 1.14. Je zřejmé, že se jedná o dva různé pojmy. Důkaz dle definice 6.1 je pro nás přesně vymezený formalizovaný pojem, který slouží k tomu abychom uměli pojem důkaz „uchopit“ a zkoumat jeho vlastnosti. Naopak důkazy tvrzení v této knize, například lemmy 1.14, nejsou formalizované, jsou popisovány přirozeným jazykem a při jejich zdůvodňování používáme intuitivně zřejmá fakta. Každý takový důkaz bychom ale přísně vzato mohli formalizovat v nějakém logickém kalkulu a převést na důkaz formální (to my ovšem dělat nebudeme, protože to pro nás nemá žádné opodstatnění).

Nyní si o syntaktickém vyplývání dokážeme několik jednoduchých tvrzení, která budeme v dalším výkladu hojně používat. Vztahy a jejich zdůvodnění, objevující se v následujícím tvrzení je proto potřeba do detailů pochopit.

Lemma 6.4. *Necht' T, S jsou systémy formulí a φ, ψ jsou formule. Pak platí*

(i) *pokud $T \vdash \varphi \Rightarrow \psi$ a $T \vdash \varphi$, pak $T \vdash \psi$;*
(ii) *pokud $T \vdash \varphi$ a pro každou $\psi \in T$ máme $S \vdash \psi$, pak $S \vdash \varphi$ (monotonie dokazatelnosti);*
(iii) *pokud $T \vdash \varphi$ a $T \subseteq S$, pak $S \vdash \varphi$;*
(iv) *pokud $T \vdash \varphi$, pak existuje konečný systém formulí T' tak, že $T' \subseteq T$ a $T' \vdash \varphi$.*

Důkaz. Důkaz bodu (i) si provedeme podrobně, abychom demonstrovali, jakým způsobem se manipuluje s důkazy jakožto s konečnými posloupnosti formulí. Zbylá tvrzení již nebudeme prokazovat tak detailně, čtenáři však doporučujeme, aby se snažil veškeré kroky v důkazech podrobně zdůvodnit.
(i): Prokážeme, že jsou-li z T dokazatelné formule $\varphi \Rightarrow \psi$ a φ, pak je z T dokazatelná i formule ψ. Jsou-li však z T dokazatelné $\varphi \Rightarrow \psi$ a φ, znamená to, že existuje důkaz $\chi_1, \ldots, \chi_n$ formule $\varphi \Rightarrow \psi$ z T a důkaz $\vartheta_1, \ldots, \vartheta_m$ formule φ z T. Podle definice 6.1 tedy máme, že χ_n je formule $\varphi \Rightarrow \psi$ a ϑ_m je formule φ. Nyní však stačí vzít posloupnost $\chi_1, \ldots, \chi_n, \vartheta_1, \ldots, \vartheta_m, \psi$ – – ta je totiž důkazem formule ψ z T. Abychom se o tom přesvědčili, stačí ověřit podmínky definice 6.1. Vezměme libovolnou formuli uvažované posloupnosti. Pak se jedná buď o formuli χ_i (pro nějaké i) nebo o formuli ϑ_j (pro nějaké j) nebo o formuli ψ. V prvním případě (to jest χ_i) uvažujme takto: protože posloupnost $\chi_1, \ldots, \chi_n$ je důkazem, je χ_i axiomem nebo je formulí z T

nebo plyne z nějakých předchozích χ_j, χ_k pomocí modus ponens. Ve druhém případě uvažujme podobně. Ve třetím případě plyne uvažovaná formule (je to ψ) pomocí modus ponens z formulí χ_n (což je $\varphi \Rightarrow \psi$) a ϑ_m (což je φ). Vidíme tedy, že posloupnost $\chi_1, \ldots, \chi_n, \vartheta_1, \ldots, \vartheta_m, \psi$ je důkazem ψ ze systému formulí T, to jest $T \vdash \psi$.
(ii): Předpokládejme, že platí $T \vdash \varphi$. To jest existuje důkaz $\chi_1, \ldots, \chi_n$ z T, kde $\chi_n = \varphi$. Uvažujme posloupnost $\vartheta_1, \ldots, \vartheta_m$, kterou vytvoříme z posloupnosti $\chi_1, \ldots, \chi_n$ tak, že každý člen χ_i, pro který máme $\chi_i \in T$, nahradíme některým jeho důkazem ze systému S (důkaz vždy existuje jelikož $S \vdash \chi_i$), jinými slovy, formuli χ_i „vyjmeme“ z posloupnosti $\chi_1, \ldots, \chi_n$ a na její místo „vložíme důkaz“ formule χ_i z S, což je opět konečná posloupnost formulí. Vzniknuvší posloupnost $\vartheta_1, \ldots, \vartheta_m$ je evidentně důkazem ze S a ϑ_m je formule φ. Dostáváme tedy $S \vdash \varphi$.
(iii): Plyne užitím bodu (ii), protože pokud je $T \subseteq S$, pak každá jednoprvková posloupnost ψ, kde $\psi \in T$, je důkazem z S.
(iv): Nechť $T \vdash \varphi$. Pak existuje důkaz $\chi_1, \ldots, \chi_n$ formule φ ze systému T. Nyní položme $T' = T \cap \{\chi_1, \ldots, \chi_n\}$. Systém formulí T' je zřejmě konečný a $T' \subseteq T$. Posloupnost $\chi_1, \ldots, \chi_n$ je navíc důkazem φ z T'. □

Poznámka 6.5. Při dokazování vlastností syntaktického vyplývání se budeme často odkazovat na odvozovací pravidlo modus ponens – nebudeme jej však používat v konkrétním důkazu, ale budeme jím zdůvodňovat možnost takový důkaz najít. Například o tvrzení (i) lemmy 6.4 můžeme říct, že „plyne užitím modus ponens“.

Průvodce studiem

Při manipulaci s důkazy na obecné úrovni musíme dbát jisté obezřetnosti. Pokud bychom například vzali důkaz $\varphi_1, \ldots, \varphi_n$ z T a „rozstřihli“ jej na dvě části $\varphi_1, \ldots, \varphi_i$ a $\varphi_{i+1}, \ldots, \varphi_n$, pak první část původního důkazu je opět důkazem. Druhá část vzniklá rozstřižením, to jest posloupnost $\varphi_{i+1}, \ldots, \varphi_n$, již důkazem být nutně nemusí, protože se v ní může vyskytovat formule, která není ani axiomem, ani předpokladem z T, ale vznikla pravidlem modus ponens z formulí φ_j, φ_k, které jsou obsaženy pouze mezi formulemi $\varphi_1, \ldots, \varphi_i$.

Pomocí následujícího tvrzení, *věty o dedukci*, se nám podaří výrazně zjednodušit některé úvahy o dokazatelnosti. Na úvod podotkněme, že věta o dedukci formulačně nápadně připomíná tvrzení 1.14 ze strany 15. Vskutku, tvrzení 1.14 je sémantickým ekvivalentem věty o dedukci, jedná se ale o úplně jiné tvrzení, protože nyní pracujeme se syntaktickým vyplýváním a o vztahu $\vdash$ a $\models$ ještě nic nevíme!

Věta 6.6 (o dedukci). *Nechť φ, ψ jsou formule a T je systém formulí. Pak*

$$T \vdash \varphi \Rightarrow \psi, \quad \textit{právě když} \quad T, \varphi \vdash \psi.$$

Důkaz. „$\Rightarrow$“: Předpokládáme-li $T \vdash \varphi \Rightarrow \psi$, pak $T, \varphi \vdash \varphi \Rightarrow \psi$ dle (iii) lemmy 6.4, následně $T, \varphi \vdash \psi$ užitím (i) lemmy 6.4.

„$\Leftarrow$“: Nechť $T, \varphi \vdash \psi$, to jest existuje důkaz $\psi_1, \ldots, \psi_n$ formule ψ z T, φ (ψ_n je ψ). Indukcí dokážeme, že $T \vdash \varphi \Rightarrow \psi_i$ platí pro $i = 1, \ldots, n$, z čehož dostaneme požadovaný vztah jako speciální případ pro $i = n$. Vezměme tedy $i \in \{1, \ldots, n\}$ a předpokládejme, že pro každé $j < i$ platí $T \vdash \varphi \Rightarrow \psi_j$ (indukční předpoklad). Dokážeme, že $T \vdash \varphi \Rightarrow \psi_i$. Podle definice důkazu mohou nastat pouze následující případy:

- ψ_i je axiom nebo formule z T. Pak je posloupnost formulí

$\psi_i \Rightarrow (\varphi \Rightarrow \psi_i)$	*axiom dle V1,*
ψ_i	*podle předpokladu axiom nebo formule z T,*
$\varphi \Rightarrow \psi_i$	*použitím modus ponens,*

  důkazem formule $\varphi \Rightarrow \psi_i$ z T.

- ψ_i je formulí φ, tedy $\varphi \Rightarrow \psi_i$ je tvaru $\varphi \Rightarrow \varphi$. Pak $T \vdash \varphi \Rightarrow \varphi$, viz příklad 6.3.
- ψ_i plyne z předchozích formulí ψ_j, ψ_k pomocí modus ponens, to jest ψ_k je ve tvaru $\psi_j \Rightarrow \psi_i$ a $j, k < i$. Dle indukčního předpokladu existuje důkaz formule $\varphi \Rightarrow \psi_j$ z T a důkaz formule $\varphi \Rightarrow \psi_k$ z T. Přidáme-li k posloupnosti

$$\underbrace{\chi, \ldots, \varphi \Rightarrow \psi_j}_{\text{důkaz } \varphi \Rightarrow \psi_j \text{ z } T}, \underbrace{\vartheta, \ldots, \varphi \Rightarrow (\psi_j \Rightarrow \psi_i)}_{\text{důkaz } \varphi \Rightarrow \psi_k \text{ z } T}$$

formule

$$\begin{array}{ll} (\varphi \Rightarrow (\psi_j \Rightarrow \psi_i)) \Rightarrow ((\varphi \Rightarrow \psi_j) \Rightarrow (\varphi \Rightarrow \psi_i)) & \textit{axiom dle V2,} \\ (\varphi \Rightarrow \psi_j) \Rightarrow (\varphi \Rightarrow \psi_i) & \textit{použitím modus ponens,} \\ \varphi \Rightarrow \psi_i & \textit{použitím modus ponens,} \end{array}$$

pak dostaneme důkaz formule $\varphi \Rightarrow \psi_i$ z T.

Tím jsme tvrzení dokázali. □

Z věty o dedukci snadno dostaneme následující tvrzení.

Lemma 6.7. *Nechť T je systém formulí a φ, ψ, χ jsou formule. Pak platí:*

(i) *$T \vdash \varphi \Rightarrow (\psi \Rightarrow \chi)$, právě když $T, \varphi, \psi \vdash \chi$, právě když $T \vdash \psi \Rightarrow (\varphi \Rightarrow \chi)$;*
(ii) *pokud $T \vdash \varphi \Rightarrow \psi$ a $T \vdash \psi \Rightarrow \chi$, pak $T \vdash \varphi \Rightarrow \chi$ (tranzitivita implikace).*

Důkaz. (i): Plyne násobným užitím věty o dedukci.
(ii): Nechť $T \vdash \varphi \Rightarrow \psi$ a $T \vdash \psi \Rightarrow \chi$. Pak $T, \varphi \vdash \psi$ a $T, \psi \vdash \chi$ z věty o dedukci, tedy užitím bodu (ii) lemmy 6.4 dostáváme $T, \varphi \vdash \chi$, užitím věty o dedukci $T \vdash \varphi \Rightarrow \chi$. □

Tranzitivita implikace je často používaným dokazovacím principem a to i při konstrukci důkazů na úrovni intuice. Význam tranzitivity implikace kopíruje běžný úsudek: platí-li „když A, pak B“ a pokud rovněž platí „když B, pak C“, pak platí „když A, pak C“.

Příklad 6.8. Pro formule φ, ψ dokážeme

$$\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \psi), \tag{6.1}$$
$$\vdash \neg\neg\varphi \Rightarrow \varphi, \tag{6.2}$$
$$\vdash \varphi \Rightarrow \neg\neg\varphi, \tag{6.3}$$
$$\vdash (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi), \tag{6.4}$$
$$\vdash \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)). \tag{6.5}$$

Vztahy (6.1)–(6.5) mají dobrý intuitivní význam. Vztah (6.1) vyjadřuje, že pokud je φ neplatná, pak z platnosti φ plyne libovolné formule. Vztahy (6.2) a (6.3) popisují vlastnosti dvojí negace – – popisují právě to, co na sémantické úrovni vyjadřuje fakt, že φ a $\neg\neg\varphi$ jsou sémanticky ekvivalentní. Vztah (6.4) je duálním vztahem k axiomovému schéma V3 a spolu s V3 popisuje to, co na sémantické úrovni vyjadřuje fakt, že $\varphi \Rightarrow \psi$ a $\neg\psi \Rightarrow \neg\varphi$ jsou sémanticky ekvivalentní. Konečně vztah (6.5) je modifikací vztahu: „z platnosti φ a z platnosti ψ plyne platnost $\varphi \wedge \psi$“.

Následující důkazy není třeba „umět provést z hlavy“, vyskytují se v nich však často používané „triky“, které se vesměs opírají o jednoduché důsledky věty o dedukci. Proto je dobré důkazy pečlivě projít a zdůvodnit si každý krok důkazu. Pro zlepšení čitelnosti je téměř každý krok důkazu stručně okomentován.

„(6.1)“:

$$\begin{array}{ll} \vdash \neg\varphi \Rightarrow (\neg\psi \Rightarrow \neg\varphi) & \textit{axiom dle V1,} \\ \vdash (\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi) & \textit{axiom dle V3,} \\ \vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \psi) & \textit{tranzitivita implikace.} \end{array}$$

„(6.2)“:

$\vdash \neg\neg\neg\varphi \Rightarrow (\neg\neg\varphi \Rightarrow \neg\neg\neg\neg\varphi)$	*tvrzení* (6.1)*,*
$\neg\neg\neg\varphi \vdash \neg\neg\varphi \Rightarrow \neg\neg\neg\neg\varphi$	*věta o dedukci,*
$\vdash (\neg\neg\varphi \Rightarrow \neg\neg\neg\neg\varphi) \Rightarrow (\neg\neg\neg\varphi \Rightarrow \varphi)$	*axiom dle V3,*
$\neg\neg\neg\varphi \vdash (\neg\neg\varphi \Rightarrow \neg\neg\neg\neg\varphi) \Rightarrow (\neg\neg\neg\varphi \Rightarrow \varphi)$	*monotonie dokazatelnosti,*
$\neg\neg\neg\varphi \vdash \neg\neg\neg\varphi \Rightarrow \varphi$	*modus ponens,*
$\neg\neg\neg\varphi \vdash \varphi$	*věta o dedukci,*
$\vdash \neg\neg\neg\varphi \Rightarrow \varphi$	*věta o dedukci.*

„(6.3)“:

$\vdash \neg\neg\neg\neg\varphi \Rightarrow \neg\neg\varphi$	*tvrzení* (6.2)*,*
$\vdash (\neg\neg\neg\neg\varphi \Rightarrow \neg\neg\varphi) \Rightarrow (\neg\neg\varphi \Rightarrow \neg\neg\neg\varphi)$	*axiom dle V3,*
$\vdash \neg\neg\varphi \Rightarrow \neg\neg\neg\varphi$	*modus ponens.*

„(6.4)“:

$\vdash \neg\neg\varphi \Rightarrow \varphi$	*tvrzení* (6.2)*,*
$\varphi \Rightarrow \psi \vdash \neg\neg\varphi \Rightarrow \varphi$	*monotonie dokazatelnosti,*
$\varphi \Rightarrow \psi \vdash \neg\neg\varphi \Rightarrow \psi$	*tranzitivita implikace spolu s* $\varphi \Rightarrow \psi \vdash \varphi \Rightarrow \psi$*,*
$\vdash \psi \Rightarrow \neg\neg\psi$	*tvrzení* (6.3)*,*
$\varphi \Rightarrow \psi \vdash \psi \Rightarrow \neg\neg\psi$	*monotonie dokazatelnosti,*
$\varphi \Rightarrow \psi \vdash \neg\neg\varphi \Rightarrow \neg\neg\psi$	*tranzitivita implikace,*
$\vdash (\neg\neg\varphi \Rightarrow \neg\neg\psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	*axiom dle V3,*
$\varphi \Rightarrow \psi \vdash (\neg\neg\varphi \Rightarrow \neg\neg\psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	*monotonie dokazatelnosti,*
$\varphi \Rightarrow \psi \vdash \neg\psi \Rightarrow \neg\varphi$	*modus ponens,*
$\vdash (\varphi \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg\varphi)$	*věta o dedukci.*

„(6.5)“:

$\varphi, \varphi \Rightarrow \psi \vdash \psi$	*lemma 6.4, bod* (i)*,*
$\varphi \vdash (\varphi \Rightarrow \psi) \Rightarrow \psi$	*věta o dedukci,*
$\vdash ((\varphi \Rightarrow \psi) \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	*tvrzení* (6.4)*,*
$\varphi \vdash ((\varphi \Rightarrow \psi) \Rightarrow \psi) \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	*monotonie dokazatelnosti,*
$\varphi \vdash \neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi)$	*modus ponens,*
$\vdash \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$	*věta o dedukci.*

Ze sporného systému je dokazatelné cokoliv.

Vezmeme-li dva systémy formulí T, S, pak k nim můžeme uvažovat množiny syntaktických důsledků $\{\varphi \mid T \vdash \varphi\}$ a $\{\varphi \mid S \vdash \varphi\}$, které jsou obecně různé. Z monotonie dokazatelnosti ale například víme, že pokud $T \subseteq S$, pak bude i $\{\varphi \mid T \vdash \varphi\} \subseteq \{\varphi \mid S \vdash \varphi\}$. O systému formulí řekneme, že je *sporný,* pokud je z něj dokazatelná jakákoliv formule. V opačném případě řekneme, že systém formulí je *bezesporný.* Je zřejmé, že pokud je T sporný, pak $\{\varphi \mid S \vdash \varphi\} \subseteq \{\varphi \mid T \vdash \varphi\}$ pro každý systém formulí S. Následující tvrzení ukazuje, že spornost systému formulí lze vyjádřit několika ekvivalentními způsoby.

Lemma 6.9. *Následující tvrzení jsou ekvivalentní.*

(i) T *je sporný systém,*
(ii) $T \vdash \varphi$ *a* $T \vdash \neg\varphi$ *pro nějakou formuli* φ*,*
(iii) $T \vdash \neg(\vartheta \Rightarrow \vartheta)$.

Důkaz. „(i) $\Rightarrow$ (ii)“: Pokud je T sporný systém, pak je z něj dokazatelná jakákoliv formule, tedy i formule φ a $\neg\varphi$.
„(ii) $\Rightarrow$ (iii)“: Nechť $T \vdash \varphi$ a $T \vdash \neg\varphi$. Dle vztahu (6.1) máme $\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta))$, z monotonie dokazatelnosti $T \vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta))$. Dvojnásobným použitím modus ponens dostaneme $T \vdash \neg(\vartheta \Rightarrow \vartheta)$.

„(iii) ⇒ (i)“: Nechť φ je libovolná formule. Platí $\vdash \neg(\vartheta \Rightarrow \vartheta) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$ opět dle (6.1). Z monotonie dokazatelnosti $T \vdash \neg(\vartheta \Rightarrow \vartheta) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$. Dále platí, že $T \vdash \vartheta \Rightarrow \vartheta$, viz příklad 6.3, z předpokladu tedy dvojnásobným použitím MP máme $T \vdash \varphi$. □

Důkaz sporem je populární dokazovací princip v informatice a matematice.

Další oblíbený princip, který se často používá v informatice a matematice, je důkaz sporem. Typickým příkladem tvrzení, které se dokazuje sporem, je například tvrzení „Prvočísel je nekonečně mnoho“. Tento fakt prokážeme tak, že předpokládáme neplatnost tvrzení, to jest vyjdeme z toho, že „Prvočísel je konečně mnoho“ a pak úvahou (kterou tu nebudeme popisovat) dojdeme ke sporu. Podrobněji: uvažujeme, že P je konečná množina obsahující všechna prvočísla, potom s využitím toho, že P je konečná, najdeme číslo $n \notin P$ splňující všechny definiční podmínky prvočísla, tudíž bychom měli mít $n \in P$, což je spor. Následující tvrzení ukazuje, že intuitivní důkaz sporem má ve výrokové logice svou formalizaci.

Věta 6.10 (o důkazu sporem). *$T \vdash \varphi$, právě když $T, \neg\varphi$ je sporný systém.*

Důkaz. Nechť $T \vdash \varphi$. Pak zřejmě $T, \neg\varphi \vdash \varphi$ a triviálně též $T, \neg\varphi \vdash \neg\varphi$, což podle bodu (ii) lemmy 6.9 znamená, že T je sporný systém. Naopak, předpokládáme-li že $T, \neg\varphi$ je sporný systém, pak je z $T, \neg\varphi$ dokazatelná formule $\neg(\vartheta \Rightarrow \vartheta)$ dle bodu (iii) lemmy 6.9. Užitím věty o dedukci máme $T \vdash \neg\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta)$. Jelikož $(\neg\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta)) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$ je instance V3, pak z monotonie dokazatelnosti a užitím MP dostáváme $T \vdash (\vartheta \Rightarrow \vartheta) \Rightarrow \varphi$. Dále $\vdash \vartheta \Rightarrow \vartheta$, takže opětovným užitím monotonie dokazatelnosti a MP máme $T \vdash \varphi$. □

Příklad 6.11. Pomocí důkazu sporem prokážeme, že $\vdash (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi)$ a využijeme při tom faktu, že systém formulí $\{\neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi, \neg\psi\}$ je sporný:

$$\begin{array}{rl}
\neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi, \neg\psi \vdash \neg\varphi & \neg\psi \Rightarrow \neg\varphi,\ \neg\psi,\ \textit{MP,} \\
\neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi, \neg\psi \vdash \varphi & \neg\psi \Rightarrow \varphi,\ \neg\psi,\ \textit{MP,} \\
\neg\psi \Rightarrow \neg\varphi, \neg\psi \Rightarrow \varphi \vdash \psi & \textit{důkaz sporem,} \\
\vdash (\neg\psi \Rightarrow \neg\varphi) \Rightarrow ((\neg\psi \Rightarrow \varphi) \Rightarrow \psi) & \textit{dvakrát věta o dedukci.}
\end{array}$$

6.2 Korektnost a úplnost výrokové logiky

Sémantické vyplývání zavádíme pro obecný systém předpokladů.

Nyní se budeme věnovat vzájemnému vztahu sémantického a syntaktického vyplývání. V kapitole 1.2.2 jsme zavedli sémantické vyplývání formule φ z formulí $\psi_1, \ldots, \psi_n$. Obecněji bychom mohli uvažovat sémantické vyplývání z libovolného systému formulí T takto: formule φ sémanticky plyne ze systému T, pokud pro každé pravdivostní ohodnocení e, při kterém máme $\|\psi\|_e = 1$ pro všechny $\psi \in T$, platí $\|\varphi\|_e = 1$. Je zřejmé, že sémantické vyplývání z konečně mnoha formulí $\psi_1, \ldots, \psi_n$ tak, jak bylo zavedeno v definici 1.11, je nyní speciálním případem sémantického vyplývání z $T = \{\psi_1, \ldots, \psi_n\}$. O systému formulí T řekneme, že je *splnitelný,* pokud existuje pravdivostní ohodnocení e takové, že pro každou $\psi \in T$ máme $\|\psi\|_e = 1$. V opačném případě se T nazývá *nesplnitelný.*

$\vdash$ a $\vDash$ lze chápat jako relace.

Ještě než ukážeme základní výsledky o vztahu syntaktického a sémantického vyplývání, zamysleme se nad tím, jak lze tyto pojmy chápat. Pokud bychom označili Fml množinu všech formulí jazyka VL, ve kterém pracujeme, pak potenční množina 2^{Fml} je vlastně množinou všech systémů formulí ($T \in 2^{Fml}$ potom znamená, že T je systém formulí). Syntaktické vyplývání je tedy relace $\vdash \subseteq 2^{Fml} \times Fml$, přitom $T \in 2^{Fml}$ je v relaci $\vdash$ s $\varphi \in Fml$, právě když φ je dokazatelná z T. Stejně tak sémantické vyplývání lze chápat jako relaci $\vDash \subseteq 2^{Fml} \times Fml$, kde $T \in 2^{Fml}$ je v relaci $\vDash$ s $\varphi \in Fml$, právě když φ sémanticky plyne z T. Vyšetřování vzájemného vztahu obou vyplývání lze tedy chápat jako určení vzájemného vztahu dvou relací. Následující tvrzení ukazuje, že $\vdash \subseteq \vDash$.

Věta 6.12 (o korektnosti VL). *Pokud $T \vdash \varphi$, pak $T \vDash \varphi$. Sporný systém formulí není splnitelný.*

Důkaz. Nejprve prokážeme, že pokud $\vdash \varphi$, pak je φ tautologie. To ukážeme indukcí tak, že o každém prvku důkazu $\varphi_1, \ldots, \varphi_n$ formule φ (z prázdné množiny předpokladů) dokážeme, že

je tautologie. Tvrzení tak získáme jako speciální případ pro formuli φ_n, kterážto je formulí φ. Uvažujme formuli φ_i ($i = 1, \ldots, n$). Mohou nastat dvě situace. V prvním případě je φ_i axiomem, je tedy instancí některého ze schémat V1–V3. Pak je φ_i tautologie, o čemž se můžete snadno přesvědčit tabulkovou metodou. V druhém případě byla formule φ_i odvozena z některých předchozích formulí pravidlem modus ponens. Mějme tedy φ_j, φ_k, kde $j, k < i$ a nechť φ_k je ve tvaru $\varphi_j \Rightarrow \varphi_i$. Pak z indukčního předpokladu jsou φ_j a $\varphi_j \Rightarrow \varphi_i$ tautologie. Vezmeme-li libovolné pravdivostní ohodnocení e, pak $\|\varphi_j\|_e = 1$ a $\|\varphi_j \Rightarrow \varphi_i\|_e = 1 \to \|\varphi_i\|_e = 1$. Odtud díky vlastnostem logické operace $\to$ dostáváme $\|\varphi_i\|_e = 1$, z čehož plyne, že φ_i je tautologie.

Nyní uvažujme, že $T \vdash \varphi$, pak dle (iv) lemmy 6.4 existuje konečná $\{\chi_1, \ldots, \chi_k\} \subseteq T$ tak, že $\chi_1, \ldots, \chi_k \vdash \varphi$. Opakovaným použitím věty o dedukci na $\chi_1, \ldots, \chi_k \vdash \varphi$ dostáváme

$$\vdash \chi_1 \Rightarrow (\chi_2 \Rightarrow (\cdots(\chi_k \Rightarrow \varphi)\cdots)).$$

Podle výše prokázaného faktu je $\chi_1 \Rightarrow (\chi_2 \Rightarrow (\cdots(\chi_k \Rightarrow \varphi)\cdots))$ tautologie, to jest

$$\vDash \chi_1 \Rightarrow (\chi_2 \Rightarrow (\cdots(\chi_k \Rightarrow \varphi)\cdots)).$$

Aplikací věty 1.14 dostáváme $\chi_1, \ldots, \chi_k \vDash \varphi$. Nyní stačí ukázat, že i $T \vDash \varphi$, což je ovšem jednoduchý důsledek vlastností sémantického vyplývání: pokud jsou při ohodnocení e pravdivé všechny formule z T, pak jsou při e pravdivé i formule $\{\chi_1, \ldots, \chi_k\} \subseteq T$, to jest z $\chi_1, \ldots, \chi_k \vDash \varphi$ dostáváme $\|\varphi\|_e = 1$. Dokázali jsme tedy $T \vDash \varphi$.

Druhá část tvrzení je nyní důsledkem první: pokud je T sporný systém, pak $T \vdash \neg(\vartheta \Rightarrow \vartheta)$, tedy $T \vDash \neg(\vartheta \Rightarrow \vartheta)$. Odtud dostáváme, že $\neg(\vartheta \Rightarrow \vartheta)$ musí být pravdivá při každém ohodnocení, při kterém jsou pravdivé všechny formule z T. Ale $\neg(\vartheta \Rightarrow \vartheta)$ je kontradikce, tedy neexistuje žádné ohodnocení e, při kterém by byly všechny formule z T pravdivé. Tím jsme prokázali, že sporný systém formulí není splnitelný. □

Poznámka 6.13. V důkazu věty jsme ukázali, že z faktu „pokud $T \vdash \varphi$, pak $T \vDash \varphi$“ vyplývá, že žádný sporný systém není splnitelný. Obě dvě části věty o korektnosti (tvrzení 6.12) jsou však ekvivalentní, tvrzení lze tedy dokázat i obráceně. Kdybychom předpokládali, že žádný sporný systém není splnitelný a $T \vdash \varphi$, pak z věty o důkazu sporem víme, že $T, \neg\varphi$ je sporný systém, tedy dle předpokladu by byl nesplnitelný. Pro každé pravdivostní ohodnocení e, při kterém by byly všechny formule z T pravdivé bychom tím pádem museli mít $\|\neg\varphi\|_e = 0$, tedy $\|\varphi\|_e = 1$. V důsledku tedy $T \vDash \varphi$.

Shrneme-li předchozí poznatky, zavedli jsme dva druhy vyplývání: $\vDash$, $\vdash$ a již víme, že každá formule dokazatelná z prázdného systému je tautologie a obecněji $T \vdash \varphi$ implikuje $T \vDash \varphi$, neboli: „to co je dokazatelné z nějakého systému, z tohoto systému rovněž sémanticky plyne“. Mnohem méně průhledná je opačná strana tohoto tvrzení, která rovněž platí. To jest platí, že „pokud je φ sémantickým důsledkem T, pak je φ z T dokazatelná“. V důsledku tedy docházíme k tomu, že relace $\vDash$ a $\vdash$ splývají ($\vdash = \vDash$), což je odpověď na motivační otázku z úvodu kapitoly. Následující tvrzení shrnuje právě popsaný vztah, tvrzení si nebudeme dokazovat, protože to přesahuje rámec tohoto textu, čtenáře odkazujeme na [Soch01, Šve02].

Věta 6.14 (o úplnosti VL).
$T \vdash \varphi$, právě když $T \vDash \varphi$. Systém formulí je bezesporný, právě když je splnitelný. □

Průvodce studiem

Výrokový kalkul, který jsme představili v kapitolách 1.2 a 6.1 je *úplný*. Znamená to, že formule φ je sémantickým důsledkem systému předpokladů T, právě když je φ z T dokazatelná. Věta o úplnosti je netriviální charakterizace logického kalkulu. Téměř všechny relevantní logické kalkuly, které pracují s pojmy *dokazatelnost* a *sémantické vyplývání* mají

„svou větu o úplnosti“, ačkoliv úplnost některých logických kalkulů prokázat nelze. Základním kritériem „rozumnosti logického kalkulu“ je platnost věty o korektnosti. Nekorektní kalkuly se nechovají přirozeně – dokázaná tvrzení v nich obecně nejsou pravdivá.

Korektnost lze využít k prokázání faktu, že některá *formule není dokazatelná z jistého systému předpokladů.* Reformulací korektnosti totiž dostáváme, že pokud φ sémanticky neplyne z T, pak φ není ze systému T ani dokazatelná (rozmyslete si podrobně proč je tomu tak). K tomu, abychom prokázali, že $T \nvdash \varphi$ tedy stačí ukázat $T \nvDash \varphi$, což je výrazně jednodušší než prokázat „neexistenci důkazu“, protože důkazů, jakožto konečných posloupností formulí, je obecně nekonečně mnoho.

Příklad 6.15. Prokážeme, že $p \Rightarrow q \nvdash \neg p \Rightarrow q$. Z věty o korektnosti výrokové logiky stačí ukázat, že $p \Rightarrow q \nvDash \neg p \Rightarrow q$. To jest zbývá najít pravdivostní ohodnocení e, takové, že $\|p \Rightarrow q\|_e = 1$, ale $\|\neg p \Rightarrow q\|_e = 0$. S využitím vlastností logické operace $\rightarrow$ zřejmě stačí vzít pravdivostní ohodnocení e, kde $e(p) = 0$ a $e(q) = 0$. Tím je důkaz hotov.

Shrnutí

Syntaktické vyplývání ve výrokové logice je založeno na pojmu důkaz, což je konečná posloupnost formulí, v níž každá formule je buď axiomem, předpokladem z daného systému formulí, nebo vzniká pomocí odvozovacího pravidla modus ponens z formulí předcházejících v této posloupnosti. Dokazatelnost formule je tedy zavedena bez jakékoliv vazby na sémantické pojmy jako je pravdivostní ohodnocení a je v podstatě založena pouze na manipulaci s formulemi, které chápeme jako řetězce symbolů jazyka výrokové logiky bez jakékoliv interpretace.
O vztahu syntaktického vyplývání (dokazatelnosti) a sémantického vyplývání vypovídají věty o korektnost a o úplnosti. Věta o korektnosti říká, že každá formule dokazatelná z daného systému předpokladů je rovněž sémantickým důsledkem tohoto systému. Úplnost výrokové logiky je netriviální charakterizace VL a vyjadřuje, že formule je dokazatelná z daného systému formulí, právě když z tohoto systému sémanticky plyne.

Pojmy k zapamatování

- odvozovací pravidlo, pravidlo odloučení, modus ponens,
- předpoklady, systém formulí,
- axiom, axiomové schéma, instance schéma, axiomatický systém,
- důkaz, dokazatelnost, syntaktické vyplývání,
- spornost, bezespornost,
- splnitelnost, nesplnitelnost,
- korektnost, úplnost

Kontrolní otázky

1. *Z čeho se skládá axiomatický systém výrokové logiky?*
2. *Může být někdy kontradikce dokazatelná?*
3. *Jaký je vztah syntaktického a sémantického vyplývání?*
4. *Může být prázdný systém formulí sporný?*

Cvičení

1. Dokažte následující tvrzení.
   (a) T je bezesporný systém, právě když $\neg(\vartheta \Rightarrow \vartheta)$ není dokazatelná z T.
   (b) Pokud $T \vdash \varphi$, pak existuje nekonečně mnoho vzájemně různých důkazů φ z T.

(c) Pokud $T \vdash \varphi \Rightarrow \psi$ a $S \vdash \psi \Rightarrow \vartheta$, pak $T \cup S \vdash \varphi \Rightarrow \vartheta$.
(d) T je bezesporný, právě když je každý konečný $T' \subseteq T$ bezesporný.

2. Bez použití věty o úplnosti VL dokažte následující tvrzení.
   (a) $\varphi \wedge \psi \vdash \varphi$,
   (b) $\varphi \wedge \psi \vdash \psi$,
   (c) $\vdash (\varphi \wedge \psi) \Rightarrow \chi$, právě když $\vdash \varphi \Rightarrow (\psi \Rightarrow \chi)$,
   (d) $T \vdash \varphi$ a zároveň $T \vdash \psi$, právě když $T \vdash \varphi \wedge \psi$.
   (e) $T \vdash \varphi \Rightarrow \psi$ a zároveň $T \vdash \psi \Rightarrow \varphi$, právě když $T \vdash \varphi \Leftrightarrow \psi$.

Úkoly k textu

1. Předpokládejme, že syntaktické vyplývání ve výrokové logice modifikujeme tak, že budeme kromě odvozovacího pravidla modus ponens uvažovat vždy navíc ještě jedno z následujících odvozovacích pravidel

$$\frac{\neg\psi,\ \varphi \Rightarrow \psi}{\neg\varphi}, \qquad \frac{\varphi}{\varphi \wedge (\varphi \vee \psi)}, \qquad \frac{\psi,\ \varphi \Rightarrow \psi}{\varphi \wedge \psi}, \qquad \frac{\varphi}{\varphi \wedge \psi}, \qquad \frac{\varphi \Rightarrow \psi,\ \neg\varphi \Rightarrow \psi}{\psi}.$$

   Rozhodněte, pro která z výše uvedených odvozovacích pravidel bude i nadále možné prokázat větu o korektnost výrokové logiky rozšířené o dané odvozovací pravidlo.

Řešení

1. (a) Dostáváme obměnou ekvivalentních tvrzení z lemmy 6.9.
   (b) Pokud $T \vdash \varphi$ pak existuje důkaz $\varphi_1, \ldots, \varphi_k$ formule φ z T. Nechť nyní $n\psi$ označuje n-prvkovou posloupnost $\psi, \ldots, \psi$. Vezmeme-li posloupnosti ve tvaru $n\psi, \varphi_1, \ldots, \varphi_k$, kde ψ je axiom a $n \in \mathbb{N}$, pak každá taková posloupnost je důkaz φ z T.
   (c) Tvrzení plyne z monotonie dokazatelnosti a z tranzitivity implikace.
   (d) Pokud je T bezesporný, pak nějaká φ není dokazatelná z T, tím spíš není dokazatelná z konečného podsystému T. To jest z bezespornosti T plyne bezespornost každého konečného podsystému $T' \subseteq T$. Pokud je T sporný, pak $T \vdash \neg(\vartheta \Rightarrow \vartheta)$ to jest existuje konečná množina formulí $\{\chi_1, \ldots, \chi_k\} \subseteq T$ taková, že $\chi_1, \ldots, \chi_k \vdash \neg(\vartheta \Rightarrow \vartheta)$, odtud dostáváme, že $\{\chi_1, \ldots, \chi_k\}$ je sporný.
2. (a) Připomeňme, že $\varphi \wedge \psi$ chápeme jako zkratku za formuli $\neg(\varphi \Rightarrow \neg\psi)$. Platí

$\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg\psi)$	*tvrzení* (6.1)*,*
$\vdash (\neg\varphi \Rightarrow (\varphi \Rightarrow \neg\psi)) \Rightarrow (\neg(\varphi \Rightarrow \neg\psi) \Rightarrow \neg\neg\varphi)$	*tvrzení* (6.4)*,*
$\vdash \neg(\varphi \Rightarrow \neg\psi) \Rightarrow \neg\neg\varphi$	*modus ponens,*
$\vdash \neg(\varphi \Rightarrow \neg\psi) \Rightarrow \varphi$	*tvrzení* (6.2)*, tranzitivita implikace,*
$\vdash (\varphi \wedge \psi) \Rightarrow \varphi$	*zkratka za formuli.*

   Tvrzení (b) se dokazuje analogicky jako (a), využijte přitom axiomové schéma V1.
   Nyní ukážeme (c). Nechť $\vdash (\varphi \wedge \psi) \Rightarrow \chi$. Z věty o dedukci máme $\varphi \wedge \psi \vdash \chi$. Navíc platí

$\varphi \Rightarrow \neg\psi, \varphi \vdash \neg\psi$	*modus ponens,*
$\varphi \vdash (\varphi \Rightarrow \neg\psi) \Rightarrow \neg\psi$	*věta o dedukci,*
$\varphi \vdash ((\varphi \Rightarrow \neg\psi) \Rightarrow \neg\psi) \Rightarrow (\neg\neg\psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi))$	*tvrzení* (6.4)*,*
$\varphi \vdash \neg\neg\psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi)$	*modus ponens,*
$\varphi \vdash \psi \Rightarrow \neg(\varphi \Rightarrow \neg\psi)$	(6.3) *a tranzitivita implikace,*
$\varphi \vdash \psi \Rightarrow (\varphi \wedge \psi)$	*zkratka za formuli,*
$\varphi, \psi \vdash \varphi \wedge \psi$	*věta o dedukci.*

   Nyní z $\varphi, \psi \vdash \varphi \wedge \psi$ a $\varphi \wedge \psi \vdash \chi$ dostáváme $\varphi, \psi \vdash \chi$. Dále dvojnásobným užitím věty o dedukci dostáváme $\vdash \varphi \Rightarrow (\psi \Rightarrow \chi)$, což bylo dokázat.

Předpokládejme $\vdash \varphi \Rightarrow (\psi \Rightarrow \chi)$. Z věty o dedukci $\varphi, \psi \vdash \chi$. Aplikací bodů (a), (b) dostáváme $\varphi \wedge \psi \vdash \varphi$ a $\varphi \wedge \psi \vdash \psi$. To jest v důsledku $\varphi \wedge \psi \vdash \chi$. Užitím věty o dedukci $\vdash (\varphi \wedge \psi) \Rightarrow \chi$, což je požadované tvrzení. Dohromady jsme prokázali platnost bodu (c).
Tvrzení (d) plyne z bodů (a), (b), věty o dedukci a užitím $\vdash \varphi \Rightarrow (\psi \Rightarrow (\varphi \wedge \psi))$.
Bod (e) je bezprostředním důsledkem (d).

Studijní cíle: Kapitola studenty seznamuje se základy predikátové logiky, zejména se základními syntaktickými pojmy. Po prostudování kapitoly by student měl umět číst a zapisovat formule v daném jazyku predikátové logiky a měl by být schopen k dané problémové doméně vhodně navrhnout jazyk a být schopen popisu pozorovaných vztahů pomocí formulí.

Klíčová slova: arita, atomická formule, existenční kvantifikátor, formule, funkční symbol, individuum, jazyk PL, jazyk s rovností, konstanta, kvantifikátor, proměnná, relační symbol, syntaxe, term, typ jazyka, všeobecný kvantifikátor

Potřebný čas: 150 minut.

6.3 Predikátová logika

Formulemi *výrokové logiky* jsme formalizovali intuitivní pojem výrok a dovedli jsme jimi popsat skládání složitějších výroků z jednodušších pomocí logických spojek. Výroky, které byly dále nedělitelné, jsme označovali výrokovými symboly a vnitřní strukturou těchto výroků jsme se nezabývali. Naproti tomu predikátová logika (PL), kterou si stručně představíme v této kapitole, formalizuje vztahy mezi *individui* neboli *objekty*, například jejich funkční závislosti, vlastnosti a vzájemné vztahy. Oproti výrokové logice se tedy na tvrzení díváme daleko jemnějším pohledem a formule predikátové logiky to musí pochopitelně zohledňovat. Nyní si na příkladu ukážeme, co máme konkrétně na mysli pod pojmem „vztahy mezi individui“. Například tvrzení

Predikátová logika formalizuje usuzování o individuích.

„Pokud je x sudé číslo, pak je $x + 1$ liché“

je z pohledu výrokové logiky ve tvaru implikace dvou výroků a je tudíž formalizovatelné výrokovou formulí $p \Rightarrow q$. Z pohledu predikátové logiky se ale ve tvrzení vyskytují individua (*čísla*), jejich vlastnosti (*být sudé*, *být liché*) a funkční závislosti ($x + 1$ *je následníkem* x, nebo podrobněji 1 označuje *individuum* a „+“ označuje funkční závislost dvou individuí, v našem případě individuí označených x a 1). Dalším typickým rysem je vytváření výroků kvantifikací, kterou ve slovním popisu vyjadřujeme obraty „každý“, „nějaký“, „právě jeden“ a podobně. Například ve tvrzení

„Každý člověk má otce“

se vyskytuje kvantifikátor „každý“. Kdybychom si toto tvrzení reformulovali poněkud kostrbatěji, mohlo by znít: „Pro každého člověka platí, že má otce“. Vazbu „mít otce“ bychom mohli chápat hned několika způsoby, například jako vlastnost (člověk A má otce), nebo třeba jako vztah dvou individuí (člověk B je otcem člověka A). V druhém případě je navíc v tvrzení skryt další kvantifikátor: „ke každému člověku A *existuje* jeho otec B“. Stejně jako ve výrokové logice se budeme v predikátové logice soustředit na *formu usuzovaného* a budeme abstrahovat od obsahu sdělení.

6.3.1 Syntax predikátové logiky

Podobně jako ve výrokové logice nejprve navrhneme formální jazyk predikátové logiky a poté zavedeme formule daného jazyka. Na rozdíl od výrokové logiky však jazyk v predikátové logice hraje daleko důležitější roli. Při popisu jednotlivých problémových domén (vlastností čísel, popisu struktury počítačové sítě a tak dále) je totiž obecně potřeba pracovat s různými

vlastnostmi a vztahy, například „být sudý“, „být menší než“, nebo „být propojen s daným uzlem“, „mít záložní zdroj“ a podobně. Jazyk predikátové logiky budeme definovat tak, aby nám vždy jednoznačně určoval, jaké funkční závislosti, vlastnosti a vztahy budeme moci ve formulích používat. Každý uvažovaný jazyk predikátové logiky je proto určen svým typem.

Jazyk PL je určen svým typem.

Definice 6.16. *Typ jazyka* predikátové logiky je trojice $\langle R, F, \sigma \rangle$, kde R je množina *relačních symbolů,* F je množina *funkčních symbolů,* kde $R \cap F = \emptyset$, σ je zobrazení $\sigma \colon R \cup F \to \mathbb{N} \cup \{0\}$, které každému relačnímu a funkčnímu symbolu $s \in R \cup F$ přiděluje jeho *aritu* $\sigma(s) \in \mathbb{N} \cup \{0\}$.

Relační symboly zastupují *jména pro vlastnosti a vztahy, funkční symboly* zastupují *jména funkčních závislostí.* Arita symbolů neformálně řečeno vyjadřuje „počet individuí“, která se daného vztahu či funkční závislosti účastní. Příkladem vztahu v němž vystupuje jedno individuum je vztah (vlastnost) „být sudý“, naproti tomu vztah „být větší než“ je vztah, jehož se účastní dvě individua a tak podobně. Je-li $\sigma(f) = 0$, pak se symbol f nazývá *nulární,* pro $\sigma(f) = 1$ se f nazývá *unární,* pro $\sigma(f) = 2$ se f nazývá *binární,* pro $\sigma(f) = 3$ se f nazývá *ternární,* pro $\sigma(f) = 4$ se f nazývá *kvaternární* a tak dále. Nulární relační symboly nazýváme *výrokové symboly* a v jazyku predikátové logiky mají analogickou roli jako výrokové symboly v jazyku výrokové logiky – jedná se tedy o vztahy, do kterých nevstupují žádná individua. Nulární funkční symboly se nazývají *konstanty.*

Relační symboly zastupují jména vlastností a vztahů.

Funkční symboly zastupují jména funkčních závislostí.

Jazyk predikátové logiky typu $\langle R, F, \sigma \rangle$ se skládá z

- (*předmětových*) *proměnných*: x, y, z, ... různých od symbolů z množin R a F,
- *množiny relačních symbolů* R,
- *množiny funkčních symbolů* F,
- *symbolů logických spojek*:
  $\neg$ (negace), $\Rightarrow$ (implikace), $\wedge$ (konjunkce), $\vee$ (disjunkce), $\Leftrightarrow$ (ekvivalence),
- *symbolů kvantifikátorů*: $\forall$ (všeobecný kvantifikátor), $\exists$ (existenční kvantifikátor),
- *pomocných symbolů*: *závorek* $(,)$.

Jazyk predikátové logiky je tedy jednoznačně určen svým typem. V predikátové logice se zvláštním způsobem pracuje s jazyky, které obsahují speciální *binární relační symbol* $\approx$ – – symbol *rovnosti.* Jazykům, které obsahují $\approx$ říkáme *jazyky s rovností.* Pro jazyk s rovností jinými slovy máme $\approx \in R$, kde $\sigma(\approx) = 2$. Jelikož je $\approx$ vždy binární symbol, nebudeme aritu symbolu $\approx$ dále zdůrazňovat. Důvod pro rozlišení jazyků s rovností objasníme v kapitole 6.5.

Příklad 6.17. Navrhneme jazyky pro formalizaci následujících tvrzení.

Před formalizací tvrzení je nejprve nutné zvolit jazyk.

(1) „Některé dopravní prostředky mají dvě kola.“
(2) „Každý uzel v počítačové síti má aspoň jednoho souseda.“
(3) „Pokud je x sudé číslo, pak je $x + 1$ liché.“

Ad (1): Uvažujme jazyk s rovností, kde $F = \{\mathit{dvě}, \mathit{pkol}\}$, $\sigma(\mathit{dvě}) = 0$, $\sigma(\mathit{pkol}) = 1$ a dále mějme $R = \{\approx, \mathit{prostředek}\}$, kde $\sigma(\mathit{prostředek}) = 1$. Relační symbol *prostředek* reprezentuje vlastnost „být dopravním prostředkem“, konstanta *dvě* reprezentuje počet a *pkol* můžeme chápat jako funkční závislost mezi individuem (třeba dopravním prostředkem) a jeho počtem kol. Navržený jazyk není jediný přípustný. Stejně tak bychom v tomto případě mohli navrhnout jazyk bez rovnosti, ve kterém bude $F = \emptyset$.

Ad (2): Uvažujme například $F = \emptyset$, $R = \{\mathit{uzel}, \mathit{sousedí}\}$, kde $\sigma(\mathit{uzel}) = 1$, $\sigma(\mathit{sousedí}) = 2$. Unární relační symbol *uzel* reprezentuje vlastnost „být uzlem v síti“, binární relační symbol *sousedí* představuje „sousedský vztah“ mezi dvěma uzly. „Sousedství uzlů“ bychom teoreticky mohli chápat i jako funkční závislost „uzel je sousedem daného uzlu“, v tomto případě by ale na každém uzlu byl funkčně závislý právě jeden uzel, který by byl jeho sousedem, což může být nežádoucí v situaci, kde je třeba zohlednit, že sousedních uzlů může být větší počet, případně nemusí být žádný.

Ad (3): Nyní již stručně, $F = \{plus, 1\}$, kde $\sigma(plus) = 2$, $\sigma(1) = 0$ a $R = \{sudé, liché\}$, kde shodně $\sigma(sudé) = \sigma(liché) = 1$. Upozorněme na fakt, že funkční symbol 1 je pro nás konstanta, kterou v žádném případě *nelze ztotožňovat* s přirozeným číslem 1. Jazyk, coby součást syntaxe predikátové logiky, nemá sám o sobě žádnou sémantickou interpretaci.

Proměnné (*předmětové proměnné*), kterých v jazyku PL uvažujeme vždy nekonečně mnoho, zastupují jednotlivá individua. Zde ovšem zdůrazněme, že dvě různé proměnné x, y mohou zastupovat totéž individuum. Ve tvrzeních formulovaných v přirozeném jazyku se často setkáme s tím, že „vyjadřujeme individua z jiných individuí" pomocí jejich vzájemných *přiřazení* neboli funkčních závislostí. Příkladem jsou obraty typu „bratrovo auto", „včerejší oběd", „přepona pravoúhlého trojúhelníka o stranách x, y a z", „druhá mocnina x" a podobně. V jazyku PL máme jména funkčních závislostí formalizována *funkčními symboly,* pro účely formalizace funkčních vztahů mezi individui zavedeme pojem *term*.

Termy vyjadřují individua z jiných individuí.

Definice 6.18 (termy). *Term* jazyka PL typu $\langle R, F, \sigma\rangle$ je definován následovně:

- každá proměnná x je term,
- nechť $f \in F$, $\sigma(f) = k$ a $t_1, \ldots, t_k$ jsou libovolné termy, pak $f(t_1, \ldots, t_k)$ je term.

Příklad 6.19. Mějme typ jazyka $\langle R, F, \sigma\rangle$, kde $F = \{f, g, s\}$, $\sigma(f) = 2$, $\sigma(g) = 1$ a $\sigma(s) = 0$. Pak například x, s, $g(x)$, $f(x, s)$, $f(g(g(x)), f(s, s))$ jsou termy jazyka tohoto typu. Na druhou stranu třeba $f(x)$, $f(s, f)$, g nejsou termy tohoto jazyka.

Individua jsou ve slovním popisu zastoupena jmennými vazbami.

Pokud bychom dostali za úkol identifikovat individua ve slovním (neformálním) popisu, pak se můžeme řídit několika jednoduchými poučkami. Individua jsou ve větách přirozeného jazyka zastoupena *podstatnými jmény* nebo *jmennými vazbami.* Po rozlišení jednotlivých individuí obsažených ve slovním popisu a po klasifikaci jejich vzájemné funkční závislosti můžeme stanovit všechny funkční symboly, které se v daném jazyku budou vyskytovat. Speciální roli zde hrají *konstanty – nulární funkční symboly,* které označují jednotlivá „neměnná individua".

Příklad 6.20. V následujících větách nalezneme individua, funkční závislosti a všechna individua formalizujeme pomocí termů.

(1) „Cigaretový kouř je nezdravý.",
(2) „Rychlost kamarádova auta je v dešti nízká.",
(3) „Součet vnitřních úhlů trojúhelníka je 180°",

Ad (1): V prvním případě je zřejmě individuem „kouř". Otevřenou otázkou ale je, zda-li bychom měli chápat slovní spojení „cigaretový kouř" jako vyjádření funkční závislosti, či nikoliv. To, že kouř je cigaretový, bychom mohli také chápat jako *vlastnost,* nikoliv funkční závislost.

V případě, že bychom potřebovali mít tento fakt vyjádřený funkční závislostí, měli bychom uvažovat funkční symboly $F = \{kouř, cigareta\}$, kde $\sigma(kouř) = 1$, $\sigma(cigareta) = 0$. Funkční symbol *cigareta* je nulární, jedná se tudíž o *konstantu.* Funkční symbol *kouř* je unární, term tvaru $kouř(x)$ chápeme jako vyjádření: „Kouř individua x". Term vyjadřující slovní spojení „cigaretový kouř" by pak měl tvar $kouř(cigareta)$.

Další slovní obrat vyskytující se ve větě je „být nezdravý". Tento obrat nerepresentuje žádné individuum ani nepopisuje žádnou funkční závislost, to jest neformalizujeme jej termem.

Ad (2): V tomto případě se nabízí formalizovat termem „rychlost kamarádova auta v dešti". Individuum označující rychlost je v tomto případě závislé na dvou argumentech – na vozidle a na podmínkách jeho provozu. Sousloví „kamarádovo auto" pak můžeme vyjádřit analogicky jako sousloví „cigaretový kouř" v předchozím příkladě. To jest položme $F = \{rychlost, auto, kamarád, déšť\}$, kde $\sigma(kamarád) = \sigma(déšť) = 0$, $\sigma(auto) = 1$ a $\sigma(rychlost) = 2$. V následující tabulce jsou uvedeny termy a jejich význam.

kamarádovo auto	$auto(kamarád)$,
rychlost x v dešti	$rychlost(x, déšť)$,
rychlost kamarádova auta v dešti	$rychlost(auto(kamarád), déšť)$,

Množinu funkčních symbolů bychom mohli zjednodušit. Například „kamarádovo auto“ bychom mohli označit jednou konstantou a podobně. Návrh jazyka a míru zjednodušení je vždy nutné pečlivě zvážit. Slovní spojení „být nízký“, které se ve větě vyskytuje, vyjadřuje vlastnosti (v tomto případě vlastnost individua reprezentující rychlost onoho vozidla za deště), takže se nejedná o funkční závislost a vazbu proto neformalizujeme termem.

Ad (3): Zde můžeme popsat termem vazbu „součet vnitřních úhlů trojúhelníka“. Metod, kterak tohoto cíle dosáhnout, je samozřejmě více. Je například možné zavést binární funkční symbol pro „sčítání“ a vyjádřit součet pomocí něj. Konkrétně, když položíme $F = \{+\}$, $\sigma(+) = 2$, pak například termem $+(+(x, y), z)$ vyjádříme požadovanou funkční závislost. Termy jako je $+(+(x, y), z)$ obvykle pro přehlednost zapisujeme v infixové notaci, tedy ve tvaru $(x + y) + z$. Důležité je uvědomit si, že pouhou definicí funkčního symbolu „$+$“ samozřejmě nijak nezajistíme „žádné očekávané vlastnosti sčítání“. Na úrovni termů nemáme ani nijak zachyceno, že x, y a z označují „strany trojúhelníka“. Druhou možností, jak vyjádřit sčítání, je zavedení ternárního funkčního symbolu. Například pro $F = \{součet\_tří\}$, $\sigma(součet\_tří) = 3$ bychom mohli předchozí fakt vyjádřit termem $součet\_tří(x, y, z)$. Dalším individuem může být velikost úhlu $180°$, i když opět ji můžeme chápat jako vlastnost „mít velikost $180°$“.

Termy někdy pro přehlednost zapisujeme v infixové notaci.

V předchozí ukázce jsme vždy zdůrazňovali, že termy samy o sobě nelze použít k popisu vlastností individuí nebo jejich vzájemných vztahů. K tomuto účelu slouží formule. *Formule* jsou přesným zavedením tvrzení o individuích, viz následující definici.

Definice 6.21 (formule). *Formule* jazyka PL typu $\langle R, F, \sigma\rangle$ je definována následovně:

- je-li $r \in R$, $\sigma(r) = n$ a $t_1, \ldots, t_n$ jsou termy jazyka PL typu $\langle R, F, \sigma\rangle$, pak $r(t_1, \ldots, t_n)$ je (*atomická*) formule.
- nechť φ, ψ jsou formule jazyka PL typu $\langle R, F, \sigma\rangle$ a nechť x je proměnná, pak $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$, $(\forall x)\varphi$, $(\exists x)\varphi$ jsou formule.

Formule jsou přesným zavedením tvrzení o individuích.

Poznámka 6.22. Dále budeme používat běžnou konvenci o vynechávání vnějších závorek, kterou jsme přijali už v úvodu do výrokové logiky. Pokud bude jazyk PL a jeho typ patrný z kontextu, nebudeme jej zdůrazňovat. Stejně tak jako ve výrokové logice bychom mohli přijmout za základní symboly výrokových spojek pouze $\neg, \Rightarrow$ a výrazy tvaru $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \Leftrightarrow \psi$ bychom mohli chápat jako zkratky za formule obsahující pouze spojky negaci a implikaci.

Příklad 6.23. Mějme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $F = \{f, c\}$, $R = \{\approx, q, r, s\}$, a $\sigma(f) = 1$, $\sigma(c) = 0$, $\sigma(q) = 0$, $\sigma(r) = 1$, $\sigma(s) = 2$. Pak například q, $c \approx f(c)$, $r(x) \Rightarrow (\forall x)r(x)$, $(\exists x)(r(f(x)) \wedge (\forall y)\neg r(y))$, $(\forall x)(\exists y)s(x, y)$, $(\forall x)x \approx x$, $(\exists x)q$ jsou formule jazyka tohoto typu. Na druhou stranu například x, $x \approx r(x)$, $\neg f(c)$, $(\forall x)r(x, y)$, $(\exists x)x$ nejsou formule jazyka tohoto typu.

Vlastnosti a vztahy jsou ve slovním popisu obvykle popisovány *přídavnými jmény* a *slovesnými vazbami. Relační symboly* mají při formalizaci úlohu *jmen,* která označují *jména vlastností a vztahů.* Množinu relačních symbolů můžeme stanovit ze slovního popisu jako množinu všech vlastností a vztahů, které se v daném popisu vyskytují.

Vlastnosti a vztahy jsou ve slovním popisu zastoupena přídavnými jmény a slovesnými vazbami.

Průvodce studiem

Nyní se ujistěte, že chápete, jaký je rozdíl mezi *termy* a *formulemi.* Rozdíl je jedním slovem značný. Termy slouží k označování individuí, kdežto formule reprezentují formalizované výpovědi o vztazích a vlastnostech individuí označovaných termy. Oba pojmy nelze v žádném případě míchat nebo volně zaměňovat.

Příklad 6.24. Navrhněte jazyk a následující tvrzení formalizujte formulemi.

(1) „Ptáci, kteří nelétají, umějí rychle běhat.“
(2) „Čím více má člověk peněz, tím je šťastnější.“

Ad (1): V textu se vyskytují vlastnosti „létat“ a „být ptákem“. Sousloví „rychle běhat“ můžeme chápat jako atomickou vlastnosti, nebo jako vyjádření, že „rychlost běhu je velká“. V druhém případě ovšem musíme specifikovat funkční závislost mezi individuem a jeho rychlostí. Rozebereme postupně oba dva přístupy.

Mějme jazyk typu $\langle R, \emptyset, \sigma\rangle$, kde $R = \{\mathit{pták}, \mathit{létat}, \mathit{rychle\_běhat}\}$, přitom $\sigma(r) = 1$ pro každý $r \in R$. Nyní můžeme požadovaný fakt vyjádřit formulí

$$(\mathit{pták}(x) \wedge \neg \mathit{létat}(x)) \Rightarrow \mathit{rychle\_běhat}(x).$$

Předchozí formule není jediná možná formalizace tvrzení (1). Z výrokové logiky víme, že výrokové formule $(p \Rightarrow (q \Rightarrow r))$ a $((p \wedge q) \Rightarrow r)$ jsou logicky ekvivalentní. Budeme-li se dívat na atomické formule PL jako na výroky, pak můžeme předchozí fakt vyjádřit ekvivalentně formulí

$$\mathit{pták}(x) \Rightarrow (\neg \mathit{létat}(x) \Rightarrow \mathit{rychle\_běhat}(x)).$$

Uvažujme nyní jazyk typu $\langle R, F, \sigma\rangle$, kde $F = \{\mathit{rychlost}\}$, $R = \{\mathit{pták}, \mathit{létat}, \mathit{rychlý}\}$ a dále nechť $\sigma(\mathit{rychlost}) = 1$ a $\sigma(r) = 1$ pro každý $r \in R$. Pak můžeme požadovaný fakt vyjádřit například formulí v tomto tvaru,

$$\mathit{pták}(x) \Rightarrow (\neg \mathit{létat}(x) \Rightarrow \mathit{rychlý}(\mathit{rychlost}(x))).$$

přitom term $\mathit{rychlost}(x)$ čteme jako „rychlost individua x“. Příklad bychom mohli dále precizovat, například pojem „být rychlý“ může být chápán kontextově. V tomto případě by stačilo uvažovat relační symbol *rychlý* jako označení pro binární vztah „individuum x je při své rychlosti y rychlý“.

Ad (2): V tomto případě lze postupovat analogicky jako v předchozím. Nejprve ukážeme formalizaci nepoužívající žádné funkční symboly. Mějme jazyk typu $\langle R, \emptyset, \sigma\rangle$, přitom máme $R = \{\mathit{člověk}, \mathit{mít\_víc\_peněz}, \mathit{být\_šťastnější}\}$ a $\sigma(\mathit{člověk}) = 1$, ostatní dva relační symboly jsou binární. Tvrzení formalizujeme následující formulí.

$$(\mathit{člověk}(x) \wedge \mathit{člověk}(y) \wedge \mathit{mít\_víc\_peněz}(x, y)) \Rightarrow \mathit{být\_šťastnější}(x, y).$$

Při formalizaci můžeme uvažovat i tak, že pro dané individuum budeme vyjadřovat počet peněz, jakožto funkční závislost a oba počtu budeme klasifikovat pomocí speciálního relačního symbolu. Podrobněji, mějme jazyk typu $\langle R, F, \sigma\rangle$, kde $F = \{\mathit{peníze}\}$ a $R = \{\mathit{menší}, \mathit{člověk}, \mathit{být\_šťastnější}\}$, přitom $\sigma(\mathit{peníze}) = 1$ a $\sigma(\mathit{menší}) = 2$, arity ostatních symbolů jsou stejné jako u předchozího jazyka. Nyní můžeme vyjádřit

$$(\mathit{člověk}(x) \wedge \mathit{člověk}(y) \wedge \mathit{menší}(\mathit{peníze}(y), \mathit{peníze}(x))) \Rightarrow \mathit{být\_šťastnější}(x, y).$$

U relačních symbolů s aritou vyšší jak 1 musíme dodržovat smluvené pořadí argumentů, evidentní je to například u vztahů typu „x je otcem y“ a podobně.

Nyní se pozastavíme u role *kvantifikátorů* $\forall$ a $\exists$. Podle definice formule PL, kvantifikátory se ve formulích vyskytují vždy ve tvaru $(\forall x)\varphi$, případně $(\exists x)\varphi$, kde x je proměnná a φ je formule. Zamýšlený význam $(\forall x)\varphi$ je „pro každé x platí φ“, zamýšlený význam $(\exists x)\varphi$ „pro nějaké x platí φ“ nebo jinak: „existuje x, pro které platí φ“.

Průvodce studiem

Při zápisu kvantifikovaných formulí je třeba dávat pozor na správné uzávorkování, například formule $(\forall x)\varphi \Rightarrow \psi$ má význam „pokud pro každé x platí φ, pak platí ψ“, kdežto formule $(\forall x)(\varphi \Rightarrow \psi)$ má význam „pro každé x platí: pokud φ, pak ψ“. Pořadí kvantifikátorů také není možné libovolně zaměňovat. Pokud bude například atomická formule $r(x, y)$ označovat tvrzení „člověk y je otcem člověka x“, pak bychom formuli $(\forall x)(\exists y)r(x, y)$ mohli číst „každý člověk má svého otce“ neboli „pro každého člověka existuje (jeho) otec“. Naproti tomu formuli $(\exists y)(\forall x)r(x, y)$ bychom nejspíš četli „existuje člověk, který je otcem každého člověka“, což jsou z pohledu intuice dvě naprosto různá tvrzení.

Vyskytují-li se ve slovním popisu vazby jako „všichni (ne)jsou . . .“, „někteří (ne)jsou, . . .“ a podobně, při vytváření formulí bychom měli vhodně použít kvantifikátory. Nyní si ukážeme vyjádření některých typických slovních spojení. Uvažujme nyní dvě atomické formule $r(x)$, $s(x)$, které vyjadřují dvě vlastnosti R a S. U některých obratů je v následujícím přehledu uvedeno několik ekvivalentních přepisů.

Každé R je S.	$(\forall x)(r(x) \Rightarrow s(x))$
Žádné R není S.	$(\forall x)(r(x) \Rightarrow \neg s(x))$, $(\forall x)\neg(r(x) \wedge s(x))$, $\neg(\exists x)(r(x) \wedge s(x))$
Některá R jsou S.	$(\exists x)(r(x) \wedge s(x))$, $\neg(\forall x)(r(x) \Rightarrow \neg s(x))$
Některá R nejsou S.	$(\exists x)(r(x) \wedge \neg s(x))$, $(\exists x)\neg(r(x) \Rightarrow s(x))$, $\neg(\forall x)(r(x) \Rightarrow s(x))$

Za pozornost stojí přepis obratu „některá R jsou S“. Intuitivně by se mohlo zdát, že bychom ve formuli měli použít implikaci místo konjunkce. Při bližším pohledu je ale jasné, že formule ϑ tvaru $(\exists x)(r(x) \Rightarrow s(x))$ by *neměla požadovaný význam.* Tato formule totiž vzhledem k zamýšlenému významu implikace nevylučuje situaci, při které „žádné R není S“.

Příklad 6.25. Navrhněte jazyk a následující tvrzení formalizujte formulemi.

(1) „Všichni studenti, kromě Petra, jsou pilní.“
(2) „Každý muž má otce, pokud je navíc sám otcem, jeho otec je dědečkem.“
(3) „Každé racionální číslo lze vyjádřit zlomkem.“
(4) „Existuje přirozené číslo, které je větší než všechna ostatní přirozená čísla.“
(5) „Číslo je sudé, právě když je rovno nule nebo následuje za lichým číslem.“

Ad (1): Nejprve navrhneme jazyk. V popisu se vyskytují dvě vlastnosti, „být student“ a „být pilný“. Neměnným individuem je „Petr“. To jest uvažujme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $F = \{\mathit{petr}\}$, $R = \{\approx, \mathit{pilný}, \mathit{student}\}$, přitom $\sigma(\mathit{petr}) = 0$. Pro relační symboly máme $\sigma(\mathit{pilný}) = \sigma(\mathit{student}) = 1$. Tvrzení můžeme formalizovat následovně,

$$(\forall x)((\mathit{student}(x) \wedge \neg\, x \approx \mathit{petr}) \Rightarrow \mathit{pilný}(x)).$$

Mohli bychom rovněž uvažovat $F = \emptyset$, jazyk bez rovnosti a vlastnost „být Petrem“, to jest $R = \{\mathit{pilný}, \mathit{student}, \mathit{je\_petr}\}$, kde $\sigma(\mathit{je\_petr}) = 1$. Potom bychom mohli tvrzení vyjádřit

$$(\forall x)((\mathit{student}(x) \wedge \neg\, \mathit{je\_petr}(x)) \Rightarrow \mathit{pilný}(x)).$$

Rozdíl proti předchozí formalizaci je v tom, že v druhém případě v naší úvaze připouštíme obecně víc individuí, která budou mít vlastnost *je_petr*. U předchozí formalizace se jednalo vždy právě o jedno individuum, které bylo označeno konstantou. Na konec podotkněme, že předchozí tvrzení bychom mohli vyjádřit ekvivalentně i bez použití univerzálního kvantifikátoru.

Ad (2): V tomto případě budeme používat jazyk bez rovnosti. V popisu se vyskytují dvě vlastnosti „být mužem“ a „být dědečkem“. Vztah „být otcem“ je přitom *binární,* to jest jedná se o vztah „x je otcem y“. Uvažujme tedy jazyk typu $\langle R, \emptyset, \sigma\rangle$, kde $R = \{\mathit{muž}, \mathit{dědeček}, \mathit{otec}\}$

a $\sigma(\mathit{muž}) = \sigma(\mathit{dědeček}) = 1$, $\sigma(\mathit{otec}) = 2$. Rozeberme tvrzení po částech, fakt „každý muž má otce“ lze zapsat

$$(\forall x)(\mathit{muž}(x) \Rightarrow (\exists y)\mathit{otec}(y, x)),$$

formuli bychom mohli zkrátit i na $(\forall x)(\exists y)\mathit{otec}(y, x)$. Pokud bychom ovšem navrhovali jazyk pro vyšetřování vztahů různých individuí, mezi nimiž by byli muži (dále třeba ženy, auta, dýmky, ...), pak bychom měli formuli zachovat v původním tvaru. Celé tvrzení může být vyjádřeno následovně:

$$(\forall x)(\mathit{muž}(x) \Rightarrow (\exists y)(\mathit{otec}(y, x) \wedge ((\exists z)\mathit{otec}(x, z) \Rightarrow \mathit{dědeček}(y)))).$$

Formuli lze opět ekvivalentně vyjádřit i bez kvantifikace proměnné x. Na příkladu si ještě uvědomte, že předchozí formuli nelze nahradit formulí

$$(\forall x)(\mathit{muž}(x) \Rightarrow (\exists y)(\mathit{otec}(y, x) \wedge ((\exists z)\mathit{otec}(x, z) \Leftrightarrow \mathit{dědeček}(y))))$$

bez ztráty zamýšleného významu (zdůvodněte proč).

Ad (3): K tomu, abychom formalizovali toto tvrzení nemusíme nutně „formalizovat aritmetiku“, dokonce ani nemusíme popisovat formulemi vlastnosti čísel. Stačí když budeme uvažovat vlastnosti „být racionální číslo“m „být celé číslo“ a zavedeme označení pro individuum, které vznikne z celočíselného čitatele a jmenovatele – z tohoto pohledu jde o funkční závislosti individuí, nikoliv o vlastnost. Podrobněji, uvažujme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde F obsahuje jediný binární funkční symbol *zlomek* a R obsahuje kromě symbolu rovnosti $\approx$ dva unární relační symboly *racionální* a *celé*. Nyní můžeme uvažovat formuli

$$\mathit{racionální}(x) \Leftrightarrow (\exists y)(\exists z)((\mathit{celé}(y) \wedge \mathit{celé}(z)) \wedge x \approx \mathit{zlomek}(y, z)),$$

která vystihuje fakt „x je racionální, právě když jej lze vyjádřit podílem dvou celých čísel y a z“.

Ad (4): Formalizace tohoto příkladu je velmi jednoduchá. Nenechte se prosím zmást tím, že tvrzení je „proti intuici“. My nezkoumáme jeho obsah či snad pravdivost, pouze jej formalizujeme formulí. Struktury, ve kterých bude tato formule pravdivá, nemusejí svými vlastnostmi korespondovat s našimi představami o vlastnostech přirozených číslech. Můžeme uvažovat jazyk s rovností typu $\langle R, \emptyset, \sigma\rangle$, kde $R = \{\approx, \mathit{číslo}, \mathit{menší}\}$, kde $\sigma(\mathit{číslo}) = 1$, $\sigma(\mathit{menší}) = 2$. Nyní máme formuli,

$$(\exists x)(\mathit{číslo}(x) \wedge (\forall y)((\mathit{číslo}(y) \wedge \neg\, y \approx x) \Rightarrow \mathit{menší}(y, x))).$$

V předchozí formuli nelze vynechat univerzální kvantifikaci $(\forall y)$, pokuste se zdůvodnit proč.

Ad (5): Při formalizaci *aritmetiky* se často zavádí konstanta 0 a unární funkční symbol s, který má význam „následovníka“. Pracujeme tedy s jazykem, kde $\{0, s\} \subseteq F$, $\sigma(0) = 0$ a $\sigma(s) = 1$. Term 0 můžeme chápat jako označení pro nulu, term $s(0)$ pro jedničku (následník nuly), $s(s(0))$ pro dvojku a tak podobně. Reprezentace přirozených čísel (včetně nuly) pomocí složených termů se využívá například v logických programovacích jazycích. Pro naše účely formalizace tvrzení z bodu (5) zvolíme jazyk $\langle R, F, \sigma\rangle$ s rovností tak, že $F = \{0, s\}$, $R = \{\approx, \mathit{sudé}, \mathit{liché}\}$, kde $\sigma(0) = 0$, $\sigma(s) = 1$ a $\sigma(\mathit{sudé}) = \sigma(\mathit{liché}) = 1$. Nyní můžeme tvrzení formalizovat

$$\mathit{sudé}(x) \Leftrightarrow (x \approx 0 \vee (\exists y)(x \approx s(y) \wedge \mathit{liché}(y))).$$

Za pozornost stojí vyjádření obratu „je následovníkem lichého čísla“. V předchozí ukázce jsme jej vyjádřili podformulí $(\exists y)(x \approx s(y) \wedge \mathit{liché}(y))$. Jinými slovy, x je následovníkem lichého čísla, právě když existuje liché y takové, že x je rovno $s(y)$.

Shrnutí

Predikátová logika formalizuje usuzování o vztazích individuí, na rozdíl od výrokové logiky lze v predikátové logice formalizovat i strukturu výroků. Základním pojmem syntaxe predikátové logiky je jazyk PL a jeho typ, kterým je jazyk jednoznačně určen. Uvažovaný typ jazyka je vždy vztažen k popisované problémové doméně. Formule predikátové logiky se skládají z proměnných, dále z funkčních a relačních symbolů, ze symbolů pro kvantifikátory a ze symbolů pro logické spojky a z pomocných symbolů. Termy formalizují funkční vztahy mezi individui, formule formalizují výpovědi o vztazích mezi individui.

Pojmy k zapamatování

- typ jazyka,
- relační symbol, funkční symbol, arita,
- konstanta, proměnná,
- všeobecný kvantifikátor, existenční kvantifikátor,
- rovnost, jazyk s rovností,
- term, formule

Kontrolní otázky

1. *Čím se liší výroková logika od predikátové logiky?*
2. *Čím se odlišuje jazyk PL od jazyka VL?*
3. *Co je to arita symbolů?*
4. *Jak lze chápat nulární funkční a relační symboly?*
5. *Jaký je rozdíl mezi termem a formulí?*

Cvičení

1. Uvažujme jazyk predikátové logiky typu $\langle R, F, \sigma\rangle$, kde $F = \{f, g, h\}$, $R = \{r, s\}$ a $\sigma(f) = \sigma(h) = \sigma(r) = 1$, $\sigma(s) = 2$, $\sigma(g) = 3$. Rozhodněte, které z následujících výrazů (ne)jsou formule tohoto jazyka a zdůvodněte proč.

$f(x)$,	$r(f(x))$,	$(\forall x)r(x) \Rightarrow s(x, h(x))$,	$(\forall x)(r(x) \Rightarrow \neg r(x))$,
$(\forall x)\neg h(x)$,	$s(g(x, x, h(x)))$,	$s(h(x), h(f(x)))$,	$s(x, x) \Rightarrow (\forall y)s(x, x)$,
$(\forall x)(\forall y)\neg r(g(x, y, z))$,	$r(\neg r(x))$,	$r(y) \Rightarrow (\forall s)s(x, y)$,	$\neg(\forall x)(k(x) \Rightarrow r(x))$.

2. Navrhněte jazyk a formalizujte slovně popsaná tvrzení formulemi.

   (1) „Nejlepší programovací jazyk je Scheme.“,
   (2) „Čím jsou programy větší, tím více obsahují chyb.“,
   (3) „Existuje právě jedno sudé prvočíslo.“.

Úkoly k textu

1. Uvažujme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde

$$F = \{\mathit{matka}, \mathit{otec}\}, \qquad R = \{\approx, \mathit{člověk}, \mathit{muž}, \mathit{manžel}\},$$

   $\sigma(\mathit{matka}) = 1$, $\sigma(\mathit{otec}) = 1$, $\sigma(\mathit{člověk}) = 1$, $\sigma(\mathit{muž}) = 1$ a $\sigma(\mathit{manžel}) = 2$. Funkční symboly budeme interpretovat jako „matka/otec daného individua“, relační symboly *člověk* a *muž* označují vlastnosti individuí a konečně *manžel* je binární vztah „x je manželem y“. Slovně popište zamýšlený význam následujících formulí.

$(\forall x)(\mathit{muž}(x) \Rightarrow \mathit{člověk}(x))$,	$\mathit{člověk}(x) \wedge \neg \mathit{muž}(x)$,
$\mathit{člověk}(x) \Rightarrow \mathit{muž}(\mathit{otec}(x))$,	$\mathit{manžel}(x, y) \Rightarrow \neg \mathit{manžel}(y, x)$,
$\mathit{manžel}(x, y) \wedge (\exists z)\mathit{otec}(z) \approx x$,	$x \approx \mathit{matka}(y) \Rightarrow \mathit{muž}(y)$.

2. Uvažujte jazyk stejného typu jako v předchozím úkolu a pomocí formulí vyjádřete následující „vlastnosti lidí“ a „rodinné vztahy“.

„x je sirotkem“,	„x nemá žádné sourozence“,
„x a y jsou sourozenci“,	„x je nevlastním sourozencem y“,
„x je švagrem y“.	„x je strýc nebo teta y“,

Řešení

1. $f(x)$ není formule (je to term); $r(f(x))$ je atomická formule; $(\forall x)r(x) \Rightarrow s(x, h(x))$ je formule; $(\forall x)(r(x) \Rightarrow \neg r(x))$ je formule; $(\forall x)\neg h(x)$ není formule; $s(g(x, x, h(x)))$ není formule; $s(h(x), h(f(x)))$ je atomická formule; $s(x, x) \Rightarrow (\forall y)s(x, x)$ je formule; $(\forall x)(\forall y)\neg r(g(x, y, z))$ je formule; $r(\neg r(x))$ není formule; $r(y) \Rightarrow (\forall s)s(x, y)$ není formule (nelze kvantifikovat „přes relační symbol“); $\neg(\forall x)(k(x) \Rightarrow r(x))$ není formule (k není relační symbol).
2. Ad (1): $R = \{\mathit{progj}, \mathit{lepší\_progj}\}$, $F = \{\mathit{Scheme}\}$,
   $\sigma(\mathit{progj}) = 1$, $\sigma(\mathit{lepší\_progj}) = 2$, $\sigma(\mathit{Scheme}) = 0$; formule:

   $$(\forall x)(\mathit{progj}(x) \Rightarrow \mathit{lepší\_progj}(\mathit{Scheme}, x)).$$

   Ad (2): $R = \{\mathit{prog}, \mathit{větší}\}$, $F = \{\mathit{velikost}, \mathit{p\_chyb}\}$,
   $\sigma(\mathit{prog}) = \sigma(\mathit{velikost}) = \sigma(\mathit{p\_chub}) = 1$, $\sigma(\mathit{větší}) = 2$; formule:

   $$(\mathit{prog}(x) \wedge \mathit{prog}(y)) \Rightarrow (\mathit{větší}(\mathit{velikost}(x), \mathit{velikost}(y)) \Rightarrow \mathit{větší}(\mathit{p\_chyb}(x), \mathit{p\_chyb}(y))).$$

   Ad (3): Jazyk s rovností, kde $R = \{\approx, \mathit{sudé}, \mathit{prvočíslo}\}$, $F = \emptyset$,
   $\sigma(\mathit{sudé}) = \sigma(\mathit{prvočíslo}) = 1$; formule:

   $$(\exists x)((\mathit{sudé}(x) \wedge \mathit{prvočíslo}(x)) \wedge (\forall y)((\mathit{sudé}(y) \wedge \mathit{prvočíslo}(y)) \Rightarrow x \approx y)).$$

Studijní cíle: Po nastudování této části by student měl mít znalosti základních sémantických pojmů predikátové logiky. Student by měl chápat interpretaci jazyka predikátové logiky a s tím související pojmy. Dále by měl znát základní pravidla pro práci s kvantifikátory a mít přehled o mezích predikátové logiky a dalších logických kalkulech.

Klíčová slova: individuum, funkce, hodnota termu, epistemická logika, fuzzy logika, interpretace jazyka, logiku času, model teorie, modální logika, nerozhodnutelnost, objekt, ohodnocení proměnných, pravdivostní hodnota formule, relace, rovnost, sémantické vyplývání, sémantika, struktura, tautologie, tautologie ve struktuře, temporální logika, teorie, univerzum, zobrazení

Potřebný čas: 150 minut.

6.3.2 Sémantika predikátové logiky

Jazyk predikátové logiky je určen svými relačními a funkčními symboly spolu s definicí jejich arity. Z těchto symbolů spolu se symboly proměnných, logických spojek a kvantifikátorů se skládají termy a formule daného jazyka. Je zcela v souladu s očekáváním, že samotné termy a formule jsou syntaktické pojmy a nemají žádný význam, to jest term sám o sobě nemá žádnou hodnotu, formule sama o sobě nemá žádnou pravdivostní hodnotu. To je dobře patrné například u termu $x + 0$: intuitivně je jasné, že k tomu, abychom mohli uvažovat hodnotu tohoto termu, musí mít přiřazenu nějakou hodnotu proměnná x a dále musíme interpretovat symboly $+$ a 0, což už možná na první pohled tak „průhledné“ není. Kdybychom uvažovali term $0 + 0$, některé

Termy a formule jsou syntaktické pojmy predikátové logiky.

čtenáře by to mohlo intuitivně svádět k jeho automatické interpretaci přirozeně používané v matematice. Z pohledu logiky však nelze říct, že hodnota termu $0 + 0$ je 0! Term $0 + 0$ je jen posloupností tří symbolů, nic víc, přitom 0 je symbol konstanty, $+$ je binární funkční symbol, který jsme zapsali v infixové notaci.

Sémantika predikátové logiky interpretuje jazyk PL.

Interpretací funkčních a relačních symbolů se zabývá *sémantika predikátové logiky,* kterou se budeme zabývat nyní. Volně řečeno, sémantika PL přiřazuje význam funkčním a relačním symbolům, přitom účelem je, aby všechny symboly mohly mít libovolnou smysluplnou interpretaci. Co tím máme na mysli? Nejprve zvolíme vhodné *univerzum* M*,* to jest, *neprázdnou množinu elementů,* které jsou pro naše úvahy relevantní. V tomto univerzu přiřadíme významy relačním a funkčním symbolům daného jazyka – pro každý relační symbol jazyka určíme konkrétní *relaci v* M*,* kterou tento relační symbol bude označovat, a pro každý funkční symbol jazyka určíme konkrétní *funkci v* M (to jest *zobrazení v* M) kterou tento funkční symbol bude označovat. Všimněte si, že intuitivní interpretace pojmů *relace* a *zobrazení* uvedená v kapitole 2.1 souhlasí s významem, který jsme přisoudili relačním a funkčním symbolům v kapitole 6.3.1. Volbou univerza, relací a funkcí provedeme *interpretaci jazyka* – je tedy vcelku jasné, že jeden jazyk predikátové logiky má mnoho možných interpretací.

Význam termů a formulí můžeme uvažovat až poté, co máme dánu interpretaci všech symbolů jazyka PL.

Zvolíme-li interpretaci jazyka, zbývá v termech a formulích ještě jeden typ symbolů, které dosud nejsou interpretovány – *proměnné.* Interpretaci proměnných definuje tak zvané *ohodnocení proměnných,* které každé proměnné jazyka přiřadí nějaký element uvažovaného univerza. Zde prosím neplést pojmy *pravdivostní ohodnocení,* což je pojem ze sémantiky výrokové logiky a *ohodnocení proměnných,* což je pojem ze sémantiky predikátové logiky! Tyto pojmy nelze zaměňovat. Je opět jasné, že při dané interpretaci jazyka existuje celá řada možných ohodnocení proměnných. Zvolíme-li interpretaci jazyka a ohodnocení proměnných, teprve pak se můžeme ptát po hodnotách termů a pravdivosti formulí.

Průvodce studiem

Vztah syntaxe a sémantiky predikátové logiky je analogický vztahu syntaxe a sémantiky programovacích jazyků. Syntaxe popisuje pouze tvar, v PL je to přípustný tvar termů a formulí, v programovacím jazyku je to přípustný tvar programu v daném jazyku. Sémantika dává význam syntaktickým objektům: sémantika PL dává význam termům a formulím, sémantika programovacích jazyků dává význam jednotlivým konstruktům jazyka. Sémantika je ale principiálně nezávislá na syntaxi, což je dobře vidět právě u programovacích jazyků. Například výraz „`a=b+1;`“ má ve standardu programovacího jazyka C význam *přiřazovacího příkazu* („do paměťového místa a přiřaď hodnotu vzniklou vyhodnocením $b + 1$“), kdežto ve standardu jazyka Metapost má význam *deklarace lineární rovnice* („hodnota a je rovna hodnotě $b + 1$“).

Vraťme se k našemu příkladu, to jest k termům $0 + 0$ a $0 + x$. Jsou to termy v jistém jazyku, kterému jsme se zatím nevěnovali. Jazykem, ve kterém lze vyjádřit tyto termy, může být například jazyk typu $\langle R, F, \sigma\rangle$, kde $R = \{\leq\}$, $F = \{0, +\}$ a $\leq$ je binární, 0 je nulární a $+$ je binární. Zvolme jednu interpretaci tohoto jazyka: univerzem M nechť je množina $\mathbb{Z}$ všech celých čísel, binární relací v $\mathbb{Z}$, kterou označuje binární relační symbol $\leq$ nechť je obvyklá relace „menší nebo rovno“ (označme ji $\leq^{\mathbf{M}}$), konstantou v $\mathbb{Z}$, kterou označuje nulární funkční symbol 0 nechť je číslo nula (označme jej $0^{\mathbf{M}}$), binární funkcí v $\mathbb{Z}$, kterou označuje binární funkční symbol $+$ nechť je obvyklé sčítání (označme ho $+^{\mathbf{M}}$). Zvolme dále interpretaci proměnných: nechť proměnným x a y jsou po řadě přiřazeny hodnoty 5 a -100, dalším proměnným přiřadíme libovolné hodnoty.

Při takové interpretaci je hodnotou termu $0 + 0$ číslo nula ($0^{\mathbf{M}} +^{\mathbf{M}} 0^{\mathbf{M}}$), hodnotou termu $x + 0$ je číslo pět ($5 +^{\mathbf{M}} 0^{\mathbf{M}}$). Formule $0 \leq x$ je při dané interpretaci pravdivá, neboť číslo, které je označeno symbolem 0, to jest číslo nula, je v relaci „menší nebo rovno“ s číslem označeným symbolem x (symbolicky $0^{\mathbf{M}} \leq^{\mathbf{M}} 5$). Z podobného důvodu (zatím ovšem zdůvodňujeme

pouze intuitivně) je pravdivá formule $0 \leq x \Rightarrow y \leq y + x$, ta je dokonce pravdivá při jakékoli interpretaci proměnných. Změníme-li interpretaci proměnných tak, že proměnné x bude přiřazeno číslo -10, bude formule $0 \leq x$ nepravdivá.

Každý jazyk PL má nekonečně mnoho interpretací.

Výše uvedená interpretace jazyka však není jediná možná. Jinou interpretaci dostaneme, změníme-li naši původní interpretaci tak, že symbol 0 bude označovat číslo 1. Při této interpretaci bude hodnotou termu $0 + 0$ číslo 2. Zcela jinou interpretaci dostaneme, zvolíme-li za univerzum množinu všech čtvercových reálných matic, a označují-li symboly $\leq, 0, +$ po řadě relaci rovnosti matic, matici skládající se ze samých nul, a operaci násobení matic. Intuitivní pojem interpretace jazyka nyní přesně zavedeme.

Definice 6.26 (struktura). *Struktura* pro jazyk typu $\langle R, F, \sigma\rangle$ je trojice $\mathbf{M} = \langle M, R^{\mathbf{M}}, F^{\mathbf{M}}\rangle$, která sestává z neprázdné množiny M, a dále z množin

$$R^{\mathbf{M}} = \left\{r^{\mathbf{M}} \subseteq M^n \mid r \in R,\, \sigma(r) = n\right\},$$
$$F^{\mathbf{M}} = \left\{f^{\mathbf{M}} \colon M^n \to M \mid f \in F,\, \sigma(f) = n\right\}.$$

Pokud $\approx \in R$, pak $\approx$ interpretujeme vždy relací identity, to jest $\approx^{\mathbf{M}} = \omega_M = \{\langle u, u\rangle \mid u \in M\}$.

Poznámka 6.27. Jinými slovy, struktura $\mathbf{M}$ pro jazyk typu $\langle R, F, \sigma\rangle$ je systém relací a funkcí na jisté množině M, přitom ke každému n-árnímu relačnímu symbolu $r \in R$ je ve struktuře $\mathbf{M}$ odpovídající n-ární relace $r^{\mathbf{M}} \in R^{\mathbf{M}}$ na M a ke každému n-árnímu funkčnímu symbolu $f \in F$ je ve struktuře $\mathbf{M}$ odpovídající n-ární funkce $f^{\mathbf{M}} \in F^{\mathbf{M}}$ v M. Nehrozí-li nebezpečí nedorozumění, budeme někdy vynechávat horní indexy a místo $r^{\mathbf{M}}$ a $f^{\mathbf{M}}$ píšeme jen r a f.

Příklad 6.28. (1) Uvažujme jazyk typu $\langle R, F, \sigma\rangle$, kde $R = \{p, d, b, s\}$, $F = \emptyset$, relační symboly p, d, b jsou unární, s binární. Nechť M je množina všech lidí z nějakého regionu. Definujme relace $p^{\mathbf{M}}$, $d^{\mathbf{M}}$, $b^{\mathbf{M}}$, $s^{\mathbf{M}}$ následovně: $p^{\mathbf{M}}$, $d^{\mathbf{M}}$, $b^{\mathbf{M}}$ jsou unární relace, to jest podmnožiny M, definované

$$p^{\mathbf{M}} = \{m \in M \mid m \text{ má čistý příjem vyšší než 17 tis. Kč/měs.}\},$$
$$d^{\mathbf{M}} = \{m \in M \mid m \text{ splácí pravidelně méně než 5 tis. Kč/měs.}\},$$
$$b^{\mathbf{M}} = \{m \in M \mid m \text{ na živobytí zbývá více než 8 tis. Kč/měs.}\}$$

a $s^{\mathbf{M}}$ je binární relace

$$s^{\mathbf{M}} = \{\langle m_1, m_2\rangle \in M \times M \mid m_1 \text{ a } m_2 \text{ jsou manželé.}\}$$

Pak $\mathbf{M} = \langle M, R^{\mathbf{M}}, \emptyset\rangle$, kde $R^{\mathbf{M}} = \{p^{\mathbf{M}}, d^{\mathbf{M}}, b^{\mathbf{M}}, s^{\mathbf{M}}\}$ je struktura pro výše uvedený jazyk.

(2) Jinou strukturu pro jazyk z bodu (1) dostaneme, pozměníme-li strukturu uvedenou v (1) tak, že

$$p^{\mathbf{M}} = \{m \in M \mid m \text{ má čistý příjem vyšší než 40 tis. Kč/měs.}\},$$
$$d^{\mathbf{M}} = \{m \in M \mid m \text{ splácí pravidelně méně než 2 tis. Kč/měs.}\},$$
$$b^{\mathbf{M}} = \{m \in M \mid m \text{ na živobytí zbývá více než 35 tis. Kč/měs.}\}$$

a $s^{\mathbf{M}}$ je binární relace $s^{\mathbf{M}} = \{\langle m_1, m_2\rangle \in M \times M \mid m_1 \text{ a } m_2 \text{ nejsou manželé.}\}$.

(3) Další strukturu pro stejný jazyk dostaneme, zvolíme-li například:
$M = \{a, b, 1, 2\}$, $p^{\mathbf{M}} = \{a, b\}$, $d^{\mathbf{M}} = \{1, 2\}$, $b^{\mathbf{M}} = \emptyset$, $s^{\mathbf{M}} = \{\langle a, b\rangle, \langle 1, 2\rangle\}$.

(4) Uvažujme jazyk typu $\langle R, F, \sigma\rangle$, kde $R = \{p, \leq\}$, $F = \{c, \circ\}$, c je nulární, p je unární, $\leq$ a $\circ$ jsou binární. Nechť $M = \mathbb{Z}$, to jest M je množina všech celých čísel. Definujme relace $p^{\mathbf{M}}$ (unární, to jest podmnožina M), $\leq^{\mathbf{M}}$ (binární) a funkce $c^{\mathbf{M}}$ (nulární, to jest vybraný prvek z M) a $\circ^{\mathbf{M}}$ (binární) následovně:

$$p^{\mathbf{M}} = \{m \in M \mid m \text{ je větší nebo rovno nule}\},$$
$$\leq^{\mathbf{M}} = \{\langle m_1, m_2\rangle \in M \times M \mid m_1 \text{ je menší nebo rovno } m_2\},$$
$$c^{\mathbf{M}} = 0,$$
$$m_1 \circ^{\mathbf{M}} m_2 = m_1 + m_2,$$

to jest $c^{\mathbf{M}}$ je číslo nula a $\circ^{\mathbf{M}}$ je operace sčítání celých čísel.

(5) Jinou strukturu pro jazyk z předchozího bodu dostaneme, pokud změníme výše uvedenou strukturu tak, že $c^{\mathbf{M}} = 1$, případně ještě definujeme $m_1 \circ^{\mathbf{M}} m_2 = m_1 \cdot m_2$ (násobení celých čísel).

(6) Mějme neprázdnou množinu znaků Σ, kterou nazveme abeceda. Řetězec nad abecedou je libovolná konečná posloupnost znaků z Σ. Například `00101`, `111`, `01010101` jsou řetězce nad abecedou $\Sigma = \{\mathtt{0}, \mathtt{1}\}$, například `eter`, `keprt`, `krep`, `krtek`, `petr`, `pretrpet`, `p`, `ret`, `tep`, `tttprt`, `etetet`,... jsou řetězce nad $\Sigma = \{\mathtt{e}, \mathtt{k}, \mathtt{p}, \mathtt{r}, \mathtt{t}\}$. Prázdnou posloupnost znaků z Σ označujeme ε a nazýváme ji *prázdný řetězec*. Pro řetězce ω_1 a ω_2 uvažujeme řetězec $\omega_1\omega_2$, který vznikne jejich *zřetězením* (to jest „slepením“) v tomto pořadí. Zřetězením libovolného řetězce s prázdným řetězce získáme opět výchozí řetězec, to jest $\omega\varepsilon = \varepsilon\omega = \omega$. Další strukturou pro jazyk z bodu (4) může být struktura s nosičem

$$M = \{\omega \mid \omega \text{ je řetězec znaků nad abecedou } \Sigma = \{\mathtt{0}, \mathtt{1}\}\},$$

kde

$$\begin{aligned} p^{\mathbf{M}} &= \{\omega \in M \mid \omega \text{ je řetězec, který má stejný počet znaků } \mathtt{0} \text{ a } \mathtt{1}\},\\ \leq^{\mathbf{M}} &= \{\langle \omega_1, \omega_2\rangle \in M \times M \mid \text{řetězec } \omega_1 \text{ je kratší než řetězec } \omega_2\},\\ c^{\mathbf{M}} &= \varepsilon,\\ \omega_1 \circ^{\mathbf{M}} \omega_2 &= \omega_1\omega_2, \end{aligned}$$

to jest $c^{\mathbf{M}}$ označuje prázdný řetězec a $\circ^{\mathbf{M}}$ je operace zřetězení řetězců.

(7) Další strukturou pro jazyk z bodu (4) je struktura s nosičem $M = \{a, b\}$, $p^{\mathbf{M}} = \{a, b\}$, $\leq^{\mathbf{M}} = \{\langle a, a\rangle, \langle b, b\rangle, \langle b, a\rangle\}$, $c^{\mathbf{M}} = b$ a operace $\circ^{\mathbf{M}}$ je dána následující tabulkou.

$\circ^{\mathbf{M}}$	a	b
a	a	b
b	a	a

Pro každý jazyk existuje nekonečně mnoho struktur.

Jak tedy vidíme, k danému jazyku predikátové logiky existuje nekonečně mnoho struktur. Variabilita je dána jednak nosičem M, který může mít libovolný počet prvků, dále každý relační symbol r může být interpretován libovolnou relací $r^{\mathbf{M}}$ příslušné arity a konečně každý funkční symbol f může být interpretován libovolnou funkcí $f^{\mathbf{M}}$ příslušné arity.

Ohodnocením proměnných interpretujeme proměnné.

Nechť $\mathbf{M}$ je struktura pro jazyk typu $\langle R, F, \sigma\rangle$. $\mathbf{M}$-*ohodnocení proměnných* je zobrazení v přiřazující každé proměnné x prvek $v(x) \in M$. Jsou-li v a v' ohodnocení a x je proměnná, píšeme $v =_x v'$ pokud pro každou proměnnou $y \neq x$ je $v(y) = v'(y)$, to jest v a v' se liší nejvýše v tom, jakou hodnotu přiřazují proměnné x. Pokud to nebude na újmu srozumitelnosti, $\mathbf{M}$-ohodnocení proměnných budeme stručně nazývat $\mathbf{M}$-*ohodnocení*, případně jen *ohodnocení*.

Definice 6.29. Nechť v je $\mathbf{M}$-ohodnocení. *Hodnota* $\|t\|_{\mathbf{M},v} \in M$ *termu* t *v* $\mathbf{M}$ *při* v je definována:

$$\|t\|_{\mathbf{M},v} = \begin{cases} v(x) & \text{pokud je } t \text{ proměnná } x,\\ f^{\mathbf{M}}\big(\|t_1\|_{\mathbf{M},v}, \ldots, \|t_k\|_{\mathbf{M},v}\big) & \text{pokud je } t \text{ ve tvaru } f(t_1, \ldots, t_k). \end{cases}$$

Poznámka 6.30. Uvědomme si, při dané struktuře $\mathbf{M}$ a při daném $\mathbf{M}$-ohodnocení v je podle definice 6.29 každému termu t přiřazena právě jedna hodnota $\|t\|_{\mathbf{M},v}$ z univerza M. Z definice 6.29 je dále patrné, že hodnota $\|t\|_{\mathbf{M},v}$ nezávisí na hodnotách přiřazených ohodnocením v těm proměnným, které se v t nevyskytují. Jinými slovy, pro každá $\mathbf{M}$-ohodnocení v_1, v_2 splňující $v_1(x) = v_2(x)$ pro každou proměnnou x vyskytující se v termu t, máme $\|t\|_{\mathbf{M},v_1} = \|t\|_{\mathbf{M},v_2}$.

Příklad 6.31. Vezmeme-li strukturu $\mathbf{M}$ z bodu (4) příkladu 6.28 a budeme-li uvažovat term $(x \circ (c \circ y)) \circ x$, pak při ohodnocení v, kde $v(x) = 10$, $v(y) = 50$ máme

$$\begin{aligned}\|(x \circ (c \circ y)) \circ x\|_{\mathbf{M},v} &= \|x \circ (c \circ y)\|_{\mathbf{M},v} + \|x\|_{\mathbf{M},v} = \\ &= (\|x\|_{\mathbf{M},v} + \|c \circ y\|_{\mathbf{M},v}) + \|x\|_{\mathbf{M},v} = \\ &= (\|x\|_{\mathbf{M},v} + (\|c\|_{\mathbf{M},v} + \|y\|_{\mathbf{M},v})) + \|x\|_{\mathbf{M},v} = \\ &= (v(x) + (c^{\mathbf{M}} + v(y))) + v(x) = \\ &= (10 + (0 + 50)) + 10 = 70.\end{aligned}$$

Všimněte si, že pokud vezmeme ohodnocení v', kde $v'(x) = v(y)$ a $v'(y) = v(x)$, pak $\|x \circ y\|_{\mathbf{M},v} = \|x \circ y\|_{\mathbf{M},v'}$. To ale obecně neplatí v každé struktuře pro tento jazyk. Vskutku, kdybychom vzali strukturu z bodu (6) téhož příkladu, což je jiná struktura pro tentýž jazyk, pak bychom při ohodnoceních $v(x) = \mathtt{0}$, $v(y) = \mathtt{1}$, a $v'(y) = \mathtt{0}$, $v'(x) = \mathtt{1}$ měli $\|x \circ y\|_{\mathbf{M},v} = \mathtt{01} \neq \mathtt{10} = \|x \circ y\|_{\mathbf{M},v}$. Vrátíme-li se k termu $(x \circ (c \circ y)) \circ x$, pak jeho hodnota v této struktuře při v bude $\|(x \circ (c \circ y)) \circ x\|_{\mathbf{M},v} = \mathtt{0}\varepsilon\mathtt{10} = \mathtt{010}$. Nechť $\mathbf{M}$ je struktura z bodu (7) příkladu 6.28 a uvažujme $\mathbf{M}$-ohodnocení v, kde $v(x) = b$ a $v(y) = b$. Pak $\|(x \circ (c \circ y)) \circ x\|_{\mathbf{M},v} = (b \circ^{\mathbf{M}} (b \circ^{\mathbf{M}} b)) \circ^{\mathbf{M}} b = (b \circ^{\mathbf{M}} a) \circ^{\mathbf{M}} b = a \circ^{\mathbf{M}} b = b$.

Nyní můžeme definovat pravdivostní hodnotu formule ve struktuře při daném ohodnocení.

Definice 6.32. *Pravdivostní hodnota* $\|\varphi\|_{\mathbf{M},v}$ *formule* φ *v* $\mathbf{M}$ *při* $\mathbf{M}$*-ohodnocení* v je definována

- pro atomické formule:

$$\|r(t_1, \ldots, t_n)\|_{\mathbf{M},v} = \begin{cases} 1 & \text{pokud } \langle \|t_1\|_{\mathbf{M},v}, \ldots, \|t_n\|_{\mathbf{M},v} \rangle \in r^{\mathbf{M}}, \\ 0 & \text{jinak.} \end{cases}$$

- pro formule φ a ψ je

$$\begin{aligned}\|\neg\varphi\|_{\mathbf{M},v} &= \neg \|\varphi\|_{\mathbf{M},v}, \\ \|\varphi \Rightarrow \psi\|_{\mathbf{M},v} &= \|\varphi\|_{\mathbf{M},v} \to \|\psi\|_{\mathbf{M},v}\end{aligned}$$

  a analogicky pro ostatní binární spojky $\wedge, \vee, \Leftrightarrow$.

- pro formuli φ a proměnnou x je

$$\|(\forall x)\varphi\|_{\mathbf{M},v} = \begin{cases} 1 & \text{pokud pro každé } v' \text{ takové, že } v' =_x v, \text{ platí } \|\varphi\|_{\mathbf{M},v'} = 1, \\ 0 & \text{jinak,} \end{cases}$$

$$\|(\exists x)\varphi\|_{\mathbf{M},v} = \begin{cases} 1 & \text{pokud existuje nějaké } v' \text{ takové, že } v' =_x v \text{ a platí } \|\varphi\|_{\mathbf{M},v'} = 1, \\ 0 & \text{jinak.} \end{cases}$$

Je-li $\|\varphi\|_{\mathbf{M},v} = 0$, říkáme, že formule φ je *nepravdivá ve struktuře* $\mathbf{M}$ *při ohodnocení* v. Je-li $\|\varphi\|_{\mathbf{M},v} = 1$, říkáme, že formule φ je *pravdivá ve struktuře* $\mathbf{M}$ *při ohodnocení* v.

Průvodce studiem

Uvědomte si, že říct „formule φ je pravdivá“ nemá smysl, protože pravdivost φ vztahujeme vždy k nějaké struktuře při některém ohodnocení proměnných. Běžně sice říkáme například „formule $(\forall x)(\forall y)\, x \leq x + \mathrm{abs}(y)$ je pravdivá“, ale to je způsobeno tím, že implicitně nějakou strukturu předpokládáme podle kontextu, ve kterém formuli uvažujeme. Například v matematické analýze jde většinou o číselné struktury, například reálná čísla s běžnými relacemi („menší nebo rovno“) a operacemi („sčítání reálných čísel“, „absolutní hodnota“).

Stejně jako u ohodnocení termů si uvědomme, že podle definice 6.32 je při daných $\mathbf{M}$ a v každé formuli přiřazena právě jedna hodnota $\|\varphi\|_{\mathbf{M},v}$. Rozebereme-li definici 6.32 po částech,

$\|r(t_1,\ldots,t_n)\|_{\mathbf{M},v} = 1$, právě když n-tice $\langle \|t_1\|_{\mathbf{M},v}, \ldots, \|t_n\|_{\mathbf{M},v}\rangle$ prvků $\|t_i\|_{\mathbf{M},v}$ z M patří do n-ární relace $r^{\mathbf{M}}$. Význam symbolů logických spojek se definuje pomocí *příslušných logických operací* stejně jako ve výrokové logice. Definice 6.32 dále říká, že $(\forall x)\varphi$ je ve struktuře $\mathbf{M}$ při v pravdivá, právě když je ve struktuře $\mathbf{M}$ pravdivá formule φ při každém ohodnocení v', které všem proměnným různým od x přiřazuje stejné prvky jaké jim přiřazuje v. To je právě zamýšlený význam všeobecného kvantifikátoru: „pro každé x platí φ“, to jest $(\forall x)\varphi$ je pravdivá při daném ohodnocení, pokud je φ pravdivá i v případě, kdy za x „dosadíme libovolný element z univerza“. Existenčně kvantifikovaná formule $(\exists x)\varphi$ je pravdivá ve struktuře $\mathbf{M}$ při v, právě když je ve struktuře $\mathbf{M}$ pravdivá formule φ aspoň při jednom ohodnocení v', které všem proměnným různým od x přiřazuje stejné prvky jaké jim přiřazuje v. To opět koresponduje se zamýšleným významem existenčního kvantifikátoru: $(\exists x)\varphi$ je pravdivá při daném ohodnocení, pokud je φ pravdivá v případě, kdy za x „dosadíme některý element z univerza“.

Kvantifikátory lze vyjádřit jeden z druhého s pomocí negace.

Existenční kvantifikace je na intuitivní úrovni nahraditelná všeobecnou kvantifikací a negací. Tvrzení „existuje x, pro které platí φ“ lze slovně vyjádřit „není pravda, že pro každé x neplatí φ“. Nyní si ukážeme, že tento vztah lze prokázat i na formální úrovni. Uvažujme formuli $\neg(\forall x)\neg\varphi$ a uvažujme její pravdivost při $\mathbf{M}$-ohodnocení v: $\|\neg(\forall x)\neg\varphi\|_{\mathbf{M},v} = 1$, právě když $\|(\forall x)\neg\varphi\|_{\mathbf{M},v} = 0$, dle definice 6.32 máme

$$\|(\forall x)\neg\varphi\|_{\mathbf{M},v} = \begin{cases} 1 & \text{pokud pro každé } v' \text{ takové, že } v' =_x v, \text{ platí } \|\neg\varphi\|_{\mathbf{M},v'} = 1, \\ 0 & \text{jinak,} \end{cases}$$

což lze rozepsat následovně

$$\|(\forall x)\neg\varphi\|_{\mathbf{M},v} = \begin{cases} 1 & \text{pokud pro každé } v' \text{ takové, že } v' =_x v, \text{ platí } \|\varphi\|_{\mathbf{M},v'} = 0, \\ 0 & \text{pokud existuje } v' \text{ takové, že } v' =_x v \text{ a platí } \|\varphi\|_{\mathbf{M},v'} = 1, \end{cases}$$

tedy $\|(\forall x)\neg\varphi\|_{\mathbf{M},v} = 0$, právě když existuje v' takové, že $v' =_x v$ a platí $\|\varphi\|_{\mathbf{M},v'} = 1$, což je právě když $\|(\exists x)\varphi\|_{\mathbf{M},v} = 1$. Existenčně kvantifikovanou formuli $(\exists x)\varphi$ tedy lze chápat jako zkratku za formuli $\neg(\forall x)\neg\varphi$. Analogicky lze ukázat, že formuli $(\forall x)\varphi$ bychom mohli chápat jako zkratku za $\neg(\exists x)\neg\varphi$. V predikátové logice proto bývá zvykem přijmout pouze všeobecný kvantifikátor $\forall$. Existenční kvantifikátor potom chápeme jako odvozený. Svým způsobem je tento počin analogický situaci, kdy jsme za základní logické spojky vzali pouze negaci a implikaci.

Nyní budeme zkoumat platnost formulí ve struktuře „přes všechna ohodnocení“ a konečně platnost formulí „přes všechny struktury“.

Tautologie je pravdivá v každé struktuře.

Definice 6.33. Formule φ se nazývá *pravdivá ve struktuře* (*tautologie ve struktuře*) $\mathbf{M}$, jestliže $\|\varphi\|_{\mathbf{M},v} = 1$ pro každé $\mathbf{M}$-ohodnocení v. Formule φ se nazývá *tautologie*, jestliže je φ tautologie v každé struktuře $\mathbf{M}$.

Ačkoliv jsme to v předchozí definici již explicitně nezdůrazňovali, je pořád nutné chápat pojmy formule a struktura vždy k jistému jazyku. Například u pojmu tautologie tedy vyžadujeme, aby formule φ jazyka typu $\langle R, F, \sigma\rangle$ byla pravdivá v každé struktuře pro jazyk typu $\langle R, F, \sigma\rangle$. Jistě by nemělo smysl vyžadovat „platnost ve struktuře jiného jazyka“, protože takový pojem jsme nezavedli – intuitivně je jasné, že pokud bychom uvažovali například formuli φ jazyka typu $\langle R, F, \sigma\rangle$, tak φ nemusí být obecně formulí chudšího jazyka, to jest jazyka vzniknuvšího z $\langle R, F, \sigma\rangle$ odebráním některých relačních a funkčních symbolů.

Příklad 6.34. (1) Mějme jazyk typu $\langle R, F, \sigma\rangle$, kde $F = \emptyset$, a R obsahuje jediný unární relační symbol r. Mějme strukturu $\mathbf{M}$ pro tento jazyk jejímž nosičem je dvouprvková množina $M = \{a, b\}$ a $r^{\mathbf{M}} = \{a\}$. Atomická formule $r(x)$ je pravdivá ve struktuře $\mathbf{M}$ při ohodnocení v, kde $v(x) = a$. Na druhou stranu, pokud $v(x) = b$, pak $\|r(x)\|_{\mathbf{M},v} = 0$. To jest $r(x)$ není pravdivá ve struktuře $\mathbf{M}$. Dále třeba formule $(\exists x)r(x)$ je pravdivá ve struktuře $\mathbf{M}$ (rozmyslete si proč). Na tomto příkladu si všimněme ještě jedné věci, ve struktuře nemusí být pravdivá

obecně ani φ, ani její negace $\neg\varphi$. Příkladem jsou právě formule $r(x)$ a $\neg r(x)$ a výše uvedená struktura $\mathbf{M}$.

(2) Uvažujme jazyk typu $\langle R, F, \sigma\rangle$, kde $F = \emptyset$ a $R = \{r, s\}$, r i s jsou unární. Mějme formuli

$$(\forall x)(r(x) \Rightarrow s(x)) \Rightarrow ((\forall x)r(x) \Rightarrow (\forall x)s(x)).$$

Ukážeme, že tato formule je tautologie. Budeme postupovat sporem, to jest předpokládejme, že existuje struktura $\mathbf{M}$ a $\mathbf{M}$-ohodnocení proměnných v při kterém je výše uvedená formule nepravdivá. Pak tedy $\|(\forall x)(r(x) \Rightarrow s(x))\|_{\mathbf{M},v} = 1$ a $\|(\forall x)r(x) \Rightarrow (\forall x)s(x)\|_{\mathbf{M},v} = 0$, to jest musí platit $\|(\forall x)r(x)\|_{\mathbf{M},v} = 1$, ale $\|(\forall x)s(x)\|_{\mathbf{M},v} = 0$. Existuje tedy $v' =_x v$ takové, že $\|r(x) \Rightarrow s(x)\|_{\mathbf{M},v'} = 1$, $\|r(x)\|_{\mathbf{M},v'} = 1$ a $\|s(x)\|_{\mathbf{M},v'} = 0$ což je ve sporu s tím jak jsme zavedli logickou operaci $\rightarrow$. $(\forall x)(r(x) \Rightarrow s(x)) \Rightarrow ((\forall x)r(x) \Rightarrow (\forall x)s(x))$ je tedy tautologie.

Definice 6.35. *Teorie* v jazyku PL typu $\langle R, F, \sigma\rangle$ je libovolná množina T formulí jazyka tohoto typu. Struktura $\mathbf{M}$ jazyka typu $\langle R, F, \sigma\rangle$ se nazývá *model teorie* T, píšeme $\mathbf{M} \vDash T$, jestliže každá formule z T je pravdivá v $\mathbf{M}$.

Teorie formalizuje soubor předpokladů.

Průvodce studiem

Pojem *teorie* je zcela přirozený. Běžně se říká „Podle má teorie . . . “, „S tvojí teorií nesouhlasím“ a podobně. Přitom teorií rozumíme soubor tvrzení, které daná osoba zastává, nebo ze kterých při svých úvahách vychází. Soubor tvrzení v predikátové logice představuje množina formulí. Rovněž pojem *model* je přirozený a často se vyskytuje v běžné komunikaci. Například obratem „Představme si (modelovou) situaci, kdy . . . “ chceme vyjádřit, abychom se soustředili na nějaký konkrétní model jisté teorie.

Příklad 6.36. (1) Uvažujme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $F = \{c\}$, $R = \{\approx, r\}$, c je nulární a r je binární. Uvažujme teorii T tohoto jazyka, která obsahuje následující čtyři formule

$$\begin{array}{l}(\forall x)r(x,x),\\ (\forall x)(\forall y)((r(x,y) \wedge r(y,x)) \Rightarrow x \approx y),\\ (\forall x)(\forall y)(\forall z)((r(x,y) \wedge r(y,z)) \Rightarrow r(x,z)),\\ (\forall x)r(c,x).\end{array}$$

Snadno nahlédneme, že první ze tří formulí popisují reflexivitu, antisymetrii a tranzitivitu relace $r^{\mathbf{M}}$ v každém modelu $\mathbf{M} \vDash T$. To jest v každém modelu $\mathbf{M} \vDash T$ je $r^{\mathbf{M}}$ uspořádání. Čtvrtá formule zajišťuje, že $\langle c^{\mathbf{M}}, m\rangle \in r^{\mathbf{M}}$ pro každý element $m \in M$. To jest $c^{\mathbf{M}}$ je konstanta, jejíž hodnotou je nejmenší prvek M vzhledem k uspořádání $r^{\mathbf{M}}$. Jinými slovy, $\mathbf{M}$ je modelem T, právě když je $r^{\mathbf{M}}$ uspořádání s nejmenším prvkem $c^{\mathbf{M}}$. Teorii T bychom tedy mohli chápat jako „teorii uspořádání s nejmenším prvkem“. Konkrétním modelem je například struktura $\mathbf{M}$, kde $M = \mathbb{N}$, $r^{\mathbf{M}} = \{\langle m, n\rangle \mid m \text{ dělí } n \text{ beze zbytku}\}$ a $c^{\mathbf{M}} = 1$.

(2) Kdybychom $r^{\mathbf{M}}$ z předchozího bodu změnili tak, že $r^{\mathbf{M}}$ by bylo přirozené uspořádání čísel (tak jak jej chápeme v matematice), výsledná struktura by byla opět modelem T. Kdybychom ale například změnili univerzum: $M = \mathbb{Z}$ a $r^{\mathbf{M}}$ by bylo přirozené uspořádání celých čísel, pak by se již nejednalo o model, protože v něm neexistuje žádné individuum, které je nejmenší vzhledem k přirozenému uspořádání celých čísel – v této struktuře by tím pádem formule $(\forall x)r(c,x)$ nebyla pravdivá nehledě na interpretaci konstanty c. Mohli bychom ale udělat následující trik: položíme $M = \mathbb{Z} \cup \{m\}$, kde m je nějaký symbol různý od všech celých čísel. Dále definujeme $c^{\mathbf{M}} = m$ a $r^{\mathbf{M}} = \{\langle a, b\rangle \mid a \text{ je } m \text{ nebo } a \leq b\}$. Potom je $\mathbf{M}$ opět model T. Element m, který jsme přidali do množiny celých čísel $\mathbb{Z}$ si lze představit jako nějaké nově přidané „nestandardní celé číslo“, které je menší než všechna ostatní celá čísla.

(3) Uvažujme nyní teorii S, která vznikne z T představené v bodu (1) tak, že k T přidáme formuli

$$(\forall x)(\forall y)(r(x,y) \vee r(y,x)),$$

pak $\mathbf{M} \vDash S$, právě když je $r^{\mathbf{M}}$ lineární uspořádání a nejmenším prvkem $c^{\mathbf{M}}$. To jest teorii S lze chápat jako teorii „lineárního uspořádání s nejmenším prvkem."

Některé teorie nemají model.

(4) Mějme jazyk typu $\langle R, F, \sigma\rangle$, kde $F = \emptyset$, $R = \{r\}$ a r je unární. Teorie

$$T = \{(\forall x)r(x), (\exists x)\neg r(x)\}$$

nemá žádný model. Vskutku, pokud by $\mathbf{M}$ byl model T, pak by pro nějaké $m \in M$ platilo $m \notin r^{\mathbf{M}}$, protože $\|(\exists x)\neg r(x)\|_{\mathbf{M},v} = 1$. Zároveň ale $\|(\forall x)r(x)\|_{\mathbf{M},v} = 1$, to jest $r^{\mathbf{M}} = M$, což je spor.

Nyní zavedeme sémantické vyplývání v predikátové logice.

Definice 6.37. Mějme teorii T jazyka typu $\langle R, F, \sigma\rangle$ a nechť φ je formule jazyka téhož typu. Formule φ *sémanticky plyne* z teorie T (neboli φ *je sémantickým důsledkem* T), což označujeme $T \vDash \varphi$, pokud pro každý model $\mathbf{M}$ teorie T platí, že φ je pravdivá v $\mathbf{M}$.

Inspekcí definice 6.37 snadno nahlédneme, že pojem sémantického vyplývání je zaveden analogicky jako v případě výrokové logiky, jen místo „pravdivostních ohodnocení" používáme z pochopitelných důvodů pojem model. Dále platí, že φ je tautologie, právě když $\vDash \varphi$, což je opět zřejmý vztah, který je analogický vztahu z výrokové logiky. Při pohledu na definici je také zřejmé, jak prokázat, že dané formule φ sémanticky *neplyne* z teorie T. Stačí najít jediný model $\mathbf{M} \vDash T$ a $\mathbf{M}$-ohodnocení v takové, že $\|\varphi\|_{\mathbf{M},v} = 0$ (což samozřejmě obecně nemusí být vůbec jednoduché). Daleko větším problémem je ověření, zda-li φ z T sémanticky plyne.

φ je tautologie, právě když $\vDash \varphi$.

Průvodce studiem

Na první pohled je zřejmé, že mechanické ověření sémantického vyplývání by vyžadovalo zkoumat pravdivost formule při všech $\mathbf{M}$-ohodnoceních, kterých je pro daný model $\mathbf{M}$ obecně nekonečně mnoho. Teorie navíc mohou mít nekonečně mnoho modelů, dokonce i když odhlédneme od identických kopií modelů, lišících se pouze „pojmenováním elementů". Mechanické ověření testováním pravdivosti hrubou silou „přes všechna $\mathbf{M}$-ohodnocení" je tedy v případě sémantického vyplývání v predikátové logice nemožné. V některých případech však lze o sémantickém vyplývání rozhodnout úvahou o pravdivostních hodnotách formulí.

Příklad 6.38. Uvažujme teorii uspořádání s nejmenším prvkem, kterou jsme představili v bodu (1) příkladu 6.36. Zřejmě formule $(\exists x)(\forall y)r(x,y)$ je sémantickým důsledkem této teorie, v každém modelu $\mathbf{M} \vDash T$ a pro každé $\mathbf{M}$-ohodnocení v můžeme vzít $\mathbf{M}$-ohodnocení $v' =_x v$, pro které položíme $v'(x) = c^{\mathbf{M}}$. Evidentně $\|(\forall y)r(x,y)\|_{\mathbf{M},v'} = 1$, tedy $\|(\exists x)(\forall y)r(x,y)\|_{\mathbf{M},v} = 1$. Na druhou stranu například formule $(\exists x)(\forall y)r(y,x)$ není sémantickým důsledkem T. Vezmeme-li model $\mathbf{M} \vDash T$, ve kterém je $M = \mathbb{N}$, $r^{\mathbf{M}}$ je přirozené uspořádání čísel a $c^{\mathbf{M}} = 1$, pak při každém $\mathbf{M}$-ohodnocení v máme $\|(\forall y)r(y,x)\|_{\mathbf{M},v} = 0$.

Výrokovou logiku lze chápat jako fragment predikátové logiky.

Doposud jsme nic neřekli o *vztahu predikátové a výrokové logiky* snad jen kromě neformálního konstatování, že výroková logika zkoumá usuzování o výrocích a predikátová logika se zabývá i samotnou strukturou výroků, to jest vztahy mezi individui. Výrokovou logiku je možné přirozeně zavést v predikátové logice a to hned několika způsoby. Nyní si stručně ukážeme jeden z nich.

Uvažujme jazyk PL typu $\langle R, F, \sigma\rangle$, kde $F = \emptyset$ a R obsahuje nekonečně mnoho nulárních relačních symbolů značených r_p, r_q, ... Dále budeme uvažovat struktury $\mathbf{M} = \langle M, R^{\mathbf{M}}, \emptyset\rangle$ pro výše uvedený jazyk. V každé takové struktuře je každý nulární relační symbol $r_p \in R$ interpretován nulární relací $r_p^{\mathbf{M}} \in R^{\mathbf{M}}$. Nulární relace je podmnožina nulté kartézské mocniny $M^0 = \{\emptyset\}$, máme tedy buď $r_p^{\mathbf{M}} = \emptyset$, nebo $r_p^{\mathbf{M}} = \{\emptyset\}$. To jest, $\|r_p\|_{\mathbf{M},v} = 1$, právě když $\emptyset \in r_p^{\mathbf{M}}$.

Nulární relační symboly z R můžeme chápat jako *výrokové symboly* a *výrokové formule* budeme chápat jako formule PL pro jazyk výše uvedeného typu, ve kterých nebudou proměnné ani kvantifikátory. Například tedy výroková formule $p \Rightarrow (\neg q \wedge p)$, kde p, q jsou výrokové symboly, bude korespondovat s formulí PL tvaru $r_p \Rightarrow (\neg r_q \wedge r_p)$, kde $r_p, r_q \in R$. Vezmeme-li pravdivostní ohodnocení e, můžeme k němu uvažovat strukturu $\mathbf{M}_e$ pro jazyk typu $\langle R, F, \sigma\rangle$, takovou, že $\emptyset \in r_p^{\mathbf{M}_e}$, právě když $e(p) = 1$. Evidentně dostáváme $\|\varphi\|_e = 1$, právě když $\|\varphi^*\|_{\mathbf{M}_e,v} = 1$, kde φ^* je formule PL jazyka typu $\langle R, F, \sigma\rangle$, která vznikla z výrokové formule φ tím, že jsme nahradili každý výrokový symbol p, q, ... ve formuli φ odpovídajícím nulárním relačním symbolem r_p, r_q, ... Syntaktické a sémantické pojmy výrokové logiky lze tedy formalizovat pomocí syntaktických a sémantických pojmů predikátové logiky.

6.4 Vlastnosti kvantifikace

V této sekci ukážeme některé vlastnosti kvantifikace, které se běžně využívají při úpravách formulí. Vlastnosti kvantifikací si budeme popisovat komentovaným výčtem tautologií. Uvedené vztahy si nebudeme dokazovat, na druhou stranu ale budeme upozorňovat na formule, které jsou uvedeným vztahům podobné, ale o tautologie se nejedná. Pro detailnější popis vlastností kvantifikátorů odkazujeme čtenáře na [Soch01, Šve02].

Následující tautologie vyjadřují *distribuci kvantifikace*:

$$\vDash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\forall x)\varphi \Rightarrow (\forall x)\psi), \tag{6.6}$$
$$\vDash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\exists x)\varphi \Rightarrow (\exists x)\psi). \tag{6.7}$$

Poznámka 6.39. Ukažme, že implikace u předchozích tautologií nelze obrátit. To jest ukážeme, že neplatí $\vDash ((\forall x)\varphi \Rightarrow (\forall x)\psi) \Rightarrow (\forall x)(\varphi \Rightarrow \psi)$ ani $\vDash ((\exists x)\varphi \Rightarrow (\exists x)\psi) \Rightarrow (\forall x)(\varphi \Rightarrow \psi)$. Vezměme si jazyk typu $\langle R, \emptyset, \sigma\rangle$, kde $R = \{r, s\}$, $\sigma(r) = \sigma(s) = 1$ a strukturu $\mathbf{M}$ pro jazyk tohoto typu, kde $M = \{a, b\}$ a $r^{\mathbf{M}} = \{a\}$, $s^{\mathbf{M}} = \{b\}$. Uvažujme, že φ je formule $r(x)$ a ψ je formule $s(x)$. Pak v $\mathbf{M}$ při libovolném ohodnocení v máme $\|(\forall x)r(x) \Rightarrow (\forall x)s(x)\|_{\mathbf{M},v} = 1$ a $\|(\exists x)r(x) \Rightarrow (\exists x)s(x)\|_{\mathbf{M},v} = 1$. Na druhou stranu ale $\|(\forall x)(r(x) \Rightarrow s(x))\|_{\mathbf{M},v} = 0$. To jest našli jsme model, ve kterém nejsou formule s obrácenými implikacemi pravdivé.

Pro popis dalších vlastností kvantifikátorů potřebujeme nejprve vymezit formule, jejichž pravdivost ve struktuře při daném ohodnocení nezávisí na ohodnocení dané proměnné.

Definice 6.40. Mějme jazyk PL typu $\langle R, F, \sigma\rangle$ a nechť φ je formule tohoto jazyka. Proměnná x *neovlivňuje pravdivost formule* φ, pokud pro libovolnou strukturu $\mathbf{M}$ jazyka typu $\langle R, F, \sigma\rangle$ platí $\|\varphi\|_{\mathbf{M},v} = \|\varphi\|_{\mathbf{M},v'}$ při každých $\mathbf{M}$-ohodnoceních v, v', kde $v' =_x v$. V opačném případě říkáme, že x *ovlivňuje pravdivost formule* φ.

Příklad 6.41. Proměnná x zřejmě ovlivňuje pravdivost například atomické formule $r(x)$ nebo formule $\neg r(x)$ a podobně. Na druhou stranu x neovlivňuje pravdivost formulí $r(y)$, $(\forall x)r(x)$, $(\exists x)r(x)$, $r(x) \Rightarrow r(x)$ a tak dále. Speciálním případem, kdy x neovlivňuje pravdivost formule φ je případ, kdy je každý výskyt proměnné x ve formuli φ obsažen v podformuli ϑ formule φ, přičemž ϑ je ve tvaru $(\forall x)\psi$, nebo $(\exists x)\psi$.

Následující tautologie vyjadřují *záměnu pořadí implikace a kvantifikace*:

$$\vDash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\forall x)\psi), \quad \text{pokud } x \text{ neovlivňuje pravdivost } \varphi, \tag{6.8}$$
$$\vDash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\exists x)\varphi \Rightarrow \psi), \quad \text{pokud } x \text{ neovlivňuje pravdivost } \psi, \tag{6.9}$$
$$\vDash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\exists x)\psi), \quad \text{pokud } x \text{ neovlivňuje pravdivost } \varphi, \tag{6.10}$$
$$\vDash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\forall x)\varphi \Rightarrow \psi), \quad \text{pokud } x \text{ neovlivňuje pravdivost } \psi. \tag{6.11}$$

Poznámka 6.42. Podmínka omezující předchozí tvrzení pouze na formule, jejichž pravdivost neovlivňuje proměnná x, je opět nutná a snadno najdeme protipříklad. Uvažujme typ jazyka

$\langle R, \emptyset, \sigma \rangle$, kde $R = \{r\}$, $\sigma(r) = 1$ a strukturu tohoto jazyka $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$, kde $M = \{a, b\}$ a relace $r^{\mathbf{M}}$ je definována $r^{\mathbf{M}} = \{a\}$. Kdyby platila tvrzení (6.8)–(6.11) v plném rozsahu, pak bychom pro formule φ, ψ rovny $r(x)$ měli $\|(\forall x)(r(x) \Rightarrow r(x))\|_{\mathbf{M},v} = 1$ v libovolném ohodnocení v. Pokud ale například pro (6.8) zvolíme ohodnocení v tak, že $v(x) = a$, pak $\|r(x) \Rightarrow (\forall x) r(x)\|_{\mathbf{M},v} = 0$.

Následující tautologie vyjadřují *záměnu pořadí kvantifikace a negace*:

$$\vDash \neg(\forall x)\varphi \Leftrightarrow (\exists x)\neg\varphi, \tag{6.12}$$
$$\vDash \neg(\exists x)\varphi \Leftrightarrow (\forall x)\neg\varphi. \tag{6.13}$$

Následující tautologie vyjadřují *záměnu pořadí kvantifikátorů*:

$$\vDash (\forall x)(\forall y)\varphi \Leftrightarrow (\forall y)(\forall x)\varphi, \tag{6.14}$$
$$\vDash (\exists x)(\exists y)\varphi \Leftrightarrow (\exists y)(\exists x)\varphi, \tag{6.15}$$
$$\vDash (\exists x)(\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi, \tag{6.16}$$

Poznámka 6.43. Pro tvrzení (6.16) opět ukážeme, že jej nelze prokázat pro obrácenou implikaci. Uvažujme jazyk typu $\langle R, \emptyset, \sigma \rangle$, kde $R = \{r\}$, $\sigma(r) = 2$ a strukturu tohoto jazyka $\mathbf{M} = \langle M, \{r^{\mathbf{M}}\}, \emptyset \rangle$, kde $M = \{a, b\}$ a relace $r^{\mathbf{M}}$ je definována $r^{\mathbf{M}} = \{\langle a, b\rangle, \langle b, a\rangle\}$. Ve struktuře $\mathbf{M}$ máme $\|(\forall y)(\exists x) r(x, y)\|_{\mathbf{M},v} = 1$ při libovolném ohodnocení v. Na druhou stranu však $\|(\exists x)(\forall y) r(x, y)\|_{\mathbf{M},v} = 0$ – máme model, ve kterém není $(\forall y)(\exists x)\varphi \Rightarrow (\exists x)(\forall y)\varphi$ pravdivá.

Průvodce studiem

Na konec letmého úvodu do predikátové logiky poznamenejme, že v predikátové logice rovněž zavádíme *syntaktické vyplývání* a že predikátová logika má *větu o úplnosti,* jejíž prokázání je výrazně méně triviální než ve výrokové logice. Výsledky predikátové logiky mají široké aplikace v informatice a matematice. Samotná predikátová logika se dělí na řadu disciplin, které se věnují různým problematikám: teorie důkazů, teorie struktur (teorie modelů), logické programování a automatické dokazování, rozhodnutelnost v logice a jiné.

6.5 Omezení klasické predikátové logiky a další logické kalkuly

Hluboké výsledky predikátové logiky ukázaly mnoho o formalizovaném myšlení, ukázaly mimo jiné i jeho meze – o některých z těchto mezí nyní víme, že je nikdy nebudeme moci překročit. Klasická predikátová logika má několik rysů, které lze v jistém smyslu chápat jako její omezení. Jeden ze základních výsledků predikátové logiky například říká, že axiomaticky nelze vymezit vlastnost „být konečný“. Jinými slovy, neexistuje žádná teorie T taková, že $\mathbf{M}$ je modelem T, právě když je $\mathbf{M}$ struktura s konečným nosičem. V kapitole 6.3.1 jsme konstatovali, že s jazyky s rovností zacházíme speciálním způsobem. Důvodem je fakt, že chceme, aby v každém modelu $\mathbf{M}$ teorie pro jazyk s rovností byl relační symbol rovnosti $\approx$ interpretován relací identity na M, to jest požadujeme $\approx^{\mathbf{M}} = \omega_M$. Toto je druhá vlastnost, kterou nelze axiomaticky vymezit. Jinými slovy, neexistuje teorie T jazyka obsahující binární relační symbol r taková, že $\mathbf{M}$ je modelem T, právě když je $r^{\mathbf{M}} = \{\langle u, u\rangle \mid u \in M\}$.

U některých tvrzení má smysl uvažovat o jejich pravdivosti, jsou tedy výroky, například „Člověk s výškou 180 cm je vysoký“, přesto se však zdráháme říci, zda-li je dané tvrzení pravdivé či nepravdivé. Pravdivostní hodnota, kterou bychom mu přiřadili, by byla někde mezi 0 a 1. Například řekneme-li, že „Člověk s výškou 180 cm je vysoký“ má pravdivostní hodnotu 0.8, říkáme tím, že dané tvrzení je pravdivé ve stupni 0.8, to jest, že je „skoro pravdivé“. Klasická výroková i predikátová logika, kterou jsme představili v předchozích kapitolách je omezená pouze na dvě základní pravdivostní hodnoty. Studiem více pravdivostních hodnot a studiem

vyplývání v prostředí vágnosti se zabývá *fuzzy logika,* která je v současné době intenzívně zkoumána.

Klasická logika rovněž nemá prostředky k formalizaci tvrzení obsahujících modality, například „je možné, že . . . “, „je nutné, že . . . “. Rozšíření klasické logiky o modality se nazývá *modální logika.* Modální logika našla uplatnění například ve formalizaci znalostních systémů. Oproti jazyku klasické výrokové logiky obsahuje jazyk modální logiky navíc unární spojky $\Box$ ($\Box\varphi$ má význam „je nutné, že φ“) a $\Diamond$ ($\Diamond\varphi$ má význam „je možné, že φ“). Sémantika modální logiky je založena na pojmu možný svět. Možný svět je obecná kategorie (v jednom možném světě může v daný okamžik pršet, ve druhém ne a podobně), která má řadu interpretací. Možné světy mohou být časové okamžiky, mohou reprezentovat názory jednotlivých expertů (co možný svět, to expert) a tak dále. Speciální interpretací světů získáme *logiku času* (*temporální logika*), což je logika zabývající se tvrzeními, jejichž pravdivostní hodnota závisí na čase. *Epistemická logika* se zabývá spojkami „ví se . . . “ a podobně.

Co se týče omezení predikátové logiky, které nelze jednoduše (respektive vůbec) vyřešit jejím rozšířením ať už o nové spojky nebo o další pravdivostní hodnoty, patří její *nerozhodnutelnost.* Neformálně řečeno, neexistuje žádný algoritmus, který by o vstupní teorii T a formuli φ dokázal po konečném počtu kroků říct, zda-li je φ sémantickým důsledkem T.

Shrnutí

Základním pojmem sémantiky predikátové logiky je struktura, která představuje interpretaci jazyka. Pro každý jazyk existuje nekonečně mnoho struktur. Proměnné jsou interpretovány ohodnocením proměnných. Pravdivost formulí má smysl uvažovat pouze máme-li dánu strukturu téhož jazyka a ohodnocení proměnných. Množiny formulí PL nazýváme teorie. Teorie formalizují intuitivní pojem souboru předpokladů. Model teorie je struktura, ve které jsou všechny formule dané teorie pravdivé. Některé teorie mají nekonečně mnoho modelů, jiné teorie nemají ani jeden model. Formule sémanticky plyne z dané teorie (téhož jazyka), pokud je tato formule pravdivá v každém modelu dané teorie. Predikátová logika má větu o úplnosti. Mezi další významné logické kalkuly patří: fuzzy logika (logika více pravdivostních hodnot), modální logika (logika modalit: možnosti, nutnosti, . . .), temporální logika (logika času), epistemická logika (logika znalosti). Predikátová logika má v mnoha směrech omezenou vyjadřovací sílu, některá z omezení predikátové logiky nelze obejít.

Pojmy k zapamatování

- individuum, univerzum, funkce, relace, struktura, ohodnocení proměnných,
- hodnota termu, pravdivostní hodnota formule,
- tautologie ve struktuře, tautologie,
- teorie, model teorie,
- fuzzy logika, modální logika, temporální logika, epistemická logika

Kontrolní otázky

1. *Proč v predikátové logice zavádíme pojem struktura?*
2. *Co je ohodnocení proměnných?*
3. *Jaký je rozdál mezi sémantickým vyplýváním ve VL a v PL?*
4. *Mají všechny teorie model?*
5. *V jakém vztahu je všeobecný a existenční kvantifikátor?*

Cvičení

1. Mějme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $R = \{\approx, r\}$, $F = \{k\}$, $\sigma(r) = 2$, $\sigma(k) = 1$. Nechť $\mathbf{M} = \langle M, R^{\mathbf{M}}, F^{\mathbf{M}}\rangle$ je struktura pro tento jazyk, kde

$$\begin{aligned} M &= \{a, b, c, d, e\}, \\ r^{\mathbf{M}} &= \{\langle a,a\rangle, \langle a,b\rangle, \langle a,c\rangle, \langle a,d\rangle, \langle a,e\rangle, \langle b,b\rangle, \langle b,d\rangle, \langle b,e\rangle, \\ &\quad \langle c,c\rangle, \langle c,e\rangle, \langle d,d\rangle, \langle d,e\rangle, \langle e,e\rangle\}, \\ k^{\mathbf{M}}(a) = e,\ k^{\mathbf{M}}(b) &= c,\ k^{\mathbf{M}}(c) = b,\ k^{\mathbf{M}}(d) = c,\ k^{\mathbf{M}}(e) = a. \end{aligned}$$

   Vyřešte následující úkoly.
   (a) Rozhodněte, zda-li je formule $r(x, y) \Rightarrow r(k(y), k(x))$ pravdivá v $\mathbf{M}$.
   (b) Určete, při jakých $\mathbf{M}$-ohodnoceních je formule $k(x) \approx k(y) \Rightarrow x \approx y$ pravdivá.
   (c) Rozhodněte, zda-li je formule $(\exists x)(\forall y)r(x, y) \Rightarrow x \approx y$ pravdivá v $\mathbf{M}$.
   (d) Modifikujte $\mathbf{M}$ tak, aby v ní byla formule $(\forall x)(\forall y)(\neg r(x, y) \Rightarrow r(y, x))$ pravdivá.
2. Mějme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $R = \{\approx, r\}$, $F = \{f\}$, r je binární, f je unární.
   Uvažujme teorii T tohoto jazyka, která sestává z formulí

$$\begin{aligned} &(\forall x)r(x, x), \\ &(\forall x)(\forall y)(r(x, y) \Rightarrow r(y, x)), \\ &f(x) \approx f(f(x)), \\ &r(x, y) \Rightarrow r(f(x), f(y)). \end{aligned}$$

   Rozhodněte, které z následujících formulí jsou sémantické důsledky T.
   (a) $x \approx f(x)$,
   (b) $(\forall x)(\forall y)(r(f(f(x)), f(f(y))) \vee \neg r(x, y))$,
   (c) $(\exists x)(\forall y)((\exists z)r(z, y) \Rightarrow (\exists z)\neg r(x, z))$,
   (d) $x \approx y \Rightarrow r(f(x), f(y))$,

Úkoly k textu

1. Uvažujme jazyk s rovností typu $\langle R, F, \sigma\rangle$, kde $F = \emptyset$ a R obsahuje kromě symbolu rovnosti $\approx$ jediný binární relační symbol r. Napište teorii T tohoto jazyka tak, aby struktura $\mathbf{M}$ pro jazyk typu $\langle R, F, \sigma\rangle$ byla modelem T, právě když $r^{\mathbf{M}}$ je *svazové uspořádání,* které nemá ani největší, ani nejmenší prvek.

Řešení

1. (a) $r(x, y) \Rightarrow r(k(y), k(x))$ je pravdivá v $\mathbf{M}$; (b) $k(x) \approx k(y) \Rightarrow x \approx y$ je pravdivá při všech ohodnoceních vyjma těch, kde $v(x) = b, v(y) = d$ nebo $v(x) = d, v(x) = b$; (c) $(\exists x)(\forall y)r(x, y) \Rightarrow x \approx y$ není pravdivá v $\mathbf{M}$, například při ohodnocení v, kde $v(x) = a$, $v(y) = b$ je $\|(\exists x)(\forall y)r(x, y) \Rightarrow x \approx y\|_{\mathbf{M},v} = 0$; (d) $r^{\mathbf{M}} = \{\langle a, b\rangle \mid a, b \in M\}$.
2. (a) není; (b) je; (c) není; (d) je.

Reference

[Goo98] Goodaire E. G., *Parmenter M. M.: Discrete Mathematics with Graph Theory*. Prentice-Hall, Inc., 1998.

[Gri99] Grimaldi R.: *Discrete and Combinatorial Mathematics. An Applied Introduction. 4th ed.* Addison Wesley, Reading, MA, 1999.

[KlYu95] Klir G. J., Yuan B.: *Fuzzy Sets and Fuzzy Loic. Theory and Applications.* Prentice Hall, Upper Saddle River, NJ, 1995.

[MaNe00] Matoušek J., Nešetřil J.: *Kapitoly z diskrétní matematiky.* Karolinum, Praha, 2000.

[Mau91] Maurer S. B., Ralston A.: *Discrete Algorithmic Mathematics*. Addison Wesley, 1991. DOPLNIT NOVEJSI REF.?

[PrYe73] Preparata F. P., Yeh R. T.: *Introduction to Discrete Structures. For Computer Science and Engineering.* Addison Wesley, Reading, MA, 1973.

[Soch01] Sochor A.: Klasická matematická logika. Karolinum, Praha, 2001 (v prodeji, velmi dobře psaná s řadou doplňujících informací).

[Šve02] Švejdar V.: Logika, neúplnost a složitost. Academia, Praha, 2002.

[Vil77] Vilenkin N. J.: *Kombinatorika.* SNTL, Praha, 1977.

A Seznam obrázků

B Seznam tabulek