1 Logika

Logika se zabývá správným usuzováním a odvozováním závěrů. Budeme se věnovat tzv. matematické logice, která se zaměřuje na vlasnosti matematických objektů, odvozování výsledků a jejich dokazování.

K zápisu matematických skutečností se používá matematického jazyka. Jeho výhodou je zestručnění a zpřesnění vyjadřování.

1.1 Výroková logika

Základním pojmem ve výrokové logice je *výrok*. Výrok může představovat nějaké jednoduché tvrzení, které je *pravdivé* nebo *nepravdivé*. Z hlediska logiky nás budou zajímat vztahy mezi výroky a posuzování pravdivosti tzv. *formulí*, což jsou tvrzení složená z výroků.

Příklad 1. „Čtverec je čtyřúhelník a 2 je prvočíslo.“ je formule složená z výroků „Čtverec je čtyřúhelník“ a „2 je prvočíslo.“ pomocí spojky „a“.

Z příkladu je zřejmé, že podobným způsobem bychom mohli vytvářet formule z libovolných výroků a dokonce i z již vytvořených formulí. Má tedy smysl zapomenout na konkrétní obsah výroků a pracovat s nimi jako s abstraktními objekty. Nechť tedy písmena $A, B, C, \ldots$ značí výroky. Formule budeme vytvářet postupným skládáním již vytvořených formulí pomocí tzv. *logických spojek*. Používat budeme následující:

negace — čteme „ne“ nebo „neplatí“, značíme $\neg$,

konjunkce — čteme „a“, značíme $\wedge$,

disjunkce — čteme „nebo“, značíme $\vee$,

implikace — čteme „jestliže . . . , potom . . . “ nebo „implikuje“, značíme $\rightarrow$,

ekvivalence — čteme „právě když“ nebo „je ekvivalentní“, značíme $\leftrightarrow$.

Definice formule (říká se jí induktivní) pak vypadá následovně:

Definice 1. (1) Každý výrok je formule.

(2) Jsou-li φ, ψ formule, pak $(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi)$ jsou formule.

Chceme-li zjistit, zda je nějaký výraz korektně vytvořenou formulí, postupujeme obráceně, tj. „rozebíráme“ výraz na jednodušší celky a kontrolujeme zda jsou spojeny v souladu s pravidly definice. Uzávorkování uvnitř formule je podstatné a může zcela změnit její smysl. Dohodněme se, že vnější závorku lze vynechat a že negace má přednost před ostatními spojkami.

Příklad 2. Nechť A, B jsou výroky. $(A \vee B) \wedge \neg A$ je formule vzniklá spojením podformulí $A \vee B$ a $\neg A$. $A \vee B$ je spojením A a B a $\neg A$ vznikla přidáním negace k A. Jedná se tedy o korektně vytvořenou formuli.

Známe-li pravdivost podformulí, z nichž je formule vytvořena, vyhodnocuje se pravdivost složené formule podle následující tabulky.

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \to \psi$	$\varphi \leftrightarrow \psi$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Zde 1 značí, že formule je pravdivá, a 0, že je nepravdivá. K posouzení pravdivosti formule výrokové logiky tedy většinou potřebujeme znát pravdivost výroků v ní obsažených a podle tabulky ji postupně dopočítáme. Můžeme také dostat za úkol dopočítat pravdivost formule pro všechna možná ohodnocení výroků, což obvykle řešíme sestrojením vhodné tabulky podformulí.

Je-li formule pravdivá pro libovolné ohodnocení výroků, nazývá se *tautologie*. Je-li formule nepravdivá pro libovolné ohodnocení výroků, nazývá se *kontradikce*.

Řekneme, že formule φ a ψ jsou *ekvivalentní*, pokud mají stejná pravdivostní ohodnocení pro všechna ohodnocení výroků (tedy stejný sloupec hodnot v pravdivostní tabulce), zapisujeme $\varphi \Leftrightarrow \psi$. Znamená to totéž jako říct, že složená formule $\varphi \leftrightarrow \psi$ je pravdivá. Zápis $\varphi \Leftrightarrow \psi$ je tedy zkratkou soudu vysloveného o dvou formulích, kdežto $\varphi \leftrightarrow \psi$ je jediná formule. (Rozdílem v zápisu se tedy nemusíme prozatím moc znepokojovat.) Ekvivalence formulí znamená, že vyjadřují stejnou skutečnost, nikoli, že jsou si rovny (to by musely mít totožný zápis).

Podobně řekneme, že z φ vyplývá ψ (neboli ψ je důsledkem φ, pokud pro ψ je pravdivá vždy, když je pravdivá φ, značíme $\varphi \Rightarrow \psi$. Opět to znamená totéž jako říct, že formule $\varphi \to \psi$ je pravdivá.

O tom, zda jsou dané formule ekvivalentní nebo jedna vyplývá z druhé, se lze kromě sestrojení výrokové tabulky přesvědčit i úpravou podle *logických pravidel*, což jsou jednoduché ekvivalence (nebo vyplývání) formulí. Tento

postup je obvyklý v *matematických důkazech*. Mezi užitečná pravidla patří:

$$\begin{aligned}
\neg\neg\varphi &\Leftrightarrow \varphi && \text{dvojí negace}\\
\varphi \wedge \varphi &\Leftrightarrow \varphi && \text{idempotence}\\
\varphi \vee \varphi &\Leftrightarrow \varphi &&\\
\varphi \wedge \psi &\Leftrightarrow \psi \wedge \varphi && \text{komutativita}\\
\varphi \vee \psi &\Leftrightarrow \psi \vee \varphi &&\\
(\varphi \wedge \psi) \wedge \chi &\Leftrightarrow \varphi \wedge (\psi \wedge \chi) && \text{asociativita}\\
(\varphi \vee \psi) \vee \chi &\Leftrightarrow \varphi \vee (\psi \vee \chi) &&\\
\varphi \wedge (\psi \vee \chi) &\Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \chi) && \text{distributivita}\\
\varphi \vee (\psi \wedge \chi) &\Leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \chi) &&\\
\varphi \wedge (\varphi \vee \psi) &\Leftrightarrow \varphi && \text{absorpce}\\
\varphi \vee (\varphi \wedge \psi) &\Leftrightarrow \varphi &&\\
\varphi \leftrightarrow \psi &\Leftrightarrow (\varphi \to \psi) \wedge (\psi \to \varphi) && \text{odstranění ekvivalence}\\
\varphi \to \psi &\Leftrightarrow \neg\varphi \vee \psi && \text{odstranění implikace}\\
\neg(\varphi \wedge \psi) &\Leftrightarrow \neg\varphi \vee \neg\psi && \text{de Morganova pravidla}\\
\neg(\varphi \vee \psi) &\Leftrightarrow \neg\varphi \wedge \neg\psi &&\\
\varphi \to \psi &\Leftrightarrow \neg\psi \to \neg\varphi && \text{obměna implikace}
\end{aligned}$$

Z pravidel vyplývá zajímavý fakt, že každá formule je ekvivalentní formuli tvořené pouze spojkami $\neg, \wedge, \vee$ nebo i pouze $\neg, \wedge$. Dokonce lze ekvivalentní formuli sestrojit pomocí jediné speciální logické spojky (využití v elektronice).

1.2 Predikátová logika

Prostředky výrokové logiky jsou poměrně slabé a k popisu většiny matematických skutečností by nestačily. V predikátové logice se výroky nahrazují tvrzeními popisujícími nějakou vlastnost objektů nebo vztahy mezi nimi, např. $x < 2$ nebo $x = y$. K jazyku výrokové logiky přidáváme symboly *proměnných* (např. $x, y, z, \dots$) a tzv. *predikátových symbolů* (např. $<, =, +, 0$, jejich přesnější vysvětlení prozatím odložíme). Krom toho máme k dispozici *kvantifikátory*:

všeobecný — čteme „každý“, „všechny“, atp., značíme $\forall$,

existenční — čteme „existuje“ nebo „aspoň jeden“, značíme $\exists$.

Za kvantifikátorem musí vždy následovat proměnná, na kterou se kvantifikátor vztahuje. Formule predikátové logiky se vytváří stejně jako ve výrokové logice a navíc podle pravidla

(3) Je-li φ formule a x proměnná, jsou i $(\forall x)\varphi$ a $(\exists x)\varphi$ formule.

Příklad 3. $(\forall x)(\forall y)(\exists z)(x + z = y)$ je formule vzniklá podle postupným (trojím) aplikováním pravidla (3) na formuli $x + z = y$.

Při posuzování pravdivosti formulí predikátové logiky je podstatné, v jaké množině nebo struktuře se pohybujeme. Např. formule $(\exists x)(\forall y)x \leq y$ říká, že existuje nejmenší prvek. V množině přirozených čísel $\mathbb{N}$ tedy platí, zatímco v množině celých čísel $\mathbb{Z}$ neplatí. Proměnné ve formuli tedy zastupují prvky množiny a predikátové symboly její strukturu (přesněji vysvětlíme v kapitole Relace). Tautologií v predikátové logice rozumíme formuli platnou všude.

V predikátové logice máme k dispozici další logická pravidla pro práci s kvantifikátory:

$$\begin{aligned}
\neg(\forall x)\varphi &\Leftrightarrow (\exists x)\neg\varphi && \text{negace kvantifikátoru}\\
\neg(\exists x)\varphi &\Leftrightarrow (\forall x)\neg\varphi &&\\
(\forall x)(\forall y)\varphi &\Leftrightarrow (\forall y)(\forall x)\varphi && \text{komutativita kvantifikátorů}\\
(\exists x)(\exists y)\varphi &\Leftrightarrow (\exists y)(\exists x)\varphi && \text{stejného typu}\\
(\exists x)(\forall y)\varphi &\Rightarrow (\forall y)(\exists x)\varphi && \text{(jen v tomto směru!)}\\
(\forall x)(\varphi \wedge \psi) &\Leftrightarrow (\forall x)\varphi \wedge (\forall x)\psi &&\\
(\exists x)(\varphi \vee \psi) &\Leftrightarrow (\exists x)\varphi \vee (\exists x)\psi &&
\end{aligned}$$

Pokud se proměnná x nevyskytuje ve φ, platí také

$$\begin{aligned}
\varphi \wedge (\forall x)\psi &\Leftrightarrow (\forall x)(\varphi \wedge \psi),\\
\varphi \vee (\forall x)\psi &\Leftrightarrow (\forall x)(\varphi \vee \psi),\\
\varphi \wedge (\exists x)\psi &\Leftrightarrow (\exists x)(\varphi \wedge \psi),\\
\varphi \vee (\exists x)\psi &\Leftrightarrow (\exists x)(\varphi \vee \psi).
\end{aligned}$$

V predikátové logice se všechny proměnné a predikátové symboly vztahují ke stejné množině. To může být někdy velmi omezující, proto se v matematice používají i formule logik vyššího řádu, např. $(\forall x > 0)(\exists n \in \mathbb{N})(0 < f(n) < x)$.

2 Množiny

Veškeré matematické teorie (včetně logiky samotné) se dnes již budují axiomaticky, tzn. stanoví se *axiomy*, což jsou určité formule, o kterých se předpokládá, že pro objekty dané teorie vždy platí. Součástí logického systému jsou dále *odvozovací pravidla*, pomocí kterých se dají dokazovat další formule.

Axiomaticky lze vybudovat i teorii množin, ale spokojíme se s „naivním“ přístupem a budeme předpokládat, že bezpečný způsob vytváření množin je nám jasný.

Základním predikátovým symbolem teorie množin je $\in$ označující náležení prvku do množiny, např. $x \in A$ značí, že x je prvkem množiny A. Tato vlastnost je pouze relativní, tzn. i prvek nějaké množiny může být sám množinou (případně obsahující jiné prvky). Pokud máme takovou složitější strukturu množin a je zřejmá jejich hierarchie, obvykle značíme malým písmenem $a, b, c, \ldots$ prvky v nejnižším „patře“, velkým písmenem $A, B, C, \ldots$ množiny, které jsou jimi tvořeny a psacím velkým písmenem $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ množiny vytvářené z předchozích množin. Pro snazší vyjadřování se posledně jmenovaným také říká *systémy množin*.

Symbolem $\emptyset$ značíme *prázdnou množinu*, tj. množinu, která neobsahuje žádný prvek. Množiny lze zapisovat *výčtem*, např. $A = \{x, y, z\}$, nebo specifikací prvků nějakou *vlastností*, např. $A = \{x \mid x \text{ je celé liché číslo}\}$. Dvě množiny jsou si *rovny*, pokud mají stejné prvky, např. $\{a, b\} = \{b, a, a\}$ nebo $\{x \mid x \text{ je přirozené číslo menší než } 4\} = \{1, 2, 3\}$. Formálně zapsáno $A = B \Leftrightarrow (x \in A \leftrightarrow x \in B)$.

Řekneme, že množina A je *podmnožinou* množiny B, pokud každý prvek množiny A je i prvkem množiny B, značíme $A \subseteq B$. Vyjádřeno formulí, $x \in A \to x \in B$.

Věta 1. *Nechť A, B, C jsou množiny. Pak platí:*
(1) $\emptyset \subseteq A$,
(2) $A \subseteq A$,
(3) $(A \subseteq B \ \wedge \ B \subseteq C) \to A \subseteq C$,
(4) $(A \subseteq B \ \wedge \ B \subseteq A) \to A = B$.

Důkaz. (1) U implikace $x \in \emptyset \to x \in A$ není splněn předpoklad, tedy platí.

(2) $x \in A \to x \in A$ je tautologie.

(3) Pokud $x \in A \to x \in C$ by byla nepravdivá, pak $x \in A$ je pravdivá a $x \in C$ pravdivá. Pak by ovšem neplatila $x \in A \to x \in B$ (pokud je $x \in B$ nepravdivá) nebo $x \in B \to x \in C$ (pokud je $x \in B$ pravdivá). Tzn. neplatí-li $A \subseteq C$, neplatí ani $A \subseteq B \ \wedge \ B \subseteq A$.

(4) Použijeme pravidlo pro odstranění ekvivalence: $((x \in A \to x \in B) \ \wedge \ (x \in B \to x \in A)) \ \Leftrightarrow \ (x \in A \ \leftrightarrow \ x \in B)$. □

Definice 2. Nechť A, B jsou množiny.
Průnikem množin A, B se nazývá množina $A \cap B = \{x \mid x \in A \wedge x \in B\}$,
sjednocením množina $A \cup B = \{x \mid x \in A \ \vee \ x \in B\}$
a *rozdílem* množina $A - B = \{x \mid x \in A \ \wedge \ \neg x \in B\}$.

Je-li $A \subseteq B$, nazývá se množina $B - A$ doplňkem množiny A v B a je-li B známa, značí se doplněk A'.

Potenční množinou množiny A se rozumí množina všech jejích podmnožin, tj. množina $\mathcal{P}(A) = \{B \mid B \subseteq A\}$.

Z vlastností logických operací $\wedge, \vee$ snadno vyplývají obdobné vlastnosti průniku a sjednocení:

$$\begin{aligned} A \cap A &= A, & A \cup A &= A, \\ A \cap B &= B \cap A, & A \cup B &= B \cup A, \\ (A \cap B) \cap C &= A \cap (B \cap C), & (A \cup B) \cup C &= A \cup (B \cup C), \text{ atd.} \end{aligned}$$

Definice 3. Nechť $\mathcal{A}$ je systém množin. Definujeme

$$\begin{aligned} \bigcap \mathcal{A} &= \{x \mid (\forall A \in \mathcal{A})\ x \in A\}, \\ \bigcup \mathcal{A} &= \{x \mid (\exists A \in \mathcal{A})\ x \in A\}. \end{aligned}$$

Pro zpřehlednění systémů množin se často používá *indexování*. Znamená to, že každá množina systému je označena ve tvaru A_i, kde i je pro každou množinu jedinečný a nazývá se *index*. Množina všech indexů, řekněme I, se nazývá *indexová množina*. Indexovat můžeme čímkoli, nejenom čísly. Systém pak zapisujeme ve tvaru $\{A_i\}_{i \in I}$ a definici „velkého“ průniku a sjednocení lze přepsat

$$\begin{aligned} \bigcap_{i \in I} A_i &= \{x \mid (\forall i \in I)\ x \in A_i\}, \\ \bigcup_{i \in I} A_i &= \{x \mid (\exists i \in I)\ x \in A_i\}. \end{aligned}$$

Uvědomme si, že $A_1 \cap A_2 = \bigcup_{i \in \{1,2\}} A_i$, „velký“ průnik je tedy rozšířením průniku dvou množin (podobně pro sjednocení). Platí např. i obecnější distributivní zákony:

Věta 2. *Nechť A je množina, $\{B_i\}_{i \in I}$ systém množin. Pak platí*

$$\begin{aligned} A \cap \bigcup_{i \in I} B_i &= \bigcup_{i \in I} (A \cap B_i), \\ A \cup \bigcap_{i \in I} B_i &= \bigcap_{i \in I} (A \cup B_i). \end{aligned}$$

Důkaz. $x \in A \cap \bigcup_{i\in I} B_i \Leftrightarrow x \in A \wedge x \in \bigcup_{i\in I} B_i \Leftrightarrow x \in A \wedge (\exists i \in I)\, x \in B_i \Leftrightarrow (\exists i \in I)(x \in A \wedge x \in B_i) \Leftrightarrow x \in \bigcup_{i\in I}(A \cap B_i)$. Důkaz druhého zákona je analogický. □

Uspořádanou dvojici prvků a, b označme (a, b). Pro dvě uspořádané dvojice $(a, b), (c, d)$ platí $(a, b) = (c, d)$, pokud $a = c$ a $b = d$.

Definice 4. Nechť A, B jsou množiny. *Kartézským součinem* množin A, B se nazývá množina

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Kartézský součin není komutativní, ačkoli dvojice (a, b) z $A \times B$ a (b, a) z $B \times A$ si vzájemně odpovídají (pořadí složek je důležité!). Dokonce není ani asociativní — $(A\times B)\times C$ má prvky tvaru $((a, b), c)$, zatímco $A\times(B\times C)$ tvaru $(a, (b, c))$. V praxi ale můžeme tento rozdíl zanedbávat a uvažovat součin $A \times B \times C$ jako množinu uspořádaných trojic (a, b, c).

Věta 3. *Nechť A je množina, $\{B_i\}_{i\in I}$ systém množin. Pak platí*

$$A \times \bigcup_{i\in I} B_i = \bigcup_{i\in I}(A \times B_i),$$
$$A \times \bigcap_{i\in I} B_i = \bigcap_{i\in I}(A \times B_i).$$

Důkaz. $(a, b) \in A \times \bigcup_{i\in I} B_i \Leftrightarrow a \in A \wedge b \in \bigcup_{i\in I} B_i \Leftrightarrow a \in A \wedge (\exists i \in I)\, b \in B_i \Leftrightarrow (\exists i \in I)(a \in A \wedge b \in B_i) \Leftrightarrow (\exists i \in I)\, (a, b) \in A \times B_i \Leftrightarrow (a, b) \in \bigcup_{i\in I}(A \times B_i)$. Důkaz druhé rovnosti je analogický. □

3 Zobrazení

Zobrazením množiny A do množiny B rozumíme předpis, který každému prvku množiny A jednoznačně přiřazuje nějaký prvek množiny B. Zobrazení f množiny A do B zapisujeme $f : A \to B$. Množina A se nazývá *definiční obor*, množina B *obor hodnot*. Skutečnost, že f zobrazí prvek $a \in A$ na prvek $b \in B$ zapisujeme $f(a) = b$ nebo $a \mapsto b$ (pokud nehrozí záměna s jiným zobrazním). Prvek a se nazývá *vzor* prvku b, prvek b se nazývá *obraz* prvku a. Lze-li pomocí proměnné takto zadat celé zobrazení, říkáme výrazu $f(x) = \ldots$ *předpis* zobrazení.

Příklad 4. (1) $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ je zobrazení.

(2) $f : \mathbb{R} \to \mathbb{R}, f(x) = \sqrt{x}$ není zobrazení. Pro $x < 0$ totiž není výraz $\sqrt{x}$ není definován (přinejmenším není reálný).

(3) $f : \mathbb{R}^+ \to \mathbb{R}, f(x) = \sqrt{x}$ je zobrazení.

(4) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = \frac{x}{2}$ není zobrazení. Pro lichá x neleží obraz $\frac{x}{2}$ v oboru hodnot.

Definice 5. Nechť $f : A \to B$ je zobrazení. f se nazývá

prosté (injektivní), jsou-li obrazy různých prvků různé, tj. $f(a) = f(b) \to a = b$,

na (surjektivní), má-li každý prvek oboru hodnot nějaký vzor, tj. $(\forall b \in B)(\exists a \in A)\ f(a) = b$,

bijektivní, je-li současně injektivní i surjektivní.

Příklad 5. (1) $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ není injektivní ani surjektivní. Máme $(-1)^2 = 1^2$, přitom $-1 \neq 1$. Např. prvek -1 nemá vzor.

(2) $f : \mathbb{R} \to [-1; 1], f(x) = \sin x$ je surjektivní, není injektivní. Každý prvek má vzor (jeden z nich můžeme najít funkcí arcsin). Každý prvek intervalu $[-1; 1]$ má ovšem nekonečně mnoho vzorů (sin má periodu 2π).

(3) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = 2x$ je injektivní, není surjektivní. Z $2x = 2y$ vyplývá $x = y$. Jakékoli liché číslo nemá vzor.

(4) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = -x$ je bijektivní. Z $-x = -y$ plyne $x = y$ a libovolné x má vzor $-x$.

Mezi důležitá zobrazení patří:

identita — $id_A : A \to A, x \mapsto x$ (bijekce),

inkluze — pro $B \subseteq A$ předpis $i : A \to B, x \mapsto x$ (injekce),

prázdné zobrazení — $o_A : \emptyset \to A$ (injekce),

projekce — $p_A : A \times B \to A, p_A((x, y)) = x$, resp. $p_B : A \times B \to B, p_B((x, y)) = y$ (surjekce pro neprázdné A, B).

Nechť A, B, C jsou množiny a $f : A \to B, g : B \to C$ zobrazení. Pak existuje *složené zobrazení* $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(x) = g(f(x)).$$

Věta 4. *Nechť $f : A \to B, g : B \to C, h : C \to D$ jsou zobrazení mezi množinami A, B, C, D. Pak platí:*

(1) $h \circ (g \circ f) = (h \circ g) \circ f$,

(2) $id_B \circ f = f$,

(3) $f \circ id_A$.

Důkaz. (1) Pro libovolné $x \in A$ platí $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. Podobně (2) $(id_B \circ f)(x) = id_B(f(x)) = f(x)$ a (3) $(f \circ id_A)(x) = f(id_A(x)) = f(x)$. □

Věta 5. *Nechť $f : A \to B, g : B \to C$ jsou zobrazení mezi množinami A, B, C. Pak platí:*

(1) Jsou-li f, g injektivní, je i $g \circ f$ injektivní.

(2) Jsou-li f, g surjektivní, je i $g \circ f$ surjektivní.

(3) Je-li $g \circ f$ injektivní, je i f injektivní.

(4) Je-li $g \circ f$ surjektivní, je i g surjektivní.

Důkaz. Cvičení. □

Zobrazení $g : B \to A$ se nazývá *inverzní* k zobrazení $f : A \to B$, jestliže $g \circ f = id_A$ a $f \circ g = id_B$.

Věta 6. *K zobrazení $f : A \to B$ existuje zobrazení inverzní právě tehdy, když f je bijekce. Inverzní zobrazení je určeno jednoznačně.*

Důkaz. Předpokládejme, že existuje zobrazení inverzní $g : B \to A$. Pro $x, y \in A$ máme $f(x) = f(y) \;\Rightarrow\; x = (g \circ f)(x) = (g \circ f)(y) = y$, tedy f je prosté. Pro $v \in B$ máme $f(g(v)) = (f \circ g)(v) = v$, tedy $g(v)$ je vzorem v a f je na. Celkem f je bijekce.

Naopak předpokládejme, že $f : A \to B$ je bijekce. Každý prvek $u \in V$ má tedy nějaký vzor, protože f je na. Tento vzor je navíc jediný, protože f je prosté. $g : B \to A$ tedy sestrojíme jako přiřazení jedinečných vzorů prvků množiny B v zobrazení f.

Konečně předpokládejme, že $g, h : B \to A$ jsou dvě inverzní zobrazení k zobrazení $f : A \to B$. Pak $g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h$. □

Inverzní zobrazení k zobrazení $f : A \to B$ (už víme že jediné) budeme značit $f^{-1} : B \to A$.

Množinu všech zobrazení množiny A do množiny B značíme B^A.

Je-li $B \subseteq A$, definujeme její *charakteristickou funkci* $\chi_B : A \to \{0, 1\}$ předpisem

$$\chi_B(x) = \begin{cases} 1, & x \in B, \\ 0, & x \notin B. \end{cases}$$

Věta 7. *Předpis $B \mapsto \chi_B$ určuje bijekci $f : \mathcal{P}(A) \to \{0, 1\}^A$.*

Důkaz. Stačí najít inverzní zobrazení $f^{-1} : \{0, 1\}^A \to \mathcal{P}(A)$. Pro $h \in \{0, 1\}^A$ položme $f^{-1}(h) = \{x \in A \mid h(x) = 1\}$. Zřejmě $\chi_{f^{-1}(h)} = h$ a $f^{-1}(\chi_B) = B$, f^{-1} je tedy skutečně inverzní k f. □

3.1 Mohutnost množiny

Řekneme, že množiny A, B *mají stejnou mohutnost*, pokud existuje bijekce $f : A \to B$. U konečných množin to znamená, že mají stejný počet prvků. Z vlastností bijekcí vyplývá, že vztah „mít stejnou mohutnost“ je relací ekvivalence na třídě všech množin (viz Relace). Každé množině pak můžeme korektně přiřadit symbol reprezentující všechny množiny o stejné mohutnosti, který nazýváme *kardinální číslo*. Pak říkáme, že množina A má příslušnou *mohutnost* a zapisujeme ji $|A|$. Pro mohutnosti konečných množin se kardinální čísla zapisují pomocí přirozených čísel a nuly (mohutnost prázdné množiny) Např. píšeme $|\{a, b, c\}| = 3$.

Množina se nazývá *spočetná*, pokud má stejnou mohutnost jako množina přirozených čísel. (Spočetná je tedy nekonečná!) Kardinální číslo spočetných množin se značí symbolem $\aleph_0$ (alef nula). Mezi spočetné množiny patří např. $\mathbb{N}, \mathbb{N} \cup \{0\}, \mathbb{Z}, \mathbb{N} \times \mathbb{N}, \mathbb{Q}$ a množina všech konečných posloupností přirozených čísel.

Nekonečná množina, která není spočetná, se nazývá *nespočetná*. Mezi nespočetné množiny patří např. $\mathbb{R}, \mathcal{P}(\mathbb{N}), \mathbb{N}^{\mathbb{N}}$ (tj. množina všech nekonečných posloupností přirozených čísel). Uvedené příklady mají stejnou mohutnost, která se nazývá *mohutnost kontinua*. Existují i množiny větších mohutností, např. množina všech reálných funkcí (ovšem množina všech *spojitých* reálných funkcí má ještě mohutnost kontinua).

4 Relace

Relace popisují vztahy mezi prvky množin. Podle počtu těchto množin rozlišujeme relace na unární, binární, ternární, atd. Budeme se zabývat výhradně binárními relacemi.

(Binární) relací R mezi množinami A, B je podmnožina $R \subseteq A \times B$. Pokud $A = B$, hovoříme o relaci *na* množině. Vztah $(x, y) \in R$ také zapisujeme xRy.

Pro znázornění relací se někdy používají *šipkové diagramy*, kde příslušnost dvojice (x, y) do relace se zakresluje jako šipka z x do y. U relací na množině je možný dvojí způsob kreslení diagramů — jedna kopie množiny a šipky uvnitř (obvyklé) nebo dvě kopie množiny a šipky mezi nimi (vhodnější pro skládání relací).

Příklad 6. (1) Nechť A je množina knih v knihovně, B množina čtenářů. Relaci R můžeme definovat jako množinu výpůjček, tj. $R = \{(x, y) \in A \times B \mid$ čtenář y má půjčenou knihu $x\}$.

(2) $<$ je relace na množině $\mathbb{N}$.

(3) $=$ je relace na jakékoli množině (tzv. identická relace, viz dále).

(4) $\subseteq$ je relace na $\mathcal{P}(A)$ pro jakoukoli množinu A.

(5) Zobrazení $f : A \to B$ je relace mezi A a B splňující podmínku $(\forall x \in A)(\exists! y \in B)(x, y) \in f$ ($\exists!$ znamená „existuje právě jedno“). Takto se správně zavádí pojem zobrazení.

Skládání relací rozšiřuje skládání zobrazení a pro relace $R \subseteq A \times B, S \subseteq B \times C$ je definováno následovně:

$$S \circ R = \{(x, y) \in A \times C \mid (\exists z \in B)((x, z) \in R \ \wedge \ (z, y) \in S)\}.$$

Identická relace id_A na množině A je totožná s identickým zobrazením na A chápaným jako relace, tj. $id_A = \{(x, x) \mid x \in A\}$.

Inverzní relace $R^{-1} \subseteq B \times A$ k relaci $R \subseteq A \times B$ je relace $R^{-1} = \{(y, x) \mid (x, y) \in R\}$. Všimněte si, že inverzi má každá relace. Pokud R je zobrazení, které není bijektivní, R^{-1} není zobrazení (proto se inverzní zobrazení definovalo jen pro bijekce). Také obecně $R \circ R^{-1} \neq id_B$ a $R^{-1} \circ R \neq id_A$.

Věta 8. *Nechť $R \subseteq A \times B, S \subseteq B \times C, T \subseteq C \times D$ jsou relace. Pak platí:*
(1) $(T \circ S) \circ R = T \circ (S \circ R)$,
(2) $R \circ id_A = R$,
(3) $id_B \circ R = R$.

Důkaz. (1) $(T \circ S) \circ R = \{(x, y) \in A \times D \mid (\exists z \in B)((x, z) \in R \ \wedge \ (z, y) \in T \circ S)\} = \{(x, y) \in A \times D \mid (\exists z \in B)((x, z) \in R \ \wedge \ (\exists w \in C)((z, w) \in S \wedge (w, y) \in T))\} = \{(x, y) \in A \times D \mid (\exists z \in B, w \in C)((x, z) \in R \wedge (z, w) \in S \ \wedge \ (w, y) \in T)\}$. Pravá strana rovnosti se analogicky upraví na stejný tvar.

(2) $R \circ id_A = \{(x, y) \mid (\exists z \in A)((x, z) \in id_A \ \wedge \ (z, y) \in R)\}$, přitom $(x, z) \in id_A$ nastává jen pro $x = z$, odtud $R \circ id_A = R$. Podobně (3). □

Relace ρ na množině A se nazývá

reflexivní — $(\forall x)(x \rho x$, tj. $id_A \subseteq \rho$,

symetrická — $(\forall x, y)(x \rho y \ \to \ y \rho x)$, tj. $\rho = \rho^{-1}$,

antisymetrická — $(\forall x, y)((x \rho y \ \wedge y \rho x) \ \to \ x = y)$, tj. $\rho \cap \rho^{-1} \subseteq id_A$,

tranzitivní — $(\forall x, y, z)((x \rho y \ \wedge \ y \rho z) \ \to \ x \rho z)$, tj. $\rho \circ \rho \subseteq \rho$.

ekvivalence, je-li reflexivní, symetrická a tranzitivní,

uspořádání, je-li reflexivní, antisymetrická a tranzitivní.

Vlastnosti symetrie a antisymetrie nejsou protikladné a lze najít relace, které splňují obě.

Příklad 7. (1) $<$ na $\mathbb{N}$ je antisymetrická a tranzitivní, není relexivní ani symetrická.

(2) $\subseteq$ na $\mathcal{P}(A)$ je relace uspořádání.

(3) Relace $\{(x, x+1) \mid x \in \mathbb{N}\}$ na $\mathbb{N}$ je antisymetrická, není reflexivní, symetrická ani tranzitivní.

(4) Identická relace splňuje všechny čtyři vlastnosti, je tedy současně relací ekvivalence i uspořádáním. (Je to současně jediná taková relace.)

4.1 Relace ekvivalence a rozklady

Rozkladem množiny A se nazývá systém podmnožin $\mathcal{R} \subseteq \mathcal{P}(A)$ splňující:

(1) $\bigcup \mathcal{R} = A$ (systém pokrývá množinu),

(2) $(\forall B, C \in \mathcal{R})(B \neq C \rightarrow B \cap C = \emptyset)$ (množiny jsou po dvou disjunktní).

Prvky rozkladu se nazývají *třídy rozkladu*. Z definice je zřejmé, že každý prvek množiny A patří do právě jedné třídy rozkladu, pro prvek x ji značíme $[x]$. Prvek x se také nazývá *reprezentantem* třídy $[x]$. Zobrazení $p : A \to \mathcal{R}$ přiřazující každému prvku třídu, ve které leží, $p(x) = [x]$ se nazývá *projekce* (neplést s projekcemi kartézského součinu).

Věta 9. *Nechť $\mathcal{R}$ je rozklad množiny A. Pak předpis $x \rho_{\mathcal{R}} y \Leftrightarrow [x] = [y]$ definuje relaci ekvivalence na A.*

Naopak, je-li ρ relace ekvivalence na A, pak systém $\mathcal{R}_\rho = \{\{y \mid y \rho x\} \mid x \in A\}$ je rozklad množiny A.

Přiřazení $\mathcal{R} \mapsto \rho_{\mathcal{R}}, \rho \mapsto \mathcal{R}_\rho$ určují bijektivní korespondenci mezi množinou všech rozkladů a množinou všech relací ekvivalence na množině A.

Důkaz. Reflexivita, symetrie a tranzitivita relace $\rho_{\mathcal{R}}$ snadno vyplývá z definice relace a vlastností rovnosti.

Relace ekvivalence je reflexivní, proto $x \in \{y \mid y \rho x\}$ pro každé $x \in A$, a tedy systém $\mathcal{R}_\rho$ pokrývá A. Zvolme $x, y \in A, B = \{z \mid z \rho x\}, C = \{z \mid z \rho y$ a předpokládejme, že $w \in B \cap C$. Tedy $w \rho x$ a ze symetrie také $x \rho w$. Pro $z \in A$ platí $z \rho x$ a z tranzitivity dostáváme $z \rho w$. Naopak, pokud $z \rho w$, pak z tranzitivity dostaneme $z \rho x$, čili $z \in B$. Celkem máme $z \in B \Leftrightarrow z \rho w$ a podobně odvodíme, že $z \in C \Leftrightarrow z \rho w$. Odtud $B = C$, tedy prvky systému $\mathcal{R}$ jsou po dvou disjunktní.

Potřebujeme ukázat, že složení $\mathcal{R} \mapsto \rho_{\mathcal{R}} \mapsto \mathcal{R}_{\rho_{\mathcal{R}}}$ vrací původní rozklad a $\rho \mapsto \mathcal{R}_\rho \mapsto \rho_{\mathcal{R}_\rho}$ původní relaci ekvivalence. Platí $T \in \mathcal{R} \Leftrightarrow T = \{y \mid [x] = [y]\} \Leftrightarrow T = \{y \mid x \rho_{\mathcal{R}} y\} \Leftrightarrow T \in \mathcal{R}_{\rho_{\mathcal{R}}}$ a s využitím úvah z předešlého odstavce také $x \rho y \Leftrightarrow \{z \mid z \rho x\} = \{z \mid z \rho y\} \Leftrightarrow [x]_{\mathcal{R}_\rho} = [y]_{\mathcal{R}_\rho} \Leftrightarrow x \rho_{\mathcal{R}_\rho} y$. □

Rozklad příslušný relaci ekvivalence ρ na množině A značíme A/ρ a někdy nazýváme *faktorizací množiny* A nebo *faktormnožinou*.

Jádro zobrazení $f : A \to B$ je relace ekvivalence J_f na množině A daná podmínkou $x\ J_f\ y \Leftrightarrow f(x) = f(y)$.

Věta 10. *Každá relace ekvivalence je jádrem své projekce.*

Důkaz. Plyne přímo z definice. □

4.2 Uspořádané množiny

Uspořádanou množinou rozumíme množinu s pevně zvoleným uspořádáním.

Nechť $(A, \leq)$ je uspořádaná množina. Pokud $x \leq y$ nebo $y \leq x$, říkáme, že x, y jsou *porovnatelné (srovnatelné)*, v opačném případě jsou *neporovnatelné (nesrovnatelné)*. $(A, \leq)$ se nazývá *lineárně uspořádaná (řetězec)*, pokud jsou každé dva prvky srovnatelné. $(A, \leq)$ se nazývá *protiřetězec*, pokud jsou každé dva prvky nesrovnatelné.

Říkáme, že prvek x *pokrývá* y nebo že y *je následníkem* x pokud $y \leq x, y \neq x$ a $(\forall z)(y \leq z \leq x \ \rightarrow \ (z = y \ \vee \ z = x))$. *Hasseovský diagram* je znázornění uspořádané množiny, kde pro každou dvojici prvků $x \leq y$ je x nakreslen níž než y a dva prvky jsou spojeny čarou, pokud jeden pokrývá druhý. Jiné prvky nesmí být spojeny (zejména neporovnatelné)! Chápeme-li následníka jako relaci na A, lze původní uspořádání $\leq$ snadno zrekonstruovat jako její reflexivní a tranzitivní obal. Hasseovský diagram tedy jednoznačně (a velmi úsporně) určuje uspořádání.

Věta 11. *Je-li* $\leq$ *relace uspořádání na množině* A*, pak* $\leq^{-1}$ *je také relace uspořádání.*

Důkaz. Přímočarý. □

Důsledkem věty je tzv. *princip duality*. Funguje tak, že každé tvrzení týkající se např. největšího prvku lze přeformulovat na analogické týkající se nejmenšího prvku (protože v duálním uspořádání se stane prvkem největším a lze na něj aplikovat původní tvrzení). Hasseovský diagram duálního uspořádání vznikne otočením původního „hlavou dolů“.

Prvek x se nazývá

největší — pokud $(\forall y)(y \leq x)$,

nejmenší — pokud $(\forall y)(x \leq y)$,

maximální — pokud $(\forall y)(x \leq y \ \rightarrow \ x = y)$,

minimální — pokud $(\forall y)(y \leq x \ \rightarrow \ x = y)$.

Věta 12. *Největší prvek je maximální a to jediný.*

Důkaz. Nechť x je největší a předpokládejme $x \leq y$. Protože x je největší, platí $y \leq x$. Z antisymetrie dostáváme $x = y$, tedy x je maximální. Předpokládejme, že x' je také maximální. Pak $x' \leq x$, protože x je největší. Potom ovšem $x' = x$, protože x' je maximální. □

Z principu duality dostáváme, že nejmenší prvek je jediný minimální. Z věty současně vyplývá, že uspořádaná množina může mít nejvýše jeden největší a nejvýše jeden nejmenší prvek. Maximálních a minimálních prvků může být víc, např. v protiřetězci to jsou všechny prvky. Není pravda, že jediný maximální prvek musí být největší.

Prvek x se nazývá *horní závorou* podmnožiny $B \subseteq A$, pokud $(\forall y \in B)(y \leq x)$. x se nazývá *dolní závorou* B, pokud $(\forall y \in B)(x \leq y)$. Množinu horních (resp. dolních) závor množiny B označme $HZ(B)$ $(DZ(B))$. Nejmenší prvek množiny $HZ(B)$ nazýváme *supremum* množiny B, největší prvek množiny $DZ(B)$ nazýváme *infimum* množiny B.

Horní závorou celé množiny A může být jen její největší prvek. Horní závorou prázdné množiny je libovolný prvek množiny A, supremem prázdné množiny je tedy nejmenší prvek. Supremum (nějaké množiny) nemusí existovat ani v případě, že množina horních závor je neprázdná.

Uspořádaná množina se nazývá *úplný svaz*, pokud každá její podmnožina má supremum i infimum (také říkáme, že má všechna suprema a infima).

Věta 13. *Má-li uspořádaná množina $(A, \leq)$ všechna suprema, má i všechna infima.*

Důkaz. Nechť $B \subseteq A$ je libovolná. Protože A má největší prvek, bude (přinejmenším) tento prvek dolní závorou B, tedy množina $C = DZ(B)$ je neprázdná. Nechť x je supremum C. Každý prvek $y \in B$ je současně horní závorou C, proto $x \leq y$ (jakožto supremum je x nejmenší horní závorou C). Odtud dostáváme, že x je také dolní závorou B. Protože je největší, jedná se o infimum množiny B. □

Příklad 8. 1) $(\mathbb{N}, \leq)$ není úplný svaz, protože nemá největší prvek. Mohlo by se zdát, že má všechna infima (a tudíž i všechna suprema), ale ta mají jen neprázdné podmnožiny. (Největší prvek jakožto $\inf \emptyset$ neexistuje.) Suprema existují právě pro konečné podmnožiny.

2) $(\mathcal{P}(A), \subseteq)$ je úplný svaz pro libovolnou množinu A. Suprema jsou sjednocení systémů množin, infima průniky (s výjimkou infima prázdné množiny).

3) Reálný uzavřený interval $[0; 1]$ je úplný svaz.

4) Racionální uzavřený interval $[0; 1] \cap \mathbb{Q}$ není úplný svaz. Má sice největší i nejmenší prvek, ale např. množina $[0; \frac{\sqrt{2}}{2}) \cap \mathbb{Q}$ nemá supremum (v $\mathbb{R}$ by to bylo $\frac{\sqrt{2}}{2}$, které ovšem není racionální).

Nechť $(A, \leq), (B, \preceq)$ jsou uspořádané množiny. Zobrazení $f : A \to B$ se nazývá *izotonní*, pokud $(\forall x, y \in A)(x \leq y \ \to \ f(x) \preceq f(y))$. f se nazývá *izomorfismus*, pokud je bijektivní a platí $(\forall x, y \in A)(x \leq y \ \leftrightarrow \ f(x) \preceq f(y))$. (Ekvivalentně lze izomorfismus definovat jako bijektivní izotonní zobrazení, k němuž je zobrazení inverzní také izotonní). Trochu zjednodušeně se dá říct, že izomorfní uspořádané množiny mají stejný hasseovský diagram.

Příklad 9. (1) Konstantní zobrazení $f(x) = k$ pro pevně zvolené $k \in B$ je vždy izotonní.

(2) Posunutí $f : (\mathbb{N}, \leq) \to (\mathbb{N}, \leq), f(n) = n + 1$ je izotonní a splňuje podmínku dokonce jako ekvivalenci. Není ovšem izomorfismem, protože není bijektivní.

(3) Nechť $(\{a, b\}, =)$ je dvouprvkový protiřetězec a $(\{1, 2\}, \leq)$ dvouprvkový řetězec. Zobrazení $a \mapsto 1, b \mapsto 2$ je izotonní, jeho inverze izotonní není.

5 Kombinatorika

5.1 Permutace

Permutace udávají počet pořadí prvků n-prvkové množiny, neboli počet bijekcí na sebe (těm se také říká permutace). Pro první prvek můžeme vybrat z n možných obrazů, pro druhý už jen $n - 1$, atd., na poslední n-tý prvek zbyde jediný použitelný obraz. Celkový počet je tedy $n!$.

5.2 Variace

Variace udávají počet uspořádaných výběrů (tj. posloupností) k neopakujících se prvků z n-prvkové množiny, neboli počet injektivních zobrazení k-prvkové množiny do n- prvkové. Odvozují se podobně jako permutace, ale posledním prvkem je k-tý, kterému odpovídá $n - k + 1$ možných obrazů. Výsledný součin $n(n-1)\dots(n-k+1)$ lze formálně rozšířit zlomkem $\frac{(n-k)!}{(n-k)!}$ a upravit na tvar $\frac{n!}{(n-k)!}$.

5.3 Kombinace

Kombinace udávají počet neuspořádaných výběrů k prvků z n-prvkové množiny, neboli počet k-prvkových podmnožin. Uvážíme-li všechny uspořádané výběry odpovídající jisté k-prvkové podmnožině, bude jich vždy tolik, kolik je všech permutací těchto k prvků, tedy $k!$. Tento počet je stejný pro všechny k-prvkové podmnožiny, můžeme tedy celkový počet uspořádaných

výběrů (variace) vydělit $k!$ a dostaneme výsledek $\frac{n!}{k!(n-k)!}$. Toto číslo se nazývá *kombinační* a značí $\binom{n}{k}$.

Věta 14. *Nechť $n, k \in \mathbb{N}_0, k \leq n$. Pak platí*
(1) $\binom{n}{0} = 1, \binom{n}{1} = n$,
(2) $\binom{n}{k} = \binom{n}{n-k}$,
(3) $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

Důkaz. (1) Zřejmé.

(2) Mezi podmnožinami dané množiny a jejími doplňky existuje zřejmá bijekce. Počet k-prvkových podmnožin tedy bude stejný jako počet jejich $(n-k)$-prvkových doplňků. Rovnost také vyplývá ze symetrie výrazu $\frac{n!}{k!(n-k)!}$ vzhledem ke k a $n-k$.

(3) Máme-li z $n+1$-prvkové množiny A vybrat $k+1$ prvků, lze to provést rovněž tak, že v ní zvolíme jeden význačný prvek x. $k+1$-prvkové podmnožiny pak můžeme rozlišit podle toho, zda x obsahují nebo ne. Ty, které ho neobsahují, vznikly jako podmnožiny n-prvkového zbytku $A - \{x\}$ a je jich tedy $\binom{n}{k+1}$. Do podmnožin, které x obsahují, se vybíralo z $A - \{x\}$ zbylých k prvků, je jich tedy $\binom{n}{k}$. Vlastnost náležení prvku x zřejmě zaručuje, že vzniklé systémy podmnožin jsou disjunktní a celkový počet podmnožin tedy získáme jako součet počtů jejich prvků. Důkaz lze rovněž provést algebraickou úpravou výrazů dosazených za kombinační čísla. □

Věta 15. *(binomická) Nechť $x, y \in \mathbb{R} - 0, n \in \mathbb{N}$. Pak platí*

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

Důkaz. Důkaz lze provést např. indukcí vzhledem k n s využitím vztahů z předchozí věty. Jednodušší je však přímá kombinatorická úvaha. Výraz $(x+y)^n$ odpovídá součinu n závorek $(x+y)$. Jejich roznásobením dostaneme výrazy tvaru $x^i y^{n-i}$, protože z každé závorky vyberem buďto x nebo y a součet exponentů tedy musí být n. Pro dané i bude výrazů celkem $\binom{n}{i}$, protože právě toto číslo odpovídá počtu (neuspořádaných) výběrů těch závorek, ze kterých se použije x (z ostatních se použije y). □

5.4 Permutace s opakováním

Uvažujme n-prvkovou množinu a na ní relaci ekvivalence. Ekvivalenci interpretujeme jako nerozlišitelnost prvků (např. stejné obarvení). Permutace s opakováním udávají počet pořadí prvků dané množiny, přičemž pořadí lišící se pouze ekvivalentními prvky považujeme za stejná. (Přesněji bychom takto

zavedli ekvivalenci pořadí a pak by jednalo by se o počet tříd příslušného rozkladu množiny všech pořadí.) Každé pořadí n prvků zřejmě určuje pořadí prvků v každé třídě, vzájemně ekvivalentních (tj. zaměnitelných) pořadí tedy bude v každé třídě $n_1!n_2!\ldots n_k!$, kde n_i jsou počty prvků v jednotlivých třídách (platí tedy $n_1 + \cdots + n_k = n$). Tímto číslem vydělíme celkový počet pořadí a dostaneme výsledek

$$\frac{n!}{n_1!n_2!\ldots n_k!}.$$

Permutace (bez opakování) jsou vlastně zvláštním případem permutací s opakováním, kde relací ekvivalence je identita.

5.5 Variace s opakováním

Variace s opakováním odpovídají uspořádaným výběrům k prvků z n-prvkové množiny, kde každý prvek může být vybírán opakovaně. Situace přesně odpovídá počtu zobrazení k-prvkové do n-prvkové (pro každý z k prvků vybíráme jeho obraz). Protože pro každou pozici (prvek) máme na výběr n možností (nezávisle na ostatních), bude celkový počet n^k.

Pozor, variace s opakováním nepředstavují zobecnění variací bez opakování ani permutací s opakováním.

5.6 Kombinace s opakováním

Kombinace s opakováním udávají počet rozdělení n nerozlišitelných prvků do k (rozlišitelných) přihrádek. Úloha se řeší tak, že k přihrádek znázorníme jako řadu rozdělenou $k-1$ oddělovači, mezi které vkládáme n prvků. Dostaneme tak řadu $n+k-1$ „prvkooddělovačů“ a výsledek určíme jako permutace s opakováním, kde rozklad sestává ze dvou tříd — třídy prvků a třídy oddělovačů. Rovněž můžeme uvažovat tak, že z $n+k-1$-prvkové řady určíme n prvků (nebo $k-1$ oddělovačů), což provedeme jako neuspořádaný výběr, tj. kombinace. V každém případě dojdeme k výsledku $\binom{n+k-1}{n}$.

5.7 Princip inkluze a exkluze

Principu se užívá v úlohách, kde prvky mohou mít nějaké vlastnosti $A_1, \ldots, A_n$ a potřebujeme určit počet prvků které buďto mají alespoň jednu z těchto vlastností nebo naopak žádnou. Relaci „mít vlastnost A_i“ můžeme interpretovat také jako příslušnost prvku do množiny A_i a jedná se pak o určení počtu prvků sjednocení $\bigcup_{i=1}^{n}$, resp. jeho doplňku. Nutným předpokladem k vyřešení

úlohy je znalost počtu prvků libovolných průniků množin A_i včetně množin samotných (a případně celé nosné množiny, ve které se úloha odehrává).

Princip inkluze a exkluze funguje na principu zpřesňování odhadu. Počet prvků sjednocení nejprve odhadneme jako součet počtu prvků jednotlivých množin. Prvky, které se nachází v průniku dvou množin, byly však započítány dvakrát, a proto je následně odečteme jako počty prvků průniků dvouprvkových podsystémů. Tento odhad ovšem nebude fungovat pro prvky nacházející se v průniku tří množin — ty byly započítány třikrát v prvním odhadu a odečteny třikrát ve druhém, musíme je tedy zase přičíst. Takto se postupně dopracujeme až k průniku celého systému podmnožin, kde teprve dostaneme přesný výsledek.

Věta 16. *Nechť M je konečná množina a $\{A_i\}_{i\in I}$ systém jejích navzájem různých podmnožin. Pak platí*

$$\left| M - \bigcup_{i\in I} A_i \right| = \sum_{J\subseteq I} (-1)^{|J|} \left| \bigcap_{j\in J} A_j \right|$$

(pro $J = \emptyset$ klademe $\bigcap \emptyset = M$).

Důkaz. Uvažujme libovolný prvek $x \in \bigcup_{i\in I} A_i$. Nechť $K \subseteq I$ je množina těch indexů i, že $x \in A_i$. Víme, že $K \neq \emptyset$ a x se objeví v $\bigcap_{j\in J} A_j$ právě tehdy, když $J \subseteq K$. Množina K má přitom $\binom{|K|}{j}$ j-prvkových podmnožin, celkový příspěvěk prvku x do součtu na pravé straně tedy bude $\sum_{j=0}^{|K|} (-1)^j \binom{|K|}{j}$, což je podle binomické věty rovno $(1-1)^{|K|} = 0$.

Naproti tomu prvek $x \in M - \bigcup_{i\in I} A_i$ se na pravé straně objeví pouze ve výrazu $M = \bigcap \emptyset$, který má kladné znaménko a do součtu tedy x přispěje hodnotou 1. □

Pro počet prvků sjednocení pak odečtením dostáváme formuli

$$\left| \bigcup_{i\in I} A_i \right| = \sum_{\emptyset\neq J\subseteq I} (-1)^{|J|+1} \left| \bigcap_{j\in J} A_j \right|.$$

Příklad 10. (1) Pro tříprvkový systém A_1, A_2, A_3 vypadá princip inkluze a exkluze po rozepsání následovně: $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.

(2) (úloha o šatnářce) Zapomětlivá šatnářka vydá n pánům zcela nahodile n kloboukú. Určete pravděpodobnost situace, že žádný pán nedostane svůj klobouk.

Řešení: Celkový počet vydání kloboukú je $n!$. Situace, že některý pán dostane svůj klobouk odhadneme číslem $\binom{n}{1}(n-1)!$, kde $\binom{n}{1}$ je počet výběrů

příslušného pána a $(n-1)!$ je počet rozdělení zbylých klobouků. Dále odhadneme číslem $\binom{n}{2}(n-2)!$ počet situací, kdy dva pánové dostanou své klobouky, atd. Celkem dostaneme řadu

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^n = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)!$$

a pravděpodobnost určíme jako podíl k celkovému počtu vydání $n!$. Pro $n \to \infty$ pravděpodobnost konverguje k číslu $\frac{1}{e}$.

(3) Určete počet surjektivních zobrazení k-prvkové množiny na n-prvkovou.

Řešení: Počet všech zobrazení je n^k. Budeme postupně odhadovat počty zobrazení, kde jeden, dva, atd. z n prvků oboru hodnot nejsou využity, tj. nezabrazuje se na ně žádný prvek z definičního oboru. Užitím principu inkluze a exkluze dojdeme k řadě

$$n^k - \binom{n}{1}(n-1)^k + \binom{n}{2}(n-2)^k - \cdots + (-1)^{(n-1)}\binom{n}{n-1}1^k = \sum_{i=0}^{n-1}(-1)^i\binom{n}{i}(n-i)^k.$$

6 Grafy

6.1 Základní pojmy

(Obyčejným neorientovaným) grafem rozumíme dvojici $G = (V, E)$, kde V je konečná množina *vrcholů*, E množina *hran* a platí $E \subseteq \binom{V}{2}$, tj. E je podmnožina množiny všech dvojprvkových podmnožin množiny V. O hraně $e = \{u, v\}$ říkáme, že spojuje vrcholy u, v. Existuje-li pro vrcholy u, v spojující hrana, tj. $\{u, v\} \in E$, říkáme také, že vrcholy spolu sousedí.

Orientovaným grafem rozumíme dvojici $G = (V, E)$, kde E je relace na V. Hranami jsou tedy uspořádané dvojice vrcholů, navíc mohou existovat smyčky na stejném vrcholu. Obyčejný graf lze chápat jako orientovaný, kde relace definující hrany je symetrická a ireflexivní (tj. $(\forall x)(x, x) \notin E$).

Lze definovat orientované grafy bez smyček nebo obyčejné se smyčkami, ale to nebudeme potřebovat. Rovněž se lze setkat s pojmem *multigrafu*, kde mezi dvěma vrcholy může existovat více hran (případně více stejně orientovaných hran u orientovaných grafů).

Grafy lze reprezentovat graficky, tj. každému vrcholu je (injektivně) přiřazen bod v rovině a každé hraně křivka s příslušnými koncovými body. Přitom křivka nesmí procházet žádným dalším vrcholem. Jelikož orientovaný (a potažmo i neorientovaný) graf je definován jako relace, lze ho reprezentovat

jako binární čtvercovou matici $E = (e_{uv})$, kde

$$e_{uv} = \begin{cases} 1, & (u,v) \in E, \\ 0, & (u,v) \notin E. \end{cases}$$

Další možností je reprezentace grafu seznamem sousedů, kde každému vrcholu je přiřazena posloupnost všech jeho sousedů. Každý z uvedených způsobů reprezentace lze zobecnit i na multigrafy (rozmyslete si).

Uvažujme nyní obyčejný graf $G = (V, E)$. *Sledem* se nazývá posloupnost vrcholů $(v_1, v_2, \ldots, v_n)$ taková, že $(\forall 1 \leq i \leq n-1)\{v_i, v_i + 1\} \in E$ (tj. dva následující vrcholy sledu jsou sousední). *Cestou* se rozumí sled, v němž se žádný vrchol neopakuje. *Uzavřeným sledem* rozumíme sled, v němž $v_1 = v_n$. *Kružnicí* se nazývá uzavřený sled, kde se neopakuje žádná hrana ani žádný vrchol s výjimkou prvního a posledního. Kružnice lišící se pouze počátečním vrcholem sledu se obvykle nerozlišují. U orientovaného grafu má smysl u definice sledu a cesty zohlednit orientaci hran. *Délkou* sledu/cesty/kružnice se nazývá počet zúčastněných hran.

Podgraf grafu $G = (V, E)$ je dvojice množin $G' = (V', E')$ splňující $V' \subseteq V$ a $E' \subseteq E \cap \binom{V'}{2}$. Pokud $E' = E \cap \binom{V'}{2}$, nazývá se podgraf *úplný*. (V definici podgrafu orientovaného grafu $\binom{V'}{2}$ nahradíme $V' \times V'$.) Je-li G' podgrafem G, říkáme také, že G obsahuje G'.

Graf se nazývá *souvislý*, pokud mezi libovolnými dvěma vrcholy existuje cesta. (Mohli bychom místo cest uvažovat pouze sledy, ovšem z každého sledu lze vypustit každý uzavřený sled mezi dvěma výskyty téhož prvku, čímž nakonec dostaneme cestu.) Každý maximální úplný souvislý podgraf se nazývá *komponentou* grafu.

Počet sousedů vrcholu v nazýváme *stupněm* a značíme $\mathrm{st}(v)$. Kružnici můžeme alternativně definovat jako souvislý podgraf, v němž má každý vrchol stupeň 2.

Graf neobsahující kružnici se nazývá *les*. Souvislý les se nazývá *strom*. Maximální podgraf souvislého grafu, který je stromem, nazýváme *kostra*.

Věta 17. *(1) Počet hran stromu je o 1 menší než počet jeho vrcholů. Naopak každý souvislý graf s touto vlastností je strom.*

(2) Každá kostra obsahuje všechny vrcholy.

Důkaz. (1) Dokážeme indukcí. Pro $|V| = 1$ je $|E| = 0$ a tvrzení platí.

Stačí dokázat, že strom s alespoň dvěma vrcholy obsahuje aspoň jeden vrchol stupně jedna. Žádná z cest spojující jiné dva vrcholy ho neobsahuje, proto jeho odstraněním spolu s příslušnou hranou dosteneme podle indukčního předpokladu souvislý podgraf vyhovující podmínce a tedy strom. Předpokládejme sporem, že stupeň každého vrcholu je alespoň 2. To umožňuje se-

strojit sled libovolné délky, ve kterém jsou dvě následující hrany různé. S ohledem na konečnost grafu se časem musí některý vrchol zopakovat. Uvážíme-li posloupnost mezi některými nejbližšími výskyty vrcholu, dostaneme kružnici, což je spor.

Přidáváme-li naopak ke stromu nový vrchol a novou hranu, aby vzniklý graf byl souvislý, lze to provést pouze tak, že nová hrana připojí nový vrchol k některému původnímu vrcholu. Pak bude mít nový vrchol stupeň 1 a nevznikne tak kružnice.

(2) Předpokládejme, že kostra neobsahuje vrchol v. Protože graf je souvislý, existuje cesta $(v, v_1, v_2, \ldots, v_n)$ do některého vrcholu kostry. Zvolme i nejmenší takové, že v_i je už kosterní vrchol. Přidáním hran $\{v, v_1\}, \{v_1, v_2\}, \ldots, \{v_{i-1}, v_i\}$ ke kostře dostaneme souvislý graf bez kružnic (žádný z vrcholů $(v, v_1, v_2, \ldots, v_{i-1})$ v kostře není a jedná se o cestu), což je spor s maximalitou kostry. □

Ohodnocením grafu (také vahou) se nazývá zobrazení $w : E \to \mathbb{R}$. Ohodnocení lze rozšířit na cesty, kružnice, kostry atd., když položíme $w(K) = \sum_{e \in K} w(e)$. Mezi důležité problémy teorie grafů patří nalezení minimální cesty a nalezení minimální kostry. (Minimalita je nyní míněna vzhledem k ohodnocení.)

6.2 Minimální cesta

Problém minimální cesty lze řešit u orientovaného i neorientovaného grafu. Většina algoritmů používá pomocné ohodnocení vrcholů $\delta : V \to \mathbb{R}$, které představuje nejlepší průběžnou hodnotu cesty do daného vrcholu. Úprava ohodnocení se provadí prostřednictvím tzv. *relaxace hran*, kdy původní hodnotu $\delta(v)$ nahrazujeme součtem $\delta(u) + w(u, v)$, pokud je menší. Znamená to, že jsme nalezli výhodnější cestu do vrcholu v přes hranu (u, v).

Je-li ohodnocení grafu nezáporné, můžeme minimální cestu z vrcholu u do vrcholu v najít pomocí Dijkstrova algoritmu. V něm se na začátku nastaví $\delta(u) := 0$, $\delta(x) := \infty$ pro $x \neq u$ a $A := V$ (inicializace). V každém kroku algortimu se z množiny A se vybere vrchol x s nejmenším $\delta(x)$ a provedou se relaxace hran do sousedních vrcholů. (Je-li takových vrcholů víc, lze zvolit libovolný.) Následně se x vyřadí z množiny A a průchod cyklem se opakuje. Hodnota $\delta(x)$ vybraného vrcholu je už výslednou hodnotou minimální cesty z u do x. Není nutné relaxovat hrany vedoucí do již vyřazených vrcholů, protože jejich δ není větší (byly vybrány dříve) a s ohledem na nezápornost ohodnocení by relaxace nic nepřinesla. Algoritmus končí návštěvou posledního vrcholu, po níž je $A = \emptyset$.

Předpoklad nezápornosti ohodnocení je důležitý, jinak může dojít k situaci, že vrchol je vyhodnocen a vyřazen dřív, než se relaxuje některá záporně

ohodnocená hrana ležící na minimální cestě.

Dijkstrův algoritmus jako vedlejší produkt počítá i minimální cesty do všech ostatních vrcholů. Hrana použitelná do minimální cesty splňuje rovnost $\delta(x) + w(x, y) = \delta(y)$ (i u neorientovaného grafu je pak důležité, kterým směrem je rovnost splněna!).

6.3 Minimální kostra

Pro hledání minimální kostry si uvedeme tři algoritmy: Kruskalův (hladový), Jarníkův (Primův) a Borůvkův. Problém budeme řešit pro neorientovaný graf.

Kruskalův algorimus začíná s množinou hran $F := E$ a průběžnou kostrou $K := \emptyset$. V každém průchodu vybere z F hranu e s nejmenším ohodnocením. Pokud $K \cup \{e\}$ neobsahuje kružnici, přidá hranu e do kostry: $K := K \cup \{e\}$. V každém případě se e odebere z F a cyklus se opakuje pro další hranu.

Zatímco v Kruskalově algoritmu vytváření kostry vypadá nahodile, u Jarníkova algoritmu se postupně buduje od pevně zvoleného výchozího vrcholu v. Algoritmus pracuje s množinou již připojených vrcholů A, na začátku je $A := \{v\}$, $K := \emptyset$. V každém průchodu algoritmus vybírá minimální hranu mezi A a $V - A$ a přidává ji do K. Připojený vrchol z $V - A$ se přidá do A a cyklus se opakuje. Protože se do K přidávají hrany připojující nové vrcholy, nemůže vzniknout kružnice. Algortimus končí navštívením posledního vrcholu, tj. $A = V$.

Borůvkův algoritmus předpokládá injektivní ohodnocení hran. (Při stejném ohodnocení některých hran bychom mohli upravit zadání přičtením drobných hodnot.) Pracuje se s relací ekvivalence ρ na množině vrcholů. Na začátku je $\rho := id_V, K := \emptyset$. V každém průchodu algoritmu se pro každou třídu rozkladu vybere minimální hrana spojující ji s jinou třídou. Všechny takové hrany přidáme do K a přepočítáme ρ jako nejmenší relaci ekvivalence obsahující K (slévání bublinek). Na konci algoritmu je $\rho = V \times V$ a K je minimální kostra.

6.4 Další grafové problémy

Graf se nazývá *rovinný*, pokud ho lze reprezentovat v rovině tak, že se žádné dvě hrany nekříží.

Příklad 11. (1) Síť mnohostěnu je rovinný graf. (Roztáhneme libovolnou stěnu a síť promítneme dovnitř.)

(2) Úplný graf o pěti vrcholech K_5 ani úplný bipartitní graf pro dvě tříprvkové množiny $K_{3,3}$ (úloha o třech studních) nejsou rovinné grafy.

Dělením grafu nazýváme graf, který vznikne opakovaným vkládáním vrcholů do hran (stará hrana se nahrazuje dvěma novými a vrcholem).

Věta 18. *(Kuratowského) Graf je rovinný právě tehdy, když neobsahuje podgraf izomorfní dělení grafu K_5 nebo $K_{3,3}$.*

Obarvením grafu se nazývá zobrazení $c : V \to C$, kde C je množina „barev", splňující $\{u, v\} \in E \to c(u) \neq c(v)$ (sousední vrcholy mají různé obarvení). Minimální počet barev $|C|$ se nazývá *barevnost grafu*.

Příklad 12. (1) Úplný graf s n vrcholy K_n má barevnost n.

(2) Každý rovinný graf má barevnost nejvýše 4 (dlouho otevřený problém, dokázáno užitím počítače).

(Uzavřeným) eulerovským tahem se nazývá uzavřený sled, který prochází každou hranou právě jednou. Graf se nazývá *eulerovský*, pokud v něm existuje eulerovský tah.

Věta 19. *Graf je eulerovský právě tehdy, když je souvislý a stupeň každého vrcholu je sudý.*

Důkaz. Pokud je graf souvislý a stupně jsou sudé, musí být každý stupeň alespoň 2. Graf je konečný, lze tedy sestrojit uzavřený sled, v němž se žádná hrana neopakuje (tzv. *tah*). Uvědomme si, že se vrcholy se mohou v tahu objevit opakovaně, ale vždy u každého se využije sudý počet hran. Pokud tah není maximální, znamená to, že z některého jeho vrcholu vede zatím nepoužitá hrana. Z této hrany lze opět sestrojit uzavřený tah s jinými hranami, než má původní tah. (I když dojde k překřížení, sudost stupňů umožňuje odchod po nepoužité hraně.) Nový tah navážeme na starý (princip přilepování uší). Postupným opakováním najdeme maximální tedy eulerovský tah.

Opačná implikace je jednoduchá. Souvislost je zřejmá, sudost vyplývá z faktu, že tah do každého vrcholu jednou hranou vstupuje a druhou jej opouští.

Hamiltonovskou kružnicí se nazývá kružnice procházející všemi vrcholy. Graf se nazývá *hamiltonovský*, pokud v něm existuje hamiltonovská kružnice.