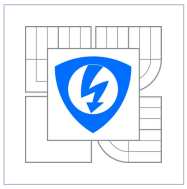


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV MATEMATIKY

Diskrétní matematika

(Informační technologie)

Martin Kovár

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Ústav matematiky FEKT VUT v Brně, 2014

http://www.umat.feec.vutbr.cz

Tento text byl vytvořen v rámci realizace projektu CZ.1.07/2.2.00/15.0156,

Inovace výuky matematických předmětů v rámci studijních programů FEKT a FIT VUT v Brně.

Součástí tohoto učebního textu jsou odkazy na tzv. webMathematica applety, tj. programy vytvořené v prostředí webMathematica. Tyto odkazy jsou v textu zvýrazněny barvou, příp. uvozeny slovy *matematický software*, *webMathematica applet* apod. Applety ke svému běhu nevyžadují software Mathematica – je však nutné mít na klientském počítači nainstalováno prostředí Java a nastavenou vhodnou úroveň zabezpečení prohlížeče i prostředí Java. Po kliknutí na odkaz appletu se v závislosti na softwarovém prostředí klientského počítače mohou zobrazit různá hlášení o zabezpečení – všechny dialogy je třeba povolit a spouštění požadovaných prvků neblokovat.

Doplňující součástí tohoto učebního textu jsou příklady zpracované v elektronické bance příkladů.

Obsah

Úvod

Úvod

Cílem tohoto textu je sloužit jako přednáškový studijní materiál k předmětu Diskrétní matematika pro 1. ročník na Fakultě informačních technologií VUT v Brně. Obsah předmětu je dán specifickými požadavky studia a proto v sobě zahrnuje základní poznatky řady matematických disciplín, které bývají tradičně přednášeny odděleně a pochopitelně také – jako například v matematicky zaměřeném studiu univerzitního typu – do podstatně větší hloubky. V rozsahu, který v celém studiu na Fakultě informačních technologií tento předmět zaujímá, není takto podrobný výklad možný. Proto například důkazy obtížnějších vět a tvrzení byly vynechány, student je v případě hlubšího zájmu odkázán na doporučenou specializovanou literaturu. Uváděna je většina důkazů vět střední obtížnosti. Jejich studium je velmi důležité k pochopení přednášené látky i k pěstování schopnosti matematického myšlení a vyjadřování. Stejně tak nebylo upuštěno od tradiční formy výkladu „definice-věta-důkaz", která přes všechny kritiky nematematiků, jíž se jí v poslední době dostává, zůstává nejpřehlednější a v podstatě jedinou možnou formou matematického výkladu. Autor je přesvědčen, že nelze podat smysluplný výklad čehokoliv, tím méně matematiky, aniž by byly definované pojmy zřetelně odděleny od tvrzení, která se těchto pojmů týkají. Dále je vhodné si uvědomit, že obecné znění matematické věty ji právě činí smysluplnou a umožňuje ji použít v řadě konkrétních příkladů a případů. Každá matematická věta má ovšem své předpoklady, které jsou neméně důležité, jako samotné tvrzení. Bez splnění těchto předpokladů si nemůžeme být jisti, zda obecné pravidlo, které věta vyjadřuje, můžeme použít. Tradiční linie výkladu „definice-věta-důkaz" je ovšem doplněna mnohými příklady, aby byl usnadněn přechod od teoretického pochopení výkladu k schopnosti získané vědomosti a dovednosti aplikovat. Přes omezený rozsah předmětu se autor pokusil začlenit do textu alespoň základní partie teorie množin, topologie, algebry, logiky a teorie grafů tak, aby měl student k dispozici potřebné matematické zázemí k pochopení celé řady souvislostí, se kterými se během svého studia v prvním ročníku i

v dalších letech setkává. Některé partie slouží rovněž jako průprava pro další navazující matematické předměty. Zejména část týkající se zobrazení, základů topologie a spojitosti, slouží také jako úvod pro navazující předmět Matematická analýza. Průřez základními matematickými strukturami, na něž je kladen v tomto textu zejména důraz, představuje rovněž jisté minimum pro úspěšné zvládnutí základů moderní a rychle se rozvíjející počítačové vědy – hlavního důvodu, proč student na relativně mladou Fakultu informačních technologií přichází.

Pro některé typy úloh je vhodné využívat matematický software, umožňující podstatně zkrátit některé rutinní postupy a soustředit se na podstatné stránky probírané látky. Ačkoliv není striktně předepsána konkrétní verze vhodného systému počítačové algebry, jako nejvhodnější se jeví program Wolfram Mathematica, který poskytuje nejširší možnosti a v němž jsou napsány všechny podpůrné a demonstrační aplikace. Vyhoví Mathematica verze 7.0 a vyšší. V některých případech jsou pro diskrétní matematiku použitelné i konkurenční systémy počítačové algebry Maple nebo Matlab. Všechny tyto vysoce komerční programy jsou vhodné k využití studenty především během řízené výuky v učebnách.

V závěru každé kapitoly jsou umístěny odkazy na jednoúčelové internetové aplikace, napsané v prostředí webMathematica pro účely samostudia především v domácím prostředí, v němž drahé komerční programy nejsou studentům dostupné. Syntaxe zadávání dat je v tomto případě prakticky shodná s programem Wolfram Mathematica, s nímž se studenti setkají v učebnách. Pro správnou funkci těchto programů je v některých případech vyžadována lokální instalace prostředí Java.

Úspěšné zvládnutí textu předpokládá studentův aktivní přístup, schopnost samostatně studovat, počítat cvičení na koncích jednotlivých kapitol, použití doporučené literatury i případné návštěvy konzultací k důkladnějšímu vysvětlení těch partií, které studentovi činí potíže. Za případné připomínky k textu a jeho možnému zdokonalení z řad studentů i kolegů je autor upřímně vděčný. Budou zohledněny v některém dalším, aktualizovaném vydání skripta.

Doc. RNDr. Martin Kovár, Ph.D., autor

1 Množiny a relace

V této kapitole studujeme základní vlastnosti množin a množinových operací a také binárních relací a zobrazení. Budeme studovat spojitost zobrazení a ukážeme, že jde o relativní pojem, závislý na matematické struktuře, které říkáme topologie. Také prozkoumáme některé typy binárních relací na množině, zvláště relace ekvivalence a uspořádání. Povšimneme si vlastností relačních uzávěrů.

Cíle

Po prostudování této kapitoly budete schopni:

- porovnávat množinové mohutnosti
- provádět základní množinové operace
- vyšetřovat vlastnosti binárních relací a zobrazení
- vyšetřovat spojitost zobrazení a funkcí
- sestrojit uzávěry množin a relací různého typu
- vytvářet rozklady množin, příslušné ekvivalencím
- zakreslit Hasseovský diagram uspořádané množiny

1.1 Intuitivní pojem množiny

Pojem množiny, historicky i věcně spjatý s pojmem nekonečna, prošel v matematice určitým a dosti rozsáhlým vývojem, který dosud není zcela ukončen. Pravděpodobně jednu z prvních „definic" množiny podal matematik Georg Cantor (1845-1918). Cantor vymezil množinu jako *„každé shrnutí určitých a navzájem různých předmětů našeho nazírání do jediného celku"* (tyto předměty pak nazýváme prvky množiny). Již z prvního pohledu je zřejmé, že nejde o přesnou matematickou definici, jako spíše o intuitivní vyjádření toho, jaké by množiny měly být a jaké by měly mít vlastnosti. Cantorova definice množiny se stala základem tzv. *intuitivní teorie množin*, která se ukázala jako sporná a byla později nahrazena teorií axiomatickou. V tomto odstavci ukážeme jeden ze sporů v intuitivní teorii množin, který v roce 1902 nalezl anglický matematik a filozof Bertrand Russell (1872-1970). Uvažujme souhrn $\mathcal{N}$ objektů S, které neobsahují sama sebe jakožto prvek:

$$\mathcal{N} = \{S |\, S \notin S\}$$

Je-li $\mathcal{N}$ množinou, je možné si položit otázku, zda $\mathcal{N}$ obsahuje sebe sama jakožto prvek. Překvapivé bylo, že obě možnosti (tedy $\mathcal{N} \in \mathcal{N}$ i $\mathcal{N} \notin \mathcal{N}$) vedou ke sporu. Tento jev v intuitivní teorii množin nazýváme *Russelovým paradoxem*. Russellův paradox byl jedním z mnoha dalších, které byly v intuitivní teorii množin během let objeveny a které posléze vedly k vzniku tzv. *axiomatické teorie množin*, v níž tyto spory nenastávají. Výklad axiomatické teorie množin je ovšem nad rámec tohoto jednoduchého učebního textu. Následující cvičení slouží k hlubšímu pochopení úvodního odstavce. Na základě cvičení 1, 3 a 4 čtenář zjistí, proč můžeme v jistých mezích bezpečně využívat intuitivní teorie množin, ačkoliv je tato jako celek sporná. Úlohy 2 a 5 jsou nepovinné.

Cvičení

1.1.1. Nalezněte spor v definici souhrnu $\mathcal{N}$ z předchozího odstavce prověřením obou možností $\mathcal{N} \in \mathcal{N}$ i $\mathcal{N} \notin \mathcal{N}$.

1.1.2. Všimněte si paralely Russelova paradoxu s principem elektromagnetického přerušovače (tzv. "zvonku") a zamyslete se nad tím, jakým způsobem se příroda vyrovnává s tímto paradoxem.

1.1.3. Nyní předpokládejme, že všechny uvažované objekty leží v nějaké, již předem dané množině $\mathcal{X}$. Místo souboru $\mathcal{N}$ definujme $\mathcal{M} = \{S | \, S \in \mathcal{X}, S \notin S\}$. Položte si nyní otázku, zda $\mathcal{M} \in \mathcal{M}$ či $\mathcal{M} \notin \mathcal{M}$. Která z obou možností je ta správná a proč v tomto případě nedochází ke sporu? Jaký je vztah $\mathcal{M}$ a $\mathcal{X}$?

1.1.4. Pokuste se na základě cvičení 3 vyvodit pravidlo, které zajistí, aby v našich matematických úvahách nemohla nastat situace podobná té, která je popsána Russelovým paradoxem.

1.1.5. Následující úloha je spíše filozofickým zamyšlením, než rigorózní úvahou. Ačkoliv je Russellův paradox v matematice něčím nežádoucím, přesto se může stát jakousi branou do rozsáhlé říše ležící "za" světem dvouhodnotové logiky a uvažování v kategoriích ano-ne. Pokuste se aplikovat konstrukci ve cvičení 3 na universum $\mathcal{X}$ "všeho existujícího". Zejména si povšimněte, co se stane s objektem $\mathcal{M}$. Můžete vyslovit různé logické obměny (tj. logicky ekvivalentní, ale jinak zformulovaná tvrzení) vašeho zjištění.

1.2 Velikost a porovnávání množin

Máme-li konečnou množinu, počet jejích prvků nejpřirozenějším způsobem definuje její velikost. S nekonečnými množinami je to poněkud složitější. Uvážíme-li například jednotkový čtverec v rovině, můžeme za jeho velikost považovat například jeho plochu, která je rovna jedné. Ovšem také si můžeme položit otázku, zda má jednotkový čtverec "stejné množství" bodů jako například jednotková úsečka, jednotková krychle, reálná přímka nebo množina přirozených čísel. Abychom mohli na tyto otázky odpovědět, musíme si nejdříve ujasnit, kdy považujeme dvě množiny (z hlediska teorie množin) za stejně velké, nebo-li přesněji, stejně *mohutné*.

Definice 1.2.1. Mějme množiny A, B, C, buď $B \subseteq C$ a nechť existuje vzájemně jednoznačné přiřazení $f : A \to B$ prvků množiny B prvkům množiny A. Pak říkáme, že množiny A, B mají stejnou *mohutnost*, a také, že množina C je alespoň tak mohutná, jako množina A. Píšeme $|A| = |B|$ a $|A| \leq |C|$.

Příklad 1.2.1. Nechť $A = \{1, 2\}$, $B = \{2, 3\}$ a $C = \{2, 3, 4, 5\}$. Je $|A| = 2 = |B| < |C| = 4$.

Příklad 1.2.2. Nechť $\mathbb{S}$ je množina kladných sudých čísel a nechť $f : \mathbb{N} \to \mathbb{S}$ je dáno předpisem $f(n) = 2n$. Pak f je vzájemně jednoznačné přiřazení, takže $|\mathbb{N}| = |\mathbb{S}|$. Všimněme si, že $\mathbb{S}$ je stejně mohutná vlastní část množiny $\mathbb{N}$, což u konečných množin není možné. Dokonce pro kladná lichá čísla $\mathbb{L} = \mathbb{N} \setminus \mathbb{S}$ platí $|\mathbb{L}| = |\mathbb{S}| = |\mathbb{N}|$ (dokažte!), takže se $\mathbb{N}$ skládá ze dvou disjunktních částí stejně mohutných, jako je původní množina $\mathbb{N}$.

Definice 1.2.2. Množina stejné mohutnosti jakou má množina přirozených čísel se nazývá *spočetná*. Nekonečná množina, která není spočetná, se nazývá *nespočetná*.

Příkladem nespočetné množiny je množina $\mathbb{R}$ všech reálných čísel. Naproti tomu, množiny čísel celých $\mathbb{Z}$ a racionálních $\mathbb{Q}$ jsou obě spočetné.

Cvičení

1.2.1. Dokažte, že množina $\mathbb{Z}$ všech celých čísel je spočetná.

1.2.2. Dokažte, že množina $\mathbb{Q}$ všech racionálních čísel je spočetná.

1.2.3. Dokažte, že číslo $\sqrt{2}$ je iracionální.

1.2.4. Dokažte, že množina $\mathbb{R}$ všech reálných čísel je nespočetná.

1.2.5. * Nechť X je množina, 2^X množina všech podmnožin množiny X. Dokažte, že $|X| < |2^X|$.

1.2.6. Povšimněte si rozdílu mezi celými a racionálními čísly. Obě množiny jsou stejně mohutné, avšak jejich prvky jsou jinak rozloženy na reálné číselné ose. Zatímco celá čísla mají své nejbližší větší a menší sousedy, mezi libovolnými dvěma racionálními čísly leží nekonečně mnoho dalších racionálních čísel (dokažte).

1.3 Operace s množinami

Ačkoliv základní množinové operace náleží do středoškolské látky, pro úplnost je připomeňme. Nechť X, Y jsou množiny. Klademe

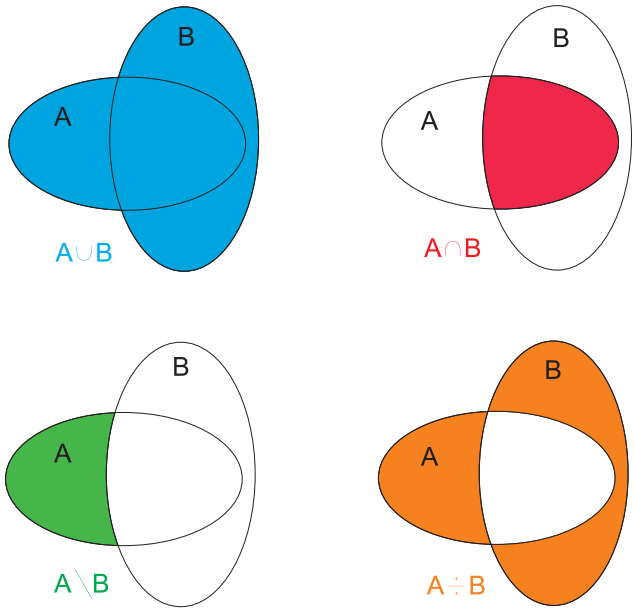
$$X \cup Y = \{x |\, x \in X \vee x \in Y\}\,,$$

$$X \cap Y = \{x |\, x \in X \wedge x \in Y\}\,,$$

$$X \setminus Y = \{x |\, x \in X \wedge x \notin Y\}\,,$$

$$X \div Y = (X \setminus Y) \cup (Y \setminus X)$$

a po řadě nazýváme tyto množiny sjednocením, průnikem, rozdílem a symetrickou diferencí množin X, Y. Je-li $Y \subseteq X$, píšeme $\bar{Y} = X \setminus Y$ a nazýváme doplňkem nebo komplementem množiny Y v množině X. Tuto symboliku používáme především tehdy, když potřebujeme vyjádřit komplementy více množin vůči jedné množině X. Výše definované množinové operace jsou schématicky znázorněny na následujícím obrázku:



Obr. 1.3.1 Množinové operace.

Některé množinové operace můžeme ovšem provádět s celými i s případně nekonečnými soubory množin a nikoli pouze se dvěma množinami. Je-li $\mathcal{S}$ soubor množin, značíme

$$\bigcup \mathcal{S} = \{x |\, (\exists X \in \mathcal{S}) : (x \in X)\}\,,$$

$$\bigcap \mathcal{S} = \{x | \, (\forall X \in \mathcal{S}) : (x \in X)\}\,.$$

Případně, je-li $\mathcal{S} = \{X_1, X_2, \dots\}$, píšeme

$$\bigcup \mathcal{S} = \bigcup_{i=1}^{\infty} X_i$$

a

$$\bigcap \mathcal{S} = \bigcap_{i=1}^{\infty} X_i.$$

Věta 1.3.1. *(Vlastnosti množinových operací) Buďte A, B, C, X množiny. Platí:*

(i) $A \cup B = B \cup A$

(ii) $A \cap B = B \cap A$

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$

(iv) $(A \cap B) \cap C = A \cap (B \cap C)$

(v) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

(vi) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

(vii) $\overline{A \cup B} = \bar{A} \cap \bar{B}$

(viii) $\overline{A \cap B} = \bar{A} \cup \bar{B}$

K předchozí větě podotkněme, že vzhledem k rovnostem (iii) a (iv) obvykle vypouštíme závorky a píšeme pouze $A \cup B \cup C$, resp. $A \cap B \cap C$. Rovnosti (vii) a (viii), v nichž jsou doplňky vyjádřeny vzhledem ke společné množině X, nazýváme De Morganovými zákony pro sjednocení a průnik množin. Analogická pravidla platí i pro počítání se soubory více než dvou množin. Důkaz věty neprovádíme, neboť je velmi jednoduchý a bude předmětem cvičení.

Softwarové nástroje: Množinové operace

Cvičení

1.3.1. Pro $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6\}$, $C = \{1, 2, 4, 8\}$ a $X = \{1, 2, \ldots, 10\}$ vyjádřete $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \div B$, $(A \cup B) \cap C$, $A \cup (B \cap C)$, $\overline{A \cup B}$, $\bar{A} \cup \bar{B}$. Vyjádřete množinu všech podmnožin pro množiny $A \cap C$ a B. Pak vyjádřete $2^{A \cap C} \cap 2^B$ a $2^{A \cap C} \setminus 2^B$. Kolik prvků má množina 2^X?

1.3.2. Rozhodněte, zda následující tvrzení jsou pravdivá:

(i) $\{x\} \subseteq \{x\}$

(ii) $\{x\} \in \{x\}$

(iii) $\{x\} \subseteq \{x, \{x\}\}$

(iv) $\{x\} \in \{x, \{x\}\}$

1.3.3. Dokažte Větu 1.3.1!

1.3.4. Dokažte nebo vyvraťte protipříkladem následující tvrzení. Pro všechny množiny $X, Y, Z \subseteq U$ platí (doplňky množin uvažujeme vůči množině U):

(i) $\overline{X \cap Y} = \bar{X} \cap \bar{Y}$

(ii) $\overline{X \cap Y} \subseteq X$

(iii) $X \setminus Y = Y \setminus X$

(iv) $(X \cap Y) \cup (Y \setminus X) = X$

(v) $X \setminus (Y \cup Z) = (X \setminus Y) \cup Z$

(vi) $\overline{X \setminus Y} = \overline{Y \setminus X}$

(vii) $X \cap (Y \setminus Z) = (X \cap Y) \setminus (X \cap Z)$

(viii) $X \cup (Y \setminus Z) = (X \cup Y) \setminus (X \cup Z)$

(ix) $X \setminus (Y \cap Z) = (X \setminus Y) \cap Z$

(x) $(X \cup Y) \cap (Y \setminus X) = Y$

1.4 Binární relace

Jsou-li a, b nějaké prvky, pak výrazem (a, b) označujeme uspořádanou dvojici prvků a, b. Ta se obecně liší od uspořádané dvojice (b, a), takže záleží na pořadí prvků uvnitř závorky. Jak lze definovat uspořádanou dvojici v teorii množin, aby bylo jasně patrné, který prvek je ve dvojici první? Existuje více možností, například můžeme položit $(a, b) = \{\{a\}, \{a, b\}\}$. Analogicky bychom mohli množinově definovat i pojem uspořádané n-tice $(a_1, a_2, \ldots, a_n)$, pro naše další úvahy však bude lhostejné, jakým přesně objektem uspořádaná n-tice v teorii množin je.

Definice 1.4.1. Jsou-li X, Y množiny, pak *kartézským součinem množin* X, Y rozumíme množinu $X \times Y = \{(x, y) | x \in X, y \in Y\}$. Kartézský součin více, ale konečně mnoha množin $X_1, X_2, \ldots X_n$ definujeme jako množinu $X_1 \times X_2 \times \ldots \times X_n = \prod_{i=1}^{n} X_i = = \{(x_1, x_2, \ldots, x_n) |\ x_1 \in X_1, x_2 \in X_2, \ldots, x_n \in X_n\}$. Kartézský součin spočetně mnoha množin $X_1, X_2, \ldots$ můžeme definovat jako množinu posloupností vybraných prvků $X_1 \times \times X_2 \times \cdots = \prod_{i=1}^{\infty} X_i = \{(x_1, x_2, \ldots) | x_1 \in X_1, x_2 \in X_2, \ldots\}$. Kartézský součin libovolného systému množin můžeme definovat rovněž, je však k tomu zapotřebí dosud korektně nezavedeného pojmu *zobrazení*.

Příklad 1.4.1. Nechť $X = \{1, 2, 3\}$ a $Y = \{a, b\}$. Pak

$$X \times Y = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Definice 1.4.2. Buďte X, Y dvě množiny. *Binární relací* z X do Y rozumíme libovolnou podmnožinu $R \subseteq X \times Y$. Je-li $Y = X$, hovoříme o *binární relaci na množině* X. Dále označujeme $\Delta X = \{(x, x) |\ x \in X\}$ a nazýváme *diagonální relací* na X.

Příklad 1.4.2. Nechť $X = \{2, 3, 4\}$ a $Y = \{3, 4, 5, 6, 7, 8, 9\}$. Například množina $R = = \{(x, y) |\ x \in X, y \in Y, x \text{ dělí } y\} = \{(2, 4), (2, 6), (2, 8), (3, 3), (3, 6), (3, 9), (4, 4), (4, 8)\}$ je binární relací z X do Y.

Definice 1.4.3. Buď $R \subseteq X \times Y$ binární relace z X do Y. Klademe

$$\operatorname{Dom} R = \{x |\ \text{existuje } y \in Y, \text{ že } (x, y) \in R\},$$

$$\operatorname{Im} R = \{y |\ \text{existuje } x \in X \text{ tak, že } (x, y) \in R\}.$$

Množinu $\operatorname{Dom} R$ nazýváme *definiční obor* nebo-li *domain* relace R. Množinu $\operatorname{Im} R$ nazýváme *obor hodnot*, *ko-obor* nebo-li *image* relace R.

Příklad 1.4.3. Nechť $X = \{1,2,3,4,5\}$, $Y = \{a,b,c,d\}$ a $R = \{(1,b),(1,c),(2,d),(4,b),(4,d)\}$. Pak $\mathrm{Dom}\, R = \{1,2,4\}$ a $\mathrm{Im}\, R = \{b,c,d\}$.

Definice 1.4.4. Buď $f \subseteq X \times Y$ relace z X do Y taková, že ke každému x z $\mathrm{Dom}\, f \subseteq X$ existuje právě jeden prvek $y \in Y$, že $(x,y) \in f$. Říkáme, že f je *zobrazení* množiny $\mathrm{Dom}\, f$ do Y resp. z X do Y, když nechceme blíže specifikovat $\mathrm{Dom}\, f$, případně zobrazení X do Y, když $\mathrm{Dom}\, f = X$. Namísto $(x,y) \in f$ píšeme $f(x) = y$ a také $f : X \to Y$ namísto abychom psali $f \subseteq X \times Y$ jako v terminologii binárních relací. Zobrazení $f : X \to Y$ se nazývá

(i) *prosté* neboli *injektivní*, když pro každé $x_1, x_2 \in X$ platí $f(x_1) = f(x_2) \implies x_1 = x_2$ (každý prvek v Y má nejvýše jeden vzor);

(ii) *na* neboli *surjektivní*, jestliže ke každému $y \in Y$ existuje $x \in X$, že $f(x) = y$ (každý prvek v Y má nějaký vzor v X);

(iii) *vzájemně jednoznačné* nebo-li $1-1$-*značné* nebo-li *bijektivní*, když $\mathrm{Dom}\, f = X$ a je zároveň prosté i na (prvky oboru množin X a Y si vzájemně odpovídají).

Zobrazení $\mathrm{id}_X : X \to X$ dané předpisem $\mathrm{id}_X(x) = x$ nazýváme *identitou* na X. Je zřejmé, že identita je vlastně pouze jinak pojmenovaná diagonální relace.

Příklad 1.4.4. Nechť $A = \{1,2,3\}$, $B = \{a,b,c\}$, $C = \{1,2,3,4\}$, $D = \{a,b,c,d\}$. Pak $R = \{(1,a),(1,b),(3,c)\}$ je binární relací z A do B, která ale není zobrazením. Relace $f = \{(1,a),(2,c),(3,b)\}$ je bijektivní zobrazení A na B, ale pouze injektivní zobrazení A do D. Relace $g = \{(1,a),(2,c),(3,b),(4,a)\}$ je surjektivním zobrazení C na B, ale pouze zobrazením C do D. Zároveň je f zobrazením z C do D (které je injekcí na svém definičním oboru $\mathrm{Dom}\, f = A$).

Definice 1.4.5. Buď $R \subseteq X \times Y$ relace. *Inverzní relací* k relaci R nazýváme relaci $R^{-1} = \{(y,x) | \exists (x,y) \in R\}$. Zřejmě $R^{-1} \subseteq Y \times X$. Jsou-li navíc R, R^{-1} zobrazení, nazývá se R^{-1} *inverzním zobrazením* k zobrazení R.

Příklad 1.4.5. Nechť R je relace z příkladu 1.4.2. Pak $R^{-1} = \{(4,2),(6,2),(8,2),(3,3),(6,3),(9,3),(4,4),(8,4)\}$.

Příklad 1.4.6. Nechť $f, g : C \to D$ jsou zobrazení z příkladu 1.4.4. Pak $f^{-1} = = \{(a,1),(b,3),(c,2)\}$ je zobrazení z D do C, které je inverzní vzhledem k zobrazení f. Relace $g^{-1} = \{(a,1),(c,2),(b,3),(a,4)\}$ je inverzní k zobrazení g, avšak sama není zobrazením.

Softwarové nástroje: Binární relace a zobrazení

Definice 1.4.6. Buďte $R \subseteq X \times Y$, $S \subseteq Y \times Z$ relace. *Složením* nebo-li *kompozicí* relací R, S nazýváme relaci

$$S \circ R = \{(x, z) | \exists y \in Y, \text{ že } (x, y) \in R \text{ a } (y, z) \in S\}.$$

Tuto relaci čteme "S *po* R".

Příklad 1.4.7. Buď $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c\}$ a $Z = \{t, u, v, w\}$. Nechť $R = \{(1, a), (1, b), (2, b), (3, c)\}$ a $S = \{(a, u), (a, v), (b, t), (c, t), (c, w)\}$. Pak $S \circ R = \{(1, u), (1, v), (1, t), (2, t), (3, t), (3, w)\}$.

Jsou-li $f : X \to Y$, $g : Y \to Z$ zobrazení, složená relace $g \circ f$ je opět zobrazení (ověřte!) a nazývá se *složené zobrazení* $g \circ f$. Místo pojmu zobrazení někdy používáme ekvivalentní pojem *funkce*. Zejména ve starší literatuře pojem funkce, případně funkce s vhodným přívlastkem, bývá vyhrazen zobrazením, jejichž definiční obor nebo obor hodnot je nějakým způsobem odvozen z číselných množin, především z množiny reálných čísel. Je vhodné si uvědomit, že hodnota složeného zobrazení $g \circ f$ v bodě $x \in X$ je rovna hodnotě zobrazení g v bodě $f(x)$. Tedy

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

Případ složených relací je odlišný v tom, že "funkčních hodnot" v daném bodě je obecně více než jedna. Například, je-li $f : X \to Y$ prosté zobrazení na Y (tedy bijekce), je $f^{-1} \circ f = \mathrm{id}_X$ a $f \circ f^{-1} = \mathrm{id}_Y$. Pro obecnou relaci $R \subseteq X \times Y$ toto neplatí, $R^{-1} \circ R$, resp. $R \circ R^{-1}$ nemusí být vždy diagonální relace $\triangle_X$, resp. $\triangle_Y$.

Příklad 1.4.8. Je-li $X = Y = Z = \mathbb{R}$, funkce $f : X \to Y$ je dána předpisem $y = \sin x$ a funkce $g : Y \to Z$ je dána předpisem $z = e^y$, je složená funkce $g \circ f$ dána předpisem $z = e^{\sin x}$. Jinak zapsáno,

$$(g \circ f)(x) = g(f(x)) = e^{f(x)} = e^{\sin x}.$$

Cvičení

1.4.1. Na množině $X = \{1, 2, 3, 4, 5, 6, 7\}$ je dána relace $R = \{(x, y) | \, x, y \in X, 3 \text{ dělí } x - y\}$. Zapište relaci R výčtem prvků. Určete její definiční obor a obor hodnot. Nalezněte relaci R^{-1}.

1.4.2. Zopakujte cvičení 1 pro relaci $R = \{(x, y) | \, x, y \in X, x \text{ dělí } y\}$.

1.4.3. Nechť $R_1 = \{(1, 2), (1, 6), (2, 4), (3, 4), (3, 6), (3, 8)\}$, $R_2 = \{(2, u), (4, s), (4, t), (6, t), (8, u)\}$. Zapište výčtem prvků relace R_1^{-1}, R_2^{-1}, $R_2 \circ R_1$, $(R_2 \circ R_1)^{-1}$, $R_1^{-1} \circ R_2^{-1}$.

1.4.4. Dokažte, že pro libovolné dvě binární relace R, S platí $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

1.4.5. Dokažte, že pro libovolné tři binární relace R, S, T platí $(T \circ S) \circ R = T \circ (S \circ R)$.

1.4.6. Nechť $f(x) = \sin x$, $g(x) = \ln x$, $h(x) = 2x$. Stanovte $\mathrm{Dom}\,(g \circ f \circ h)$ a $\mathrm{Im}\,(g \circ f \circ h)$. Určete $(g \circ f \circ h)(\pi/4)$.

1.5 Topologie a spojitost zobrazení

Ve cvičení 1.2 jsme si všimli, že množiny celých čísel i čísel racionálních jsou stejně mohutné a z hlediska teorie množin mezi nimi není podstatný rozdíl, snad kromě označení jejich prvků a způsobu, jakým je možno je sestrojit. Uvažujeme-li však obě množiny jako součást číselné osy, zjistíme, že na číselné ose jsou obě množiny rozloženy zcela odlišně. Podobně – z hlediska teorie množin – není podstatný rozdíl mezi body reálné přímky a roviny, jednotkové krychle, kruhu nebo čtverce. Je možné dokázat, že také tyto množiny mají stejnou, tentokrát však nespočetnou mohutnost. Vzniká otázka, čím je způsobeno, že se nám jeví pokaždé jinak.

Velmi volně a zjednodušeně řečeno, prvky některých množin mají ve svém blízkém okolí pokaždé jiné prvky. Tato vlastnost není ovšem dána množinou samotnou, ale tím, jak vnímáme okolí jednotlivých bodů. Proto se nám jeví stejná množina jednou jako přímka, podruhé jako rovina, případně úsečka, čtverec, kruh, nebo krychle. Matematická struktura, která dokáže zachytit okolí jednotlivých bodů, se nazývá topologie. V následujícím textu si upřesníme, co to vlastně topologie je.

Definice 1.5.1. Buď X množina, $\tau \subseteq 2^X$ systém jistých podmnožin množiny X. Řekneme, že τ je *topologie* na X, jestliže platí:

(i) $\varnothing, X \in \tau$

(ii) Jestliže $U_i \in \tau$ pro všechna $i \in I$, pak $\bigcup_{i\in I} U_i \in \tau$.

(iii) Jestliže $U, V \in \tau$, pak $U \cap V \in \tau$.

Prvky systému τ nazýváme *otevřené množiny*, doplňky otevřených množin nazýváme *uzavřené množiny*. Dvojici (X, τ) nazýváme *topologický prostor*. Obsahuje-li otevřená množina $U \in \tau$ bod $x \in X$, nazývá se *okolím* bodu x. Dále pro libovolnou množinu $A \subseteq X$ klademe

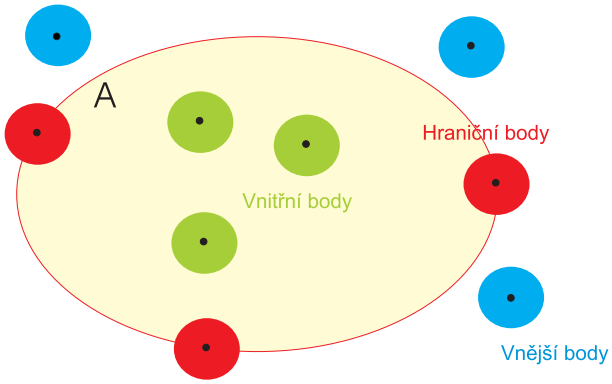
$$\operatorname{int} A = \{x |\, x \in X, (\exists U \in \tau) : x \in U \subseteq A\},$$

$$\operatorname{ext} A = \{x |\, x \in X, (\exists U \in \tau) : x \in U \wedge U \cap A = \varnothing\},$$

$$\operatorname{fr} A = \{x |\, x \in X, (\forall U \in \tau) : x \in U \Rightarrow (U \cap A \neq \varnothing \wedge U \cap (X \setminus A) \neq \varnothing)\}$$

a

$$\operatorname{cl} A = A \cup \operatorname{fr} A = \operatorname{int} A \cup \operatorname{fr} A = \{x |\, x \in X, (\forall U \in \tau) : x \in U \Rightarrow U \cap A \neq \varnothing\}.$$

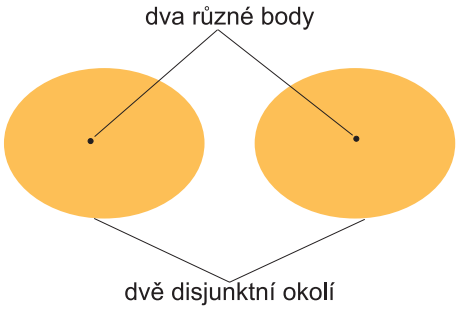


Obr. 1.5.1 Vnitřní, hraniční a vnější body.

Množinám $\operatorname{int} A$, $\operatorname{ext} A$, $\operatorname{fr} A$ a $\operatorname{cl} A$ po řadě říkáme *vnitřek*, *vnějšek*, *hranice* a *uzávěr* množiny A. Snadno nahlédneme, že vnitřek a vnějšek množiny jsou množiny otevřené, zatímco hranice a uzávěr množiny jsou vždy množiny uzavřené. Následující obrázek, který se vztahuje k přirozené, tzv. Eukleidově topologii roviny (viz Příklad 1.5.4) ilustruje rozdíl mezi otevřenou a uzavřenou množinou. Otevřená množina neobsahuje své hraniční body, naopak uzavřená množina je obsahuje všechny. Mohou ovšem existovat množiny, které nejsou ani otevřené, ani uzavřené.

Obr. 1.5.2 Otevřené a uzavřené množiny

Topologický prostor (X, τ) se nazývá *Hausdorffův*, *oddělitelný* nebo-li také T_2*-prostor*, jestliže ke každým dvěma různým $x, y \in X$ existují $U, V \in \tau$, že $x \in U$, $y \in V$ a $U \cap V = \varnothing$.



Obr. 1.5.3 Hausdorffův topologický prostor.

Hausdorffovy prostory mají velký význam zejména v klasické topologii. Z hlediska topologie orientované na informatiku takový význam nemají. Naopak, většina topologických prostorů, které mají význam z hlediska informatiky, Hausdorffovy nejsou. Uvedeme příklady několika důležitých topologických prostorů.

Příklad 1.5.1. Nechť X je libovolná množina, $\tau = \{\varnothing, X\}$. Pak (X, τ) se nazývá *triviální topologický prostor* a τ *triviální topologie* na X. Tento prostor není Hausdorffův, pokud $|X| > 1$.

Příklad 1.5.2. Nechť X je libovolná množina, $\tau = 2^X$. Pak (X, τ) se nazývá *diskrétní topologický prostor* a τ *diskrétní topologie* na X. Tento prostor je Hausdorffův.

Příklad 1.5.3. Nechť $X = \mathbb{R}$, $\tau = \{U | U$ je sjednocením otevřených intervalů v $\mathbb{R}\}$. Pak (X, τ) se nazývá *jednorozměrný Eukleidův topologický prostor* a τ *Eukleidova topologie* na $X = \mathbb{R}$. Tento prostor je Hausdorffův.

Příklad 1.5.4. Nechť $X = \mathbb{R}^n$, $\tau = \{U | U$ je sjednocením otevřených koulí v $\mathbb{R}^n\}$. Pak (X, τ) se nazývá *n-rozměrný Eukleidův topologický prostor* a τ *Eukleidova topologie* na $X = \mathbb{R}^n$. Tento prostor je Hausdorffův.

Příklad 1.5.5. Nechť $X = \{0, 1\}$, $\tau = \{\varnothing, \{0\}, \{0, 1\}\}$. Pak (X, τ) se nazývá *Serpiǹského topologický prostor* a τ *Serpiǹského topologie* na X. Tento prostor není Hausdorffův.

Příklad 1.5.6. Nechť $X = \mathbb{N}$, $\tau = \{U | U \subseteq X, X \setminus U$ je konečná$\} \cup \{\varnothing\}$. Pak τ se nazývá *kofinitní topologie* nebo *topologie konečných doplňků* na $X = \mathbb{N}$. Tento prostor není Hausdorffův.

Příklad 1.5.7. Buď (X, τ) topologický prostor, $Y \subseteq X$ podmnožina. Klademe $\sigma = \{U \cap$ $\cap\, Y | U \in \tau\}$. Pak σ je topologie na Y, jíž říkáme *indukovaná topologie* (na Y z prostoru (X, τ)). Prostoru (Y, σ) říkáme *topologický podprostor* prostoru (X, τ).

Softwarové nástroje: Topologie na konečné množině, Topologie na konečné množině 2

Systém všech otevřených množin topologického prostoru někdy obsahuje příliš mnoho množin. Proto bývá užitečné pracovat s některým jeho význačným podsystémem, který budeme nazývat jeho bází, pokud bude splňovat určité vlastnosti.

Definice 1.5.2. Buď (X, τ) topologický prostor a $\tau_0 \subseteq \tau$. Řekneme, že τ_0 je *bází topologie* τ, jestliže každou množinu $U \in \tau$ lze vyjádřit jako sjednocení jistých množin z τ_0.

Uvedeme příklady bází některých topologických prostorů.

Příklad 1.5.8. Každá topologie je svou vlastní bází.

Příklad 1.5.9. Otevřené intervaly v $\mathbb{R}$ tvoří bázi Eukleidovy topologie na $\mathbb{R}$.

Příklad 1.5.10. Otevřené koule (kvádry, krychle, jehlany,...) v $\mathbb{R}^n$ tvoří bázi Eukleidovy topologie na $\mathbb{R}^n$.

Abychom mohli pokračovat v příkladech bází topologických prostorů, připomeneme si následující důležitý pojem.

Definice 1.5.3. Buď X množina, $\rho : X \times X \to \mathbb{R}$ zobrazení, splňující podmínky

(i) $\rho(x, y) \geq 0$, rovnost nastává právě když $x = y$

(ii) $\rho(x, y) = \rho(y, x)$

(iii) $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$

Pak ρ se nazývá *metrika* na X a dvojice (X, ρ) se nazývá *metrický prostor*.

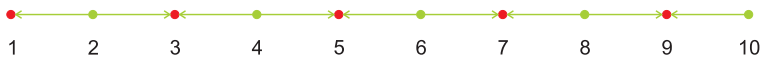
Metrika vlastně zobecňuje pojem vzdálenosti. Máme-li k dispozici strukturu vektorového prostoru se skalárním součinem, můžeme definovat metriku pomocí skalárního součinu.

Příklad 1.5.11. Nechť X je vektorový prostor se skalárním součinem $s : X \times X \to \mathbb{R}$. Pak $\rho(x, y) = \sqrt{s(x - y, x - y)}$ je metrika na X, které se říká *metrika indukovaná skalárním součinem*. Metrika definovaná standardním skalárním součinem na R^n, tedy metrika tvaru $\rho(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}$, se nazývá *Eukleidova metrika*.

Příklad 1.5.12. Je-li (X, ρ) metrický prostor, pak otevřené koule tvaru $B(x, r) = \{y | \, y \in X, \rho(x, y) < r\}$, kde $x \in X$ a $r > 0$ tvoří bázi jisté topologie na X. Této topologii se říká *topologie indukovaná metrikou*. Je zřejmé, že tato topologie je Hausdorffova.

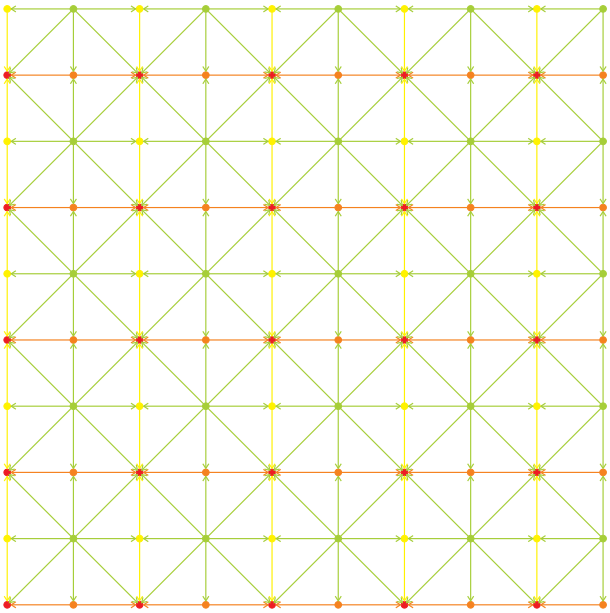
Příklad 1.5.13. Jsou-li (X, τ) a (Y, σ) topologické prostory s bázemi topologií τ_0 a σ_0, pak množina $\tau_0 \square \sigma_0 = \{U \times V | \, U \in \tau_0, V \in \sigma_0\}$ je bází jisté topologie na množině $X \times Y$. Této topologii říkáme *topologie součinu*. Například Eukleidova topologie reálné roviny $\mathbb{R}^2$ je topologií součinu dvou jednorozměrných Eukleidových topologií na obou reálných přímkách.

Příklad 1.5.14. Nechť $K = \mathbb{N}$, $\tau_0 = \{\{1\}, \{1, 2, 3\}, \{3\}, \{3, 4, 5\}, \{5\}, \dots\}$, τ množina všech sjednocení množin z τ_0. Pak (K, τ) je tzv. *Khalimského polopřímka*.



Obr. 1.5.4 Úsek Khalimského polopřímky.

Součinová topologie na K^2 je tzv. *dvourozměrná Khalimského topologie*, důležitá pro počítačové vidění a rozlišování obrazu. V předchozím i v následujícím obrázku je nejmenší okolí daného bodu dáno bodem samotným a koncovými body šipek, které z daného bodu vychází. Typy různých bodů a jejich nejmenší okolí jsou znázorněna různými barvami.



Obr. 1.5.5 Dvourozměrná Khalimského topologie.

Je zřejmé, že oba Khalimského prostory nejsou Hausdorffovy.

Příklad 1.5.15. Nechť $X = \mathbb{R}$. Pak τ_0, množina všech polouzavřených intervalů tvaru $\langle a, b) \subseteq \mathbb{R}$, je bází tzv. *Sorgenfreyovy topologie* na X, která má některé výrazně odlišné vlastnosti od topologie Eukleidovy. Tato topologie ovšem je, stejně jako Eukleidova topologie na $\mathbb{R}$, Hausdorffova.

K tomu, abychom poznali, zda jistý soubor podmnožin množiny X je bází nějaké topologie na X, slouží následující věta.

Věta 1.5.1. *Buď X množina a $\tau_0 \subseteq 2^X$. Pak τ_0 je bází nějaké topologie na X právě když jsou splněny následující podmínky:*

(i) $\bigcup \tau_0 = X$

(ii) *Je-li $U, V \in \tau_0$ a $x \in U \cap V$, pak existuje $W \in \tau_0$, že $x \in W \subseteq U \cap V$.*

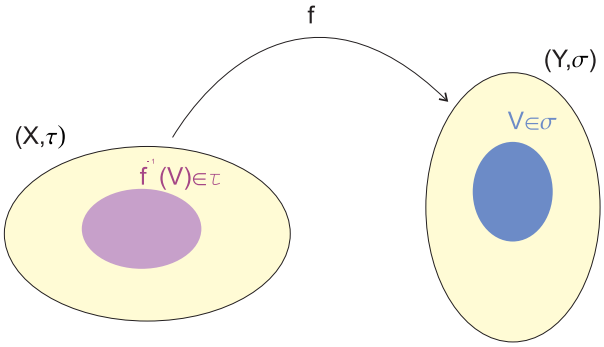
Důkaz. Nechť τ_0 je bází topologie τ na X. Pak zřejmě $X \in \tau$ je sjednocením jistých množin z τ_0, takže $\bigcup \tau_0 = X$. Je-li $U, V \in \tau_0$ a $x \in U \cap V$, je $U \cap V \in \tau$, takže existuje $W \in \tau_0$, že $x \in W \subseteq U \cap V$.

Naopak, nechť τ_0 splňuje podmínky (1) a (2). Buď τ soubor všech množin, které jsou sjednocením jistých množin z τ_0. Je zřejmé, že $\varnothing$ je sjednocením prázdného systému, takže $\varnothing \in \tau$. Z (1) plyne $X \in \tau$. Rovněž je zřejmé, že systém τ je uzavřený na operaci sjednocení libovolného svého podsystému. Buďte $U, V \in \tau$. Ukážeme, že $U \cap V \in \tau$. Nechť $x \in U \cap V$. Existují $U_0, V_0 \in \tau_0$, $U_0 \subseteq U$, $V_0 \subseteq V$, že $x \in U_0 \cap V_0$. Podle (2) existuje $W \in \tau_0$, že $x \in W \subseteq U_0 \cap V_0 \subseteq U \cap V$. Tedy $U \cap V$ je sjednocením jistých množin z τ_0 a tedy $U \cap V \in \tau$. Tím je prověřeno, že τ je topologie na X.

□

Nyní můžeme přistoupit k definici pojmu spojitosti zobrazení.

Definice 1.5.4. Buďte (X, τ), (Y, σ) topologické prostory, $f : X \to Y$ zobrazení. Říkáme, že f je *spojité*, jestliže pro každou otevřenou množinu $V \in \sigma$ je množina $f^{-1}(V) = \{x | \, x \in X, f(x) \in V\}$ otevřená v (X, τ), tedy $f^{-1}(V) \in \tau$.



Obr. 1.5.6 Zobrazení a jeho spojitost.

Příklad 1.5.16. Identické zobrazení na topologickém prostoru je vždy spojité.

Příklad 1.5.17. Buď $X = \{0, 1\}$, $\tau = \{\varnothing, \{0\}, \{0, 1\}\}$, $Y = \{a, b\}$, $\sigma = \{\varnothing, \{b\}, \{a, b\}\}$ a $f : X \to Y$ takové zobrazení, že $f(0) = a$, $f(1) = b$. Pak f není spojité, protože $\{b\} \in \sigma$, ale $f^{-1}(\{b\}) = \{1\} \notin \tau$.

Příklad 1.5.18. Elementární funkce $\sin x$, $\cos x$ a e^x jsou spojité na $\mathbb{R}$ s Eukleidovou topologií. Funkce $\operatorname{tg} x$, $\ln x$ jsou spojité na svém definičním oboru (který je však vlastní podmnožinou $\mathbb{R}$!!).

Příklad 1.5.19. Funkce $\operatorname{sgn} x : \mathbb{R} \to \mathbb{R}$, která nabývá hodnot

$$\operatorname{sgn} x = \begin{cases} -1, & \text{pro } x < 0, \\ 0, & \text{pro } x = 0, \\ 1, & \text{pro } x > 0, \end{cases}$$

není spojitá na $\mathbb{R}$ s Eukleidovou topologií, protože $\operatorname{sgn}^{-1}((-\frac{1}{2}, \frac{1}{2})) = \{0\}$ není otevřená množina v Eukleidově topologii. Na následujícím obrázku uvádíme grafy některých nespojitých reálných funkcí. Na ose y je vyznačen otevřený interval, jehož inverzní obraz není množina otevřená v Eukleidově topologii. Tyto funkce jsou definovány předpisy

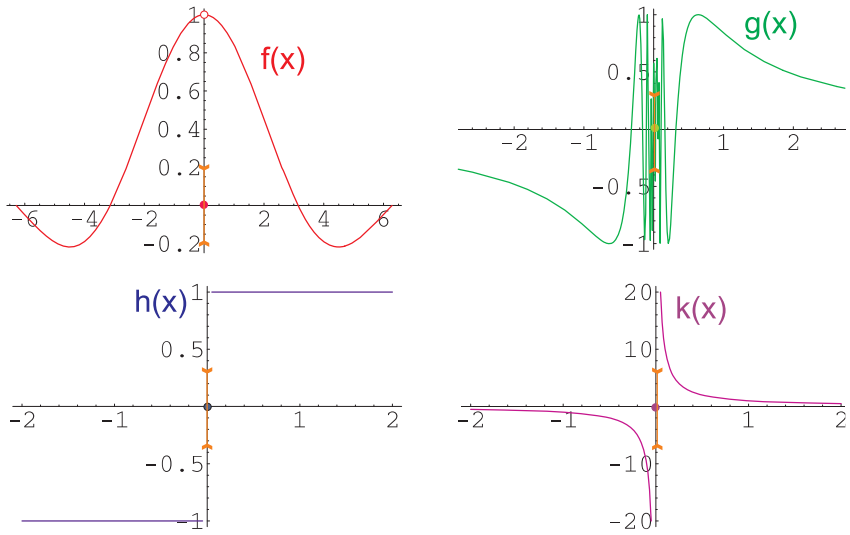
$$f(x) = \begin{cases} \frac{\sin x}{x}, & \text{pro } x \neq 0, \\ 0, & \text{pro } x = 0, \end{cases}$$

$$g(x) = \begin{cases} \sin \frac{1}{x}, & \text{pro } x \neq 0, \\ 0, & \text{pro } x = 0, \end{cases}$$

$$h(x) = \operatorname{sgn} x$$

a

$$k(x) = \begin{cases} \frac{1}{x}, & \text{pro } x \neq 0, \\ 0, & \text{pro } x = 0. \end{cases}$$



Obr. 1.5.7 Některé nespojité reálné funkce

Definice 1.5.5. Buď $f : X \to Y$ spojité vzájemně jednoznačné zobrazení mezi topologickými prostory (X, τ), (Y, σ). Nechť je spojité i zobrazení f^{-1}. Pak se f (i f^{-1}) nazývá *homeomorfismem*. O prostorech (X, τ), (Y, σ) říkáme, že jsou *homeomorfní*.

Homeomorfní prostory jsou z topologického hlediska stejné, až na označení svých prvků. Uveďme příklady homeomorfních prostorů.

Příklad 1.5.20. Reálná přímka $\mathbb{R}$ a otevřený interval (a, b), kde $a < b$, jsou homeomorfní. Například funkce $\operatorname{tg} x$ je homeomorfismus intervalu $(-\frac{\pi}{2}, \frac{\pi}{2})$ na $\mathbb{R}$.

Příklad 1.5.21. Reálná rovina $\mathbb{R}^2$ a dvourozměrná sféra $S^2 \setminus \{p\}$, z níž je vyjmut jediný bod $p \in S^2$, jsou homeomorfní.

Naopak, přímka a rovina homeomorfní nejsou, uzavřený a otevřený interval také ne. Zatímco v teorii množin byly tyto útvary až na označení prvků totožné, nová struktura vnesená či zachycená topologií již mezi některými z nich dokáže rozlišit. Podobně bychom

zjistili, že otevřený interval a reálná přímka, které topologie považuje za stejné, struktura metriky již rozliší – interval (a, b) má konečnou délku, zatímco přímka $\mathbb{R}$ nikoliv. Pozorný čtenář si může položit otázku, proč se tedy zabýváme topologickými prostory, když se metrická struktura zdá být výhodnější, protože dokáže rozlišit od sebe i objekty, které v topologii splývají. Bohužel, existuje řada topologických prostorů, které se nedají definovat metrikou. A právě tyto topologické prostory jsou mnohdy zajímavé z hlediska computer science či některých odvětví moderní matematiky. Příkladem je topologický prostor z příkladu 1.5.14 nebo 1.5.15. Rozhodnout, zda jsou dva topologické prostory homeomorfní může být někdy dosti obtížné, například i důkaz klasického a dobře známého výsledku nehomeomorfnosti reálné roviny a reálné přímky přesahuje rozsah tohoto základního učebního textu.

Softwarové nástroje: Spojitost zobrazení na konečných množinách

Definice 1.5.6. Buď X množina, Ω soubor množin. Řekneme, že Ω pokrývá X nebo-li Ω je pokrytí X, jestliže $X \subseteq \bigcup \Omega$.

Definice 1.5.7. Řekneme, že topologický (X, τ) je *kompaktní*, jestliže z každého jeho pokrytí $\Omega \subseteq \tau$ otevřenými množinami lze vybrat konečné podpokrytí. O množině $Y \subseteq X$ říkáme, že je kompaktní, je-li kompaktní jako topologický podprostor prostoru (X, τ), tedy v topologii indukované z prostoru (X, τ).

Pojem kompaktnosti je jedním z nejdůležitějších pojmů topologie. Kompaktní prostory mají vlastnosti, které se v mnohém ohledu blíží konečným množinám, ačkoli mohou být například nespočetné. V reálné analýze se cení především vlastnost, že spojité funkce na nich nabývají svého minima i maxima. Uvedeme některé příklady kompaktních prostorů.

Příklad 1.5.22. Každý konečný topologický prostor je kompaktní.

Příklad 1.5.23. Reálný uzavřený interval je kompaktní.

Důkaz. K důkazu tohoto tvrzení potřebujeme poněkud hlubší znalosti vlastností uspořádání reálných čísel. Říkáme, že reálné číslo $h \in \mathbb{R}$ je *horní závora* množiny $M \subseteq \mathbb{R}$, jestliže pro každé $m \in M$ platí $m \leq h$. Podobně, reálné číslo $d \in \mathbb{R}$ je *dolní závora* množiny M, jestliže pro každé $m \in M$ platí $m \geq d$. Nejmenší horní závoru množiny M označujeme $\sup M$ a nazýváme

suprémem množiny M. Největší dolní závoru množiny M označujeme $\inf M$ a nazýváme *infimem* množiny M. Reálná čísla se vyznačují příjemnou vlastností, že totiž všechny neprázdné omezené množiny v $\mathbb{R}$ mají suprémum a infimum.Pozorný čtenář si jistě povšimne rozdílu mezi maximem a suprémem, případně minimem a infimem množiny. Zatímco maximum i minimum, pokud existují, musí být prvkem dané množiny, suprémum ani infimum nemusí. Pojmy, které jsme zde pro potřeby důkazu uvedli, vyložíme podrobněji v kapitole věnované uspořádaným množinám. Nyní můžeme zahájit vlastní důkaz.

Nechť $a, b \in \mathbb{R}$ a $a < b$. Nechť Ω je otevřené pokrytí intervalu $I = \langle a, b\rangle$. Položme $M = \{x | \, x \in I$, interval $\langle a, x\rangle$ lze pokrýt konečně mnoha množinami z $\Omega\}$. Protože zajisté $a \in U$ pro nějaké $U \in \Omega$, existuje $\varepsilon > 0$ takové, že $(a - \varepsilon, a + \varepsilon) \subseteq U$. Pak ovšem $\left\langle a, a + \frac{\varepsilon}{2}\right\rangle \subseteq U$, odkud $a + \frac{\varepsilon}{2} \in M \neq \varnothing$. Označme tedy $m = \sup M$. Zřejmě $a < m \leq b$, odkud $m \in I$. Tedy existuje $V \in \Omega$, že $m \in V$. Existuje $\delta > 0$, že $(m - \delta, m + \delta) \subseteq V$, neboť V je otevřená. Protože je m suprémum množiny M, existuje $x \in M \cap (m - \delta, m\rangle$. Všimněme si, že také interval $\left\langle a, m + \frac{\delta}{2}\right\rangle$ lze pokrýt konečně mnoha množinami z Ω. Nyní je zřejmé, že musí být $m = b$. Kdyby bylo $m < b$, nebylo by totiž $m = \sup M$.

□

Příklad 1.5.24. Topologický prostor z příkladu 1.5.6 je kompaktní.

Věta 1.5.2. *Obraz kompaktního topologického prostoru ve spojitém zobrazení je kompaktní topologický prostor.*

Důkaz. Buď (X, τ) kompaktní topologický prostor,(Y, σ) topologický prostor, $f : X \to Y$ spojité surjektivní zobrazení. Nechť Ω je otevřené pokrytí Y. Klademe $\Phi = \{f^{-1}(V) | \, V \in \Omega\}$. Pak Φ je otevřené pokrytí X, z něhož lze vybrat konečné podpokrytí $\{f^{-1}(V_1), f^{-1}(V_2), \ldots, f^{-1}(V_k)\}$. Pak $\bigcup_{i=1}^{k} V_i = Y$, takže $\{V_1, V_2, \ldots, V_k\}$ je konečné podpokrytí Ω. Tedy (Y, σ) je kompaktní.

□

Věta 1.5.3. *Množina $K \subseteq \mathbb{R}^n$ je kompaktní v Eukleidově topologii na $\mathbb{R}^n$, právě když je omezená a uzavřená.*

Důkaz je v principu analogický důkazu kompaktnosti uzavřeného reálného intervalu, jeho obtížnost však přesahuje možnosti tohoto učebního textu.

Důsledek 1.5.1. *Spojitá funkce s reálnými hodnotami nabývá na kompaktní množině svého minima a maxima.*

Důkaz. Buď (X, τ) topologický prostor a $K \subseteq X$ kompaktní. Nechť $f : K \to \mathbb{R}$ je spojité zobrazení. Pak $f(K) \subseteq \mathbb{R}$ je kompaktní podle věty 1.5.2. Podle věty 1.5.3 je $f(K)$ omezená a uzavřená. Tedy existují $\sup f(K), \inf f(K) \in \mathbb{R}$, přičemž s uzavřenosti množiny $f(K)$ plyne $\sup f(K), \inf f(K) \in f(K)$.

□

Cvičení

1.5.1. V příkladech 1.5.1 až 1.5.7 prověřte axiómy topologie, uvedené v 1.5.1.

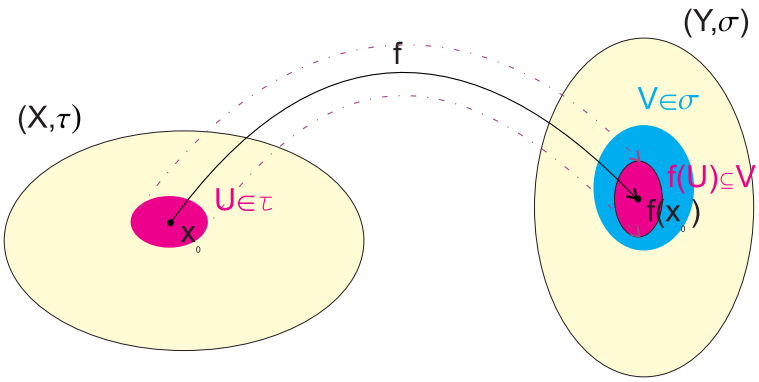
1.5.2. V příkladech 1.5.8 až 1.5.15 prověřte axiómy báze topologie, uvedené v 1.5.1.

1.5.3. Dokažte, že Eukleidova metrika na $\mathbb{R}^2$ indukuje Eukleidovu topologii.

1.5.4. Najděte všechna spojitá zobrazení a všechny homeomorfismy mezi dvěma Serpiňského topologickými prostory.

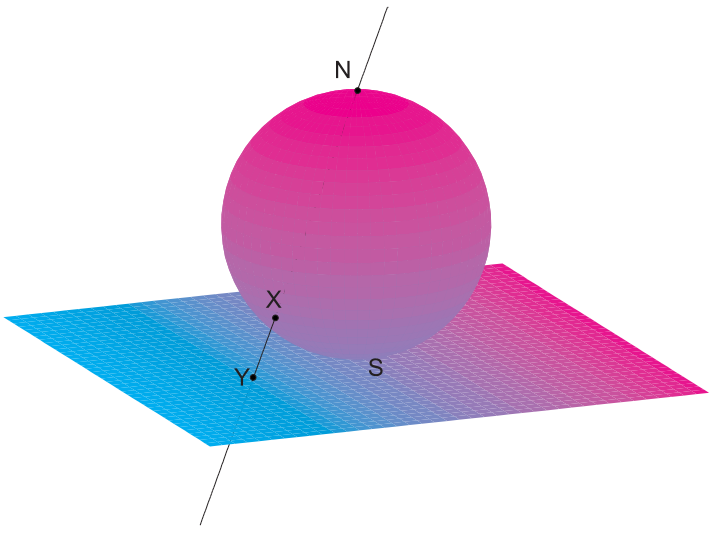
1.5.5. Najděte všechny topologie na dvouprvkové a tříprvkové množině. Určete, které z nich jsou navzájem homeomorfní.

1.5.6. Dokažte, že reálná funkce $f : \mathbb{R} \to \mathbb{R}$ daná předpisem $f(x) = 2x$ je spojitá.



Obr. 1.5.8 Spojitost zobrazení v bodě

1.5.7. * Buďte (X, τ), (Y, σ) topologické prostory. Zobrazení $f : X \to Y$ se nazývá *spojité v bodě* $x \in X$, jestliže ke každému okolí $V \in \sigma$ bodu $f(x)$ existuje okolí $U \in \tau$ bodu x takové, že $f(U) \subseteq V$ (viz. Obr. 1.5.8). Dokažte, že zobrazení f je spojité, právě když je spojité v každém bodě prostoru X.



Obr. 1.5.9 Stereografická projekce

1.5.8. * Dokažte tvrzení příkladu 1.5.21. Návod: Požadovaný homeomorfismus naleznete, když sestrojíte sféru, dotýkající se roviny. Protějším bodem na sféře k bodu dotyku veďte polopřímku, která je různoběžná s rovinou. Polopřímka protne sféru i rovinu v sobě si odpovídajících bodech (viz. Obr. 1.5.9). Zbývá prověřit, že vznikající zobrazení (tzv. stereografická projekce) je homeomorfismus.

1.5.9. Prověřte, že topologický prostor z příkladu 1.5.6 je kompaktní.

1.5.10. Dokažte, že nekonečný diskrétní prostor není kompaktní.

1.5.11. Dokažte, že množina $\mathbb{R}$ s Eukleidovou topologií není kompaktní.

1.5.12. Dokažte, že uzavřený interval a reálná přímka nejsou homeomorfní.

1.6 Relace na množině

Nyní se budeme zabývat dalšími typy binárních relací na množině.

Definice 1.6.1. Buď $R \subseteq X \times X$ relace na X. Řekneme, že R je:

(i) *reflexivní*, jestliže $(x, x) \in R$ pro každé $x \in X$;

(ii) *symetrická*, jestliže platí implikace $(x, y) \in R \implies (y, x) \in R$;

(iii) *antisymetrická*, jestliže platí $[(x, y) \in R \wedge (y, x) \in R] \implies x = y$;

(iv) *tranzitivní*, jestliže $[(x, y) \in R \wedge (y, z) \in R] \implies (x, z) \in R$.

Dále, relaci R nazveme *ekvivalencí* na množině X, je-li současně reflexivní, symetrická i tranzitivní. Podobně, relace R se nazývá *(částečné) uspořádání* na množině X, je-li současně reflexivní, antisymetrická a tranzitivní. Relace, která je reflexivní a symetrická (nemusí být tranzitivní), se nazývá *tolerance*. Podobně, je-li relace reflexivní a tranzitivní (nemusí být antisymetrická), nazývá se *kvaziuspořádání*.

Příklad 1.6.1. Nechť $X = \{1, 2, 3, 4\}$, $R = \{(x, y) | \, x, y \in X, x \leq y\}$. Pak R je reflexivní, antisymetrická a tranzitivní, ale není symetrická. R je uspořádání na X.

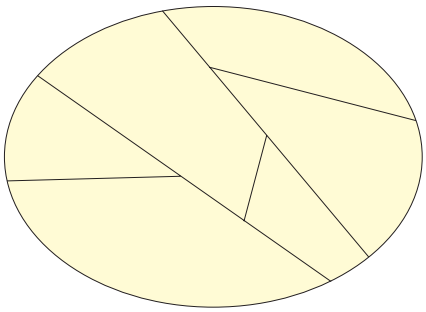
Příklad 1.6.2. Nechť $X = \{1, 2, 3, 4\}$, $R = \{(x, y) | \, x, y \in X, x < y\}$. Pak R je antisymetrická a tranzitivní, ale není reflexivní ani symetrická. R je není uspořádání na X.

Příklad 1.6.3. Nechť $X = \{1, 2, 3, 4\}$, $R = \{(x, y) | \, x, y \in X, x = y\}$. Pak R je reflexivní, symetrická, antisymetrická a tranzitivní. R je ekvivalence i uspořádání na X.

Příklad 1.6.4. Nechť $X = \{1, 2, 3, 4\}$, $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (2, 4), (4, 2), (1, 3), (3, 1)\}$. Relace R je reflexivní, symetrická i tranzitivní, tj. je ekvivalencí na X. Není však antisymetrická, proto to není uspořádáním na X.

Softwarové nástroje: Binární relace na množině

Definice 1.6.2. Buď X množina a $\mathfrak{S}$ soubor podmnožin množiny X ($\mathfrak{S}$ je tzv. gotické S). Jestliže $\bigcup \mathfrak{S} = X$ a soubor $\mathfrak{S}$ je po dvou disjunktní (tj. libovolné dvě množiny z $\mathfrak{S}$ mají prázdný průnik), nazývá se $\mathfrak{S}$ *rozkladem na množině* X.



Obr. 1.6.1 Rozklad na množině

Buď R binární relace na X. Abychom zjednodušili způsob zápisu, budeme někdy psát xRy místo $(x, y) \in R$.

Věta 1.6.1. *Buď $\mathfrak{S}$ rozklad na X. Definujme xRy pro všechna taková $x, y \in X$, že $x, y \in S$ pro nějakou množinu $S \in \mathfrak{S}$. Potom relace R je relací ekvivalence na množině X.*

Důkaz. Prověříme reflexivitu, symetrii a tranzitivitu relace R. Buď $x \in X$. Protože $X = \bigcup \mathfrak{S}$, $x \in S$ pro nějakou $S \in \mathfrak{S}$. Tedy xRx, tj. relace R je reflexivní. Předpokládejme, že xRy. Pak x, y patří do nějaké množiny $S \in \mathfrak{S}$. Z toho plyne, že i y, x patří do téže množiny S, čili yRx. To znamená, že R je symetrická. Konečně, nechť xRy a yRz. Pak existují množiny $S, T \in \mathfrak{S}$, že $x, y \in S$ a $y, z \in T$. Tedy $y \in S \cap T$. Protože však je $\mathfrak{S}$ po dvou disjunktní systém, musí být $S = T$. Proto i x, z patří do stejné množiny S rozkladu $\mathfrak{S}$, takže xRz. Tedy R je tranzitivní. Ověřili jsme, že R je ekvivalencí na X.

□

Relace R z 1.6.1 se nazývá *ekvivalence určená rozkladem* $\mathfrak{S}$.

Věta 1.6.2. *Buď R ekvivalence na množině X. Pro každé $a \in X$ klademe*

$$[a] = \{x | x \in X,\ xRa\}.$$

Potom

$$\mathfrak{S} = \{[a] | a \in X\}$$

je rozkladem na X.

Důkaz. Musíme ověřit, že $X = \bigcup \mathfrak{S}$ a že $\mathfrak{S}$ je po dvou disjunktní. Buď $a \in X$. Protože aRa, je $a \in [a]$. Tedy $X = \bigcup \mathfrak{S}$.

Zbývá ověřit, že $\mathfrak{S}$ je po dvou disjunktní systém. Nechť pro nějaké $a, b \in X$ je $[a] \cap [b] \neq \varnothing$. Pak existuje $c \in [a] \cap [b]$. Tedy cRa, cRb. Ze symetrie plyne, že aRc, což spolu s cRb dává užitím tranzitivity aRb. Buď nyní $x \in [a]$. Pak xRa a aRb, odtud xRb. Tedy $x \in [b]$. Potom však $[a] \subseteq [b]$. Je-li naopak $y \in [b]$, analogicky yRb, což spolu s bRa dává yRa, takže $y \in [a]$. Tedy $[b] \subseteq [a]$. Celkem dostáváme $[a] = [b]$. Tím je dokázáno, že $\mathfrak{S}$ je tvořen po dvou disjunktními množinami, tedy $\mathfrak{S}$ je rozklad na X.

□

Množiny $[a] = \{x | x \in X, xRa\}$ se nazývají *třídy rozkladu* příslušného k ekvivalenci R.

Příklad 1.6.5. Buď $X = \{1, 2, \ldots, 10\}$. Nechť je dána relace $R = \{(x, y) |\, x, y \in X, 3 \text{ dělí } x - y\}$. Je snadné ověřit, že R je reflexivní, symetrická a tranzitivní, a tedy je ekvivalencí na X. Pak

$$[1] = [4] = [7] = [10] = \{1, 4, 7, 10\},$$
$$[2] = [5] = [8] = \{2, 5, 8\},$$
$$[3] = [6] = [9] = \{3, 6, 9\}.$$

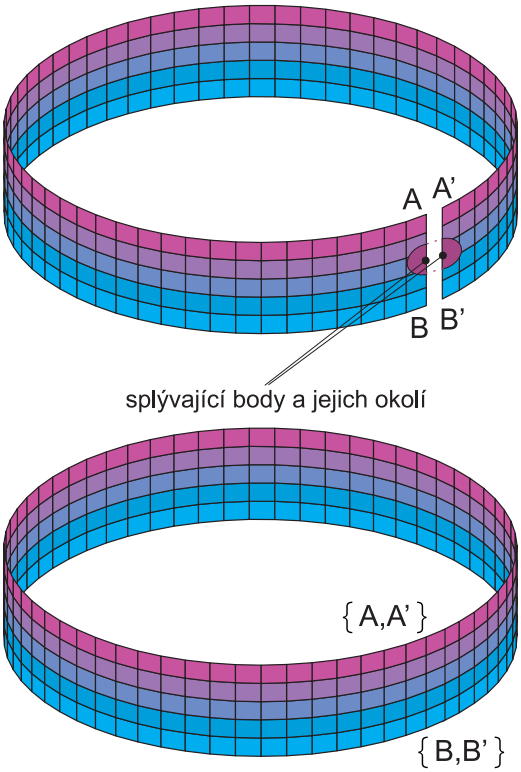
Ekvivalence a rozklady vlastně mění rozlišení v náhledu na původně definovaný objekt. Původní prvky jsou nahrazeny třídami ekvivalence, čímž vzniká nový objekt, nebo se alespoň mění náhled na objekt původní podobně, jako když na obrazovce počítače snížíme grafické rozlišení – některé pixely splynou. Pokud je ekvivalence vhodně volena, určitá závislost či zákonitost, kterou chceme pozorovat, zůstává zachována, ale celkový pohled se zjednoduší, neboť máme méně nových prvků – tříd ekvivalence. V předchozím příkladě jsme například modelovali dělitelnost třemi, původně na desetiprvkové množině, ale zjistili jsme, že podstatné jsou pouze tři třídy ekvivalence, vlastně určené zbytkem po dělení.

Příklad 1.6.6. Mějme obdélník $\langle 0, 2\rangle \times \langle 0, 1\rangle$ v reálné rovině. Pokud na jeho hranách, rovnoběžných s osou y ztotožníme prvky ve stejné výšce, po opatření vhodnou topologií dostáváme válcovou plochu

$$\mathfrak{V} = \{\{(x, y)\} | 0 < x < 2, 0 \leq y \leq 1\} \cup \{\{(0, y), (2, y)\} | 0 \leq y \leq 1\}$$

Následující obrázek ilustruje "slepení" obdélníka na válec. Aniž bychom si dělali nároky na matematickou přesnost, můžeme říci, že "slepení" zhruba spočívá v ztotožnění bodů, které padnou do téže třídy rozkladu a konstrukci otevřených okolí těmto novým bodům.

Za "nové" body můžeme dokonce považovat samotné třídy rozkladu. Vzniklý objekt je definovaný abstraktně a nelze ho dále považovat za součást reálné roviny s její Eukleidovou topologií. Potřebujeme jednu dimenzi navíc, abychom mohli obdélník "ohnout" a slepit. V označení z obrázku je $A = (0, 1)$, $A' = (2, 1)$, $B = (0, 0)$ a $B' = (0, 2)$.

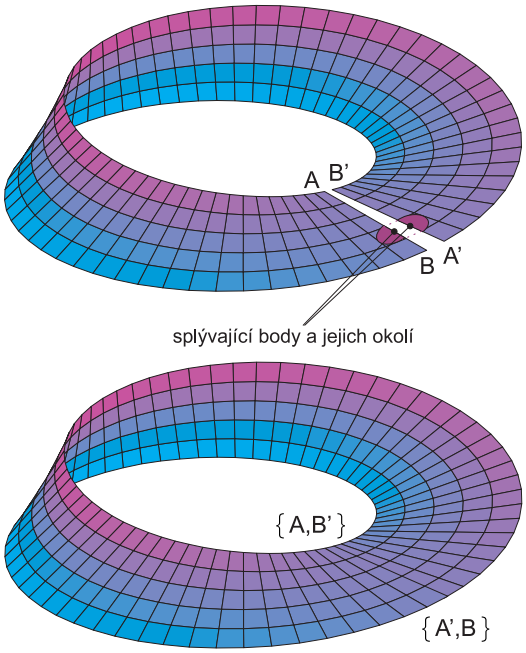


Obr. 1.6.2 Body válcové plochy jako třídy rozkladu obdélníka

Analogickou konstrukcí, avšak pokud výšku měříme na každé z obou hran čtverce z opačné základny, dostáváme – po opatření vhodnou topologií – tzv. Mőbiův pruh

$$\mathfrak{M} = \{\{(x, y)\}|0 < x < 2, 0 \leq y \leq 1\} \cup \{\{(0, y), (2, 1 - y)\}|0 \leq y \leq 1\}.$$

Dvouprvkové třídy ekvivalence značí ztotožněné či "slepené" body, jednoprvkové třídy odpovídají vnitřním bodům původního obdélníka a jeho základen.



Obr. 1.6.3 Body Mőbiovy plochy jako třídy rozkladu obdélníka

Příklad 1.6.7. Na množině Z celých čísel definujme ekvivalenci R způsobem podobným příkladu 1.6.5: $xRy \iff n$ dělí $x - y$. Příslušné třídy rozkladu se nazývají *zbytkové třídy*. Na těchto třídách lze definovat sčítání i násobení:

$$[x] + [y] := [x + y], \quad [x] \cdot [y] := [x \cdot y].$$

Množinu tříd ekvivalence označíme $\mathbb{Z}_n$. Například pro $n = 5$ vystačíme s reprezentanty tříd $0, 1, 2, 3, 4$. Vzniknou matematické struktury $(\mathbb{Z}_5, +)$, resp. $(\mathbb{Z}_5, +, \cdot)$, kde platí například

$$[1] + [2] = [3], \ [2] + [3] = [0], \ [2] \cdot [3] = [1], \text{ apod.}$$

Někdy se hranaté závorky vynechávají a pak nastává zajímavé počítání, zejména když někdo neví, že se počítá v grupě, resp. tělese zbytkových tříd.

Softwarové nástroje: Ekvivalence a rozklady na množině – rozklad příslušný ekvivalenci, Ekvivalence a rozklady na množině – ekvivalence příslušná rozkladu, Ekvivalence a rozklady na množině – výpis a počet ekvivalencí

Dalším a velmi důležitým typem binárních relací jsou relace uspořádání. Doplníme některé pojmy.

Definice 1.6.3. Buď X množina $R \subseteq X \times X$ relace uspořádání na X. Pak dvojici (X, R), či méně přesně množinu X nazýváme *uspořádanou množinou*. Pro relaci R pak často užíváme symbolu $\leq$, kde klademe $x \leq y \iff (x, y) \in R$. Je-li $x \leq y$ a $x \neq y$, píšeme $x < y$.

Definice 1.6.4. Buď $(X, \leq)$ uspořádaná množina. Říkáme, že uspořádání $\leq$ je *lineární* (nebo-li *úplné* jako protiklad částečného), jestliže pro každé $x, y \in X$ platí $x \leq y$ nebo $y \leq x$.

Příklad 1.6.8. $(\mathbb{N}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ jsou lineárně uspořádané množiny. Přitom $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ jsou uspořádány *hustě* : Je-li např. $r, s \in \mathbb{Q}$, $r < s$, pak např. $\frac{t=}{r+s2 \in \mathbb{Q}}$ a $r < t < s$. Tedy mezi libovolnými dvěma různými prvky z $\mathbb{Q}$ leží další prvek z $\mathbb{Q}$.

Příklad 1.6.9. Buď $A = \{1, 2, 3\}$, $X = 2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, A\}$. Množina $(X, \subseteq)$ je uspořádaná, ale není lineárně uspořádaná.

Příklad 1.6.10. Buď $M = \{1, 2, 3, 4, 5, 6\}$, $|$ relace dělitelnosti na M. Pak $(M, |)$ je uspořádaná, ale ne lineárně.

Definice 1.6.5. Buď $(X, \leq)$ uspořádaná množina. Nechť $a, b \in X$. Řekneme, že b *pokrývá* a, jestliže $a < b$ a neexistuje $x \in X$ takové, že $a < x < b$.

Příklad 1.6.11. V množině $(\mathbb{N}, \leq)$ 2 pokrývá 1, 7 pokrývá 6, ale 8 nepokrývá 5.

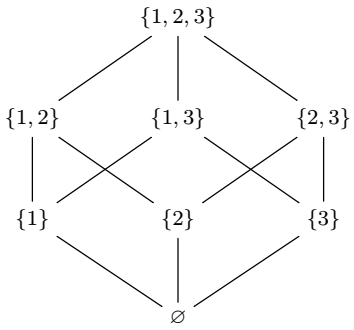
Příklad 1.6.12. Buď $A = \{1, 2, 3\}$, $X = 2^A$. V množině $(X, \subseteq)$ množiny $\{1\}$, $\{2\}$, $\{3\}$ pokrývají $\varnothing$, $\{1, 2\}$ pokrývá množiny $\{1\}$, $\{2\}$, A pokrývá množiny $\{1, 2\}$, $\{2, 3\}$, $\{1, 3\}$.

Je-li X konečná množina, lze prvky množiny X reprezentovat body v rovině, a to tak, že menší prvky jsou zakresleny níže než větší, přičemž pokrývaný prvek je s pokrývajícím spojen úsečkou. Vzniká tzv. *Hasseův diagram*.

Příklad 1.6.13. Buď $\mathbb{N}_4 = \{1, 2, 3, 4\}$ s přirozeným uspořádáním. Pak Hasseův diagram tohoto uspořádání má tvar

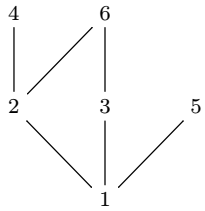
$(\mathbb{N}_4, \leq)$

Dále označme $A = \{1, 2, 3\}$, $X = 2^A$. V uspořádání X inkluzí je Hasseův diagram tvaru



$(X, \subseteq)$

Položme $M = \{1, 2, 3, 4, 5, 6\}$. Potom Hasseův diagram uspořádání M dělitelností je



$(M, |)$

Definice 1.6.6. Buď $(X, \leq)$ uspořádaná množina, $A \subseteq X$ podmnožina. Řekneme, že $a \in X$ je *horní závorou* (resp. *dolní závorou*) množiny A, jestliže pro všechna $x \in A$ je $x \leq a$ (resp. $a \leq x$). Existuje-li mezi všemi horními závorami množiny A nejmenší, označujeme ji $\sup A$ a nazýváme *suprémem* množiny A. Naopak, existuje-li největší dolní závora množiny A, označujeme ji $\inf A$ a nazýváme *infimem* množiny A.

Příklad 1.6.14. Uvažujme $(\mathbb{R}, \leq)$ a buď $I = (0, 1)$. Pak $\sup I = 1$, $\inf I = 0$. Všimněte si, že $\sup I$ nebo $\inf I$ nemusí být prvkem množiny I!

Příklad 1.6.15. Nechť $A = \{1, 2, 3\}$, $X = 2^A$. Pak $(X, \subseteq)$ je uspořádaná množina. Pro $B = \{\{1\}, \{3\}\}$ máme $\sup B = \{1, 3\}$, $\inf B = \varnothing$; pro $C = \{\{1, 2\}, \{2, 3\}\}$ je $\sup C = A$, $\inf C = \{2\}$; pro $D = \{\{1, 2\}, \{2, 3\}, \{3\}\}$ máme $\sup D = A$, $\inf D = \varnothing$.

Buď $(X \leq)$ uspořádaná množina, $A \subseteq X$. Má-li A největší prvek, je tento zároveň suprémem množiny A. Opak však obecně neplatí. Podobně má-li A nejmenší prvek, je tento současně infimem množiny A. Opak rovněž obecně neplatí.

Věta 1.6.3. *V množině $\mathbb{R}$ reálných čísel má každá shora omezená množina suprémum a každá zdola omezená množina infimum.*

Větu uvádíme bez důkazu. Příslušný důkaz by byl totiž závislý na způsobu zavedení reálných čísel. Reálná čísla je v zásadě možno zavést axiomaticky a pak je tvrzení věty jedním z axiomů, který se nedokazuje, nebo některou z metod zúplnění množiny racionálních čísel, což však přesahuje požadovaný rozsah tohoto učebního textu. Proto se spokojíme s pouhým konstatováním uvedeného tvrzení a případného zájemce z řad studentů odkazujeme na literaturu.

Definice 1.6.7. Buď $(X, \leq)$ uspořádaná množina. Prvek $m \in X$ se nazývá *maximálním* (resp. *minimálním*) prvkem množiny X, jestliže v X neexistuje prvek větší (resp. menší) než on.

Příklad 1.6.16. Uvažujme $(M, |)$ z příkladu 1.6.10. Tato uspořádaná množina má tři maximální prvky $4, 5, 6$, žádný z nich však není největším prvkem. Dále má jeden minimální prvek 1, který je zároveň nejmenším prvkem množiny M.

Věta 1.6.4. *Buď $R \subseteq X \times X$ relace uspořádání na X. Pak také relace R^{-1} je uspořádáním na X (toto uspořádání se nazývá duální k $\leq$ a značíme jej symbolem $\geq$).*

Důkaz. Triviální, prověřením axiomů reflexivity, antisymetrie a tranzitivity.

□

Definice 1.6.8. Buď $(X, \leq)$ uspořádaná množina. Řekneme, že $(X, \leq)$ je *svazově uspořádaná*, jestliže každá dvouprvková podmnožina množiny X má v X supremum i infimum.

Příklad 1.6.17. $(M, |)$ je uspořádaná, ale není svazově uspořádaná, protože např. podmnožina $\{3, 4\}$ nemá v M supremum.

Příklad 1.6.18. $Y = \{\{1, 2, 3\}, \{1, 2\}, \{2, 3\}, \{2\}, \{3\}, \varnothing\}$, $(Y, \subseteq)$ je svazově uspořádaná: např. $\sup\{\{2\}, \{3\}\} = \{2, 3\}$, $\inf\{\{1, 2\}\{2, 3\}\} = \{2\}$.

Softwarové nástroje: Uspořádání na množině

Cvičení

1.6.1. Na množině $X = \{1, 2, 3, 4, 5\}$ jsou dány relace
$P = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1)\}$,
$Q = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (3,4), (4,3)\}$,
$R = \{(1,1), (2,2), (3,3), (4,4)\}$,
$S = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,5), (5,1), (3,5), (5,3), (1,3), (3,1)\}$,
$T = X^2$.
Určete, které z nich jsou relacemi ekvivalence na X a v kladných případech sestrojte příslušné rozklady množiny X.

1.6.2. K rozkladům množiny $X = \{1, 2, 3, 4\}$ najděte odpovídající ekvivalence na X:
$\mathfrak{P} = \{\{1,2\}, \{3,4\}\}$,
$\mathfrak{Q} = \{\{1\}, \{2\}, \{3,4\}\}$,
$\mathfrak{R} = \{\{1,2,3\}, \{4\}\}$,
$\mathfrak{S} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$,
$\mathfrak{T} = \{\{1,2,3,4\}\}$.

1.6.3. Najděte všechny ekvivalence na množině o 2, 3 a 4 prvcích.

1.6.4. Nechť $X = \{(a,b) | \, a, b \in \mathbb{Z}, b \neq 0\}$. Definujeme $(a,b)R(c,d)$ právě když $ad = bc$. Dokažte, že R je ekvivalence na množině X. Jakou známou množinu tvoří třídy ekvivalence?

1.6.5. * Nalezněte obecné vztahy pro nejmenší reflexivní relaci $\rho(Q)$, nejmenší symetrickou relaci $\sigma(Q)$, nejmenší tranzitivní relaci $\tau(Q)$ a nejmenší ekvivalenci $\epsilon(Q)$ obsahující danou relaci Q. Tyto vztahy dokažte. Relacím $\rho(Q)$, $\sigma(Q)$, $\tau(Q)$ se říká po řadě *reflexivní, symetrický a tranzitivní uzávěr* relace Q.

1.6.6. Řešte úlohu 5 pro konkrétní relaci $Q = \{(1,2), (2,1), (3,1), (4,5), (5,5)\}$ na $X = \{1, 2, 3, 4, 5\}$.

1.6.7. Nechť E_1, E_2 jsou ekvivalence na X. Dokažte, že $E_1 \cap E_2$ je ekvivalence na X.

1.6.8. Nechť R je reflexivní a tranzitivní relace na X. Dokažte, že $R \cap R^{-1}$ je ekvivalence na X.

1.6.9. Dokažte nebo vyvraťte protipříkladem pro libovolné dvě relace R_1, R_2 na množině X:
$\rho(R_1 \cup R_2) = \rho(R_1) \cup \rho(R_2)$,
$\sigma(R_1 \cap R_2) = \sigma(R_1) \cap \sigma(R_2)$,
$\tau(R_1 \cup R_2) = \tau(R_1) \cup \tau(R_2)$,
$\tau(R_1 \cap R_2) = \tau(R_1) \cap \tau(R_2)$,
$\sigma(\tau(R_1)) = \tau(\sigma(R_1))$,
$\sigma(\rho(R_1)) = \rho(\sigma(R_1))$,
$\rho(\tau(R_1)) = \tau(\rho(R_1))$.

1.6.10. Na množině $X = \{1, 2, 3, 4, 5, 6\}$ jsou dány relace
$P = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,5), (2,6), (3,3), (3,5), (3,6), (4,4), (4,5), (5,5), (6,5), (6,6)\}$,
$Q = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,5), (3,3), (3,5), (3,6), (4,4), (4,5), (5,5), (6,5), (6,6)\}$,
$R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,5), (3,6), (4,4), (4,5), (5,5), (6,5), (6,6)\}$,
$S = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,5), (3,3), (3,5), (3,6), (4,4), (4,5), (5,5), (6,5), (6,6)\}$,
$T = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$,
$U = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,5), (2,6), (3,3), (3,4), (3,5), (3,6), (4,4), (4,5), (5,5), (6,5), (6,6)\}$,
Rozhodněte, které z nich jsou uspořádání na X. V kladném případě nakreslete Hasseův diagram.
Která z těchto uspořádání jsou svazová?

1.6.11. * Buď (X, τ) topologický prostor. Pro libovolné $x, y \in X$ klademe $x \leq y$, právě když každé otevřené okolí bodu x obsahuje bod y. Dokažte, že relace $\leq$ je kvaziuspořádání. Toto kvaziuspořádání se nazývá *specializace* prostoru (X, τ). Zformulujte ekvivalentní podmínku, kterou musí splňovat prostor (X, τ), aby jeho specializace byla uspořádáním. Tato podmínka se nazývá T_0*-axiom* a prostor, který ji splňuje, se nazývá T_0*-prostor*.

1.6.12. Nechť $X = \{1, 2, 3, 4, 5\}$ a τ buď topologie na X indukovaná z Khalimského přímky. Ověřte, zda je prostor (X, τ) T_0-prostorem. Pokud ano, nakreslete Hasseův diagram jeho specializace.

1.6.13. Uvažujte množinu $\mathcal{E}_n$ všech ekvivalencí na množině o $n = 3$ prvcích s uspořádáním inkluzí. Nakreslete její Hasseův diagram a rozhodněte, zda je $(\mathcal{E}_3, \subseteq)$ svazově uspořádaná.

1.6.14. * Opakujte předchozí cvičení pro $n = 4$.

1.6.15. Uvažujte množinu $\mathcal{T}_n$ všech topologií na množině o $n = 2$ prvcích s uspořádáním inkluzí. Nakreslete její Hasseův diagram a rozhodněte, zda je $(\mathcal{T}_2, \subseteq)$ svazově uspořádaná.

1.6.16. * Opakujte předchozí cvičení pro $n = 3$.

Počítačová cvičení

1.6.17. Napište program, který reprezentuje množinové operace $X \cup Y$, $X \cap Y$, $X \setminus Y$, $X \div Y$ pro dvě uživatelem zadané konečné množiny X, Y.

1.6.18. Napište program, který nalezne všechny podmnožiny zadané konečné množiny.

1.6.19. Napište program, který o zadané binární relaci zjistí, zda je tato relace zobrazení a v kladném případě zjistí, zda je toto zobrazení injektivní, surjektivní nebo bijektivní.

1.6.20. Napište program, který zjistí, zda zadaný konečný soubor množin τ na zadané konečné množině X je topologie.

1.6.21. Napište program, který zjistí, zda zadaný konečný soubor množin τ_0 na zadané konečné množině X je báze jisté topologie.

1.6.22. Napište program, který zjistí, zda dané zobrazení mezi dvěma zadanými konečnými topologickými prostory je spojité.

1.6.23. Napište program, který zjistí, zda je zadaná binární relace na konečné množině reflexivní, symetrická, antisymetrická, tranzitivní.

1.6.24. Napište program, který zjistí, zda je zadaná binární relace na konečné množině tolerance, ekvivalence, kvaziuspořádání, uspořádání.

1.6.25. Napište program, který zjistí, zda je zadaná binární relace na konečné množině X svazové uspořádání a v kladném případě ověří, zda je tento svaz komplementární – tedy že ke každému $x \in X$ existuje prvek $y \in X$, že $\sup\{x, y\}$ je největším prvkem a $\inf\{x, y\}$ je nejmenším prvkem množiny X v zadaném uspořádání.

Pojmy k zapamatování

- Množina. Mohutnost množiny.
- Množinové operace. Sjednocení, průnik, rozdíl, symetrická diference. Kartézský součin.
- Binární relace jako podmnožina kartézského součinu.
- Zobrazení jako binární relace. Injekce, surjekce, bijekce.
- Topologie. Systém otevřených množin. Body vnitřní, hraniční a vnější. Topologický uzávěr.
- Spojitost jako přenos vlastností otevřených množin.
- Reflexivnost, symetrie, antisymetrie a tranzitivnost binárních relací. Relační uzávěry.
- Ekvivalence a rozklady.
- Uspořádání. Pokrývání prvku. Hasseovský diagram. Svazové uspořádání.

Klíčové myšlenky kapitoly

- Velikost množin porovnáváme pomocí zobrazení - zejména injekcí a bijekcí.
- Spojité zobrazení „přenáší" systém otevřených množin v opačném směru, než samo vede.
- Ekvivalence a rozklady spolu vzájemně jednoznačně souvisí.
- Uspořádání na množině svými vlastnostmi napodobuje přirozené uspořádání čísel, ale je na něm nezávislé.
- I čísla samotná mohou být uspořádána jinak, než podle velikosti, například vzájemnou dělitelností.
- Množiny mohou být uspořádány na základě toho, jak jedna druhou obsahuje - tedy inkluzí.

Odkazy na literaturu

Převážnou část obsahu této kapitoly lze nalézt ve většině učebnic obecné algebry a diskrétní matematiky, například [15], [17], [34]. Výjimku tvoří topologická část, vycházející především z koncepce [42], kde lze také nalézt řadu informací k uspořádaným množinám v kontextu, který je informatice velice blízký. Dalšími oporami pro topologickou část je standardní a velmi rozsáhlá monografie [4]. Rozšiřující poznatky směrem k digitální topologii čtenář nalezne například v [13]. Všechny citace se vztahují k seznamu literatury na konci učebního textu. Uvedeny jsou zde učebnice a monografie, obsahující nebo rozšiřující partie probírané v této kapitole.

[3], [5], [4], [9], [10], [12], [13], [15], [17], [20], [21], [26], [27], [33], [32], [34], [35], [36], [37], [42]

Další příklady k procvičení

Elektronická banka příkladů

Matematický software

Množinové operace
Binární relace a zobrazení
Topologie na konečné množině
Topologie na konečné množině – výpis a počet
Spojitost zobrazení
Binární relace na množině
Ekvivalence a rozklady na množině – rozklad příslušný ekvivalenci
Ekvivalence a rozklady na množině – ekvivalence příslušná rozkladu
Ekvivalence a rozklady na množině – výpis a počet
Uspořádání na množině

2 Struktury s operacemi na množině

V této kapitole se zabýváme převážně algebrami různého typu - množinami, vybavenými obecně jednou nebo více operacemi a jejich morfismy. Mezi algebrami s jednou operací prozkoumáme především grupy. Jako reprezentantům algeber se dvěma operacemi budeme hlavní pozornost věnovat svazům. Konec kapitoly věnujeme Booleovým algebrám.

Cíle

Po prostudování této kapitoly budete schopni:

- rozlišit vybrané algebraické struktury včetně vlastností jejich objektů a morfismů
- vyšetřovat vlastnosti operací na množině
- vytvářet faktorové algebry
- vyšetřovat vlastnosti algeber s jednou a dvěma operacemi
- pracovat se svazovým uspořádáním jako s algebrou
- vyšetřovat vlastnosti svazů
- vyšetřovat vlastnosti Booleových algeber

2.1 Kategorie

Definice 2.1.1. *Kategorií* nazýváme uspořádanou pětici $\mathfrak{K} = (\mathfrak{O}, \mathfrak{M}, \mathrm{Dom}\,, \mathrm{Im}\,, \circ)$, kde $\mathfrak{O}, \mathfrak{M}$ jsou nějaké třídy, Dom a Im jsou zobrazení definovaná na $\mathfrak{M}$ s hodnotami v $\mathfrak{O}$, $\circ$ je operace, která libovolným dvěma $f, g \in \mathfrak{M}$ takovým, že $\mathrm{Dom}\, g = \mathrm{Im}\, f$, přiřazuje prvek $g \circ f \in \mathfrak{M}$. Prvky třídy $\mathfrak{O}$ se nazývají *objekty* kategorie $\mathfrak{K}$, prvky třídy $\mathfrak{M}$ *morfismy* kategorie $\mathfrak{K}$. Je-li $f \in \mathfrak{M}$, pak $\mathrm{Dom}\, f \in \mathfrak{O}$ se nazývá *oborem* morfismu f, $\mathrm{Im}\, f \in \mathfrak{O}$ se nazývá *kooborem* morfismu f. Operace $\circ$ je operací *skládání morfismů*.

Pojem *třída* použitý v předchozí definici je teoreticko-množinový. Pro naše účely postačí vědět, že jde o souhrn prvků, který může být obecně rozsáhlejší, než jsou množiny. Například objekt $\mathcal{N}$ z 1.1 je třída, která není množinou.

Příklad 2.1.1. Jedním ze základních příkladů kategorie je Set (objekty jsou zde množiny, morfismy jsou zde zobrazení, $\circ$...operace skládání zobrazení).

Definice 2.1.2. Množinu $\mathfrak{D}$ objektů a morfismů z kategorie $\mathfrak{K}$ nazýváme *diagramem* v $\mathfrak{K}$, jestliže s každým morfismem $f : A \to B$ z $\mathfrak{D}$ také objekty A, B a identické morfismy id_A a id_B patří do $\mathfrak{D}$. Diagram $\mathfrak{D}$ nazýváme *komutativním*, jestliže pro libovolné dvě posloupnosti morfismů

$$A \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \dots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} B$$

a

$$A \xrightarrow{g_1} B_1 \xrightarrow{g_2} B_2 \xrightarrow{g_3} \dots \xrightarrow{g_{m-1}} B_{m-1} \xrightarrow{g_m} B$$

platí

$$f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1 = g_m \circ g_{m-1} \circ \cdots \circ g_2 \circ g_1.$$

Příklad 2.1.2.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ C & \xrightarrow{k} & D \end{array}$$

Tento diagram komutuje, když $h \circ f = k \circ g$.

Cvičení

2.1.1. V příkladě 2.1.1 jsme uvedli, že třída všech množin spolu se zobrazeními tvoří kategorii. Jmenujte ještě alespoň dvě další kategorie. Co tvoří v těchto kategoriích třídu objektů a co jsou v nich morfismy?

2.2 Algebry

Definice 2.2.1. Buď A množina a $\omega : A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ krát}} \to A$ zobrazení. Pak ω nazýváme *n-ární operací* na A. Číslo n nazýváme *četností (aritou)* operace ω.

Příklad 2.2.1. $A = \mathbb{R}$, $\omega = +$, $\omega(a, b) = a + b$ je binární operace na $A = R$ (arita $n = 2$). Příklad unární operace ($n = 1$): výběr komplementárního prvku ve svazově uspořádané množině. Příklad nulární operace ($n = 0$): výběr největšího prvku ve svazově uspořádané množině.

Definice 2.2.2. Buď A množina, $\omega_1, \omega_2, \ldots, \omega_k$ operace na A s četnostmi (aritami) $n_1, n_2, \ldots, n_k$. Pak $(k+1)$-tici $(A, \omega_1, \omega_2, \ldots, \omega_k)$ nazýváme *algebrou*. Zkráceně označujeme tuto algebru jen symbolem A její nosné množiny a hovoříme o algebře A.

Příklad 2.2.2. $(\mathbb{R}, +, \cdot)$ je algebra se dvěma binárními operacemi.

Příklad 2.2.3. Nechť X je nějaká množina. Pak $(2^X, \cup, \cap)$ je algebra se dvěma binárními operacemi.

Definice 2.2.3. Buďte $(A, \alpha_1, \alpha_2, \ldots, \alpha_k)$ a $(B, \beta_1, \beta_2, \ldots, \beta_k)$ dvě algebry se stejnými četnostmi n_i operací α_i,β_i pro $i = 1, 2, \ldots, k$. Nechť $h : A \to B$ je zobrazení takové, že pro libovolné $i \in \{1, 2, \ldots, k\}$ a $x_1, x_2, \ldots, x_{n_i} \in A$ platí

$$h(\alpha_i(x_1, x_2, \ldots, x_{n_i})) = \beta_i(h(x_1), h(x_2), \ldots, h(x_{n_i})).$$

Pak h se nazývá *morfismem* algebry A do algebry B.

Graficky lze předchozí definici vyjádřit následujícím komutativním diagramem pro $i = 1, 2, \ldots, k$:

$$\begin{array}{ccc} A^{n_i} & \xrightarrow{h^{n_i}} & B^{n_i} \\ {\scriptstyle \alpha_i}\downarrow & & \downarrow{\scriptstyle \beta_i} \\ A & \xrightarrow{h} & B \end{array}$$

Pro názvosloví morfismů platí následující označení:

(i) *monomorfismus*...injektivní morfismus

(ii) *epimorfismus*...surjektivní morfismus

(iii) *izomorfismus*...bijektivní morfismus

(iv) *endomorfismus*...morfismus algebry A do A

(v) *automorfismus*...izomorfismus A na A

Příklad 2.2.4. Položme $A = \mathbb{R}$, $B = \mathbb{R} \setminus \{0\}$, $h = e^x$. Pak $h : A \to B$ je morfismem algeber $(A, +, -)$ a $(B, \cdot, ^{-1})$, neboť platí

$$h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot h(y);$$

$$h(-x) = e^{-x} = (e^x)^{-1} = (h(x))^{-1}.$$

Dále, h je monomorfismus, neboť e^x je prosté neboli injektivní zobrazení.

Příklad 2.2.5. Nechť $A = \mathbb{R}$, $f(x) = -x$. Pak f je automorfismus algebry $(\mathbb{R}, +)$ na sebe. Vskutku,

$$f(x + y) = -(x + y) = (-x) + (-y) = f(x) + f(y),$$

takže f je morfismus. Ale navíc f je bijekce, tedy izomorfismus $(\mathbb{R}, +)$ na $(\mathbb{R}, +)$, čili automorfismus.

Definice 2.2.4. Buď $(A, \omega_1, \omega_2, \ldots, \omega_k)$ algebra a nechť $B \subseteq A$ je taková podmnožina, že pro libovolné $i \in \{1, 2, \ldots, k\}$ a $x_1, x_2, \ldots, x_{n_i} \in B$ je $\omega_i(x_1, x_2, \ldots x_{n_i}) \in B$ (n_i je četnost operace ω_i). Pak algebru $(B, \omega_1, \omega_2, \ldots, \omega_k)$ nazýváme podalgebrou algebry $(A, \omega_1, \ldots, \omega_k)$.

Příklad 2.2.6. Jestliže $\mathbb{S} \subseteq \mathbb{Z}$ jsou sudá čísla, pak $(\mathbb{S}, +, \cdot)$ je podalgebrou algebry $(\mathbb{Z}, +, \cdot)$.

Softwarové nástroje: Algebry s jednou operací

Cvičení

2.2.1. Najděte všechny algebry s jednou operací na množině $\{0, 1\}$.

2.2.2. Nechť $A = \{1, 2\}$ a $X = 2^A$. Najděte všechny podalgebry algebry $(X, \cup, \cap)$.

2.2.3. * Buď $X = \mathbb{N} \cup \{0\}$ a nechť $a \diamond b = b + 1$ pro všechna $a, b \in X$. Určete všechny neprázdné podalgebry algebry $(X, \diamond)$. Jaký je jejich společný průnik?

2.2.4. Dokažte, že průnik libovolného souboru podalgeber algebry A je buď prázdný, nebo opět podalgebra algebry A.

2.3 Faktorové algebry

Definice 2.3.1. Buďte X, Y množiny, $f : X \to Y$ zobrazení. *Jádrem* zobrazení f nazýváme relaci $\operatorname{Ker} f = f^{-1} \circ f$.

Věta 2.3.1. *Nechť $f : X \to Y$ je zobrazení. Pak* $\operatorname{Ker} f$ *je ekvivalence.*

Důkaz. Ukážeme, že relace $\operatorname{Ker} f \subseteq X \times X$ je reflexivní, symetrická a tranzitivní.

(i) Buď $x \in X$ a označme $y := f(x)$. Pak $(x, y) \in f$, takže $(y, x) \in f^{-1}$, odkud $(x, x) \in f^{-1} \circ f = \operatorname{Ker} f$. Tedy $\operatorname{Ker} f$ je reflexivní.

(ii) Zvolme libovolně $(x, y) \in \operatorname{Ker} f$. Pak $(x, y) \in f^{-1} \circ f$, čili existuje $z \in X$, že $(x, z) \in f$ a $(z, y) \in f^{-1}$, odkud $(z, x) \in f^{-1}$ a $(y, z) \in f$. Pak ovšem $(y, x) \in f^{-1} \circ f = \operatorname{Ker} f$. Tedy relace $\operatorname{Ker} f$ je symetrická.

(iii) Nechť $(x, y) \in \operatorname{Ker} f$ a $(y, z) \in \operatorname{Ker} f$. Potom $(x, y) \in f^{-1} \circ f$ a $(y, z) \in f^{-1} \circ f$, tj. existují $u, v \in Y$, že $(x, u) \in f$, $(u, y) \in f^{-1}$, $(y, v) \in f$ a $(v, z) \in f^{-1}$. To však znamená, že $(y, u) \in f$ a $(z, v) \in f$, odkud dohromady $f(x) = u = f(y) = v = f(z)$. Zejména tedy $u = v$, takže $(x, u) \in f$ a $(u, z) \in f^{-1}$. Potom $(x, z) \in f^{-1} \circ f = \operatorname{Ker} f$. Tedy $\operatorname{Ker} f$ je tranzitivní.

Tím je důkaz hotov.

□

Poznamenejme, že dva prvky $x, y \in X$ jsou v relaci $\operatorname{Ker} f$ na X, právě když mají stejný obraz, tj. když $f(x) = f(y)$.

Příklad 2.3.1. Nechť $X = \{1, 2, 3, 4, 5, 6, 7\}$, $Y = \{a, b, c, d, e\}$ a $f = \{(1, a), (2, c), (3, a), (4, b), (5, d), (6, b), (7, a)\}$. Jádro zobrazení $\operatorname{Ker} f =$ je tvořeno prvky $(1, 1)$, $(1, 3)$, $(1, 7)$, $(2, 2)$, $(3, 1)$, $(3, 3)$, $(3, 7)$, $(4, 4)$, $(4, 6)$, $(5, 5)$, $(6, 4)$, $(6, 6)$, $(7, 1)$, $(7, 3)$, $(7, 7)$. Struktuře $\mathfrak{S} = X/\operatorname{Ker} f = \{\{1, 3, 7\}, \{2\}, \{4, 6\}, \{5\}\}$ se říká *faktorová množina* příslušná ekvivalenci R.

Definice 2.3.2. Buď $R \subseteq X \times X$ ekvivalence na X. Zobrazení $g : X \to X/R$ přiřazující prvku $x \in X$ třídu $[x]_R \in X/R$, tj. $g(x) = [x]_R$, se nazývá *přirozené* neboli *kanonické* zobrazení.

Věta 2.3.2. *Buď $f : X \to Y$ zobrazení, $g : X \to X/\mathrm{Ker}\, f$ kanonické zobrazení. Pak existuje jediné zobrazení $h : X/\mathrm{Ker}\, f \to Y$, že diagram komutuje, tj. že $f = h \circ g$, přičemž h je injektivní (a má stejný obor hodnot jako f). Speciálně, je-li f surjekce, je h bijekcí.*

Důkaz.

(i) Nechť $t \in X/\mathrm{Ker}\, f$ je libovolné. Pak existuje $x \in X$, že $t = g(x)$, tj. $t = [x]_{\mathrm{Ker}\, f}$. Klademe $h(t) := f(x)$. Protože na všech ostatních prvcích $y \in [x]_{\mathrm{Ker}\, f}$, má f stejnou hodnotu $f(y) = f(x) = h(t)$, je zobrazení $h : X/\mathrm{Ker}\, f \to Y$ korektně definováno.

(ii) Naopak, předpokládejme, že rovněž pro nějaké zobrazení $h' : X/\mathrm{Ker}\, f \to Y$ platí $f = h' \circ g$. Kanonické zobrazení g je zřejmě surjektivní a tedy h, h' mají na všech prvcích z $X/\mathrm{Ker}\, f$ stejné funkční hodnoty; tedy $h = h'$.

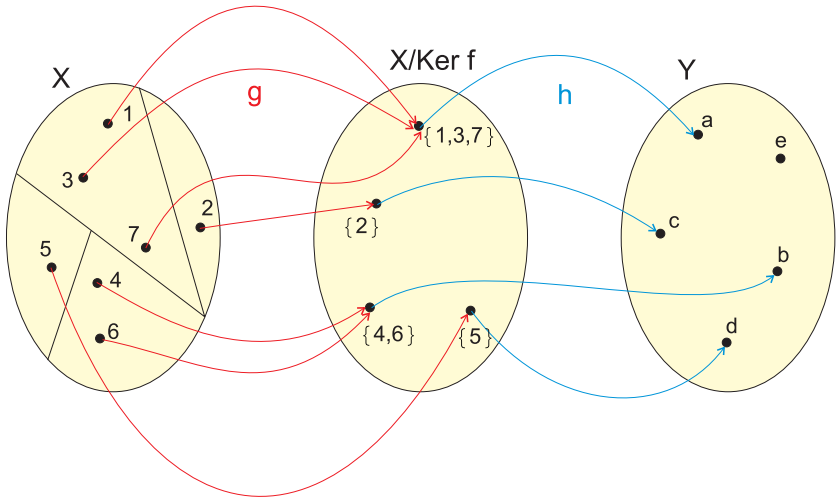
(iii) Ukážeme ještě, že h je injekce. Nechť $t_1, t_2 \in X/\mathrm{Ker}\, f$. Pak $t_1 = g(x_1) = [x_1]_{\mathrm{Ker}\, f}$ a $t_2 = g(x_2) = [x_2]_{\mathrm{Ker}\, f}$. Když $h(t_1) = h(t_2)$, pak ovšem $f(x_1) = h(g(x_1)) = h(t_1) = h(t_2) = h(g(x_2)) = f(x_2)$, takže $(x_1, x_2) \in \mathrm{Ker}\, f$, což dává $t_1 = [x_1]_{\mathrm{Ker}\, f} = [x_2]_{\mathrm{Ker}\, f} = t_2$, neboť $\mathrm{Ker}\, f$ je ekvivalence.

Tím je důkaz hotov.

□

Rozkladu zobrazení f na kompozici $f = h \circ g$ v předchozí větě se říká *faktorizace zobrazení* f (přes $X/\mathrm{Ker}\, f$).

Příklad 2.3.2. Nechť $f : X \to Y$ je stejné zobrazení jako v příkladě 2.3.1. Pak $f = h \circ g$, kde $g : X \to X/\mathrm{Ker}\, f$, $g = \{(1, \{1,3,7\}), (2, \{2\}), (3, \{1,3,7\}), (4, \{4,6\}), (5, \{5\}), (6, \{4,6\}), (7, \{1,3,7\})\}$ a $h : X/\mathrm{Ker}\, f \to Y$, $h = \{(\{1,3,7\}, a), (\{2\}, c), (\{4,6\}, b), (\{5\}, d)\}$ (viz. Obr. 2.3.1).



Obr. 2.3.1 Faktorizace zobrazení

Definice 2.3.3. Buď R ekvivalence na A a $(A, \omega_1, \omega_2, \ldots, \omega_k)$ algebra s operacemi $\omega_1, \omega_2, \ldots, \omega_k$ o četnostech $n_1, n_2, \ldots, n_k$. Řekneme, že R je *kongruence* na A, jestliže pro každé $i \in \{1, 2, \ldots, k\}$ a $x_1, x_2, \ldots, x_{n_i}$, $y_1, y_2, \ldots, y_{n_i}$ platí implikace

$$x_1 R y_1 \wedge x_2 R y_2 \wedge \cdots \wedge x_{n_i} R y_{n_i} \implies \omega_i(x_1, x_2, \ldots, x_{n_i}) R \omega_i(y_1, y_2, \ldots, y_{n_i}).$$

Věta 2.3.3. *Buď f libovolný morfismus algebry $(A, \alpha_1, \alpha_2, \ldots, \alpha_k)$ do algebry $(B, \beta_1, \beta_2, \ldots, \beta_k)$. Pak je relace $R = \operatorname{Ker} f$ kongruencí na A.*

Důkaz. Podle věty 2.3.1 je $\operatorname{Ker} f$ ekvivalence na A. Zbývá prověřit vlastnost kongruence.

Zvolme $i \in \{1, 2, \ldots, k\}$ libovolně, ale pro další úvahy pevně. Nechť pro nějaké $x_1, x_2, \ldots, x_{n_i}$, $y_1, y_2, \ldots, y_{n_i}$ platí $x_1 R y_1 \wedge x_2 R y_2 \wedge \cdots \wedge x_{n_i} R y_{n_i}$. Pak $f(x_1) = f(y_1)$, $f(x_2) = f(y_2)$, $\ldots$, $f(x_{n_i}) = f(y_{n_i})$. Potom však

$$f(\alpha_i(x_1, \ldots, x_{n_i})) = \beta_i(f(x_1), \ldots, f(x_{n_i})) =$$

$$= \beta_i(f(y_1), \ldots, f(y_{n_i})) = f(\alpha_i(y_1, \ldots, y_{n_i})).$$

To je ale přesně $\alpha_i(x_1, \ldots, x_{n_i}) R \alpha_i(y_1, \ldots, y_{n_i})$. Tedy $R = \operatorname{Ker} f$ je kongruencí na A. Tím je věta dokázána.

□

Definice 2.3.4. Buď $(A, \omega_1, \omega_2, \ldots, \omega_k)$ algebra a R kongruence na A. Pro libovolné $i \in \{1, 2, \ldots, k\}$ a $x_1, x_2, \ldots, x_{n_i} \in A$ klademe

$$\overline{\omega_i}([x_1]_R, [x_2]_R, \ldots, [x_{n_i}]_R) := [\omega_i(x_1, x_2, \ldots, x_{n_i})]_R.$$

Jelikož je R kongruencí, je korektně definována nová algebra s nosnou množinou A/R a operacemi $\overline{\omega_1}, \overline{\omega_2}, \ldots, \overline{\omega_k}$. Tuto algebru nazýváme *faktorovou algebrou* původní algebry A příslušnou kongruenci R.

Věta 2.3.4. *Buď $f : A \to B$ epimorfismus algebry $(A, \alpha_1, \alpha_2, \ldots, \alpha_k)$ na algebru $(B, \beta_1, \beta_2, \ldots, \beta_k)$. Pak je faktorová algebra $(A/\mathrm{Ker}\, f, \overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_k})$ izomorfní s algebrou $(B, \beta_1, \beta_2, \ldots, \beta_k)$.*

Důkaz. Podle věty 2.3.2 existuje jediné (a bijektivní) zobrazení $h : A/\mathrm{Ker}\, f \to B$, že diagram komutuje ($g$ je kanonické zobrazení, h je injekce podle věty 2.3.2 a jelikož je f epimorfismus, je h také surjektivní, a tedy bijekce). Zbývá ukázat, že je h morfismem algeber $A/\mathrm{Ker}\, f$ a B. Nechť $i \in \{1, 2, \ldots, k\}$ a $x_1, x_2, \ldots, x_{n_i} \in A$. Pak

$$h(\overline{\alpha_i}([x_1], [x_2], \ldots, [x_{n_i}])) = h([\alpha_i(x_1, x_2, \ldots, x_{n_i})]) =$$

$$= h \circ g(\alpha_i(x_1, x_2, \ldots, x_{n_i})) = f(\alpha_i(x_1, x_2, \ldots, x_{n_i})) =$$

$$= \beta_i(f(x_1), f(x_2), \ldots, f(x_{n_i})) = \beta_i(h \circ g(x_1), h \circ g(x_2), \ldots, h \circ g(x_{n_i})) =$$

$$= \beta_i(h([x_1]), h([x_2]), \ldots, h([x_{n_i}])),$$

takže h je vskutku morfismus. Protože h je také bijekcí, je h izomorfismus algeber. Tím je věta dokázána.

□

Softwarové nástroje: Kongruence na algebrách s jednou operací

Cvičení

2.3.1. Nechť $A = \{a, b\}$ a $a \diamond a = b$, $a \diamond b = b \diamond a = b \diamond b = a$. Najděte všechny kongruence na A. K nim sestrojte příslušné faktorové algebry.

2.3.2. Nechť $A = \mathbb{Z}$, $R = \{(x, y) | x, y \in Z,\ 5|x - y\}$. Dokažte, že R je kongruencí na $(A, +, \cdot)$. (Návod: když $x_1 R y_1 \wedge x_2 R y_2$, pak $x_1 = 5p_1 + r_1, x_2 = 5p_2 + r_2, y_1 = 5q_1 + r_1, y_2 = 5q_2 + r_2$.)

2.3.3. Sestrojte faktorovou algebru A/R z předchozí úlohy.

2.3.4. Položme $X = \{0, 1, 2, 3, 4, 5\}$ a $Y = \{0, 1, 2\}$. Dále klademe $x_1 \oplus x_2 = (x_1 + x_2) \mod 6$, $x_1 \odot x_2 = (x_1 \cdot x_2) \mod 6$, $y_1 \boxplus y_2 = (y_1 + y_2) \mod 3$ a $y_1 \boxdot y_2 = (y_1 \cdot y_2) \mod 3$ pro všechna $x_1, x_2 \in X$ a $y_1, y_2 \in Y$. Dokažte, že $f : X \to Y$, kde $f(x) = x \mod 3$ je morfismus algeber $(X, \oplus, \odot)$ a $(Y, \boxplus, \boxdot)$.

2.3.5. V předchozím příkladě nalezněte $\operatorname{Ker} f$ a sestrojte faktorovou algebru $X/\operatorname{Ker} f$. Faktorizujte zobrazení f přes faktorovou algebru.

2.3.6. Opakujte cvičení 4 a 5 pro $Y = \{0, 1\}$, $y_1 \boxplus y_2 = (y_1 + y_2) \mod 2$, $y_1 \boxdot y_2 = (y_1 \cdot y_2) \mod 2$ a $f(x) = x \mod 2$.

2.4 Algebry s jednou a dvěma binárními operacemi

Definice 2.4.1. Nechť $(A, *)$ je algebra s binární operací $*$. Pak $(A, *)$ se nazývá *grupoid*. Řekneme, že $(A, *)$ je *pologrupa*, jestliže operace $*$ splňuje asociativní zákon, tj. pro každé $a, b, c \in A$ platí

$$(a * b) * c = a * (b * c).$$

Dále řekneme, že pologrupa $(A, *)$ je *grupa*, jestliže A navíc

(i) obsahuje tzv. jednotkový prvek $e \in A$ s vlastností

$$a * e = a = e * a \text{ pro libovolné } a \in A;$$

(ii) obsahuje s každým $a \in A$ tzv. *inverzní prvek* a^{-1} s vlastností

$$a * a^{-1} = e = a^{-1} * a.$$

Dále řekneme, že $(A, *)$ je *komutativní* neboli *abelovská*, jestliže operace $*$ splňuje tzv. komutativní zákon $a * b = b * a$ pro každé $a, b \in A$. Pologrupa s jednotkovým prvkem se nazývá *monoid*.

Příklad 2.4.1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$ jsou příklady komutativních grup. $(S_3, \circ)$, kde S_3 je množina všech permutací tříprvkové množiny, nebo $(RegMat, \cdot)$ jsou nekomutativní grupy.

Věta 2.4.1. *Platí:*

(i) *V grupoidu existuje nejvýše jeden jednotkový prvek.*

(ii) *V monoidu existuje ke každému prvku nejvýše jeden inverzní prvek.*

Důkaz.

(i) Nechť $(G, *)$ je grupoid s jednotkami e, f. Pak $e = e * f = f$.

(ii) Nechť $(M, *)$ je monoid s jednotkou e, a nechť $b, c \in M$ jsou inverzní prvky k $a \in M$. Pak $b = b * e = b * (a * c) = (b * a) * c = e * c = c$.

Tím je důkaz hotov. □

Každý monoid $(M, *)$ lze chápat jako algebru $(M, *, e)$ s binární operací $*$ a nulární operací e. Každou grupu $(G, *)$ lze chápat jako algebru $(G, *, e, ^{-1})$ s binární operací $*$, nulární operací e a unární operací $^{-1}$. U algeber s jednou binární operací často užíváme tzv. multiplikativní symboliky (tj. místo $*$ píšeme $\cdot$), pak značíme jednotkový prvek jako 1 a inverzní prvek k a jako a^{-1}. U jiných grup také někdy používáme tzv. aditivní symboliky (tj. místo $*$ píšeme $+$), pak jednotkovému prvku říkáme neutrální prvek a značíme jej 0, inverznímu prvku k a říkáme prvek opačný a značíme $-a$. Pologrupový epimorfismus zobrazí jednotku na jednotku a inverzní prvek na inverzní (dokonce vynutí existenci těchto prvků v cílové pologrupě): Je-li $f : A \to B$ epimorfismus pologrupy $(A, \circ)$ do pologrupy $(B, *)$ a má-li A jednotku e_A, pak $f(e_A)$ je jednotkou pologrupy B. Jsou-li a, b navzájem inverzní v A, pak $f(a), f(b)$ jsou navzájem inverzní v B (důkaz je snadný).

Softwarové nástroje: Algebry s jednou operací, Kongruence na algebrách s jednou operací

Definice 2.4.2. Buď $(G, \cdot)$ grupa, $H \subseteq G$. Říkáme, že H je *podgrupa* grupy G, jestliže pro $x, y \in H$ platí $x \cdot y \in H$, jednotka e grupy $(G, \cdot)$ je prvkem H a pro každé $x \in H$ platí $x^{-1} \in H$ (pak se říká, že množina H je uzavřená vzhledem k operacím definovaným v G). Podgrupa $(H, \cdot)$ grupy $(G, \cdot)$ se nazývá *normální podgrupa*, jestliže pro libovolné $a \in G$, $h \in H$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad 2.4.2. V komutativní grupě je libovolná její podgrupa normální. V nekomutativních grupách (např. S_3) mohou existovat i podgrupy, které nejsou normální.

Věta 2.4.2. *Buď $(G, \cdot)$ grupa, R kongruence na G. Nechť $1 \in G$ je jednotkový prvek v G. Pak $H = [1]_R$ je normální podgrupou grupy G.*

Důkaz.

(i) Nejprve ověříme, že $(H, \cdot)$ je podgrupa. Zvolme $a, b \in H$. Pak $aR1$, $bR1$, neboť a, b patří do téže třídy jako 1. Protože je však R kongruence, nutně z toho plyne, že $(a \cdot b)R(1 \cdot 1)$, tedy $(a \cdot b)R1$. Tedy $a \cdot b \in H$, tj. $(H, \cdot)$ je grupoid. Asociativní zákon je v H splněn, protože platí v G a $G \supseteq H$. Také $1 \in H$, takže $(H, \cdot)$ je monoid. Buď $a \in H$. Je-li $b \in G$ prvek k a inverzní, pak $a \cdot b = 1 = b \cdot a$. zřejmě $aR1$ (neboť $a \in H$) a bRb (neboť R je reflexivní), odtud $(a \cdot b)R(1 \cdot b) = 1Rb$, takže i $b \in H$, tedy H je uzavřená i vzhledem k inverzi. Celkem máme, že H je grupa.

(ii) Nyní ukážeme, že $(H, \cdot)$ je normální podgrupou. Buď $a \in G$, $h \in H$. Chceme dokázat, že $aha^{-1} \in H$. Jelikož $hR1$, a zjevně aRa, $a^{-1}Ra^{-1}$, dostáváme vynásobením zleva $ahRa$, a dále vynásobením zprava

$$aha^{-1}Raa^{-1} = aha^{-1}R1, \text{ a tedy } aha^{-1} \in H.$$

Tím je důkaz hotov.

□

Věta 2.4.3. *Buď $(G, \cdot)$ grupa a $H \subseteq G$ její normální podgrupa. Pak relace $R = \{(x, y)|x, y \in G, y^{-1}x \in H\}$ je kongruence na G.*

Důkaz.

(i) Ukážeme nejprve, že R je ekvivalencí na G. Buď $x \in G$ libovolný prvek. Jelikož $x^{-1}x = 1$ a $1 \in H$, relace R je reflexivní. Buď xRy. Pak $y^{-1}x \in H$, takže existuje $h \in H$, že $y^{-1}x = h$, tedy $x = y \cdot h$, odkud $y = xh^{-1}$, takže $x^{-1}y = h^{-1} \in H$. Tedy yRx,tj. R je symetrická. Nechť $xRy \wedge yRz$. Pak $y^{-1}x \in H \wedge z^{-1}y \in H$, takže $z^{-1}x = z^{-1}yy^{-1}x \in H$. Tedy R je i tranzitivní, čili celkově ekvivalence.

(ii) Ukážeme, že R je kongruencí na G. Nechť xRy a uRv pro nějaké $x, y, u, v \in G$. Potom $y^{-1}x, v^{-1}u \in H$, takže existují $h, g \in H$, že $x = y \cdot h$, $u = v \cdot g$. Tedy $xu = yhvg = yvv^{-1}hvg = yvpg$, kde $p = v^{-1}hv \in H$, neboť $(H, \cdot)$ je normální podgrupa. Pak ovšem $k = pg \in H$, odkud dostáváme $xu = yvk$, čili $(yv)^{-1}(xu) \in H$, tj. $(xu)R(yv)$. Tedy R je kongruence a věta je dokázána.

□

Všimněme si, že k důkazu, že R je ekvivalence, nebylo potřeba normálnosti podgrupy H. Faktorové třídy podle R mají tvar:

$$[x]_R = \{y|y \in G, yRx\} = \{y|y \in G, x^{-1}y \in H\} = \{y|y = x \cdot h, h \in H\} =$$

$$= \{xh|h \in H\},$$

což značíme zjednodušeně $[x]_R = x \cdot H$ a těmto třídám říkáme *levé třídy podle* H. Vzniklému rozkladu G/R říkáme *levý rozklad grupy G podle H*. Analogicky lze definovat tzv. *pravý rozklad podle H* na třídy $H \cdot x = \{h \cdot x|h \in H\}$. Obecně (pro nekomutativní grupy) se tento rozklad může lišit od levého rozkladu. Je-li H normální podgrupa v G,

jsou oba rozklady stejné: Nechť $y \in xH$. Pak existuje $h \in H$, že $y = xh$. Potom $yx^{-1} = = xhx^{-1} = g \in H$ (H je normální), a tedy $y = gx$, což dává $y \in Hx$. Tedy $xH \subseteq Hx$. Analogicky se ukáže opačná inkluze $Hx \subseteq xH$, tj. celkem $xH = Hx$.

Věta 2.4.4. *Počet prvků podgrupy je dělitelem počtu prvků grupy.*

Důkaz. Je-li H podgrupa v G (ne nutně normální), má každá třída xH, kde $x \in G$, stejně prvků jako H. Tedy $|G| = |G/H| \cdot |H|$, což dává ihned tvrzení.

□

Definice 2.4.3. Buď $(G, \cdot)$ grupa a H její normální podgrupa. Nechť

$$R = \{(x, y) | x, y \in G, y^{-1}x \in H\}$$

je kongruenční relace příslušná podgrupě H. Pak faktorovou grupu G/R (je to grupa díky existenci přirozeného epimorfismu $G \to G/R$) nazýváme *faktorovou grupou grupy G podle H* a značíme G/H.

Buď $f : G \to F$ morfismus grup $(G, \cdot)$ a $(F, *)$. Označme $R = \operatorname{Ker} f$. Podle věty 2.3.3 je R kongruencí na G, takže třída $\mathfrak{I}(f) := [1_G]_{\operatorname{Ker} f}$ je normální podgrupa grupy G podle věty 2.4.2. Přitom přesněji,

$$\mathfrak{I}(f) = \{x | x \in g, xR1_G\} = \{x | x \in G, f(x) =$$

$$= f(1_G)\} = \{x | x \in G, f(x) = 1_F\} = f^{-1}(1_F),$$

tedy $\mathfrak{I}(f)$ je množina všech vzorů jednotky 1_F. Relaci $R = \operatorname{Ker} f$ lze vyjádřit také jako

$$R = \{(x, y) | x, y \in G, f(x) = f(y)\} = \{(x, y) | x, y \in G, (f(y))^{-1} * f(x) = 1_F\} =$$

$$= \{(x, y) | x, y \in G, f(y^{-1}x) = 1_F\} = \{(x, y) | x, y \in G, y^{-1}x \in f^{-1}(1_F)\} =$$

$$= \{(x, y) | x, y \in G, y^{-1}x \in \mathfrak{I}(f)\}.$$

Existuje tedy vzájemně jednoznačná korespondence mezi jádrem $\operatorname{Ker} f$ a normální podgrupou $\mathfrak{I}(f)$ (která se díky svému charakteru nazývá *jádro morfismu f*).

Věta 2.4.5. *Buď $f : G \to F$ epimorfismus grup $(G, \cdot)$ a $(F, *)$. Pak grupy $(G/\mathfrak{I}(f), \cdot)$ a $(F, *)$ jsou izomorfní.*

Důkaz. přímý důsledek věty 2.3.4. □

Příklad 2.4.3. Nechť $(\mathbb{Z}_n, \oplus)$ je grupa s operací sčítání modulo n, tj.

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, \quad a \oplus b = (a + b) \mod n.$$

Položme $f : \mathbb{Z} \to \mathbb{Z}_n$ tak, že $f(x) := x \mod n$. Zřejmě f je epimorfismus $\mathbb{Z}$ na $\mathbb{Z}_n$, je totiž

$$f(x+y) = (x+y) \mod n = (\text{ podle věty o dělení se zbytkem }) =$$

$$= [(x \mod n) + (y \mod n)] \mod n = (f(x) + f(y)) \mod n = f(x) \oplus f(y),$$

přičemž f je surjektivní.

Pak

$$\mathfrak{I}(f) = \{x | f(x) = 0\} = \{x | x = ny, y \in \mathbb{Z}\} = \{ny | y \in \mathbb{Z}\} = n\mathbb{Z}$$

a jednotlivé třídy rozkladu příslušného kongruenci $\operatorname{Ker} f$ mají tvar $[x]_{\operatorname{Ker} f} = x + n\mathbb{Z}$, je tedy patrné, že $[x]_{\operatorname{Ker} f}$ je množina právě těch prvků ze $\mathbb{Z}$, které lze vyjádřit ve tvaru $x+ny$, kde $y \in \mathbb{Z}$, tj. právě těch prvků ze $\mathbb{Z}$, které po dělení číslem n dávají stejný zbytek. Tedy

$$[x]_{\operatorname{Ker} f} = \{z | z = x + ny, y \in \mathbb{Z}\} = \{z | z \in \mathbb{Z}, n | z - x\} =$$

$$= \{z | z \in \mathbb{Z}, z \mod n = x \mod n\}.$$

Faktorová grupa $\mathbb{Z}/\mathfrak{I}(f) = \mathbb{Z}/n\mathbb{Z}$ je tedy právě grupa zbytkových tříd, izomorfní s původní grupou $\mathbb{Z}_n$. Proto se tyto dvě grupy často ztotožňují.

Definice 2.4.4. Buď $(A, +, \cdot)$ algebra s operacemi $+$ a $\cdot$ taková, že

(i) $(A, +)$ je komutativní grupa;

(ii) $(A, \cdot)$ je monoid;

(iii) pro libovolné $a, b, c \in A$ platí

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Pak $(A, +, \cdot)$ se nazývá *okruh*. Je-li $|A| > 1$, nazývá se $(A, +, \cdot)$ *netriviální okruh*. Nechť $0 \in A$ je neutrální prvek grupy $(A, +)$. Pak 0 se nazývá *nulou* okruhu $(A, +, \cdot)$. Nechť 1 je označení pro jednotkový prvek monoidu $(A, \cdot)$. Pak 1 se nazývá *jednotkou (jedničkou)* okruhu $(A, +, \cdot)$. Je-li navíc $(A \setminus \{0\}, \cdot)$ komutativní grupa, okruh $(A, +, \cdot)$ se nazývá *těleso*.

Příklad 2.4.4. Příklady těles: $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ pro p prvočíslo. Konečných těles se využívá např. v teorii kódování.

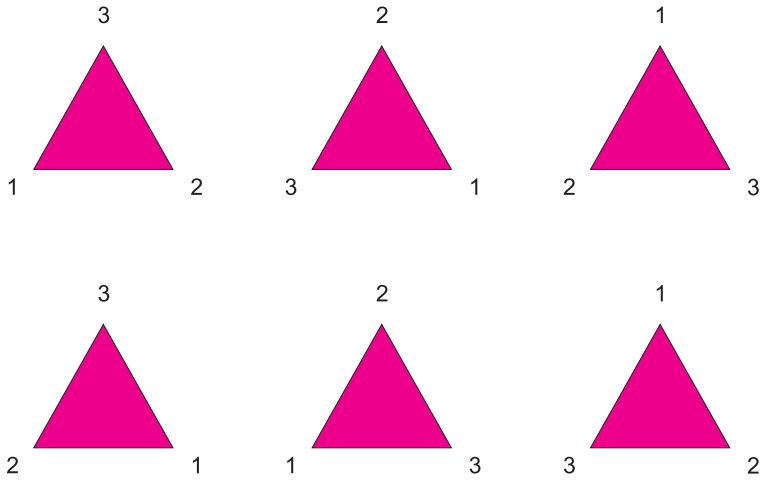
Cvičení

2.4.1. Dokažte, že $(A, \diamond)$, kde $A = \{0, 1, \ldots, n-1\}$ a $a \diamond b = (a + b) \mod n$ pro všechna $a, b \in A$ je komutativní grupa. Zapište její tabulku pro $n = 1, 2, 3, 4, 5, 6$.

2.4.2. Dokažte, že $(A, \bullet)$, kde $A = \{0, 1, \ldots, n-1\}$ a $a \bullet b = (a \cdot b) \mod n$ pro všechna $a, b \in A$ je komutativní monoid. Zapište jeho tabulku pro $n = 1, 2, 3, 4, 5, 6$.

2.4.3. * Nechť $(A, \bullet)$ je algebra z předchozí úlohy. Dokažte, že její podmnožina $A \setminus \{0\}$ s operací $\bullet$ je komutativní grupa, právě když n je prvočíslo.

2.4.4. Nechť $M = \{1, 2, 3\}$ a $S_3 = \{(1,2,3), (3,1,2), (2,3,1), (3,2,1), (1,3,2), (2,1,3)\}$ množina všech permutací množiny M (tj. bijekcí $M \to M$). Zapište tabulku algebry $(S_3, \circ)$. Dokažte, že $(S_3, \circ)$ je nekomutativní grupa. Ukažte také, že každou permutaci množiny M lze reprezentovat jako symetrii (tj. zobrazení na sebe, zachovávající geometrický tvar) rovnostranného trojúhelníka (viz Obr. 2.4.1).



Obr. 2.4.1. Symetrie rovnostranného trojúhelníka

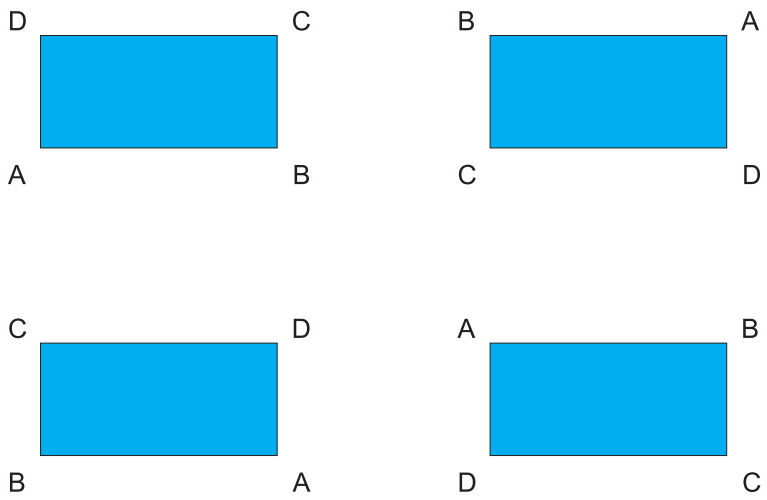
2.4.5. Najděte všechny podgrupy grupy $(\mathbb{Z}_4, \oplus)$. Které z nich jsou normální?

2.4.6. Najděte všechny podgrupy grupy $(\mathbb{Z}_6, \oplus)$. Které z nich jsou normální?

2.4.7. Je dána algebra $(K_4, \diamond)$, kde $K_4 = \{a, b, c, d\}$ a operace $\diamond$ je dána tabulkou:

$\diamond$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Dokažte, že $(K_4, \diamond)$ je grupa (tzv. *Kleinova grupa*). Ukažte, že její prvky lze reprezentovat jako symetrie obdélníka (s nestejnými stranami, viz. Obr. 2.4.2).



Obr. 2.4.2. Symetrie obdélníka

2.4.8. Najděte všechny podgrupy Kleinovy grupy $(K_4, \diamond)$. Které z nich jsou normální?

2.4.9. Najděte všechny normální podgrupy grupy $(S_3, \circ)$.

2.4.10. K normálním podgrupám v příkladech 5 až 9 sestrojte příslušné faktorové grupy.

2.4.11. Rozhodněte a dokažte, zda existuje epimorfismus algeber:

(i) $(\mathbb{Z}_4, \oplus)$ na $(\mathbb{Z}_2, \oplus)$

(ii) $(\mathbb{Z}_4, \oplus)$ na $(\mathbb{Z}_3, \oplus)$

(iii) $(\mathbb{Z}_6, \oplus)$ na $(\mathbb{Z}_2, \oplus)$

(iv) $(\mathbb{Z}_6, \oplus)$ na $(\mathbb{Z}_3, \oplus)$

(v) $(\mathbb{Z}_6, \oplus)$ na $(\mathbb{Z}_4, \oplus)$

(vi) $(\mathbb{Z}_4, \oplus)$ na $(K_4, \diamond)$

(vii) $(K_4, \diamond)$ na $(\mathbb{Z}_2, \oplus)$

(viii) $(K_4, \diamond)$ na $(\mathbb{Z}_3, \oplus)$

(ix) $(K_4, \diamond)$ na $(\mathbb{Z}_4, \oplus)$

(x) $(S_3, \circ)$ na $(\mathbb{Z}_2, \oplus)$

(xi) $(S_3, \circ)$ na $(\mathbb{Z}_3, \oplus)$

(xii) $(S_3, \circ)$ na $(\mathbb{Z}_4, \oplus)$

(xiii) $(S_3, \circ)$ na $(\mathbb{Z}_6, \oplus)$

(xiv) $(S_3, \circ)$ na $(K_4, \diamond)$

2.5 Svazy

V této kapitole se budeme hlouběji zabývat zvláštním typem algeber se dvěma (a více) operacemi – svazy.

Definice 2.5.1. Buď X množina, $\wedge$ a $\vee$ operace na X s vlastnostmi pro všechna $x, y, z \in X$:

(i) $x \vee x = x,\ x \wedge x = x$ (idempotence)

(ii) $x \vee y = y \vee x,\ x \wedge y = y \wedge x$ (komutativita)

(iii) $(x \vee y) \vee z = x \vee (y \vee z),\ (x \wedge y) \wedge z = x \wedge (y \wedge z)$ (asociativita)

(iv) $x \wedge (x \vee y) = x,\ x \vee (x \wedge y) = x$ (absorbční zákony)

Pak trojici $(X, \vee, \wedge)$ nazýváme *svazem na* X. O svazu $(X, \vee, \wedge)$ někdy říkáme, že je *algebraicky definovaný*, abychom zdůraznili, že jej chápeme jako algebru, na rozdíl od *svazově uspořádané množiny* (viz. kapitola 1.6).

Příklad 2.5.1. Buď $A = \{1, 2, 3\}$, $X = 2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$. Pak $(X, \cup, \cap)$ je algebraicky definovaný svaz. Např. $\{1, 2\} \cup \{1, 3\} = A$, $\{1, 2\} \cap \{1, 3\} = = \{1\}$.

Příklad 2.5.2. Buď $D = \{1, 2, 3, 4, 6, 12\}$. Pro $x, y \in D$ klademe $x \vee y = \text{nsn}\,(x, y)$, $x \wedge y = \text{nsd}\,(x, y)$. Pak $(D, \vee, \wedge)$ je algebraicky definovaný svaz. Např. $4 \wedge 6 = 2$, $4 \vee 6 = 12$, $3 \vee 4 = 12$, $3 \vee 2 = 6$, atd.

Příklad 2.5.3. $\mathbb{R}^3$, $\mathcal{V} = \{X | X \subseteq \mathbb{R}^3$ je vektorový podprostor v $\mathbb{R}^3\}$ Pak $(\mathcal{V}, \oplus, \cap)$ je algebraicky definovaný svaz ($\oplus$ je tzv. součet vektorových prostorů, viz. lineární algebra).

Algebraická definice svazu a svazové uspořádání na množině spolu úzce souvisí. Buď X množina, na níž je definováno svazové uspořádání $\leq$. Klademe pro $x, y \in X$

$$x \vee y = \sup\{x, y\}, \quad x \wedge y = \inf\{x, y\}.$$

Pak $(X\vee,\wedge)$ je algebraicky definovaný svaz. Naopak, mějme $(X,\vee,\wedge)$ algebraicky definovaný svaz. Klademe pro $x,y\in X$

$$x\leq y\iff x\vee y=y.$$

$$(\text{alternativně } x\leq y\iff x\wedge y=x)$$

Pak $(X,\leq)$ je svazově uspořádaná množina. Je tedy zřejmé, že není třeba rozlišovat mezi svazovým uspořádáním na množině a algebraicky definovaným množinovým svazem – hovoříme zde prostě o *svazu*.

Softwarové nástroje: Uspořádání na množině

Cvičení

2.5.1. Buď X množina, na níž je definováno svazové uspořádání $\leq$. Klademe pro $x, y \in X$ $x \vee y = \sup\{x, y\}$, $x \wedge y = \inf\{x, y\}$. Prověřte, že $(X, \vee, \wedge)$ je algebraicky definovaný svaz.

2.5.2. Mějme $(X, \vee, \wedge)$ algebraicky definovaný svaz. Klademe pro $x, y \in X$ $x \leq y \iff x \vee y = y$. Prověřte, že $(X, \leq)$ je svazově uspořádaná množina. Dokažte, že relace $x \leq y \iff x \wedge y = x$ definuje na X stejné uspořádání.

2.5.3. V příkladě 10 ze cvičení 1.6 svazová uspořádání vyjádřete jako algebraicky definované svazy. Vyjádřete operace spojení a průseku.

2.5.4. V příkladech 13 až 16 ze cvičení 1.6 svazová uspořádání vyjádřete jako algebraicky definované svazy. Vyjádřete operace spojení a průseku.

2.5.5. Sestrojte svaz všech podgrup grupy $(\mathbb{Z}_n, \oplus)$ pro n=1,2,3,4,5,6.

2.5.6. Sestrojte svaz všech podgrup grupy $(K_4, \diamond)$ z příkladu 7 ve cvičení 2.4.

2.5.7. Sestrojte svazy všech podgrup a normálních podgrup grupy $(S_3, \circ)$ z příkladu 4 ve cvičení 2.4.

2.6 Podsvazy a izomorfismy svazů

Definice 2.6.1. Buď $(X, \vee_X, \wedge_X)$ svaz, $Y \subseteq X$. Řekneme, že $(Y, \vee_Y, \wedge_Y)$ je *podsvazem* svazu $(X, \vee_X, \wedge_X)$, jestliže platí:

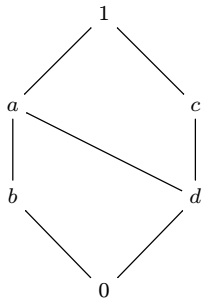
(i) $(Y, \vee_Y, \wedge_Y)$ je svaz;

(ii) pro každé $x, y \in Y$ platí

$$x \vee_Y y = \sup_Y\{x, y\} = \sup_X\{x, y\} = x \vee_X y;$$

$$x \wedge_Y y = \inf_Y\{x, y\} = \inf_X\{x, y\} = x \wedge_X y.$$

Příklad 2.6.1. Nechť $X = \{0, a, b, c, d, 1\}$ je uspořádaná množina s Hasseovým diagramem



a uvažujme $Y = \{0, a, b, d, 1\}$, $Z = \{0, a, b, c, 1\}$ s uspořádáním indukovaným z množiny X. Uspořádané množiny $(X, \leq)$, $(Y, \leq)$, $(Z, \leq)$ jsou svazy. Navíc, uspořádání svazů Y a Z splývá s původním uspořádáním na X. Avšak Z není podsvazem svazu X: pro $a, c \in Z \subseteq$ $\subseteq X$ platí

$$a \wedge_Z c = \inf_Z\{a, c\} = 0,$$

$$a \wedge_X c = \inf_X\{a, c\} = d \neq 0.$$

Naopak, Y je podsvazem svazu X: jediné dva nesrovnatelné prvky v Y jsou b, d a pro ně platí

$$b \vee_Y d = a = b \vee_X d, \quad b \wedge_Y d = 0 = b \wedge_X d$$

(pro srovnatelné prvky vztahy nemusíme ověřovat, výsledkem operace $\vee$ nebo $\wedge$ je totiž vždy jeden z nich).

Definice 2.6.2. Buďte $(X, \vee_X, \wedge_X)$, $(Y, \vee_Y, \wedge_Y)$ svazy. Nechť existuje vzájemně jednoznačné zobrazení $f : X \to Y$ takové, že pro každé $x, y \in X$ platí

$$f(x \vee_X y) = f(x) \vee_Y f(y), \quad f(x \wedge_X y) = f(x) \wedge_Y f(y).$$

Pak říkáme, že $(X, \vee_X, \wedge_X)$ a $(Y, \vee_Y, \wedge_Y)$ jsou *izomorfní*. Zobrazení f nazýváme *izomorfismem* svazů $(x, \vee_X, \wedge_X)$ a $(Y, \vee_Y, \wedge_Y)$.

Příklad 2.6.2. Mějme $X = \{1, 2, 3, 4, 6, 12\}$ s uspořádáním dělitelnosti, Y s uspořádáním $\subseteq$, $Y = \{\varnothing, \{2\}, \{3\}, \{2, 3\}, \{1, 2\}, \{1, 2, 3\}\}$. Pak X a Y jsou izomorfní svazy, stačí definovat

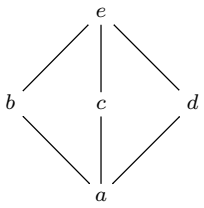
$$f(1) = \varnothing, \ f(2) = \{2\}, \ f(3) = \{3\}, \ f(4) = \{1, 2\},$$

$$f(6) = \{2, 3\}, \ f(12) = \{1, 2, 3\}.$$

Cvičení

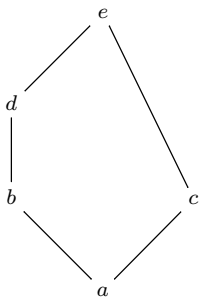
2.6.1. Najděte všechny neizomorfní svazy o n prvcích pro $n = 1, 2, 3, 4, 5$.

2.6.2. Najděte všechny podsvazy svazu M_5 s Hasseovým diagramem



Které z nich jsou neizomorfní?

2.6.3. Najděte všechny podsvazy svazu N_5 s Hasseovým diagramem



Které z nich jsou neizomorfní?

2.6.4. Najděte všechny neizomorfní podsvazy svazu z příkladu 2.6.2.

2.7 Klasifikace svazů

Definice 2.7.1. Buď $(X, \vee, \wedge)$ svaz. Řekneme, že $(X, \vee, \wedge)$ je

(i) *modulární*, jestliže platí pro všechna $x, y, z \in X$:

$$x \leq z \implies x \vee (y \wedge z) = (x \vee y) \wedge z;$$

(ii) *distributivní*, jestliže platí pro všechna $x, y, z \in X$:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z);$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z);$$

(iii) *komplementární*, jestliže v X existuje nejmenší prvek $0 \in X$, největší prvek $1 \in X$ a pro každé $x \in X$ existuje $\overline{x} \in X$ s vlastností

$$x \wedge \overline{x} = 0,\ x \vee \overline{x} = 1.$$

Prvek $\overline{x}$ se nazývá *doplňkem (komplementem)* prvku x.

Věta 2.7.1. *Každý distributivní svaz je modulární.*

Důkaz. Buď $(X, \vee, \wedge)$ distributivní svaz. Nechť $x, y, z \in X$ a nechť $x \leq z$. Pak

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z.$$

Tedy $(X, \vee, \wedge)$ je modulární.

□

Věta 2.7.2. *Buď X distributivní svaz. Pak každý prvek v X má nejvýše jeden komplement.*

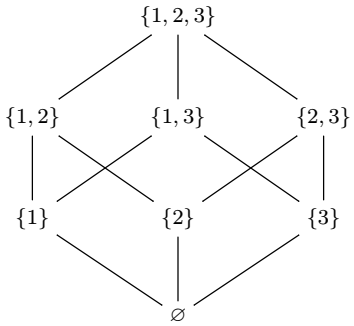
Důkaz. Nechť $(X, \vee, \wedge)$ je distributivní. Nechť $x \in X$ má komplementy y a z. Pak

$$y = y \vee 0 = y \vee (x \wedge z) = (\text{využíváme distributivity}) = (y \vee x) \wedge (y \vee z) = 1 \wedge (y \vee z) =$$

$$= (x \vee z) \wedge (y \vee z) = (\text{využíváme distributivity}) = (x \wedge y) \vee z = 0 \vee z = z.$$

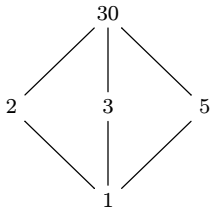
□

Příklad 2.7.1. Nechť A je množina, $X = 2^A$. Svaz $(X, \cup, \cap)$ je distributivní (a tedy i modulární) i komplementární. Nejmenším prvkem (=nulou) svazu je $\varnothing$, největším prvkem (=jedničkou) svazu X je množina A. Pro $A = \{1, 2, 3\}$, $X = 2^A$ je Hasseův diagram svazu $(X, \cup, \cap)$ tvaru



$(X, \cup, \cap)$

Příklad 2.7.2. Modulární svaz, který není distributivní. Následující svaz nebo libovolný s ním izomorfní se nazývá *diamantový svaz* a značíme jej M_5. Položme $X = \{1, 2, 3, 5, 30\}$ a zvolme uspořádání dělitelností, jak ukazuje Hasseův diagram.



Pak svaz X je komplementární s nejmenším prvkem 1, největším prvkem 30. Prvek 2 má dva komplementy, 3 a 5:

$$2 \wedge 3 = 2 \wedge 5 = 1, \quad 2 \vee 3 = 2 \vee 5 = 30.$$

Tedy podle věty 2.7.2 nemůže být distributivní. Vskutku, např.

$$2 \vee (3 \wedge 5) = 2 \vee 1 = 2, \text{ ale } (2 \vee 3) \wedge (2 \vee 5) = 30 \wedge 30 = 30.$$

Ukážeme, že X je modulární. Pro $x = z$ je podmínka modularity z definice 2.7.1 splněna triviálně. Je-li pro $x, z \in X$ $x < z$, pak buď $x = 1$, nebo $z = 30$. Je-li $x = 1$, pak

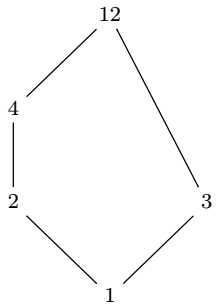
$$x \vee (y \wedge z) = 1 \vee (y \wedge z) = y \wedge z = (1 \vee y) \wedge z = (x \vee y) \wedge z.$$

Je-li $z = 30$, pak

$$x \vee (y \wedge z) = x \vee (y \wedge 30) = x \vee y = (x \vee y) \wedge 30 = (x \vee y) \wedge z.$$

Tedy je splněna podmínka modularity z definice 2.7.1

Příklad 2.7.3. Svaz, který není modulární. Následující svaz nebo libovolný s ním izomorfní se nazývá *pentagonální (pětiúhelníkový) svaz* a značíme jej N_5. Položme $X = \{1, 2, 3, 4, 12\}$ s uspořádáním dělitelností, jak je zřejmé z Hasseova diagramu.

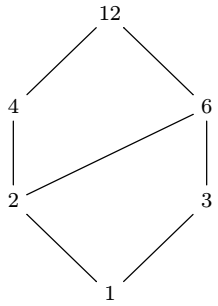


Pak je zřejmě $2 \leq 4$. Přitom

$$2 \vee (3 \wedge 4) = 2 \vee 1 = 2, \quad (2 \vee 3) \wedge 4 = 12 \wedge 4 = 4.$$

Tedy X není modulární (tedy není ani distributivní). Je to však komplementární svaz. Prvek 3 má dva různé komplementy 2 a 4, prvky $2, 4$ mají jediný komplement 3, komplementem 1 je 12 a komplementem 12 je 1.

Příklad 2.7.4. Svaz, který není komplementární. Klademe $X = \{1, 2, 3, 4, 6, 12\}$ a uvažujme opět uspořádání dělitelností.



Prvek 2 nemá komplement: jediným kandidátem na komplement prvku 2 je 3, neboť chceme $2 \wedge \overline{2} = 1$, avšak $2 \vee 3 = 6$, zatímco požadujeme $2 \vee \overline{2} = 12$.

Příklad 2.7.5. Další možné příklady svazů: svazy abelovských grup, svaz ekvivalencí na dané množině, svaz vektorových podprostorů daného vektorového prostoru (tento svaz je vždy modulární, ale nemusí být distributivní).

Věta 2.7.3. *Svaz $(X, \vee, \wedge)$ je*

(i) *modulární $\iff$ neobsahuje podsvaz izomorfní s N_5;*

(ii) *distributivní $\iff$ neobsahuje podsvaz izomorfní s M_5 ani N_5.*

Důkaz. Je-li X modulární, resp. distributivní, pak z definice podsvazu ihned plyne, že každý podsvaz svazu X je také modulární (resp. distributivní). Tedy X nemůže obsahovat podsvaz izomorfní s N_5 (resp. s N_5 ani M_5). Ve druhém směru ukážeme pro ilustraci pouze část (i).

(i) Předpokládejme naopak, že $(X, \vee, \wedge)$ není modulární. Pak pro nějaké prvky $x, y, z \in X$ platí

$$x \leq z, \text{ a přitom } x \vee (y \wedge z) \neq (x \vee y) \wedge z.$$

Označme $a := x \vee (y \wedge z)$, $b := (x \vee y) \wedge z$. Ukážeme, že $a < b$. Zřejmě $a \leq x \vee y$, $a \leq x \vee z \leq z$, tedy $a \leq (x \vee y) \wedge z = b$. Protože však $a \neq b$, je $a < b$. Dále ukážeme, že y není srovnatelné ani s a, ani s b. Předpokládejme, že $a \leq y$. Pak $a \vee y = y$, takže $y = x \vee (y \wedge z) \vee y = x \vee y$, takže je $x \leq y$. Potom však $x \leq y \wedge z$, a tedy $a = x \vee (y \wedge z) = y \wedge z = (x \vee y) \wedge z = b$, což je spor. Tedy $a \not\leq y$. Nyní předpokládejme, že $y \leq b$. Pak $y \wedge b = y$, takže $y = y \wedge (x \vee y) \wedge z = y \wedge z$, odkud $y \leq z$. Potom však $x \vee y \leq z$, odkud $a = x \vee (y \wedge z) = x \vee y = (x \vee y) \wedge z = b$, spor. Tedy $y \not\leq b$. Celkem dostáváme, že y není srovnatelné ani s a, ani s b. Klademe $c := x \vee y$, $d := y \wedge z$. Potom

$$a \vee y = x \vee (y \wedge z) \vee y = x \vee y = c;$$

$$b \vee y = [(x \vee y) \wedge z] \vee y \leq (x \vee y) \vee y = x \vee y = c;$$

ovšem $c = a \vee y \leq b \vee y \leq c$, tedy $b \vee y = c$. Analogicky

$$b \wedge y = y \wedge (x \vee y) \wedge z = y \wedge z = d,$$

$$a \wedge y = [x \vee (y \wedge z)] \wedge y \geq (y \wedge z) \wedge y = y \wedge z = d.$$

Ovšem $d \leq a \wedge y \leq b \wedge y = d$, tedy $a \wedge y = d$. Pak množina $S = \{a, b, c, d, y\}$ tvoří podsvaz izomorfní s N_5.

(ii) Důkaz této části tvrzení věty je veden analogicky, je pouze poněkud složitější. Zájemce o podrobnosti odkazujeme na dostupnou literaturu.

□

Softwarové nástroje: Uspořádání na množině

Cvičení

2.7.1. Najděte všechny modulární svazy o 5 prvcích.

2.7.2. Najděte všechny distributivní svazy o 5 prvcích.

2.7.3. * Najděte všechny nemodulární svazy o 6 prvcích.

2.7.4. Zjistěte typy svazů z příkladů 10, 13,14,15,16 ve cvičení 1.6.

2.7.5. Zjistěte typy svazů z příkladů 5,6,7 ve cvičení 2.5.

2.7.6. Určete typy svazů z příkladu 4 ve cvičení 2.6.

2.8 Booleovské svazy a algebry

Definice 2.8.1. Buď $(X, \vee, \wedge)$ distributivní komplementární svaz s nejmenším prvkem $0 \in X$ a největším prvkem $1 \in X$. Pak $(X, \vee, \wedge)$ nazýváme *Booleovým svazem*. Uspořádanou šestici $(X, \vee, \wedge, ^-, 0, 1)$, kde $^- : X \to X$ je operace komplementu v X, nazýváme *Booleovou algebrou* na X.

Příklad 2.8.1. Je-li A množina, pak pro $X = 2^A$ je $(X, \cup, \cap)$ Booleův svaz.

Věta 2.8.1. *Buď $(X, \oplus, \odot, ', 0, 1)$ algebra se dvěma binárními operacemi $\oplus, \odot$, unární operací $'$ a dvěma nulárními operacemi $0, 1$. Pak $(X, \oplus, \odot, ', 0, 1)$ je Booleova algebra, právě když jsou pro všechna $x, y, z \in X$ splněny tyto podmínky:*

(i) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, $(x \odot y) \odot z = x \odot (y \odot z)$,

(ii) $x \oplus y = y \oplus x$,$x \odot y = y \odot x$,

(iii) $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$, $x \oplus (y \odot z) = (x \oplus y) \odot (x \oplus z)$,

(iv) $x \oplus 0 = x$, $x \odot 1 = x$,

(v) $x \oplus x' = 1$, $x \odot x' = 0$.

Důkaz. Je-li $(X, \oplus, \odot, ', 0, 1)$ Booleova algebra, je $(X, \oplus, \odot)$ Booleův svaz se spojením $\oplus$ a průsekem $\odot$. Splnění podmínek (1) až (5) je důsledkem definice Booleova svazu. Nechť naopak algebra $(X, \oplus, \odot, ', 0, 1)$ splňuje podmínky (1) až (5). Musíme dokázat platnost idempotenčních a absorbčních zákonů z definice 2.5.1.

Buď $x \in X$. Platí $x = x \odot 1 = x \odot (x \oplus x') = (x \odot x) \oplus (x \odot x') = (x \odot x) \oplus 0 = x \odot x$ a také $x = x \oplus 0 = x \oplus (x \odot x') = (x \oplus x) \odot (x \oplus x') = (x \oplus x) \odot 1 = x \oplus x$, čímž jsou idempotenční zákony dokázány. Dále platí $x \odot (x \oplus y) = (x \odot x) \oplus (x \odot y) = x \oplus (x \odot y) = (x \odot 1) \oplus (x \odot y) = x \odot (1 \oplus y) = = [x \odot (1 \oplus y)] \odot 1 = x \odot [(1 \oplus y) \odot (y \oplus y')] = x \odot [y \oplus y' \oplus (y \odot y) \oplus (y \odot y')] = x \odot (y \oplus y') = x \odot 1 = x$, čímž jsou i absorbční zákony dokázány. Odtud a z podmínek (1), (2) a (3) plyne, že $(X, \oplus, \odot)$ je distributivní svaz, jehož nejmenším prvkem je 0 a největším 1 podle (4). Podle (5) je $(X, \oplus, \odot)$ komplementární, a tedy je Booleův. Tím je věta dokázána.

□

Definice 2.8.2. Buď $(X, \vee, \wedge)$ Booleův svaz s nejmenším prvkem $0 \in X$. Řekneme, že $a \in X$ je *atom* svazu X, jestliže a pokrývá nejmenší prvek 0 (tj. $0 < a$, a přitom mezi 0 a a neleží další prvky).

Věta 2.8.2. *Buď $(X, \vee, \wedge)$ konečný Booleův svaz. Pak X je izomorfní s Booleovským množinovým svazem $(2^P, \cup, \cap)$, kde P je množina všech atomů svazu X.*

Důkaz věty přesahuje možnosti tohoto učebního textu. Zájemce z řad studentů odkazujeme na dostupnou literaturu.

Důsledek 2.8.1. *Počet prvků každé Booleovy algebry je $2^{|P|}$.*

Důsledek 2.8.2. *Dvě Booleovy algebry se stejným počtem prvků jsou izomorfní (opak je zřejmý).*

Softwarové nástroje: Uspořádání na množině

Cvičení

2.8.1. Buď $(X, \oplus, \odot, ', 0, 1)$ Booleova algebra. Dokažte, že pro libovolné $x \in X$ platí $x \oplus 1 = 1$, $x \odot 0 = 0$.

2.8.2. Buď $(X, \oplus, \odot, ', 0, 1)$ Booleova algebra. Dokažte, že pro libovolné $x \in X$ platí $(x')' = x$.

2.8.3. Buď $(X, \oplus, \odot, ', 0, 1)$ Booleova algebra. Dokažte, že $0' = 1$, $1' = 0$.

2.8.4. Buď $(X, \oplus, \odot, ', 0, 1)$ Booleova algebra. Dokažte, že pro libovolné $x, y \in X$ platí $(x \oplus y)' = x' \odot y'$, $(x \odot y)' = x' \oplus y'$.

2.8.5. V Booleově algebře $(X, \oplus, \odot, ', 0, 1)$ zjednodušte výrazy:

(i) $(x' \odot y')'$

(ii) $(a \oplus b) \oplus (c \oplus a) \oplus (b \oplus c)$

(iii) $(x \odot y) \oplus (z \odot x) \oplus (x' \odot y')'$

2.8.6. * Dokažte tzv. *Poretzkyho zákon*: Nechť $(X, \oplus, \odot, ', 0, 1)$ je Booleova algebra. Buď $x, t \in X$. Pak $x = 0$, právě když $t = (x \odot t') \oplus (x' \odot t)$.

2.8.7. V Booleově algebře $(X, \oplus, \odot, ', 0, 1)$ dokažte:

(i) $y \leq x'$ právě když $x \odot y = 0$

(ii) $y \geq x'$ právě když $x \oplus y = 1$

2.8.8. V Booleově algebře $(X, \oplus, \odot, ', 0, 1)$ nalezněte komplementy následujících výrazů:

(i) $x \oplus y \oplus z'$

(ii) $(x \oplus y' \oplus z') \odot (x \oplus y \oplus z')$

(iii) $(x \odot y) \oplus (z \odot x) \oplus (x' \odot y')'$

(iv) $(x' \oplus y)' \odot (x \oplus y')$

2.8.9. * V Booleově algebře $(X, \oplus, \odot, ', 0, 1)$ dokažte:

$$(x \oplus y) \odot (x' \oplus z) = (x' \odot y) \oplus (x \odot z)$$

2.8.10. Nechť $X = \{1, 2, 5, 7, 10, 14, 35, 70\}$. Položme $x \oplus y = \operatorname{nsn}(x, y)$, $x \odot y = \operatorname{nsd}(x, y)$, $x' = \frac{70}{x}$ pro všechna $x, y \in X$. Dokažte, že $(X, \oplus, \odot, ', 1, 70)$ je Booleova algebra. Nakreslete její Hasseův diagram.

2.8.11. Dokažte, že množina všech dělitelů čísla 210 s vhodnými operacemi tvoří Booleovu algebru. Popište tyto operace a nakreslete její Hasseův diagram.

2.8.12. Buď X množina n-bitových řetězců. Definujeme $(x \oplus y)_i = \sup\{x_i, y_i\}$, $(x \odot y)_i = \inf\{x_i, y_i\}$, $(x')_i = (x_i + 1) \bmod 2$ pro $x, y \in X$ a $i = 1, 2, \ldots n$. Dokažte, že $(X, \oplus, \odot, ', \mathbf{0}, \mathbf{1})$ je Booleova algebra.

2.8.13. Pro $n = 7$, $a = 1101010$ a $b = 1011011$ v předchozím příkladě spočítejte $a \oplus b$, $a \odot b$ a a'.

2.8.14. Najděte všechny Booleovy podalgebry Booleovy algebry z příkladu 10.

2.8.15. Určete, kolik Booleových podalgeber má Booleova algebra z příkladu 11.

Počítačová cvičení

2.8.16. Napište program, který prověří, že zadaná operace na konečné množině, která je určena tabulkou, je komutativní.

2.8.17. Napište program, který prověří, že zadaná operace na konečné množině, která je určena tabulkou, je asociativní.

2.8.18. Napište program, který pro zadanou operaci $\circ$ na konečné množině X, která je určena tabulkou, nalezne všechny její levé a pravé jednotkové prvky, tj. prvky e, f takové, že $e \circ x = x$, resp. $x \circ f = x$ pro všechna $x \in X$

2.8.19. Napište program, který prověří, že zadané operace $\vee$, $\wedge$ na konečné množině, které jsou určeny tabulkami, splňují distributivní zákony.

2.8.20. Napište program, který prověří, že zadané operace $\vee$, $\wedge$ na konečné množině, které jsou určeny tabulkami, splňují absorbční zákony.

2.8.21. Implementujte grupu všech permutací n-prvkové množiny, tj. grupovou operaci $\circ$ a operaci $^{-1}$ inverzního prvku.

2.8.22. Implementujte Booleovu algebru (s příslušnými operacemi) všech dělitelů čísla 210.

Pojmy k zapamatování

- Kategorie. Objekty a morfismy.
- Operace na množině. Četnost. Algebra.
- Kongruence. Faktorová algebra.
- Grupoid, pologrupa, monoid, grupa. Komutativita.
- Podgrupa, její normálnost. Faktorové grupy.
- Okruh, Těleso.
- Svaz jako algebra se dvěma operacemi.
- Různé svazové vlastnosti. Distributivnost, modularita, komplementárnost.
- Booleova algebra.

Klíčové myšlenky kapitoly

- Morfismus mezi algebrami je zobrazení, které „zachovává" operace.
- Kongruence je ekvivalence na algebře, která se „shoduje" s jejími operacemi.
- Jádro morfismu je kongruence.
- V grupě je třída rozkladu podle kongruence, obsahující jednotkový prvek, normální podgrupou.
- A naopak. Z normální podgrupy lze kongruenci zrekonstruovat.
- Lagrangeova věta. Řád podgrupy je dělitelem řádu grupy.
- Svazové uspořádání a svaz jako algebra jsou dva ekvivalentní popisy téže struktury.
- Podsvaz svazu je chápán jako podalgebra - musí se zachovávat supréma a infíma.

- Booleova algebra se liší od Booleova svazu jen formálně – tím, které operace se „počítají" jako operace dané algebry. Ale implicitně jsou vždy k dispozici.
- Booloevy algebry se stejným, konečným počtem prvků jsou navzájem izomorfní. Všechny „vypadají" jako Booleova algebra na potenční množině.
- Booleovu algebru lze zadat axiomaticky, bez nutnosti zavádět svazy a uspořádání.

Odkazy na literaturu

Hlavními výchozími prameny pro tuto kapitolu se staly publikace [17] a [34]. Podrobnější informace o uspořádaných množinách a svazech čtenář nalezne například v [8]. Booleovým algebrám je věnována monografie [5]. Níže jsou uvedeny další odkazy na učebnice a monografie, rozšiřující látku probranou v této kapitole.

[5], [8], [9], [10], [14], [17], [20], [21], [18], [33], [32], [35], [36], [37], [42]

Další příklady k procvičení

Elektronická banka příkladů

Matematický software

Algebry s jednou operací
Kongruence na algebrách s jednou operací
Uspořádání na množině

3 Výrokový a predikátový počet

Tato kapitola je věnována základům výrokového a predikátového počtu. V závěru kapitoly probereme úvod do systémů přirozené dedukce.

Cíle

Po prostudování této kapitoly budete schopni:

- vytvářet formule výrokového (resp. predikátového) počtu podle syntaktických pravidel
- vyšetřovat vlastnosti formulí
- zjišťovat zda formule je tautologickým důsledkem množiny předpokladů
- počítat normální disjunktivní a konjunktivní formy formulí
- deduktivně odvozovat nebo dokazovat formule z jiných formulí

3.1 Základní pojmy

Definice 3.1.1. *Prvky jazyka $\mathcal{L}$ výrokového počtu (bez kvantifikátorů) jsou tvořeny:*

(i) *Symboly pravdivostních hodnot:* **true** , **false** .

(ii) *Spojkami:* $\neg$ *(negace),* $\Rightarrow$ *(implikace),* $\wedge$ *(a),* $\vee$ *(nebo),* $\Leftrightarrow$ *(ekvivalence).*

(iii) *Výrokovými konstantami p_i, i=1,2..., kterým se také říká atomické výroky nebo prvotní formule.*

(iv) *Pomocnými symboly (,) - závorkami.*

Definujeme nyní dvě třídy výrazů, vytvořených nad jazykem $\mathcal{L}$: atomické formule a formule.

(i) *Atomické formule:*

(1) **true** a **false** jsou atomické formule.

(2) Každá výroková konstanta p_i je atomická formule.

(ii) *Formule:*

(1) Každá atomická formule je formule.

(2) Jsou-li A, B, C formule, jsou i $(\neg A)$, $(A \Rightarrow B)$, $(A \wedge B)$, $(A \vee B)$ a $(A \Leftrightarrow B)$ formule.

(3) Všechny formule jsou utvořeny pouze konečným počtem použití předchozích dvou pravidel.

V předchozí definici jsme definovali tzv. výrokové konstanty. Můžeme si položit otázku, proč používáme právě termín „konstanty", když tyto symboly mají zastupovat ve formulích různé výroky s různými pravdivostními hodnotami. Důvod bude zřejmější, jakmile zavedeme do formulí kvantifikátory. Zde budeme potřebovat ještě objekty jiného typu, jejichž význam bude proměnný i v rámci jedné dané konkrétní formule. Těm budeme říkat *výrokové proměnné*. Výrokové konstanty jsou tedy „konstantami" právě proto, že jejich význam je v rámci jedné formule neměnný. Poznamenejme ovšem, že některé jiné přístupy mezi výrokovými konstantami a proměnnými formálně nerozlišují (a nazývají objekty obojího typu „proměnnými"). Jiní autoři se raději tomuto pojmenování vyhýbají a používají raději termín *prvotní formule* nebo *atomické výroky*.

Příklad 3.1.1. Nechť p, q, r jsou atomické výroky. Pak správně vytvořené formule jsou například $(p \vee \neg q) \Rightarrow r$, $(r \Rightarrow (q \wedge p)) \vee (\neg p \Rightarrow r)$, $\neg(q \Rightarrow p) \wedge (p \Rightarrow (r \vee \neg q))$. Naopak výrazy $\vee(\Rightarrow r \wedge q)\neg r$, $r \wedge (r \Rightarrow \neg) \wedge p$ formulemi výrokového počtu nejsou.

Definice 3.1.2. Výrazy predikátového počtu jsou tvořeny z těchto symbolů:

(i) *Symboly pravdivostních hodnot:* **true** , **false** .

(ii) *Spojkama:* $\neg$ *(negace),* $\Rightarrow$ *(implikace),* $\wedge$ *(a),* $\vee$ *(nebo),* $\Leftrightarrow$ *(ekvivalence).*

(iii) *Operátory:* $=$ *(rovnost).*

(iv) *Kvantifikátory:* $\forall$ *(obecný* neboli *univerzální kvantifikátor),* $\exists$ *(existenční kvantifikátor).*

(v) *Konstanty:*

(1) *n-ární funkční konstanty* f_i^n *(kde* $i \geq 1$, $n \geq 0$*),* f_i^0 se nazývají *individuové konstanty a* označujeme je také a_i.

(2) *n-ární predikátové konstanty* p_i^n *(kde* $i \geq 1$, $n \geq 0$*);* p_i^0 se nazývají *výrokové konstanty.*

(vi) *Proměnné:*

(1) *n-ární funkční proměnné* F_i^n *(kde* $i \geq 1$, $n \geq 0$*);* F_i^0 se nazývají *individuové proměnné* a označujeme je *také* x_i.

(2) *n-ární predikátové proměnné* P_i^n *(kde* $i \geq 1$, $n \geq 0$*);* P_i^0 se nazývají *výrokové proměnné.*

Definujeme nyní rekurzívně tři třídy výrazů: termy, atomické formule a formule.

(i) *Termy:*

(1) Každá individuová konstanta a_i a individuová proměnná x_i je term.

(2) Jsou-li $t_1, t_2, \ldots, t_n$ $(n \geq 1)$ termy, jsou $f_i^n(t_1, t_2, \ldots, t_n)$ a $F_i^n(t_1, t_2, \ldots, t_n)$ termy.

(ii) *Atomické formule:*

(1) **true** a **false** jsou atomické formule.

(2) Každá výroková konstanta p_i^0 a výroková proměnná P_i^0 je atomická formule.

(3) Jsou-li $t_1, t_2, \ldots, t_n$ $(n \geq 1)$ termy, jsou $p_i^n(t_1, t_2, \ldots, t_n)$ a $P_i^n(t_1, t_2, \ldots, t_n)$ atomické formule.

(4) Jsou-li t_1 ,t_2 termy, je $(t_1 = t_2)$ atomická formule.

(iii) *Formule:*

(1) Každá atomická formule je formule.

(2) Jsou-li A, B, C formule, jsou i $(\neg A)$, $(A \Rightarrow B)$, $(A \wedge B)$, $(A \vee B)$ a $(A \Leftrightarrow B)$ formule.

(3) Je-li v_i proměnná (tj. F_i nebo P_i) a A formule, jsou $((\forall v_i)A)$ a $((\exists v_i)A)$ formule. Pro jednoduchost předpokládáme, že tuto definici lze použít jedině tehdy, když se ani $(\forall v_i)$ ani $(\exists v_i)$ již nevyskytuje v A.

Upozorňujeme na rozdíl mezi použitím spojky $\Leftrightarrow$ a operátoru rovnosti $=$. Ekvivalence vytváří z formulí formule tvaru:

$$\langle \text{formule} \rangle \Leftrightarrow \langle \text{formule} \rangle \,,$$

zatímco rovnost vytváří formule z termů:

$$\langle \text{term} \rangle = \langle \text{term} \rangle \,.$$

Formule, která je částí (podvýrazem) formule A, se nazývá *podformule* formule A. Buď dána formule $(\forall v_i)A$. Říkáme, že výskyt proměnné v_i je *kvantifikován* v $(\forall v_i)$ a *vázán* v A. Každý výskyt proměnné v_i v dané formuli, který není kvantifikovaný ani vázaný se nazývá *volný*. Proměnná je v dané formuli *volná*, existuje-li v ní aspoň jeden volný výskyt. Formule bez volných proměnných je *uzavřená*.

Příklad 3.1.2. Uvažujme formuli F:

$$(q \vee r) \Rightarrow \neg(p \wedge q).$$

Například řetězce:

$$q \vee r,\ \neg(p \wedge q),\ (p \wedge q),\ p \wedge q$$

jsou správně utvořenými podformulemi formule F. Naopak výrazy:

$$q \Rightarrow \neg(p \wedge q),\ (q \vee r) \Rightarrow (p \wedge q),\ (q \vee r) \Rightarrow \neg p$$

jsou sice syntakticky správně utvořené formule, ale nejsou podformulemi podformule F. Výrazy:

$$(\vee r)\neg(p \wedge q),\ \Rightarrow \neg(p\wedge),\ (q\vee) \Rightarrow \neg$$

nejsou ani samy formulemi a tedy ani podformulemi formule F.

Příklad 3.1.3. Uvažujme formuli P:

$$(\exists F)\{(F(a) = b) \wedge (\forall x)[p(x) \Rightarrow (F(x) = g(x, F(f(x))))]\}.$$

Její podvýrazy:

$$F(a),\ b,\ x,\ F(x),\ g(x, F(f(x)))$$

jsou termy, podvýrazy:

$$(F(a) = b),\ p(x),\ (F(x) = g(x, F(f(x))))$$

jsou atomické formule, podvýrazy

$$[p(x) \Rightarrow (F(x) = g(x, F(f(x))))],$$

$$(\forall x)[p(x) \Rightarrow (F(x) = g(x, F(f(x))))],$$

$$\{(F(a) = b) \wedge (\forall x)[p(x) \Rightarrow (F(x) = g(x, F(f(x))))]\}$$

a

$$(\exists F)\{(F(a) = b) \wedge (\forall x)[p(x) \Rightarrow (F(x) = g(x, F(f(x))))]\}$$

jsou formule.

Definice 3.1.3. Třída formulí popsaná definicí 3.1.2 se nazývá predikátový počet druhého řádu. Definujeme její čtyři podtřídy výčtem povolených symbolů:

(i) *Výrokový počet:*

(1) výrokové konstanty p_i^0.

(ii) *Výrokový počet s kvantifikátory:*

(1) výrokové konstanty p_i^0,

(2) výrokové proměnné P_i^0.

(iii) *Počet rovnosti:*

(1) individuové konstanty a_i,

(2) individuové proměnné x_i.

(iv) *Predikátový počet prvního řádu s rovností:*

(1) n-ární ($n \geq 0$) funkční konstanty f_i^n,

(2) n-ární ($n \geq 0$) predikátové konstanty p_i^n,

(3) individuové proměnné x_i.

Příklad 3.1.4. Uvažujme formule

$A:\ (p_1 \Rightarrow p_2) \Leftrightarrow ((\neg p_2) \Rightarrow (\neg p_1))$,

$B:\ \forall P_1(P_1 \Leftrightarrow p) \Rightarrow \exists P_2(P_2 \Leftrightarrow (\neg P_1))$,

$C:\ \forall x_1 \forall x_2 \forall x_3[(x_1 = x_2 \wedge x_2 = x_3) \Rightarrow x_1 = x_2]$,

$D:\ (x_1 \neq a) \wedge \forall x_2[\exists x_3 p(x_1, f(x_2, x_3)) \Rightarrow [p(x_2, x_1) \vee p(x_2, a)]]$.

Formule A až D příslušejí po řadě podtřídám 1 až 4. Formule P z příkladu 3.1.3 je formule predikátového počtu druhého řádu a nepatří do žádné z uvedených tříd, protože obsahuje unární funkční proměnnou F, což definice podtříd 1-4 nepřipouští.

Všimněme si, že ve výrokovém počtu nejsou povoleny žádné funkční symboly ani konstanty a proměnné. Výrokový počet proto neobsahuje žádné termy a proto ani operátor rovnosti "=" nemůže být použit. Totéž platí i pro výrokový počet s kvantifikátory. Nejdůležitější třídou je predikátový počet prvního řádu, který obsahuje výrokový počet a počet rovnosti jako své vlastní podtřídy. Jediné proměnné, které tato třída formulí obsahuje (a přes které lze tedy kvantifikovat), jsou individuové proměnné.

Každé formuli lze přiřadit význam tím, že vhodně "interpretujeme" její konstanty a volné proměnné. Při různých interpretacích dané formule dostáváme různé *výroky*, tj. tvrzení, která jsou buď pravdivá nebo nepravdivá.

Definice 3.1.4. *Booleovskou funkcí n argumentů* nebo-li *Booleovskou n-ární funkcí* nazýváme libovolné zobrazení $f : \{0,1\}^n \to \{0,1\}$.

Příklad 3.1.5. Uvažujme formuli $(p \vee \neg q) \Rightarrow r$. Tato formule definuje jistou Booleovskou funkci $f : \{0,1\}^3 \to \{0,1\}$ tří argumentů, pokud prvky množiny $\{0,1\}$ chápeme jako symboly pro pravdivostní hodnoty, nad nimiž pak můžeme provádět logické operace. Tak například $f(1,0,1) = ((1 \vee \neg 0) \Rightarrow 1) = (1 \vee 1) \Rightarrow 1) = (1 \Rightarrow 1) = 1$. Tedy, volbou (interpretací) p jako *pravda*, q jako *nepravda* a r jako *pravda* jsme získali interpretací formule $(p \vee \neg q) \Rightarrow r$ pravdivý výrok.

V předchozím příkladě jsme přiřadili pravdivostní hodnotu výrokovým konstantám p, q, r a na základě vyhodnocení logických operací jsme získali i pravdivostní hodnotu složitější formule. V následujícím kroku tento postup zobecníme. Co tedy potřebujeme k tomu, abychom pomocí dané formule výrokového počtu vytvořili Booleovskou funkci n argumentů?

(i) Potřebujeme formuli, řekněme F, která obsahuje právě n výrokových konstant, například $\{p_1, p_2, \ldots p_n\}$,

(ii) zvolíme nějaké pravdivostní ohodnocení $\vartheta : \{p_1, p_2, \ldots p_n\} \to \{0,1\}$ výrokových konstant

(iii) a toto ohodnocení konzistentně rozšíříme na celou formuli F pomocí rekurze.

Hodnotu $\vartheta(F)$ vezmeme jako hodnotu právě definované Booleovské funkce f na vektoru pravdivostních hodnot z množiny $\{0,1\}^n$, přiřazených výrokovým konstantám z množiny $\{p_1, p_2, \ldots p_n\}$. Pravdivostní hodnoty z n-rozměrného vektoru z $\{0,1\}^n$ jsou přiřazovány funkcí ϑ výrokovým konstantám podle jejich přirozeného pořadí, v kontextu příkladu 3.1.5 při $n = 3$ byl vybrán vektor $(1,0,1) \in \{0,1\}^3$ a tedy $\vartheta(p) = 1$, $\vartheta(q) = 0$, $\vartheta(r) = 1$. Zadaná formule $F = (p \vee \neg q) \Rightarrow r$ pak získá ohodnocení $\vartheta(F) = 1$, vypočítané v příkladě 3.1.5, takže také $f(1,0,1) = 1$. Vše lze ještě poněkud zjednodušit, použijeme-li $\{p_1, p_2, \ldots p_n\}$ jako indexovou množinu kartézského součinu $\{0,1\}^n$ n kopií množiny $\{0,1\}$. Potom ϑ je přímo prvek z $\{0,1\}^n$ a lze tedy položit $f(\vartheta) = \vartheta(F)$. V kontextu příkladu 3.1.5 tedy $\vartheta = (1,0,1)$, a po dosazení jednotlivých formulí máme $\vartheta(p) = (1,0,1)(p) = 1$,

$\vartheta(q) = (1,0,1)(q) = 0$, $\vartheta(r) = (1,0,1)(r) = 1$, $\vartheta(F) = (1,0,1)(F) = 1$. K úplnosti celé konstrukce už zbývá jen vhodně pojmenovat funkci ϑ a popsat způsob, jakým ji rozšíříme z výrokových konstant (nebo-li atomických výroků, prvotních formulí) na libovolnou formuli výrokového počtu.

Definice 3.1.5. Buď P množina výrokových konstant. Zobrazení $\vartheta : P \to \{0,1\}$ se nazývá *evaluační funkcí*. Jiný název pro evaluační funkci je *ohodnocení formulí* nebo *valuace*.

Předpokládejme nyní, že jsou již definovány hodnoty $\vartheta(A)$, $\vartheta(B)$ pro dvě formule A, B. Pro formule $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$ definujeme rozšíření ϑ podle tabulky:

$\vartheta(A)$	$\vartheta(B)$	$\vartheta(\neg A)$	$\vartheta(A \wedge B)$	$\vartheta(A \vee B)$	$\vartheta(A \Rightarrow B)$	$\vartheta(A \Leftrightarrow B)$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Poznamenejme, že existuje formální rozdíl mezi funkcí a jejím rozšířením na větší definiční obor. Pro větší jednoduchost však budeme rozšíření libovolné evaluační funkce ϑ na všechny formule výrokového počtu značit stejným symbolem ϑ. Nyní tedy můžeme považovat všechny evaluační funkce za definované na celé množině formulí výrokového počtu, sestrojenými nad jazykem $\mathcal{L}$ a množinou výrokových konstant ve smyslu definice 3.1.1.

Definice 3.1.6. Buď M neprázdná množina. Pod *n-ární funkcí* Φ nad M rozumíme zobrazení $\Phi : M^n \to M$. Pod *n-árním predikátem* Ψ rozumíme zobrazení $\Psi : M^n \to \{\textit{pravda}, \textit{nepravda}\}$. Připouštíme i případ $n = 0$, kde 0-*ární funkce* nad M označuje pevný prvek z M, 0-*ární predikát* nad M označuje pevnou pravdivostní hodnotu (*pravda* nebo *nepravda*).

Booleovská funkce n-argumentů je tedy zvláštním případem n-ární funkce nad $M = \{0,1\}$. Zároveň však plní i roli n-árního predikátu, pokud prvky z množiny $\{0,1\}$ identifikujeme se symboly pro pravdivostní hodnoty *nepravda*, *pravda* (v tomto pořadí).

Příklad 3.1.6. Buď $M = \mathbb{Z}$. Termy $x_1 + 2$, $x_1 - 3 \cdot x_2$, $x_1 \cdot x_2 + x_3$ můžeme chápat interpretovaně jako unární, binární a ternární funkce nad $\mathbb{Z}$. Formule $x_3 = 1$, $x_1 < x_2$, $x_1 - x_3 = x_2$ můžeme chápat interpretovaně jako unární, binární a ternární predikát nad $\mathbb{Z}$. Přitom symboly 0 a 1 jsou individuové konstanty, představující pevné prvky ze $\mathbb{Z}$, individuové proměnné $x_1, x_2, \ldots$ interpretujeme jako libovolné prvky ze $\mathbb{Z}$, binární funkční konstanty "+", "$\cdot$" interpretujeme jako klasické sčítání a násobení v $\mathbb{Z}$ a binární predikátový symbol "$<$" interpretujeme jako klasickou nerovnost v $\mathbb{Z}$.

Definice 3.1.7. *Interpretací* formule A rozumíme trojici $(M, \mathcal{I}_c, \mathcal{I}_v)$, kde:

(i) $M \neq \varnothing$, zvaná *obor interpretace (nad M)*,

(ii) $\mathcal{I}_c$ udává interpretaci *konstant* z formule A:

(1) Každé funkční konstantě f_i^n, $(n \geq 0)$, která se vyskytuje v A, je přiřazena jistá n-ární funkce nad M. Speciálně, pro $n = 0$ je každé individuové konstantě a_i z A přiřazen jistý prvek z M,

(2) Každé predikátové konstantě p_i^n, $(n \geq 0)$, která se vyskytuje v A, je přiřazen jistý n-ární predikát nad M. Speciálně, pro $n = 0$ je každé výrokové konstantě z A přiřazena pravdivostní hodnota *pravda* nebo *nepravda*.

(iii) $\mathcal{I}_v$ udává interpretaci *volných proměnných* z formule A:

(1) Každé volné funkční proměnné F_i^n, $(n \geq 0)$, která se vyskytuje v A, je přiřazena jistá n-ární funkce nad M. Speciálně pro $n = 0$ je každé volné individuové proměnné x_i z A přiřazen jistý prvek z M.

(2) Každé volné predikátové proměnné P_i^n, $(n \geq 0)$, která se vyskytuje v A, je přiřazen n-ární predikát nad M. Speciálně pro $n = 0$ je každé volné výrokové proměnné z A přiřazena pravdivostní hodnota *pravda* nebo *nepravda*.

Je-li dána interpretace $\mathcal{I}$ formule A, pak nechť $\langle A, \mathcal{I} \rangle$ označuje výrok (někdy také nazývaný *interpretovanou formulí*) s pravdivostní hodnotou *pravda* nebo *nepravda*, získanou tímto postupem: Nejprve provedeme všechna přiřazení konstantám v A tak, jak předepisuje I_c a přiřazení volným proměnným v A tak, jak předepisuje $\mathcal{I}_v$. Pak stanovíme *význam* neboli *sémantiku* formule A, a to na základě významu symbolů pravdivostních hodnot, spojek, operátorů a kvantifikátorů, jenž je určen takto:

(i) *Význam symbolů pravdivostních hodnot*: Význam **true** je *pravda*, význam **false** je *nepravda*.

(ii) *Význam spojek je určen následující tabulkou*:

$\langle A, \mathcal{I} \rangle$	$\langle B, \mathcal{I} \rangle$	$\langle \neg A, \mathcal{I} \rangle$	$\langle A \wedge B, \mathcal{I} \rangle$	$\langle A \vee B, \mathcal{I} \rangle$	$\langle A \Rightarrow B, \mathcal{I} \rangle$	$\langle A \Leftrightarrow B, \mathcal{I} \rangle$
pravda	*pravda*	*nepravda*	*pravda*	*pravda*	*pravda*	*pravda*
pravda	*nepravda*	*nepravda*	*nepravda*	*pravda*	*nepravda*	*nepravda*
nepravda	*pravda*	*pravda*	*nepravda*	*pravda*	*pravda*	*nepravda*
nepravda	*nepravda*	*pravda*	*nepravda*	*nepravda*	*pravda*	*pravda*

(iii) *Význam kvantifikátorů*: Uvažujme formule a podformule tvaru $(\forall F_i^n)A$, $(\forall P_i^n)A$, $(\exists F_i^n)A$, $(\exists P_i^n)A$.

(1) Kvantifikátor $\forall$ zastupuje frázi "pro všechna. . . ,. . . je pravda". Hodnota podformule $(\forall F_i^n)A$ je tedy *pravda*, právě když platí, že hodnota podformule A je pravda při přiřazení libovolné n-ární funkce Φ nad M všem výskytům F_i^n; jinak význam $(\forall F_i^n)A$ je *nepravda*. Podobně, hodnota $(\forall P_i^n)A$ je *pravda*, právě když hodnota podformule A je *pravda* při přiřazení libovolného n-árního predikátu Ψ nad M všem výskytům P_i^n; jinak hodnota $(\forall P_i^n)A$ je *nepravda*.

(2) Kvantifikátor $\exists$ zastupuje frázi "existuje... tak, že ...je pravda". Hodnota podformule $(\exists F_i^n)A$ je tedy pravda, právě když platí, že hodnota podformule A je *pravda* při přiřazení vhodné n-ární funkce Φ nad M všem výskytům F_i^n; jinak hodnota $(\exists F_i^n)A$ je *nepravda*. Podobně, hodnota podformule $(\exists P_i^n)A$ je *pravda*, právě když hodnota podformule A je *pravda* při přiřazení vhodného n-árního predikátu Ψ nad M všem výskytům P_i^n; jinak hodnota $(\exists P_i^n)A$ je *nepravda*.

(iv) *Význam operátorů*: Význam operátoru "=" je dán binární funkcí zobrazující množinu $M \times D$ do množiny $\{pravda, nepravda\}$, která je určena tímto vztahem: Pro $d_1, d_2 \in D$, $d_1 = d_2$ je *pravda*, právě když d_1 a d_2 označují týž prvek z M.

Příklad 3.1.7. Formule

$$\exists x \forall y [p(y) \Rightarrow x = y]$$

říká, že "existuje x takové, že pro všechna y, je-li $p(y)$, pak je $x = y$", čili jednodušeji, "existuje nejvýše jedno x takové, že $p(x)$". Tato formule nabývá hodnoty *pravda* v každé interpretaci s libovolným oborem interpretace M a libovolným přiřazením unárního predikátu nad M predikátové konstantě p, pokud $p(d)$ je *pravda* pro nejvýše jeden prvek d z M.

Definice 3.1.8. Formule výrokového počtu A se nazývá *pravdivá vzhledem k evaluační funkci* $\vartheta : P \to \{0, 1\}$, jestliže $\vartheta(A) = 1$. Formule výrokového počtu A se nazývá *logicky pravdivá* neboli *tautologie*, jestliže je pravdivá vzhledem ke každé evaluační funkci ϑ. Pokud naopak existuje aspoň jedna evaluační funkce, pro kterou je $\vartheta(A) = 0$, říkáme, že ϑ *vyvrací* formuli A. Formule A se nazývá *nesplnitelná* nebo-li *kontradikce*, pokud $\vartheta(A) = 0$ pro každou evaluační funkci ϑ. Formule A se nazývá *splnitelná*, jestliže $\vartheta(A) = 1$ pro aspoň jednu evaluaci ϑ. V takovém případě se nazývá ϑ *model* formule A. Je zřejmé, že formule A je tautologie, právě když je $\neg A$ kontradikce.

K vymezení pojmu pravdivosti formulí predikátového počtu slouží následující definice:

Definice 3.1.9. Formule predikátového počtu A se nazývá *pravdivá vzhledem k interpretaci* $\mathcal{I}$, nabývá-li pro tuto interpretaci hodnoty *pravda*. Formule A se nazývá *logicky pravdivá* neboli *tautologie*, je-li pravdivá vzhledem ke každé interpretaci. Existuje-li naopak aspoň jedna interpretace $\mathcal{I}$, v níž formule A nabývá hodnoty *nepravda*, říkáme, že interpretace $\mathcal{I}$ *vyvrací* formuli A. Formule A se nazývá *nesplnitelná*, nabývá-li pro každou interpretaci hodnoty *nepravda*. Formule A je naopak splnitelná, existuje-li nějaká interpretace, v níž A nabývá hodnoty *pravda*; každá taková interpretace se nazývá *model* formule A. Je zřejmé, že formule A je logicky pravdivá, právě když formule $\neg A$ je nesplnitelná.

Definice 3.1.10. Pojem modelu můžeme přirozeným způsobem rozšířit také na množinu formulí. Je-li T množina jistých formulí výrokového počtu, evaluační funkci $\vartheta : P \to \{0, 1\}$ nazýváme *modelem* množiny T, jestliže $\vartheta(A) = 1$ pro každou formuli $A \in T$. Je zřejmé, že pro konečnou množinu T je to právě tehdy, když ϑ je modelem formule, která vznikne

konjunkcí všech formulí z množiny T. Analogicky můžeme na množinu formulí rozšířit pojem splnitelnosti. Množina formulí T se nazývá *splnitelná*, existuje-li její model. Podobně můžeme pojmy modelu a splnitelnosti rozšířit i na komplikovanější třídy formulí predikátového počtu.

Definice 3.1.11. Formule A výrokového počtu se nazývá *tautologickým důsledkem* množiny formulí T, jestliže pro každý model $\vartheta : P \to \{0,1\}$ množiny T je $\vartheta(A) = 1$.

Věta 3.1.1. *Následující podmínky jsou pro formuli A a množinu formulí T výrokového počtu ekvivalentní:*

(i) *Formule A je tautologickým důsledkem množiny formulí T.*

(ii) *Množina formulí $T \cup \{\neg A\}$ je nesplnitelná.*

(iii) *Pro každou evaluační funkci ϑ je některá formule z množiny $\{\neg B |\, B \in T\} \cup \{A\}$ pravdivá vzhledem k ϑ.*

Důkaz. (i) $\Rightarrow$ (ii). Předpokládejme, že A je tautologickým důsledkem T. Kdyby ϑ byl model množiny $T \cup \{\neg A\}$, pak ϑ je model i menší množiny T, přičemž $\vartheta(\neg A) = 1$, což znamená $\vartheta(A) = 0$. To je ovšem spor s předpokladem, že A je tautologickým důsledkem množiny T.

(ii) $\Rightarrow$ (iii). Nechť je množina $T \cup \{\neg A\}$ nesplnitelná. Pak pro každou evaluační funkci ϑ, pro kterou $\vartheta(A) = 0$ (a tedy $\vartheta(\neg A) = 1$) existuje formule $B \in T$, pro kterou $\vartheta(B) = 0$ – jinak by totiž byla $T \cup \{\neg A\}$ splnitelná. Pak ovšem $\vartheta(\neg B) = 1$. Tedy, každá evaluační funkce ϑ nabývá na některé formuli z množiny $\{\neg B |\, B \in T\} \cup \{A\}$ hodnoty 1, tj. je pro tuto evaluační funkci pravdivá.

(iii) $\Rightarrow$ (i). Předpokládejme, že pro každou evaluační funkci ϑ je některá formule z $\{\neg B |\, B \in T\} \cup \{A\}$ pravdivá. Zvolme nyní ϑ tak, že je modelem množiny T. Pak pro všechny $B \in T$ je $\vartheta(\neg B) = 0$, což znamená, že $\vartheta(A) = 1$. Tedy A je tautologickým důsledkem množiny formulí T. □

Softwarové nástroje: Tautologický důsledek

Příklad 3.1.8. Formule

$$\exists P \forall x \exists y [P(x,x) \wedge \neg P(x,y)]$$

není ani logicky pravdivá ani nesplnitelná: Je-li v oboru interpretace M jediný prvek, pak $P(x,x) \wedge \neg P(x,y)$ je *nepravda* při libovolné interpretaci predikátové proměnné P, neboť prvky přiřazené proměnným x a y jsou stejné. Jsou-li v M aspoň dva prvky, přiřadíme predikátové proměnné P libovolný binární predikát nad M, který nabývá hodnoty *pravda* právě nad dvojicemi $(d,d) \in D \times D$. Pro každé přiřazení prvku $d_x \in D$ proměnné x lze tedy najít přiřazení $d_y \in D$ proměnné y, že $d_y \neq d_x$. Pak ovšem $P(x,x) \wedge \neg P(x,y)$ je pravda, takže i $\exists P \forall x \exists y [P(x,x) \wedge \neg P(x,y)]$ nabude v této interpretaci hodnoty *pravda*.

Věta 3.1.2. *(O logické pravdivosti ve výrokovém počtu, W. V. Quine, 1950) Existují algoritmy, které rozhodnou, zda je nebo není daná formule výrokového počtu pravdivá.*

Podrobný důkaz je poměrně zdlouhavý a základní učebnice jej většinou v plné šíři neuvádí. Zájemce z řad studentů odkazujeme na dostupnou literaturu. Místo toho uvedeme princip důkazu věty poněkud obecnější.

Věta 3.1.3. *Existují algoritmy, které rozhodnou, zda je nebo není daná formule výrokového počtu s kvantifikátory pravdivá.*

Důkaz. Princip důkazu Nechť je dána formule výrokového počtu s kvantifikátory. Upravíme ji nejprve na ekvivalentní formuli bez výrokových proměnných, a to tak, že každou podformuli tvaru $(\forall P_i^0)(B_i^0)$ nahradíme podformulí $B(\mathbf{true}) \wedge B(\mathbf{false})$ a každou podformuli tvaru $(\exists P_i^0)(B_i^0)$ podformulí $B(\mathbf{true}) \vee B(\mathbf{false})$; výslednou formuli označme A. V dalším kroku eliminujeme postupně zvolenou konstantu p_i^0 tak, že $A(p_i^0)$ nahradíme podformulí $A(\mathbf{true}) \wedge A(\mathbf{false})$. Tento proces je postupně opakován pro všechny výrokové konstanty. Jestliže zjednodušujeme současně získávané formule ve shodě s významem výrokových spojek, získáme nakonec terminální formuli **true** nebo **false**. Daná formule je logicky pravdivá, právě když z ní popsaným způsobem vznikne formule **true**.

□

Rozhodnutelnost výrokového počtu lze převést i na další třídy formulí predikátového počtu ve smyslu následující věty.

Věta 3.1.4. *(O tautologiích) Nechť A je formule výrokového počtu s výrokovými konstantami $p_1, p_2, \ldots, p_n$. Nechť A' vznikne tak, že každý výskyt konstanty $p_i (1 \leq i \leq n)$ v A nahradíme jistou formulí B_i predikátového počtu. Je-li A logicky pravdivá, je i A' logicky pravdivá.*

Pojem ekvivalence formulí, o němž jsme se zmínili v ukázce důkazu věty 3.1.3 budeme dále precizovat.

Definice 3.1.12. Dvě formule A, B výrokového počtu se nazývají ekvivalentní, jestliže $\vartheta(A) = \vartheta(B)$ pro libovolnou evaluační funkci $\vartheta : P \to \{0,1\}$.

Věta 3.1.5. *Dvě formule A, B výrokového počtu (nad stejnou množinou výrokových konstant) jsou ekvivalentní, právě když definují stejnou Booleovskou funkci.*

Důkaz. Nechť $f_A : \{0,1\}^n \to \{0,1\}$, $f_B : \{0,1\}^m \to \{0,1\}$ jsou Booleovské funkce, definované formulemi A, B. Předpokládejme, že $f_A = f_B$. Pak $n = m$ a pro libovolnou evaluační funkci $\vartheta \in \{0,1\}^n$ platí $\vartheta(A) = f_A(\vartheta) = f_B(\vartheta) = \vartheta(B)$. Tedy, formule A, B jsou ekvivalentní.

Naopak, mějme dvě ekvivalentní formule A, B. Pak pro libovolnou evaluační funkci $\vartheta : P \to \{0,1\}$ platí $\vartheta(A) = \vartheta(B)$. Pak ovšem $f_A(\vartheta) = \vartheta(A) = \vartheta(B) = f_B(\vartheta)$, což znamená, že $f_A = f_B$. □

Definice 3.1.13. Řekneme, že formule A, B jsou ekvivalentní, jestliže nabývají stejné pravdivostní hodnoty v každé interpretaci, která přiřazuje vhodné objekty všem konstantám a volným proměnným vyskytujícím se v A, B. Jinak řečeno, formule A, B jsou ekvivalentní, právě když je formule $(A \Leftrightarrow B)$ logicky pravdivá.

Věta 3.1.6. *(O náhradě) Nechť A' je formule, obsahující podformuli A a nechť B' vznikne náhradou některých výskytů podformule A v A' formulí B. Jsou-li A, B ekvivalentní, jsou ekvivalentní i A' a B'.*

Další důležitou vlastností ekvivalence formulí je její tranzitivnost. Jsou-li A, B ekvivalentní formule a B, C ekvivalentní formule, jsou také formule A, C ekvivalentní.

Příklad 3.1.9. Příklady ekvivalentních formulí (ekvivalence formulí je zapsána ve tvaru tautologie užitím spojky "⇔"):

$$\neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B),$$

De Morganovy zákony

$$\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B),$$

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B),$$

komutativní zákony

$$A \vee B \Leftrightarrow B \vee A,$$

$$A \wedge B \Leftrightarrow B \wedge A,$$

$$(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A),$$

asociativní zákony

$$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C),$$

$$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C),$$

$$[(A \Leftrightarrow B) \Leftrightarrow C] \Leftrightarrow [A \Leftrightarrow (B \Leftrightarrow C)],$$

a distributivní zákony

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C),$$

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C).$$

Definice 3.1.14. Buď $p \in P$ výroková konstanta. Pak formule p a $\neg p$ se nazývají jejími *literály*.

Definice 3.1.15. Buď F formule výrokového počtu. Řekneme, že je F v *disjunktivní normální formě*, jestliže je F disjunkcí konečně mnoha podformulí (tzv. disjunktů), z nichž každá je konjunkcí konečně mnoha literálů. Disjunktivní normální forma formule A se nazývá *úplná*, jestliže každý disjunkt obsahuje literály všech výrokových konstant, vyskytujících se ve formuli A, přičemž se v žádném z disjunktů nevyskytuje výroková konstanta současně se svojí negací.

Definice 3.1.16. Buď F formule výrokového počtu. Řekneme, že je F v *konjunktivní normální formě*, jestliže je F konjunkcí konečně mnoha podformulí (tzv. konjunktů), z nichž každá je disjunkcí konečně mnoha literálů. Konjunktivní normální forma formule A se nazývá *úplná*, jestliže každý konjunkt obsahuje literály všech výrokových konstant, vyskytujících se ve formuli A, přičemž se v žádném z konjunktů nevyskytuje výroková konstanta současně se svojí negací.

Věta 3.1.7. *Každá formule výrokového počtu, která není kontradikcí, je ekvivalentní některé formuli v úplné disjunktivní normální formě.*

Věta 3.1.8. *Každá formule výrokového počtu, která není tautologií, je ekvivalentní některé formuli v úplné konjunktivní normální formě.*

Příklad 3.1.10. Uvažujme formuli $F = (p \Rightarrow q) \vee r$. Tato formule je ekvivalentní formuli $G = \neg p \vee q \vee r$. Formule G je v normální disjunktivní formě, jejíž disjunkty jsou podformule $\neg p$, q, r. Každý z těchto disjunktů je konjunkcí právě jednoho literálu – sebe sama, neboť je každý z nich sám literálem. Zároveň je G v normální

konjunktivní formě s jediným konjunktem, kterým je sama formule G, tj. $\neg p \vee q \vee r$. Jako disjunktivní normální forma není G úplná, neboť disjunkty neobsahují literály všech výrokových konstant, použitých ve formuli F, resp. G. Naopak jako konjunktivní forma je G úplná. Úplnou disjunktivní normální formou formulí F, G je formule $N = (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$.

Příklad 3.1.11. Ukážeme nyní detailní postup nalezení normální disjunktivní formy formule F z předchozího příkladu. Každý řádek následující tabulky představuje jinou evaluační funkci ϑ pro množinu výrokových konstant $P = \{p, q, r\}$. Tuto evaluační funkci můžeme přímo ztotožnit s vektorem jejích funkčních hodnot na prvcích množiny P:

$\vartheta(p)$	$\vartheta(q)$	$\vartheta(r)$	$\vartheta((p \Rightarrow q) \vee r)$	Disjunkty:
1	1	1	1	$p \wedge q \wedge r$
1	1	0	1	$p \wedge q \wedge \neg r$
1	0	1	1	$p \wedge \neg q \wedge r$
1	0	0	0	
0	1	1	1	$\neg p \wedge q \wedge r$
0	1	0	1	$\neg p \wedge q \wedge \neg r$
0	0	1	1	$\neg p \wedge \neg q \wedge r$
0	0	0	1	$\neg p \wedge \neg q \wedge \neg r$

Každé evaluační funkci, která na formuli F nabývá hodnoty 1 přísluší právě jeden disjunkt, na němž právě tato evaluace (a žádná jiná) nabývá hodnoty 1. V daném případě máme tedy 7 disjunktů, jejichž celková disjunkce $N = (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$ je ekvivalentní zadané formuli F. Podle definice 3.1.15 je tato formule úplnou normální formou formule F.

Dále budeme hledat minimální tvar této normální disjunktivní formy pomocí Quine-McCluskeyova algoritmu. Především si můžeme povšimnout, že každý z disjunktů, které tvoří úplnou normální disjunktivní formu, je ve vzájemně jednoznačné korespondenci s vektorem ohodnocení výrokových konstant, tedy vlastně s příslušnou evaluační funkcí, která je v daném případě charakterizována trojicí číslic, nul nebo jedniček. Proto můžeme pro jednoduchost pracovat s těmito posloupnostmi číslic, místo s disjunkty, a nakonec se opět můžeme vrátit k výrokovým formulím.

V daném případě máme tedy celkem 7 uspořádaných trojic $(1,1,1)$, $(1,1,0)$, $(1,0,1)$, $(0,1,1)$, $(0,1,0)$, $(0,0,1)$, $(0,0,0)$. Budeme hledat všechny možné případy, kdy se dvě tro-

jice shodují s výjimkou jedné pozice. Pokud takovou shodu nalezneme, vytvoříme trojici, v níž číslice, v nichž se obě trojice liší, nahradíme symbolem $*$. Například, první a druhá trojice se shodují, a tedy dávají vzniknout jejich společné instanci $(1, 1, *)$. Postupně takto vzniká posloupnost $(1, 1, *)$, $(1, *, 1)$, $(*, 1, 1)$, $(*, 1, 0)$, $(*, 0, 1)$, $(0, 1, *)$, $(0, *, 1)$, $(0, *, 0)$, $(0, 0, *)$. Pokud by vzniklo v této fázi postupu více stejných posloupností, duplikáty vynecháme. Postup opakujeme tak dlouho, až se všechny posloupnosti liší na více než jednom místě. V daném případě potřebujeme ještě jeden krok, v němž vznikne posloupnost $(*, 1, *)$, $(*, *, 1)$, $(*, 1, *)$, $(*, *, 1)$, $(0, *, *)$, $(0, *, *)$, což po odstranění duplikátů dává $(*, 1, *)$, $(*, *, 1)$, $(0, *, *)$.

Posloupnosti, které jsme nalezli, představují „šablony" (skutečný význam pravděpodobně vystihuje nejlépe anglické slovo „pattern"), které ve hvězdičkové konvenci musí pokrýt všechny původní posloupnosti, asociované s disjunkty, aby vyjádřily původní formuli F. To lze přehledně znázornit tabulkou:

	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$
$(*,1,*)$	$\times$	$\times$		$\times$	$\times$		
$(*,*,1)$	$\times$		$\times$	$\times$		$\times$	
$(0,*,*)$				$\times$	$\times$	$\times$	$\times$

Pokud se příslušná šablona, zapsaná v prvním sloupci tabulky shoduje s posloupností v prvním řádku, zapíšeme do příslušného pole tabulky symbol $\times$. Nyní je nutné zajistit, aby byl každý disjunkt pokryt příslušnou šablonou. Prohlédneme sloupce tabulky a tam, kde je v příslušném sloupci přítomen pouze jediný symbol $\times$, jej změníme na $\otimes$. Totéž pak provedeme v celém řádku, kde tento symbol leží. Konkrétně tedy, vidíme, že například druhý sloupec obsahuje jediný symbol $\times$, a to v prvním řádku. Abychom pokryli v pořadí druhý disjunkt, tj. $p \wedge q \wedge \neg r$, musíme nutně použít šablonu z prvního řádku, která vyjadřuje formuli q. Tím však jsme zároveň pokryli, kromě druhého disjunktu, také disjunkt první, čtvrtý a pátý, což jsme vyjádřili umístěním symbolu $\otimes$ do průsečíků příslušných řádků a sloupců. Totéž provedeme i pro ostatní sloupce, přičemž hledáme minimální množinu „šablon", které pokrývají všechny posloupnosti, asociované s disjunkty, tvořícími úplnou normální disjunktivní formu formule F:

	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$
$(*,1,*)$	$\otimes$	$\otimes$		$\otimes$	$\otimes$		
$(*,*,1)$	$\otimes$		$\otimes$	$\otimes$		$\otimes$	
$(0,*,*)$				$\otimes$	$\otimes$	$\otimes$	$\otimes$

V daném případě jsme museli použít všechny tři „šablony" a tedy hledaná, minimalizovaná normální disjunktivní forma formule F má tvar $\neg p \vee \ q \vee r$.

Příklad 3.1.12. Nalezneme úplnou normální konjunktivní formu formule $F = \neg(p \Rightarrow q) \vee r$. Její pravdivostní tabulka má tvar:

$\vartheta(p)$	$\vartheta(q)$	$\vartheta(r)$	$\vartheta(\neg(p \Rightarrow q) \vee r)$	Konjunkty:
1	1	1	1	
1	1	0	0	$\neg p \vee \neg q \vee r$
1	0	1	1	
1	0	0	1	
0	1	1	1	
0	1	0	0	$p \vee \neg q \vee r$
0	0	1	1	
0	0	0	0	$p \vee q \vee r$

Pro každou evaluační funkci, v níž má daná formule pravdivostní hodnotu 0, jsme vytvořili konjunkt, který má pravdivostní hodnotu 0 pouze pro tuto jedinou evaluaci. Pak ovšem společná konjunkce těchto konjunktů tvoří úplnou normální konjunktivní formu $K = (\neg p \vee \neg q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee r)$ formule F. Tuto konjunktivní formu dále minimalizujeme Quine-McCluskeyovým algoritmem. Nalezeným konjunktům odpovídají evaluační funkce, vyjádřené posloupnostmi $(1,1,0)$, $(0,1,0)$ a $(0,0,0)$, které generují (postupem analogickým jako v příkladě 3.1.11) šablony $(*,1,0)$ a $(0,*,0)$. Ty odpovídají formulím $\neg q \vee r$ a $p \vee r$, přičemž obě šablony jsou nutné k pokrytí všech tří posloupností, asociovaných s konjunkty. Jejich konjunkce $M = (\neg q \vee r) \wedge (p \vee r)$ je proto hledanou minimalizovanou normální konjunktivní formou.

Softwarové nástroje: Formule výrokového počtu

Definice 3.1.17. Řekneme, že formule $A(x)$, $A(y)$ jsou si *podobné*, jestliže jsou všechny volné výskyty proměnné y ve formuli $A(y)$ právě na těch místech, kde v $A(x)$ jsou volné výskyty proměnné x.

Příklad 3.1.13. Formule

$$A(x): \quad \exists z[x \neq z \wedge P(z,x)] \quad \text{a} \quad A(y): \quad \exists z[y \neq z \wedge P(z,y)]$$

jsou podobné, zatímco formule

$$B(x): \quad \exists z(x \neq z) \wedge \forall y P(x,y) \quad \text{a} \quad B(y): \exists z(y \neq z) \wedge \forall y P(y,y)$$

podobné nejsou, neboť v $B(x)$ je proměnná x v $P(x,y)$ volná, ale v $B(y)$ je proměnná y v $P(y,y)$ vázaná.

Je zřejmé, že pokud jsou formule $A(x)$, $A(y)$ podobné, pak formule $\forall x A(x)$, $\forall y A(y)$ jsou ekvivalentní.

Definice 3.1.18. Nechť A je formule a $v_1, v_2, \ldots, v_n$ všechny její navzájem různé volné proměnné. Formuli $\forall v_1 \forall v_2 \ldots \forall v_n A$, resp. $\exists v_1 \exists v_2 \ldots \exists v_n A$ říkáme *univerzální uzávěr*, resp. *existenční uzávěr* formule A.

Je zřejmé, že formule je logicky pravdivá, právě když je její univerzální uzávěr logicky pravdivý; a nesplnitelná, právě když je její existenční uzávěr nesplnitelný.

Definice 3.1.19. Říkáme, že je formule v *prenexní konjunktivní normální formě*, má-li tvar

$$(\square v_1)(\square v_2)\ldots(\square v_n)\{[A_{11} \vee A_{12} \vee \ldots \vee A_{1t_1}] \wedge$$

$$\wedge [A_{21} \vee A_{22} \vee \ldots \vee A_{2t_2}] \wedge \ldots \wedge [A_{m1} \vee A_{m2} \vee \ldots \vee A_{mt_m}]\},$$

kde $\square$ označuje buď obecný nebo existenční kvantifikátor, $v_1, v_2, \ldots, v_n$ jsou navzájem různé funkční a predikátové proměnné vystupující v podformulích A_{ij}. Každá z podformulí A_{ij} je buď atomická formule, nebo je to negace atomické formule. Začátek formule, tj. $\square v_1)(\square v_2)\ldots(\square v_n)$ se nazývá *prefix* formule, zbytek se nazývá *matice* formule. Nepožaduje se, aby všechny proměnné vyskytující se v matici byly obsaženy v prefixu, tj. formule v prenexní konjunktivní normální formě nemusí být uzavřená.

Definice 3.1.20. Říkáme, že je formule v *prenexní disjunktivní normální formě*, má-li tvar

$$(\square v_1)(\square v_2)\ldots(\square v_n)\{[A_{11} \wedge A_{12} \wedge \ldots \wedge A_{1t_1}] \vee$$

$$\vee [A_{21} \wedge A_{22} \wedge \ldots \wedge A_{2t_2}] \vee \ldots \vee [A_{m1} \wedge A_{m2} \wedge \ldots \wedge A_{mt_m}]\},$$

kde $\square$ označuje buď obecný, nebo existenční kvantifikátor, $v_1, v_2, \ldots, v_n$ jsou navzájem různé funkční a predikátové proměnné vystupující v podformulích A_{ij}. Každá z podformulí A_{ij} je buď atomická formule, nebo je to negace atomické formule. Začátek formule, tj. $\square v_1)(\square v_2)\ldots(\square v_n)$ se nazývá *prefix* formule, zbytek se nazývá *matice* formule. Nepožaduje se, aby všechny proměnné vyskytující se v matici byly obsaženy v prefixu, tj. formule v prenexní disjunktivní normální formě nemusí být uzavřená.

Věta 3.1.9. *Každá formule může být převedena na ekvivalentní formuli prenexní konjunktivní normální formě.*

Věta 3.1.10. *Každá formule může být převedena na ekvivalentní formuli prenexní disjunktivní normální formě.*

Důkaz obou vět je poměrně jednoduchý, avšak zdlouhavý. Spočívá v postupné eliminaci nadbytečných proměnných, přejmenování proměnných, eliminaci spojek "$\Rightarrow$" a "$\Leftrightarrow$", které lze vyjádřit pomocí spojek "$\vee$", "$\wedge$" a "$\neg$", a použití dalších ekvivalentních úprav. V podrobnostech odkazujeme zájemce na dostupnou literaturu.

Příklad 3.1.14. Uvažujme formuli

$$D: \quad \forall x[(\forall y p(x) \vee \forall z q(z,y)) \Rightarrow \neg \forall y r(x,y)].$$

1. Eliminace nadbytečného kvantifikátoru $\forall y$:

$$D_1: \quad \forall x[(p(x) \vee \forall z q(z,y)) \Rightarrow \neg \forall y r(x,y)]$$

2. Přejmenování proměnné y, která se vyskytuje jako volná i vázaná:

$$D_2: \quad \forall x[(p(x) \vee \forall z q(z,y)) \Rightarrow \neg \forall y_1 r(x,y_1)]$$

3. Eliminace spojky "$\Rightarrow$":

$$D_3: \quad \forall x[\neg(p(x) \vee \forall z q(z,y)) \vee \neg \forall y_1 r(x,y_1)]$$

4. Přesun spojek "$\neg$" dovnitř:

$$D_4: \quad \forall x[(\neg p(x) \wedge \exists z \neg q(z,y)) \vee \exists y_1 \neg r(x,y_1)]$$

5. Přesun kvantifikátorů doleva:

$$D_5: \quad \forall x \exists z \exists y_1[(\neg p(x) \wedge \neg q(z,y)) \vee \neg r(x,y_1)]$$

6. Použití distributivního zákona:

$$D': \quad \forall x \exists z \exists y_1[(\neg p(x) \vee \neg r(x,y_1)) \wedge (\neg q(z,y) \vee \neg r(x,y_1))]$$

Formule D' je v prenexní konjunktivní normální formě a je ekvivalentní formuli D.

Definice 3.1.21. Říkáme, že je formule v *prenexní normální formě*, má-li tvar

$$(\Box v_1)(\Box v_2)\ldots(\Box v_n)A$$

kde $\Box$ označuje buď obecný nebo existenční kvantifikátor, $v_1, v_2, \ldots, v_n$ jsou navzájem různé funkční a predikátové proměnné vystupující v A a v A se nevyskytuje žádný kvantifikátor. Posloupnost kvantifikátorů tu opět nazýváme *prefixem* a formuli A nazýváme *maticí* dané formule. Jak prenexní konjunktivní normální forma, tak prenexní normální disjunktivní forma jsou zvláštní případy prenexní normální formy.

Věta 3.1.11. *(Gödel) Problém logické pravdivosti v predikátovém počtu druhého řádu není ani parciálně rozhodnutelný.*

Důkaz věty neuvádíme, je pro tento základní učební text příliš složitý. Věta v podstatě tvrdí, že neexistuje algoritmus, který by pro každou předloženou formuli predikátového počtu druhého řádu přešel k příkazu AKCEPTOVÁNO v případě, že daná formule je logicky pravdivá a přešel k příkazu ZAMÍTNUTO nebo cykloval v případě, že daná formule pravdivá není.

Věta 3.1.12. *(Church) Problém logické pravdivosti v predikátovém počtu prvního řádu je nerozhodnutelný, avšak je parciálně rozhodnutelný.*

Podobně jako u předchozí věty ani zde ze stejného důvodu neuvádíme důkaz. Věta říká, že neexistuje algoritmus, který by pro každou předloženou formuli predikátového počtu prvního řádu přešel k příkazu AKCEPTOVÁNO v případě, že jde o formuli logicky pravdivou a k příkazu ZAMÍTNUTO v opačném případě. Na druhé straně však existuje algoritmus, který pro každou formuli predikátového počtu prvního řádu přejde k příkazu AKCEPTOVÁNO v případě, že daná formule je logicky pravdivá a přejde k příkazu ZAMÍTNUTO nebo cykluje v případě, že logicky pravdivá není.

Podotkněme, že ačkoliv problém logické pravdivosti není v predikátovém počtu druhého řádu rozhodnutelný ani parciálně rozhodnutelný, existuje řada významných a zajímavých podtříd formulí, pro něž problém logické pravdivosti rozhodnutelný je. Hlubší rozbor této problematiky je však opět nad rámec tohoto textu a čtenář je odkázán na dostupnou literaturu.

Cvičení

3.1.1. Je dána formule predikátového počtu druhého řádu

$$(\forall P)\{[P(a) \wedge (\forall x)[[\neg(x = a) \wedge P(f(x))] \Rightarrow P(x)]] \Rightarrow (\forall x)P(x)\}.$$

Vypište všechny její atomické podformule a podformule.

3.1.2. Uvažujme formuli

$$\forall z \exists u \exists v[(z = u \vee z = v) \wedge u \neq v] \wedge \forall x \forall y \forall P[x \neq y \vee (P(x, x) \vee \neg P(y, y))].$$

Dokažte, že tato formule nabývá hodnoty *nepravda* v každé interpretaci $\mathcal{I}$ s jednoprvkovým oborem M.

3.1.3. * Dokažte, že formule z předchozího příkladu nabývá hodnoty *pravda* v každé interpretaci $\mathcal{I}$ s dvouprvkovým oborem M.

3.1.4. Ukažte, že formule

$$\forall x \forall y \forall P[x \neq y \vee (P(x, x) \vee \neg P(y, y)]$$

je logicky pravdivá.

3.1.5. Dokažte, že formule

$$\exists P \exists x \exists y[(P(x, x) \wedge \neg P(x, y)) \wedge x = y]$$

je nesplnitelná.

3.1.6. Dokažte logickou pravdivost formulí výrokového počtu:

$$D_1 : \quad ((p \Rightarrow p) \Rightarrow p) \Rightarrow p,$$

$$D_2 : \quad [((p \wedge q) \Rightarrow r) \wedge (p \Rightarrow q)] \Rightarrow (p \Rightarrow r).$$

3.1.7. Rozhodněte o logické pravdivosti, resp. splnitelnosti formulí predikátového počtu prvního řádu:

$$A_1 : \quad \forall p_1(x) \Rightarrow \exists x p_1(x),$$

$$A_2 : \quad \exists x p_1(x) \Rightarrow \forall x p_1(x),$$

$$A_3 : \quad \forall x q_1(x) \Rightarrow q_1(a),$$

$$A_4 : \quad q_1(a) \Rightarrow \forall x q_1(x),$$

$$A_5 : \quad \exists y \forall x p_2(x, y) \Rightarrow \forall x \exists y p_2(x, y),$$

$$A_6 : \quad \forall x \exists y p_2(x, y) \Rightarrow \exists y \forall x p_2(x, y),$$

$$A_7 : \quad \forall x(p_1(x) \Rightarrow p_1(x)) \Rightarrow [\exists x p_1(x) \Rightarrow \forall x p_1(x)],$$

$$A_8 : \quad [\exists x p_1(x) \Rightarrow \forall x q_1(x)] \Rightarrow \forall x(p_1(x) \Rightarrow q_1(x)).$$

3.1.8. Dokažte logickou ekvivalenci formulí:

$$A : \quad \forall x \exists P\{\exists y[x \neq y \wedge P(y)] \wedge \exists z \forall u[x \neq z \wedge (z \neq u \vee \neg P(u))]\}$$

$$B : \forall x \exists y \exists z[x \neq y \wedge x \neq z \wedge y \neq z].$$

3.1.9. Najděte prenexní disjunktivní normální formu formule D z příkladu 3.1.14.

3.2 Přirozená dedukce

Dedukční systém klasického výrokového počtu se skládá ze systémů několika axiomů a odvozovacího pravidla, kterým je pravidlo *modus ponens*.

Definice 3.2.1. Axióm je třída formulí výrokového počtu, které jsou utvořené podle jednoho z následujících schémat:

(1) $A \Rightarrow (B \Rightarrow A)$

(2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(3) $(A \wedge B) \Rightarrow A$

(4) $(A \wedge B) \Rightarrow B$

(5) $A \Rightarrow (B \Rightarrow (A \wedge B))$

(6) $A \Rightarrow (A \vee B)$

(7) $B \Rightarrow (A \vee B)$

(8) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))$

(9) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$

(10) $\neg\neg A \Rightarrow A$

Schémata axiomů jsou konstruována na základě tautologií výrokového počtu, takže každý axiom lze považovat za logicky pravdivou formuli.

Definice 3.2.2. Odvozovací pravidlo modus ponens je schéma, které je založeno na faktu, že jsou-li A, B formule výrokového počtu ve smyslu předchozí kapitoly, je formule B je tautologickým důsledkem množiny formulí $\{A, A \Rightarrow B\}$. Toto pravidlo umožňuje odvodit z formulí tvaru A, $A \Rightarrow B$ jako závěr formuli B, což se formálně zapisuje ve tvaru

$$\frac{A, A \Rightarrow B}{B} \quad .$$

Definice 3.2.3. Nechť T je množina formulí výrokového počtu. Řekneme, že posloupnost formulí $A_1, A_2, \dots A_k$ je *odvozením* nebo-li *důkazem* formule A z předpokladů T, jestliže

(i) $A_k = A$,

(ii) pro libovolné $i \in \{1, 2, \dots, k\}$ je A_i buď některý z axiómů, nebo prvek množiny T nebo výsledek použití pravidla modus ponens, kde předpoklady tohoto pravidla leží v množině $\{A_1, A_2, \dots A_k\}$.

Existuje-li takový důkaz, formule A se nazývá *odvoditelná* nebo-li *dokazatelná* z předpokladů T. Je-li navíc $T = \varnothing$, nazývá se A *dokazatelná*, nebo také *teorém*.

Příklad 3.2.1. Ukážeme příklad odvození formule z jistých předpokladů v rámci systému přirozené dedukce výrokového počtu:

1. $A \Rightarrow B$ ... (předpoklad)
2. $B \Rightarrow C$ ... (předpoklad)
3. $(B \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$ ... (axiom (1), kde místo A bylo dosazeno $B \Rightarrow C$ a místo B bylo dosazeno A)
4. $A \Rightarrow (B \Rightarrow C)$ ... (použitím modus ponens z 2. a 3.)
5. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$ ... (axiom (2))
6. $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$ ... (použitím modus ponens z 4. a 5.)
7. $A \Rightarrow C$ ... (odvozená formule; použitím modus ponens z 1. a 6.)

Tedy z předpokladů $A \Rightarrow B$, $B \Rightarrow C$ jsme odvodili formuli $A \Rightarrow C$.

Poznamenejme, že existují i jiné systémy axiómů než ty, které byly uvedeny v rámci definice 3.2.1. Tyto axiomatické systémy mohou ale nemusí být ekvivalentní s již zavedeným systémem. Mezi ekvivalentní axiomatické systémy patří například systém axiómů, který navrhl A. Tarski:

(1) $A \Rightarrow (B \Rightarrow A)$

(2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(3) $(\neg A \Rightarrow \neg B) \Rightarrow (B \Rightarrow A)$

(4) $(A \Rightarrow (A \Rightarrow B)) \Rightarrow (A \Rightarrow B)$

Dedukční systém predikátového počtu vyžaduje poněkud vyšší stupeň formalizace, než tomu bylo u výrokového počtu.

Definice 3.2.4. Dedukční systém pro predikátový počet sestává z rekurzivní množiny logicky pravdivých formulí, nazývaných *axiómy* a konečné množiny *odvozovacích pravidel*, z nichž každé přiřazuje jedné nebo více logicky pravdivým formulím jistou logicky pravdivou formuli. Formule B je *odvoditelná (dokazatelná)* v takovém systému, právě když existuje konečná posloupnost formulí taková, že B je její poslední člen a každá formule z této posloupnosti je buď axiom, nebo je odvoditelná z předcházejících formulí posloupnosti pomocí vhodného odvozovacího pravidla. Taková posloupnost se nazývá *odvození* nebo též *důkaz* formule B.

Protože každý axiom je logicky pravdivá formule a odvozovací pravidla přecházejí od logicky pravdivých formulí opět k formulím logicky pravdivým, je každá odvoditelná formule logicky pravdivá. Opak obecně neplatí. Mohou existovat dedukční systémy, v nichž nelze odvodit všechny logicky pravdivé formule.

Definice 3.2.5. Dedukční systém se nazývá *úplný*, jestliže v něm lze odvodit každou logicky pravdivou formuli.

Důkaz logické pravdivosti dané formule je v úplném dedukčním systému ekvivalentní důkazu odvoditelnosti takové formule. Bohužel, ne vždy je možné zkonstruovat úplný dedukční systém.

Věta 3.2.1. *(Gödel) Pro predikátový počet druhého řádu neexistuje úplný dedukční systém. Pro predikátový počet prvního řádu existují úplné dedukční systémy.*

V následujícím textu popíšeme jistý úplný dedukční systém predikátového počtu prvního řádu, který je modifikací Gentzenova (1934-35) dedukčního systému. Systémy vycházející z Gentzenových myšlenek a prací se obvykle nazývají *systémy přirozené dedukce*.

Definice 3.2.6. *Sekvence* je výraz tvaru $A_1, A_2, \ldots, A_n \Rrightarrow B$, kde A_i a B jsou formule, který zastupuje formuli $(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Rightarrow B$.

Protože na pořadí formulí ani na jejich vícenásobném výskytu v konjunkci nezáleží, lze posloupnost $A_1, A_2, \ldots, A_n$ v sekvenci považovat za konečnou množinu (i případně prázdnou). K jejímu označení používáme obvykle řecké písmeno Γ. Sekvence $\Rrightarrow B$ zastupuje formuli B samu. axiómy a odvozovací pravidla systému přirozené dedukce rozčleníme do čtyř částí:

(i) axiómy a základní pravidla,

(ii) pravidla pro spojky,

(iii) pravidla pro kvantifikátory,

(iv) pravidla pro operátory.

axiómy jsou sekvence, odvozovací pravidla zapisujeme ve tvaru

$$\frac{\langle\text{sekvence}\rangle \text{ a } \ldots \text{ a } \langle\text{sekvence}\rangle}{\langle\text{sekvence}\rangle},$$

který udává, že ze sekvencí nad čarou lze odvodit sekvenci pod čarou.

1. Axiómy a základní pravidla

(i) Základní axiom:

$$\Gamma, A \Rrightarrow A$$

Zavedení předpokladu:

$$\frac{\Gamma \Rrightarrow B}{\Gamma, A \Rrightarrow B}$$

Eliminace předpokladu:

$$\frac{\Gamma, A \Rrightarrow B \text{ a } \Gamma, \neg A \Rrightarrow B}{\Gamma \Rrightarrow B}$$

(ii) **true**-axiom:

$$\Gamma \Rrightarrow \mathbf{true}$$

false-axiom:

$$\Gamma \Rrightarrow \neg\mathbf{false}$$

2. Pravidla pro spojky

(i) Pravidla pro spojku $\vee$

Zavedení $\vee$:

$$\frac{\Gamma \Rrightarrow A}{\Gamma \Rrightarrow A \vee B}$$

$$\frac{\Gamma \Rrightarrow B}{\Gamma \Rrightarrow A \vee B}$$

Eliminace $\vee$:

$$\frac{\Gamma, A \Rrightarrow C \text{ a } \Gamma, B \Rrightarrow C \text{ a } \Gamma \Rrightarrow A \vee B}{\Gamma \Rrightarrow C}$$

(ii) Pravidla pro spojku $\wedge$

Zavedení $\wedge$:

$$\frac{\Gamma \Rrightarrow A \text{ a } \Gamma \Rrightarrow B}{\Gamma \Rrightarrow A \wedge B}$$

Eliminace $\wedge$:

$$\frac{\Gamma \Rrightarrow A \wedge B}{\Gamma \Rrightarrow A}$$

$$\frac{\Gamma \Rrightarrow A \wedge B}{\Gamma \Rrightarrow B}$$

(iii) Pravidla pro spojku $\Rightarrow$

Zavedení $\Rightarrow$:

$$\frac{\Gamma, A \Rrightarrow B}{\Gamma \Rrightarrow A \Rightarrow B}$$

Eliminace $\Rightarrow$ (modus ponens):

$$\frac{\Gamma \Rrightarrow A \text{ a } \Gamma \Rrightarrow A \Rightarrow B}{\Gamma \Rrightarrow B}$$

(iv) Pravidla pro spojku $\neg$

Zavedení $\neg$(reductio ad absurdum):

$$\frac{\Gamma, A \Rrightarrow B \text{ a } \Gamma, A \Rrightarrow \neg B}{\Gamma \Rrightarrow \neg A}$$

Eliminace $\neg$:

$$\frac{\Gamma \Rrightarrow A \text{ a } \Gamma \Rrightarrow \neg A}{\Gamma \Rrightarrow B}$$

(v) Pravidla pro dvojici spojek $\neg\neg$

Zavedení $\neg\neg$:

$$\frac{\Gamma \Rrightarrow A}{\Gamma \Rrightarrow \neg\neg A}$$

Eliminace $\neg\neg$:

$$\frac{\Gamma \Rrightarrow \neg\neg A}{\Gamma \Rrightarrow A}$$

(vi) Pravidla pro spojku $\Leftrightarrow$

Zavedení $\Leftrightarrow$:

$$\frac{\Gamma \Rrightarrow A \Rightarrow B \text{ a } \Gamma \Rrightarrow B \Rightarrow A}{\Gamma \Rrightarrow A \Leftrightarrow B}$$

Eliminace $\Leftrightarrow$:

$$\frac{\Gamma \Rrightarrow A \Leftrightarrow B}{\Gamma \Rrightarrow A \Rightarrow B}$$

$$\frac{\Gamma \Rrightarrow A \Leftrightarrow B}{\Gamma \Rrightarrow B \Rightarrow A}$$

3. Pravidla pro kvantifikátory

Řekneme, že term t je *volný vzhledem k proměnné* x ve formuli A, jestliže po substituci t za všechny volné výskyty x v A nevznikne žádný nový výskyt vázané proměnné.

(i) Pravidla pro kvantifikátor $\forall$

Zavedení $\forall$:

$$\frac{\Gamma \Rrightarrow A(x)}{\Gamma \Rrightarrow \forall x A(x)}$$

kde proměnná x se nevyskytuje volně v žádné formuli z Γ.

Eliminace $\forall$:

$$\frac{\Gamma \Rrightarrow \forall x A(x)}{\Gamma \Rrightarrow A(t)}$$

kde term t je volný vzhledem k x v $A(x)$.

Speciální případy:

$$\frac{\Gamma \Rrightarrow \forall x A(x)}{\Gamma \Rrightarrow A(x)}$$

$$\frac{\Gamma \Rrightarrow \forall x A(x)}{\Gamma \Rrightarrow A(a)}$$

(ii) Pravidla pro kvantifikátor $\exists$

Zavedení $\exists$:

$$\frac{\Gamma \Rrightarrow A(t)}{\Gamma \Rrightarrow \exists x A(x)}$$

Speciální případy:

$$\frac{\Gamma \Rrightarrow A(x)}{\Gamma \Rrightarrow \exists x A(x)}$$

$$\frac{\Gamma \Rrightarrow A(a)}{\Gamma \Rrightarrow \exists x A(x)}$$

Eliminace $\exists$:

$$\frac{\Gamma \Rrightarrow \exists x A(x) \text{ a } \Gamma, A(b) \Rrightarrow C}{\Gamma \Rrightarrow C}$$

kde b je individuová konstanta, nevyskytující se v žádné formuli z Γ ani v $\exists A(x)$ ani v C.

Všimněme si, že v pravidle zavedení $\exists$ označuje $A(t)$ výsledek substituce t za všechny volné výskyty x v $A(x)$. Můžeme tedy např. z $\Gamma \Rrightarrow p(a,a)$ odvodit kteroukoliv ze sekvencí $\Gamma \Rrightarrow \exists x p(x,a)$, $\Gamma \Rrightarrow \exists x p(a,x)$, $\Gamma \Rrightarrow \exists x p(x,x)$.

4. Pravidla pro operátory

Pravidla pro operátor $=$

Axiom rovnosti:

$$\Gamma \Rrightarrow t = t$$

Pravidlo rovnosti:

$$\frac{\Gamma \Rrightarrow t_1 = t_2}{\Gamma \Rrightarrow A(t_1) = A(t_2)}$$

Nyní uvedeme některé příklady použití výše uvedených odvozovacích pravidel.

Příklad 3.2.2. Odvození formule $p \vee \neg p$:

1. Základní axiom:
$$p \Rrightarrow p$$
2. Zavedení $\vee$ do formule 1:
$$p \Rrightarrow p \vee \neg p$$
3. Základní axiom:
$$\neg p \Rrightarrow \neg p$$
4. Zavedení $\vee$ do formule 3:
$$\neg p \Rrightarrow p \vee \neg p$$
5. Eliminace předpokladu z formulí 2. a 4:
$$\Rrightarrow p \vee \neg p$$

čímž byla požadovaná formule odvozena.

Příklad 3.2.3. Odvození formule $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$:

1. Základní axiom:
$$p \Rightarrow q, \neg q, p \Rrightarrow p$$
2. Základní axiom:
$$p \Rightarrow q, \neg q, p \Rrightarrow p \Rightarrow q$$
3. Eliminace $\Rightarrow$ z formulí 1. a 2:
$$p \Rightarrow q, \neg q, p \Rrightarrow q$$
4. Základní axiom:
$$p \Rightarrow q, \neg q, p \Rrightarrow \neg q$$
5. Zavedení $\neg$ z formulí 3. a 4:
$$p \Rightarrow q, \neg q \Rrightarrow \neg p$$
6. Zavedení $\Rightarrow$ do formule 5:
$$p \Rightarrow q \Rrightarrow \neg q \Rightarrow \neg p$$
7. Zavedení $\Rightarrow$ do formule 6:
$$\Rrightarrow (p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$$
8. Základní axiom:
$$\neg q \Rightarrow \neg p, p, \neg q \Rrightarrow \neg q$$
9. Základní axiom:
$$\neg q \Rightarrow \neg p, p, \neg q \Rrightarrow \neg q \Rightarrow \neg p$$
10. Eliminace $\Rightarrow$ z formulí 8. a 9:
$$\neg q \Rightarrow \neg p, p, \neg q \Rrightarrow \neg p$$
11. Základní axiom:
$$\neg q \Rightarrow \neg p, p, \neg q \Rrightarrow p$$
12. Zavedení $\neg$ z formulí 10 a 11:
$$\neg q \Rightarrow \neg p, p \Rrightarrow \neg\neg q$$
13. Eliminace $\neg\neg$ z formule 12:
$$\neg q \Rightarrow \neg p, p \Rrightarrow q$$
14. Zavedení $\Rightarrow$ do formule 13:
$$\neg q \Rightarrow \neg p \Rrightarrow p \Rightarrow q$$
15. Zavedení $\Rightarrow$ do formule 14:
$$\Rrightarrow (\neg q \Rightarrow \neg p) \Rightarrow (p \Rightarrow q)$$
16. Zavedení $\Leftrightarrow$ z formulí 7 a 15:
$$\Rrightarrow (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$$

čímž byla požadovaná formule odvozena.

Pro efektivní a stručné odvozování formulí je vhodné mít k dispozici knihovnu pomocných odvozovacích pravidel, z nichž některá uvedeme:

Věta 3.2.2. *Platí následující odvozovací pravidla:*

(i)

(1)

$$\frac{\Gamma \Rrightarrow A \Rightarrow (B \Rightarrow C)}{\Gamma \Rrightarrow (A \wedge B) \Rightarrow C}$$

(2)

$$\frac{\Gamma \Rrightarrow (A \wedge B) \Rightarrow C}{\Gamma \Rrightarrow A \Rightarrow (B \Rightarrow C)}$$

(ii)

(1) Zobecněné pravidlo zavedení $\Rightarrow$:

$$\frac{\Gamma, A_1, \ldots, A_n \Rrightarrow B}{\Gamma \Rrightarrow (A_1 \wedge \cdots \wedge A_n) \Rightarrow B}$$

(2) Zobecněné pravidlo eliminace $\Rightarrow$:

$$\frac{\Gamma \Rrightarrow A_1 \ a \ \ldots \ a \ \Gamma \Rrightarrow A_n \ a \ \Gamma \Rrightarrow A_1 \wedge \cdots \wedge A_n \Rightarrow B}{\Gamma \Rightarrow B}$$

(iii)

(1) Modus tollendi ponens:

$$\frac{\Gamma \Rrightarrow A \vee B \ a \ \Gamma \Rrightarrow \neg A}{\Gamma \Rrightarrow B}$$

$$\frac{\Gamma \Rrightarrow A \vee B \ a \ \Gamma \Rrightarrow \neg B}{\Gamma \Rrightarrow A}$$

(2) Modus tollens:

$$\frac{\Gamma \Rrightarrow A \Rightarrow B \ a \ \Gamma \Rrightarrow \neg B}{\Gamma \Rrightarrow \neg A}$$

(3) Důkaz rozborem možností:

$$\frac{\Gamma, A \Rrightarrow C \ a \ \Gamma, B \Rrightarrow C}{\Gamma, A \vee B \Rrightarrow C}$$

(iv)

(1) Tranzitivita implikace:

$$\frac{\Gamma \Rrightarrow A \Rightarrow B \ a \ \Gamma \Rrightarrow B \Rightarrow C}{\Gamma \Rrightarrow A \Rightarrow C}$$

(2) Tranzitivita ekvivalence:

$$\frac{\Gamma \Rrightarrow A \Leftrightarrow B \ a\ \Gamma \Rrightarrow B \Leftrightarrow C}{\Gamma \Rrightarrow A \Leftrightarrow C}$$

(v)

(1) Zavedení $\forall$ vlevo:

$$\frac{\Gamma, A(x) \Rrightarrow B(x)}{\Gamma, \forall x A(x) \Rrightarrow B(x)}$$

(2) Zavedení $\forall\forall$:

$$\frac{\Gamma, A(x) \Rrightarrow B(x)}{\Gamma, \forall x A(x) \Rrightarrow \forall x B(x)}$$

(vi)

(1) Zavedení $\exists$ vlevo:

$$\frac{\Gamma, A(x) \Rrightarrow B}{\Gamma, \exists x A(x) \Rrightarrow B}$$

(2) Zavedení $\exists\exists$:

$$\frac{\Gamma, A(x) \Rrightarrow B(x)}{\Gamma, \exists x A(x) \Rrightarrow \exists x B(x)}$$

Důkaz věty přenecháváme čtenáři jako cvičení; jako ukázku užití odvozovacích pravidel odvodíme pravidlo $(\mathrm{i})_1$.

Příklad 3.2.4. Odvození pravidla $(\mathrm{i})_1$ z věty 3.2.2:

1. Daná formule:
$$\Gamma \Rrightarrow A \Rightarrow (B \Rightarrow C)$$
2. Zavedení předpokladu:
$$\Gamma, A \wedge B \Rrightarrow A \Rightarrow (B \Rightarrow C)$$
3. Základní axiom:
$$\Gamma, A \wedge B \Rrightarrow A \wedge B$$
4. Eliminace $\wedge$:
$$A \wedge B \Rrightarrow A$$
5. Eliminace $\Rightarrow$ z formulí 2. a 4:
$$\Gamma, A \wedge B \Rrightarrow B \Rightarrow C$$
6. Eliminace $\wedge$ z formule 3:
$$\Gamma, A \wedge B \Rrightarrow B$$

7. Eliminace $\Rightarrow$ z formulí 5. a 6:

$$\Gamma, A \wedge B \Rrightarrow C$$

8. Zavedení $\Rightarrow$:

$$\Gamma \Rrightarrow (A \wedge B) \Rightarrow C$$

což je výsledná formule.

Cvičení

3.2.1. Odvoďte formuli $(p \wedge \neg p) \Leftrightarrow \mathbf{false}$.

3.2.2. Dokažte větu 3.2.2 odvozením uvedených pomocných odvozovacích pravidel.

3.2.3. Odvoďte formuli $[(p \wedge q \Rightarrow r) \wedge (p \Rightarrow q)] \Rightarrow (p \Rightarrow r)$. Návod: odvoďte $(p \wedge q \Rightarrow r), (p \Rightarrow q), p \Rrightarrow r$ a pak použijte pravidla zavedení $\Rightarrow$ a zobecněného pravidla zavedení $\Rightarrow$.

3.2.4. Odvoďte formuli $\forall x A(x) \Rightarrow \exists x A(x)$.

3.2.5. Odvoďte formuli $\exists x \forall y A(x,y) \Rightarrow \forall y \exists x A(x,y)$.

3.2.6. Odvoďte formuli $(\forall x A(x) \vee \forall x B(x)) \Rightarrow \forall x (A(x) \vee B(x))$.

3.2.7. Odvoďte formuli $\forall x (A \Rightarrow B(x)) \Leftrightarrow (A \Rightarrow \forall x B(x))$, kde x není volná v A.

3.2.8. Odvoďte formuli $\neg \exists x A(x) \Leftrightarrow \forall x \neg A(x)$.

3.2.9. Odvoďte formuli $\exists x (A(x) \wedge B(x)) \Rightarrow (\exists x A(x) \wedge \exists x B(x))$.

3.2.10. Odvoďte formuli $\forall x (A(x) \Leftrightarrow B(x)) \Rightarrow (\forall x A(x) \Leftrightarrow \forall x B(x))$.

3.2.11. Odvoďte formuli $A(t) \Leftrightarrow \forall (x = t \Rightarrow A(x))$, kde term t je volný vzhledem k proměnné x ve formuli $A(x)$ a proměnná x není volná ve formuli $A(t)$.

3.2.12. Odvoďte formuli $A(t) \Leftrightarrow \exists x (x = t \wedge A(x))$, kde term t je volný vzhledem k proměnné x ve formuli $A(x)$.

3.2.13. Dokažte odvozovací pravidlo:

$$\frac{\Gamma \Rrightarrow t_1 = t_2}{\Gamma \Rrightarrow t_2 = t_1}$$

3.2.14. Dokažte odvozovací pravidlo:

$$\frac{\Gamma \Rrightarrow t_1 = t_2 \text{ a } \Gamma \Rrightarrow t_2 = t_3}{\Gamma \Rrightarrow t_1 = t_3}$$

3.2.15. Dokažte odvozovací pravidlo:

$$\frac{\Gamma \Rrightarrow t_1 = t_2}{\Gamma \Rrightarrow \tau(t_1) = \tau(t_2)}$$

Počítačová cvičení

3.2.16. Napište program, který generuje pravdivostní tabulku formule výrokového počtu se třemi výrokovými konstantami p, q, r. Použijte programovací jazyk, který umožňuje vyhodnocení Booleovských výrazů.

3.2.17. Napište program, který pro dvě formule $A(p,q,r)$, $B(p,q,r)$ výrokového počtu se třemi výrokovými konstantami p, q, r testuje, zda $A(p,q,r) \Rightarrow B(p,q,r)$.

3.2.18. Napište program, který pro dvě formule $A(p,q,r)$, $B(p,q,r)$ výrokového počtu se třemi výrokovými konstantami p, q, r testuje, zda $A(p,q,r) \Leftrightarrow B(p,q,r)$.

3.2.19. Napište program, který formuli výrokového počtu se třemi výrokovými konstantami p, q, r převede na normální konjunktivní formu.

3.2.20. Napište program, který formuli výrokového počtu se třemi výrokovými konstantami p, q, r převede na normální disjunktivní formu.

Pojmy k zapamatování

- Jazyk výrokového počtu a jeho konstrukce. Atomické formule a formule.
- Predikátový počet druhého řádu a jeho čtyři vlastní podtřídy.
- Booleovská funkce.
- Interpretace formulí. Evaluační funkce.
- Pravdivost a splnitelnost formulí. Tautologie a kontradikce.
- Model. Tautologický důsledek.
- Normální formy formulí.
- Systém přirozené dedukce klasického výrokového počtu.
- Axiomy a odvozovací pravidla. Modus ponens.
- Odvození, důkaz, teorém.

Klíčové myšlenky kapitoly

- Výrokový počet je jednou z vlastních podtříd predikátového počtu druhého řádu.
- Každá formule výrokového počtu určuje jednoznačně jistou Booleovskou funkci (ale ne naopak).
- Evaluační funkci rozšiřujeme rekurzí konzistentně na všechny formule pomocí významu logických spojek.
- Dvě formule jsou ekvivalentní, když se na všech evaluačních funkcích chovají stejně.
- A to je právě tehdy, když definují stejnou Booleovskou funkci.
- O pravdivosti formule výrokového počtu lze algoritmicky rozhodnout (Quine).

- Analogicky i pro výrokový počet s kvantifikátory, pravdivost formulí predikátového počtu prvního řádu však lze rozhodnout pouze parciálně (Church).
- Pravdivost formulí predikátového počtu druhého řádu nelze rozhodnout ani parciálně (Gödel).
- Věta o náhradě. Když podformule v nějaké formuli nahradíme ekvivalentními formulemi, dostaneme ekvivalentní formuli.
- Normální formy formulí výrokového počtu se efektivně hledají pomocí pravdivostní tabulky.
- Jejich minimalizaci provádíme například pomocí Quine-McCluskeyova algoritmu.
- Existuje několik ekvivalentních axiomatik pro systém přirozené dedukce klasického výrokového počtu.

Odkazy na literaturu

Autor si je vědom toho, že právě probraná kapitola nemůže zdaleka pokrýt dané téma. Je velmi obtížné poměrně komplikovanou a rozsáhlou látku shrnout na několika málo stránkách. Nakonec byla pro predikátový počet zvolena koncepce vycházející z [24], kde je podán dostatečně reprezentativní přehled nejdůležitějších výsledků a vět. Pro výrokový počet se stala východiskem publikace [23], která byla porovnávána s [24] a [31]. Odkazy na seznam rozšiřující literatury následují.

[3], [10], [14], [11], [16], [17], [20], [21], [24], [30], [36], [39], [41]

Další příklady k procvičení

Elektronická banka příkladů

Matematický software

Formule výrokového počtu

Tautologický důsledek

4 Grafy

Ústředními pojmy této kapitoly jsou neorientované i orientované grafy. Povšimneme si několika jednoduchých grafových algoritmů a na příkladech si ukážeme jejich základní principy. Vysvětlíme si takové pojmy, jako například rovinnost a Eulerovskost grafu, Hamiltonovská kružnice a chromatické nebo cyklomatické číslo. Probereme některé vlastnosti stromů a jejich aplikací. Vysvětlíme si princip Huffmanova kódu.

Cíle

Po prostudování této kapitoly budete schopni:

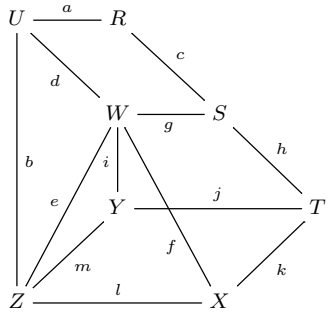
- vyšetřovat základní vlastnosti a morfismy grafů
- hledat nejkratší cestu v ohodnoceném grafu
- zjišťovat, zda je graf Eulerovský
- vyšetřovat rovinnost grafu
- vyšetřovat vybrané vlastnosti stromů
- hledat minimální kostru v ohodnoceném grafu
- hledat maximální tok v orientovaném grafu

4.1 Základní pojmy

Definice 4.1.1. *Neorientovaný graf* G se skládá z množiny V *vrcholů (uzlů)* a množiny H *hran* tak, že každá hrana $h \in H$ je přiřazena neuspořádané dvojici (tj. dvouprvkové množině) vrcholů $u, v \in V$. Existuje-li jediná hrana $h \in H$ přiřazená dvojici vrcholů $u, v \in V$, píšeme $h \equiv \{u, v\}$. Obecně může být jedné dvojici vrcholů přiřazeno více hran, tyto hrany se nazývají *násobné*.

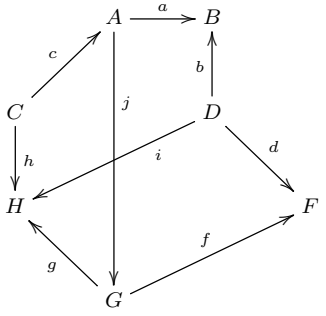
Podobně, *orientovaný graf* G se skládá z množiny V vrcholů a množiny H hran tak, že každé hraně $h \in H$ je přiřazena uspořádaná dvojice $(u, v) \in V \times V$ vrcholů $u, v \in V$. Existuje-li jediná hrana $h \in H$ přiřazená dvojici (u, v) vrcholů $u, v \in V$, píšeme $h \equiv (u, v)$.

Příklad 4.1.1. Neorientovaný graf $\mathcal{G} = (\mathcal{V}, \mathcal{H})$:



$\mathcal{V} = \{U, R, X, Y, Z, S, T, W\}$, $\mathcal{H} = \{a, b, c, d, e, f, g, h, i, j, k, l, m\}$. Například $m \equiv \{Y, Z\}$, $g \equiv \{S, W, \}$.

Příklad 4.1.2. Orientovaný graf $\mathcal{G} = (\mathcal{V}, \mathcal{H})$:



$\mathcal{V} = \{A, B, C, D, E, F, G, H\}$, $H = \{a, b, c, d, e, f, g, h, i, j\}$. Například $c \equiv (C, A)$, $g \equiv (G, H)$, $j \equiv (A, G)$.

Definice 4.1.2. Buď G graf s množinou vrcholů (= uzlů) V a množinou hran H. Nechť $f : V \to R$ a $g : H \to R$ jsou zobrazení. Pak f se nazývá *vrcholovým ohodnocením* grafu G, g se nazývá *hranovým ohodnocením* grafu G. Dvojice (G, f), resp. (G, g) se nazývá *vrcholově*, resp. *hranově ohodnocený graf*.

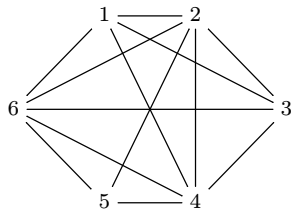
Někdy se popis jednotlivých hran grafu vynechává a píše se jen jejich ohodnocení (zejména v případě, kdy jsou popsány vrcholy a graf nemá násobné hrany).

Definice 4.1.3. Nechť G je graf. *Sledem délky* n v grafu G nazýváme posloupnost vrcholů v_i a hran h_j grafu G tvaru

$$v_0 h_1 v_1 h_2 v_3 \dots v_{n-1} h_n v_n,$$

kde hraně h_i je přiřazena dvojice vrcholů $\{v_{i-1}, v_i\}$ (resp. (u, v) v orientovaném grafu). *Tahem* v grafu G nazýváme sled, v němž se každá hrana grafu vyskytuje nejvýše jednou. *Cestou* v grafu G nazýváme sled, v němž se každý vrchol grafu vyskytuje nejvýše jednou. Sled se nazývá *uzavřený*, jestliže $v_0 = v_n$. Uzavřený sled se nazývá *uzavřenou cestou*, vyskytuje-li se v něm každý vrchol grafu, s výjimkou počátečního vrcholu, který je současně i koncový, nejvýše jednou.

Příklad 4.1.3. V grafu



$$6\{6,3\}3\{3,6\}6\{6,2\}2\{2,4\}4$$

je sled délky 4, ale není to tah ani cesta (např. vrchol 6 a hrana $\{6,3\}$ se vyskytují dvakrát).

$$6\{6,2\}2\{2,4\}4\{4,6\}6\{6,3\}3$$

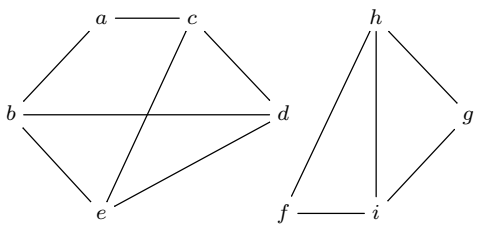
je tah délky 4, ale ne cesta (vrchol 6 je zde dvakrát).

$$2\{2,4\}4\{4,6\}6\{6,3\}3$$

je cesta délky 3 (a zároveň také tah).

Definice 4.1.4. Graf G se nazývá *souvislý*, jestliže mezi libovolnými dvěma vrcholy existuje sled.

Příklad 4.1.4. Graf z předchozího příkladu je souvislý, následující graf je nesouvislý:



Věta 4.1.1. *Graf G je souvislý, právě když mezi jeho libovolnými dvěma vrcholy existuje cesta.*

Důkaz věty je snadný, a proto jej přenecháváme čtenáři jako cvičení.

Softwarové nástroje: Vlastnosti neorientovaných grafů – grafové charakteristiky

Cvičení

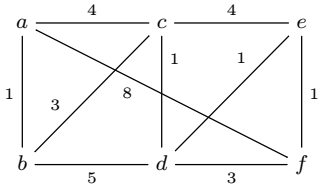
4.1.1. Graf $G = (V, H)$ bez smyček a násobných hran se nazývá *úplný*, jestliže jsou každé jeho dva vrcholy spojeny hranou. Určete, kolik hran má konečný úplný graf o $|V|$ vrcholech.

4.1.2. Nechť $G_1 = (V, H_1)$ a $G_2 = (V, H_2)$. Říkáme, že G_1 a G_2 jsou vzájemně *komplementární*, jestliže $H_1 \cap H_2 = \varnothing$ a $G = (V, H_1 \cup H_2)$ je úplný graf. Dokažte, že je-li G_1 nesouvislý, je G_2 souvislý.

4.1.3. Buď G úplný graf o n vrcholech. Určete počet cest délky 2, které začínají v pevně zvoleném vrcholu a a končí v jiném pevně zvoleném vrcholu b. Kolik existuje takových cest délky 3? Zobecněte tento výsledek pro libovolné k, kde $1 \leq k < n$.

4.2 Problém nalezení minimální cesty v ohodnoceném grafu

Příklad 4.2.1. Nalezněte nejkratší cestu v grafu G (tedy s minimálním součtem jednotlivých ohodnocení) mezi vrcholy a a f.



Algoritmus 4.2.1. (Dijkstra, 1959) Nechť G je neorientovaný ohodnocený konečný graf s kladným hranovým ohodnocením $c : H \to R^+$. Nalezneme nejkratší cestu mezi vrcholy x, y grafu G. Definujme rekurentně pomocná vrcholová ohodnocení f_i grafu G takto:

(i) Klademe $f_0(x) = 0$, $f_0(z) = +\infty$ pro $z \in V$, $z \neq x$.

(ii) Poté, co jsme sestrojili vrcholová ohodnocení $f_0, f_1, \ldots, f_i$, najdeme hranu $h \equiv \{u, v\}$ takovou, že $c(h) < f_i(v) - f_i(u)$ a položíme $f_{i+1}(v) := f_i(u) + c(h)$, $f_{i+1}(z) := = f_i(z)$ pro $z \neq v$, pokud taková hrana existuje. Jestliže taková hrana h neexistuje, ohodnocení f_i nazveme *výsledným* a cyklus končí.

Nechť f_i je výsledné ohodnocení. Pak ke každému $v \in V$, $v \neq x$, existuje hrana $h \equiv \{u, v\}$ taková, že $c(h) = f_i(v) - f_i(u)$ (jinak by f_i nebylo výsledné). Protože $f_i(u) < f_i(v)$, a x je vrchol s nejmenším ohodnocením $f_i(x) = 0$, začneme-li v $y = v_0$ a postupně nalézáme vrcholy $v_1, v_2, \ldots$ s vlastností $c(\{v_{j-1}, v_j\}) = f_i(v_{j-1}) - f_i(v_j)$, nakonec skončíme s $v_j = x$ a cesta

$$x\{x, v_{j-1}\}v_{j-1}\{v_{j-1}, v_{j-2}\}\ldots\{v_2, v_1\}v_1\{v_1, y\}y$$

je cesta s nejmenším celkovým ohodnocením mezi všemi cestami z x do y. Její celkové ohodnocení je

$$\sum_{k=1}^{j} c(\{v_{j-1}, v_j\}) = f_i(v_0) - f_i(v_j) = f_i(y).$$

Vskutku, nechť $x = w_0, w_1, w_2, \ldots, w_m = y$ jsou vrcholy nějaké jiné cesty mezi x a y. Pak platí

$$c(w_k, w_{k-1}) \geq f_i(w_k) = f_i(w_{k-1}) \tag{4.1}$$

(kdyby $c(\{w_k, w_{k-1}\}) < f_i(w_k) - f_i(w_{k-1})$, nebylo by f_i výsledné ohodnocení). Sečtením rovnic typu (4.1) pro $k = 1, 2, \ldots, m$ dostaneme

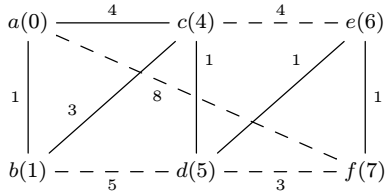
$$\sum_{k=1}^{m} c(\{w_k, w_{k-1}\}) \geq f_i(w_m) - f_i(w_0) = f_i(y).$$

Tím je důkaz minimálnosti nalezené cesty hotov.

Příklad 4.2.2. Dokončení příkladu Následující tabulka ukazuje pomocná vrcholová ohodnocení v jednotlivých krocích:

	f_0	f_1	f_2	f_3	f_4	f_5	f_6
a	0	0	0	0	0	0	0
b	∞	1	1	1	1	1	1
c	∞	∞	4	4	4	4	4
d	∞	∞	∞	5	5	5	5
e	∞	∞	∞	∞	6	6	6
f	∞	∞	∞	∞	∞	8	7

Ohodnocení f_0 je výchozí. Postupně byly vybrány hrany $\{a, b\}$, $\{a, c\}$, $\{b, d\}$, $\{d, e\}$ a $\{d, f\}$, čímž vzniklo postupně ohodnocení f_5. Jako poslední jsme vybrali hranu $\{e, f\}$, neboť je ohodnocena číslem 1, zatímco $f_5(f) - f_5(e) = 2 > 1$. Ve vrcholu f tedy můžeme dostat nižší hodnotu $f_6(f) = 7$ prostřednictvím vrcholu e a vybrané hrany $\{e, f\}$. Ohodnocení f_6 je výsledné, protože další hrana s nižším ohodnocením, než je rozdíl ohodnocení jejích koncových vrcholů v daném grafu neexistuje. Jak je vidět z následujícího obrázku, existují dvě cesty minimální délky:



Cesty minimální délky jsou

$$a\{a, c\}c\{c, d\}d\{d, e\}e\{e, f\}f$$

a

$$a\{a, b\}b\{b, c\}c\{c, d\}d\{d, e\}e\{e, f\}f$$

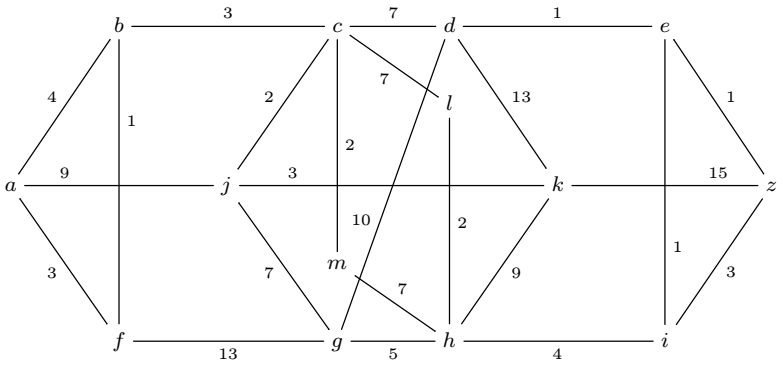
s celkovým ohodnocením 7.

Softwarové nástroje: Vlastnosti neorientovaných grafů – nalezení nejkratší cesty

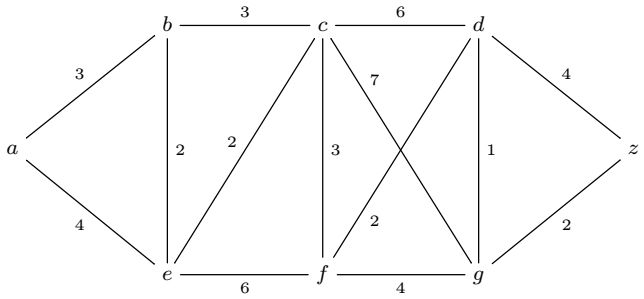
Cvičení

4.2.1. Nechť $G = (V, H)$ je souvislý graf, jehož všechny hrany jsou ohodnoceny číslem 1. Označme $d(x, y)$ délku nejkratší cesty mezi dvěma vrcholy $x, y \in V$. Dokažte, že $d : V \times V \to \mathbb{R}$ je metrika na V.

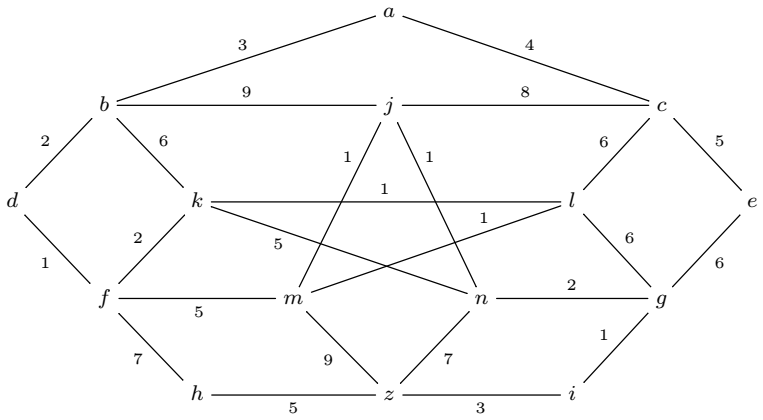
4.2.2. V daném grafu najděte nejkratší cestu z a do z:



4.2.3. V daném grafu najděte nejkratší cestu z a do z:



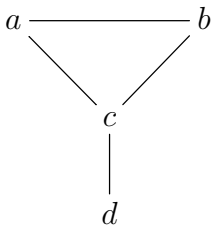
4.2.4. V daném grafu najděte nejkratší cestu z a do z:



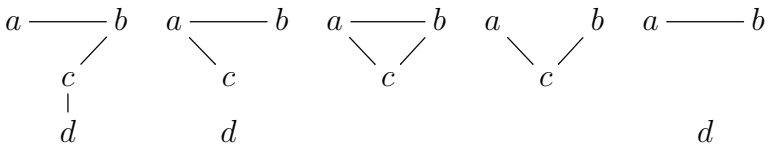
4.3 Další grafové pojmy

Definice 4.3.1. Buď $G_1 = (V_1, H_1)$, $G_2 = (V_2, H_2)$ grafy. Řekneme, že graf G_2 je *podgrafem* grafu G_1, jestliže $V_2 \subseteq V_1$, $H_2 \subseteq H_1$.

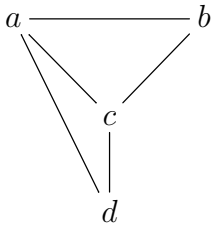
Příklad 4.3.1. Nechť G je graf:



Pak jeho podgrafy jsou například grafy:



Podgrafem grafu G není například graf:



Definice 4.3.2. Nechť $G_1 = (V_1, H_1)$, $G_2 = (V_2, H_2)$ jsou grafy. Řekneme, že G_2 je *podgraf grafu* G_1 *indukovaný grafem* G_1, jestliže platí:

(i) $V_2 \subseteq V_1$;

(ii) pro každou hranu $h \in H_1$ s koncovými vrcholy $x, y \in V_2$ platí $h \in H_2$.

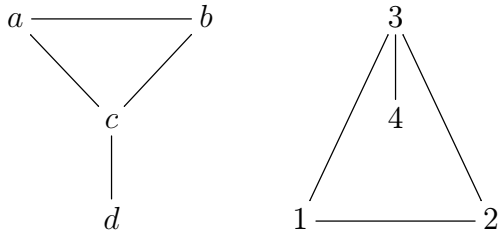
Příklad 4.3.2. Nechť G je graf z příkladu 4.3.1. Pak třetí a pátý z uvedených podgrafů jsou indukované podgrafy grafu G. První, druhý a čtvrtý podgraf není indukovaným podgrafem grafu G.

Definice 4.3.3. Buď $G = (V, H)$ graf, $G_1 = (V_1, H_1)$ podgraf grafu G. Jestliže $V_1 = V$, G_1 se nazývá *faktorem* grafu G.

Příklad 4.3.3. Nechť G je graf z příkladu 4.3.1. Pak první a druhý z uvedených podgrafů jsou faktory grafu G. Třetí, čtvrtý a pátý podgraf není faktorem grafu G.

Definice 4.3.4. Grafy $G_1 = (V_1, H_1)$ a $G_2 = (V_2, H_2)$ se nazývají *izomorfní*, jestliže existují bijekce $f : V_1 \to V_2$ a $g : H_1 \to H_2$ takové, že libovolná hraně $h \in H_1$ jsou přiřazeny vrcholy $x, y \in V_1 \iff$ hraně $g(h) \in H_2$ jsou přiřazeny vrcholy $f(x), f(y) \in V_2$.

Příklad 4.3.4. Grafy na obrázku jsou izomorfní:



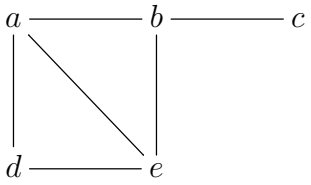
Příslušné bijekce f a g lze definovat takto:

$$f(a) = 1,\ f(b) = 2,\ f(c) = 3,\ f(d) = 4,$$

$$g(\{a, b\}) = \{1, 2\},\ g(\{b, c\}) = \{2, 3\},\ g(\{c, d\}) = \{3, 4\},\ g(\{a, c\}) = \{1, 3\}.$$

Definice 4.3.5. Graf G se nazývá *rovinný*, jestliže jej lze zakreslit v rovině tak, že se jeho hrany (které jsou reprezentovány křivkami) neprotínají. Je-li rovinný graf G zakreslen v rovině, tak, že se jeho hrany neprotínají, pak jeho hrany rozdělují rovinu na navzájem oddělené části, které nazýváme *oblastmi grafu*.

Příklad 4.3.5. Buď G rovinný graf podle obrázku:



Oblast $\mathfrak{O}_1$ je ohraničena uzavřenou cestou

$$a\{a, d\}d\{d, e\}e\{e, a\}a,$$

oblast $\mathfrak{O}_2$ je ohraničena uzavřenou cestou

$$a\{a, b\}b\{b, e\}e\{e, a\}a,$$

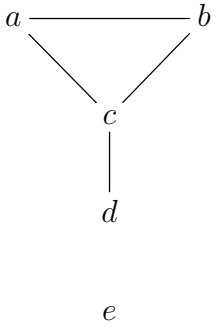
oblast $\mathfrak{O}_3$ je ohraničena uzavřeným sledem

$$a\{a,d\}d\{d,e\}e\{e,b\}b\{b,c\}c\{c,b\}b\{b,a\}a$$

a je tvořena "vnějškem" grafu G.

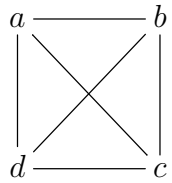
Definice 4.3.6. *Stupeň* $\mathrm{st}\,(u)$ vrcholu u neorientovaného grafu G je číslo udávající počet hran, které z daného vrcholu u vychází, přičemž každá smyčka se počítá dvakrát. Má-li daný graf G všechny vrcholy stejného stupně, nazývá se *pravidelný*. Pravidelný souvislý graf se všemi vrcholy stupně 2 se nazývá *kružnice*. Kružnice o n vrcholech se značí C_n. Hodnota $\mu(G) = |H| - |V| + k$, kde k je počet souvislých komponent grafu G, se nazývá *cyklomatické číslo* grafu G. Udává počet tzv. *nezávislých kružnic* v grafu G. Hrana, která nepatří žádné kružnici, se nazývá *most*.

Příklad 4.3.6. Buď G graf

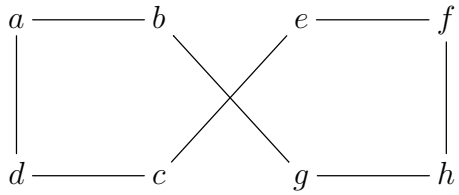


Pak $\mathrm{st}\,(a) = 2$, $\mathrm{st}\,(b) = 2$, $\mathrm{st}\,(c) = 3$, $\mathrm{st}\,(d) = 1$, $\mathrm{st}\,(e) = 0$.

Příklad 4.3.7. Graf na obrázku je pravidelným grafem stupně 3. o čtyřech vrcholech:



Příklad 4.3.8. Graf na obrázku je kružnice o osmi vrcholech C_8:



Věta 4.3.1. *(Eulerova) Buď $G = (V, H)$ souvislý rovinný graf s m oblastmi. Pak*

$$m = |H| - |V| + 2.$$

Důkaz. Důkaz provedeme indukcí vzhledem k počtu hran grafu G.

(i) Nechť $|H| = 1$. Pak $m = 1$, $|V| = 2$, a skutečně

$$1 = 1 - 2 + 2,$$

tedy tvrzení platí.

(ii) Předpokládejme, že věta platí pro $|H| = n \in N$, $n \geq 1$, a dokažme její platnost i pro $|H| = n + 1$. Nechť G je souvislý rovinný graf s $|H| = n + 1$. Nejprve předpokládejme, že G neobsahuje žádnou kružnici. Zvolme vrchol $v \in V$. Protože je G souvislý, vychází z v aspoň jedna hrana. Zvolme dále libovolnou cestu vycházející z v. Protože G neobsahuje kružnice, je tato cesta obsažena v některé maximální cestě, která končí hranou $x \in H$, z jejíhož koncového bodu $a \in V$ již další hrana nevychází, tj. $\mathrm{st}\,(a) = 1$.

Označme $G' = (V', H')$ graf vzniklý z G odstraněním vrcholu a a hrany x. Pak $V' = V \setminus \{a\}$, $H' = H \setminus \{x\}$. Tedy $|V| = |V'| + 1$, $|H| = |H'| + 1$. Protože $m = m'$ (počet oblastí se nezměnil), máme podle indukčního předpokladu

$$m = |H'| - |V'| + 2,$$

čili také $m = |H| - |V| + 2$, což je dokazované tvrzení.

Nyní předpokládejme, že G obsahuje kružnici. Buď nyní x hrana této kružnice. Hrana x je tedy částí hranice dvou oblastí $\mathfrak{O}_1$, $\mathfrak{O}_2$ grafu G, odstraněním této hrany dojde ke spojení oblastí $\mathfrak{O}_1$, $\mathfrak{O}_2$ v jednu oblast. Označíme-li $G' = (V', H')$ graf vzniklý odstraněním hrany x z G, pak platí $V' = V$, $H' = H \setminus \{x\}$, takže $|V'| = |V|$, $|H| = |H'| + 1$, $m = m' + 1$. Z indukčního předpokladu plyne

$$m' = |H'| - |V'| + 2,$$

takže

$$m = m' + 1 = |H'| + 1 - |V'| + 2 = |H| - |V| + 2.$$

Platnost věty pro $|H| = n + 1$ je tedy dokázána.

Věta platí pro všechna $n \in N$, tedy také pro libovolný konečný souvislý graf G.

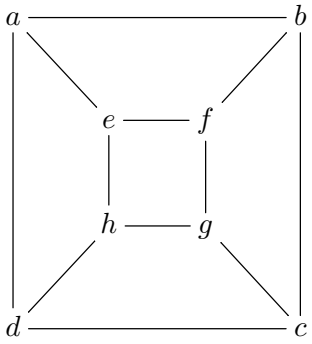
□

Důsledek 4.3.1. *Je-li $G = (V, H)$ graf, jehož každá oblast je ohraničena kružnicí délky n (tzv. graf typu C_n), pak*

$$|H| = \frac{}{n \cdot (|V| - 2)n - 2.}$$

Důkaz. Pro graf na obrázku platí $|V| = 8$, $n = 4$,

$$|H| = \overline{4 \cdot (8-2)2 = 12.}$$



Obecněji, každá hrana odděluje dvě oblasti grafu G, je tedy $\frac{|H|=}{n \cdot m2}$. Dále podle věty 4.3.1 je

$$|H| = m + |V| - 2, \text{ tedy}$$

$$n \cdot |H| = n \cdot m + n \cdot |V| - 2 \cdot n, \text{ a celkem}$$

$$n \cdot |H| = 2|H| + n|V| - 2n, \text{ čili}$$

$$|H| = \overline{n \cdot (|V|-2)n - 2.}$$

□

Důsledek 4.3.2. *Buď $G = (V, H)$ rovinný graf s maximálním počtem hran, $|V| \geq 3$. Pak*

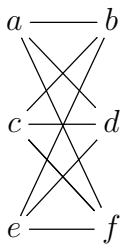
$$|H| = 3 \cdot |V| - 6.$$

Důkaz. Hranicí každé oblasti je kružnice délky $n = 3$. Podle důsledku 1 je

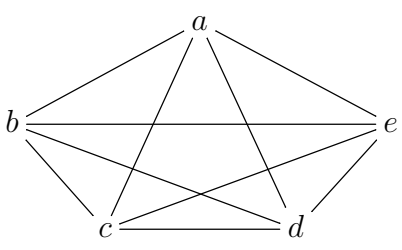
$$|H| = \overline{3 \cdot (|V|-2)1 = 3 \cdot |V| - 6.}$$

□

Důsledek 4.3.3. *Graf $K_{3,3}$ a graf K_5 (tzv. pentagram) nejsou rovinné.*



$K_{3,3}$



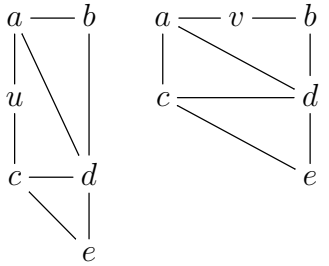
K_5

Důkaz. Pro K_5: K_5 má 10 hran, podle důsledku 4.3.17 však 5-tivrcholový rovinný graf může mít hran maximálně $9 = 3 \cdot 5 - 6$. Důkaz pro $K_{3,3}$ je podobný, ale o něco složitější.

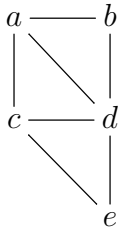
□

Definice 4.3.7. Nechť $G = (V, H)$ je graf a $v \in V$ vrchol stupně 2, z něhož vedou hrany h_1, h_2 do vrcholů $v_1, v_2 \in V$. *Redukcí* grafu G rozumíme nový graf $G' = (V', H')$, v němž $V' = V \setminus \{v\}$, $H' = (H \setminus \{h_1, h_2\}) \cup \{h\}$, kde h je nová hrana spojující vrcholy v_1, v_2. Grafy G_1, G_2 nazýváme *homeomorfní*, jestliže mohou být redukované na izomorfní grafy pomocí konečného počtu redukcí.

Příklad 4.3.9. Grafy



jsou homeomorfní, protože je lze oba redukovat na graf izomorfní s grafem:



Věta 4.3.2. *Graf G je rovinný, právě když neobsahuje podgraf homeomorfní s K_5 nebo $K_{3,3}$.*

Důkaz této věty přesahuje možnosti a rozsah tohoto učebního textu, a proto jej neuvádíme.

Definice 4.3.8. Konečný graf, jehož všechny vrcholy jsou sudého stupně, se nazývá *eulerovský.*

Lemma 4.3.1. *Každý vrchol eulerovského grafu $G = (V, H)$ je obsažen alespoň v jedné kružnici grafu G.*

Důkaz. Zvolme v G vrchol $x \in V$ a hranu $h \in H$, incidentní s x. Tedy existuje $y \in V$, že $h \equiv \{x, y\}$. Předpokládejme, že hrana h není částí kružnice, což znamená, že mezi vrcholy x, y

existuje jediná cesta. Buď G_1 maximální souvislý podgraf grafu G, který obsahuje vrchol x. Pak G_1 má všechny vrcholy sudého stupně s výjimkou vrcholu x, což není možné, protože součet stupňů všech vrcholů musí být sudé číslo (každá hrana přispívá do celkového součtu číslem 2). Tedy h a s ní i vrchol x leží na nějaké kružnici grafu G.

□

Věta 4.3.3. *Konečný graf $G = (V, H)$ bez izolovaných vrcholů lze sestrojit jedním uzavřeným tahem, právě když G je souvislý eulerovský graf.*

Důkaz. Jestliže G lze sestrojit jedním tahem, pak G je zřejmě souvislý. Přitom všechny vrcholy jsou sudého stupně, neboť kolikrát do vrcholu vstupujeme, tolikrát také vystupujeme. Tedy G je eulerovský.

Naopak, buď G souvislý a eulerovský. Zvolme libovolný vrchol $x \in V$. Protože podle lemma 4.3.1 leží x na kružnici, existuje tedy aspoň jeden uzavřený tah, začínající a končící v x. Nechť T má maximální délku ze všech takových tahů. Předpokládejme, že T neprochází všemi hranami grafu G. Označme množinu těchto hran H_1 a množinu vrcholů incidentních s těmito hranami V_1. Je zřejmé, že graf $G_1 = (V_1, H_1)$ je eulerovský. Protože je původní graf G souvislý, existuje vrchol $y \in H_1$, kterým prochází také tah T. Ovšem podle lemma 4.3.1 leží y na jisté kružnici C_k grafu G_1. Existuje tedy delší tah než T, složený z T a kružnice C_k. To je ale spor s předpokladem, že tah T má maximální délku. Tedy T prochází všemi hranami grafu G a důkaz je hotov.

□

Důsledek 4.3.4. *Konečný graf G lze sestrojit jedním otevřeným tahem právě když G je souvislý a má právě dva vrcholy lichého stupně. Má-li G takové dva vrcholy, pak otevřený tah v jednom z nich začíná a ve druhém končí.*

Definice 4.3.9. Buď G graf a C_k kružnice v G. Říkáme, že C_k je *hamiltonovská*, jestliže je faktorem grafu G.

Následující dvě věty uvádíme bez důkazu.

Věta 4.3.4. *Nechť G je graf s $n \geq 3$ vrcholy takový, že stupeň každého vrcholu je aspoň $\frac{n}{2}$. Pak G obsahuje hamiltonovskou kružnici.*

Věta 4.3.5. *Nechť G je graf s $n \geq 3$ vrcholy takový, že*

$$\operatorname{st} x + \operatorname{st} y \geq n$$

pro každou dvojici nesousedních vrcholů. Pak G obsahuje hamiltonovskou kružnici.

Poslední odstavec této kapitoly věnujeme barvení grafu.

Definice 4.3.10. *Obarvení* grafu G je přiřazení barev jeho vrcholům takové, že vrcholy spojené hranou mají různé barvy. Minimální počet barev, nutný k obarvení grafu G, se nazývá *chromatické číslo* grafu G a značí se $\chi(G)$.

Následující věta byla dlouho otevřeným problémem teorie grafů. Byla vyřešena v roce 1976 Appelem a Hakenem, kteří prověřili na počítači téměř 2000 grafů, zahrnujících miliony možností obarvení.

Věta 4.3.6. *(Appel & Haken, 1976) Každý rovinný graf má chromatické číslo nejvýš* 4.

Softwarové nástroje: Vlastnosti neorientovaných grafů – grafové charakteristiky

Cvičení

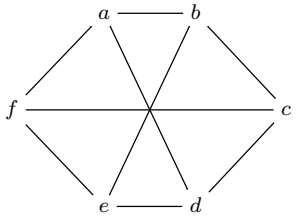
4.3.1. Dokažte, že v neorientovaném grafu $G = (V, H)$ platí $\sum_{v \in V} \mathrm{st}\,(v) = 2|H|$.

4.3.2. Najděte všechny podgrafy grafu z příkladu 4.3.1.

4.3.3. Najděte všechny faktory grafu z příkladu 4.3.1.

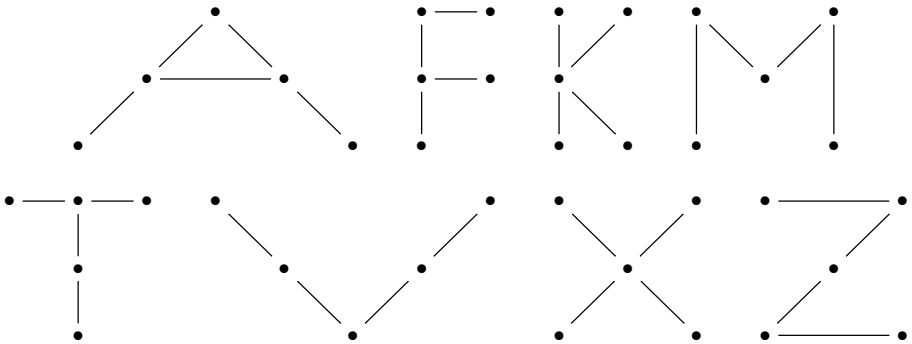
4.3.4. Najděte všechny indukované podgrafy grafu z příkladu 4.3.1.

4.3.5. Dokažte, že graf



je izomorfní s $K_{3,3}$.

4.3.6. Jsou dány grafy:



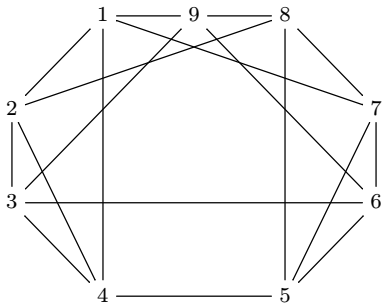
Zjistěte, které z nich jsou navzájem izomorfní. Rozdělte je do skupin tak, že v každé skupině budou grafy navzájem izomorfní. Kolik bude skupin?

4.3.7. Uvažujte graf z příkladu 2 ve cvičení 4.2. Rozhodněte a dokažte, zda je či není rovinný.

4.3.8. Uvažujte graf z příkladu 3 ve cvičení 4.2. Rozhodněte a dokažte, zda je či není rovinný.

4.3.9. Uvažujte graf z příkladu 4 ve cvičení 4.2. Rozhodněte a dokažte, zda je či není rovinný.

4.3.10. V grafu G (tzv. eneagram)



najděte podgraf homeomorfní s $K_{3,3}$. Je graf G rovinný?

4.3.11. * V grafu G z předchozího příkladu nalezněte podgraf homeomorfní s K_5.

4.3.12. Dokažte, že neexistuje neorientovaný graf bez smyček a násobných hran o 5 vrcholech, jehož vrcholy mají navzájem různé stupně.

4.3.13. * Řešte předchozí úlohu pro libovolné n.

4.3.14. Zjistěte, kolik různých kružnic existuje v grafu K_5.

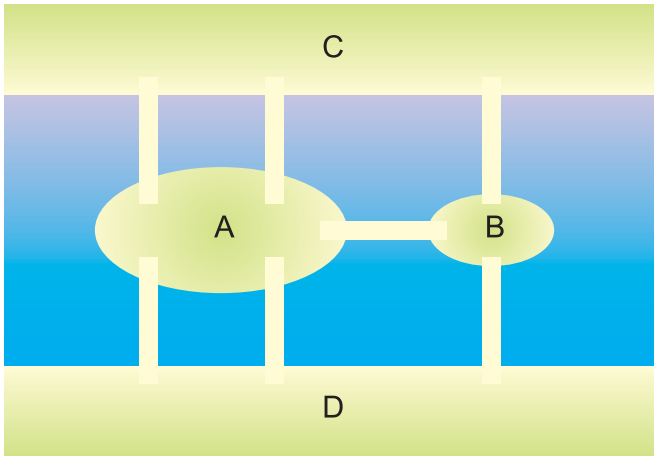
4.3.15. * Zjistěte, kolik různých kružnic délky k existuje v úplném grafu K_n o n vrcholech ($n \geq k \geq 3$).

4.3.16. Nakreslete graf K_5 jedním uzavřeným tahem.

4.3.17. Nakreslete graf K_7 jedním uzavřeným tahem.

4.3.18. Určete nutnou a postačující podmínku pro to, aby bylo možno nakreslit úplný graf K_n o n vrcholech jedním tahem.

4.3.19. Dokažte 4.3.4. Návod: rozšiřte vhodně graf G o nový vrchol a použijte větu 4.3.3.



Obr. 4.3.1 Mosty v městě Královci

4.3.20. Ve městě Královci (Konigsberg, Kaliningrad) na řece Pregel jsou dva ostrovy A a B, spojené mostem. Ostrov A je spojen s každým z břehů C, D dvěma rovnoběžnými mosty, ostrov B je s každým z obou břehů spojen pouze jedním mostem. Rozhodněte, je-li možné projít městem tak, abychom po každém z mostů přešli právě jednou a skončili na původním místě. (Hlavolam řešil a vyřešil švýcarský matematik L. Euler (1707-1783).)

4.3.21. Nakreslete graf se šesti vrcholy, v němž existuje hamiltonovská kružnice, ale který nelze nakreslit jedním uzavřeným tahem.

4.3.22. Nakreslete graf se šesti vrcholy, který lze nakreslit jedním uzavřeným tahem, ale v němž neexistuje hamiltonovská kružnice.

4.3.23. Nakreslete graf z příkladu 10 jedním uzavřeným tahem.

4.3.24. V příkladech 2,3 a 4 ve cvičení 4.2 určete, který z grafů lze nakreslit jedním uzavřeným tahem. Který z nich lze nakreslit jedním otevřeným tahem?

4.3.25. * Nechť G_1 a G_2 jsou komplementární grafy. Dokažte, že má-li G_1 aspoň 11 vrcholů, pak aspoň jeden z grafů G_1, G_2 není rovinný.

4.3.26. Určete chromatická čísla grafů $K_{3,3}$ a K_5.

4.3.27. Určete chromatické číslo grafu K_n, kde $n \in \mathbb{N}$.

4.3.28. Určete chromatické číslo grafu z příkladu 4.3.1.

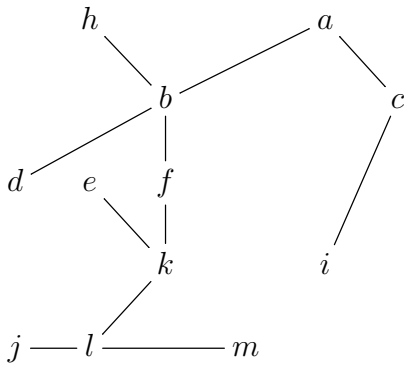
4.3.29. Určete chromatické číslo grafu z příkladu 4.3.7.

4.3.30. Určete chromatické číslo grafu na obrázku z důsledku 4.3.1.

4.4 Stromy a kostry. Nalezení minimální kostry grafu

Definice 4.4.1. Buď $G = (V, H)$ graf. Řekneme, že G je strom, jestliže G je souvislý graf bez násobných hran, který neobsahuje kružnici.

Příklad 4.4.1. Graf, který je strom:



Přidáním libovolné další hrany či naopak odstraněním hrany vznikne graf s kružnicí či nesouvislý graf, a tedy nebude stromem.

Věta 4.4.1. *Buď $G = (V, H)$ graf bez násobných hran. Následující podmínky jsou ekvivalentní:*

(i) *G je strom;*

(ii) *Mezi libovolnými dvěma vrcholy v G existuje jediná cesta;*

(iii) *G je souvislý a $|H| = |V| - 1$;*

(iv) *G neobsahuje kružnici a $|H| = |V| - 1$.*

Důkaz. (i)⇒ (ii): Kdyby např. $x, y \in V$ byly spojeny dvěma různými cestami

$$xh_1v_1 \dots h_ky \text{ a } yh_{k+1}v_{k+1} \dots h_mx,$$

spojením těchto dvou cest bychom dostali sled z x do x délky m, $m \geq 2$. Protože G nemá násobné hrany, $m \geq 3$. Zvolme tedy mezi všemi sledy z x do x ten, který má nejkratší nenulovou délku $n \geq 3$, řekněme $xg_1u_1g_2u_2 \dots g_nx$. Kdyby pro některé i, j nastala situace $u_i = u_j$, mohli bychom

tento sled zkrátit vypuštěním hran mezi u_i a u_j, což by byl spor s tím, že jsme předpokládali, že sled je nejkratší. Tedy $xg_1u_1 \dots g_nx$ je cesta, tj. kružnice v G.

(ii)⇒ (iii): Postupujme indukcí vzhledem k $n = |V|$. Pro $n = 1$ tvrzení zřejmě platí. Předpokládejme dále, že tvrzení platí pro jisté $n \in N$ a dokažme jeho platnost i pro $n + 1$. Nechť $G = (V, H)$ je graf s $|V| = n+1$, kde mezi libovolnými dvěma vrcholy existuje jediná cesta. Pak v G existuje vrchol $a \in V$, z něhož vychází jediná hrana $h \in H$. Položme $G' = (V', H')$, kde $V' = V \setminus \{a\}$, $H' = H \setminus \{h\}$. Ovšem v G' je splněn indukční předpoklad, takže $|H'| = |V'| - 1$, odkud $|H| = |H'| + 1 = |V'| = |V| - 1$, přičemž G je souvislý.

(iii)⇒(iv): Předpokládejme, že G je souvislý graf s $|H| = |V| - 1$, který obsahuje aspoň jednu kružnici. Odstraňme z G právě tolik hran, abychom dostali souvislý graf $G' = (V, H')$, $H' \subseteq H$, bez kružnic. Pak mezi libovolnými dvěma vrcholy z G' existuje právě jedna cesta, takže podle b)⇛c) dostáváme, že $|H'| = |V| - 1$. Avšak $|H| > |H'| = |V| - 1$, což je spor. Tedy G nemůže obsahovat kružnici.

(iv)⇒(i): Stačí ukázat, že graf splňující (iv) je souvislý. Buď $G = (V, H)$ graf s k komponentami $G_i = (V_i, H_i)$, pro $i = 1, 2, \dots, k$ (*komponenta* je maximální souvislá část grafu), které jsou souvislé, a nechť G neobsahuje kružnici, čili komponenty jsou stromy. Pak podle a)⇛b)⇛c) dostáváme $|H_i| = |V_i| - 1$, takže

$$|H| = \sum_{i=1}^{k} |H_i| = \sum_{i=1}^{k} (|V_i| - 1) = |V| - k.$$

Je-li podle předpokladu $|H| = |V| - 1$, pak $k = 1$, takže G je souvislý (má jednu komponentu). Tím je věta dokázána.

□

Příklad 4.4.2. (Huffmanovy kódy) Jedná se o kódy s proměnnou délkou reprezentace znaku. Například v ASCII kódu je každý znak vyjádřen 7-bitovým (nebo 8-bitovým) řetězcem:

$$A \dots 1000000,$$

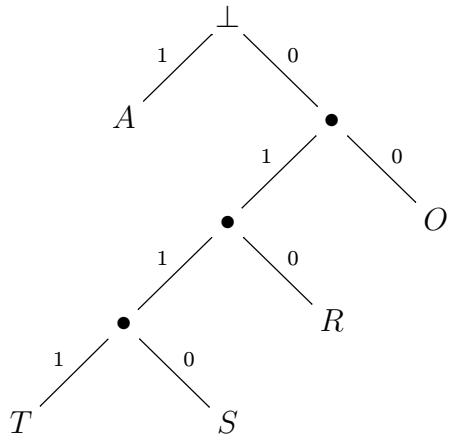
$$B \dots 1000001,$$

$$C \dots 1000010,$$

$$1 \dots 0110001.$$

Huffmanův kód je reprezentován stromem s význačným vrcholem $\perp$ kterému se říká *kořen*

nebo (anglicky) *root*:



Dekódujme např. řetězec 01010111: začneme v rootu a postupujeme po větvích podle 0 a 1, dokud nenarazíme na koncový vrchol popsaný nějakým znakem:

$$010\ldots R,$$

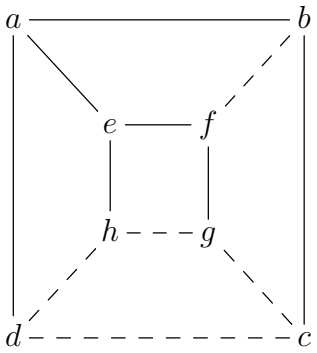
$$1\ldots A,$$

$$0111\ldots T.$$

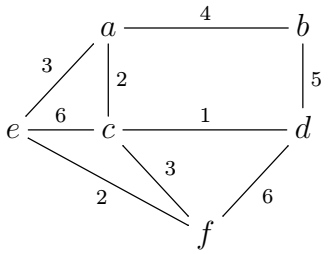
Řetězec znamená "RAT". Podobně 0111000101 znamená "TORA". V praxi se vytvářejí Huffmanovy kódy pro mnohem bohatší soubory znaků (abecedy), než v tomto jednoduchém příkladě. Nejvýhodnější je, aby nejčastěji užívané znaky byly ve stromu umístěny blízko kořene, což uspoří paměťové místo. Jako jeden z algoritmů používají tyto kódy také populární komprimační algoritmy (ARJ, ZIP, RAR,...).

Definice 4.4.2. Buď $G = (V, H)$ graf. Faktor grafu G, který je stromem, se nazývá *kostra* grafu G.

Příklad 4.4.3. Plně vyznačené hrany náleží do kostry grafu G.



Příklad 4.4.4. V daném grafu G najděte kostru s minimálním součtem ohodnocení jednotlivých hran (tzv. *minimální kostru*):



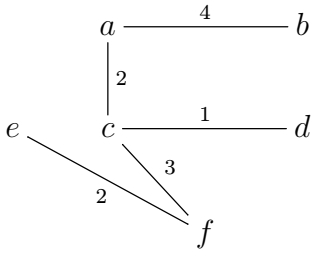
Jednou z nejstarších prací, zabývající se nalezením kostry grafu s minimálním součtem ohodnocení hran je práce českého matematika Otakara Borůvky z roku 1926. Algoritmus byl publikován jako metoda nalezení efektivní elektrické sítě na části Moravy. Následující algoritmus vychází z Borůvkovy práce z roku 1926, ale jeho autorem je americký matematik Joseph Kruskal.

Algoritmus 4.4.1. (Nalezení minimální kostry, Kruskal 1956) Seřadíme hrany grafu $G = (V, H)$ do neklesající posloupnosti podle jednotlivých ohodnocení a postupně vybíráme hrany tak, aby nevznikla kružnice. Po $|V| - 1$ krocích (věta 4.4.1) dostaneme strom se všemi vrcholy z množiny V, tedy kostru grafu G.

Příklad 4.4.5. Řešení příkladu Postupně přidáváme hrany

$$\{c, d\}, \{a, c\}, \{e, f\}, \{c, f\},$$

Hranu $\{a, e\}$ nepřidáme, protože by vznikla kružnice. Nakonec přidáme $\{a, b\}$ a máme strom se stejnými vrcholy jako v původním grafu, tedy kostru s minimálním součtem ohodnocení 12:



Algoritmus 4.4.2. (Jiná varianta Kruskalova algoritmu nalezení minimální kostry) Seřadíme hrany grafu G do neklesající posloupnosti vzhledem k jejich ohodnocení, a postupně odstraňujeme hrany s největším ohodnocením, dokud graf obsahuje kružnice.

Softwarové nástroje: Vlastnosti neorientovaných grafů – nalezení minimální kostry

Definice 4.4.3. Buď $G = (V, H)$ strom, $\perp \in V$. Pak dvojici $(G, \perp)$ říkáme *kořenový strom*. *Výškou* kořenového stromu $(G, \perp)$ rozumíme maximální délku cesty, začínající v $\perp$. Řekneme, že vrchol $y \in V$ je *následníkem* vrcholu x, jestliže existuje cesta $\perp\{\perp, t_1\}t_1\{t_1, t_2\}\ t_2 \ldots x\{x, y\}y$. Kořenový strom se nazývá *binární strom*, jestliže má každý vrchol $x \in V$ nejvýše dva následníky. Binární strom se nazývá *plný*, jestliže každý vrchol má oba následovníky, nebo nemá žádné následovníky. Vrchol, který nemá následovníka, se nazývá *koncový*. Vrchol, který má následovníka, se nazývá *vnitřní*.

Příklad 4.4.6. 4.4.11 Strom z příkladu 4.4.2 je plný binární strom výšky 4 s kořenem $\perp$. Kostra z příkladu 4.4.4 s kořenem f je binární strom výšky 3, ale není plný.

Věta 4.4.2. *Buď $(G, \perp)$ plný binární strom, který má i vnitřních vrcholů. Pak $(G, \perp)$ má $i + 1$ koncových vrcholů a $2i + 1$ všech vrcholů.*

Důkaz. Protože v $(G, \perp)$ existuje i vnitřních vrcholů, existuje $2i$ následovníků. Přitom $\perp$ je jediný vrchol, který není následovníkem.

□

Věta 4.4.3. *Jestliže binární strom výšky h má t koncových vrcholů, pak $t \leq 2^h$.*

Důkaz. Tvrzení dokážeme indukcí vzhledem k výšce stromu. Pro $h = 0$ tvrzení evidentně platí. Předpokládejme, že tvrzení platí pro libovolný binární strom výšky menší než h. Buď $(G, \perp)$ binární strom výšky $h > 0$. Předpokládejme nejprve, že $\perp$ má jednoho následovníka. Podle předpokladu je $t \leq 2^{h-1}$, takže $t \leq 2^h$. Má-li $\perp$ dva následovníky, můžeme po odstranění kořene rozdělit $(G, \perp)$ na dva stromy výšky menší než h s t_1 a t_2 koncovými vrcholy. Pak $t = t_1 + t_2 \leq 2^{h-1} + 2^{h-1} = 2^h$. Tím je indukce provedena a věta dokázána.

□

Definice 4.4.4. *Binární vyhledávací strom* je binární strom $(G, \perp)$ ve kterém jsou data asociována s vrcholy. Data jsou uspořádána tak, že pro každý vrchol x, data v levém (resp. pravém) podstromu s kořenem x jsou menší (resp. větší) než data v x.

Algoritmus 4.4.3. (Prohledávání binárního stromu) Mějme binární vyhledávací strom $(G, \perp)$. Jestliže v je vrchol grafu $(G, \perp)$, funkce LEFT (v) vrátí levého následníka vrcholu v. Podobně, funkce RIGHT (v) vrátí pravého následníka vrcholu v. Funkce VALUE (v) vrací hodnotu (tj. data) ve v. Když v nemá levého či pravého následníka, příslušná funkce vrátí kód λ. Následující algoritmus vrátí v proměnné P vrchol v obsahující předem zadanou datovou hodnotu W, nebo λ, pokud datová hodnota W není ve stromu $(G, \perp)$.

(i) [Inicializace]

$P := \perp$;

(ii) [Nalezeno?]

IF $P = \lambda$, THEN STOP (hledání končí neúspěšně);

IF VALUE $(P) = W$, THEN STOP (hledání končí úspěšně, P je vrchol, obsahující W);

(iii) [Přechod na další]

IF $W >$ VALUE (P), THEN $P :=$ RIGHT (P) ELSE $P :=$ LEFT (P);

GOTO (2);

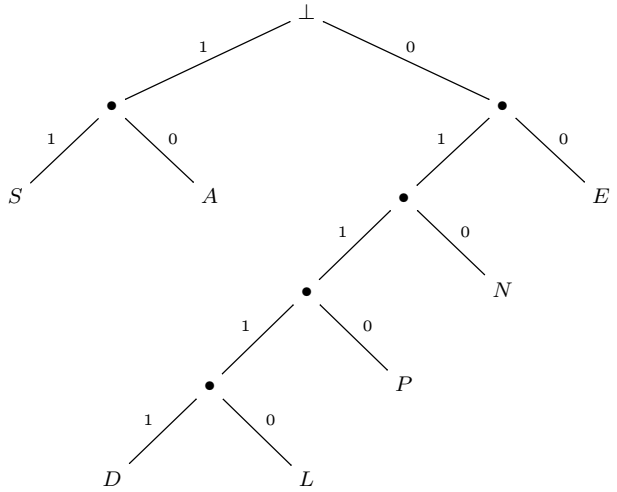
Cvičení

4.4.1. Určete počet koster úplného grafu K_n o n vrcholech pro $n = 1, 2, 3, 4$.

4.4.2. * Pokuste se zobecnit výsledek předchozího cvičení a dokázat pro libovolné $n \in \mathbb{N}$.

4.4.3. Dokažte, že strukturní vzorec uhlovodíku C_nH_{2n+2} je strom.

4.4.4. V Huffmanově kódu s kořenovým binárním stromem



dekódujte řetězce 011000010, 01110100110 a 01111001001110.

4.4.5. V Huffmanově kódu z předchozího příkladu zakódujte řetězce “DEN”, “NEED” a “LEADEN”.

4.4.6. Využijte text aktuálního příkladu k definici Huffmanova kódu, ve kterém tento text zakódujte.

4.4.7. V grafech z příkladů 2,3,4 ze cvičení 4.2 najděte kostru s minimálním celkovým ohodnocením.

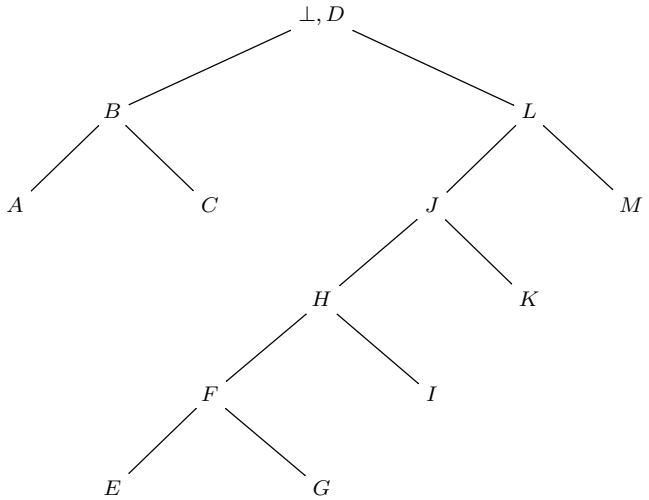
4.4.8. Najděte všechny binární stromy s 2,3 a 4 vrcholy.

4.4.9. Najděte všechny plné binární stromy se 7, 8 a 9 vrcholy.

4.4.10. Najděte (pokud existuje) plný binární strom se 4 vnitřními a 5 koncovými vrcholy.

4.4.11. Najděte (pokud existuje) plný binární strom výšky 3 s 9 koncovými vrcholy.

4.4.12. Aplikujte algoritmus 4.4.3 na binární vyhledávací strom

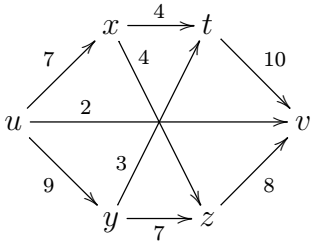


a simulujte vyhledání vrcholu se znakem “I”, jsou-li data v binárním stromu řazena abecedně.

4.5 Tok v orientovaném grafu

Definice 4.5.1. Buď $G = (V, H)$ souvislý orientovaný graf a $u \in V$ vrchol, z něhož hrany pouze vychází, $v \in V$ vrchol, do něhož hrany pouze vchází. *Tokem v G mezi vrcholy u, v* nazýváme takové ohodnocení hran v G, že součet ohodnocení hran, které vychází z vrcholu $x \notin \{u, v\}$, je roven součtu ohodnocení hran, které do vrcholu x vchází.

Příklad 4.5.1. Najděte maximální tok mezi vrcholy u, v v grafu G, kde ohodnocení každé hrany znamená maximální tok příslušnou hranou a určete maximální propustnost grafu G:



Algoritmus 4.5.1. (Nalezení maximálního toku)

0. Najdeme nějaký, libovolný tok F_0 z u do v v G.

1. K danému toku F_n sestrojíme pomocný graf $G(F_n)$ takto: Vynecháme z G každou nasycenou hranu a ke každé hraně $[a, b]$ kladně ohodnocené tokem F_n v takto vzniklém grafu přidáme hranu opačně orientovanou $[b, a]$, pokud $[b, a] \notin H$. Vzniklý graf je graf $G(F)$.

Jestliže nyní v $G(F_n)$ neexistuje cesta z u do v, je F_n maximální tok.

2. Jestliže v $G(F_n)$ existuje cesta z u do v $P = (U_P, H_P)$, sestrojíme tok F_{n+1} z u do v takto:

   a) Jestliže $[a, b] \in H_P \cap H$, ohodnotíme ji číslem $\varepsilon > 0$, které určíme dodatečně.

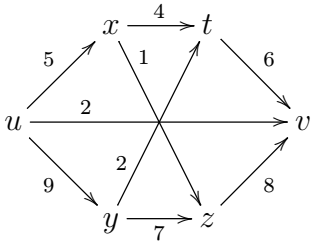
   b) Jestliže $[a, b] \in H_P \setminus H$, ohodnotíme ji číslem $-\varepsilon$.

   c) Jestliže $[a, b] \notin H_P$, ohodnotíme ji číslem 0.

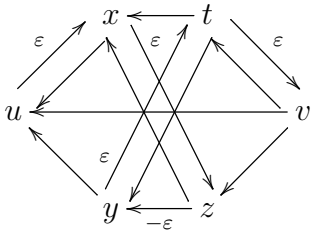
d) Za ε zvolíme maximální číslo takové, aby $F_{n+1} := F_n + F'_n(\varepsilon)$ byl přípustný tok v grafu G (tj. aby ohodnocení žádné hrany nepřekročilo maximální přípustné ohodnocení, ani nebylo záporné).

Dále pokračujeme bodem 1., kde místo F_n bereme F_{n+1}.

Příklad 4.5.2. Řešení příkladu Sestrojme nějaký tok F_0:



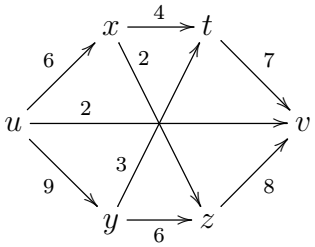
Pak $G(F_0)$ je graf



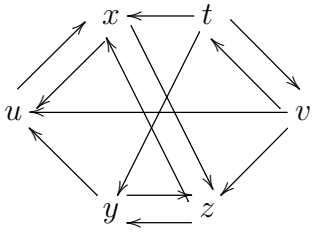
V $G(F_0)$ existuje cesta

$$u(u,x)x(x,z)z(z,y)y(y,t)t(t,v)v$$

z u do v, pokračujeme tedy sestrojením $F_1 = F_0 + F'_0(\varepsilon)$ pro $\varepsilon = 1$:



Pak $G(F_1)$ je graf



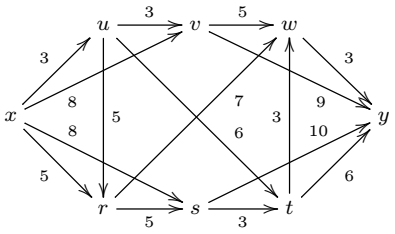
V $G(F_1)$ už neexistuje cesta z u do v, tedy tok F_1 je maximální. Přitom maximální propustnost grafu G mezi vrcholy u, v je součet ohodnocení hran, které vychází z x, tedy 17.

Softwarové nástroje: Vlastnosti orientovaných grafů – maximální tok

Cvičení

4.5.1. Aplikujte algoritmus 4.5.1 na příklad 4.5.1 tak, že vyjdete z jiného základního toku F_0 než ve výše uvedeném řešení příkladu.

4.5.2. Najděte maximální tok mezi vrcholy x a y v grafu



a určete jeho propustnost.

Počítačové cvičení

4.5.3. Uvažujte neorientovaný graf $G = (V, H)$ bez smyček a násobných hran s množinou $V = \{1, 2, \ldots, n\}$ reprezentovaný pomocí

(i) množiny H, reprezentované množinou dvojic vrcholů spojených hranou,

(ii) *matice sousednosti*, v níž řádky a sloupce odpovídají vrcholům grafu; číslo 1 je v pozicích, které odpovídají vrcholům, které jsou spojeny hranou, číslo 0 je v ostatních pozicích.

(iii) *matice incidence*, v níž řádky odpovídají vrcholům a sloupce hranám grafu; číslo 1 je pozicích, které odpovídají incidentním vrcholům a hranám, 0 je v ostatních pozicích.

Napište program, který ze zadání grafu podle (a) vygeneruje reprezentace podle (b) a (c).

4.5.4. Napište program, který ze zadání grafu podle (b) vygeneruje reprezentace podle (a) a (c) (viz. příklad 1).

4.5.5. Napište program, který ze zadání grafu podle (c) vygeneruje reprezentace podle (a) a (b) (viz. příklad 1).

4.5.6. Napište program, který zjistí, zda je daný graf Eulerovský.

4.5.7. Napište program, který zjistí, zda je daný graf souvislý.

4.5.8. Implementujte algoritmus nalezení nejkratší cesty v neorientovaném grafu.

4.5.9. Napište program, který nalezne komplementární graf k zadanému grafu.

4.5.10. Napište program, který zjistí, zda je daný graf strom.

4.5.11. Napište program, který zakóduje zadaný řetězec pomocí zadaného Huffmanova kódu.

4.5.12. Napište program, který dekóduje zadaný řetězec pomocí zadaného Huffmanova kódu.

Pojmy k zapamatování

- Neorientovaný a orientovaný graf. Vrcholy a hrany.
- Sled, tah a cesta. Souvislost grafů.
- Podgraf, indukovaný podgraf, faktor grafu.
- Rovinný graf, charakteristické grafy $K_{3,3}$, K_5.
- Nejkratší cesta v ohodnoceném grafu.
- Eulerovský a Hamiltonovský graf.
- Stromy, kostry. Minimální kostra.
- Konstrukce Huffmanova kódu.
- Tok v orientovaném grafu.

Klíčové myšlenky kapitoly

- Graf je souvislý, právě když mezi každými dvěma jeho vrcholy existuje cesta.
- Algoritmus nalezení nejkratší cesty v ohodnoceném grafu.
- Rovinnost grafu se vyvrací vztahem mezi vrcholy, hranami a oblastmi, případně pomocí podgrafů, homeomorfních s $K_{3,3}$ nebo K_5. Nikoliv tím, že „ se hrany kříží".
- O možnosti kreslit graf jedním tahem rozhoduje sudost stupně jeho vrcholů - Eulerovskost grafu, a jeho souvislost.
- Barvení grafu. Rovinné grafy mají chromatické číslo nejvýše 4.
- Algoritmus nalezení minimální kostry v ohodnoceném grafu.
- Algoritmus nalezení maximálního toku v orientovaném, ohodnoceném grafu.

Odkazy na literaturu

Aplikace teorie grafů jsou v informatice velmi časté a je velmi obtížné vybrat a pokrýt ty nejdůležitější partie. Hlavními zdroji pro tuto kapitolu byly publikace [15], [17] a [18], které ovšem studovanou problematiku zdaleka nevyčerpávají. Následující citace se vztahují k seznamu literatury na konci učebního textu. Uvedeny jsou zde učebnice a monografie, rozšiřující látku probranou v této kapitole.

[1], [9], [10], [14], [15], [16], [17], [18], [19], [20], [21], [22], [26], [27], [28], [33], [32], [35], [36], [37], [38]

Další příklady k procvičení

Elektronická banka příkladů

Matematický software

Vlastnosti neorientovaných grafů – grafové charakteristiky
Vlastnosti neorientovaných grafů – nalezení nejkratší cesty
Vlastnosti neorientovaných grafů – nalezení minimální kostry
Vlastnosti orientovaných grafů – maximální tok

Literatura

[1] Anderson I., *A First Course in Discrete Mathematic*, Springer-Verlag, London, 2001.

[2] Acharjya D. P., Sreekumar, *Fundamental Approach to Discrete Mathematics*, New Age International Publishers, New Delhi, 2005.

[3] Bender A. E., Williamson S. G., *A Short Course on Discrete Mathematics*, Bender & Williamson, 2004.

[4] Engelking R., *General Topology*, Heldermann Verlag, Berlin, 1989.

[5] Faure R., Heurgon E., *Uspořádání a Booloeovy algebry*, Academia, Praha, 1984.

[6] Gantmacher, F. R., *The Theory of Matrices*, Chelsea Publ. Comp., New York, 1960.

[7] Garnier R.,Taylor J., *Discrete Mathematics for New Technology*, Institute of Physics Publishing, Bristol and Philadelphia, 2002.

[8] Gratzer G., *General Lattice Theory*, Birkhauser Verlag, Berlin, 2003.

[9] Grimaldi R. P., *Discrete and Combinatorial Mathematics*, Pearson Addison Valley, Boston, 2004.

[10] Grossman P., *Discrete mathematics for computing*, Palgrave Macmillan, New York, 2002.

[11] Hellerstein N. S., *Diamond – a Paradox Logic*, World Scientific, Singapore, 1997.

[12] Herman, G. T., *Geometry of Digital Spaces*, Birkhauser, Boston, 1998.

[13] Chen L., *Discrete Surfaces and Manifolds*, Scientific and Practical Computing, Rockville, 2004.

[14] Jablonskij S. V., *Úvod do diskrétnej matematiky*, Alfa, Bratislava, 1984.

[15] Johnsonbaugh R., *Discrete mathematics*, Macmillan Publ. Comp, New York 1984.

[16] Klazar M., Kratochvíl J, Loebl M., Matoušek J. Thomas R., Valtr P., *Topics in Discrete Mathematics*, Springer-Verlag, Berlin, 2006.

[17] Kolář J., Štěpánková O., Chytil M., *Logika, algebry a grafy*, SNTL, Praha, 1989.

[18] Kolibiar M. a kol., *Algebra a príbuzné disciplíny*, Alfa, Bratislava, 1992.

[19] Kučera L., *Kombinatorické algoritmy*, SNTL, Praha, 1983.

[20] Lipschutz S., Lipson M. L., *2000 Solved Problems in Discrete Mathematics*, McGraw-Hill, New York, 1992.

[21] Lipschutz S., Lipson M. L., *Theory and Problems of Discrete Mathematics*, McGraw-Hill, New York, 1997.

[22] Lovász L., Pelikán J., Vesztergombi„ *Discrete Mathematics*, Springer-Verlag, New York, 2003.

[23] Lukasová A., *Formální logika v umělé inteligenci*, Computer Press, Brno, 2003.

[24] Manna Z., *Matematická teorie programů*, SNTL, Praha, 1981.

[25] Mannucci M. A., Yanofsky N. S., *Quantum Computing For Computer Scientists*, Cambridge University Press, Cambridge, 2008.

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

[27] Matoušek J., Nešetřil J., *Invitation to Discrete Mathematics*, Oxford University Press, Oxford, 2008.

[28] Nešetřil J., *Teorie grafů*, SNTL, Praha, 1979.

[29] Novák V., *Fuzzy množiny a jejich aplikace*, SNTL, Praha, 1986.

[30] O'Donnell, J., Hall C., Page R., *Discrete Mathematics Using a Computer*, Springer-Verlag, London, 2006.

[31] Peregrin J., *Logika a logiky*, Academia, Praha, 2004.

[32] Pemmaraju, Skiena S., *Computational Discrete Mathematics*, Cambridge University Press, Cambridge, 2003.

[33] Preparata F. P.,Yeh R. T., *Úvod do teórie diskrétnych štruktúr*, Alfa, Bratislava, 1982.

[34] Procházka L. akol., *Algebra*, Academia, Praha, 1990.

[35] Rosen K. H., *Discrete Mathematics and its Applications*, AT & T Information Systems, New York, 1988.

[36] Rosen, K. H. et al., *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Boca Raton, 2000.

[37] Ross, S. M., *Topics in Finite and Discrete Mathematics*, Cambridge University Press, Cambridge, 2000.

[38] Sedláček J., *Úvod do teorie grafů*, Academia, Praha, 1977.

[39] Sochor, A., *Klasická matematická logika,*, Karolinum, Praha, 2001.

[40] Štěpán J., *Diskrétní matematik*, Univerzita Palackého, Olomouc, 1990 (skriptum).

[41] Švejdar, V., *Logika, neúplnost, složitost a nutnost*, Academia, Praha, 2002.

[42] Vickers S., *Topology Via Logic*, Cambridge University Press, Cambridge, 1989.