

Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Miroslav Řezáč

Booleova algebra

Katedra didaktiky matematiky

Vedoucí bakalářské práce: doc. RNDr. Oldřich Odvárko, DrSc.

Studijní program: Matematika, matematika zaměřená na vzdělání,
matematika-informatika

2009

Rád bych poděkoval zejména mému vedoucímu práce doc. RNDr. O. Odvárkovi, DrSc. za výběr tématu, odbornou pomoc hlavně po matematické a metodické stránce a za laskavé zapůjčení odborné literatury. Dále mé poděkování náleží doc. RNDr. E. Caldovi, CSc., který mi v kombinatorickém semináři problematiku Booleovy algebry přiblížil a poskytl mi další potřebnou literaturu. V neposlední řadě bych chtěl poděkovat slečně A. Mottlové, která mi pomohla s korekturou textu po stránce jazykové.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Kladně dne 20. 5. 2009

Miroslav Řezáč

Obsah

Úvod	5
1 Vybudování Booleovy algebry	7
1.1 Kartézský součin množin	7
1.2 Relace	8
1.3 Uspořádání a Hasseův diagram	13
1.4 Supremum a infimum	21
1.5 Svazy	26
1.6 Distributivní svazy, Booleova algebra	30
1.7 Vlastnosti Booleovy algebry	36
1.8 Početní postupy	40
2 Využití Booleovy algebry	43
2.1 Množinová algebra	43
2.2 Algebra pravdivostních hodnot výroků	47
Závěr	54
Literatura	55

Název práce: Booleova algebra

Autor: Miroslav Řezáč

Katedra (ústav): Katedra didaktiky matematiky

Vedoucí bakalářské práce: doc. RNDr. Oldřich Odvárko, DrSc.

e-mail vedoucího: Oldrich.Odvarko@mff.cuni.cz

Abstrakt: Tento text je určen především pro vyučující středoškolské matematiky, jako pomůcka při přípravě výběrových seminářů, a pro nadané studenty středních škol, kteří mají hlubší zájem o matematiku. V této práci budujeme Booleovu algebru jakožto speciální případ uspořádané množiny. Využíváme matematický aparát středoškolské matematiky k zavádění pojmů, jakými jsou např. relace, uspořádání, supremum, infimum nebo svaz. Všechny tyto pojmy vysvětlujeme na konkrétních příkladech. Výklad je doplněn obrázky, zejména jde o Hasseovy a Vennovy diagramy. Práce obsahuje řešené příklady a detailněji se zabývá množinovou algebrou a algebrou pravdivostních hodnot výroků.

Klíčová slova: uspořádaná množina, svaz, Booleova algebra

Title: Boolean algebra

Author: Miroslav Řezáč

Department: Didactics of mathematics

Supervisor: doc. RNDr. Oldřich Odvárko, DrSc.

Supervisor's e-mail address: Oldrich.Odvarko@mff.cuni.cz

Abstract: This article is meant as a tool for high school math teachers during facultative seminars preparation as well as for talented high school students with a deeper interest in math. This work concerns with a formation of Boolean algebra and its application. It deals with Boolean algebra as with a particular case of partially ordered set (poset) in contrast to its frequent axiomatic perception. It tries to concentrate on this issue and to open it up to non-experts. The interpretation is accompanied by various pictures especially Hasse and Venn diagrams. The work contains also resolved examples and deals with set algebra and algebra of truth-value. Another subject of interest is simplifying of set records and solution of set formulas in set algebra. As for the truth-value algebra the correctness of conclusions from given set of presumptions is verified and logical word exercises are solved.

Keywords: partially ordered set (poset), lattice, Boolean algebra

Úvod

V této práci se věnujeme budování Booleovy algebry a její aplikaci. Booleova algebra je často zaváděna až v okamžiku, kdy je potřeba její praktická aplikace v logice, respektive v logických obvodech. Často je tato struktura zavedena axiomaticky (někdy jen výčtem pravidel) a je předložena jako „početní kuchařka“ pro řešení konkrétních příkladů.

Odborné knihy, které se zabývají algebrou a uspořádanými množinami, sice Booleovu algebru konstruují, ale pouze jako jeden z mnoha vedlejších produktů této teorie. Zároveň jsou tyto texty těžko přístupné čtenáři, který není odborníkem v oboru matematiky, a studují tuto problematiku příliš rozsáhle.

Naším cílem je vybudovat Booleovu algebru podobným způsobem jako odborné knihy, ale omezit se jen na fakta, která jsou při této konstrukci nutná, výklad výrazně zjednodušit a demonstrovat na názorných příkladech a obrázcích. Výrazně tedy zúžíme pohled na uspořádané množiny. Zbylé vlastnosti a souvislosti buď úplně vynecháme nebo se o nich zmíníme v poznámkách a komentářích.

Tento text je určen především pro vyučující středoškolské matematiky, jako pomůcka při přípravě výběrových seminářů, a pro nadané studenty středních škol, kteří mají hlubší zájem o matematiku.

U čtenáře této práce se předpokládá, že má dobré znalosti matematiky, zejména o učivu o množinách, v němž rozumí symbolům \in , \subseteq , \cup , \cap a umí je používat. Důležitá je i znalost výrokové logiky, ve které se předpokládá dovednost pracovat s logickými spojkami \Rightarrow , \Leftrightarrow , \wedge , \vee a kvantifikátory \forall , \exists . Ve znění vět a definic budeme psát kvantifikátory a logické spojky slovně, aby byl text lépe srozumitelný pro čtenáře, který není zvyklý na tuto symboliku. Ze stejného důvodu jsou některé definice a věty formulovány volněji. Dále se předpokládá znalost elementární matematiky, teorie dělitelnosti a Vennových diagramů, které se uplatňují v konkrétních příkladech.

Celý text je členěn do dvou kapitol, přičemž každá kapitola obsahuje několik oddílů. Při budování teorie se nevyhneme zavádění nových pojmů, **definic**, které v textu zvýrazníme modrou barvou. V poznámkách pod definicí se pokusíme tyto pojmy ještě neformálně vysvětlit a doplnit, případně upozornit na některé souvislosti. Pokud zjistíme nějaké další vlastnosti nebo zákonitosti, vyznačíme je v textu klíčovým slovíčkem **věta** a zvýrazníme je červenou barvou. Ke každé takové větě je předložen **důkaz**.

První kapitola se věnuje budování Booleovy algebry. Každý oddíl se zabývá jedním důležitým pojmem, který názorně ukážeme na konkrétních příkladech. Dále budeme dokazovat důležité vlastnosti, které později využijeme při řešení konkrétních příkladů. Tato kapitola se opírá zejména o odbornou literaturu [2], [4], ze které čerpá věty a definice.

Metodické zpracování (celková koncepce, řazení pojmů, využívání diagramů, ilustrace na konkrétních příkladech) je vlastní prací. Poslední dva oddíly této kapitoly se zabývají odvozováním dalších vlastností a početními metodami v Booleově algebře. Velká část těchto poznatků je také obsažena v knihách [1], [3], ze kterých bylo čerpáno.

Druhá kapitola se zabývá aplikací Booleovy algebry na množinové algebře a na algebře pravdivostních hodnot výroků. Naučíme se zjednodušovat množinové zápisy, řešit množinové rovnice a ověřovat správnost úsudku z množiny předpokladů. Na závěr je uvedeno několik logických slovních úloh, na které lze aplikovat Booleovu algebru. Většinou jde o úlohy přeformulované z literatury [3], [5]. Zadání příkladu 8 a cvičení 9 a 11 jsou citována z literatury [5]. Řešení příkladů jsem koncipoval tak, aby byla optimálně využita teorie budovaná v první kapitole.

Kapitola 1

Vybudování Booleovy algebry

1.1 Kartézský součin množin

Nejprve zavedeme jednu ze základních operací s množinami, kartézský součin.

Definice 1. *Kartézským součinem* dvou množin A a B budeme rozumět množinu všech uspořádaných dvojic (a, b) , kde $a \in A$ a $b \in B$. Značíme symbolem $A \times B$.

Poznámka 1. Kartézský součin bychom mohli definovat i pro více než dvě množiny. Například kartézský součin tří množin A , B a C je množina všech uspořádaných trojic (a, b, c) , kde $a \in A$, $b \in B$ a $c \in C$ atd. Protože kartézský součin více než dvou množin nebudeme v našem textu využívat, omezíme se pouze na dvě množiny.

Poznámka 2. **Konvence závorkování:** V matematice jsou kulaté závorky vyhrazeny pro uspořádané dvojice, v nichž závisí na pořadí prvků, a proto $(a, b) \neq (b, a)$ (za předpokladu, že $a \neq b$). Na rozdíl od složených závorek, které se používají pro neuspořádané dvojice, kde na pořadí prvků nezáleží, a proto $\{a, b\} = \{b, a\}$. Složené závorky se například využívají i při výčtu prvků množin, ve kterém na pořadí prvků nezáleží.

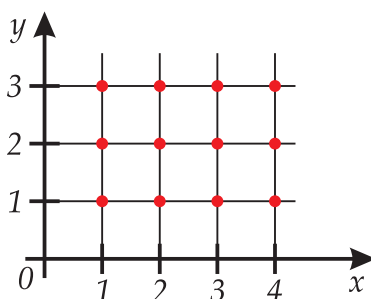
Poznámka 3. Ještě pro přesnost a kontrolu našeho výsledku můžeme zmínit, že pokud množina A obsahuje m prvků a množina B obsahuje n prvků, potom kartézský součin $A \times B$ obsahuje právě $m \cdot n$ prvků.

Nyní se již pokusíme vytvořit kartézský součin konkrétních množin.

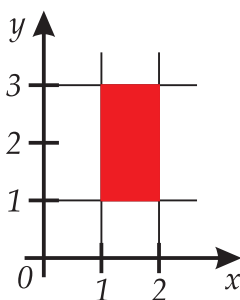
Příklad 1. Nechť množina $A = \{1, 2, 3\}$ a $B = \{\square, \triangle\}$. Chceme vytvořit kartézský součin $A \times B$. Pro znázornění kartézského součinu konečných množin lze s výhodou využít tabulky. Do prvního sloupce opišeme všechny prvky množiny A a do prvního řádku opišeme všechny prvky množiny B . Následuje vyplnění zbylých polí tabulky, kterými budou dvojice prvků, kde na prvním místě bude prvek napsaný na začátku aktuálního řádku a na druhém místě bude prvek napsaný na začátku příslušného sloupce. Tím získáme všechny uspořádané dvojice takové, že první prvek je z množiny A a druhý z množiny B . Kartézský součin $A \times B = \{(1, \square), (1, \triangle), (2, \square), (2, \triangle), (3, \square), (3, \triangle)\}$.

	□	△
1	(1, □)	(1, △)
2	(2, □)	(2, △)
3	(3, □)	(3, △)

Příklad 2. Nechť množina $A = \{1, 2, 3, 4\}$ a $B = \{1, 2, 3\}$. Hledáme kartézský součin $A \times B$. Obě množiny jsou konečné, proto bychom mohli opět využít tabulky. Ukážeme ovšem ještě jiný způsob grafického znázornění kartézského součinu dvou množin, jejichž prvky jsou čísla. Nakreslíme kartézskou soustavu souřadnic, na osu x vyneseme prvky první množiny, na osu y prvky druhé množiny a v každém takovém bodě vztyčíme kolmici k příslušné ose. Kartézským součinem těchto dvou množin je množina všech souřadnic průsečíků těchto kolmic. $A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (4, 3)\}$.



Příklad 3. Nechť A, B jsou uzavřené intervaly $A = \langle 1, 2 \rangle$, $B = \langle 1, 3 \rangle$. Vzhledem k tomu, že obě množiny mají nekonečně mnoho prvků, není možné zapsat kartézský součin $A \times B$ výčtem prvků. Kartézský součin můžeme velice snadno znázornit pomocí kartézské soustavy souřadnic jako oblast vymezenou těmito intervaly. Kartézský součin $A \times B$ je množina všech bodů zapsaná v souřadnicích z této oblasti.



1.2 Relace

Definice 2. *Relací* U na množině A budeme rozumět každou podmnožinu kartézského součinu $A \times A$.

Poznámka 1. Definici bychom mohli vyslovit obecněji pro relaci mezi množinami A a B , jako podmnožinu kartézského součinu $A \times B$. Protože bychom tuto definici v následujícím textu nevyužili, omezujeme se jen na relace **na množině** A .

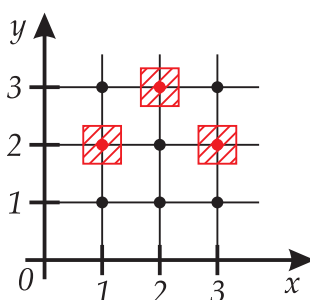
Poznámka 2. Přesněji bychom měli používat pojem **binární** relace na množině A , abychom zdůraznili, že se jedná o podmnožinu kartézského součinu dvou množin. My ovšem slovo binární, stejně jako většina matematiků, budeme vynechávat.

Než ukážeme relace, které v matematice prakticky využíváme a na kterých budeme budovat i naši teorii, řekneme si, jak takovou relaci můžeme zadat. Pro názornost budeme zkoumat relace na množině $A = \{1, 2, 3\}$.

- Z definice víme, že relace je podmnožina jisté množiny. Jestliže je tato množina konečná, můžeme ji snadno zapsat výčtem všech prvků, např. $U_1 = \{(1, 2), (2, 3), (3, 2)\}$.
- Pokud využijeme tabulku pro znázornění kartézského součinu, můžeme příslušnost dvojice prvků v relaci znázornit symbolem \oplus na dané pozici. Naopak symbol \ominus nám bude signalizovat nepřítomnost dvojice prvků v relaci. Relace U_1 by se potom zapsala:

	1	2	3
1	\ominus	\oplus	\ominus
2	\ominus	\ominus	\oplus
3	\ominus	\oplus	\ominus

- Stejně bychom mohli relaci zadat pomocí grafického znázornění relace v kartézské soustavě souřadnic. Prvky, které jsou v relaci, bychom vizuálně odlišili od prvků, které v relaci nejsou. U_1 znázorněná graficky v kartézské soustavě souřadnic:



- Uvažujme relaci $U_2 = \{(1, 2), (1, 3), (2, 3)\}$. Je zřejmé, že $a, b \in U_2 \Leftrightarrow a < b$. Pomocí tohoto „matematického předpisu“ se relace zadává častěji než výčtem prvků, kterým jsme relaci zaváděli v předchozích příkladech.

Protože budeme relace často zadávat pomocí „matematického předpisu“ zavedeme novou konvenci zápisu a značení relace, kterou zformulujeme jako definici.

Definice 3. Necht U je relace na množině A .

Řekneme, že dva prvky $a, b \in A$ **jsou v relaci** U , jestliže $(a, b) \in U$.

Tuto skutečnost budeme zkráceně zapisovat aUb .

Poznámka. Tato definice slouží především k lepší korespondenci s matematickými zápisy, které již známe. Jestliže například za relaci U zvolíme $<$, potom zápis $1 < 3$ je nám bližší než zápis $(1, 3) \in <$.

Nyní již ukážeme některé konkrétní příklady relací. První tři relace budeme zkoumat na množině $A = \{1, 2, 3, 4\}$. Budeme hledat všechny prvky, které jsou v dané relaci. Ukážeme, jak se tyto relace zapisují a jak tyto relace čteme.

Příklad 4. Relace U_3 zvaná „rovná se“ v matematice značená symbolem $=$.

$$U_3 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$$

Píšeme: $1 = 1, 2 = 2, 3 = 3, 4 = 4$.

Příklad 5. Relace U_4 zvaná „je menší než“ v matematice značená symbolem $<$.

$$U_4 = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

Píšeme: $1 < 2, 1 < 3, 1 < 4, 2 < 3, 2 < 4, 3 < 4$.

Čteme: „Jedna je menší než dva.“

Podobně by se zavedly relace: „je menší nebo rovno než“, „je větší (nebo rovno) než“.

Příklad 6. Relace U_5 zvaná „dělí“ v matematice občas značená symbolem $|$.

$$U_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$$

Píšeme: $1|1, \dots, 2|4, 3|3, 4|4$.

Čteme: „Jedna dělí jedna.“, „Dvě dělí čtyři.“

Poznámka. Pro dvě čísla $a, b \in \mathbb{N}$ platí: $a|b$, právě tehdy, když existuje $x \in \mathbb{N}$ takové, že $ax = b$.

Abychom ukázali ještě jednu velice důležitou relaci, budeme zkoumat množinu, která bude obsahovat všechny podmnožiny dané množiny.

Definice 4. *Potenční množinou* množiny X budeme rozumět množinu $P(X)$, která obsahuje všechny podmnožiny množiny X .

Poznámka 1. Při tvorbě potenční množiny $P(X)$ nesmíme zapomenout, že celá množina X je také podmnožinou X a zároveň prázdná množina \emptyset je podmnožinou X .

Poznámka 2. Lze ukázat, že pokud množina X má n prvků, potom množina $P(X)$ má právě 2^n prvků. My tuto skutečnost dokazovat nebudeme.

Pro názornost vytvoříme potenční množinu $P(A)$ množiny $A = \{1, 2\}$.

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

V následujících dvou příkladech budeme zkoumat relace na této potenční množině.

Příklad 7. Relace U_6 zvaná „je podmnožinou“ v matematice značená symbolem \subseteq .

$$U_6 = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}$$

Píšeme: $\emptyset \subseteq \{1\}, \emptyset \subseteq \{2\}, \dots, \{2\} \subseteq \{1, 2\}, \{1, 2\} \subseteq \{1, 2\}$.

Čteme tak, jak jsme zvyklí, např. „množina $\{1\}$ je podmnožinou množiny $\{1, 2\}$.“

Příklad 8. Relace U_7 je definovaná takto: Dva prvky $a, b \in P(A)$ jsou v relaci U_7 na množině $P(A)$, jestliže počet prvků množiny $a \cap b$ je roven jedné.

Abychom zjistili, které dvojice prvků jsou v této relaci, musíme probrat všechny možné dvojice prvků, kterých je celkem 16. Pokud systematicky vyloučíme některé dvojice množin (například takové, které obsahují prázdnou množinu) snadno pak ověříme, které dvojice prvků jsou v této relaci.

$$U_7 = \{(\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{2, 1\}), (\{2, 1\}, \{1\}), (\{2, 1\}, \{2\})\}$$

Bohužel nemáme jednoduchý název pro tuto relaci, proto bychom museli říkat „množina $\{1\}$ je v relaci U_7 s množinou $\{1, 2\}$.“ Zkráceně zapsáno $\{1\}U_7\{1, 2\}$.

Zatím jsme každou relaci zapisovali buď předpisem nebo výčtem prvků. Nyní si ukážeme ještě jeden způsob zápisu relace, který bude graficky mnohem názornější a který se nám bude hodit při vyšetřování některých dalších vlastností.

Nejlépe ho vysvětlíme na konkrétním případu. Vezměme například relaci U na množině $A = \{1, 2, 3, 4, 5\}$, kde $U = \{(1, 2), (1, 3), (2, 3), (3, 2), (5, 5)\}$. Tuto relaci se nyní pokusíme názorně graficky reprezentovat.

Každý prvek znázorníme kroužkem a připíšeme k němu název tohoto prvku:



Nyní budeme chtít znázornit příslušnou relaci. Uvědomíme-li si, že relace znázorňuje spojitosti mezi dvojicemi prvků, můžeme to v našem obrázku snadno znázornit tak, že příslušné dva prvky, které jsou v relaci, spojíme čarou. Víme, že prvek 1 je v relaci U s prvkem 2, proto spojíme tyto dva prvky čarou:



To ovšem není přesné. Víme totiž, že prvek 1 je v relaci U s prvkem 2, ale prvek 2 není v relaci U s prvkem 1 (že platí $1U2$ nikoli $2U1$). Z našeho obrázku tuto skutečnost zatím vyčíst nelze. Můžeme se ale dohodnout, že na konec čáry u druhého prvku z relace nakreslíme šipku:



Nyní můžeme pokračovat a dokreslit zbylé čáry se šipkami do našeho obrázku:



Když se podíváme, jak jsme graficky znázornili relaci U , je zřejmé, že ji dokážeme zcela přesně zrekonstruovat.

Poznámka. Takovým obrázkům se v diskretní matematice říká **graf**. Kroužkům, které jsme využívali pro znázornění prvků, se říká **uzly** a čáry se šipkou se nazývají **orientované hrany**. Speciálnímu případu orientované hrany, která začíná i končí ve stejném uzlu, říkáme **smyčka**.

Ještě ve stručnosti uvedeme postup, jak danou relaci graficky znázornit:

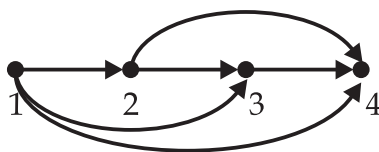
1. Zobrazíme všechny prvky množiny pomocí uzlů.
2. Mezi dvojicí prvků, která je v relaci, nakreslíme orientovanou hranu od prvního prvku ke druhému.

Graficky znázorníme relace uvedené v předchozích příkladech:

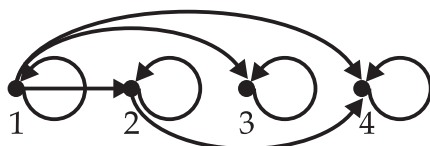
Příklad 9. $U_3 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ z příkladu 4.



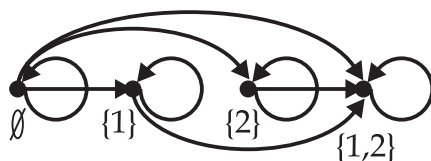
Příklad 10. $U_4 = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$ z příkladu 5.



Příklad 11. $U_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$ z příkladu 6.



Příklad 12. $U_6 = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}$ z příkladu 7.



Příklad 13. $U_7 = \{(\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{2, 1\}), (\{2, 1\}, \{1\}), (\{2, 1\}, \{2\})\}$ z příkladu 8.



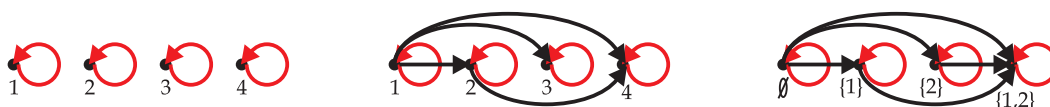
1.3 Uspořádání a Hasseův diagram

V tomto oddílu se budeme zabývat některými speciálními případy relací.

Definice 5. Relaci U na množině A budeme nazývat **reflexivní**, jestliže pro každý prvek $a \in A$ platí aUa .

Poznámka. Grafické znázornění reflexivní relace musí obsahovat smyčku u každého uzlu.

Z grafického znázornění určíme reflexivnost relací zavedených v předchozím oddílu. Po prozkoumání příslušných obrázků zjistíme, že relace U_3, U_5, U_6 jsou reflexivní.



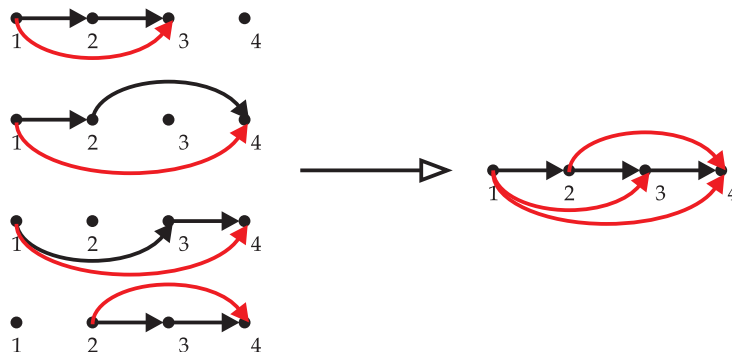
Ostatní relace (U_4, U_7) zmíněné v předchozím oddílu reflexivní nejsou, neboť některé uzly neobsahují smyčky.

Definice 6. Relaci U na množině A budeme nazývat **tranzitivní**, jestliže pro každé tři prvky $a, b, c \in A$ platí: Jestliže aUb a zároveň bUc , potom aUc .

Poznámka. Grafické znázornění tranzitivní relace musí s každými dvěma navazujícími orientovanými hranami obsahovat i orientovanou hranu vedoucí z počátečního uzlu do koncového:



Opět se podíváme, které z výše uvedených relací jsou tranzitivní. Jistě hned vidíme, že relace U_4 „je menší než“ je tranzitivní relace.



Podobně by se ověřilo, že relace U_5 „dělí beze zbytku“ a U_6 „je podmnožinou“ jsou tranzitivní. Nyní se podíváme na relaci U_3 „rovná se.“ Z grafického znázornění relace U_3 poznáme, že žádné dvě orientované hrany na sebe nenavazují. Nemusíme nic ověřovat a můžeme prohlásit, že relace U_3 je tranzitivní.

Zbývá poslední relace U_7 . Podívejme se například na uzly $\{1\}$, $\{2\}$ a $\{1,2\}$. Vidíme, že orientovaná hrana vede z uzlu $\{2\}$ do uzlu $\{1,2\}$ a další orientovaná hrana vede z uzlu $\{1,2\}$ do uzlu $\{1\}$. Pokud by byla tato relace tranzitivní musela by vést orientovaná hrana i z uzlu $\{2\}$ do uzlu $\{1\}$.



Proto relace U_7 nemůže být tranzitivní.

Definice 7. Relaci U na množině A budeme nazývat *antisymetrickou*, jestliže pro každé dva prvky $a, b \in A$ platí: Jestliže aUb a zároveň bUa , potom $a = b$.

Poznámka. V grafickém znázornění antisymetrické relace se nesmí vyskytovat tento případ:



Z grafického znázornění opět určíme, které z výše zmíněných relací jsou antisymetrické. Z obrázků snadno vyvodíme, že relace U_3, U_4, U_5, U_6 jsou antisymetrické. Zbývá už jen poslední relace U_7 . Například vede orientovaná hrana z uzlu $\{2\}$ do uzlu $\{1,2\}$ a zároveň vede orientovaná hrana z uzlu $\{1,2\}$ do uzlu $\{2\}$.



Proto relace U_7 nemůže být antisymetrická.

Zjišťování vlastností relací pomocí grafického znázornění relace je sice velice názorné, ale v praxi velice obtížné nebo dokonce nemožné. Kdybychom například vyšetřovali relaci „rovná se“ na množině všech přirozených čísel, určitě by si každý dokázal představit, že se každá dvě stejná čísla rovnají, tudíž že tato relace je reflexivní. Nakreslit všechna přirozená čísla jistě nebude možné a náš postup selže. Proto vlastnosti příslušné relace budeme většinou zjišťovat z matematického předpisu relace, jak si ukážeme dále.

Definice 8. *Uspořádáním* na množině X budeme rozumět každou reflexivní, tranzitivní a antisymetrickou relaci na množině X .

Abychom zjistili, zda je daná relace uspořádáním, musíme ověřit uvedené tři vlastnosti relace. Ukážeme si několik významných příkladů relací.

1 Relace „je podmnožinou“ na množině všech podmnožin dané množiny.

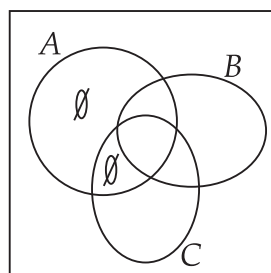
2 Relace „menší nebo rovno“ na množině všech přirozených čísel.

3 Relace „dělí“ na množině všech přirozených čísel.

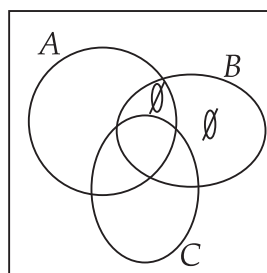
Zjistíme, zda tyto relace splňují vlastnosti uspořádání.

1 Relace \subseteq na množině $P(X)$.

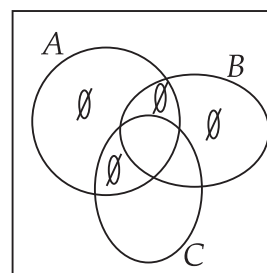
- reflexivní: Pro každé $A \in P(X)$ platí $A \subseteq A$.
Využijeme definici podmnožiny, která říká, že každá množina je podmnožinou sebe sama.
- tranzitivní: Pro každé $A, B, C \in P(X)$ platí: Jestliže $A \subseteq B$ a zároveň $B \subseteq C$, potom $A \subseteq C$.
Tuto vlastnost ukážeme pomocí Vennova diagramu pro množiny A, B, C za předpokladu, že $A \subseteq B$ a $B \subseteq C$.



$A \subseteq B$



$B \subseteq C$

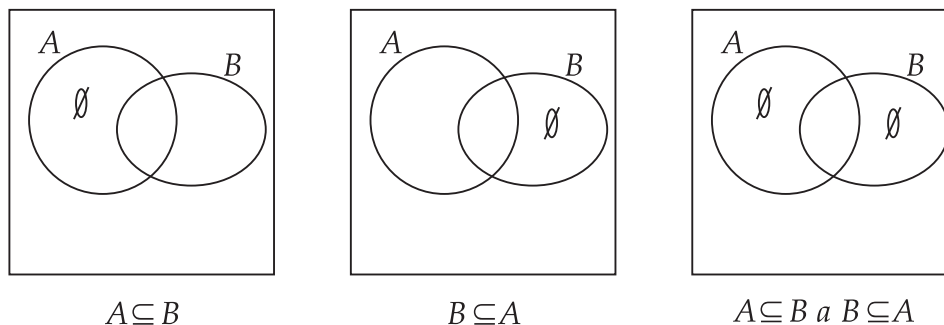


$A \subseteq B$ a $B \subseteq C$

Je vidět, že $A \subseteq C$.

- antisymetrická: Pro každé $A, B \in P(X)$ platí: Jestliže $A \subseteq B$ a zároveň $B \subseteq A$, potom $A = B$.

Opět využijeme Vennův diagram, z kterého je vidět, že $A = B$.



2 Relace \leq na množině \mathbb{N} :

- reflexivní: Pro každé $a \in \mathbb{N}$ platí $a \leq a$.
- tranzitivní: Pro každé $a, b, c \in \mathbb{N}$ platí: Jestliže $a \leq b$ a zároveň $b \leq c$, potom $a \leq c$.
- antisymetrická: Pro každé $a, b \in \mathbb{N}$ platí: Jestliže $a \leq b$ a zároveň $b \leq a$, potom $a = b$.

Všechny tyto vlastnosti přirozených čísel známe z elementární matematiky.

3 Relace $|$ na množině \mathbb{N} .

Využijeme definici symbolu $|$ pro $a, b \in \mathbb{N}$:

$a|b$ právě tehdy, když existuje $x \in \mathbb{N}$ takové, že $ax = b$.

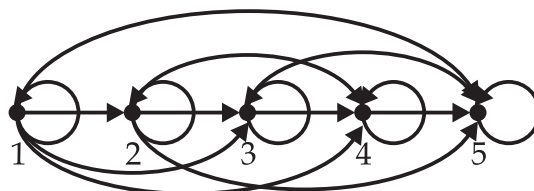
- reflexivní: Pro každé $a \in \mathbb{N}$ platí $a|a$.
Podle definice: $a \cdot 1 = a$
- tranzitivní: Pro každé $a, b, c \in \mathbb{N}$ platí: Jestliže $a|b$ a zároveň $b|c$, potom $a|c$.
Jestliže $a|b$, pak existuje $x \in \mathbb{N}$ takové, že $b = x \cdot a$.
Jestliže také $b|c$, potom musí existovat $y \in \mathbb{N}$ takové, že $c = y \cdot b$.
Po dosazení za číslo b : $c = y \cdot x \cdot a$.
 $y \cdot x$ je přirozené číslo, proto $a|c$.
- antisymetrická: Pro každé $a, b \in \mathbb{N}$ platí: Jestliže $a|b$ a zároveň $b|a$, potom $a = b$.
Jestliže $a|b$, potom $a \leq b$.
Jestliže také $b|a$, potom $b \leq a$.
Jak jsme již ukázali dříve: Jestliže $a \leq b$ a zároveň $b \leq a$, potom $a = b$.

Definice 9. *Uspořádanou množinou* budeme rozumět dvojici (X, U) , kde X je množina a U je uspořádání na X .

Z výše zmíněných úvah plynou následující závěry:

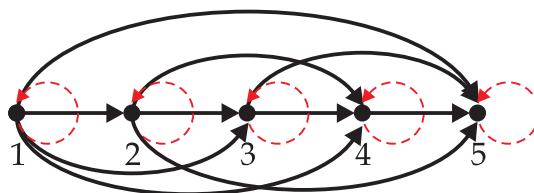
- 1** (\mathbb{N}, \leq) je uspořádaná množina.
- 2** $(P(X), \subseteq)$ je uspořádaná množina.
- 3** $(\mathbb{N}, |)$ je uspořádaná množina.

Ještě než zavedeme operace na uspořádaných množinách, ukážeme si, jak graficky znázornit uspořádanou množinu. Jistě můžeme použít nám již dobře známé grafické znázornění. Když si například zkusíme nakreslit obrázek uspořádané množiny „menší nebo rovno“ na množině prvních pěti přirozených čísel zjistíme, že je obrázek plný orientovaných hran a těžko se v něm orientujeme. Uspořádaná množina $(\{1, 2, 3, 4, 5\}, \leq)$:

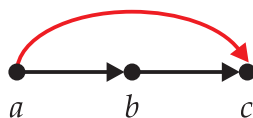


Pokud bychom pokračovali v přidávání dalších prvků a k nim příslušných orientovaných hran, brzy bychom z obrázku nedokázali nic vyčíst. Proto teď zkusíme něco z našeho obrázku odebrat.

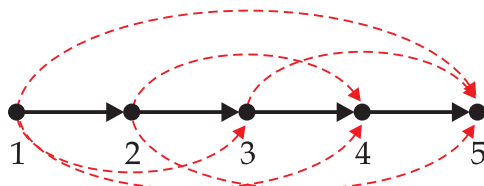
Nejprve si uvědomíme, že každý prvek je v relaci sám se sebou, a proto se v obrázku u každého prvku objevuje smyčka. To nám zajišťuje reflexivnost relace uspořádání. Proto bychom u uspořádaných množin nemuseli tyto smyčky kreslit, protože informaci o tom, že prvek je v relaci sám se sebou, máme zajištěnou.



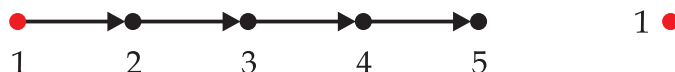
Dále si všimneme, že díky tranzitivitě uspořádání platí: Jestliže vede orientovaná hrana z a do b a z b do c , pak musí vést i orientovaná hrana z a do c .



Orientovaná hrana z a do c nám v tomto případě nepřidává žádnou novou informaci, a můžeme ji tedy také vynechat. Stejně tak i ostatní šipky, které jsou vynucené tranzitivitou uspořádání.



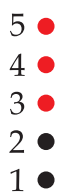
Nyní se pokusíme prvky nějakým způsobem seřadit tak, aby nebylo nutné kreslit šipky u orientovaných hran. Všimněme si, že v obrázku existuje uzel, do kterého nevede žádná orientovaná hrana. V našem případě uzel 1. Mohli bychom si říct, že tento uzel budeme považovat za první a nakreslit si ho stranou.



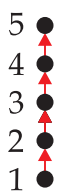
Když tento uzel odebereme z našeho obrázku, včetně orientovaných hran, které z něho vycházejí, zjistíme, že nám opět vznikl uzel, do kterého nevede žádná orientovaná hrana (uzel 2). Můžeme ho opět odebrat a nakreslit stranou. Tentokrát ho umístíme nad uzel 1 do druhé vrstvy.



Tento proces budeme opakovat, dokud nepřekreslíme celý graf. Výsledný obrázek vypadá následovně.



Nakreslíme zpět orientované hrany mezi prvky tak, jak tomu bylo před překreslováním obrázků.



Tímto překreslením jsme si zajistili, že všechny šipky u orientovaných hran se kreslí směrem nahoru (je to díky tomu, že máme zabezpečeno, aby do prvku, který právě překreslujeme, nevedla žádná šipka). Proto již šipku u orientovaných hran nebudeme kreslit.

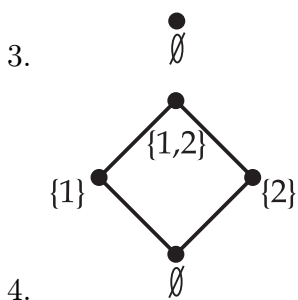
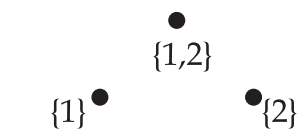
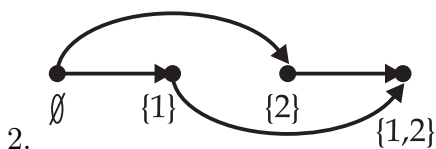
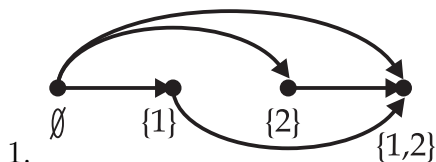


Poznámka. Orientovanou hranu bez šipky budeme zkráceně nazývat **hranou**. Takovému grafickému znázornění uspořádané množiny se říká **Hasseův diagram**.

Opět ve stručnosti uvedeme algoritmus, jak převést grafické znázornění uspořádané množiny na Hasseův diagram.

1. Odebereme smyčky u každého uzlu.
2. Odebereme orientované hrany, které jsou vynucené tranzitivitou.
3. Postupně odebíráme uzly, do kterých nevede žádná orientovaná hrana, a překreslujeme je do vrstev.
4. Dokreslíme zpět hrany (neorientované) mezi uzly.

Algoritmus ukážeme na uspořádané množině $(\{\emptyset, \{1\}, \{2\}, \{1,2\} \subseteq)$ z příkladu 12.



Nakreslíme Hasseův diagram pro uspořádané množiny zmíněné na začátku tohoto od-
 dílu:

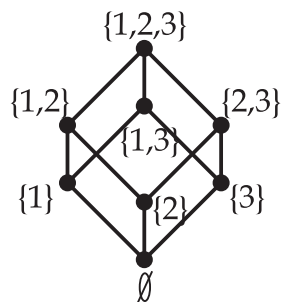
- $(\{1, 2, \dots, 10\}, \leq)$.



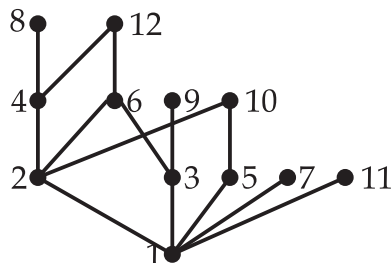
- (\mathbb{N}, \leq) .



- $(P(X), \subseteq)$, kde množina $X = \{1, 2, 3\}$.



- $(\{1, 2, \dots, 12\}, |)$.



1.4 Supremum a infimum

V minulém oddílu jsme zavedli pojem uspořádaní a uspořádané množiny. Protože nyní budeme chtít definovat další obecné pojmy a hledat mezi nimi souvislosti, bude potřeba obecně pracovat s uspořádanými množinami včetně obecné symboliky. Relaci uspořádání budeme obecně značit symbolem \preceq (a budeme ho číst „je menší nejvýše rovno“) a budeme si pod ním představovat libovolnou relaci uspořádání jakou je např. \leq , \subseteq , $|$. Podobně bude vhodné zavést obecný symbol \succeq , který bude symbolizovat opačné uspořádání pro nás známé jako \geq , \supseteq , je dělitelné. Od tohoto okamžiku musíme symboly \preceq a \leq od sebe striktně rozlišovat. Určitě platí, že číslo $3 \leq 4$, pokud \leq chápeme jako symbol pro porovnávání velikosti dvou čísel. Obecně neplatí, že $3 \preceq 4$, pokud by například symbol \preceq naznačoval operaci $|$.

Definice 10. Mějme uspořádanou množinu (X, \preceq) . Řekneme, že prvek $a \in X$ je

- **nejmenší**, jestliže pro každý prvek $b \in X$ platí $b \succeq a$.
- **největší**, jestliže pro každý prvek $b \in X$ platí $b \preceq a$.

Poznámka 1. Všimněme si, že nejmenší prvek musí být v Hasseově diagramu umístěn v nejnižší vrstvě a největší prvek ve vrstvě nejvyšší. Jde pouze o nutnou podmínku nikoli postačující.

Poznámka 2. Pro určení nejmenšího nebo největšího prvku můžeme také využít matematického předpisu a znalosti příslušných matematických operací. Uspořádaná množina $(N, |)$ má nejmenší prvek 1, neboť víme, že jedna dělí libovolné přirozené číslo. Stejně tak můžeme říct, že v uspořádané množině $(P(X), \subseteq)$ je největší prvek množina X , neboť libovolná množina $A \in P(X)$ je podmnožinou X .

Příklad 14. Uspořádaná množina $(\{1, 2, 3, 4, 5, 6\}, \leq)$ má za nejmenší prvek číslo 1 a za největší prvek číslo 6.

Příklad 15. Uspořádaná množina (\mathbb{Z}, \leq) nemá žádný nejmenší ani největší prvek (\mathbb{Z} je množina všech celých čísel).

Příklad 16. Uspořádaná množina $(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, |)$ má za nejmenší prvek číslo 1 a žádný největší prvek nemá, protože množina neobsahuje číslo, které by bylo dělitelné všemi zbylými čísly.

Příklad 17. Uspořádaná množina $(P(X), \subseteq)$ má za nejmenší prvek prázdnou množinu \emptyset a za největší prvek množinu X .

Všimněme si, že každá uspořádaná množina z příkladů má nejvýše jeden nejmenší a jeden největší prvek.

Věta 1. *Každá uspořádaná množina má nejvýše jeden nejmenší a nejvýše jeden největší prvek.*

Důkaz. Že tomu tak vždy bude, můžeme snadno nahlédnout přímo z definice nejmenšího a největšího prvku. Pokud by byly dva prvky a, b uspořádané množiny nejmenší, pak by muselo platit, že $a \preceq b$ a $b \preceq a$. Protože víme, že uspořádaní je antisymetrická relace, musí $a = b$. To znamená, že takový prvek je pouze jeden. \square

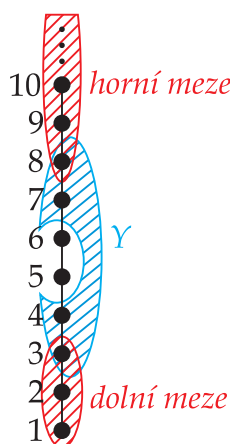
Definice 11. Mějme uspořádanou množinu (X, \preceq) . Zvolme libovolnou podmnožinu $Y \subseteq X$. Řekneme, že prvek $a \in X$ je

- *dolní mezí* množiny Y , jestliže pro každé $y \in Y$ platí $a \preceq y$.
- *horní mezí* množiny Y , jestliže pro každé $y \in Y$ platí $a \succeq y$.

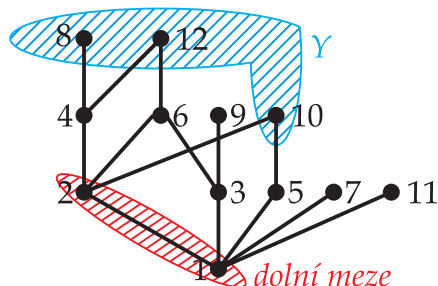
Poznámka. Dolní mezí podmnožiny Y je každý prvek, který je menší nebo roven než všechny prvky množiny Y .

Nejlépe se vše ukáže na konkrétních případech s využitím Hasseova diagramu.

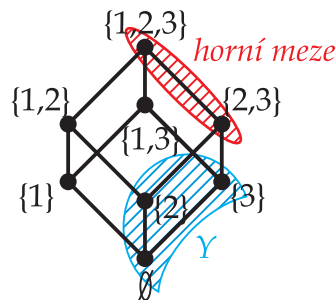
Příklad 18. Mějme uspořádanou množinu (\mathbb{N}, \leq) a její podmnožinu $Y = \{3, 4, 7, 8\}$. Potom dolní mezí množiny Y jsou prvky 1, 2, 3. Naopak horní mezí množiny Y jsou prvky 8, 9, 10...



Příklad 19. Mějme uspořádanou množinu $(\{1, 2, \dots, 12\}, |)$ a její podmnožinu $Y = \{8, 10, 12\}$. Potom dolní mezí množiny Y jsou prvky 1, 2.



Příklad 20. Mějme uspořádanou množinu $(P(\{1, 2, 3\}), \subseteq)$ a její podmnožinu $Y = \{\emptyset, \{2\}, \{3\}\}$. Potom horní mezí množiny Y jsou prvky $\{2, 3\}, \{1, 2, 3\}$.



Definice 12. Mějme uspořádanou množinu (X, \preceq) . Zvolme libovolnou podmnožinu $Y \subseteq X$. Řekneme, že prvek $a \in X$ je

- *infimem* podmnožiny Y , jestliže a je největší dolní mezí Y . Značíme $a = \inf(Y)$.
- *supremem* podmnožiny Y , jestliže a je nejmenší horní mezí Y . Značíme $a = \sup(Y)$.

Nejprve si uvědomíme, že infimum, respektive supremum, může mít každá podmnožina nejvýše jedno.

Věta 2. *Každá podmnožina uspořádané množiny má nejvýše jedno infimum a nejvýše jedno supremum.*

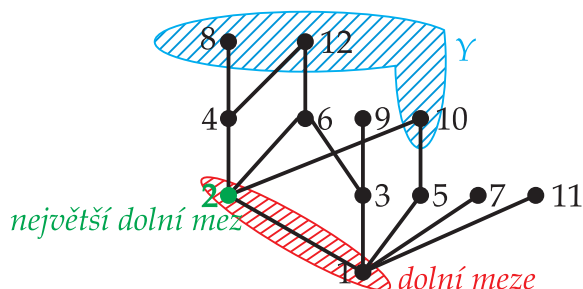
Důkaz. Zjistili jsme, že uspořádaná množina má nejvýše jeden největší, respektive nejmenší, prvek. Nyní si pouze uvědomíme, že množina všech dolních, respektive horních, mezí je také uspořádaná množina a může mít nejvýše jeden největší, respektive nejmenší, prvek. \square

Uvedeme již známé uspořádané množiny a určíme infima a suprema zvolených podmnožin. Vždy budeme hledat dolní, respektive horní, meze a vybírat z nich největší, respektive nejmenší, prvek, pokud bude existovat.

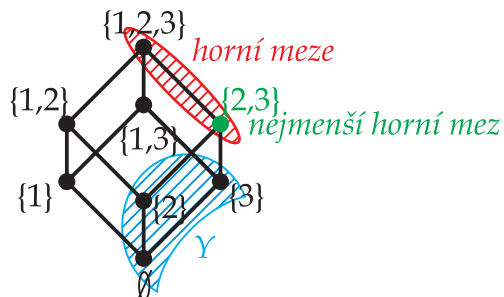
Příklad 21. Mějme uspořádanou množinu (\mathbb{N}, \leq) a její podmnožinu $Y = \{3, 4, 7, 8\}$. Zjistili jsme, že dolní mezí množiny Y jsou prvky 1, 2, 3. Nyní z nich vybereme ten největší. Tím je prvek 3: $\inf(Y) = 3$. Horní mezí množiny Y jsou prvky 8, 9, 10... Nyní z nich vybereme ten nejmenší. Tím je prvek 8: $\sup(Y) = 8$.



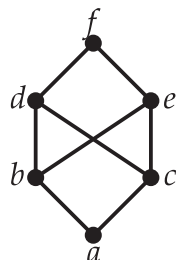
Příklad 22. Mějme uspořádanou množinu $(\{1, 2, \dots, 12\}, |)$ a podmnožinu $Y = \{8, 10, 12\}$. Dolní mezí množiny Y jsou prvky 1, 2. Nyní z nich vybereme ten největší: $\inf(Y) = 2$.



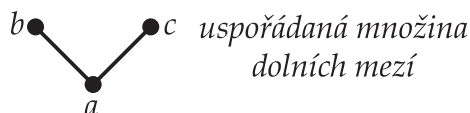
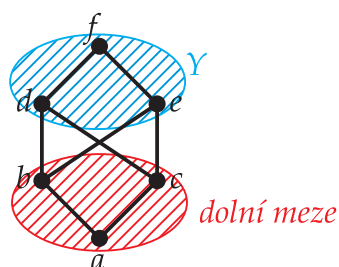
Příklad 23. Mějme uspořádanou množinu $(P(\{1, 2, 3\}), \subseteq)$ a její podmnožinu $Y = \{\emptyset, \{2\}, \{3\}\}$. Horní mezí množiny Y jsou prvky $\{2, 3\}, \{1, 2, 3\}$. Teď vybereme ten nejmenší: $\sup(Y) = \{2, 3\}$



Příklad 24. Následující Hasseův diagram reprezentuje uspořádanou množinu.



Pokusíme se najít infimum podmnožiny $Y = \{d, e, f\}$. Dolní mezí této podmnožiny jsou prvky a, b, c .



Žádná největší dolní mez neexistuje, proto $\inf(Y)$ neexistuje.

Věta 3. Mějme uspořádanou množinu (X, \preceq) a prvky $a, b \in X$.

- Jestliže $a \preceq b$, potom $\inf(a, b) = a$.
- Jestliže $a \preceq b$, potom $\sup(a, b) = b$.

Důkaz. Dokazujeme, že a je největší dolní mezí $\{a, b\}$.

1. $a \preceq b$ a zároveň $a \preceq a$, proto a je dolní mezí $\{a, b\}$.
2. Nechť existuje $c \in X$, které je dolní mezí $\{a, b\}$ a $a \preceq c$.
Pokud je c dolní mezí $\{a, b\}$, potom $c \preceq a$.
Z antisymetrie plyne, že $c = a$.

Stejným způsobem by se ukázala i druhá vlastnost. □

1.5 Svazy

V předchozím oddílu jsme na příkladech ukázali, že některé podmnožiny uspořádané množiny mají infimum a supremum a jiné je mít nemusí. Nyní se zaměříme pouze na uspořádané množiny, jejichž dvouprvkové podmnožiny budou mít supremum a infimum.

Definice 13. Řekneme, že uspořádaná množina (X, \preceq) je **svaz**, jestliže existuje supremum a infimum každé dvouprvkové podmnožiny množiny X .

Poznámka 1. Pro každou jednoprvkovou podmnožinu $Y = \{a\}$ uspořádané množiny (X, \preceq) platí, že $\inf(Y) = a$ a $\sup(Y) = a$, proto ve svazu existují suprema a infima i jednoprvkových podmnožin. Abychom nemuseli stále rozlišovat, zda se jedná o jednoprvkové či dvouprvkové podmnožiny, připustíme značení $\inf(\{a, b\})$ a $\sup(\{a, b\})$ i pro případ, že $a = b$. Zápis $\inf(\{a, b\})$, respektive $\sup(\{a, b\})$, budeme od teď zjednodušeně značit $\inf(a, b)$, respektive $\sup(a, b)$.

Poznámka 2. V uspořádané množině (X, \preceq) platí, že pro každé dva prvky $a, b \in X$ $\inf(a, b)$ a $\sup(a, b)$ opět prvek z množiny X . Hledání suprema a infima jsou tedy binární operace na množině X . Pro tyto binární operace se někdy používají symboly \sqcap (čtème průsek) a \sqcup (čtème spojení), kde $a \sqcap b = \inf(a, b)$ a $a \sqcup b = \sup(a, b)$. S výhodou budeme tyto operace používat při vyslovování vět a definic.

Nyní začneme ověřovat, které uspořádané množiny jsou svazy a které ne. Prvním možným způsobem je využití Hasseova diagramu. Tento způsob lze dobře použít při zjišťování, zda některá uspořádaná množina není svaz. Stačí nám najít pouze jednu dvojici, pro kterou nebude existovat supremum nebo infimum.

Příklad 25. Uspořádaná množina reprezentovaná Hasseovým diagramem z příkladu 24 není svazem, neboť pro dvojici prvků d, c neexistuje infimum.

Příklad 26. Uspořádaná množina $(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, |)$ není svazem, neboť neexistuje supremum pro dvojici čísel 11, 12.

Na známých uspořádaných množinách, kterými jsme se již zabývali, budeme konkretizovat operace \sqcap a \sqcup . Pokud ukážeme, že jsou tyto operace jednoznačně určené pro každé dva prvky, budeme moci říci, že se jedná o svaz.

1 Uspořádaná množina $(P(X), \subseteq)$ je svaz.

2 Uspořádaná množina (\mathbb{N}, \leq) je svaz.

3 Uspořádaná množina $(\mathbb{N}, |)$ je svaz.

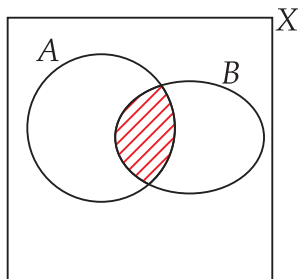
1 Uspořádaná množina $(P(X), \subseteq)$: $A \sqcap B$ budeme konkretizovat jako $A \cap B$ a $A \sqcup B$ budeme konkretizovat jako $A \cup B$. Ukážeme, že pro každé $A, B \in P(X)$ je

$$A \cap B = \inf(A, B).$$

1. $A \cap B$ je dolní mezí $\{A, B\}$:

Musíme ukázat, že $A \cap B \subseteq A$ a $A \cap B \subseteq B$

To je patrné přímo z Vennova diagramu:



2. $A \cap B$ je nejmenší dolní mez $\{A, B\}$:

Předpokládejme, že existuje větší prvek než $A \cap B$ (označme ho C) a ukážeme, že je to ve sporu s tím, že by C bylo dolní mezí.

Neboť $C \supset A \cap B$ ($C \neq A \cap B$), musí existovat prvek $c \in C$ takový, že $c \notin A$ nebo $c \notin B$.

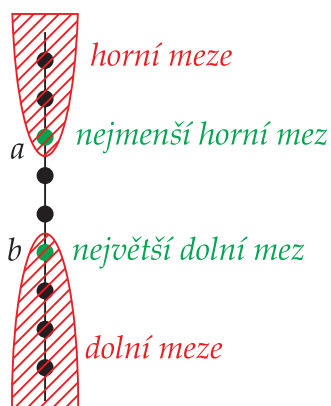
Potom ale buď $C \not\subseteq A$ nebo $C \not\subseteq B$.

Proto C není dolní mezí $\{A, B\}$. Tedy žádná taková dolní mez $C \supset A \cap B$ neexistuje.

Podobně by se ukázalo, že pro každé $A, B \in P(X)$ je $A \cup B = \sup(A, B)$.

2 Uspořádaná množina (\mathbb{N}, \leq) : $a \sqcap b$ budeme konkretizovat jako $\min(a, b)$ a $a \sqcup b$ budeme konkretizovat jako $\max(a, b)$.

Ukážeme, že jde o svaz pomocí Hasseova diagramu. Nejprve budeme předpokládat, že $a > b$.



Z obrázku vidíme, že $\sup(a, b) = a = \max(a, b)$ a $\inf(a, b) = b = \min(a, b)$.

Pro úplnost bychom ještě měli ověřit situaci $a < b$ a $a = b$, která by se ukázala podobně.

3 Uspořádaná množina $(\mathbb{N}, |)$: $a \sqcap b$ budeme konkretizovat jako $NSD(a, b)$ a $a \sqcup b$ budeme konkretizovat jako $NSN(a, b)$, kde symbol $NSD(a, b)$ značí největšího společného dělitele čísel a, b a symbol $NSN(a, b)$ značí nejmenší společný násobek čísel a, b . Zde využijeme tzv. základní větu aritmetiky, která říká, že každé přirozené číslo lze jednoznačně rozložit na součin prvočísel. Nyní tuto větu aplikujeme na čísla $a, b, NSD(a, b), NSN(a, b)$: $NSD(a, b)$ rozložíme na součin prvočísel.

$$NSD(a, b) = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

Čísla a, b také tento součin obsahují, protože $NSD(a, b) | a$ a $NSD(a, b) | b$:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_l$$

$$b = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot r_1 \cdot r_2 \cdot \dots \cdot r_m$$

Navíc čísla $q_i \neq r_j$ pro $i = 1, \dots, l$ a $j = 1, \dots, m$, jinak by totiž $NSD(a, b)$ nebyl největší společný dělitel čísel a, b .

Číslo $NSN(a, b)$ obsahuje všechna prvočísla, která obsahují a i b , protože $a | NSN(a, b)$ a $b | NSN(a, b)$ a žádné další prvočíslu, jinak by to nebyl nejmenší společný násobek:

$$NSN(a, b) = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_l \cdot r_1 \cdot r_2 \cdot \dots \cdot r_m$$

Nyní už jen ověříme, že

1. $NSD(a, b)$ je největší dolní mez:

$NSD(a, b) | a$ a $NSD(a, b) | b$, proto je $NSD(a, b)$ dolní mez.

Díky jednoznačnosti rozkladů čísel a, b víme, že každé číslo, které obě dvě dělí (a je tedy dolní mezí) nemůže v součinu obsahovat jiná prvočísla než p_1, \dots, p_k . Proto žádná větší dolní mez než číslo $NSD(a, b)$ neexistuje.

2. $NSN(a, b)$ je nejmenší horní mez:

$a | NSN(a, b)$ a $b | NSN(a, b)$, proto $NSN(a, b)$ je horní mez.

Díky jednoznačnosti rozkladů čísel a, b víme, že každé číslo, které je těmito dvěma čísly děleno (a je tedy horní mezí), musí v součinu obsahovat všechna prvočísla $p_1, \dots, p_k, q_1, \dots, q_l, r_1, \dots, r_m$. Proto žádná menší dolní mez než číslo $NSN(a, b)$ neexistuje.

Nyní ještě ukážeme důležité vlastnosti operací \sqcap, \sqcup .

Věta 4. *Nechť uspořádaná množina (X, \preceq) je svaz.*

- *Operace \sqcap je komutativní. Pro každé $a, b \in X$ platí $a \sqcap b = b \sqcap a$.*
- *Operace \sqcup je komutativní. Pro každé $a, b \in X$ platí $a \sqcup b = b \sqcup a$.*

Důkaz. Že tomu tak skutečně je, můžeme snadno zjistit z definice operace \sqcap .

$$a \sqcap b = \inf(a, b) = \inf(\{a, b\}) = \inf(\{b, a\}) = \inf(b, a) = b \sqcap a$$

Stejným způsobem by se ukázalo, že také operace \sqcup je komutativní. □

Věta 5. *Nechť uspořádaná množina (X, \preceq) je svaz.*

- Pro operaci \sqcap platí zákon idempotence. Pro každé $a \in X$ platí $a \sqcap a = a$.
- Pro operaci \sqcup platí zákon idempotence. Pro každé $a \in X$ platí $a \sqcup a = a$.

Důkaz. Že tomu tak skutečně je, můžeme opět nahlédnout z definice operace \sqcap .

$$a \sqcap a = \inf(a, a) = \inf(\{a, a\}) = \inf(\{a\}) = a$$

Stejným způsobem by se ukázalo, že také pro operaci \sqcup platí zákon idempotence. \square

Věta 6. *Nechť uspořádaná množina (X, \preceq) je svaz. Pro operace \sqcap a \sqcup platí zákon absorpce.*

- Pro každé $a, b \in X$ platí $a \sqcup (a \sqcap b) = a$.
- Pro každé $a, b \in X$ platí $a \sqcap (a \sqcup b) = a$.

Důkaz. Dokážeme, že $a \sqcup (a \sqcap b) = a$.

Nejprve si uvědomíme, že $a \sqcap b = \inf(a, b) \preceq a$.

$$a \sqcup (a \sqcap b) = \sup(a, (a \sqcap b)) = a \quad [\text{dle věty 3 neboť } (a \sqcap b) \preceq a]$$

Stejným způsobem by se ukázalo, že také pro operaci \sqcup platí zákon absorpce. \square

Věta 7. *Nechť uspořádaná množina (X, \preceq) je svaz.*

- Operace \sqcap je asociativní. Pro každé $a, b, c \in X$ platí $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$.
- Operace \sqcup je asociativní. Pro každé $a, b, c \in X$ platí $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$.

Důkaz. Musíme dokázat, že $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$, čili $\inf(\inf(a, b), c) = \inf(a, \inf(b, c))$. Vyslovíme ještě dvě pomocná tvrzení, která budeme využívat:

1. $\inf(a, b) \preceq a$
Zřejmě to platí, neboť $\inf(a, b)$ je dolní mezí a .
2. Jestliže $x \preceq a$ a zároveň $x \preceq b$, potom $x \preceq \inf(a, b)$
Prvek x je dolní mezí $\{a, b\}$ a $\inf(a, b)$ je největší dolní mezí $\{a, b\}$, proto musí $x \preceq \inf(a, b)$.

Pomocí těchto tvrzení a příslušných nerovností dokážeme tuto větu:

$$\inf(\inf(a, b), c) \preceq \inf(a, b) \preceq a \text{ [podle 1. tvrzení]} \quad (1.1)$$

$$\inf(\inf(a, b), c) \preceq \inf(a, b) \preceq b \text{ [podle 1. tvrzení]} \quad (1.2)$$

$$\inf(\inf(a, b), c) \preceq c \text{ [podle 1. tvrzení]} \quad (1.3)$$

$$\inf(\inf(a, b), c) \preceq \inf(b, c) \text{ [podle 2. tvrzení na 1.2, 1.3] } \quad (1.4)$$

$$\inf(\inf(a, b), c) \preceq \inf(a, \inf(b, c)) \text{ [podle 2. tvrzení na 1.11, 1.4] } \quad (1.5)$$

$$\inf(a, \inf(b, c)) \preceq \inf(b, c) \preceq b \text{ [podle 1. tvrzení]} \quad (1.6)$$

$$\inf(a, \inf(b, c)) \preceq \inf(b, c) \preceq c \text{ [podle 1. tvrzení]} \quad (1.7)$$

$$\inf(a, \inf(b, c)) \preceq a \text{ [podle 1. tvrzení]} \quad (1.8)$$

$$\inf(a, \inf(b, c)) \preceq \inf(a, b) \text{ [podle 2. tvrzení na 1.6, 1.8] } \quad (1.9)$$

$$\inf(a, \inf(b, c)) \preceq \inf(\inf(a, b), c) \text{ [podle 2. tvrzení na 1.7, 1.9] } \quad (1.10)$$

$$\inf(a, \inf(b, c)) = \inf(\inf(a, b), c) \text{ [podle antisymetrie na 1.5, 1.10]}$$

□

1.6 Distributivní svazy, Booleova algebra

Nyní přidáme další požadavky na svazy a vytvoříme tak vhodnou matematickou strukturu, se kterou budeme dále pracovat.

Definice 14. Nechť (X, \preceq) je svaz. Jestliže pro každé $a, b, c \in X$ platí

$$a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c),$$

potom řekneme, že (X, \preceq) je **distributivní svaz**.

Věta 8. Nechť (X, \preceq) je svaz. Tento svaz je distributivní právě tehdy, když

$$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c).$$

Důkaz. Musíme dokázat dvě implikace.

$$1. \ a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c) \Rightarrow a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$$

$$\begin{aligned} a \sqcup (b \sqcap c) &= \\ &= [a \sqcup (a \sqcap c)] \sqcup (b \sqcap c) = \text{[absorbce: } a \sqcup (a \sqcap c) = a \text{]} \\ &= a \sqcup [(a \sqcap c) \sqcup (b \sqcap c)] = \text{[asociativnost]} \\ &= a \sqcup [(a \sqcup b) \sqcap c] = \text{[distributivnost]} \\ &= [(a \sqcup b) \sqcap a] \sqcup [(a \sqcup b) \sqcap c] = \text{[absorbce: } (a \sqcup b) \sqcap a = a \text{]} \\ &= (a \sqcup b) \sqcap (a \sqcup c) \quad \text{[distributivnost]} \end{aligned}$$

$$2. a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c) \Rightarrow a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$$

Totéž by se dokázalo použitím pravidel s opačnými operacemi.

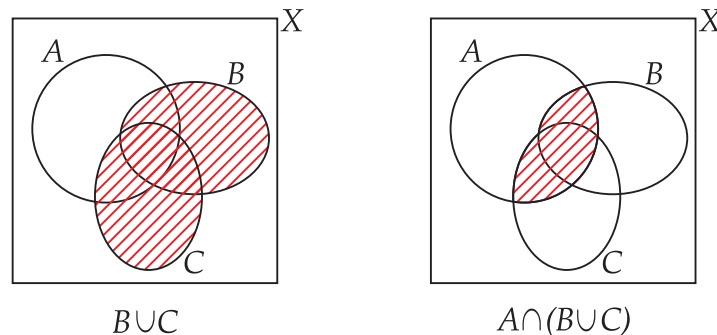
□

1 $(P(X), \subseteq)$ je distributivní svaz.

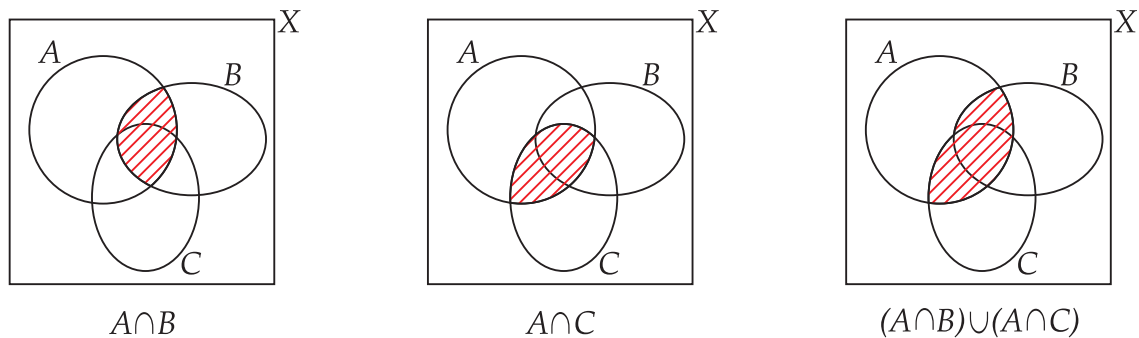
2 (\mathbb{N}, \leq) je distributivní svaz.

3 $(\mathbb{N}, |)$ je distributivní svaz.

1 Ukážeme, že pro všechna $A, B, C \in P(X)$ platí $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Využijeme Vennův diagram pro množiny A, B, C . Zakreslíme obraz množiny $A \cap (B \cup C)$:



Nyní nakreslíme obraz množiny $(A \cap B) \cup (A \cap C)$:



Z obrázků je vidět, že obě množiny jsou stejné.

2 Ukážeme, že pro každé $a, b, c \in \mathbb{N}$ platí $\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$. Uvažujme například, že $a \leq b \leq c$. Potom:
 $\min(a, \max(b, c)) = \min(a, c) = a$.
 $\max(\min(a, b), \min(a, c)) = \max(a, a) = a$.

Tím je důkaz hotov pro situaci $a \leq b \leq c$.

Ještě musíme probrat ostatní možnosti. K tomu využijeme tabulku:

	$\max(b, c)$	$\min(a, \max(b, c))$	$\min(a, b)$	$\min(a, c)$	$\max(\min(a, b), \min(a, c))$
$a \leq b \leq c$	c	a	a	a	a
$a \leq c \leq b$	b	a	a	a	a
$b \leq a \leq c$	c	a	b	a	a
$b \leq c \leq a$	c	c	b	c	c
$c \leq a \leq b$	b	a	a	c	a
$c \leq b \leq a$	b	b	b	c	b

Když porovnáme třetí a šestý sloupec tabulky, zjistíme, že jsou stejné. Protože jiné možnosti nastat nemohou, dokázali jsme, že $\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$.

3 Ukážeme, že pro každé $a, b, c \in \mathbb{N}$ platí $NSD(a, NSN(b, c)) = NSN(NSD(a, b), NSD(a, c))$. Opět čísla a, b, c vhodně rozložíme na součin prvočísel:

$$a = p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j \cdot r_1 \cdot \dots \cdot r_k \cdot s_1 \cdot \dots \cdot s_l,$$

$$b = p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j \cdot t_1 \cdot \dots \cdot t_m \cdot u_1 \cdot \dots \cdot u_n,$$

$$c = p_1 \cdot \dots \cdot p_i \cdot r_1 \cdot \dots \cdot r_k \cdot t_1 \cdot \dots \cdot t_m \cdot v_1 \cdot \dots \cdot v_o,$$

Slovičkem vhodně myslíme, že všechna společná prvočísla čísel a, b, c jsou obsažena v součinu $p_1 \cdot \dots \cdot p_i$, zbylá společná prvočísla čísel a, b v součinu $q_1 \cdot \dots \cdot q_j$ atd. Potom:

$$NSD(a, NSN(b, c)) = NSD(a, p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j \cdot t_1 \cdot \dots \cdot t_m \cdot u_1 \cdot \dots \cdot u_n \cdot r_1 \cdot \dots \cdot r_k \cdot v_1 \cdot \dots \cdot v_o) =$$

$$= p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j \cdot r_1 \cdot \dots \cdot r_k$$

$$NSN(NSD(a, b), NSD(a, c)) = NSN(p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j, p_1 \cdot \dots \cdot p_i \cdot r_1 \cdot \dots \cdot r_k) =$$

$$= p_1 \cdot \dots \cdot p_i \cdot q_1 \cdot \dots \cdot q_j \cdot r_1 \cdot \dots \cdot r_k$$

Jak vidíme, $NSD(a, NSN(b, c)) = NSN(NSD(a, b), NSD(a, c))$.

Definice 15. Nechť (X, \preceq) je svaz.

- Jestliže existuje $\bar{0} \in X$ tak, že pro každé $a \in X$ platí $\bar{0} \preceq a$, potom řekneme, že (X, \preceq) je **svaz s nulovým prvkem** $\bar{0}$.
- Jestliže existuje $\bar{1} \in X$ tak, že pro každé $a \in X$ platí $a \preceq \bar{1}$, potom řekneme, že (X, \preceq) je **svaz s jednotkovým prvkem** $\bar{1}$.

Poznámka 1. Nulovým prvkem rozumíme nejmenší prvek uspořádané množiny a jednotkovým prvkem rozumíme největší prvek uspořádané množiny, pokud tyto prvky existují.

Poznámka 2. Opět musíme rozlišovat mezi symboly $\bar{0}, \bar{1}$ a symboly $0, 1$. Může se například stát, že nulovým prvkem $\bar{0}$ může být 1 a naopak.

1 Svaz $(P(X), \subseteq)$ má za nulový prvek prázdnou množinu \emptyset a za jednotkový prvek množinu X .

2 Svaz (\mathbb{N}, \leq) má za nulový prvek číslo 1, ale nemá žádný jednotkový prvek. Pokud bychom chtěli, aby uspořádaná množina (X, \leq) byla svaz s jednotkovým prvkem, museli bychom množinu X shora omezit. Např. $(\{1, 2, \dots, 100\}, \leq)$ je svaz s nulovým a jednotkovým prvkem.

3 Svaz $(\mathbb{N}, |)$ má za nulový prvek číslo 1, ale nemá žádný jednotkový prvek. U uspořádané množiny $(X, |)$ nám již nepomůže, když množinu X pouze shora omezíme. Tím bychom totiž vyřadili NSN některých prvků, a naše množina by nebyla ani svaz. Vezměme ale množinu všech dělitelů čísla k , označme \mathbb{K} (pro $k = 12$, $\mathbb{K} = \{1, 2, 3, 4, 6, 12\}$). Nejmenším prvkem $(\mathbb{K}, |)$ je stále číslo 1 a největším prvkem je číslo k (to jsme zajistili definicí množiny \mathbb{K}). $(\mathbb{K}, |)$ je svaz s nulovým a jednotkovým prvkem.

Věta 9. *Nechť (X, \preceq) je svaz s nulovým prvkem $\bar{0}$ a jednotkovým prvkem $\bar{1}$. Pro $\bar{0}, \bar{1}$ platí zákon neutrality.*

- Pro každé $a \in X$ platí $a \sqcap \bar{1} = a$.
- Pro každé $a \in X$ platí $a \sqcup \bar{0} = a$.

Důkaz. Dokážeme, že $a \sqcap \bar{1} = a$.

$$a \sqcap \bar{1} = \inf(a, \bar{1}) = a \text{ [dle věty 3 neboť } a \preceq \bar{1} \text{]}$$

Stejným způsobem by se ukázalo, že $a \sqcup \bar{0} = a$. □

Věta 10. *Nechť (X, \preceq) je svaz s nulovým prvkem $\bar{0}$ a jednotkovým prvkem $\bar{1}$. Pro $\bar{0}, \bar{1}$ platí zákon agresivity.*

- Pro každé $a \in X$ platí $a \sqcup \bar{1} = \bar{1}$.
- Pro každé $a \in X$ platí $a \sqcap \bar{0} = \bar{0}$.

Důkaz. Dokážeme, že $a \sqcup \bar{1} = \bar{1}$.

$$a \sqcup \bar{1} = \sup(a, \bar{1}) = \bar{1} \text{ [dle věty 3 neboť } a \preceq \bar{1} \text{]}$$

Stejným způsobem by se ukázalo, že $a \sqcap \bar{0} = \bar{0}$. □

Definice 16. Nechť (X, \preceq) je svaz s nulovým a jednotkovým prvkem. Jestliže ke každému $a \in X$ existuje $a' \in X$ po němž platí $a \sqcap a' = \bar{0}$ a zároveň $a \sqcup a' = \bar{1}$, potom nazveme tento svaz **komplementárním svazem**.

Poznámka 3. Prvku a' se říká komplement prvku a .

Věta 11. *V distributivním komplementárním svazu je komplement každého prvku určen jednoznačně.*

Důkaz. Nechť existují dva komplementy prvku a , označme je a'_1, a'_2 .

Dle definice splňují: $a \sqcup a'_1 = \bar{1} = a \sqcup a'_2$, $a \sqcap a'_1 = \bar{0} = a \sqcap a'_2$.

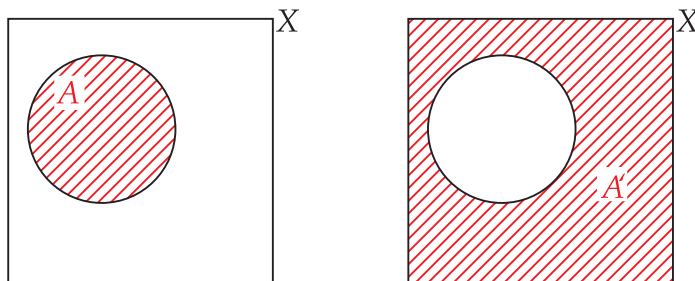
Ukážeme, že $a'_1 = a'_2$:

$$\begin{aligned}
 a'_1 &= a'_1 \sqcup \bar{0} && \text{[Podle věty 9]} \\
 &= a'_1 \sqcup (a \sqcap a'_2) && \text{[Dle předpokladu]} \\
 &= (a'_1 \sqcup a) \sqcap (a'_1 \sqcup a'_2) && \text{[Distributivnost]} \\
 &= (a'_2 \sqcup a) \sqcap (a'_1 \sqcup a'_2) && \text{[Dle předpokladu]} \\
 &= a'_2 \sqcup (a'_1 \sqcap a) && \text{[Distributivnost]} \\
 &= a'_2 \sqcup \bar{0} && \text{[Dle předpokladu]} \\
 &= a'_2 && \text{[Podle věty 9]}
 \end{aligned}$$

□

Rozhodneme, které ze známých příkladů jsou komplementární svazy.

1 Distributivní svaz $(P(X), \subseteq)$ s nulovým prvkem \emptyset a jednotkovým prvkem X . Pro libovolnou množinu $A \in P(X)$ definujeme její komplement jako doplněk množiny A značený A' . Nyní stačí ověřit, že $A \cap A' = \emptyset$ a $A \cup A' = X$. Což naznačuje Vennův diagram:



$(P(X), \subseteq)$ je komplementární svaz.

2 Svaz (\mathbb{N}, \leq) nemůže být komplementární, protože neexistuje jednotkový prvek tohoto svazu. Proto uvažujme nad svazem $(\{1, 2, \dots, 100\}, \leq)$, který má nulový a jednotkový prvek. Pokusíme se definovat např. komplement čísla 10 (označme ho symbolem $10'$), který musí splňovat: $\min(10, 10') = 1$ a $\max(10, 10') = 100$. Jak ale vidíme, z první rovnosti plyne, že $10' = 1$, ale dle druhé rovnosti $10' = 100$. Pro číslo 10 tedy komplement neexistuje. $(\{1, 2, \dots, 100\}, \leq)$ není komplementární svaz.

Pokusme se proto množinu X uspořádané množiny (X, \leq) ještě více omezit. Uvažujme pouze dvouprvkovou množinu $X = \{0, 1\}$ (z praktických důvodů jsme zvolili právě tato

dvě čísla, následující úvahy lze provést pro libovolnou dvouprvkovou množinu čísel). Víme, že $(\{0, 1\}, \leq)$ je distributivní svaz s nulovým a jednotkovým prvkem: $\bar{0} = 0$ a $\bar{1} = 1$. Zvolme $0' = 1$ a $1' = 0$. Potom:

$$0 \sqcup 0' = 0 \sqcup 1 = \max(0, 1) = 1 \text{ a zároveň } 0 \sqcap 0' = 0 \sqcap 1 = \min(0, 1) = 0.$$

$$1 \sqcup 1' = 1 \sqcup 0 = \max(1, 0) = 1 \text{ a zároveň } 1 \sqcap 1' = 1 \sqcap 0 = \min(1, 0) = 0.$$

Komplementy obou prvků splňují požadované vlastnosti, proto $(\{0, 1\}, \leq)$ je komplementární svaz.

3 Svaz $(\mathbb{N}, |)$ nemůže být komplementární, protože neexistuje jednotkový prvek tohoto svazu. Proto uvažujme nad svazem $(\mathbb{K}, |)$. Vezměme v úvahu množinu $\mathbb{K} = \{1, 2, 3, 4, 6, 12\}$ všech dělitelů čísla $k = 12$. Pokusíme se najít komplement prvku 6, který musí splňovat $NSD(6, 6') = 1$ a $NSN(6, 6') = 12$. Pokud $NSD(6, 6') = 1$, potom $6' = 1$. Pokud $NSN(6, 6') = 12$, potom $6' = 4$ nebo $6' = 12$. Komplement prvku 6 tedy neexistuje, proto svaz $(\{1, 2, 3, 4, 6, 12\}, |)$ není komplementární.

Uvažujme nyní nad svazem $(\mathbb{K}, |)$ pro číslo k , které v prvočíselném rozkladu neobsahuje žádné prvočíslo vícekrát než jednou (vhodné číslo k je např. číslo $30 = 2 \cdot 3 \cdot 5$ a nevhodné je číslo $12 = 2 \cdot 2 \cdot 3$, protože číslo 2 je v prvočíselném rozkladu dvakrát). Prvek l' prvku $l \in \mathbb{K}$ definujeme jako $l' = \frac{k}{l}$. Ukážeme, že se jedná o komplement. Rozložme čísla na součin prvočísel:

$$l = a_1 \cdot a_2 \cdot \dots \cdot a_m$$

$$k = a_1 \cdot a_2 \cdot \dots \cdot a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n$$

$$l' = \frac{k}{l} = a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n$$

Přičemž víme, že $a_i \neq a_j$ pro všechna $i \neq j$.

$$NSD(l, l') = NSD(a_1 \cdot a_2 \cdot \dots \cdot a_m, a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n) = 1.$$

$$NSN(l, l') = NSN(a_1 \cdot a_2 \cdot \dots \cdot a_m, a_{m+1} \cdot a_{m+2} \cdot \dots \cdot a_n) = k.$$

Komplement l' splňuje požadované vlastnosti, proto $(\mathbb{K}, |)$ pro číslo k , které v prvočíselném rozkladu neobsahuje žádné prvočíslo vícekrát než jednou, je komplementární svaz.

Definice 17. Distributivní komplementární svaz nazveme **Booleovým svazem** či **Booleovou algebrou**.

Podívejme se opět na naše známé uspořádané množiny a pokusme se o nich říci, zda jsou Booleovou algebrou či nikoli.

1 $(P(X), \subseteq)$ je Booleovou algebrou.

2 $(\{0, 1\}, \leq)$ je Booleovou algebrou.

3 $(\mathbb{K}, |)$ pro číslo k , které v prvočíselném rozkladu neobsahuje žádné prvočíslo vícekrát než jednou, je Booleovou algebrou.

1.7 Vlastnosti Booleovy algebry

Zatím jsme většinu vět psali vždy ve dvou zněních. První pro operaci \sqcap a druhou pro operaci \sqcup . Všimněme si, že z prvního znění věty dostaneme druhé záměnou operace \sqcup za operaci \sqcap a obráceně a záměnou symbolu $\bar{0}$ za $\bar{1}$ a obráceně. Stejnou záměnu můžeme provést i u definice distributivního svazu a komplementárního svazu. (Platnost druhého distributivního zákona je ekvivalentní s definicí distributivního svazu a u definice komplementárního svazu se pouze změní pořadí požadavků na komplement.) Této možnosti záměny operací se říká **princip duality**. V Booleově algebře tedy platí princip duality. Znamená to, že pokud platí nějaká věta v Booleově algebře, platí zde i duální věta, neboť v důkazu duální věty by stačilo zaměnit jednotlivé kroky za kroky duální. Duální větu získáme touto záměnou:

- $\sqcup \mapsto \sqcap$
- $\sqcap \mapsto \sqcup$
- $\bar{0} \mapsto \bar{1}$
- $\bar{1} \mapsto \bar{0}$

Odvodíme několik dalších vlastností Booleovy algebry. Duální větu vždy vyslovíme, ale již se nebudeme zabývat jejím důkazem.

Věta 12. *Nechť (X, \preceq) je Booleova algebra. Potom platí:*

- $\bar{1}' = \bar{0}$.
- $\bar{0}' = \bar{1}$.

Důkaz. Víme, že $\bar{1}' \preceq \bar{1}$, proto dle věty 3 je $\bar{1} \sqcap \bar{1}' = \inf(\bar{1}, \bar{1}') = \bar{1}'$.

Z definice komplementu je $\bar{1} \sqcap \bar{1}' = \bar{0}$. Z pravých stran rovnic dostáváme $\bar{1}' = \bar{0}$. \square

Věta 13. *Nechť (X, \preceq) je Booleova algebra. Pro každé $a \in X$ platí $(a')' = a$.*

Důkaz. Musíme ukázat, že komplement prvku a' je a . Aby byl a komplement prvku a' , musí splňovat:

$$a' \sqcup a = \bar{1} \text{ a zároveň } a' \sqcap a = \bar{0}$$

Protože víme, že operace \sqcup, \sqcap jsou komutativní, je tento požadavek ekvivalentní s:

$$a \sqcup a' = \bar{1} \text{ a zároveň } a \sqcap a' = \bar{0}$$

což je splněno, neboť Booleova algebra je komplementární svaz. a je tedy komplement prvku a' . \square

Věta 14. *Nechť (X, \preceq) je Booleova algebra. Pro operace \sqcap, \sqcup platí de Morganovy zákony.*

- *Pro každé $a, b \in X$ platí $(a \sqcup b)' = a' \sqcap b'$.*
- *Pro každé $a, b \in X$ platí $(a \sqcap b)' = a' \sqcup b'$.*

Důkaz. Aby byl prvek $a' \sqcap b'$ komplementem prvku $(a \sqcup b)$, musí splňovat:

$$(a \sqcup b) \sqcup (a' \sqcap b') = \bar{1} \text{ a zároveň } (a \sqcup b) \sqcap (a' \sqcap b') = \bar{0}$$

$$1. (a \sqcup b) \sqcup (a' \sqcap b') = \bar{1}$$

$$\begin{aligned} (a \sqcup b) \sqcup (a' \sqcap b') &= \\ &= [(a \sqcup b) \sqcup a'] \sqcap [(a \sqcup b) \sqcup b'] = \text{ [distributivnost]} \\ &= [(a \sqcup a') \sqcup b] \sqcap [(b \sqcup b') \sqcup a] = \text{ [asociativnost]} \\ &= [\bar{1} \sqcup b] \sqcap [\bar{1} \sqcup a] = \text{ [definice komplementu]} \\ &= \bar{1} \sqcap \bar{1} = \bar{1} \text{ [věta 10]} \end{aligned}$$

$$2. (a \sqcup b) \sqcap (a' \sqcap b') = \bar{0}$$

$$\begin{aligned} (a \sqcup b) \sqcap (a' \sqcap b') &= \\ &= [a \sqcap (a' \sqcap b')] \sqcup [b \sqcap (a' \sqcap b')] = \text{ [distributivnost]} \\ &= [(a \sqcap a') \sqcap b'] \sqcup [(b \sqcap b') \sqcap a'] = \text{ [asociativnost]} \\ &= [\bar{0} \sqcap b'] \sqcup [\bar{0} \sqcap a'] = \text{ [definice komplementu]} \\ &= \bar{0} \sqcup \bar{0} = \bar{0} \text{ [věta 10]} \end{aligned}$$

□

Věta 15. *Nechť (X, \preceq) je Booleova algebra. Pro operace \sqcap, \sqcup platí zákon absorpce negace.*

- *Pro každé $a, b \in X$ platí $a \sqcup (a' \sqcap b) = a \sqcup b$.*
- *Pro každé $a, b \in X$ platí $a \sqcap (a' \sqcup b) = a \sqcap b$.*

Důkaz.

$$\begin{aligned} a \sqcup (a' \sqcap b) &= \\ &= (a \sqcup a') \sqcap (a \sqcup b) = \text{ [distributivnost]} \\ &= \bar{1} \sqcap (a \sqcup b) = \text{ [definice komplementu]} \\ &= a \sqcup b \quad \text{ [věta 9]} \end{aligned}$$

□

Přidáme několik pravidel, které v budoucnu využijeme při řešení rovnic v Booleově algebře. Následující věty bychom mohli nazvat "ekvivalentní úpravy rovnic v Booleově algebře".

Věta 16. *Nechť (X, \preceq) je Booleova algebra.*

- *Pro každé $a, b \in X$ platí $a \sqcup b = \bar{0}$ právě tehdy, když $a = \bar{0}$ a zároveň $b = \bar{0}$.*
- *Pro každé $a, b \in X$ platí $a \sqcap b = \bar{1}$ právě tehdy, když $a = \bar{1}$ a zároveň $b = \bar{1}$.*

Důkaz. Dokážeme postupně obě implikace.

1. $a \sqcup b = \bar{0} \Rightarrow a = \bar{0}$ a zároveň $b = \bar{0}$. Ukážeme, že $a = \bar{0}$ (druhá rovnost $b = \bar{0}$ by se ukázala stejně).

$$\begin{aligned}
 a \sqcup b &= \bar{0} \\
 a \sqcap (a \sqcup b) &= \bar{0} && \text{[agresivita } \bar{0} \text{]} \\
 (a \sqcap a) \sqcup (a \sqcap b) &= \bar{0} && \text{[distributivnost]} \\
 a \sqcup (a \sqcap b) &= \bar{0} && \text{[idempotence]} \\
 a &= \bar{0} && \text{[absorpce]}
 \end{aligned}$$

2. $a = \bar{0}$ a zároveň $b = \bar{0} \Rightarrow a \sqcup b = \bar{0}$

$$\text{Dosadíme } a = \bar{0}, b = \bar{0} \text{ do rovnice } a \sqcup b: \bar{0} \sqcup \bar{0} = \bar{0}$$

□

Věta 17. *Nechť (X, \preceq) je Booleova algebra.*

- *Pro každé $a, b \in X$ platí $a = b$ právě tehdy, když $(a \sqcap b') \sqcup (a' \sqcap b) = \bar{0}$.*
- *Pro každé $a, b \in X$ platí $a = b$ právě tehdy, když $(a \sqcup b') \sqcap (a' \sqcup b) = \bar{1}$.*

Důkaz. Dokážeme postupně obě implikace.

1. $a = b \Rightarrow (a \sqcap b') \sqcup (a' \sqcap b) = \bar{0}$

$$(a \sqcap b') \sqcup (a' \sqcap b) \stackrel{a=b}{\Rightarrow} (a \sqcap a') \sqcup (a' \sqcap a) = \bar{0} \sqcup \bar{0} = \bar{0}$$

$$2. (a \sqcap b') \sqcup (a' \sqcap b) = \bar{0} \Rightarrow a = b$$

$$(a \sqcap b') \sqcup (a' \sqcap b) = \bar{0}$$

právě tehdy, když

$$\begin{array}{lll} a \sqcap b' = \bar{0} & \text{a zároveň} & a' \sqcap b = \bar{0} \text{ [věta 16]} \\ (a \sqcap b') \sqcup b = b & \text{a zároveň} & (a' \sqcap b) \sqcup a = a \text{ [neutralita } \bar{0} \text{]} \\ a \sqcup b = b & \text{a zároveň} & b \sqcup a = a \text{ [věta 15] } \\ & & a = b \text{ [z předchozí rovnosti-pravé strany]} \end{array}$$

□

Věta 18. *Nechť (X, \preceq) je Booleova algebra.*

- *Pro každé $a, b \in X$ platí $a \preceq b$ právě tehdy, když $a \sqcap b' = 0$.*
- *Pro každé $a, b \in X$ platí $a \succeq b$ právě tehdy, když $a \sqcup b' = 1$.*

Důkaz. Dokážeme postupně obě implikace.

$$1. a \preceq b \Rightarrow a \sqcap b' = 0$$

Jestliže $a \preceq b$, potom $a \sqcap b = a$ a zároveň $a \sqcup b = b$.

$$\begin{aligned} a \sqcap b' &= \\ &= (a \sqcap b) \sqcap (a \sqcup b') && \text{[dosadíme za } a, b \text{]} \\ &= (a \sqcap b) \sqcap (a' \sqcap b') && \text{[de Morgan]} \\ &= (a \sqcap a') \sqcap (b \sqcap b') && \text{[asociativnost]} \\ &= \bar{0} \sqcap \bar{0} && = \bar{0} \text{ [definice komplementu]} \end{aligned}$$

$$2. a \sqcap b' = 0 \Rightarrow a \preceq b$$

Nechť $a \sqcap b' = 0$ a zároveň $a \succ b$.

Jestliže $a \succ b$, potom $a \sqcap b = b$ a zároveň $a \sqcup b = a$.

$$\begin{aligned} \bar{0} = a \sqcap b' &= \\ &= (a \sqcup b) \sqcap (a \sqcap b') && \text{[dosadíme za } a, b \text{]} \\ &= (a \sqcup b) \sqcap (a' \sqcup b') && \text{[de Morgan]} \\ &= [(a \sqcup b) \sqcap a'] \sqcup [(a \sqcup b) \sqcap b'] && \text{[distributivnost]} \\ &= [(a \sqcap a') \sqcup (b \sqcap a')] \sqcup [(a \sqcap b') \sqcup (b \sqcap b')] && \text{[distributivnost]} \\ &= [\bar{0} \sqcup (b \sqcap a')] \sqcup [\bar{0} \sqcup (a \sqcap b')] && \text{[definice komplementu]} \\ &= (b \sqcap a') \sqcup (a \sqcap b') && \text{[neutralita } \bar{0} \text{]} \end{aligned}$$

Poslední řádek rovnice se má rovnat $\bar{0}$. To je splněno právě tehdy, když $a = b$ [Věta 17], což je ale spor s předpokladem, že $a \succ b$.

Důkaz druhé části by se provedl obdobně.

□

1.8 Početní postupy

V tomto oddílu shrneme všechny dosavadní poznatky, které jsme se o Booleově algebře dozvěděli, a odvodíme další početní postupy a metody, které jsou obecně platné pro Booleovu algebru. V následující kapitole se na tyto vlastnosti budeme odvolávat při řešení příkladů. Všechna pravidla a vzorce zachytíme v přehledných tabulkách, čímž vytvoříme „početní kuchařku“, stejně jako tomu bylo v „klasické“ algebře, se kterou jsme se setkali na střední škole.

Nejprve zjednodušíme zápis operací \sqcup, \sqcap a od teď budeme používat symboly $+, \cdot$, které používáme v běžné matematice, a místo symbolů $\bar{0}, \bar{1}$ budeme používat číslice $0, 1$. Musíme si uvědomit, že se jedná o jiné operace (než v „klasické“ matematice), a smíme tudíž užívat pouze pravidla, která jsme odvodili v předchozích oddílech a nikoli ta pravidla, která známe z algebry (např. zápis $a + a \neq 2a$, ale $a + a = a$). Využijeme však některé konvence zápisu, na něž jsme zvyklí. V první řadě budeme brát v úvahu, že operace \cdot má přednost před operací $+$, a budeme vynechávat závorky, které již budou od tohoto okamžiku zbytečné (např. zápis $a + (b \cdot c)$ zredukujeme na $a + b \cdot c$). Dále budeme vynechávat symbol \cdot v součinu, stejně jako tomu bylo v algebře (např. zápis $a + b \cdot c$ zredukujeme na $a + bc$).

Nyní použijeme tento zápis a do tabulky napíšeme všechna pravidla (zákony), která jsme dosud poznali:

Zákon	Pravidlo	Duální pravidlo
Komutativní	$a + b = b + a$	$ab = ba$
Idempotence	$a + a = a$	$aa = a$
Absorbce	$a + ab = a$	$a(a + b) = a$
Asociativní	$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$
Distributivní	$a(b + c) = ab + ac$	$a + bc = (a + b)(a + c)$
Neutrality	$a + 0 = a$	$a \cdot 1 = a$
Agresivity	$a + 1 = 1$	$a \cdot 0 = 0$
	$a + a' = 1$	$aa' = 0$
	$1' = 0$	$0' = 1$
	$(a')' = a$	
de Morganův	$(a + b)' = a'b'$	$(ab)' = a' + b'$
Absorbce negace	$a + a'b = a + b$	$a(a' + b) = ab$
	$a + b = 0 \Leftrightarrow (a = 0) \wedge (b = 0)$	$ab = 1 \Leftrightarrow (a = 1) \wedge (b = 1)$
	$a = b \Leftrightarrow ab' + a'b = 0$	$a = b \Leftrightarrow (a + b')(a' + b) = 1$
	$a \leq b \Leftrightarrow ab' = 0$	$a \geq b \Leftrightarrow a + b' = 1$

Díky asociativnímu zákonu víme, že nezáleží na pořadí, ve kterém vyhodnocujeme stejné operace, a tudíž můžeme vynechávat příslušné závorky (např. zápis $a + (b + c)$ zredukujeme na $a + b + c$ stejně tak zápis $a(bc)$ na zápis abc).

Zjednodušování zápisů v Booleově algebře

V tabulce jsme shrnuli pravidla, která můžeme využívat při zjednodušování zápisů v Booleově algebře. Nyní ještě uvedeme zobecněná pravidla, která také můžeme využít, abychom se rychleji dostali k výsledku. Jde o algoritmus, který nám ze součtů a součinů mnohočlenů vyrobí součet jednočlenů. Všechna tato pravidla by se dokázala pomocí matematické indukce. Tato „redukční pravidla“ očíslovujeme, abychom na ně mohli dále v textu odkazovat (stejně jako můžeme odkazovat na věty a definice).

č.	Pravidlo
$R1$	$(a_1 + a_2 + \dots + a_i)(b_1 + b_2 + \dots + b_j) = a_1b_1 + a_1b_2 + \dots + a_1b_j + a_2b_1 + \dots + a_ib_j$
$R2(a)$	$\forall n \in \mathbb{N} : a^n = a$
$R2(b)$	$a + a + \dots + a = a$
$R2(c)$	$a_1a_2\dots a_ibb' + c = c$
$R2(d)$	$a_1a_2\dots a_i + a_1a_2\dots a_ib = a_1a_2\dots a_i$
$R2(e)$	$a_1a_2\dots a_ib + a_1a_2\dots a_ib' = a_1a_2\dots a_i$

Pravidlo $R1$ nám umožňuje roznásobovat mnohočleny na součet jednočlenů (stejně jako v „klasické“ algebře). Pravidla $R2$ nám radí, jak zredukovat výsledný součet jednočlenů.

- $R2(a)$ říká, že na rozdíl od „klasické“ algebry nebudeme u roznásobování mnohočlenů uvažovat mocniny.
- $R2(b)$ říká, že pokud je nějaký jednočlen stejný jako jiný, můžeme ho vynechat (ne-uvažujeme násobnost nějakého členu).
- $R2(c)$ říká, že pokud se v jednočlenu objeví proměnná i její negace, můžeme tento jednočlen vynechat.
- $R2(d)$ říká, že můžeme vypustit ten jednočlen, který v součinu obsahuje nějaký prvek navíc oproti jinému jednočlenu (naopak můžeme do rovnice přidat jednočlen, který obsahuje nějaký prvek navíc).
- $R2(e)$ říká, že můžeme vytýkat před závorku. Ve speciálním případě nám to umožní zredukovat dva jednočleny na jeden jednodušší jednočlen.

Rovnice o jedné neznámé

Díky pravidlu $R2(a)$ budou rovnice o jedné neznámé vždy lineární. Řešení takových rovnic je ale složitější než v „klasické“ algebře. Nemůžeme totiž k oběma stranám rovnice přičíst nějaký prvek, a ani nemůžeme obě strany rovnice vynásobit nějakým prvkem.

Uvažujme nyní obecnou lineární rovnici v Booleově algebře (X, \preceq) :

$$ax + bx' + c = dx + ex' + f$$

kde x je proměnná a $a, b, c, d, e, f \in X$.

$$\begin{aligned}
 ax + bx' + c &= dx + ex' + f \\
 (ax + bx' + c)(dx + ex' + f)' + (ax + bx' + c)'(dx + ex' + f) &= 0 \text{ [věta 17]} \\
 (ax + bx' + c)(d' + x')(e' + x)f' + (a' + x')(b' + x)c'(dx + ex' + f) &= 0 \text{ [de Morgan]} \\
 x \cdot A + x' \cdot B + C &= 0 \text{ [R1, R2]} \\
 \text{právě tehdy, když} & \\
 x \cdot A = 0 \text{ a zároveň } x' \cdot B = 0 \text{ a zároveň } C = 0 & \text{ [věta 17]}
 \end{aligned}$$

A, B, C jsou mnohočleny tvořené prvky a, b, c, d, e, f .

Z předchozích rovnic můžeme vyčíst následující výsledky:

- $C = 0$ je nutná podmínka pro existenci řešení této rovnice.
- $Bx' = 0$ dle věty 18 znamená, že: $B \preceq x$.
- $xA = 0$ znamená, že $A' \succeq x$.

Ještě ověříme poslední tvrzení:

$$\begin{aligned}
 xA &= 0 \\
 \text{právě tehdy, když} & \\
 (xA + 0)'[(xA)' + 0] &= 1 \text{ [věta 17]} \\
 (xA + 1)(x' + A' + 0) &= 1 \text{ [de Morgan]} \\
 1 \cdot (x' + A' + 0) &= 1 \text{ [agresivita 1]} \\
 x' + A' &= 1 \text{ [neutralita 0,1]} \\
 \text{právě tehdy, když} & \\
 A' &\succeq x \text{ [věta 18]}
 \end{aligned}$$

Tím jsme vyřešili obecnou lineární rovnici pro jednu neznámou.

Poznámka. Při zjednodušování zápisů a při řešení lineárních rovnic jsme mohli též využívat duální pravidla. Vznikly by nám algoritmy, které by také byly správné. Důvodem našeho postupu byla přirozená znalost prvního distributivního zákona, který běžně používáme v „klasické“ algebře.

Kapitola 2

Využití Booleovy algebry

2.1 Množinová algebra

V tomto oddílu se budeme věnovat aplikaci Booleovy algebry na množinách, respektive na potenční množině nějaké množiny. Názorně ukážeme aplikaci předchozí kapitoly na konkrétních příkladech a snadno ověříme správnost výsledku.

Nejprve si musíme ukázat, jak převedeme příklad z množinové algebry do Booleovy algebry. Množinová algebra využívá velká písmena pro množiny, se kterými provádí operace sjednocení \cup , průnik \cap a doplněk $'$, případně rozdíl $-$. Všechny tyto symboly budeme muset převést do Booleovy algebry. Dále pak využívá závorky (oddělovače mezi operacemi) a symbol $=$. Tyto symboly mají v Booleově algebře stejný význam jako v množinové algebře, takže je nebude nutné převádět.

Převod zápisu z množinové algebry do Booleovy algebry a zpět ukazuje následující tabulka pro množiny $A, B, C, X, Y \dots \subseteq M$.

Množinová algebra	Booleova algebra
$A, B, C \dots$	$a, b, c \dots$
$X, Y \dots$	$x, y \dots$
\emptyset	0
M	1
\cup	$+$
\cap	\cdot
$'$	$'$
$A - B$	ab'
\subseteq	\leq

Zjednodušování zápisu množin

Příklad 1. Zjednodušíme množinový zápis $[C \cap (A \cap C)'] \cup \{A \cup [B \cap (A \cap B)']\}$.

Převědeme do Booleovy algebry: $[c(ac)'] + \{a + [b(ab)']\}$.
Výraz zjednodušíme:

$$\begin{aligned}
 & [c(ac)'] + \{a + [b(ab)']\} = \\
 & = [c(a' + c')] + \{a + [b(a' + b')]\} = \\
 & = [ca' + cc'] + \{a + [ba' + bb']\} = \\
 & = [ca'] + \{a + ba'\} = \\
 & = ca' + a + ba' = \\
 & = ca' + ac + a + ba' + ab = \\
 & = c(a' + a) + a + b(a' + a) = \\
 & = c + a + b = a + b + c
 \end{aligned}$$

Převědeme výraz v Booleově algebře zpět do množinové algebry: $A \cup B \cup C$.

$$[C \cap (A \cap C)'] \cup \{A \cup [B \cap (A \cap B)']\} = A \cup B \cup C$$

Cvičení 1. Zjednodušte následující množinové zápisy:

- $[(A \cup B) \cap B] \cup [A \cap (A \cap B)]$
- $(C \cap A \cap B) \cup [A \cap (C' \cup B)']$
- $(C \cap B \cap A) \cup (C' \cap B \cap A) \cup [(B \cup A') \cap C']$
- $[(A \cup B)' \cup (B \cup C)] \cap (C \cup A)$
- $[(A \cup B')' \cap C] \cup (A \cap C \cap B') \cup (A' \cap C \cap B') \cup [(B' \cup A')' \cap C]$

Rovnost množin, nutná a postačující podmínka

Příklad 2. Uvažujme libovolné podmnožiny A, B, C dané neprázdné množiny M . Zjistíme, zda platí:

$$A \cup (B \cap C') = [(A \cup B) \cap (A \cup C)'] \cup (A \cap C')$$

Jestliže rovnost neplatí, určíme nutnou a postačující podmínku rovnosti.

Převědeme rovnost do Booleovy algebry: $a + (bc') = [(a + b)(a + c)'] + ac'$.

Výraz upravíme:

$$[(a + b)(a + c)'] + ac' = a + (bc')$$

$$(a + b)a'c' + ac' = a + bc'$$

$$aa'c' + ba'c' + ac' = a + bc'$$

$$ba'c' + ac' = a + bc'$$

$$c'(a'b + a) = a + bc'$$

$$c'(a + b) = a + bc'$$

$$c'a + c'b = a + bc'$$

právě tehdy, když

$$(a + bc')(c'a + c'b)' + (a + bc')'(c'a + c'b) = 0$$

$$(a + bc')(c + a')(c + b') + a'(b' + c)(c'a + c'b) = 0$$

$$(ac + bc'a')(c + b') + (a'b' + a'e)(c'a + c'b) = 0$$

$$ac + acb' = 0$$

$$ac = 0$$

Poslední řádek rovnosti dokazuje, že se původní množinové zápisy nerovnají. Poslední rovnost určuje nutnou a postačující podmínku. Po převodu do množinové algebry dostáváme podmínku $A \cap C = \emptyset$.

Cvičení 2. Nechť A, B, C, D jsou podmnožiny neprázdné množiny M . Rozhodněte, zda platí následující rovnosti. Pokud neplatí, určete nutnou a postačující podmínku.

- $A \cap (B \cup C)' = (A \cap B') \cap (A \cap C')$
- $(A \cup B) \cap (A \cup C)' = A \cup (B \cap C')$
- $(A \cap B) \cup (C \cap D) = (B \cap D) \cup (A \cap C)$
- $[(A \cup B) \cap D'] \cup (C \cup D) = M$
- $A \cup B \subseteq A \cup C$
- $(A \cup B)' \cap (A \cap B') \subseteq A \cup B$
- $A \cap (C' \cup B) \cap (B' \cup A) \subseteq (A' \cup B) \cap (C' \cup A)$
- $[(A \cup B) \cap (C \cup A)'] \cup (A \cap C') = (C' \cap B) \cup A$

Množinové rovnice

Příklad 3. Uvažujme množinu $M = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Vyřešíme množinovou rovnici s neznámou X v množině $P(M)$:

$$(X' \cup \{4, 6, 7, 8\}) \cap (X \cup \{1, 5, 8\}) = \{1, 8\}$$

Zavedeme označení těchto množin:

A	$\{4, 6, 7, 8\}$	A'	$\{1, 2, 3, 5\}$
B	$\{1, 5, 8\}$	B'	$\{2, 3, 4, 6, 7\}$
C	$\{1, 8\}$	C'	$\{2, 3, 4, 5, 6, 7\}$

Převédeme rovnici do Booleovy algebry:

$$(x' + a)(x + b) = c$$

Z rovnice vyjádříme neznámou x :

$$\begin{aligned} (x' + a)(x + b) &= c \\ bx' + ax + ab &= c \\ (bx' + ax + ab)c' + (bx' + ax + ab)c &= 0 \\ bc'x' + ac'x + abc' + (b' + x)(a' + x')(a' + b')c &= 0 \\ bc'x' + ac'x + abc' + (a'b' + b'x' + a'x)(a'c + b'c) &= 0 \\ bc'x' + ac'x + abc' + a'b'c + a'b'c + a'b'cx' + b'cx' + a'cx + a'b'cx &= 0 \\ x(ac' + a'c) + x'(bc' + b'c) + abc' + a'b'c &= 0 \\ \text{právě tehdy, když} \\ abc' + a'b'c = 0 &\wedge \\ ac' + b'c \leq x &\wedge \\ x \leq (ac' + a'c)' = (a' + c)(a + c') = a'c' + ac \end{aligned}$$

Z posledních tří řádků (a po převodu do množinové algebry) plyne:

- Nutná podmínka: $(A \cap B \cap C') \cup (A' \cap B' \cap C) = \emptyset$.
- $(B \cap C') \cup (B' \cap C) \subseteq X$
- $X \subseteq (A' \cap C') \cup (A \cap C)$

Po zpětném dosazení za A, B, C a výpočtu zjistíme, že nutná podmínka je splněna a pro množinu X vzniknou následující podmínky:

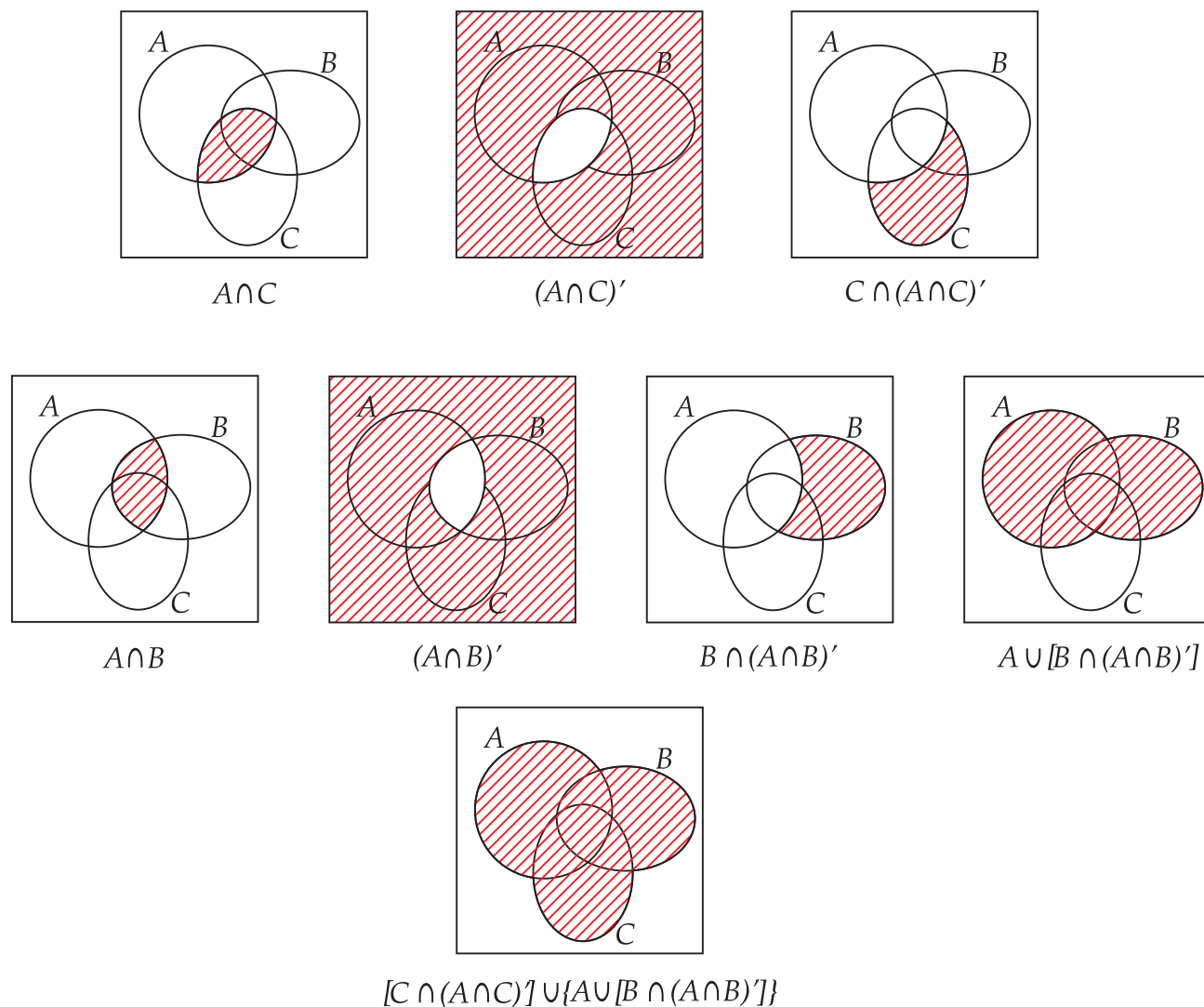
$$\{5\} \subseteq X \subseteq \{2, 5, 8\}$$

Cvičení 3. Řešte rovnice o neznámé X v množině $P(M)$, kde $M = \{1, 2, 3, 4, 5, 6, 7\}$

- $(X \cap \{4, 6, 7\}) \cup \{3, 5, 7\} = X$
- $(X' \cup \{1, 4, 5\}) \cap (X \cup \{2, 3\}) = \emptyset$
- $(X \cup \{1, 4, 5\}) \cap (X' \cup \{1, 2, 3\}) = \emptyset$
- $(\{2, 4, 7\} \cap X') \cup (X \cap \{1, 2, 5\}) = \{3, 4, 5, 6\}$

Vennovy diagramy Při řešení množinových úloh, které jsme zmínili výše, můžeme s výhodou využít Vennova diagramu.

Příklad 4. Vyřešíme příklad 1 za pomoci Vennových diagramů. Zjednodušíme množinový zápis $[C \cap (A \cap C)] \cup \{A \cup [B \cap (A \cap B)]\}$.



Vidíme, že zápis můžeme zjednodušit na $A \cup B \cup C$.

Cvičení 4. Řešte příklady z cvičení 1,2 za pomoci Vennových diagramů.

2.2 Algebra pravdivostních hodnot výroků

Tento oddíl se bude zabývat výrokovou logikou. Budeme zkoumat pravdivost výroků, které vzniknou z daných výroků pomocí logických spojek $\wedge, \vee, ', \Rightarrow, \Leftrightarrow$. Výroky budeme

značit velkými písmeny A, B, \dots . Jestliže je výrok A pravdivý, zapíšeme tuto skutečnost $A = 1$ a budeme číst: A má pravdivostní hodnotu 1. Jestliže je výrok A nepravdivý, zapíšeme tuto skutečnost $A = 0$ a budeme číst: A má pravdivostní hodnotu 0. Velká písmena z konce abecedy X, Y, \dots budeme využívat pro výrokové proměnné, které smějí nabývat hodnot 0,1.

Připomeneme si pravdivostní tabulky konjunkce, disjunkce, negace, implikace a ekvivalence:

X	Y	$X \wedge Y$	$X \vee Y$	Y'	$X \Rightarrow Y$	$X \Leftrightarrow Y$
0	0	0	0	1	1	1
0	1	0	1	0	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Nejprve se pokusíme zredukovat počet logických spojek. Omezíme se jen na $\wedge, \vee, '$ a zbylé dvě pomocí těchto spojek odvodíme:

- $X \Rightarrow Y$ právě tehdy, když $X' \vee Y$.
- $X \Leftrightarrow Y$ právě tehdy, když $(X' \vee Y) \wedge (Y' \vee X)$, neboli $(X \wedge Y) \vee (X' \wedge Y')$.

Abychom mohli využít kalkul vybudovaný v předchozí kapitole musíme ukázat, že se jedná o Booleovu algebru. Uvažujme množinu $X = \{0, 1\}$ jakožto množinu všech hodnot, kterých smí nabývat výrokové proměnné. Definujeme uspořádání \leq na X : $0 \leq 0, 0 \leq 1, 1 \leq 1$ (relace \leq je skutečně uspořádání, jedná se o reflexivní, tranzitivní a antisymetrickou relaci). Dostáváme tedy uspořádanou množinu $(\{0, 1\}, \leq)$, o které jsme se v minulé kapitole dozvěděli, že je to Booleova algebra. Po prozkoumání pravdivostních tabulek navíc zjistíme, že operace \vee odpovídá hledání maxima dvou prvků (odpovídá hledání suprema) a operace \wedge odpovídá hledání minima dvou prvků (odpovídá hledání infima).

Nyní můžeme Booleovu algebru aplikovat na algebru pravdivostních hodnot výroků. Následující tabulka uvádí převod mezi algebrou pravdivostních hodnot výroků a Booleovou algebrou.

Algebra pravdivostních hodnot výroků	Booleova algebra
A, B, \dots	a, b, \dots
X, Y, \dots	x, y, \dots
1	1
0	0
A'	a'
$A \wedge B$	ab
$A \vee B$	$a + b$
$A \Rightarrow B$	$a' + b$
$A \Leftrightarrow B$	$ab + a'b'$

Tautologie

Příklad 5. Ověříme, zda $(X \wedge Y) \Rightarrow (X \vee Y)$ je tautologie, tj. zda je o pravdivý výrok při všech možných hodnotách X, Y .

Musíme zjistit, zda $[(X \wedge Y) \Rightarrow (X \vee Y)] = 1$. Převédeme rovnost do Booleovy algebry a upravíme:

$$\begin{aligned}(X \wedge Y) \Rightarrow (X \vee Y) \\ (X \wedge Y)' \vee (X \vee Y) \\ (xy)' + (x + y) &= \\ = x' + y' + x + y &= \\ = 1 + 1 &= 1\end{aligned}$$

Můžeme prohlásit, že se jedná o tautologii.

Cvičení 5. Rozhodněte, zda v následujících případech jde o tautologie.

- $(X' \Rightarrow Y) \Leftrightarrow (X \wedge Y)'$
- $[(X \Rightarrow Z) \Rightarrow Y] \Leftrightarrow [(X \wedge Z) \Rightarrow Y]$
- $[X \Rightarrow (Y \vee Z)] \Leftrightarrow [(X \Rightarrow Y) \vee (X \Rightarrow Z)]$
- $[X \Rightarrow (Y \Rightarrow Z)] \Leftrightarrow [(X \wedge Y) \Rightarrow Z]$
- $[X \Rightarrow (Y \Leftrightarrow Z)] \Leftrightarrow [(X \Rightarrow Y) \Leftrightarrow (X \Rightarrow Z)]$

Ověřování správnosti úsudků

Mějme neprázdnou množinu výroků T_1, \dots, T_n , o kterých víme, že jsou všechny pravdivé, řekněme jim předpoklady. Chceme ověřit, zda z těchto předpokladů plyne závěr Z . Ověřujeme:

$$[(T_1 \wedge \dots \wedge T_n) \Rightarrow Z] = 1$$

Jednodušší je dokázat negovanou rovnost:

$$[(T_1 \wedge \dots \wedge T_n) \Rightarrow Z]' = 0$$

Levou stranu rovnosti ještě můžeme upravit dle pravidla pro negaci implikace ($A \Rightarrow B$ právě tehdy, když $A \wedge B'$):

$$(T_1 \wedge \dots \wedge T_n) \wedge Z' = 0$$

Po převodu do Booleovy algebry dostáváme:

$$t_1 \cdot \dots \cdot t_n z' = 0$$

Příklad 6. Víme, že platí výroky $A \wedge B$, $B \Rightarrow C$ a $(C' \vee B') \Rightarrow A'$. Chceme zjistit, zda odtud vyplývá, že

1. $A \vee C$
2. $A \Rightarrow B'$

Nejprve převedeme množinu předpokladů do Booleovy algebry a zjednodušíme výraz:

$$ab(b' + c)[(c' + b')' + a'] = abc[cb + a'] = abc$$

Nyní aplikujeme podmínku: $t_1 \cdot \dots \cdot t_n z' = 0$:

1. $abc(a + c)' = abc(a'c') = 0$ Z uvedených předpokladů skutečně plyne, že $A \vee C$.
2. $abc(a' + b')' = abc(ab) = abc \neq 0$ Z uvedených předpokladů neplyne, že $A \Rightarrow B'$.

Cvičení 6. Rozhodněte, zda z předpokladů $(A' \wedge B') \Rightarrow D'$, $(A \vee C) \Rightarrow B'$, $(A' \vee D') \Rightarrow (B \wedge C)'$, $(A \vee B \vee C \vee D)$ vyplývá:

- $A \vee C$
- $B' \Rightarrow C$
- $C \Rightarrow D'$
- $A \Leftrightarrow D$
- $B' \Rightarrow (A \vee C)$

Cvičení 7. Rozhodněte, zda z předpokladů $A \Rightarrow (B' \wedge D')$, $B \Rightarrow (C' \wedge E')$, $C \Rightarrow E'$, $(A \wedge C) \Rightarrow D'$, $A' \Rightarrow B$ vyplývá:

- $A \vee C$
- $B' \Rightarrow C$

Logické slovní úlohy

Logické slovní úlohy budou využívat stejných postupů jako předchozí příklady, tedy zjednodušování výrazů a ověřování správnosti úsudku. Důležitý bude převod tvrzení zapsaného v českém jazyce do jazyka výrokové logiky. Následující tabulka vystihuje tyto převody:

Implikace	$A \Rightarrow B$	Jestliže platí A , potom platí B .
Ekvivalence	$A \Leftrightarrow B$	A platí právě tehdy, když platí B .
Konjunkce	$A \wedge B$	Platí A a zároveň platí B .
Disjunkce	$A \vee B$	Platí A nebo platí B .
Negace	A'	Neplatí A .

V textech slovních úloh nemusí být předpoklady podány vždy jednoznačně. Někdy proto může dojít k nedorozumění a dosažení jiných výsledků.

Příklad 7. Skupina pěti spolužáků (Alice, Bětka, Cecilka, David a Emil) chce jet na výlet. Přátelské vztahy v této skupině jsou všelijaké a jsou dány následujícími tvrzeními: Bětka pojede, pojede-li Alice.

Alice a David pojede, pojede-li Emil.

Bětka a Cecilka nepojedou společně.

Cecilka a David pojedou oba nebo žádný z nich.

Z dvojice David a Emil pojede alespoň jeden.

Chceme zjistit kdo pojede na výlet, jestliže budou akceptovány požadavky všech spolužáků.

Nejprve jednotlivá tvrzení lehce přeformulujeme, zapíšeme je v jazyce výrokové logiky a převedeme do Booleovy algebry. Tvrzení „Pojede Alice“ budeme značit A atd.:

Jestliže pojede Alice, potom pojede Bětka.	$A \Rightarrow B$	$a' + b$
Jestliže pojede Emil, potom pojede Alice a David.	$E \Rightarrow (A \wedge D)$	$e' + ad$
Jestliže pojede Bětka, potom nepojede Cecilka.	$B \Rightarrow C'$	$b' + c'$
Jestliže pojede Cecilka, potom nepojede Bětka.	$C \Rightarrow B'$	$c' + b'$
Cecilka pojede právě tehdy, když pojede David.	$C \Leftrightarrow D$	$cd + c'd'$
Jestliže nepojede David, potom pojede Emil.	$D' \Rightarrow E$	$d + e$
Jestliže nepojede Emil, potom pojede David.	$E' \Rightarrow D$	$e + d$

Nyní zjistíme, při kterých ohodnoceníh a, b, c, d, e jsou splněny všechny podmínky:

$$\begin{aligned}
 (a' + b)(e' + ad)(b' + c')(cd + c'd')(d + e) &= 1 \\
 (a'e' + be' + abd)(b' + c')(cd + cde + c'd'e) &= 1 \\
 (a'b'e' + a'c'e' + bc'e' + abc'd)(cd + c'd'e) &= 1 \\
 a'b'cde' &= 1
 \end{aligned}$$

Aby byla splněna poslední rovnost je nutné, aby $a = 0, b = 0, c = 1, d = 1, e = 0$. Po zpětném převodu do českého jazyka dostáváme závěr, že Alice, Bětka a Emil nepojedou a Cecilka s Davidem pojedou.

Příklad 8. Nechtě jsou dána tři tvrzení o kterých víme, že jsou pravdivá:

1. Nemluvňata jsou nelogická.
2. Nepohrdáme nikým, kdo dokáže ovládnout krokodýla.
3. Pohrdáme nelogickými osobami.

Chceme zjistit, zda z těchto tvrzení plyne závěr: Nemluvňata nedovedou ovládnout krokodýla.

Nejprve si označíme jednotlivá tvrzení:

N ...Osoba je nemluvně.

L ...Osoba je logická.

P ...Osoba je v našem opovržení.

K ...Osoba ovládá krokodýla.

Přeformulujeme tato tvrzení, převedeme do výrokové logiky a zapíšeme je v Booleově algebře:

Jestliže je někdo nemluvnětem, potom je nelogický.	$N \Rightarrow L'$	$n' + l'$
Jestliže někdo dokáže ovládnout krokodýla, potom jím nepohrdáme.	$K \Rightarrow P'$	$k' + p'$
Jestliže je někdo nelogická osoba, potom jí pohrdáme.	$L' \Rightarrow P$	$l + p$
Jestliže je někdo nemluvnětem, potom nedokáže ovládnout krokodýla.	$N \Rightarrow K'$	$n' + k'$

Ověřujeme správnost úsudku z množiny předpokladů:

$$[(N \Rightarrow L') \wedge (K \Rightarrow P') \wedge (L' \Rightarrow P)] \Rightarrow (N \Rightarrow K')$$

právě tehdy, když

$$(N \Rightarrow L') \wedge (K \Rightarrow P') \wedge (L' \Rightarrow P) \wedge (N \Rightarrow K')' = 0$$

$$(n' + l')(k' + p')(l + p)(n' + k')' = 0$$

$$(n' + l')(k'l + k'p + lp')kn = 0$$

$$(n' + l')(k'l + k'p + lp')kn = 0$$

$$(n' + l')(klnp') = 0$$

$$0 = 0$$

Úsudek je správný.

Cvičení 8. Ve státě Papua-Nová Guinea se tři největší parlamentní strany (Modrá, Bílá a Červená) dohodnou na schvalování zákonů následující dohodou:

1. Jestliže pro zákon nehlasuje Bílá strana, nehlasuje pro zákon ani Modrá strana.
2. Jestliže pro zákon hlasuje Bílá strana, hlasuje pro zákon i Modrá a Červená strana.

Jednoho dne se zástupci Bíle strany nedostaví na hlasování. Pro zákon hlasuje Modrá strana. Je povinností Červené strany hlasovat také pro tento zákon, jestliže nechtějí porušit danou dohodu?

Cvičení 9. Protože na území budoucí plánované přehrady se vyskytuje několik obcí, jejichž obyvatelé musí být přesídleni, byla vydána vyhláška, která měla předběžně upozornit občany na to, že:

Obce, které se vysídlují a přemísťují (mimo oblast přehrady) na stanovené místo, leží v oblasti budoucí přehrady.

O týden později byla vydaná nová vyhláška:

Obce, které se nevysídlují, nejsou v oblasti budoucí přehrady. Obce, které se nepřemísťují, nejsou určeny k vysídlení.

Říkají tyto vyhlášky totéž? Pokud ne, je alespoň jedna z vyhlášek zobecněním druhé?

Cvičení 10. Zákazník si objednává u architekta návrh na projekt rodinného domku s těmito požadavky:

1. Dům nemá být dvoupatrový, obsahuje-li solární panel a venkovní terasu.
2. Když dům nebude dvoupatrový nebo nebude mít venkovní terasu, musí obsahovat solární panel.
3. Když dům není dvoupatrový, nemá obsahovat solární panel nebo venkovní terasu.

Rozhodněte, zda architekt usuzuje správně, když říká:

- Dům musí obsahovat solární panel nebo musí být dvoupatrový.
- Jestliže dům bude mít venkovní terasu, musí mít i solární panel.

Cvičení 11. Jsou dána následující tvrzení:

1. Žádný žralok nepochybuje o tom, že je dobře vybaven.
2. Ryba, která nedovede tančit čtverylku, je hodna politování.
3. Žádná ryba si není jista svým vybavením, nemá-li alespoň tři řady zubů.
4. Všechny ryby s výjimkou žraloků jsou laskavy k dětem.
5. Těžké ryby nedovedou tančit čtverylku.
6. Ryba se třemi řadami zubů není politováníhodná.

Posuďte, zda z těchto tvrzení plyne závěr: Těžké ryby jsou laskavy k dětem.

Tabulková metoda

Všechny příklady z algebry pravdivostních hodnot výroků, lze také řešit tabulkovou metodou. Ukážeme, jak vyřešit jeden z výše zmíněných příkladů.

Příklad 9. Pomocí tabulkové metody ověříme, zda $(X \wedge Y) \Rightarrow (X \vee Y)$ je tautologií:

X	Y	$X \wedge Y$	$X \vee Y$	$(X \wedge Y) \Rightarrow (X \vee Y)$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	1
1	1	1	1	1

Vidíme, že pravdivostní hodnota $[(X \wedge Y) \Rightarrow (X \vee Y)] = 1$ při libovolném ohodnocení X, Y . Jde o tautologii.

Cvičení 12. S využitím tabulkové metody řešte příklady ze cvičení 5,6,7.

Závěr

V bakalářské práci jsme vybudovali Booleovu algebru jako speciální případ uspořádané množiny. Snažili jsme se objasnit některé pojmy vysokoškolské matematiky. Čtenář této práce měl možnost seznámit se s pojmy jako relace, uspořádání a supremum či infimum, které byly názorně předvedeny a zviditelněny pomocí Hasseových diagramů. Dále jsme dokázali definovat pojem Booleovy algebry, ve které jsme odvodili a následně dokázali některá pravidla, přičemž nebylo potřeba axiomaticky zavádět abstraktní algebraickou strukturu, jako to dělá velké množství textů, které se zabývají aplikací Booleovy algebry. Nakonec jsme ukázali, ve kterých konkrétních příkladech lze Booleovu algebru využít.

Tento text by bylo možné dále nadstavbově rozšířit. Po teoretické stránce je vše připraveno k tomu, aby se v dalších případných publikacích ukázalo, že tento způsob zavedení Booleovy algebry je ekvivalentní s axiomatickým zavedením Booleovy algebry, a dále se mohli ukázat jiné způsoby zavedení Booleovy algebry. V aplikační části by bylo možné rozšířit práci o využití Booleovy algebry v elektronice a výpočetní technice, kde Booleova algebra nalézá své uplatnění.

Literatura

- [1] O. Odvárko: *Booleova algebra*, ÚV matematické olympiády v nakladatelství Mladá fronta, Praha, 1973.
- [2] A. G. Kuroš: *Kapitoly z obecné algebry*, Academia, Praha, 1977.
- [3] O. Odvárko, E. Calda, J. Šedivý, S. Židek: *Metody řešení matematických úloh*, Státní pedagogické nakladatelství Praha, 1990.
- [4] J. Kopka: *Svazy a Booleovy algebry*, Univerzita J. E. Purkyně, Ústí nad Labem, 1991.
- [5] O. Zich, A. Kolman: *Zajímavá logika*, Mladá fronta, Praha, 1965.