Základy matematického vyjadřování

Ondřej Pangrác

3. března 2023

1 Výroky a výroková logika

Co to je výrok? Výrokem romzumíme sdělení, u kterého má smysl ptát se, zde je či není pravdivý. Příklady výroků tak jsou:

- Součet úhlů v trojúhelníku je vždy 180°.
- Druhá mocninna reálného čísla je vždy kladná.
- Číslo 13 je součtem druhých mocnin dvou celých čísel.
- Žádné celé sudé přirozené číslo není prvočíslo.
- Brno je hlavní město České republiky.

Příklady výpovědí, které výroky nejsou:

- Vstávat a cvičit!
- Kolik je hodin?
- Dej do hrnce vodu, brambory a cibuli a vař půl hodiny.

1.1 Negace

Negace výroku V je výrok „Není pravda, že V.“. Negaci výroku V značíme $\neg V$ a platí:
Je-li výrok V pravdivý, je výrok $\neg V$ nepravdivý.
Je-li výrok V nepravdivý, je výrok $\neg V$ pravdivý.

Negaci výroku lze často vytvořit předřazením slov „Není pravda, že ...“, ale obvykle lze dále výrok upravit na jiný ekvivalentní tvar. Například negace výroku „Číslo 8 je liché.“ může být „Není pravda, že číslo 8 je liché.“ nebo zkráceně „Číslo 8 není liché.“, nebo také „Číslo 8 je sudé.“.

1.2 Složené výroky

Dále se budeme zabývat způsoby, jak jednodušších výroků vytvářet složitější konstrukce, tzv. složené výroky. K tomu nám slouží logické spojky. Obvykle uvažujeme binární logické spojky, tedy spojujeme dva jednodušší výroky do jednoho složeného. Formálně ale lze za logickou spojku považovat i negaci, v tom případě se jedná o unární spojku.

Z běžném životě se nejčastěji setkáme se spojkami konjunkce a disjunkce.

Konjunkcí výroků A a B je výrok, který vznikce spojením spojkou „a“, zapisujeme ji $(A \wedge B)$ a je pravdivá pouze tehdy, když jsou pravdivé oba výroky A i B.

Disjunkcí výroků A a B je výrok, který vznikce spojením spojkou „nebo“, zapisujeme ji $(A \vee B)$ a je pravdivá tehdy, když je pravdivý alespoň jeden z výroků A, B.

Další běžnou logickou spojkou je implikace. Ta bývá vyjádřenou souvětím se spojkou „jestliže“, „pokud“ či jinak podobně. Implikaci výroků A, B zapisujeme $A \Rightarrow B$ a je pravdivá, pokud je nepravdivý výrok A nebo je pravdivý B. Výrok A nazýváme předpoklad implikace a výrok B důsledek.

Tyto tři logické spojky jsou asi nejběžnější, ale než se budeme věnovat jejich vlastnostem, zmíníme ještě ekvivalenci. Tu vyjadřujeme slovním spojením „právě tehdy, když“ a zapisujeme ji $A \Leftrightarrow B$. Ekvivalence výroků A, B je pravdivá, pokud jsou buď oba výroky pravdivé nebo naopak oba nepravdivé.

Vše si shrneme v tabulce:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Skládání výroku do složitějších může kombinovat více logických spojek včetně negací a pro vyhodnocení pravdivosti potom bude velmi záležet na pořadí vyhodnocení jednotlivých logických spojek. Z toho důvodu je často podstatné správné závorkování, které se ale špatně zachyczje v běžné řeči. Na druhou stranu je možné jeden výrok zapsat různými ekvivalentními zápisy. Poznamenejme, že výrok, který je pravdivý při každém ohodnocení elementárních výroků (výrokových proměnných reprezentovaných v našich příkladech písmeny A, B, C apod.), se nazývá tautologie. Výrok, který je při každém ohodnocení nepravdivý, se nazývá kontradikce nebo také sporný výrok. Příkladem tautologie je $(A \Rightarrow A)$, příkladem kontradikce třeba $(A \wedge \neg A)$.

1.3 Vlastnosti logických spojek

Podívejme se nyní na některé vlastnosti logických spojek. V první řadě z výše uvedené tabulky snadno poznáme, že logické spojky konjunkce, disjunkce a ekvivalence jsou komutativní. To znamená, že ve složeném výroku nezáleží na pořadí argumentů a konjunkce (resp. disjunkce, ekvivalence) výroků A, B má vždy stejnou pravdivostní hodnotu jako konjunkce (resp. disjunkce, ekvivalence) výroků B, A. S využitím značky $\equiv$ pro ekvivalentní vyjádření výroků lze tak psát:

$$\begin{aligned}(A \wedge B) &\equiv (B \wedge A)\\ (A \vee B) &\equiv (B \vee A)\\ (A \Leftrightarrow B) &\equiv (B \Leftrightarrow A)\end{aligned}$$

To, že uvedené logické spojky jsou ekvivalentní poznáme vlastně tak, že na druhém a třetím řádku tabulky jsou v odpovídajících sloupcích stejné symboly.

Naopak, implikace komutativní není, což nahlédneme z tabulky pravdivostních ohodnocení, v které se hodnota u implikace ve druhém a třetím řádku liší. Platí však jiný zajímavý vztah, který umožňuje měnit pořadí argumentů implikace, ale je třeba je nahradit negacemi. Výrok $(A \Rightarrow B)$ je ekvivalentní výroku $(\neg B \Rightarrow \neg A)$. To se nazývá obměna implikace a je to velmi užitečná vlastnost, kterou lze využít pro tzv. nepřímý důkaz.

Další vlastností, na kterou se zaměříme, je asociativita. Porovnáním pravdivostních hodnot (použijeme tabulku se třemi elementárními výroky) ověříme, že konjunkce i disjunkce jsou asociativní logické spojky. Tedy

$$
\begin{aligned}
((A \wedge B) \wedge C) &\equiv (A \wedge (B \wedge C)) \\
((A \vee B) \vee C) &\equiv (A \vee (B \vee C))
\end{aligned}
$$

Díky tomu, že nezáleží na pořadí vyhodnocení několi konjunkcí, resp. disjunkcí, může vnitřní závorky vynechat a psát pouze $(A \wedge B \wedge C)$, resp. $(A \vee B \vee C)$.

Logická spojka ekvivalence je také asociativní, ale je třeba si neplást asociativitu ekvivalence se strukturou tvrzení typu „Výroky $A, B, C, \ldots$ jsou navzájem ekvivalentní“, která znamená $((A \Leftrightarrow B) \wedge (A \Leftrightarrow C) \wedge (B \Leftrightarrow C) \ldots)$.

Naproti tomu implikace není asociativní a výroky $(A \Rightarrow (B \Rightarrow C))$ a $((A \Rightarrow B) \Rightarrow C)$ nejsou ekvivalentní (např. pro ohodnocení $A = 0, B = 1, C = 0$ je první výrok pravdivý, kdežto druhý je nepravdivý). Navíc řetězení implikací není v matematických výrocích příliš běžné, první výrok lze ekvivalentně formulovat

$$(A \Rightarrow (B \Rightarrow C)) \equiv ((A \wedge B) \Rightarrow C)$$

a druhý způsob uzávornkování se, až na nějaké umělé případy, nepoužívá. S řetězením implikací se ale můžeme setkat v důkazech. Tam je třeba zápis $A \Rightarrow B \Rightarrow C \ldots$ chápat jako konjunkci jednotlivých implikací $(A \Rightarrow B) \wedge (B \Rightarrow C) \ldots$. Potom, díky tranzitivitě implikace dostáváme

Poslední vlastností, na kterou se zaměříme, je distributivita. Tu známe z číselných oborů pro operace násobení a sčítání. U logických spojek funguje distributivita pro konjunkci a disjunkci a to překvapivě oběma směry:

$$
\begin{aligned}
(A \wedge (B \vee C)) &\equiv ((A \wedge B) \vee (A \wedge C)) \\
(A \vee (B \wedge C)) &\equiv ((A \vee B) \wedge (A \vee C))
\end{aligned}
$$

U jiných běžných kombinací logických spojek distributivita nefunguje nebo nemá význam z hlediska použití. Poznamenejme, že stejné vlastnosti jako konjunkce a disjunkce mají množinové operace průnik a sjednocení. Tato podobnost není náhodná a později se k ní vrátíme.

1.4 Negace složených výroků

Dále se zaměříme na to, jak se chová negace složených výroků. Negací konjunkce výroků A, B je výrok, který je pravdivý právě když je konjukce A, B nepravdivá. To nastane, je-li nepravdivý alespoň jeden z výroků A, B, jde tak o disjunkci negací těchto dvou výroků. To můžeme zapsat symbolicky:

$$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$$

Analogicky pro negaci disjunkce výroků A, B můžeme nalézt ekvivalentní výrok, kterým je konjunkce jejich negací:

$$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$$

Zamyslíme-li se nad negováním implikace, resp. se podíváme do tabulky pravdivostního ohodnocení, zjistíme, že negace je nepravdivá pouze tehdy, když je její předpoklad pravdivý a důsledek nepravdivý. Tedy:

$$\neg(A \Rightarrow B) \equiv (A \wedge \neg B)$$

Nakonec, negací ekvivalence výroků A, B je výrok, který je pravdivý právě tehdy, když je pravdivý právě jeden z výroků A, B. Ten lze zapsat:

$$\neg(A \Leftrightarrow B) \equiv (\neg A \Leftrightarrow B) \equiv (A \Leftrightarrow \neg B)$$

Případně je možné zavést novou logickou spojku „výlučné nebo“ („výlučnou disjunkci“).

1.5 Odvození logických spojek

Zavádíme-li logické spojky, je obvyklé, že nezavedeme všechny jejich popisem, případně tabulkou hodnot, ale zavedeme jen některé základní a ostaní pak definujeme pomocí těchto základních. Obvykle je jednou ze základních spojek negace. Pokud jako druhou základní zvolíme konjunkci, lze pak disjunkci definovat

$$(A \vee B) \equiv \neg(\neg A \wedge \neg B)$$

Pokud naopak zvolíme disjunkci, konjunkci definujeme

$$(A \wedge B) \equiv \neg(\neg A \vee \neg B)$$

. Máme-li teď k dispozici konjunkci a hlavně disjunkci, lze implikaci zavést

$$(A \Rightarrow B) \equiv (\neg A \vee B)$$

Pokud naopak k negaci zavedeme jako základní logickou spojku implikaci (to je obvyklé v Matematické logice), zavedeme disjunkci snadno

$$(A \vee B) \equiv (\neg A \Rightarrow B)$$

Konjunkci pak lye definovat pomocí disjunkce, případně v této definici expandovat zápis disjunkce pomocí implikace.

Pokus definovat ostatní logické spojky pomocí negace a ekvivalence by byl, bohužel, neúspěšný. Na druhou stranu, lze vytvořit systémy, v kterých budeme mít jen jednu základní spojku (binární) a z ní odvodít ostatní. To je ale spíše zajímavost a okrajová záležitost a řešit to nebudeme.

1.6 Normální formy

Boolevskou funkcí n proměnných rozumíme libovolné zobrazení $\varphi : \{0,1\}^n \to \{0,1\}$. Je-li V výrok s n různými výrokovými proměnnými, pak pravdivostní ohodnocení výroku V při různých ohodnoceních určuje booleovskou funkci φ_V s n proměnnými. Říkáme potom, že φ_V je realizována formulí V. Pravdivostní tabulka představuje jednoduchý způsob, jak funkci φ_V spočítat.

Než si ukážeme, jak najít výrok realizující zadanou booleovskou funkci, definujeme si tzv. normální tvary výroků. Výrok je v disjunktní normální formě, je-li disjunkcí několika výroků takových, že *(i)* každý je konjunkcí (konečně mnoha) výrokových proměnných nebo jejich negací a *(ii)* v žádném se nevyskytuje současně výroková proměnná i její negace. Platí následující tvrzení, které si uvedeme bez důkazu.

Tvrzení 1.1 *Každá výrok, který není kontradikcí, je ekvivalentní nějakému výroku v disjunktní normální formě.*

Důvodem, proč vylučujeme kontradikci, je bod *(ii)*. Pokud ho vynecháme, je libovolná kontradikce ekvivalentní výroku $(A \wedge \neg A)$.

Nyní si ukážeme jednoduchý způsob, jak pro danou booleovskou funkci B, najdeme výrok, který je její realizací. Pokud je φ identicky rovna nule, je její realizací libovolná kontradikce. Jinak budeme hledat výslednou formuly v disjunktním normálním tvaru. To si ukážeme na následujícím příkladu. Nechť je φ funkce tří proměnných a, b, c dána tabulkou:

a	b	c	$\varphi(a,b,c)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Odpovídající výrok budeme nejprve konstruovat jako disjunkci konjukcí. Z prvního řádku vidíme, že při ohodnocení všech proměnných hodnotou 0 je hodnota φ rovna 1. Do výsledného výroku tedy dáme $(\neg A \wedge \neg B \wedge \neg C)$. Podobně pro ostatní řádky, na nichž je φ rovno 1 přidáme do realizujícího výroku odpovídající konjunkci elementárních výroků nebo jejich negací. Výsledný výrok pak bude disjunkcí výroků odpovídajícím jednotlivým řádkům, v našem případě tedy $((\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge C))$, což lze zjednodušit na $((\neg A \wedge \neg B) \vee (B \wedge C))$. Poznamenejme, že v předchozím jsme hojně využívali asociativitu logických spojek konjunkce a disjunkce.

Druhým normálním tvarem je konjunktivní normální forma. Výrok je v konjunktivní normální formě, je-li konjunkcí několika výroků takových, že *(i)* každý je disjunkcí (konečně mnoha) elementárních výroků nebo jejich negací a *(ii)* v žádné se nevyskytuje současně tentýž elementární výrok i jeho negace. Podobně jako pro disjunktivní normální tvar, platí i pro konjuktivní normální tvar analogické tvrzení.

Tvrzení 1.2 *Každý výrok, který není tautologií, je ekvivalentní nějakému výroku v konjunktivní normální formě.*

Podobně jako v předchozím případě vylučujeme tautologie kvůli bodu *(ii)*. Pokud ho vynecháme, je libovolná tautologie ekvivalentní výroku $(A \vee \neg A)$.

Pomocí distributivity lze formuli v disjunktivně normálním tvaru převést na tvar konjunktivně normální. Postupnými úpravami na výše uvedený příklad dostaneme $((\neg A) \vee B) \wedge (\neg A \vee C) \wedge (\neg B \vee C))$.

Druhou možností, jak převést booleovskou funkci na konjuktivní normální tvar je najít výrok odpovídající její negaci v disjunktním normálním tvaru a pak pomocí pravidel pro negování převést na konjuktivní normální tvar.

2 Predikátová logika

Doteď jsme pracovali pouye se dvěma hodnotami – pravdivý a nepravdivý výrok. Pro práci s dalšími objekty, v první řadě s čísly a různými číselnými obory a pak i s ostatními matematickými objekty, budeme potřebovat nové prostředky v jazyce. Prvním typem jsou predikáty (nebo též relace, to je v podstatě totéž). Predikát arity $n \geq 1$ na množině X je podmnožina kartézského součinu n kopií X. Predikát popisuje nějakou vlastnost a určuje, zda ji n-tice prvků z množiny X tu vlastnost má nebo nemá. Výsledkem predikátu je tedy opět hodnota pravda nebo nepravda a tak lze s predikáty pracovat vlastně jako s elementárními výroky.

Druhým typem symbolů jsou funkce. Ty lze formálně také zavést pomocí relací, ale protože se běžně chápou poněkud odlišně a v případě jejich definice pomocí relací je třeba mít zajištěné další podmínky, budeme je považovat za jiný typ objektů. Mezi funkcemi mají zvláštní postavení funkce arity 0, které reprezentují konstanty.

2.1 Kvantifikátory

Nyní konečně můžeme začít hovořit o kvantifikátorech, které nám umožní popsat, že nějaké tvrzení platí všeobecně, nebo že můžeme najít alespoň jednu hodnotu, pro kterou platí.

Všeobecný, obecný, nebo také velký kvantifikátor se značí symbolem $\forall$ a výrok

$$(\forall x)V(x)$$

se čte „Pro každé x platí výrok V“ a znamená, že V (obsahující proměnnou x) je pravdivý, ať za x jakooukoli hodnotu, která v dané teorii dává smysl.

Naproti tomu existenční, neboli malý kvantifikátor $\exists$ použijeme, chceme-li vyjádřit, že výrok je pravdivý pro alespoň jednu volbu proměnná. Tedy

$$(\exists x)V(x)$$

budeme číst „Existuje x takové, že platí výrok V“ a přesně takový je i význam.

Někdy se lze setkat ještě se zesíleným existenčním kvantifikátorem $\exists!$, přičemž

$$(\exists! x)V(x)$$

znamená, že existuje právě jedno x, pro které platí výrok V. To lze ekvivalentně zapsat jako

$$(\exists! x)V(x) \equiv (\exists x)(V(x) \wedge (\forall y)(V(y) \Rightarrow x = y))$$

2.2 Kvantifikace přes množiny

Obecně do kvantifikované proměnné dosazujeme libovolný prvek univerza ve kterém v dané teorii pracujeme. Pokud například budeme pracovat v oboru celých čísel, pak $(\forall x)V(x)$ znamená, že výrok V platí pro všechna celá čísla, která dosazujeme za x a už nemusí (ale může) platit pro neceločíselné hodnoty, i kdyby pro ně dával smysl. Třeba výrok

$$(\forall x)(2x \in \mathbb{Z})$$

je v oboru celých čísel pravdivý (dvojnásobek každého celého čísla je opět celé číslo), ale v obroru racionálních čísel už pravdivý není. Analogicky to bude fungovat i pro existenční kvantifikátor, jen s tím rozdílem, že problémy s platností se vyskytnou při zmenšování uvažévaného univerza místo při jeho rozšiřování.

Pokud fakt, že kvantifikovanou proměnnou volíme z nějaké konkrétní množiny, zahrneme tuto vlastnost do tvrzení následujícím zápisem:

$$(\forall x \in M)V(x)$$

znamená, že výrok V platí pro všechna prvky z množiny M a

$$(\exists x \in M)V(x)$$

má význam takový, že existuje alespoň jeden prvek množiny M, pro který je V pravdivý.

Pokud nechceme množinu, z které máme prvky používat, zahrnovat přímo do kvantifikace, lze tento fakt zahrnout přimo do výroku a kvantifikovat bez omezení na množinu. V případě všeobecného kvantifikátoru pak ve výroku použijeme implikaci a pro existenční kvantifikátor konjukci:

$$\begin{aligned}(\forall x \in M)V(x) &\equiv (\forall x)(x \in M \Rightarrow V(x))\\ (\exists x \in M)V(x) &\equiv (\exists x)(x \in M \wedge V(x))\end{aligned}$$

Jen pro úplnost je třeba upozornit na případ, kdy kvantifikujeme přes prázdnou množinu. Pro $M = \emptyset$ je výrok $(\forall x \in M)V(x)$ vždy pravdivý bez ohledu na to, co je výrok V a naopak výrok $(\exists x \in M)V(x)$ je vždy nepravdivý.

2.3 Kvantifikátory a negace

Pro negování kvantifikovaných výroku platí jednoduchá pravidla. Negací výroku „Pro každé x platí výrok V." je přirozeně „Existuje alespoň jedno x, pro které výrok V naplatí.". Analogicky negací „Existuje x, pro které platí V." je výrok „Pro žádné x V neplatí.". Zapsáno symbolicky

$$\begin{aligned}\neg(\forall x)V(x) &\equiv (\exists x)\neg V(x)\\ \neg(\exists x)V(x) &\equiv (\forall x)\neg V(x)\end{aligned}$$

To nás přivádí k pozorování, že stejně jako u logických spojek, ani u kvantifikátorů není třeba oba zavádět přímo, ale je možné jeden odvodit od druhého:

$$\begin{aligned}(\exists x)V(x) &\equiv \neg(\forall x)\neg V(x)\\ (\forall x)V(x) &\equiv \neg(\exists x)\neg V(x))\end{aligned}$$

O tom, jak odvodit zesílený existenční kvantifikátor jsme se již zmiňovali.

2.4 Více kvantifikátorů

Pokud výrok obsahuje dva stejné kvantifikátory za sebou, je možné jejich pořadí prohazovat, nebo-li

$$\begin{aligned}(\forall x)(\forall y)V(x,y) &\equiv (\forall y)(\forall x)V(x,y)\\ (\exists x)(\exists y)V(x,y) &\equiv (\exists y)(\exists x)V(x,y)\end{aligned}$$

Toto lze zobecnit i na více stejných kvantifikátorů.

Pro různé kvantifikátory jejich prohození není obecně možné

$$(\forall x)(\exists y)V(x,y) \not\equiv (\exists y)(\forall x)V(x,y)$$

Obecně platí, že pokud je výrok $(\exists y)(\forall x)V(x,y)$ je pravdivý, je pravdivý i výrok $(\forall x)(\exists y)V(x,y)$. Druhá implikace ale neplatí, jako protipříklad lze použít jednoduše $V(x,y)$ jako rovnost $x = y$.

Další otázkou je, jak se chová kombinace kvantifikátoru a logických spojek. V některých případech je jednoduše možné použít pravidlo analogické distributivitě

$$\begin{aligned}(\forall x)(A(x) \wedge B(x)) &\equiv ((\forall x)A(x) \wedge (\forall x)B(x))\\ (\exists x)(A(x) \vee B(x)) &\equiv ((\exists x)A(x) \vee (\exists x)B(x))\end{aligned}$$

nicméně nefunguje to pro

$$\begin{aligned}(\forall x)(A(x) \vee B(x)) &\not\equiv ((\forall x)A(x) \vee (\forall x)B(x))\\ (\exists x)(A(x) \wedge B(x)) &\not\equiv ((\exists x)A(x) \wedge (\exists x)B(x))\end{aligned}$$

Možností, jak najít ekvialentní vyjádření výroku $((\forall x)A(x) \vee (\forall x)B(x))$ do tvaru s kvantifikátory před samotným výrokem je v každé části použít jinou proměnnou. Přepíšeme si výrok do tvaru $((\forall x)A(x) \vee (\forall y)B(y))$, kde výrok A neobsahuje proměnnou y a výrok B neobsahuje x. Pak

$$((\forall x)A(x) \vee (\forall y)(B(y)) \equiv (\forall x)(\forall y)(A(x) \vee B(y))$$

Podobně lze

$$((\exists x)A(x) \wedge (\exists x)(B(x)) \equiv (\exists x)(\exists y)(A(x) \wedge B(y))$$

2.5 Kvantifikátory v implikaci

Pro složený výrok s logickou spojkou implikace si pravidla pro přesun kvantifikátorů před výrok odvodíme snadno díky přepsání implikace na disjunkci a po přesunu kvantifikátoru opět na implikaci. V následujícím předpokládejme, že výrok $A(x)$ neobsahuje proměnnou y a naopak výrok $B(y)$ nemá žádný výskyt proměnné x. Pak

$$\begin{aligned}
(A(x) \Rightarrow (\forall y)B(y)) &\equiv (\neg A(x) \vee (\forall y)B(y)) \equiv (\forall y)(\neg A(x) \vee B(y)) \\
&\equiv (\forall y)(A(x) \Rightarrow B(y)) \\
(A(x) \Rightarrow (\exists y)B(y)) &\equiv (\neg A(x) \vee (\exists y)B(y)) \equiv (\exists y)(\neg A(x) \vee B(y)) \\
&\equiv (\exists y)(A(x) \Rightarrow B(y)) \\
((\forall x)A(x) \Rightarrow B(y)) &\equiv (\neg(\forall x)A(x) \vee B(y)) \equiv ((\exists x)\neg A(x) \vee B(y)) \\
&\equiv (\exists x)(\neg A(x) \vee B(y)) \equiv (\exists x)(A(x) \Rightarrow B(y)) \\
((\exists x)A(x) \Rightarrow B(y)) &\equiv (\neg(\exists x)A(x) \vee B(y)) \equiv ((\forall x)\neg A(x) \vee B(y)) \\
&\equiv (\forall x)(\neg A(x) \vee B(y)) \equiv (\forall x)(A(x) \Rightarrow B(y))
\end{aligned}$$

Tím pádem jsme schopni pro libovolný výrok obsahujícím logické spojky negace, konjunkce, disjunkce a implikace najít jeho ekvivalentní vyjádření, v kterém budou nejprve všechny kvantifikované proměnné a poté výrok bez kvantifikátorů. Stačí nejprve vhodně substituovat proměnné, které se ve výroku vyskytují kvantifikované ve více než jednom podvýroku a postupot dle výše uvedených pravidel. Takovémuto tvaru výroku, kdy jsou všechny kvantifikátora před samotným výrokem, se říká prenexní tvar.

3 Množiny a jejich zápis

Chceme-li definovat pojem množina, může říct, že se jedná o soubor (kolekci) prvků. Pak bysme ale měli říct, co to je soubor nebo kolekce atd.. Zjistíme, že pojem množina je obtížné definovat. Jde spíše o tzv. primitivní pojem, který není možné definovat na základě jiných pojmů, ale je třeba ho zevést axiomaticky. Prostě říct, že některé v matematice používané objekty jsou množiny, a pak zavést přípustné operace s množinami.

V principu lze říct, že množina je objekt, u kterého má smysl se ptát, zda jiný objekt je jejím prvke. Relace „být prvkem“ je vlastně základem celé teorie množin. Používá se pro ni symbol $\in$ a pomocí této relace a relace rovnosti je možné další symboly jazyka teorie množin odvodit. Pro začátek $x \notin X \equiv \neg(x \in X)$ definuje relaci nebýt prvkem a $x \neq y \equiv \neg(x = y)$ relaci nebýt roven. Dále si definujeme relaci „být podmnožinou“ se symbolem $\subseteq$ pomocí vztahu

$$Y \subseteq X \equiv (\forall x)(x \in Y \Rightarrow x \in X)$$

My se přímo axiomatickým vystavěním teorie množin zabývat nebudeme a k množinám budeme přistupovat spíše intuitivně, přesto bude třeba na některé formální aspekty upozornit, protože ne vše je v množinách povolené.

3.1 Výčet prvků a prázdná množina

Chceme-li popsat množinu, je nejjednodušším způsobem vypsat všechny její prvky, které zapíšeme do složených závorek a oddělíme čárkami, resp. středníky (čárka by se nám mohla splést s desetinou čárkou u necelých čísel). Tak například množinu lichých jednociferných čísel zapíšeme $\{1, 3, 5, 7, 9\}$.

Velmi důležité postavení mezi množinami má prázdbá množina. Někdy se lze setka se zápisem $\{\}$, my se ale raději budeme držet značení $\emptyset$. Prázdnou množinu definujeme

$$(\forall x) x \notin \emptyset$$

3.2 Sjednocení a potence

Základní množinové operace, které je třeba zavést axiomaticky jsou sjednocení (někdy též nazívaná suma množiny) a potence. Sjednocení dvou množin je množina, které obsahuje právě ty prvky, které jsou v alespoň jedné z množin. Tedy pro množiny X, Y označíme jejich sjednocení $X \cup Y$ a definujeme ho

$$(\forall x)(x \in X \cup Y \Leftrightarrow (x \in X \vee x \in Y))$$

Sjednocení lze definovat i pro množinové systémy, tj. sjednocení systému (více než dvou) množin. Mějme X množinu, jejímiž prvky jsou množiny. Pak její suma $\bigcup X$ obsahuje takové prvky x, které jsou v některé z množin patřící do X.

$$(\forall x)(x \in \bigcup X \Leftrightarrow (\exists Y)(x \in Y \wedge Y \in X))$$

Potenční množinou množiny X budeme nazývat množinu všech jejích podmnožin. To, že takový systém tvoří množinu je třeba zavést axiomaticky. Potenční množina množina X se značí $\mathcal{P}(X)$ nebo také 2^X a definuje se

$$Y \in 2^X \Leftrightarrow Y \subseteq X$$

3.3 Vydělení vlastností

Dalším způsobem, jak vytvářet množiny je pomocí nějakých vlastností, které lze popsat pomocí výroku. Je ale třeba pracovat s jistou opatrností. Intuitivní pojetí je v tomto případě nedostatečné, jak se ukázalo objevením Russellova paradoxu. Uvažme M množinu všech množin, které nejsou svými prvky. Zapsáno symbolicky

$$x \in M \leftrightarrow x \notin x\,.$$

Je množina M prvkem M? Pokud ano, pak ale musí mít vlastnost $M \notin M$, tedy $M \in M \to M \notin M$. Pokud ne, pak $M \notin M$, tedy má požadovanou vlastnost a dle definice M do ní patří, tedy $M \notin M \to M \in M$. Obě možnosti vedou ke sporu.

Tento rozpor vyřešíme tak, že vůbec nepřipustíme definici takovéto nebo podobné množiny. Postupovat můžeme pouze tak, že nějakou vlastností, kterou lze popsat matematickým výrokem, vydělíme prvky z již existující množiny a vytvoříme tak její podmnožinu. V důsledku toho nemůže existovat „množina všech množin“ a univerzum U obsahující všechny objekty, s kterými pracujeme, které lze definovat jako

$$(\forall x)(x \in U \Leftrightarrow x = x)$$

není množinou, ale tzv. třídou.

Nyní lze definovat další operace s množinami

- průnik $X \cap Y = \{x \in X; x \in Y\}$
- rozdíl $X \setminus Y = \{x \in X; x \notin Y\}$
- symetrický rozdíl $X \Delta Y = \{x \in X \cup Y; x \notin X \cap Y\}$
- doplněk $\overline{X} = \{x; (x \notin X)\} = U \setminus X$

V definici dopňku pracujeme s U jako s množinou, což ale být nemusí. Pokud je v rámci nějaké teorie univerzum, v kterém pracujeme, množinou, pak je doplňek korektně definován a doplňek množiny je množinou.

3.4 Vlastnosti množinových operací

Pro takto zavedené operace platí algebraické zákonitosti podobné vztahům mezi čísly a číselnými operacemi. Uvedeme si zde ty základní, jejich důkazy jsou většinou snadné z rozepsaných definic.
Zákony typu uspořádání:

- $(\forall X)\ \emptyset \subseteq X$
- $(\forall X) X \subseteq X$ - reflexivita,
- $(\forall X, Y)(X \subseteq Y \wedge Y \subseteq X) \rightarrow X = Y$ - antisymetrie.
- $(\forall X, Y, Z)(X \subseteq Y \wedge Y \subseteq Z) \rightarrow X \subseteq Z$ - tranzitivita.

Relace „být podmnožinou" je reflexivní, antisymetrická a tranzitivní, jedná se tedy o částečné uspořádání. Uspořádání potenční množiny prvních n přirozených čísel relací $\subseteq$ se nazývá Booleovské uspořádání (řádu n).
Algebraické vlastnosti $\cap, \cup, \overline{}$:

- dvojí doplněk $\overline{(\overline{X})} = X$
- komutativita $X \cap Y = Y \cap X$ a $X \cup Y = Y \cup X$
- asociativita $X \cap (Y \cap Y) = (X \cap Y) \cap Z$ a $X \cup (Y \cup Y) = (X \cup Y) \cup Z$
- distributivita $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ a $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

Jak si můžeme všimnout, na rozdíl od násobení a sčítání čísel, platí pro sjednocení a průnik množin obě možné distributivity, podobně jako to bylo u logickýc spojek disjunkce a konjunkce.

Posledních několik vlastností je odlišných od těch, které známe z operací v číselných oborech, ale odpovídají operacím v Booleových svazech. (Operace, v kterých se vyskytuje univerzum platí, pokud je univerzum množinou, jinak nemusí dávat smysl.)

- idempotence $X \cap X = X$ a $X \cup X = X$
- $X \cap \emptyset = \emptyset$ a $X \cup \emptyset = X$,
- $X \cap U = X$ a $X \cup U = U$,
- $X \cap \overline{X} = \emptyset$ a $X \cup \overline{X} = U$,
- De Morganovy vzorce $\overline{(X \cap Y)} = \overline{X} \cup \overline{Y}$ a $\overline{(X \cup Y)} = \overline{X} \cap \overline{Y}$.

De Morganovy vzorce jsou někdy známé spíše ve tvaru

- $A \setminus (\bigcup_i B_i) = \bigcap_i (A \setminus B_i)$,
- $A \setminus (\bigcap_i B_i) = \bigcup_i (A \setminus B_i)$.

3.5 Množinová interpretace logckých spojek

Nyní se pokusíme dát do souvislosti množinové operace s logické spojky výrokové logiky. Budeme-li za univerzum uvažovat množinu všech možných ohodnocení proměnných (elemntárních výroků nebo např. číselných proměnných v číselných oborech), pak výroku V lze přiřadit množinu všech ohodnocení $M(V)$ pro která je V pravdivý.

$$M(V(x)) = \{x \in U; V(x)\}$$

Negace vvýroku pak odpovídá doplňku množiny, konjunkce dvou výroků operaci průnik a disjunkce operaci sjednocení.

$$\begin{aligned} M(\neg V) &= \overline{M(V)} \\ M(V \wedge W) &= M(V) \cap M(W) \\ M(V \vee W) &= M(V) \cup M(W) \end{aligned}$$

3.6 Nekonečné množiny

Nakonec se podívejme na nekonečné množiny. Vlastně zatím žádnou takovou množinu nemáme vytvořenu, protože ani výčtem prvků, ani sjednocemím množin a operací potenční množiny nemůžeme (z konečných množin) vztvořit množinu nekonečnou. Ostatní operace nám neumožňují množiny zvětšovat, až snad na doplněk, ale ten je vždy podmnožinou univerza, které bysme předním museli vztvořit jako nekonečnou množinu. Kde se tady nekonečné množiny vezmou? Je nutné zavést nějakou nekonečnou množinu axiomaticky. Znění takového axiomu si uvádět nebudeme, berte to pouze jako fakt. Celá teorie množin a s ní i (téměř) celá matematika stojí nikoli na nevyvratitelných přírodní zákonech, ale na dohodě matematiků, že něco „tak je“ – přijmeme axiomy matematické logiky a teorie množin. Bez toho by nebylo možné vybudovat přirozená čísla a jejich aritmetiku.

4 Cvičení

Několik příkladů na procvičování.

Příklad: Přepište slovní tvrzení do formulí s kvantifikátory a logickými spojkami. Pokud není uvedeno jinak (a je to potřeba), použijte jako universum množinu přirozených čísel $\mathbb{N} = \{1, 2, \ldots\}$.

1. V množině A existuje číslo větší než 3.
2. Žádné číslo z množiny B není větší než 57.
3. Pro každé číslo z množiny C platí, že pokud je sudé, potom jeho trojnásobek není prvkem C.
4. Pro žádné číslo z množiny A neexistuje číslo z množiny B takové, že jejich součin je větší než 57.
5. V množině A existuje číslo, jehož každý dělitel je menší než 57.
6. Pokud množina B obsahuje všechny dělitele čísla 15, pak B obsahuje i všechny dělitele čísla 27.
7. Množina C obsahuje právě dvě sudá a právě dvě lichá čísla.
8. Pokud každé celé sudé číslo patří do množiny A, pak žádné celé sudé číslo nepatří do množiny B.

Příklad: Zapište tvrzení jako matematický výrok. Pokud je to potřebné, berte všechny zmíněné množiny jako podmnožiny celých čísel.

1. Každé číslo z množiny A je součtem dvou různých čísel z množiny B.
2. Součet každých dvou různých čísel z množiny B je prvkem množiny A.
3. Množina A je právě množina součtů dvojic různých čísel z množiny B.
4. Každá dvě různá čísla z množiny M se buď liší nejvýše o 5 nebo je jedno kladné a jedno záporné.
5. Jestliže množina C obsahuje pouze celá sudá čísla, pak je každé číslo z B dělitelné nějakým nenulovým číslem z množiny D.

Příklad: Definujte následující množiny:

1. A je množina všech přirozených trojciferných čísel,
2. B je množina druhých mocnin jednociferných provočísel,
3. C je množina celých čísel, která jsou druhou mocninou celého lichého čísla,
4. D je množina celých čísel, která jsou druhou odmocninou celého sudého čísla,
5. E je množina přirozených čísel, která nemají žádného dělitele v rozmezí čísel 10 až 100 (včetně),
6. F je množina přirozených čísel, která mají právě dva přirozené dělitele (tedy F je množina prvočísel),
7. G je množina přirozených čísel, která mají právě tři přirozené dělitele,
8. H je množina přirozených dělitelů přirozeného čísla n.

Příklad: Dány množiny $A, B \subseteq \mathbb{Z}$, definujte:

1. množinu všech čísel, která lze zapsat jako součet čísla z A s číslem z B,
2. množinu všech čísel, která jsou celočíselným násobkem některého z čísel z množin A nebo B.

Příklad: Porovnejte následující dvojice množin:

1. $2^{A \setminus B}$ a $2^A \setminus 2^B$,
2. $2^{A \cup B}$ a $2^A \cup 2^B$,
3. $2^{A \cap B}$ a $2^A \cap 2^B$.

Příklad: Nechť $a_1, a_2, a_3, \ldots$ je posloupnost reálných čísel. Rozhodněte, jaké vztahy (které implikace) platí mezi následujícími tvrzeními a pokuste se výroky popsat pomocí známých pojmů (monotonie, omezenost apod.).

$$\begin{array}{ll}
\textbf{T1:} & \forall c \in \mathbb{R}^+ \, \forall n \in \mathbb{N} : \; a_n > c \\
\textbf{T2:} & \forall c \in \mathbb{R}^+ \, \exists n \in \mathbb{N} : \; a_n > c \\
\textbf{T3:} & \exists c \in \mathbb{R}^+ \, \forall n \in \mathbb{N} : \; a_n > c \\
\textbf{T4:} & \forall n \in \mathbb{N} \, \forall c \in \mathbb{R}^+ : \; a_n > c \\
\textbf{T5:} & \forall n \in \mathbb{N} \, \exists c \in \mathbb{R}^+ : \; a_n > c \\
\textbf{T6:} & \exists n \in \mathbb{N} \, \forall c \in \mathbb{R}^+ : \; a_n > c
\end{array}$$

Co se změní, pokud ve všech trzeních množinu kladných reálných čísel $\mathbb{R}^+$ nahradíme všemi reálnými čísly $\mathbb{R}$?