Logika, množiny, důkazy

1 Logika a množiny

Matematická logika poskytuje formální prostředí pro práci s *výroky*. Výrok je pro nás jakákoli věta, o které lze rozhodnout, zda **platí**, či **neplatí**.

Příklad 1.0.1.

- „Mám žízeň." a „Nikdo nemá rád matiku." jsou výroky.
- „Jak se máš?" a „Ať už je konec!" nejsou výroky.
- „Trump vyhraje příští volby." je taky výrok, i když neumíme říct, jestli platí, nebo ne. Naše schopnost rozhodnout o pravdivosti věty nesouvisí s tím, že věta je nebo není výrokem.

1.1 Logika prvního řádu

Logikou prvního řádu se v matice myslí jazyk o dvou číslech/konstantách a pěti (obvykle pěti) operacích na výrocích.

Konstanty 0 a 1 (někdy taky $\perp$ a $\top$) se obvykle interpretují jako „lež" a „pravda". V tomto kontextu můžeme říct, že výrok je věta, které můžeme přiřadit hodnotu 0 nebo 1.

Výrazy se v logice obvykle reprezentují malými písmeny latinské abecedy (pokud jste o nich neslyšeli, jsou to a, b, c, atd.).

Definice 1.1.1 (Logické operace)**.** Řekněme, že p a q jsou výroky „Prší." a „Mám žízeň." Pak

- $\neg p$ (**ne** p; **negace** p) je výrok s opačnou pravdivostní hodnotou k p. V tomto případě

  $$\neg p = \text{„Neprší."}$$

  Operaci $\neg$ říkáme **negace**.

- $p \wedge q$ (p **a (zároveň)** q) platí jenom tehdy, když platí p i q. V našem případě je
$$p \wedge q = \text{„Prší a mám žízeň.“}$$
Operaci $\wedge$ říkáme **konjunkce**.

- $p \vee q$ (p **nebo** q) platí tehdy, když platí aspoň jeden z výroků p, q. Tedy,
$$p \vee q = \text{„Prší nebo mám žízeň.“}$$
Pozor! Tohle „nebo“ není výlučné. Výrok $p \vee q$ platí i v případě, že platí p i q. Operaci $\vee$ říkáme **disjunkce**.

- $p \Rightarrow q$ (p **implikuje** q; **z** p **plyne** q; **když** p, **pak** q) platí v jedné ze dvou možností:
  (1) Platí p a platí q.
  (2) Neplatí p.

  V našem případě
$$p \Rightarrow q = \text{„Když prší, mám žízeň.“}$$
Operaci $\Rightarrow$ říkáme **implikace**. Implikace může být trochu ošemetná na pochopení. Možná pomůže fakt, že výroku p se někdy říká *předpoklad* a výroku q *důsledek*. Jde o to, že když platí předpoklad, musí platit i důsledek; když ale předpoklad neplatí, důsledek může i nemusí být pravdivý.

  Pro naše zvolené výroky to konkrétně znamená, že **vždy** když prší, tak mám žízeň, ale když neprší, tak můžu mít žízeň, ale taky nemusím.

- $p \Leftrightarrow q$ (p **právě tehdy, když** q; p **je ekvivalentní** q) platí přesně v situaci, kdy p má stejnou pravdivostní hodnotu jako q. V našem případě
$$p \Leftrightarrow q = \text{„Prší právě tehdy, když mám žízeň.“}$$
Operaci $\Leftrightarrow$ se říká **ekvivalence**.

Definice 1.1.2 (Logická formule)**.** Logická formule je pro nás jakákoli *smysluplná* posloupnost výroků, logických operací a závorek. Smysluplnost znamená, že za $\neg$ je výrok a na obou stranách $\wedge, \vee, \Rightarrow, \Leftrightarrow$ je vždy výrok. Závorky určují prioritu logických operací.

Obecně se matematici nedohodli na nějaké přirozené prioritě logických operací, ale nejčastější úzus je, že nejvyšší prioritu má $\neg$, pod ní jsou $\wedge, \vee$ a nejnižší prioritu mají $\Rightarrow, \Leftrightarrow$.

Příklad 1.1.3. Třeba
$$((\neg p) \vee q) \Leftrightarrow ((p \vee (\neg q)) \Rightarrow r)$$
je formule, ale
$$p \Leftrightarrow \Rightarrow q \neg r$$
není.

V logice člověk často potřebuje zjistit, jakou pravdivostní hodnotu má formule v závislosti na pravdivostních hodnotách původních výroků. K tomu slouží tzv. *tabulka pravdivostních hodnot*, kam si člověk napíše všechny možné pravdivostní hodnoty výroků a prostě počítá. Třeba pro formuli

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

bychom sestrojili tabulku

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

Pro představu, kdyby p bylo „Prší.“, q bylo „Mám žízeň.“ a r bylo „Stíhám autobus.“, pak by výrok $((\neg p) \vee q) \Rightarrow r$ znamenal

Když neprší nebo mám žízeň, tak stíhám autobus.

Hodně štěstí bez pomoci rozluštit, kdy je tahle věta pravdivá.

1.2 Množiny

Množiny jsou základní stavební prvky moderní matematiky. Oproti tomu, co se vám někdo možná pokusí tvrdit, matematika neodpovídá na otázku „Co je množina?“. Matika jenom používá množiny k modelování struktur, které obvykle mají šanci někoho zajímat. Ta otázka je veskrze filosofická.

Asi každý si představuje množiny jako soubory prvků, které mají něco společného. Téhle interpretace se budeme taky držet. Fakt, že prvek x patří do množiny A budeme zapisovat $x \in A$, kde symbol $\in$ je pokroucené e z anglického **e**lement. Když chci tvrdit opak, tedy, že prvek x *neleží* v množině A, píšu $x \notin A$.

S množinami se táhne v závěsu pár vztahů a operací, které si teď zadefinujeme pomocí logických operací.

Definice 1.2.1 (množinové vztahy)**.** Vztahy mezi množinami budeme velmi pravděpodobně potřebovat jen dva, a to *inkluzi* a *rovnost*. Mějme dvě množiny A, B.

- $A \subseteq B$ (A **je podmnožina/součást** B; A **leží v/patří do** B) značí skutečnost, že každý prvek A je taky prvkem B. V logice

  $$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B).$$

  Vztahu $\subseteq$ se říká **inkluze**. Samozřejmě můžu psát i $A \supseteq B$ pro inkluzi opačným směrem.

- $A = B$ (A **je rovno** B) znamená, že A a B sdílejí všechny prvky. Logicky buď třeba

  $$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$$

  nebo

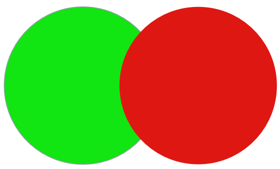
  $$A = B \Leftrightarrow (x \in A \Leftrightarrow x \in B).$$

Když píšu $A \subseteq B$ může se stát i to, že $A = B$. Pokud chci zdůraznit fakt, že $A \subseteq B$, ale $A \neq B$, napíšu $A \subsetneq B$.

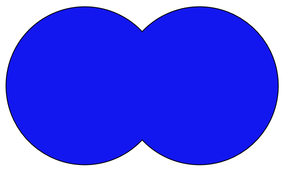
Definice 1.2.2 (množinové operace)**.** Budeme rozeznávat čtyři množinové operace. Podobně jako výsledkem logických operací na výrocích je zase výrok, výsledkem množinové operace na množinách je množina (to je ale překvápko).

- $A \cup B$ (A **sjednoceno s** B) je množina, která obsahuje prvky ležící v A *nebo* v B. Logicky

  $$x \in A \cup B \Leftrightarrow (x \in A \vee x \in B).$$

  Množiny A a B.

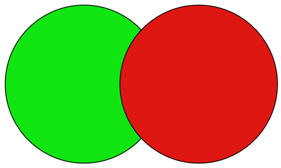
  

  Sjednocení $A \cup B$.

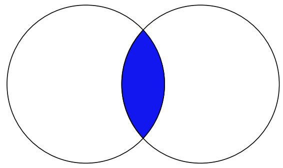
  Operaci $\cup$ říkáme **sjednocení**. Sjednocení z typografického hlediska příliš velkého množství množin $A_1, \ldots, A_n$, kde $n \in \mathbb{N}$, píšeme

  $$\bigcup_{i=1}^{n} A_i.$$

- $A \cap B$ (A **proniknuto s** B) je množina, která obsahuje jen ty prvky, které leží v obou množinách A, B.



Množiny A a B.



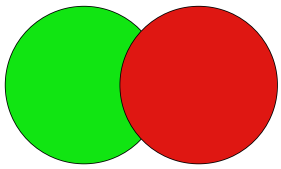
Průnik $A \cap B$.

Operaci $\cap$ říkáme **průnik**. Průnik spousty množin $A_1, \ldots, A_n$ píšeme

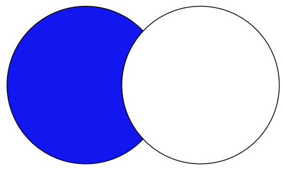
$$\bigcap_{i=1}^{n} A_i.$$

- $A \setminus B$ (A **bez**/**méně** B) obsahuje právě ty prvky, které jsou v A, ale nejsou v B. Logikou například takto:

$$x \in A \setminus B \Leftrightarrow (x \in A \wedge x \notin B).$$



Množiny A a B.



Rozdíl $A \setminus B$.

Operaci $\setminus$ říkáme rozdíl. Pozor! Operace $\setminus$ **není komutativní**, tzn., že $A \setminus B \neq B \setminus A$. Z toho důvodu nemá rozdíl více než dvou množin smysl, protože není jasné, v jakém pořadí třeba zápis

$$A \setminus B \setminus C$$

chápat.

- $A \times B$ (A **krát** B) je množina všech dvojic, kde první prvek je z A a druhý z B. Logicky

$$(x, y) \in A \times B \Leftrightarrow (x \in A \wedge y \in B).$$

Operaci $\times$ říkáme **součin** nebo **produkt**. Součin mnoha množin $A_1, \ldots, A_n$ píšeme

$$\prod_{i=1}^{n} A_i,$$

kde symbol Π je velké řecké „pí“ pro **p**rodukt. V případě, že násobíme množinu samu se sebou, můžeme taky psát

$$A^n := \prod_{i=1}^{n} A.$$

Příklad 1.2.3. Uvážíme množiny

$$A = \{\heartsuit, \clubsuit, \diamondsuit\}, \quad B = \{\clubsuit, \spadesuit\}, \quad C = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}.$$

Pak

$$\begin{aligned} A \cup B &= \{\heartsuit, \clubsuit, \diamondsuit, \spadesuit\} = C, \\ A \cap B &= \{\clubsuit\}, \\ C \setminus A &= \{\spadesuit\}, \\ A \times B &= \{(\heartsuit, \clubsuit), (\heartsuit, \spadesuit), (\clubsuit, \clubsuit), (\clubsuit, \spadesuit), (\diamondsuit, \clubsuit), (\diamondsuit, \spadesuit)\}. \end{aligned}$$

Pozor! Sjednocení $\cup$ a rozdíl $\setminus$ se nechovají jako $+$ a $-$. Všimněte si, že i když $A \cup B = C$, tak $C \setminus A \neq B$.

1.3 Kvantifikátory

Poslední základní ingrediencí matematického jazyka jsou kvantifikátory, které nám umožňují charakterizovat prvky množin pomocí logických výrazů.

Definice 1.3.1 (kvantifikátory). Rozlišujeme dva druhy kvantifikátorů – univerzální a existenční. Řekněme, že $p(x)$ značí výrok p, který v sobě obsahuje proměnnou x. Takový výrok může vypadat třeba jako $x \geq 2$ nebo $x + 1 = 5$. Pokud A je nějaká množina, pak výrazem

- $\forall x \in A : p(x)$ (**pro každé** x **z** A **platí** $p(x)$) myslíme, že pro každý prvek $x \in A$ platí výrok $p(x)$. Jinak řečeno, ať už si vyberu libovolný prvek množiny A a dosadím ho za x do $p(x)$, tak $p(x)$ bude pravdivý. Symbol $\forall$ je obrácené „A“ z německého ***A****llgemein* (pro všechny).
- $\exists x \in A : p(x)$ (**existuje** x **z** A **takové, že platí** $p(x)$) myslíme, že v A se nachází prvek, po jehož dosazení za x do $p(x)$ je výrok $p(x)$ pravdivý. Symbol $\exists$ je obrácené „E“ z anglického ***E****xists*.

Kromě těchto kvantifikátorů budeme ještě používat symbol $\exists!$, který znamená „existuje právě jeden“. Logicky, napíšu-li $\exists! x \in A : p(x)$, myslím tím

$$(\exists x \in A : p(x)) \wedge (\forall y \in A : p(y) \Rightarrow y = x).$$

Tedy, existuje prvek $x \in A$ splňující $p(x)$ a kdykoli $y \in A$ je prvek splňující $p(y)$, pak $y = x$. Konečně, symbolem $\nexists$ myslím „neexistuje“.

Příklad 1.3.2.

(1) Řekněme, že $p(x)$ je výrok $x \geq 2$. Pak výroky $\forall x \in \mathbb{R} : p(x)$ a $\exists! x \in \mathbb{R} : p(x)$ jsou lživé a $\exists x \in \mathbb{R} : p(x)$ je pravdivý.

- $\forall x \in \mathbb{R} : p(x)$ je lživý, protože každé reálné číslo určitě není větší než 2. Například -420 není.
- $\exists! x \in \mathbb{R} : p(x)$ je taky lživý, protože existuje víc reálných čísel větších než 2. 69 a 911 jsou dvě z nich.
- $\exists x \in \mathbb{R} : p(x)$ je pravdivý, protože umím najít reálné číslo větší než dva. Například 1337.

(2) Písmenem P označíme množinu všech lidí. Pro $x, y \in P$ znamená výrok $p(x, y)$, že „Člověk x zná jméno člověka y." Pak výrok

- $\forall x\, \forall y : p(x, y)$ znamená, že všichni lidé znají navzájem svá jména.
- $\forall x\, \exists y : p(x, y)$ znamená, že každý člověk zná jméno aspoň jednoho člověka.
- $\forall x\, \exists! y : p(x, y)$ znamená, že každý člověk zná jméno přesně jednoho člověka.
- $\exists x\, \forall y : p(x, y)$ znamená, že je na světě člověk, který zná jména všech lidí.
- $\exists x\, \exists y : p(x, y)$ znamená, že existuje člověk, který zná jméno nějakého člověka.

1.4 Relace a zobrazení

Operace součinu na množinách je zvlášť zajímavá pro to, že nám umožňuje definovat vztahy mezi prvky množin. Hádám, že vás nikdy neučili dívat se třeba na $\leq$ nebo na funkci $f(x) = 2x + 3$ jako na množiny...

Definice 1.4.1 (relace/vztah)**.** Mějme množiny A, B. Jakékoli podmnožině $R \subseteq A \times B$ budeme říkat **relace/vztah mezi A a B**. O prvku $x \in A$ řekneme, že je v relaci/vztahu R s prvkem $y \in B$, pokud $(x, y) \in R$. Tohle často zapisujeme jako xRy.

Pokud $A = B$, pak $R \subseteq A \times A$ je **relace na** A.

Příklad 1.4.2. Vztah „menší nebo rovno" je relace na reálných číslech. Smysl zápisu xRy je opodstatněn tím, že důležité relace v matice mají často vlastní symboly. Když totiž $R = \leq \subseteq \mathbb{R} \times \mathbb{R}$, pak nepíšeme třeba $\leq(2, 3)$, abychom vyjádřili, že 2 je menší nebo rovno 3, ale spíš $2 \leq 3$.

Jinak řečeno, relace je doslova výpis všech dvojic prvků, které jsou v tom daném vztahu. Takto lze vnímat právě relaci $\leq$ (třeba na $\mathbb{R}$) jako množinu všech dvojic $(x, y) \in \mathbb{R}^2$ pro $x \leq y$.

Příklad 1.4.3. Zkusím jednu analogii ze života. To nedopadne... Když bude P zase označovat množinu všech lidí, tak „svazek manželský" je relace na P. Relaci intuitivně interpretujeme jako nějaké pouto mezi objekty (v tomto případě dvěma), ale v matematice je pouto mezi prvky zase množina.

Jde o to si uvědomit, že v matice tohle funguje obráceně než v životě. Neříkám, že dva lidé jsou či nejsou manželé podle definice svazku manželského. Říkám, že definice svazku manželského je právě množina všech manželských párů. V moment, co se někdo rozvede nebo ožení/vdá, změní se moje definice manželského svazku.

Tohle je jedna z těch divných věcí v matice, které sice ze začátku nedávají úplně intuitivní smysl, ale příliš snadno se s nimi pracuje, než aby se je někdo snažil předělávat.

Definice 1.4.4 (zobrazení)**.** Pokud A, B jsou množiny, pak relaci R mezi A a B nazveme **zobrazením (mezi A a B)**, pokud

$$\forall x \in A \, \forall y, z \in B : (xRy \wedge xRz) \Rightarrow (y = z).$$

V případě, že $A = \mathbb{R}^n$ pro nějaké přirozené n a $B = \mathbb{R}$, můžeme relaci mezi A a B splňující výrok výše říkat **funkce**. To slovo je ale hodně naprd, takže budu spíš vždycky říkat **zobrazení**. Fakt, že f je zobrazení mezi A a B budeme zapisovat buď jako

$$f : A \to B \quad \text{nebo} \quad A \xrightarrow{f} B.$$

Cvičení. *Rozluštěte předchozí definici.*

Příklad 1.4.5. Zobrazení $\mathbb{R} \xrightarrow{f} \mathbb{R}$, $f(x) = 2x + 3$ je množina všech dvojic $(x, 2x + 3) \in \mathbb{R}^2$. Když je zobrazení definováno na prvcích první množiny (jako v tomto případě), často budu psát $x \mapsto 2x + 3$ místo $f(x) = 2x + 3$.

Definice 1.4.6 (doména, kodoména, vzor, obraz)**.** Mějme zobrazení $A \xrightarrow{f} B$. Pak se

- množina A nazývá **doménou** zobrazení f.
- množina B nazývá **kodoménou** zobrazení f.
- pro každé $x \in A$, nazývá $f(x)$ **obrazem** prvku x při zobrazení f.
- pro každé $y \in B$ nazývá prvek $x \in A$ takový, že $f(x) = y$ **vzorem** prvku y při zobrazení f. Značíme $y = f^{-1}(x)$.

  Pozor! Vzor prvku nemusí vždy existovat. Například při $\mathbb{R} \xrightarrow{f} \mathbb{R}, x \mapsto 1/x$ nemá 0 žádný vzor.

Tahle sekce ještě není hotová.

1.5 Metody důkazů

Zatím nic. rip