Olomoucký informatický korespondenční seminář – Olinx

Matematická logika a strojové myšlení, 3. díl

Radim Bělohlávek

olinx.inf.upol.cz

V tomto díle se seznámíme s aspekty matematické logiky, které mají zásadní význam jak pro logiku samotnou, tak pro problematiku strojového myšlení. Seznámíme se s axiomatizací matematické logiky. Jako v předchozích dílech se při tom i v tomto díle pro jednoduchost omezíme na výrokovou logiku. V axiomatizaci jde o to, jak z daných logických formulí odvodit formule, které z nich vyplývají, a to pouhou manipulací se symboly podle daných jednoduchých pravidel. To je pro strojové myšlení důležité, protože manipulovat symboly podle přesně definovaných pravidel počítač umí, a to velmi rychle. Kromě toho si vysvětlíme, proč je axiomatizace pro matematiku, informatiku a další exaktní vědy důležitá a popíšeme si několik zajímavých historických událostí a objevů.

1 Strojové myšlení a logika

Mohou stroje myslet? To je složitá otázka, na kterou není jednoduchá odpověď. Problém strojového myšlení úzce souvisí s matematickou logikou.[1] To je pochopitelné a dokonce můžeme říct, že je to přirozené a nutné. Řekneme-li o stroji (o počítači), že myslí, míníme tím, že dělá to, co bychom u člověka nazvali myšlením. Člověk ale myslí podle pravidel logiky. To je na jednu stranu tvrzení poněkud nadsazené, protože lidské myšlení je složité a zahrnuje i řadu faktorů, které jsou logikou postižitelné jen v omezené míře nebo vůbec. Na druhou stranu logika vznikla proto, aby alespoň v základních rysech lidské myšlení popsala, a představuje dnes solidní základ. Chceme-li sestrojit stroj (naprogramovat počítač), který má myslet, musíme se o nějaký pevný základ opřít a logika se jako takový základ nabízí.[2]

Strojové myšlení využívá symbolický charakter logiky. Jak víme, je logická formule, např. $(p \wedge q) \to r$, posloupností symbolů, tedy v našem případě symbolů $($, p, $\wedge$ atd. Takové posloupnosti lze v počítači snadno reprezentovat. Navíc lze logické usuzování prováděné s formulemi chápat jako manipulaci se symboly, která probíhá podle jednoduchých pravidel. Počítač je schopen takové manipulace rychle provádět. Právě popsaný proces, ve kterém se z formulí pomocí jistých pravidel odvozují nové formule, je v logice znám jako formální dokazování a je základem axiomatické metody, se kterou se teď seznámíme.

[1] V angličtině se používá termín „reasoning“, který je zřejmě poněkud výstižnější než český termín „myšlení“, který používáme. Další možností v češtině je termín „usuzování“. Význam termínu „reasoning“ leží někde mezi významy termínů „usuzování“ a „myšlení“.

Používáme termín „strojové myšlení“, který používá poněkud zastaralý termín „stroj“. Počítačům se totiž dříve říkalo výpočetní stroje nebo matematické stroje a odtud tento termín pochází. V jistých spojeních se termín „stroj“ (anglicky „machine“) stále používá. Hovoříme například o strojovém učení (machine learning), o strojové inteligenci (machine intelligence) a podobně.

[2] Není to jistě jediný možný základ. Alternativou jsou například tzv. umělé neuronové sítě, které vycházejí z principů činnosti lidského mozku. Nicméně strojové myšlení na bázi logiky dosáhlo větších úspěchů než zmíněné alternativy.

2 Axiomatizace výrokové logiky

V běžném životě argumentujeme tak, že vycházíme z jistých tvrzení, která považujeme za platná, z nich odvodíme další tvrzení, z nich pak další, až se nakonec dostaneme k tvrzení, které je nějak zajímavé. O tom tvrzení řekneme, že jsme ho prokázali (nebo dokázali).

Uveďme jednoduchý příklad. Víme, že když prší, pak jsou silnice mokré. Zjistíme, že prší. Z toho odvodíme, že silnice jsou mokré. Navíc zjistíme, že teplota je kolem nuly. Protože víme, že jestliže jsou silnice mokré a teplota je kolem nuly, hrozí nebezpečí smyku, odvodíme nakonec, že hrozí nebezpečí smyku.

Provedli jsme tři úsudky. První lze graficky znázornit takto:

$$\frac{\text{Prší.}\qquad \text{Jestliže prší, pak jsou silnice mokré.}}{\text{Silnice jsou mokré.}}$$

Druhý takto:

$$\frac{\text{Silnice jsou mokré.}\qquad \text{Teplota je kolem nuly.}}{\text{Silnice jsou mokré a teplota je kolem nuly.}}$$

Třetí takto:

$$\frac{\text{Silnice jsou mokré a teplota je kolem nuly.}\qquad \text{Jestliže jsou silnice mokré a teplota je kolem nuly, pak hrozí nebezpečí smyku.}}{\text{Hrozí nebezpečí smyku.}}$$

K logickému odvození tvrzení „Hrozí nebezpečí smyku.“ jsme tedy použili následující tvrzení, která jsme považovali za platná:

Prší.
Teplota je kolem nuly.
Jestliže prší, pak jsou silnice mokré.
Jestliže jsou silnice mokré a teplota je kolem nuly, pak hrozí nebezpečí smyku.

a tři výše uvedené úsudky.

Všimněme si, že první a třetí úsudek mají stejný tvar, stejnou formu, kterou můžeme vyjádřit schématem

$$\frac{\begin{array}{l}\varphi\\ \varphi \to \psi\end{array}}{\psi},$$

popř. úsporněji zapsaným

$$\frac{\varphi, \varphi \to \psi}{\psi} \tag{1}$$

a čteme ho následovně:

z φ a $\varphi \to \psi$ odvoď ψ.

Formu druhého úsudku můžeme podobně vyjádřit schématem

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi},$$

popř.

$$\frac{\varphi, \psi}{\varphi \wedge \psi}. \tag{2}$$

Takovým schématům se v logice říká odvozovací pravidla (někdy inferenční nebo také dedukční pravidla). Uvedená odvozovací pravidla jsou takzvaně korektní. To znamená, že bez ohledu na obsah tvrzení φ a ψ platí, že když jsou předpoklady těchto pravidel pravdivé, je pravdivý i závěr pravidla.

Vysvětleme si to na prvním pravidle, tj. na pravidle (1). Podíváme-li se na následující tabulku pravdivostních hodnot, vidíme, že kdykoli jsou φ i $\varphi \to \psi$ pravdivé (což v tomto případě nastává jen v posledním řádku tabulky), je pravdivé i ψ.

φ	ψ	$\varphi \to \psi$
0	0	1
0	1	1
1	0	0
1	1	1

(3)

Tato vlastnost pravidla se tedy nazývá korektnost. Uvědomme si, že korektnost tohoto pravidla znamená, že

$$\varphi, \varphi \to \psi \models \psi,$$

tedy že závěr ψ sémanticky vyplývá z předpokladů φ a $\varphi \to \psi$.

Pravidlo (1), které je nejdůležitějším odvozovacím pravidlem v logice, se nazývá pravidlo *modus ponens*, česky pravidlo odloučení. Je to pravidlo, které denodenně používáme v běžném životě,[3] viz příklady:

Mám 30 korun.
Jestliže mám 30 korun, pak si můžu koupit čokoládu.
———
Můžu si koupit čokoládu.

Mám vysokoškolský diplom.
Když mám vysokoškolský diplom, budu mít vysoký plat.
———
Budu mít vysoký plat.

Všimněme si, že druhý z právě uvedených úsudků je poněkud zvláštní. Vyvolá přinejmenším zvednuté obočí, možná dokonce výtku, že takový úsudek není správný. Vždyť samotný diplom z vysoké školy žádnou záruku ohledně platu nedává, záleží na tom, jaká je to škola, jaký mám vystudovaný obor a jak jsem ke studiu přistupoval. To je pravda, přesto je uvedený úsudek správný. Problém je v druhém předpokladu, tj. tvrzení „Když mám vysokoškolský diplom, budu mít vysoký plat.“, který je nepravdivý.[4] Vidíme tedy, že pokud korektní odvozovací pravidlo použijeme na nepravdivé předpoklady, můžeme odvodit nepravdivé tvrzení.

Pravidlem *modus ponens* lze tedy mechanicky odvodit tvrzení ψ, kdykoli považujeme za prokázaná (platná) tvrzení φ a $\varphi \to \psi$. Nezáleží při tom na obsahu (smyslu) tvrzení φ a ψ. Pravidlo je čistě syntaktické, při odvození záleží jen na formě (tvaru) předpokladů pravidla, tj. na syntaktických aspektech, nikoli na obsahu těchto předpokladů, tj. na sémantických aspektech.

Stejným způsobem se přesvědčíme, že i pravidlo[5]

$$\frac{\varphi, \psi}{\varphi \wedge \psi}$$

je korektní, tedy, že kdykoli jsou pravdivé oba předpoklady, φ a ψ, je pravdivý i závěr, $\varphi \wedge \psi$. To plyne přímo z pravdivostní tabulky spojky konjunkce.

Uvažujme však pravidlo

$$\frac{\psi, \varphi \to \psi}{\varphi}.$$

Tomu se říká pravidlo abdukce.[6] Není to korektní pravidlo, jak je vidět z výše uvedené pravdivostní tabulky (3): Ve druhém řádku mají oba předpoklady, ψ i $\varphi \to \psi$, hodnotu 1, ale závěr, φ, má hodnotu 0. Uvědomme si, co to prakticky znamená: Použitím pravidla abdukce bychom mohli z pravdivých předpokladů odvodit nepravdivý závěr. Například z tvrzení „Jestliže prší, pak jsou silnice mokré.“ a „Silnice jsou mokré.“ bychom odvodili tvrzení „Prší.“ Přitom silnice mohou být mokré proto, že je namokřil kropicí vůz.

Usuzování lze chápat jako opakované provádění elementárních úsudků, jako např. výše popsaného úsudku podle pravidla *modus ponens*. Odkud se berou předpoklady těchto úsudků? Takové předpoklady lze rozdělit následovně:

1. Tvrzení, která jsou pravdivá vždy, a to kvůli jejich logické struktuře. Říká se jim logické axiomy, popř. jen axiomy.
2. Tvrzení, která nemusí být vždy pravdivá, ale v daném kontextu je předpokládáme. Říká se jim speciální axiomy.
3. Tvrzení, která byla odvozena pomocí úsudků provedených dříve.

Příkladem logického axiomu je tvrzení „Prší nebo neprší.“ To je pravdivé vždy, protože každé tvrzení tvaru $\varphi \vee \neg\varphi$ je vždy pravdivé (formule tvaru $\varphi \vee \neg\varphi$ je tautologie). Příkladem speciálního axiomu je tvrzení „Teplota je kolem nuly.“ To je tvrzení, které nemusí být – na rozdíl od předchozího tvrzení „Prší nebo neprší.“ – vždy pravdivé. My nicméně toto tvrzení předpokládáme, např. proto, že jsme ho zjistili nebo jsme z jiného důvodu přesvědčeni o jeho pravdivosti. Všem speciálním axiomům, které v dané situaci uvažujeme, se v logice říká teorie a značí se obvykle T (tj. T je množina tvrzení, speciálních axiomů). Opakovaným používáním

[3] Kdybychom se měli shodnout na tom, které odvozovací pravidlo používáme v běžném životě nejčastěji, popř. bez kterého bychom se těžko obešli, bylo by to patrně pravidlo *modus ponens*. V tomto smyslu je třeba chápat to, co jsme uvedli v předchozí větě, totiž že je to nejdůležitější odvozovací pravidlo. Z formálního hlediska je toto pravidlo prostě korektním pravidlem, stejně jako mnoho jiných pravidel, viz také níže.

[4] Úsudek podle daného pravidla může být jen správný (pokud odpovídá schématu odvozovacího pravidla), nebo nesprávný (pokud schématu neodpovídá). Úsudek nemůže být, na rozdíl od tvrzení, pravdivý nebo nepravdivý.

[5] Pravidlo se někdy nazývá pravidlo zavedení konjunkce.

[6] Toto pravidlo má význam pro tzv. abduktivní usuzování, kterým se v tomto seriálu nezabýváme. My se z tohoto pohledu zabýváme usuzováním deduktivním.

odvozovacích pravidel na logické axiomy, speciální axiomy a výsledky předchozího odvozování tak tvoříme posloupnost tvrzení, na jejímž konci je tvrzení φ, které jsme chtěli prokázat. Takové posloupnosti tvrzení se v logice říká důkaz. Uvědomme si, že to je zcela přirozený pojem.[7] Vraťme se k našemu příkladu se třemi úsudky o mokrých silnicích. Důkazem v tomto případě je následující posloupnost:

Prší.
Jestliže prší, pak jsou silnice mokré.
Silnice jsou mokré.
Teplota je kolem nuly.
Silnice jsou mokré a teplota je kolem nuly.
Jestliže jsou silnice mokré a teplota je kolem nuly, pak hrozí nebezpečí smyku.
Hrozí nebezpečí smyku.

V tomto důkazu jsou první a druhé tvrzení speciální axiomy, třetí je z nich odvozeno pravidlem *modus ponens*, čtvrté je speciálním axiomem, páté je odvozeno třetího a čtvrtého odvozovacím pravidlem (2), šesté je speciálním axiomem, sedmé – tedy dokázané tvrzení – je odvozené z předchozích dvou pomocí *modus ponens*.

To, co jsme právě popsali, se týká úsudků, které běžně provádíme a které můžeme popsat v přirozeném jazyce. Stejným způsobem se v matematické logice přistupuje k usuzování ve formálních logických systémech, tedy i v systému výrokové logiky, kterým se zabýváme. Popišme si teď jednotlivé složky.

Axiomatický systém výrokové logiky, který teď popíšeme, používá *modus ponens* jako jediné odvozovací pravidlo. Má následující tři *logické axiomy*:

$$\varphi \to (\psi \to \varphi) \tag{4}$$
$$(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) \tag{5}$$
$$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi) \tag{6}$$

Snadno ověříme, že každý z těchto axiomů je tautologie, tj. vždy pravdivá formule, a jejich volba je tedy v souladu s tím, co jsme uvedli výše. (Ověřte pomocí tabulky pravdivostních hodnot, že skutečně jde o tautologie.) Platí ovšem i značně netriviální a pozoruhodné tvrzení, kterému se budeme věnovat níže, totiž že každou jinou tautologii lze z těchto tří axiomů dokázat. To v tuto chvíli uvádíme, jen abychom zdůvodnili volbu těchto axiomů. *Teorie* v našem systému je libovolná množina T formulí, které se nazývají *speciální axiomy*. Teorie může být i prázdná, tj. $T = \emptyset$.

Přesněji řečeno, axiomem je každá formule, které má jeden z těchto tří uvedených tvarů, tedy formule, která vznikne z (4), (5) nebo (6) nahrazením symbolů φ, ψ a χ libovolnými formulemi.[8] Tedy například z (4) vznikne pro $\varphi = p$ a $\psi = q$ axiom

$$p \to (q \to p).$$

Nahrazením $\varphi = p$ a $\psi = (p \to p)$ vznikne jiný axiom, totiž

$$p \to ((p \to p) \to p).$$

Poznamenejme dále, že za axiomy lze zvolit i jiné formule, pokud mají vhodné vlastnosti (je přirozeně rozumné, aby měly výše uvedené vlastnosti, tj. jsou to tautologie a každou jinou tautologii z nich lze odvodit).

Přistoupíme nyní k pojmu důkaz. *Důkaz* formule φ z daných logických axiomů (4), (5) a (6) a z teorie T je libovolná posloupnost $\varphi_1, \dots, \varphi_n$, pro kterou platí, že $\varphi_n = \varphi$ a každá φ_i

1. je logickým axiomem,
2. nebo je speciálním axiomem, tj. je formulí z T,
3. nebo plyne z předchozích formulí důkazu pomocí odvozovacího pravidla *modus ponens*.

Formule se nazývá *dokazatelná* z logických axiomů (4), (5) a (6) a z teorie T, existuje-li důkaz této formule z těchto logických axiomů a z T. Tuto skutečnost zapisujeme

$$T \vdash \varphi.$$

Uveďme si nyní příklad důkazu. Dokážeme, že libovolná formule tvaru $\varphi \to \varphi$ je dokazatelná z logických axiomů a z libovolné teorie T, tedy i prázdné ($T = \emptyset$). Dokážeme tedy, že $\emptyset \vdash \varphi \to \varphi$. V takovém případě symbol „$\emptyset$“ vynecháváme, a píšeme tedy jen

$$\vdash \varphi \to \varphi. \tag{7}$$

Máme ukázat, že existuje důkaz, který vychází jen z logických axiomů a jehož posledním prvkem je $\varphi \to \varphi$. Aby se nám nepletl symbol „φ“ se symbolem použitým v logických axiomech, budeme dokazovat $A \to A$, kde A je libovolná formule.

První formulí důkazu je

$$A \to ((A \to A) \to A).$$

To je axiom, protože vznikne z (4) substitucí $\varphi = A$ a $\psi = (A \to A)$, a jako takový může tedy být členem důkazu.

Druhou formulí důkazu je

$$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)).$$

To je opět axiom, protože vznikne z (5) substitucí $\varphi = A$, $\psi = (A \to A)$, $\chi = A$. Jako třetí formuli důkazu přidáme

$$(A \to (A \to A)) \to (A \to A),$$

což můžeme provést, protože tuto formuli lze odvodit z první a druhé pomocí *modus ponens*. Čtvrtou formulí je

$$A \to (A \to A),$$

což je axiom, protože vznikne z (4) substitucí $\varphi = A$ a $\psi = A$.

Ze čtvrté a třetí formule důkazu nakonec pomocí *modus ponens* odvodíme formuli

$$A \to A,$$

kterou jsme měli dokázat a kterou přidáme jako poslední, pátou formuli důkazu. Posloupnost těchto pěti formulí je důkazem formule $A \to A$.

Na tomto příkladu vidíme, že důkaz i poměrně jednoduché formule, jako je $\varphi \to \varphi$, může být poměrně dlouhý. O to ale teď nejde. Jde o to, které formule vůbec důkaz mají, a tedy jsou dokazatelné.

Uvědomme si teď důležitou skutečnost. Na jedné straně máme pojem sémantického vyplývání: $T \models \varphi$ znamená, že při každém pravdivostním ohodnocení, při kterém jsou

[7] Zkuste se zamyslet nad tím, jak byste přesně definovali pojem důkaz nějakého tvrzení bez ohledu na to, co jsme si teď řekli. Pravděpodobně dojdete k podobné definici jako je ta, kterou jsme právě uvedli.

[8] (4), (5) a (6) jsou přísně vzato schémata, a ne konkrétní axiomy. Proto se někdy nazývají axiomová schémata. My budeme dále říkat axiomy.

všechny formule z množiny T pravdivé, je pravdivá i formule φ. Na druhé straně máme pojem dokazatelnosti: $T \vdash \varphi$ znamená, že formule φ je dokazatelná z logických axiomů a z formulí z množiny T pomocí pravidla *modus ponens*. $T \vdash \varphi$ má tedy zcela jinou povahu než $T \models \varphi$. Zatímco $T \models \varphi$ je sémantický pojem, $T \vdash \varphi$ je pojem syntaktický. Mezi oběma pojmy však existuje důležitá souvislost, kterou nyní popíšeme.

Z toho, co jsme si výše uvedli, je zřejmé, že *modus ponens* zachovává pravdivost v tom smyslu, že jsou-li předpoklady φ a $\varphi \to \psi$ pravdivé (při nějakém ale libovolném pravdivostním ohodnocení e), je pravdivý (při tomto ohodnocení e) i závěr ψ. Uvažujme libovolné ohodnocení e, při kterém jsou pravdivé všechny formule z T. Logické axiomy jsou vždy pravdivé, a tedy i při ohodnocení e. Pokud z logických axiomů a z formulí z množiny T odvodíme, tedy dokážeme, nějakou formuli φ, musí tedy tato formule být při ohodnocení e pravdivá. Ukázali jsme tak první část vztahu mezi sémantickým vyplýváním a dokazatelností:

Věta 1 (o korektnosti)**.** *Jestliže $T \vdash \varphi$, pak $T \models \varphi$. Tedy, jestliže φ je z T (a z logických axiomů) dokazatelná, pak φ z T sémanticky vyplývá.*

Zatímco větu o korektnosti lze snadno dokázat, obrácené tvrzení, tzv. věta o úplnosti, je mnohem hlubší a jeho důkaz vynecháme:

Věta 2 (o úplnosti)**.** *Jestliže $T \models \varphi$, pak $T \vdash \varphi$. Tedy, jestliže φ z T sémanticky vyplývá, pak je φ z T (a z logických axiomů) dokazatelná.*

Uvědomme si, co tyto věty říkají v případě $T = \emptyset$ (T neobsahuje žádný speciální axiom). Pak $T \models \varphi$ znamená, že φ je pravdivá při každém pravdivostním ohodnocení, tedy že φ je tautologie, a $T \vdash \varphi$ znamená, že φ je dokazatelná jen z logických axiomů. Věta o korektnosti a věta o úplnosti tedy v tomto případě říkají, že formule je tautologie, právě když je dokazatelná z uvedených tří logických axiomů.

Pojem pravdivosti a vyplývání formule lze tedy zjistit čistě syntaktickými prostředky, manipulací se symboly. Toto propojení sémantické a symbolické roviny logiky, které existuje nejen ve výrokové logice, ale i v dalších formálních systémech, patří mezi nejdůležitější výsledky logiky.

Další informace k axiomatizaci výrokové logiky a systémů, které jsou rozšířením klasické výrokové logiky, může čtenář najít v knihách [2, 3].

3 Automatické počítačové dokazování a rezoluční metoda

Formální dokazování v logice lze chápat jako odvozování nových znalostí ze znalostí, které máme k dispozici. Najdeme-li důkaz formule φ z množiny T předpokladů, můžeme se na věc dívat tak, že T představuje bázi znalostí, tj. množinu tvrzení týkajících se nějakého problému nebo oblasti, a že φ je nový poznatek, který jsme z této báze znalostí odvodili. Tím se nejen dozvíme nový poznatek φ, ale také zdůvodnění, proč tento poznatek z naší báze znalostí vyplývá. Tímto zdůvodněním je pochopitelně nalezený důkaz. Najde-li takový důkaz počítač, tj. automaticky bez pomoci člověka, můžeme říct, že počítač něco sám z našich znalostí logicky odvodil, tedy vymyslel.

Ukažme si jednoduchý příklad. V tomto příkladu opustíme svět výrokové logiky a nakročíme do světa predikátové logiky. To proto, že úvahy o odvozování nových znalostí mají význam zejména ve světě predikátové logiky. Predikátová logika je rozšířením výrokové logiky v tom, že její formule mohou vypovídat o vztazích (relacích) mezi objekty.[9] Například výraz $(\forall X)\,(X \leq X+1)$ nebo výraz $\mathrm{syn}(\mathrm{petr},\mathrm{jan})$ jsou formule predikátové logiky, jejichž význam nelze dost dobře vyjádřit formulemi výrokové logiky. První z nich říká, že pro každé X je X menší nebo rovno $X+1$, druhá říká, že individuum (objekt) petr je synem individua jan (v našem kontextu je zvykem objekty a relace označovat malými písmeny, velkými pak proměnné). Představme si, že báze znalostí, tedy množina formulí T, obsahuje následující formule:

$$
\begin{aligned}
&\mathrm{syn}(X,Y) \wedge \mathrm{muz}(Y) \to \mathrm{otec}(Y,X),\\
&\mathrm{syn}(X,Y) \wedge \mathrm{zena}(Y) \to \mathrm{matka}(Y,X),\\
&\mathrm{otec}(X,Y) \to \mathrm{potomek}(Y,X),\\
&\mathrm{matka}(X,Y) \to \mathrm{potomek}(Y,X),\\
&\mathrm{potomek}(X,Y) \wedge \mathrm{potomek}(Y,Z) \to \mathrm{potomek}(X,Z),\\
&\vdots\\
&\mathrm{muz}(\mathrm{petr}), \mathrm{muz}(\mathrm{pavel}),\\
&\mathrm{zena}(\mathrm{alena}), \mathrm{zena}(\mathrm{eva}), \mathrm{zena}(\mathrm{jana}),\\
&\mathrm{syn}(\mathrm{petr},\mathrm{alena}), \mathrm{syn}(\mathrm{pavel},\mathrm{alena}),\\
&\mathrm{matka}(\mathrm{jana},\mathrm{alena}),\\
&\mathrm{potomek}(\mathrm{jana},\mathrm{eva}),\\
&\vdots
\end{aligned}
$$

První skupina formulí popisuje (částečně) rodinné vztahy. První formule říká, že je-li osoba X synem osoby Y a je-li osoba Y muž, pak je Y otcem X. Podobně další formule této skupiny, včetně poslední, která říká, že je-li X potomkem Y a je-li Y potomkem Z, pak X je potomkem Z. Druhá skupina popisuje konkrétní instance některých relací, tedy např. že osoba petr je synem osoby alena. Pak nás může zajímat, zda z takové báze znalostí lze dokázat, a tedy zda z ní vyplývá, například to, že petr je potomkem evy. V termínech logiky se tedy ptáme, zda z uvedené množiny formulí T je dokazatelná formule $\mathrm{potomek}(\mathrm{petr},\mathrm{eva})$, tj. zda

$$T \vdash \mathrm{potomek}(\mathrm{petr},\mathrm{eva}).$$

Intuitivně nahlédneme, že to tak je (nebudeme se pouštět do přesné formalizace predikátové logiky). Přesný formální důkaz by byl přepisem následujícího argumentu: Podle báze znalostí je petr synem aleny a vzhledem k tomu, že alena je žena, je dle druhé formule matkou petra. Podle čtvrté formule je tedy petr potomkem aleny. Jana je matkou aleny, podle čtvrté formule je tedy alena potomkem jany. Podle páté formule je tedy petr potomkem jany. Protože je také jana potomkem evy, je podle páté formule petr potomkem evy.

Jak má ale počítač takový důkaz najít? Ptáme se tedy, zda existuje efektivní algoritmus, který je schopný rozhodnout, zda formule φ je dokazatelná z předpokladů T. Takový algoritmus bohužel obecně neexistuje (více v příští kapitole). Pro speciální případy, které pokrývají prakticky významné problémy i výše uvedený jednoduchý příklad, však prakticky

[9] Tento text je třeba brát jako kratičké nahlédnutí do toho, o čem predikátová logika pojednává. Podrobné informace o predikátové logice najde čtenář například v knihách [2, 3].

uspokojivé algoritmy byly navrženy. Ty se staly základem různých systémů automatického počítačového dokazování i základem programovacího jazyka Prolog, který má význam pro umělou inteligenci. Lze v něm totiž vyvíjet takzvané expertní systémy, tedy počítačové programy, do kterých může expert, například lékař nebo geolog, vložit logicky popsané poznatky o daném problému, například o diagnostice nemocí. Lékař pak může do systému vložit informace o konkrétním pacientovi a expertní systém z báze znalostí a z informací o pacientovi automaticky odvodí diagnózu pacienta, popř. si vyžádá dodatečná vyšetření. Takový systém má lékaři pomoci v určení správné diagnózy.

Programovacímu jazyku Prolog bude věnován některý z příštích kurzů tohoto semináře. Zájemcům doporučujeme knihu [1]. Ukážeme si nicméně základní princip automatického dokazování, na kterém jsou Prolog i jiné systémy založeny. Tímto principem je tzv. *rezoluční metoda*. Nebudeme popisovat obecnou rezoluční metodu, ale její zjednodušenou variantu, která z ní vznikne, omezíme-li se na systém výrokové logiky.

Rezoluční metoda vychází z toho, že báze znalostí obsahuje dva typy formulí. První jsou tzv. pravidla, což jsou formule tvaru

$$p_1 \wedge \cdots \wedge p_n \ \rightarrow \ p, \tag{8}$$

tedy implikace, které říkají, že když platí $p_1, p_2, \ldots, p_n$, pak platí p. Druhým typem jsou fakta, což jsou formule tvaru

$$p, \tag{9}$$

které zastupují elementární tvrzení (výroky). Naše znalosti totiž skutečně formulujeme nejčastěji prostřednictvím výše uvedených pravidel a faktů. Oba tyto typy formulí lze nahlížet jako speciální případy takzvaných hornovských klauzulí. Přesněji řečeno, každé pravidlo je logicky ekvivalentní nějaké hornovské klauzuli, stejně tak je to s fakty. *Hornovská klauzule* je přitom disjunkce výrokových symbolů a negací výrokových symbolů, která obsahuje nejvýše jeden výrokový symbol bez negace. Hornovská klauzule ekvivalentní pravidlu (8) je

$$\neg p_1 \vee \cdots \vee \neg p_n \vee p.$$

(Ověřte to.) Fakt, tedy formule (9), je sám o sobě hornovskou klauzulí. Výrokové symboly a jejich negace se nazývají *literály*; literál je *pozitivní*, pokud neobsahuje negaci, je *negativní*, pokud obsahuje negaci. Výrazy p a $\neg p_i$ jsou tedy literály, přitom p je pozitivní a $\neg p_i$ negativní. Jinými slovy, hornovská klauzule je libovolná disjunkce

$$L_1 \vee \cdots \vee L_n,$$

kde L_i jsou literály, přičemž nejvýše jeden z těchto literálů je pozitivní. Taková klauzule se v rezolučním dokazování označuje také

$$\{L_1, \ldots, L_n\},$$

protože rezoluční metoda pracuje s hornovskými klauzulemi jako s množinami literálů.

Základem rezoluční metody je tzv. *rezoluční pravidlo*. To je odvozovací pravidlo, podobně jako je odvozovacím pravidlem *modus ponens*. Rezoluční pravidlo vypadá takto:

$$\frac{\begin{array}{c}\{L_1, \ldots, L_{i-1}, p, L_{i+1}, \ldots, L_n\} \\ \{L'_1, \ldots, L'_{j-1}, \neg p, L'_{j+1}, \ldots, L'_m\}\end{array}}{\{L_1, \ldots, L_{i-1}, L_{i+1}, \ldots, L_n, L'_1, \ldots, L'_{j-1}, L'_{j+1}, \ldots, L'_m\}}$$

Tedy pokud jedna klauzule obsahuje pozitivní literál p a druhá negativní literál $\neg p$, odvodíme klauzuli, která vznikne odstraněním literálů p a $\neg p$ a sloučením obou klauzulí. Tato klauzule se nazývá *rezolventa* první a druhé klauzule. Příkladem použití tohoto pravidla je následující úsudek:

$$\frac{\begin{array}{c}\{\neg p, \neg q, r\} \\ \{\neg r, \neg s, t\}\end{array}}{\{\neg p, \neg q, \neg s, t\}}$$

Uvědomme si, že takový úsudek je přirozený. První klauzule totiž reprezentuje implikaci $p \wedge q \rightarrow r$, druhá implikaci $r \wedge s \rightarrow t$. Odvozená klauzule reprezentuje $p \wedge q \wedge s \rightarrow t$, což je přirozený důsledek uvedených implikací. Všimněme si také, že *modus ponens* lze chápat jako speciální případ rezolučního pravidla: p a $p \rightarrow q$ jsou ekvivalentní klauzulím p a $\neg p \vee q$, ze kterých lze rezolučním pravidlem odvodit q.

Uveďme dále, že za hornovskou klauzuli je považována i „prázdná klauzule“, tedy $\{\ \}$. Ta má v rezoluční metodě důležitou roli, protože signalizuje nalezení důkazu. Označme nyní F libovolnou konečnou množinu hornovských klauzulí a dále symbolem $R(F)$ množinu všech klauzulí, které z nich lze použitím rezolučního pravidla odvodit. Tedy pokud

$$F = \{\{\neg p, \neg q, r\}, \{\neg r, \neg s, t\}, \{p\}\},$$

pak

$$R(F) = \{\{\neg p, \neg q, \neg s, t\}, \{\neg q, r\}\},$$

protože kromě výše popsaného odvození formule $\{\neg p, \neg q, \neg s, t\}$ lze z formulí $\{\neg p, \neg q, r\}$ a $\{p\}$, které jsou obě v F, odvodit i formuli $\{\neg q, r\}$. Jiné formule z F odvodit nelze. Operaci odvození R lze provádět opakovaně. Označme symbolem $R^n(F)$ množinu všech možných výsledků odvození, provedených v nejvýše n krocích z počáteční množiny F, tedy

$$R^0(F) = F \quad \text{a} \quad R^{n+1}(F) = R^n(F) \cup R(R^n(F)).$$

Je tedy například

$$R^3(F) = F \cup R(F) \cup R(R(F)) \cup R(R(R(F))).$$

Smysluplnost rezoluční metody je založena na následující větě, kterou uvedeme bez důkazu:

Věta 3. *Fakt p vyplývá z množiny F hornovských klauzulí, právě když existuje $n \geq 0$ tak, že množina $R^n(F \cup \{\{\neg p\}\})$ obsahuje prázdnou klauzuli $\{\ \}$.*

Přitom „vyplývá“ znamená, že vyplývá sémanticky (což je, jak víme dle věty o korektnosti a úplnosti, ekvivalentní s tím, že p je dokazatelné z F v axiomatickém systému). Tato věta má pro rezoluční metodu zásadní význam. Říká totiž, že zjistit, zda tvrzení reprezentované formulí p je dokazatelné z báze znalostí reprezentované konečnou množinou F (tedy z nějakých faktů a pravidel) je možné systematickým prohledáváním všech možných rezolvent, které se vytvářejí z klauzulí z množiny F a z klauzule $\{\neg p\}$.[10] Uvědomme si také, že taková metoda skončí, protože vzhledem k tomu, že F je konečná, obsahuje jen konečný počet výrokových symbolů a z nich lze utvořit jen konečně mnoho klauzulí. Proces

[10] $\{\neg p\}$ je výše uvedeným způsobem zapsaná hornovská klauzule (disjunkce sestávající z $\neg p$ jako jediného literálu).

generování nových klauzulí tedy musí jednou skončit, tedy dostat se do stavu, kdy už nové klauzule nepřibývají.[11]

Rezoluční metodu si nyní ukážeme na příkladu. Úkolem je pomocí rezoluční metody zjistit, zda formule q vyplývá z následující množiny pravidel a faktů:

$$p$$
$$t$$
$$w$$
$$p \wedge r \rightarrow u$$
$$u \wedge v \rightarrow q$$
$$t \rightarrow r$$
$$p \wedge w \rightarrow v$$

Začneme počítat množiny $R^n(F \cup \{\{\neg q\}\})$, kde F je množina hornovských klauzulí odpovídajících výše uvedeným faktům a pravidlům; pro stručnost budeme psát jen R^n. Množina $F \cup \{\{\neg q\}\}$ výchozích klauzulí tedy obsahuje tyto klauzule:

$$\{p\}$$
$$\{t\}$$
$$\{w\}$$
$$\{\neg p, \neg r, u\}$$
$$\{\neg u, \neg v, q\}$$
$$\{\neg t, r\}$$
$$\{\neg p, \neg w, v\}$$
$$\{\neg q\}$$

V prvním kroku získáme jako nové rezolventy, které přibudou do R^1, tyto klauzule:

$$\{\neg r, u\}$$
$$\{\neg w, v\}$$
$$\{r\}$$
$$\{\neg p, v\}$$
$$\{\neg p, \neg r, \neg v, q\}$$
$$\{\neg p, u, \neg t\}$$
$$\{\neg u, q, \neg p, \neg w\}$$
$$\{\neg u, \neg v\}$$

Například první z těchto rezolvent vznikne použitím rezolučního pravidla na klazule $\{p\}$ a $\{\neg p, \neg r, u\}$ z předchozího seznamu. Nebudeme dále vypisovat všechny klauzule, které by následně vznikaly. Všimneme si jen toho, že do R^2 přibudou i klauzule

$$\{u\} \text{ a } \{v\}.$$

První vznikne z dříve odvozených klauzulí $\{\neg r, u\}$ a $\{r\}$, druhá z klauzulí $\{w\}$ a $\{\neg w, v\}$. Do R^3 pak přibude klauzule $\{\neg v, q\}$, která vznikne z $\{\neg u, \neg v, q\}$ a $\{u\}$. Do R^4 přibude $\{q\}$, která vznikne z $\{\neg v, q\}$ a z $\{v\}$. Z $\{q\}$ a z $\{\neg q\}$ pak vznikne prázdná klauzule, $\{\ \}$, která bude přidána do R^5. Protože jsme odvodili prázdnou klauzuli, výpočet v souladu s větou 3 ukončíme se závěrem, že q z dané množiny pravidel a faktů vyplývá.

[11] V praxi totiž mohou být množiny $R^n(F)$ značně velké, což prohledávání všech možných rezolvent zpomaluje. Byly tedy navrženy různé strategie prohledávání. Těmi se zde nezabýváme.

Úkol 1 *10 bodů*

Rozhodněte, zda jsou následující odvozovací pravidla korektní. Odpověď zdůvodněte.

$$\frac{\varphi \rightarrow \psi, \neg\psi}{\neg\varphi}$$

$$\frac{\neg\varphi \leftrightarrow \neg\psi, \psi \leftrightarrow \chi}{\varphi \leftrightarrow \chi}$$

$$\frac{\varphi \rightarrow (\psi \vee \chi)}{\varphi \rightarrow \psi}$$

$$\frac{\varphi \rightarrow \psi}{\varphi \rightarrow (\psi \vee \chi)}$$

Úkol 2 *15 bodů*

Rozhodněte pomocí rezoluční metody, zda q vyplývá z dané množiny pravidel a faktů. Uveďte příslušný výpočet.

(a) Množinou pravidel a faktů je:

$$p \rightarrow s$$
$$s \rightarrow p$$
$$s \rightarrow q$$
$$u \wedge v \rightarrow p$$
$$u$$
$$v$$

(b) Množinou pravidel a faktů je:

$$p \wedge r \rightarrow q$$
$$q \rightarrow r$$
$$s \rightarrow p$$
$$s$$

4 Historické poznámky a zajímavosti

Axiomatická metoda vznikla v antice v pracích řeckých geometrů, zejména Euklida (asi 325–260 př. n. l.). Do popředí zájmu se dostala v době bouřlivého rozvoje matematické logiky v 1. polovině 20. století. Větu o úplnosti pro výrokovou logiku dokázali nezávisle na sobě švýcarský matematik Paul Bernays (1888–1977) a americký logik Emil Post (1897–1954).[12] Důkaz věty o úplnosti pro predikátovou logiku, který je značně složitější, podal zřejmě největší logik 20. století Kurt Gödel (1906–1978).[13] Skutečnost, že pro predikátovou logiku neexistuje žádný algoritmus, který by v obecném případě dokázal rozhodnout, zda daná formule je dokazatelná z dané množiny formulí, dokázal anglický matematik a informatik Alan M. Turing (1912–1954). To byl průlomový výsledek. Odhalil meze, kterých si při používání

[12] P. Bernays, Beiträge zur axiomatischen Behandlung des Logik-Kalküls. Habilitační práce (Habilitationsschrift), Universität Göttingen, 1918. E. Post, Introduction to a general theory of elementary propositions. American J. Math 43 (3)(1921): 163–185.

[13] Die Vollständigkeit der Axiome des logischen Funktionenkalküls. Monatshefte für Mathematik und Physik 37(1930): 349–360.

logiky musíme být vědomi. Obecný dokazovací algoritmus tedy neexistuje. Proto byla později pozornost věnována různým heuristickým algoritmům a algoritmům pro automatické dokazování pro speciální, ne zcela obecné, avšak prakticky důležité formální systémy. Jedním z výsledků tohoto zkoumání byla i rezoluční metoda, jejíž základy vypracoval americký matematik, informatik a filozof John Alan Robinson (1930–2016) v 60. letech minulého století.

Studium axiomatické metody a automatického dokazování bylo od 2. poloviny 20. století motivováno zejména snahou o sestrojení myslícího počítače. V 1. polovině 20. století však byla axiomatická metoda studována zejména proto, že se v matematice objevily vážné problémy. Ty ukazovaly, že matematika potřebuje pevné formální základy. Logika a axiomatická metoda budování matematiky od základních pojmů a tvrzení ke složitějším se nabízela jako přirozená varianta. Do té doby se totiž matematika pěstovala neformálně. Nikdo si například příliš nelámal hlavu s tím, jak definovat pojem množina. Na problémy takového neformálního přístupu, který je založen na intuitivním chápání množiny (množina je intuitivně soubor nějakých prvků), důrazně upozornil britský logik, matematik a filozof Bertrand Russell (1872–1970) svým dnes klasickým paradoxem. Russellův paradox je formulován takto. Označme N množinu všech množin, které nejsou prvky sama sebe, tedy

$$N = \{x \mid x \notin x\}.$$

Takové množiny Russell nazýval normálními, protože známé množiny x splňují $x \notin x$. Russell položil otázku, zda množina N je normální, tedy zda $N \in N$. Pokud $N \in N$, pak N má vlastnost, kterou mají všechny množiny v N, totiž vlastnost $x \notin x$, a tedy $N \notin N$. Pokud ovšem $N \notin N$, pak N má vlastnost prvů množiny N, a tedy patří do množiny N, tj. $N \in N$. Všimněme si, že jsme vlastně odvodili, že $N \in N$, právě když $N \notin N$. Odvodili jsme tedy spor, tj. tvrzení, které je vždy nepravdivé. To je ale vážný problém, protože ze sporu lze logicky odvodit jakékoli tvrzení. Teorie, ve které odvodíme spor, je tedy bezcenná.

V logice existuje celá řada dalších paradoxů, tedy zvláštních jevů, které spočívají v tom, že se z všeobecně přijímaných předpokladů jednoduchými úsudkovými kroky dostaneme do situace, která je sporná nebo se příčí zdravému rozumu. Takové paradoxy zpravidla umožní nahlédnout, že uvažování v přirozeném jazyce, které se řídí intuicí, má svá úskalí a své meze. Řada takových paradoxů vedla k dalšímu rozvoji formální logiky. Uvedeme si jeden z nejznámějších paradoxů, tzv. paradox lháře.

Kréťan říká: „Lžu“. Mluví pravdu? Když ano, pak je pravda, co říká, a tedy lže. Když ne, pak není pravda, co říká, tedy nelže, a tedy mluví pravdu. Odvodili jsme, že Kréťan mluví pravdu, právě když nemluví pravdu, a to je spor. (Dostali bychom spor, kdyby Kréťan říkal, že všichni Kréťani lžou?)

Jiný známý paradox, tzv. paradox hromady, vede k vytvoření nové logiky, tzv. fuzzy logiky, která našla uplatnění v mnoha výrobcích, které běžně používáme. Ukážeme si ho v příštím díle, ve kterém se fuzzy logikou budeme zabývat. Další logické paradoxy a hádanky čtenář najde například v knížce [4].

Literatura

[1] P. Jirků a kol., 1991. *Programování v jazyku Prolog.* Praha: Státní nakladatelství technické literatury.

[2] A. Sochor, 2011. *Logika pro všechny ochotné myslet.* Praha: Karolinum.

[3] A. Sochor, 2001. *Klasická matematická logika.* Praha: Karolinum.

[4] R. M. Smullyan,1986. *Jak se jmenuje tahle knížka?* Praha: Mladá fronta.

Katedra informatiky
Univerzita Palackého v Olomouci
www.inf.upol.cz

Katedra informatiky
Univerzita Palackého v Olomouci
17. listopadu 12
771 46 Olomouc