INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Logika: systémový rámec rozvoje oboru v ČR a koncepce logických propedeutik pro mezioborová studia (reg. č. CZ.1.07/2.2.00/28.0216, OPVK)

Úvod do logiky (VL): 13. Axiomatické systémy VL a pojem důkazu

doc. PhDr. Jiří Raclavský, Ph.D.

(raclavsky@phil.muni.cz)

13. Axiomatické systémy VL a pojem důkazu

Už Euklidés, který položil základy moderním úvahám o *axiomatických* (*formálních*) *systémech*, narazil na to, že množina – v jeho případě geometrických – pravd je nekonečná. Kromě problému s určením takovéto rozsáhlé množiny tu jde i o problém, jak se ujistit, že libovolná pravda z dané množiny skutečně je pravdou. Pojem axiomatického systému pak vlastně řeší oba naznačované problémy najednou. Při sestavování axiomatického systému nejprve zvolíme (konečnou) množinu základních, evidentních a tedy důkaz nevyžadujících pravd, tzv. *axiomů*. Dále zvolíme (konečnou) množinu bezpečných prostředků, tzv. *odvozovacích pravidel* (někdy zvaných *dedukční* či *derivační pravidla*), jež umožňují z množiny axiomů generovat další pravdy, tzv. *teorémy*. Axiomatický systém je tedy dán axiomy a pravidly odvození. Jednotlivé teorémy, tedy dokazované pravdy, jsou vždy demonstrovány pomocí *důkazů*, tj. posloupností pravd daných (čili axiomů) nebo již dokázaných (čili teorémů), přičemž jednotlivé prvky této posloupnosti jsou získávány pomocí pravidel odvozování. Ve 20. století se zjistilo (zvl. díky Gödelovým výsledkům), že pojem pravdy ve smyslu pravdivé formule a pojem dokazatelné formule je žádoucí od sebe oddělit. Mohli bychom říci, že mnohé zde prováděné úvahy patří do tzv. *metalogiky*, v tuzemsku se tento termín ale neužívá.

13.1 Axiomatické systémy pro VL

V následujícím výkladu předkládáme několik možných *axiomatických systémů VL*. V prostředí matematické logiky se často mluví o *kalkulech* k *VL*. Struktura jiných axiomatických systémů VL je analogická. Každý axiomatický systém *S* je zadán:

1) formálním jazykem (bez sémantiky),
2) množinou axiomů,
3) množinou odvozovacích pravidel.

Tato struktura je vynucena tím, že bod 1) určuje množinu správně utvořených formulí VL, jež jediné nás na rozdíl od nesprávně utvořených formulí zajímají. Určením množiny axiomů, bod 2), vyčleňujeme v množině správně utvořených formulí určitou množinu pravd; zbylé pravdy pak generujeme pomocí pravidel odvození, bod 3), jakožto teorémy.

Toto rozdělení axiomatického systému (kalkulu) do tří částí je však do jisté míry artificiální, například jazyk je obsažen ve formulích a tedy i v axiomech. Takováto úvaha však může jít dále k názoru, že axiomy jsou jakási bezprostřední pravidla. To by pak znamenalo, že axiomatický systém (kalkul) můžeme jednoduše chápat jako jednoznačně určený množinou pravidel.

1) Formální jazyk

Formální jazyk, zadaný abecedou a gramatikou, je tedy relativní k danému axiomatickému systému. V případě standardního axiomatického systému VL je často vybírán jazyk, jehož jedinými spojkami jsou $\neg$ a $\rightarrow$.

2) Axiomy

Axiomy daného axiomatického systému *S* jsou základní vybrané formule *S*. Volba axiomů totiž není libovolná. Aby byl daný axiomatický systém korektní, tedy abychom dokazovali jen logicky pravdivé formule, volba podléhá dvěma kritériím: a) každý axiom je tautologie, b) množina axiomů musí umožňovat, aby se z nich daly odvodit pokud možno všechny logicky platné formule. Přitom je rozumné, aby tato množina byla minimální, tedy aby žádný axiom nebyl dokazatelný z jiných axiomů; volíme tedy tzv. *nezávislou množinu axiomů* – axiom je nezávislý tehdy, když by množina teorémů byla menší, kdyby byl tento axiom odejmut.

Tzv. *formalizované* (či *axiomatizované*, *axiomatické*) *teorie* mají kromě axiomů definovány i *mimologické axiomy* či jinak řečeno *postuláty*, které obsahují *mimologické pojmy*, tj. pojmy z předmětné oblasti, o níž daná teorie vypovídá. Tyto postuláty nebývají logicky pravdivé, nebývají to tautologie. Příkladem je třeba některá axiomatická teorie množin.

Běžně uvažovanými axiomy VL jsou:

Axiom 1: $p\rightarrow(q\rightarrow p)$

Axiom 2: $(p\rightarrow(q\rightarrow r))\rightarrow((p\rightarrow q)\rightarrow(p\rightarrow r))$

Axiom 3: $(\neg q\rightarrow\neg p)\rightarrow(p\rightarrow q)$

Aby bylo možno z pravidel odvození vypustit Pravidlo substituce (srov. níže), jsou obvykle volena *axiomová schémata*. Protože obsahují metaproměnné pro formule, každé axiomové schéma reprezentuje nekonečně mnoho jednotlivých axiomů, které by vznikly substitucí.

Axiom 1: $A\rightarrow(B\rightarrow A)$

Axiom 2: $(A\rightarrow(B\rightarrow C))\rightarrow((A\rightarrow B)\rightarrow(A\rightarrow C))$

Axiom 3: $(\neg B\rightarrow\neg A)\rightarrow(A\rightarrow B)$

Existují i jiné sady axiomových schémat, například:

$A\rightarrow(B\rightarrow A)$

$(A\rightarrow(B\rightarrow C))\rightarrow((A\rightarrow B)\rightarrow(A\rightarrow C))$

$(\neg B\rightarrow\neg A)\rightarrow((\neg A\rightarrow B)\rightarrow A)$

$(A\wedge B)\rightarrow A$ alt. $(A\wedge B)\rightarrow B$

$A\rightarrow (B\rightarrow(A\wedge B))$

$A\rightarrow(A\vee B)$ alt. $B\rightarrow(A\vee B)$

$(A\rightarrow B)\rightarrow((A\rightarrow B)\rightarrow (A\vee B)\rightarrow C))$

Dokonce je možná i jednoprvková množina axiomů pro jazyk s ¬ a →, obsahuje:

$$((((A\to B)\to(\neg C\to\neg D))\to C)\to E)\to((E\to A)\to(D\to A))$$

Pro axiomatický systém, jehož jazyk obsahuje jako operátor jen ↑, je takovým jediným axiomem:

$$(A\uparrow(B\uparrow C))\uparrow((D\uparrow(D\uparrow D))\uparrow((E\uparrow B)\uparrow((A\uparrow E)\uparrow(A\uparrow E))))$$

(Pravidlem odvození v tomto systému není Modus ponens, ale A, $A\uparrow(A\uparrow C)$ / C.) (Tautologičnost všech těchto axiomů lze snadno ověřit například tabulkovou metodou.)

3) Pravidla odvozování

Modus ponens (MP)

$$\begin{array}{l} A\to B \\ A \\ \hline B \end{array}$$

Pravidlo substituce

$$\begin{array}{l} A \\ \hline A[B/a] \end{array}$$

(pomocí $[B/a]$ vyznačujeme nahrazení všech výskytů a v A pomocí B)

MP je obligátním pravidlem odvozování (Modus ponendo ponens, lat. způsob kladně kladný; alternativní název je pravidlo odloučení, angl. „rule of detachment“; byl objeven Stoiky, kteří ho nazývali hypoteticko-kategorický sylogismus). Pravidlo substituce je nezbytné pouze pokud nepoužíváme axiomová schémata.

Podotkněme, že volba odvozovacích pravidel není libovolná. Aby byl systém korektní, musí pravidla zachovávat pravdivost v tom smyslu, že formule, kterou aplikací pravidla obdržíme, je pravdivá alespoň ve všech modelech množiny předpokladů pravidla, tedy že z těchto předpokladů vyplývá. Hovoří se zde proto o *korektnosti odvozovacích pravidel*, přičemž takováto korektnost může být vyjádřena větou, jejíž platnost je následně dokazována. Pro příklad uvažme *Větu o korektnosti pravidla Modus ponens* a to v této podobě: Jestliže formule A a $A\to B$ jsou tautologiemi, tak i B je tautologií. Důkaz této věty je poměrně jednoduchý, a proto si ho teď předvedeme. Předpokládejme, že A i $A\to B$ jsou logicky pravdivé formule; proto nemůže existovat v, při níž by B mohla být nepravdivá, poněvadž to by $A \to B$ nemohla být při této v pravdivá a tedy ani tautologií.

Kromě výše uvedených dvou pravidel si lze odvodit i další pomocná odvozovací pravidla. Mnohá z nich mají svou obdobu v zákonech VL, jež jsou tvaru implikace; to ukazuje důležitost implikace pro vyplývání. Viz takováto pravidla níže v sekci o přirozené dedukci (14.4), popř. gentzenovské dedukci (14.5).

13.2 Důkazy

Posloupnosti formulí, jež jsou výsledky aplikací odvozovacích pravidel, nazýváme *důkazy*. Jejich závěrečnými formulemi jsou formule dokázané, tedy teorémy. Je žádoucí si uvědomit, že jak pojem teorému, tak hlavně pojem důkazu jsou syntaktické pojmy. K získání teorému tedy není nezbytná nějaká sémantická úvaha či snad intuice, ale pouhá manipulace symbolů. Mechaničnost takovéto ‚strukturální' práce se symboly umožňuje nejenom lepší produktivitu pravd po kvalitativní stránce, ale i po stránce kvantitativní, což ukazuje zajímavá oblast počítačově generovaných důkazů, automatické dokazování. Jednotlivé důkazy jsou samozřejmě relativní k jednotlivým axiomatickým systémům, od čehož ovšem mnozí autoři ve svých definicích abstrahují. Podobně abstrahují od toho, že se jedná o důkazy v tom či jiném důkazovém systému. Je však třeba podotknout, že důkazy například v hilbertovském a gentzenovském systému (k oběma v následujících dvou kapitolách) jsou vzájemně přeložitelné.

Důkaz

Konečná posloupnost formulí A_1, A_2, ..., A_n je v daném axiomatickém systému S *důkazem* právě tehdy, když pro každé i takové, že $1 \leq i \leq n$, je formule A_i buď

1) axiomem S nebo

2) je odvozena aplikací některého pravidla odvození systému S na formule A_j, ..., A_k, přičemž $j, ..., k < i$.

Všimněme si, že podmínky 1) a 2) nejsou vzájemně se vylučující. Na konci důkazů se z historických důvodů někdy uvádí *QED*, příp. q.e.d., což je zkratka za latinské „quod erat demonstrandum", česky „což bylo třeba dokázat". Po straně důkazů se píší *anotace*, které indikují, že daný *krok důkazu* vznikl uplatněním kterého pravidla na které předchozí kroky.

Uveďme si hned jednoduchou ukázku takového obyčejného přímého důkazu bez předpokladů. Dokažme $q \to (\neg p \to q)$. V důkazu použijeme axiom $p \to (q \to p)$ (tj. Ax 1) a pak uplatníme Pravidlo substituce (v následujících kapitolách budeme tyto dva kroky obvykle psát do jednoho řádku):

1. $p \to (q \to p)$	Ax 1
2. $q \to (\neg p \to q)$	Pravidlo substituce (1; q/p, $\neg p/q$)

Důkaz z předpokladů, někdy nazývaný *důkaz z hypotéz*, odděluje předpoklady a vlastní dokazované formule, a proto je formální obdobou běžných úsudků, jež se sestávají z premis a závěrů.

Důkaz z předpokladů

Nechť T je systém formulí. Konečná posloupnost formulí A_1, A_2, ..., A_n je v daném axiomatickém systému S *důkazem ze systému předpokladů T* právě tehdy, když pro každé i takové, že $1 \leq i \leq n$, je formule A_i buď

1) axiomem S nebo
2) je prvkem T nebo
3) je odvozena aplikací některého pravidla odvození systému S na formule A_j, ..., A_k, přičemž $j, ..., k < i$.

Na ukázku dokážeme z předpokladů formuli $q \to p$, naším předpokladem bude formule p, tj. naší T je $\{p\}$.

1. $p \to (q \to p)$	Ax 1
2. p	předpoklad
3. $q \to p$	MP (1,2)

Tímto jsme mimochodem dokázali (odvozené) pravidlo $p \to (q \to p)$, p / $q \to p$. Všimněme si, že v důkazu z předpokladů není každý krok logicky pravdivý, formule p i $q \to p$ jsou totiž netautologické.

Všimněme si ještě, že máme-li v axiomatickém systému S dokázat jeho axiom, pak jeho nejjednodušší důkaz má nula kroků, čili důkazem axiomu S v systému S je axiom sám. (Existují i delší než jednokrokové důkazy axiomů, například Ax 1 odvodíme z Ax 1 pomocí substituce q/p, p/q a pak pomocí substituce p/q, q/p.)

Konečně jsou tu ještě pojmy dokazatelné formule a teorému. (V případě VL ke každé tautologické formuli existuje důkaz bez předpokladů, proto není třeba hovořit o dokazatelnosti z předpokladů.)

Dokazatelnost formule

Formule A je *dokazatelná v axiomatickém systému S* právě tehdy, když v tomto systému S existuje důkaz, jehož je tato formule posledním členem.

Bylo by užitečné si rezervovat termín „dokazatelná“ pro formule dokázané důkazem bez předpokladů a termín „odvoditelná“ pro formule dokázané (odvozené) důkazem z předpokladů, ale v přirozeném jazyce zakotvená tendence tyto dva termíny zaměňovat činí takovouto úmluvu těžko udržitelnou.

Teorém

Formule A je *teorémem axiomatického systému* S právě tehdy, když je dokazatelná v systému S. Značíme pomocí $\vdash_S A$.

Někdy se teorémům říká *věty*, ale v případě teorémů studovaných kalkulů (nikoli teorémů naší metalogiky), je tento termín spíš vzácný. (Dodejme, že formule A je *vyvratitelná v axiomatickém systému* S právě tehdy, když v S existuje důkaz $\neg A$.)

Protože se jedná o dokazování (níže pak vyplývání) vzhledem k S, u $\vdash_S$ (v textu níže zase $\models_S$) píšeme „S" v dolním indexu. Pokud ale není nezbytné tuto relativizaci k určitému axiomatickému systému zmiňovat, bývá „S" v dolním indexu vypouštěno.

Nyní uvedeme Davidem Hilbertem dokázaný *Metateorém dedukce* (či *Dedukční teorém*), v současnosti nejčastěji nazývaný *Věta o dedukci*. Ten umožňuje účinně zkracovat důkazy, zejm. důkazy z předpokladů.

Věta o dedukci (VD)

Nechť T je teorie (soubor předpokladů), A a B formule. Potom $T \vdash A \rightarrow B$ právě tehdy, když $T \cup \{A\} \vdash B$.

Všimněme si, že VD vlastně mluví o existenci důkazů: důkaz formule B z A (a z T) existuje právě tehdy, když existuje důkaz formule $A \rightarrow B$ (z T). „$T \cup \{A\}$" bývá obvykle zkracováno na „T, A".

Z hlediska základního praktického užití umožňuje VD převádět platné úsudky na tautologie, a naopak. Díky této souvislosti s úsudky někteří autoři uvádějí tzv. *sémantickou variantu Věty o dedukci*: Nechť T je teorie, A a B formule; potom $T \models A \rightarrow B$ právě tehdy, když $T, A \models B$.

Fungování VD si ukážeme na výše uváděném přímém důkazu z předpokladů:

1. $p \rightarrow p$
2. $p \rightarrow (q \rightarrow p)$
3. $(p \rightarrow p) \rightarrow (p \rightarrow (q \rightarrow p))$ VD (1,2)

V našem dalším příkladu si ukážeme, jak se (přímý) důkaz z předpokladů použitý dohromady s VD využívá k dokazování nových pravidel v systémech tzv. přirozené dedukce. Mějme za úkol odvodit pravidlo:

$p \rightarrow q$
——————
$\neg q \rightarrow \neg p$

To znamená, že máme dokázat $\neg q \rightarrow \neg p$ z předpokladu $p \rightarrow q$, tj. $p \rightarrow q \vdash \neg q \rightarrow \neg p$. Důkaz využívá odvozené pravidlo Modus tollens (tj. $A \rightarrow B, \neg B$ / $\neg A$; srov. níže):

1. $p \rightarrow q$	předpoklad
2. $\neg q$	předpoklad
3. $\neg p$	Modus tollens (1,2)
4. $\neg q \rightarrow \neg p$	VD (2,3)

Nyní uvedeme tři další druhy důkazů, jež jsou kromě přímého důkazu z nebo bez předpokladů často používány. *Nepřímý důkaz* odvoditelnosti B z A je vlastně přímým důkazem odvoditelnosti $\neg A$ z $\neg B$. Pro praktickou ilustraci užití dokažme $p \rightarrow q$, $\neg q \mid\!- \neg p$. Náš nepřímý důkaz využívá odvozené Pravidlo eliminace dvojité negace (tj. $\neg\neg A$ / A; srov. níže):

1. $p \rightarrow q$	předpoklad
2. $\neg q$	předpoklad
3. $\neg\neg p$	předpoklad nepřímého důkazu
4. p	Pravidlo eliminace dvojité negace (3)
5. q	MP (1,4)

V daném příkladu dále vede důsledek 5. našeho předpokladu nepřímého důkazu 3. ke sporu s přímým předpokladem 2., takže lze z našich předpokladů 1. a 2. odvodit negaci předpokladu nepřímého důkazu (přesněji to, čeho byl předpoklad nepřímého důkazu negací), totiž:

6. $\neg p$	na základě sporu (3,5)

Takže daný příklad zároveň můžeme pochopit i jako ukázku často používaného *důkazu sporem* (v anglicky píšícím prostředí „reductio ad absurdum“, častěji jen „reductio“, což se dopisuje do anotace příslušného kroku). (Náš příklad byl záměrně vybrán právě proto, aby ukázal rozdíl mezi nepřímým důkazem a důkazem sporem, který mnohdy není jasný.) Důkaz sporem se zakládá na *Větě o důkazu sporem*: $T \mid\!- A$ právě tehdy, když $T, \neg A \mid\!- \neg(B \rightarrow B)$ (kde formule $\neg(B \rightarrow B)$ reprezentuje spor); v sémantické obdobě této věty, tj. s $\models$ namísto $\mid\!-$, je $T \cup \{\neg A\}$ nesplnitelnou množinou formulí. Budeme-li teď T (jež je konečnou množinou) chápat jednoduše jako formuli, tak to znamená, že $T \rightarrow A$ právě tehdy, když $\neg(T \wedge \neg A)$. V matematice mnohdy užívaný *důkaz rozborem případů* se zase zakládá na *Větě o důkazu rozborem případů*: $T, A \vee B \mid\!- C$ právě tehdy, když $T, A \mid\!- C$ a zároveň $T, B \mid\!- C$.

13.3 Vlastnosti axiomatických systémů VL

U axiomatických systémů nás zajímají tři důležité vlastnosti, jež mohou mít, totiž rozhodnutelnost, bezespornost a úplnost. Prvá zmiňovaná vlastnost, jež v poslední době nebývá příliš často zmiňována, znamená to, že dovedeme rozhodnout, zda je daná formule teorémem daného systému nebo ne. Bezespornost v zásadě znamená, že daný systém negeneruje kromě formule i její negaci, což by v důsledku obnášelo, že by generoval všechny formule vůbec. Úplnost je nejzajímavější, neboť znamená, že daný axiomatický systém generuje všechny logicky pravdivé formule.

Než uvedeme přesné definice, zmíníme důležitý fakt, totiž že pro VL existují rozhodnutelné, bezesporné a úplné axiomatické systémy (kalkuly). Stručně se pak říká, že *VL je rozhodnutelná, bezesporná, a úplná*. Příkladem takového axiomatického systému je výše uváděný systém s trojicí axiomových schémat a MP.

Pro porozumění pojmu rozhodnutelnosti axiomatického systému musíme nejdříve definovat, co rozhodnutelnost znamená obecně: *množina M* je *rozhodnutelná* ve své nadmnožině *N* právě tehdy, když existuje efektivní algoritmus (tj. procedura o konečném počtu kroků) aplikovatelný na prvky množiny *N*, který o každém prvku množiny *N* určí, zda je, či není, prvkem množiny *M*. Samozřejmě platí, že abeceda jazyka daného axiomatického systému musí být rozhodnutelná v množině všech možných symbolů. Také množina správně utvořených formulí musí být rozhodnutelná v množině všech možných kombinací znaků abecedy. Množina axiomů daného axiomatického systému musí být rozhodnutelná v množině správně utvořených formulí. Když se hovoří o rozhodnutelnosti axiomatického systému, je tím míněn následující pojem.

Rozhodnutelnost

Axiomatický systém *S* je *rozhodnutelný* právě tehdy, když o každé formuli *A* je rozhodnutelné, zda je či není teorémem *S*.

To znamená, že množina teorémů *S* je rozhodnutelná v množině všech formulí VL.

Ve sporném systému je dokazatelná formule *A* i formule ¬*A*; systém je bezesporný, pokud v něm *A* i ¬*A* dokazatelné nejsou.

Syntaktická bezespornost

Axiomatický systém *S* je *syntakticky bezesporný* (*konzistentní*) právě tehdy, když v *S* není dokazatelná věta $A\wedge\neg A$ (tj. spor).

Někdy bývá přidávána následující definice: Axiomatický systém *S* je *syntakticky úplný* právě tehdy, když přidáme-li k množině axiomů *S* formuli, která není teorémem, tak dostaneme syntakticky sporný systém.

To, že axiomatický systém má být bezesporný, je samozřejmý požadavek. Co už tak samozřejmé být nemusí, je to, zda axiomatický systém jako teorémy generuje pouze tautologie (což je korektnost) a hlavně zda generuje všechny tautologie (což je úplnost).

Korektnost (sémantická bezespornost)

Axiomatický systém S je *korektní (sémanticky bezesporný)* právě tehdy, když pro každou formuli A a systém formulí T platí, že je-li A dokazatelná v S z T, tak A vyplývá z T (je tautologickým důsledkem T).

Čili je-li $T \vdash_S A$, pak $T \models_S A$.

Speciálním případem je, že je-li A dokazatelná v S, tak A je logicky pravdivá (je tautologií):

Čili je-li $\vdash_S A$, pak $\models_S A$.

Tuto větu je možno reformulovat v tom smyslu, že žádný sporný systém T není splnitelný.

Sémantická úplnost

Axiomatický systém S je *sémanticky úplný* právě tehdy, když pro každou formuli A a systém formulí T platí, že jestliže A vyplývá z T (A je tautologickým důsledkem T), tak A je dokazatelná v S z T.

Čili je-li $T \models_S A$, pak $T \vdash_S A$.

Speciálním případem je, že je-li A logicky pravdivá (je tautologií), tak A je dokazatelná v S.

Čili je-li $\models_S A$, pak $\vdash_S A$.

Zde je definována tzv. *silná* sémantická úplnost, *slabá* sémantická úplnost obnáší omezení na konečný soubor formulí T (proto pod slabou úplnost spadá, že je-li $\models_S A$, pak $\vdash_S A$).