Matematická logika

přednáška čtvrtá

Miroslav Kolařík

Zpracováno dle textu R. Bělohlávka:
Matematická logika – poznámky k přednáškám, 2004.

a dle učebního textu R. Bělohlávka a V. Vychodila:
Diskrétní matematika pro informatiky II, Olomouc 2006.

Spornost a bezespornost

Definice

Množina formulí T se nazývá **sporná** (nekonzistentní), jestliže je z ní dokazatelná jakákoliv formule. Není-li T sporná (tj. existuje formule, která není z T dokazatelná), nazývá se **bezesporná** (konzistentní).

Lemma

Následující tvrzení jsou ekvivalentní:

(i) Množina formulí T je sporná;

(ii) $T \vdash \varphi$ a $T \vdash \neg\varphi$ pro nějakou formuli φ;

(iii) $T \vdash \neg(\vartheta \Rightarrow \vartheta)$.

Důkaz: "(i) $\Rightarrow$ (ii)": Pokud je T sporný systém formulí, pak je z něj dokazatelná jakákoliv formule, tedy i formule φ a $\neg\varphi$.

"(ii) $\Rightarrow$ (iii)": Nechť $T \vdash \varphi$ a $T \vdash \neg\varphi$. Dle ($a_\vdash$) máme $\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta))$, z monotonie dokazatelnosti $T \vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta))$. Dvojnásobným použitím MP dostaneme $T \vdash \neg(\vartheta \Rightarrow \vartheta)$.

"(iii) $\Rightarrow$ (i)": Nechť φ je libovolná formule. Platí $\vdash \neg(\vartheta \Rightarrow \vartheta) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$ opět dle ($a_\vdash$). Z monotonie dokazatelnosti $T \vdash \neg(\vartheta \Rightarrow \vartheta) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$. Dále platí, že $T \vdash \vartheta \Rightarrow \vartheta$; z předpokladu $T \vdash \neg(\vartheta \Rightarrow \vartheta)$ tedy dvojnásobným použitím MP máme $T \vdash \varphi$.

O důkazu sporem

Důkaz sporem je populární dokazovací princip v informatice a matematice. Sporem se snadno dokazuje například tvrzení: "prvočísel je nekonečně mnoho" nebo "$\sqrt{2} \notin \mathbb{Q}$" atd. Při dokazování postupujeme tak, že předpokládáme neplatnost tvrzení a dojdeme ke sporu, čímž dokážeme platnost daného tvrzení.
Následující věta ukazuje, že intuitivní důkaz sporem má ve VL svou formalizaci.

Důkaz sporem

Věta o důkazu sporem

Nechť T je množina formulí, nechť φ je libovolná formule. Pak platí: $T \vdash \varphi$, právě když $T, \neg\varphi$ je sporná množina.

Důkaz: Nechť $T \vdash \varphi$. Pak zřejmě $T, \neg\varphi \vdash \varphi$ a triviálně též $T, \neg\varphi \vdash \neg\varphi$, což dle (ii) předchozí Lemmy znamená, že $T, \neg\varphi$ je sporná množina.

Naopak, předpokládáme-li, že $T, \neg\varphi$ je sporná množina, pak je z $T, \neg\varphi$ dokazatelná formule $\neg(\vartheta \Rightarrow \vartheta)$ dle (iii) předchozí Lemmy. Užitím VoD máme $T \vdash \neg\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta)$. Jelikož $(\neg\varphi \Rightarrow \neg(\vartheta \Rightarrow \vartheta)) \Rightarrow ((\vartheta \Rightarrow \vartheta) \Rightarrow \varphi)$ je axiom dle (A3), pak z monotonie dokazatelnosti a užitím MP dostáváme $T \vdash (\vartheta \Rightarrow \vartheta) \Rightarrow \varphi$. Dále $\vdash \vartheta \Rightarrow \vartheta$, odkud opětovným užitím monotonie dokazatelnosti a MP máme $T \vdash \varphi$.

Označení: Jsou-li $\varphi, \varphi_1, \ldots, \varphi_n$ formule a $p_1, \ldots, p_n$ po dvou různé výrokové symboly, označíme symbolem $\varphi(p_1/\varphi_1, \ldots, p_n/\varphi_n)$ formuli, která vznikne z formule φ nahrazením všech výskytů symbolů $p_1, \ldots, p_n$ po řadě formulemi $\varphi_1, \ldots, \varphi_n$.

Věta o nahrazení

Pro libovolné formule $\varphi, \varphi_1, \ldots, \varphi_n$ a libovolné po dvou různé výrokové symboly $p_1, \ldots, p_n$ platí, že z $\vdash \varphi(p_1, \ldots, p_n)$ plyne $\vdash \varphi(p_1/\varphi_1, \ldots, p_n/\varphi_n)$.

Důkaz: Jednoduchý, zkuste si ho!

Věta o ekvivalenci

Vznikne-li formule ψ z formule φ nahrazením jejích podformulí $\varphi_1, \ldots, \varphi_n$ po řadě formulemi $\psi_1, \ldots, \psi_n$, pak
$\varphi_1 \Leftrightarrow \psi_1, \ldots, \varphi_n \Leftrightarrow \psi_n \vdash \varphi \Rightarrow \psi$.
Z $\vdash \varphi$ tedy plyne $\varphi_1 \Leftrightarrow \psi_1, \ldots, \varphi_n \Leftrightarrow \psi_n \vdash \psi$.

Věta o důkazu rozborem případů

Pro množinu formulí T a formule φ, ψ, χ platí $T, \varphi \vee \psi \vdash \chi$, právě když $T, \varphi \vdash \chi$ a $T, \psi \vdash \chi$.

Věta o neutrální formuli (VoNF)

Pro množinu formulí T a formule φ a ψ platí $T \vdash \psi$, právě když $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$.

Důkaz: Dle předchozí věty je $T, \varphi \vee \neg\varphi \vdash \psi$, právě když $T, \varphi \vdash \psi$ a $T, \neg\varphi \vdash \psi$. Dále však platí, že $T, \varphi \vee \neg\varphi \vdash \psi$, právě když $T \vdash \psi$ (neboť $\varphi \vee \neg\varphi$ je zkratkou za $\neg\varphi \Rightarrow \neg\varphi$, což (jak víme) je dokazatelná formule; pro dokazatelnou formuli α je vždy $T, \alpha \vdash \beta$, právě když $T \vdash \beta$), a tím je důkaz hotov.

Viděli jsme formule, které jsou v našem axiomatickém systému dokazatelné. Brzy se lehce přesvědčíme, že každá dokazatelná formule je tautologií.
Nabízí se otázka, zda také naopak je každá tautologie dokazatelná. Uvidíme, že ano (a uvidíme i více). Jinými slovy, naše axiomy a odvozovací pravidlo jsou zvoleny tak vhodně, že umožňují dokázat všechny tautologie, ale žádné další formule (tj. formule, které jsou někdy nepravdivé).

Poznámka: Pokud bychom označili Fml množinu všech formulí jazyka VL, ve kterém pracujeme, pak potenční množina 2^{Fml} je vlastně množinou všech systémů formulí ($T \in 2^{\mathrm{Fml}}$ potom znamená, že T je systém formulí). Syntaktické vyplývání je tedy relace $\vdash \subseteq 2^{\mathrm{Fml}} \times \mathrm{Fml}$, přitom $T \in 2^{\mathrm{Fml}}$ je v relaci $\vdash$ s $\varphi \in \mathrm{Fml}$, právě když je φ dokazatelná z T. Stejně tak sémantické vyplývání lze chápat jako relaci $\models \subseteq 2^{\mathrm{Fml}} \times \mathrm{Fml}$, kde $T \in 2^{\mathrm{Fml}}$ je v relaci $\models$ s $\varphi \in \mathrm{Fml}$, právě když φ sémanticky plyne z T.

Následující tvrzení ukazuje, že $\vdash \subseteq \models$.

Věta o korektnosti (VoK)

Věta o korektnosti

Pro libovolnou množinu formulí T a formuli φ platí, že je-li $T \vdash \varphi$, pak $T \models \varphi$. Speciálně tedy, každá dokazatelná formule je tautologií.

Důkaz: Nejprve pro $T = \emptyset$. Každý axiom je tautologie (o čemž se lze snadno přesvědčit tabelací). Dále zřejmě platí, že jsou-li φ a $\varphi \Rightarrow \psi$ tautologie, je i ψ tautologie. Indukcí tedy dostáváme, že každý člen důkazu je tautologie. Tedy každá dokazatelná formule je tautologie.
Je-li $T \neq \emptyset$, pak z $T \vdash \varphi$ plyne, že pro nějaké $\psi_1, \ldots, \psi_n \in T$ je $\psi_1, \ldots, \psi_n \vdash \varphi$. Opakovaným ($n$-násobným) použitím VoD odtud dostaneme $\vdash \psi_1 \Rightarrow (\psi_2 \Rightarrow (\ldots(\psi_n \Rightarrow \varphi)\ldots))$, z čehož dle výše dokázaného plyne $\models \psi_1 \Rightarrow (\psi_2 \Rightarrow (\ldots(\psi_n \Rightarrow \varphi)\ldots))$. Nyní n-násobně použijeme "sémantické verze" VoD a dostaneme $\psi_1, \ldots, \psi_n \models \varphi$, z čehož plyne $T \models \varphi$.

Důsledek

Sporný systém formulí není splnitelný.

Důkaz: Pokud je T sporný systém, pak $T \vdash \neg(\vartheta \Rightarrow \vartheta)$, tedy (dle VoK) $T \models \neg(\vartheta \Rightarrow \vartheta)$. Odtud dostáváme, že $\neg(\vartheta \Rightarrow \vartheta)$ musí být pravdivá při každém ohodnocení, při kterém jsou pravdivé všechny formule z T. Ale $\neg(\vartheta \Rightarrow \vartheta)$ je kontradikce, tedy neexistuje žádné ohodnocení e, při kterém by byly všechny formule z T pravdivé. Tím jsme prokázali, že sporný systém formulí není splnitelný.

Poznámka: Korektnost lze využít k prokázání faktu, že některá formule není dokazatelná z jistého systému předpokladů. Reformulací korektnosti totiž dostáváme, že pokud φ sémanticky neplyne z T, pak φ není ze systému T ani dokazatelná. K tomu, abychom prokázali, že $T \nvdash \varphi$ tedy stačí ukázat $T \nvDash \varphi$, což je výrazně jednodušší než prokázat "neexistenci důkazu", protože důkazů, jakožto konečných posloupností formulí, je obecně nekonečně mnoho.

Příklad

Prokážeme, že $p \Rightarrow q \nvdash \neg p \Rightarrow q$. Z Věty o korektnosti VL stačí ukázat, že $p \Rightarrow q \nvDash \neg p \Rightarrow q$. To jest zbývá najít pravdivostní ohodnocení e takové, že $\| p \Rightarrow q \|_e = 1$, ale $\| \neg p \Rightarrow q \|_e = 0$. S využitím vlastností logické operace $\rightarrow$ zřejmě stačí vzít pravdivostní ohodnocení e, kde $e(p) = 0$ a $e(q) = 0$. Tím je důkaz hotov.

Shrneme-li předchozí poznatky, zavedli jsme dva druhy vyplývání: $\models, \vdash$ a již víme, že každá formule dokazatelná z prázdného systému je tautologie a obecněji $T \vdash \varphi$ implikuje $T \models \varphi$, neboli: "to co je dokazatelné z nějakého systému, z tohoto systému rovněž sémanticky plyne".
Ukážeme, že to platí i obráceně.

Před důkazem věty o úplnosti zavedeme následující značení.
Pro formuli φ a ohodnocení e je

$$\varphi^e = \begin{cases} \varphi, & \text{pokud } \| \varphi \|_e = 1 \\ \neg\varphi, & \text{pokud } \| \varphi \|_e = 0. \end{cases}$$

Churchovo lemma (ChL)

Pro libovolnou formuli $\varphi(p_1, \ldots, p_n)$ platí $p_1^e, \ldots, p_n^e \vdash \varphi^e$.

Důkaz: Tvrzení dokážeme strukturální indukcí přes složitost formule φ.

I. Nechť φ je výrokový symbol p. Pak je tvrzení zřejmé ($p^e \vdash p^e$).

II. Nechť tvrzení platí pro φ. Ukažme, že pak platí i pro $\neg\varphi$, tj., že $p_1^e, \ldots, p_n^e \vdash (\neg\varphi)^e$. Rozlišme dva případy, $\| \varphi \|_e = 0$ a $\| \varphi \|_e = 1$. Pro $\| \varphi \|_e = 0$ je $\varphi^e = \neg\varphi$ a $(\neg\varphi)^e = \neg\varphi$. Požadované tvrzení $p_1^e, \ldots, p_n^e \vdash (\neg\varphi)^e$ tedy přímo plyne z předpokladu. Pro $\| \varphi \|_e = 1$ je $\varphi^e = \varphi$ a $(\neg\varphi)^e = \neg\neg\varphi$. Máme tedy dokázat, že $p_1^e, \ldots, p_n^e \vdash \neg\neg\varphi$. To však plyne z předpokladu: $p_1^e, \ldots, p_n^e \vdash \varphi$ a z ($c_\vdash$): $\vdash \varphi \Rightarrow \neg\neg\varphi$ pomocí MP.

III. Nechť tvrzení platí pro φ a ψ. Ukažme, že pak platí i pro $\varphi \Rightarrow \psi$, tj., že $p_1^e, \dots, p_n^e \vdash (\varphi \Rightarrow \psi)^e$. Mohou nastat následující případy:

- $\| \varphi \|_e = 0$: Pak je $\| \varphi \Rightarrow \psi \|_e = 1$, tedy $(\varphi \Rightarrow \psi)^e = \varphi \Rightarrow \psi$. Podle předpokladu máme $p_1^e, \dots, p_n^e \vdash \neg\varphi$. Dle ($a_\vdash$) je $\vdash \neg\varphi \Rightarrow (\varphi \Rightarrow \psi)$, odkud pomocí MP dostaneme požadované $p_1^e, \dots, p_n^e \vdash \varphi \Rightarrow \psi$.
- $\| \psi \|_e = 1$: Pak je $\| \varphi \Rightarrow \psi \|_e = 1$, tedy opět $(\varphi \Rightarrow \psi)^e = \varphi \Rightarrow \psi$. Dle předpokladu máme $p_1^e, \dots, p_n^e \vdash \psi$. Z (A1): $\psi \Rightarrow (\varphi \Rightarrow \psi)$ a MP dostaneme požadované $p_1^e, \dots, p_n^e \vdash \varphi \Rightarrow \psi$.
- $\| \varphi \|_e = 1$ a $\| \psi \|_e = 0$: Pak $\| \varphi \Rightarrow \psi \|_e = 0$, tedy $(\varphi \Rightarrow \psi)^e = \neg(\varphi \Rightarrow \psi)$. Podle předpokladu je $p_1^e, \dots, p_n^e \vdash \varphi$ a $p_1^e, \dots, p_n^e \vdash \neg\psi$. Použitím ($e_\vdash$): $\vdash \varphi \Rightarrow (\neg\psi \Rightarrow \neg(\varphi \Rightarrow \psi))$ a dvojnásobným použitím MP dostaneme požadované $p_1^e, \dots, p_n^e \vdash \neg(\varphi \Rightarrow \psi)$.

Věta o úplnosti, slabá verze

Pro libovolnou **konečnou** množinu T formulí a formuli φ platí, že z $T \models \varphi$ plyne $T \vdash \varphi$. Speciálně, každá pravdivá formule je dokazatelná.

Důkaz: Tvrzení dokážeme nejprve pro případ $T = \emptyset$. Nechť tedy $\models \varphi$. Pro každé ohodnocení e tedy platí $\varphi^e = \varphi$ (protože podle předpokladu je $\| \varphi \|_e = 1$). Jsou-li $p_1, \ldots, p_n$ všechny výrokové symboly z φ, je dle ChL

$$p_1^e, p_2^e, \ldots, p_n^e \vdash \varphi.$$

Uvažujme nyní ohodnocení e', které se od e liší právě v hodnotě, kterou přiřazuje symbolu p_1. Předpokládejme, že $e(p_1) = 1$ a $e'(p_1) = 0$ (případ $e(p_1) = 0$ a $e'(p_1) = 1$ se ošetří symetricky). Dle ChL je opět

$$p_1^{e'}, p_2^{e'}, \ldots, p_n^{e'} \vdash \varphi.$$

Protože je však podle předpokladu $p_2^e = p_2^{e'}$, ..., $p_n^e = p_n^{e'}$, $p_1^e = p_1$ a $p_1^{e'} = \neg p_1$, dostáváme

$$p_1, p_2^e, \ldots, p_n^e \vdash \varphi \qquad \text{a} \qquad \neg p_1, p_2^e, \ldots, p_n^e \vdash \varphi,$$

odkud dle VoNF máme

$$p_2^e, \ldots, p_n^e \vdash \varphi.$$

Opakovaným použitím právě provedené úvahy postupně dostaneme

$$p_3^e, \ldots, p_n^e \vdash \varphi$$

až po

$$p_n^e \vdash \varphi$$

a nakonec

$$\vdash \varphi.$$

Nechť nyní $T = \{\varphi_1, \ldots, \varphi_n\}$. Podle sémantické verze VoD dostaneme z $T \models \varphi$, že $\models \varphi_1 \Rightarrow (\ldots(\varphi_n \Rightarrow \varphi))$. Odtud podle právě dokázaného plyne $\vdash \varphi_1 \Rightarrow (\ldots(\varphi_n \Rightarrow \varphi))$, odkud pomocí VoD dostáváme $\varphi_1, \ldots, \varphi_n \vdash \varphi$, tj. požadované $T \vdash \varphi$. Tím je důkaz hotov.

Pro důkaz tzv. silné verze věty o úplnosti (ta se neomezuje na konečné T) potřebujeme následující větu:

Věta o kompaktnosti

(1) Množina T formulí je splnitelná, právě když je splnitelná každá konečná podmnožina množiny T.

(2) Pro každou formuli φ je $T \models \varphi$, právě když existuje konečná $S \subseteq T$ tak, že $S \models \varphi$.

Věta o úplnosti, silná verze

S použitím věty o kompaktnosti již snadno dokážeme silnou verzi věty o úplnosti.

Věta o úplnosti, silná verze

Pro libovolnou množinu T formulí a formuli φ platí, že z $T \models \varphi$ plyne $T \vdash \varphi$.

Důkaz: Je-li $T \models \varphi$, pak dle věty o kompaktnosti (2) existuje konečná $S \subseteq T$ tak, že $S \models \varphi$. Dle slabé verze věty o úplnosti je $S \vdash \varphi$, a z toho samozřejmě plyne $T \vdash \varphi$.

Uvědomme si, že věta o úplnosti je velmi netriviální tvrzení:
Z toho, že nějaká formule má při všech (intuitivně zcela přirozeně definovaných) možných ohodnoceních pravdivostní hodnotu 1 plyne, že je dokazatelná pomocí tří (jednoduchých a intuitivně přijatelných) axiomů a jednoho (jednoduchého a intuitivně přijatelného) odvozovacího pravidla. Pojem pravdivého tvrzení, tak jak je formalizován v rámci VL, je tedy plně syntakticky charakterizovatelný (a navíc velmi jednoduchým způsobem).

Následující věta ukazuje další vztah dvojice pojmů, jednoho sémantického (splnitelnost) a druhého syntaktického (bezespornost), které spolu na první pohled nesouvisí.

Věta

Množina T formulí je splnitelná, právě když je bezesporná.

Důkaz: Nechť je T splnitelná. Pak existuje ohodnocení e, ve kterém jsou pravdivé všechny formule z T. Kdyby byla T sporná, pak by pro libovolnou formuli φ bylo $T \vdash \varphi$ a $T \vdash \neg\varphi$, a tedy dle VoK $T \models \varphi$ a $T \models \neg\varphi$. To znamená, že při každém ohodnocení, při kterém jsou pravdivé všechny formule z T (jedním z nich je e), je pravdivá jak formule φ, tak formule $\neg\varphi$. To je ale pochopitelně nemožné.
Nechť T je bezesporná. Pak existuje formule φ, pro kterou neplatí $T \vdash \varphi$, tj. (podle úplnosti) neplatí $T \models \varphi$. To ale znamená, že existuje ohodnocení, ve kterém není pravdivá φ, a přitom jsou pravdivé všechny formule z T. Tedy T je splnitelná.