Matematická logika

přednáška sedmá

Miroslav Kolařík

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

Obsah

Axiomy jsou formule tvaru (A1) – (A5)

(A1) $\varphi \Rightarrow (\psi \Rightarrow \varphi)$,

(A2) $(\varphi \Rightarrow (\psi \Rightarrow \chi)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \chi))$,

(A3) $(\neg\psi \Rightarrow \neg\varphi) \Rightarrow (\varphi \Rightarrow \psi)$,

(A4) $(\forall x)\varphi \Rightarrow \varphi(x/t)$,
je-li t substituovatelný za x,

(A5) $(\forall x)(\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow (\forall x)\psi)$,
nemá-li x ve φ volný výskyt,

kde φ, χ, ψ jsou formule PL, t je term a x je proměnná. (A4) se nazývá **axiom specifikace** (**substituce**), (A5) se nazývá **axiom distribuce**.
Odvozovací pravidla jsou **modus ponens** (MP), a **pravidlo generalizace** (G) (též **pravidlo zobecnění**), které říká z φ odvoď $(\forall x)\varphi$.

Poznámka: Všechny axiomy jsou tautologie. Omezení u (A4) a (A5) jsou podstatná (tj. bez nich by se nejednalo o tautologie). Skutečně, je-li φ formule $\neg(\forall y)r(x,y)$, t proměnná y, pak (A4) je formule

$$(\forall x)\neg(\forall y)r(x,y) \Rightarrow \neg(\forall y)r(y,y),$$

která není tautologií (např. není splněna v žádné struktuře **M** s alespoň dvěma prvky, ve které $r^{\mathbf{M}}$ je relace identity).
Dále jsou-li obě φ i ψ formulí $r(x)$, je (A5) formulí

$$(\forall x)(r(x) \Rightarrow r(x)) \Rightarrow (r(x) \Rightarrow (\forall x)r(x)),$$

což není tautologie (například není splněna ve struktuře **M** s alespoň dvěma prvky, ve které je $r^{\mathbf{M}}$ jednoprvková množina).

Definice

Důkaz formule φ z množiny formulí T je libovolná posloupnost formulí $\varphi_1, \ldots, \varphi_n$, pro kterou platí, že $\varphi_n = \varphi$ a každá φ_i (pro $i \leq n$)

- je axiomem PL
- nebo je formulí z T (je axiomem z T)
- nebo plyne z předchozích formulí důkazu pomocí MP nebo odvozovacího pravidla G (tj. existuje $j < i$ tak, že φ_i je formule $(\forall x)\varphi_j$).

Formule se nazývá **dokazatelná z T** (**věta teorie T**), existuje-li důkaz této formule z T (zapisujeme $T \vdash \varphi$, popř. jen $\vdash \varphi$, je-li $T = \emptyset$).

Poznámka: Stejně jako ve VL máme dva pojmy vyplývání formule φ z množiny formulí T: sémantické ($T \models \varphi$) a syntaktické ($T \vdash \varphi$). Máme také dva pojmy platnosti formule: $\models \varphi$ označuje platnost φ v sémantickém smyslu (pravdivost), $\vdash \varphi$ označuje platnost φ v syntaktickém smyslu (dokazatelnost).

Formule se nazývá **výrokově dokazatelná** z T, existuje-li její důkaz z T, ve kterém se vyskytují pouze axiomy typů (A1) – (A3) a MP. T se nazývá **výrokově sporná**, jestliže každá formule z T je výrokově dokazatelná.

Lemma

Nahradíme-li v tautologii VL výrokové symboly libovolnými formulemi PL, dostaneme formuli PL, která je výrokově dokazatelná.

Idea důkazu: Je-li φ ona tautologie, pak dle VoÚ pro VL je dokazatelná. Nahradíme-li v jejím důkazu ve VL výrokové symboly zmíněnými formulemi PL, dostaneme důkaz v PL, prokazující, že výsledná formule je výrokově dokazatelná.

Příklad

Jelikož $p \Rightarrow (p \vee q)$ a $(p \wedge q) \Rightarrow q$ jsou tautologie VL, jsou formule $(\forall x, y)x \leq x + y \Rightarrow ((\forall x, y)x \leq x + y \vee (\exists y)x \leq y)$ a $(\neg x \approx 0 \wedge y \approx x) \Rightarrow y \approx x$ (výrokově) dokazatelné formule PL.

Všimněme si, že není vždy $\vdash \varphi \Rightarrow (\forall x)\varphi$. Na druhé straně jest triviálně $\varphi \vdash (\forall x)\varphi$, protože přijímáme generalizaci jako dedukční pravidlo. Vidíme tedy, že v PL nemůže platit VoD pro všechny dvojice formulí.

Věta o dedukci (VoD)

Pro formuli φ bez volných proměnných a množinu formulí T platí: $T, \varphi \vdash \psi$ právě když $T \vdash \varphi \Rightarrow \psi$.

Důkaz: Analogicky jako ve VL.

Ukažme, že požadavek, aby φ neměla volné proměnné je nutný. Nechť φ je $r(x)$, kde r je unární relační symbol, ψ nechť je $(\forall x)r(x)$ a $T = \emptyset$. Pak užitím G dostaneme $T, \varphi \vdash \psi$, ale $T \vdash \varphi \Rightarrow \psi$ neplatí. Kdyby to platilo, pak by dle VoK (věty o korektnosti, kterou uvedeme za chvíli) bylo $T \models \varphi \Rightarrow \psi$, tj. $r(x) \Rightarrow (\forall x)r(x)$ by byla tautologie, což obecně neplatí, např. ve struktuře s množinou přirozených čísel jako univerzem ($M = \mathbb{N}$), kde r je interpretován jako množina čísel větších než 5 (nebo jakákoli množina různá od množiny všech přirozených čísel).

S VoD můžeme prokázat další pomocné dokazovací prostředky PL, které jsou analogiemi principů používaných ve VL. Mějme dánu množinu T formulí PL. Jestliže formule φ a ψ nemají volné proměnné a je-li ϑ libovolná formule, pak platí věty

- o důkazu sporem
  $T \vdash \varphi \;\Leftrightarrow\; (T, \neg\varphi \vdash \neg(\vartheta \Rightarrow \vartheta))$
- o důkazu rozborem případů
  $T, \varphi \vee \psi \vdash \vartheta \;\Leftrightarrow\; (T, \varphi \vdash \vartheta$ a současně $T, \psi \vdash \vartheta)$
- o neutrální formuli
  $T \vdash \vartheta \;\Leftrightarrow\; (T, \varphi \vdash \vartheta$ a současně $T, \neg\varphi \vdash \vartheta)$.

Poznamenejme, že důkaz se provede s využitím VoD a s využitím principu dosazení do tautologie VL.
Pro formule φ a ψ, které mají volné proměnné předchozí tři principy neplatí.
Podobně (s jistou znalostí kvantifikace) se dá dokázat i věta o ekvivalenci.

Věta o uzávěru

Kvantifikace je jevem PL, který nemá obdobu ve VL.

Věta o uzávěru (VoU)

Pro teorii T, formuli φ a každou proměnnou x platí: $T \vdash \varphi$ právě když $T \vdash (\forall x)\varphi$.

Důkaz: Předpokládejme $T \vdash \varphi$. Pak $T \vdash (\forall x)\varphi$ díky G; podrobněji: je-li $\ldots, \varphi$ důkaz φ z T, je $\ldots, \varphi, (\forall x)\varphi$ důkazem $(\forall x)\varphi$ z T.
Obráceně, předpokládejme $T \vdash (\forall x)\varphi$. Protože $(\forall x)\varphi \Rightarrow \varphi$ je axiom dle (A4), kde $t = x$, je $\vdash (\forall x)\varphi \Rightarrow \varphi$, tedy $T \vdash \varphi$ použitím MP.

Tvrzení o formulích s kvantifikátory

Věta

Pro formule φ, ψ a proměnné x, y platí:

- $\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\forall x)\varphi \Rightarrow (\forall x)\psi)$,
- $\vdash (\forall x)(\varphi \Rightarrow \psi) \Rightarrow ((\exists x)\varphi \Rightarrow (\exists x)\psi)$,
- $\vdash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\forall x)\psi)$; není-li x volná ve φ,
- $\vdash (\forall x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\exists x)\varphi \Rightarrow \psi)$; není-li x volná v ψ,
- $\vdash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow (\varphi \Rightarrow (\exists x)\psi)$; není-li x volná ve φ,
- $\vdash (\exists x)(\varphi \Rightarrow \psi) \Leftrightarrow ((\forall x)\varphi \Rightarrow \psi)$; není-li x volná v ψ,
- $\vdash (\forall x)(\forall y)\varphi \Leftrightarrow (\forall y)(\forall x)\varphi$,
- $\vdash (\exists x)(\exists y)\varphi \Leftrightarrow (\exists y)(\exists x)\varphi$,
- $\vdash (\exists x)(\forall y)\varphi \Rightarrow (\forall y)(\exists x)\varphi$.

Více na cvičení.

Obsah

Cílem je dostat se k větě o úplnosti PL.
Nejdříve uvedeme větu o korektnosti. Úplnost poté ukážeme metodou tzv. henkinovských rozšíření teorií.

Věta o korektnosti (VoK)

Pro libovolnou teorii T a libovolnou formuli φ jazyka teorie T platí, že z $T \vdash \varphi$ plyne $T \models \varphi$.

Důkaz: Analogicky jako ve VL.

Poznámka: Jednoduchým důsledkem je fakt: sporná teorie nemá model. Totiž byla-li by T sporná, pak pro každou formuli φ by platilo $T \vdash \varphi$ i $T \vdash \neg\varphi$. Dle VoK by muselo být v každém modelu teorie T pravdivé φ i $\neg\varphi$, což není možné.

Obsah

Před důkazem VoÚ se budeme zabývat několika pomocnými tvrzeními, která jsou sama o sobě zajímavá.

Definice

Teorie S se nazývá **rozšířením** teorie T (S **obsahuje** T), jestliže jazyk S obsahuje jazyk T a je-li každý axiom teorie T dokazatelný v S. Rozšíření S teorie T se nazývá **konzervativní**, jestliže každá formule jazyka teorie T, která je dokazatelná v S, je dokazatelná v T. Jestliže teorie T a S jsou rozšířeními jedna druhé, pak říkáme, že jsou **ekvivalentní**.

Poznámka: Je-li S rozšířením T, je každá formule dokazatelná v T dokazatelná také v S.
Vztahy teorií "být rozšířením" a "být konzervativním rozšířením" jsou tedy tranzitivní a reflexivní.

Věta o konstantách (VoKonst)

Je-li S rozšíření T takové, že jazyk S obsahuje nové konstanty $c_1, \ldots, c_n$, které jsou od sebe různé, ale S neobsahuje nové axiomy, pak pro každou formuli φ jazyka teorie T platí:
$T \vdash \varphi$ právě když $S \vdash \varphi(x_1/c_1, \ldots, x_n/c_n)$.
Speciálně je tedy S konzervativním rozšířením T.

Důkaz: Tvrzení dokážeme nejdříve pro jednu konstantu; poté ho indukcí rozšíříme na více konstant. Předpokládejme tedy $n = 1$ a pro jednoduchost pišme c místo c_1.
"$\Rightarrow$" Nechť $T \vdash \varphi$, tj. $\ldots, \varphi$ je důkaz φ z T. V teorii S lze tento důkaz prodloužit o formule $(\forall x)\varphi$ (G na φ), $(\forall x)\varphi \Rightarrow \varphi(x/c)$ (axiom specifikace), $\varphi(x/c)$ (MP na předchozí formule). Tedy $\ldots, \varphi, (\forall x)\varphi, (\forall x)\varphi \Rightarrow \varphi(x/c), \varphi(x/c)$ je důkaz z S, a proto $S \vdash \varphi(x/c)$.

"$\Leftarrow$" Nechť $S \vdash \varphi(x/c)$, tj. nechť existuje důkaz $\varphi_1, \ldots, \varphi_k$ formule $\varphi(x/c)$ z S (tj. $\varphi_k = \varphi(x/c)$). Zvolme proměnnou y, která se v tomto důkaze nevyskytuje (tj. nevyskytuje se v žádné φ_i). (Při této volbě je proměnná y substituovatelná za c v každé formuli φ_i.) Indukcí se dá dokázat (viz přednáška), že $\varphi_1(c/y), \ldots, \varphi_k(c/y)$ je důkaz z T.
Tedy $T \vdash (\varphi(x/c))(c/y)$, tj. $T \vdash \varphi(x/y)$. Uvědomme si, že proměnná x je substituovatelná za proměnnou y ve formuli $\varphi(x/y)$. Proto platí, že prodloužíme-li důkaz $\ldots, \varphi(x/y)$ z T na posloupnost $\ldots, \varphi(x/y), (\forall y)\varphi(x/y), (\forall y)\varphi(x/y) \Rightarrow (\varphi(x/y))(y/x), (\varphi(x/y))(y/x)$ dostaneme důkaz formule $(\varphi(x/y))(y/x)$ z T (postupně použitím G, (A4), MP).
Uvědomíme-li si, že $(\varphi(x/y))(y/x)$ je formulí φ, vidíme $T \vdash \varphi$.

Nyní tvrzení snadno rozšíříme na $c_1, \ldots, c_n$. Zatím jsme dokázali, že za uvedených podmínek platí $T \vdash \varphi$ právě když $S \vdash \varphi(x/c)$. Označíme-li T' teorii S (tj. její jazyk obsahuje c_1) a jako S' teorii, která vznikne z S přidáním c_2 do jazyka, dostaneme použitím dokázaného tvrzení na formuli $\psi = \varphi(x_1/c_1)$, že $T' \vdash \psi$, právě když $S' \vdash \psi(x_2/c_2)$, tj. máme $S \vdash \varphi(x_1/c_1)$, právě když $S' \vdash \varphi(x_1/c_1, x_2/c_2)$. Zároveň máme $T \vdash \varphi$, právě když $S \vdash \varphi(x_1/c_1)$, tedy celkem $T \vdash \varphi$, právě když $S' \vdash \varphi(x_1/c_1, x_2/c_2)$. Opakovaným použitím této úvahy nakonec dostaneme požadované tvrzení.

Definice

Formule φ je **variantou** formule ψ, jestliže existuje posloupnost $\varphi = \theta_1, \theta_2, \ldots, \theta_n = \psi$ formulí tak, že pro každé $i < n$ vznikne formule θ_{i+1} z formule θ_i nahrazením jedné podformule formule θ_i, která je ve tvaru $(\forall x)\chi$ (popř. $(\exists x)\chi$) formulí $(\forall y)\chi(x/y)$ (popř. $(\exists y)\chi(x/y)$), kde proměnná y je substituovatelná za x v χ a není volná v χ.

Věta o variantách

Je-li formule φ variantou formule ψ, pak $\vdash \varphi \Leftrightarrow \psi$.