

Výroková a predikátová logika

Petr Štěpánek

Historie

Prehistorie

Aristoteles 384 – 322 př. n. l. Sylogistická logika

Příklad sylogismu

Teze Každý člověk je smrtelný

Antiteze Aristoteles je člověk

Synteza Aristoteles je smrtelný

Formální zápis

Jazyk obsahuje dva predikáty C (člověk) a S (smrtelný), kvantifikátor $\forall$ a proměnnou x . Oba predikáty jsou *unární* (to znamená s jedním argumentem).

Teze $\forall x(C(x) \rightarrow S(x))$

Antiteze $C(\text{Aristoteles})$

Synteza $S(\text{Aristoteles})$

V predikátové logice můžeme tezi vyjádřit také ve tvaru

$$C(x) \rightarrow S(x) \quad \text{Věta o uzávěru}$$

a odvodit její instanci (speciální případ)

$$C(\text{Aristoteles}) \rightarrow S(\text{Aristoteles}) \quad \text{Instance}$$

Z antiteze potom můžeme odvodit syntezu

$$S(\text{Aristoteles}) \quad \text{Modus ponens}$$

5

Aristoteles zkoumal také modality

$$\Box A \quad \text{„je nutné } A\text{“}$$

$$\Diamond A \quad \text{„je možné } A\text{“}$$

Tak položil základy *modální logiky*.

6

Středověká scholastika

- Komentuje Aristotela
- Vychází ze sylogismů
- Zavádí prvky „logiky času“ (temporální logiky)

7

William Occam (1290 - 1349)

- scholastický filosof představitel nominalismu
- usiloval o oddělení filosofie od teologie
- Occamova břitva

8

Temporální logika je druhem modální logiky, modalita se týká času.

Čas $\{0, 1, 2, 3, \dots\}$ v tomto případě je diskretní

Modality

$\bigcirc A$ „v příštím okamžiku bude platit A “

$\square A$ „od jistého okamžiku bude stále platit A “

$\diamond A$ „někdy v budoucnu bude platit A “

9

Novověká logika

- základem stále Aristoteles
- ve stínu filosofie
- a hledání univerzálního jazyka
- po velkých objevech ve fyzice a astronomii přihlíží více ke zkušenosti

10

Gotfried Wilhelm Leibniz (1646 - 1716)

- polyhistor, filozof, matematik
- filozofie dualismu substance a ducha
- monády („tento svět je nejlepší ze všech možných světů“)
- ve stejnou dobu jako Newton a nezávisle na něm položil základy diferenciálního a integrálního počtu. Jeho značení se používá dodnes.
- věnoval se též
 - hledání univerzálního jazyka
 - logice („ars calculandi“)

11

Leibniz zavedl do logiky znaménko rovnosti $a = b$, aby ukázal, že a je totožné s b .

Idea: Mohu-li říci o b všechno, co mohu říci o a a také mohu-li říci o a všechno, co mohu říci o b pak a a b jsou totožné. Píšeme ' $a = b$ '. Potom a mohu nahradit v každém tvrzení tvrzením b a pravdivostní hodnota původního tvrzení zůstane zachována.

(Identitatis indiscernibilum) Totožnost nerozlišitelného.

12

Leibnizovy principy

- 1. $a = a$
- 2. Jestliže $a = b$ a $b = c$ pak $a = c$.
- 3. $a = \text{ne } (a)$
- 4. „ a je b “ = „ $(\text{ne } b)$ “ je „ $(\text{ne } a)$ “ „

13

Bernard Bolzano (1781 - 1848)

- průkopník moderních metod v matematice
- *Vědosloví* 1837 se jako první systematicky zabývá základy (výrokové) logiky
- *Paradoxy nekonečna* 1851

14

George Boole (1815 - 1864)

- irský matematik
- položil základy moderní matematické logiky
- autor knihy „*Matematická analýza logiky jsoucí esejem ke kalkulu deduktivního uvažování*“ 1847
- rozpracoval výrokovou logiku

15

Gottlob Frege (1848 - 1925)

- německý matematik a logik
- zavedl formální jazyk vedle přirozeného
- habilitační spis „*Begriffsschrift ...*“ (pojmové písmo) 1879
- předjal základní pojmy moderní matematické logiky
- zavedl kvantifikátory
„všichni“, „někteří“, „mnoho“, „většina“.
- *Základy aritmetiky* 1884

16

Georg Cantor (1845 -1912)

- je zakladatelem Teorie množin

$$x \in y$$

- predikát náležení vyžaduje dva argumenty, je binární.

17

Úspěchy

- Cantor ukázal, že skoro všechna reálná čísla jsou transcendentní. Do té doby bylo známo, že transcendentní jsou čísla e a π .
- Hilbert řeší Gordonův problém.
- Množinová symbolika se začíná běžně používat v algebře a geometrii.

18

Paradoxy teorie množin

- Paradox množiny všech množin (1895)
- Paradox Burali-Forti (1897)
- **Russelův paradox (1902)**
- Richardsův paradox (1905)
- Grellingův paradox (1908)

19

Russelův paradox

$$Z = \{x \mid x \notin x\}$$

Kdyby Z byla množina, potom buď $Z \in Z$ nebo $Z \notin Z$.

Ale $Z \in Z \Rightarrow Z \notin Z$

$Z \notin Z \Rightarrow Z \in Z$

Tedy

$$Z \in Z \Leftrightarrow Z \notin Z$$

20

Bertrand Russell (1872 - 1970)

- *Principia Mathematica* s Alfredem N. Whiteheadem
- *Logicismus*
- *Stratifikace proměnných* $x_n \in x_m$ jen když $m = n + 1$
- *Teorie Typů*

21

Aktéři

- **David Hilbert** (1862-1943)
- **Bertrand Russell** (1872-1970)
- **Alfred Tarski** (1902-1983)
- **Arend Heyting** (1898- 1980)
- **L.E.J. Brouwer** (1881 - 1966) „Bertus“

22

Situace na počátku minulého století

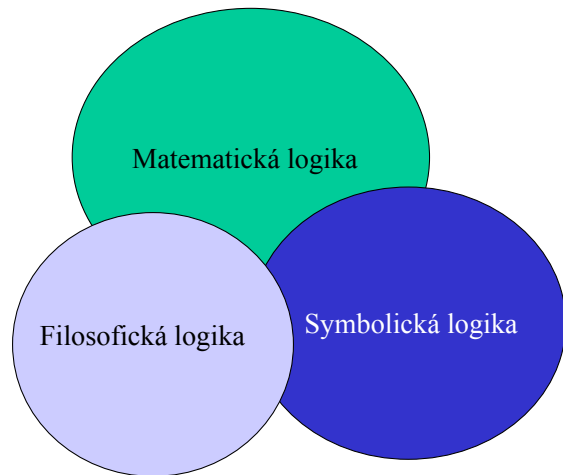
- **Formalismus (1904) Hilbert:** Matematika je „formální systém“ pracujeme jen se symboly, slovy ze symbolů a konečnými posloupnostmi slov. Jejich význam je ryze formální, samy o sobě nemají žádný smysl. **Tarski (1932)** Symboly mají smysl. (sémantika)
- **Logicismus (1908) Russell** Matematika je součástí logiky, pracujeme s vybranou podmnožinou přirozeného jazyka.
- **Intuicionismus (1908) Brouwer a Heyting** Intuicionistická logika, vylučuje zákon vyloučeného třetího (tertium non datur), důkazy sporem, klade důraz na konstruktivní charakter důkazů.

23

Logiky vyšších řádů

- predikátová logika prvního řádu: jeden druh proměnných pro individua. (přirozená čísla, množiny, prvky grupy atd.)
- predikátová logika prvního řádu s více druhy proměnných pro individua (body, přímky, roviny atd.)
- predikátová logika druhého řádu: dva druhy proměnných, pro individua a (meta)proměnné pro množiny individuí, predikáty a funkce.
- Teorie typů má proměnné všech řádů
- **Příklad.** Axiom indukce v aritmetice druhého řádu
$$(0 \in X \ \& \ \forall x [x \in X \Rightarrow s(x) \in X]) \Rightarrow \forall x [x \in X]$$

24



25

Každá z těchto logik má své části, například matematická a symbolická logika pracují s těmito logikami

- logika prvního řádu
- logika druhého řádu
- modální logika
- temporální logika
- konstruktivní logika
- přirozená dedukce
- teorie typů
- a další

26

Logika prvního řádu

- je nejpoužívanější a nejlépe prozkoumaná
- v různé míře je součástí některých dalších logik
- představíme ji jako *formální systém* (à la Hilbert)
- je výhodné začít výkladem této logiky
- proto se jí budeme v této přednášce zevrubně zabývat

27

Formální systém logiky prvního řádu obsahuje

- jazyk
- axiomy
- odvozovací pravidla
- důkazy a věty

28

Jazyk prvního řádu

Jazyk obsahuje

- (i) **Proměnné** $x, y, z, x_1, x_2, \dots, y', y'', \dots$ neomezeně mnoho
- (ii) **Funkční symboly** $f, g, h, \dots, f_1, f_2, \dots$ každý má svou četnost (počet argumentů) $n \geq 0$.
- (iii) **Predikátové symboly** $p, q, r, \dots, p_1, p_2, \dots$ každý má svou četnost $n > 0$.
- (iv) **Symboly pro logické spojky** $\neg$ negace, $\vee$ disjunkce, $\wedge$ konjunkce, $\rightarrow$ implikace, $\leftrightarrow$ ekvivalence.
- (v) **Symboly pro kvantifikátory** $\forall$ univerzální $\exists$ existenční.

29

Jazyk prvního řádu může (ale nemusí) obsahovat binární predikát rovnosti „ $=$ “, který se liší od ostatních predikátů, na které logika neklade žádné požadavky.

V logice respektujeme praxi s jakou se s predikátem rovnosti nakládá v matematice, informatice a jinde. Chceme aby sobě rovná individua (termy) měla stejné vlastnosti. Z toho pak plyne, že rovnost musí být reflexivní, symetrická a tranzitivní, tedy musí mít vlastnosti ekvivalence.

30

Logické a speciální symboly

- Proměnné, logické spojky a kvantifikátory jsou společné všem jazykům prvního řádu. Říkáme jim proto *logické symboly*.
- Z důvodů, které jsme uvedli, predikát rovnosti také řadíme k logickým symbolům.
- Obsahuje-li jazyk predikát rovnosti, mluvíme o jazyku s rovností, jinak mluvíme o jazyku bez rovnosti (je-li to vůbec potřebné).
- Ostatní predikáty a všechny funkční symboly budeme nazývat *speciální*. Vyjadřují vlastnosti operací a pojmů v nějaké speciální teorii.

31

Jazyk je tedy určen svými speciálními symboly.
(u běžných teorií jich nebývá mnoho)

Příklady

- (a) Teorie množin má jazyk s rovností a jediným speciálním symbolem $\in$. Píšeme $L_1 = \{\in\}$.
- (b) Teorie grup má jazyk s rovností a dvěma speciálními symboly, konstantou e a binárním funkčním symbolem $\bullet$. Píšeme $L_2 = \{e, \bullet\}$.
- (c) Jazyk aritmetiky (prvního řádu) je s rovností a obsahuje pět speciálních symbolů, konstantu 0 , symboly pro operace $S, +, \bullet$ a binárním predikátem $\leq$. Píšeme $L_3 = \{0, S, +, \bullet, \leq\}$.

32

Postup výkladu

- Nebudeme pracovat se všemi logickými symboly najednou. Nejprve se budeme zabývat logickými spojkami, výsledkem bude takzvaná *výroková logika*.
- Potom k nim přidáme oba kvantifikátory a budeme mluvit o *predikátové logice (bez rovnosti)*.
- Nakonec přidáme predikát rovnosti a budeme mluvit o *predikátové logice s rovností*.

33

Výroková logika

34

Jazyk prvního řádu pro potřeby výrokové logiky můžeme zjednodušit. Vyjdeme z neprázdné množiny P , která může být konečná i nekonečná. Její prvky nazýváme *prvotní formule* nebo *výrokové proměnné*.

Jazyk výrokové logiky obsahuje

- (i) výrokové proměnné, tedy prvky množiny P .
- (ii) logické spojky $\neg, \vee, \&, \rightarrow, \leftrightarrow$.
- (iii) pomocné symboly (závorky) $(,), [,], \{, \}, \dots$.

35

Formule

Je-li dán jazyk výrokové logiky pak následující výrazy jsou formule.

- (i) každá výroková proměnná $p \in P$ je formule.
- (ii) jsou-li výrazy A, B formule, pak výrazy $\neg A, (A \vee B), (A \& B), (A \rightarrow B), (A \leftrightarrow B)$ jsou také formule.
- (iii) každá formule vznikne konečným užitím pravidel (i) a (ii).

36

Příklad

Je-li $P = \{ p, q, r, s \}$ množina výrokových proměnných, pak

p, q, r, s jsou formule podle (i)
 $(p \vee q)$ $(p \& r)$ jsou formule podle (ii)
 $((p \vee q) \rightarrow (p \& r))$ je formule podle (iii)

Snadno se nahlédne, že výrazy

ppr $(\rightarrow p)$ $(\rightarrow \rightarrow)$

nejsou formule.

37

Sémantika výrokové logiky

Formule výrokové logiky jsou konstruovány nad množinou P výrokových proměnných (prvotních formulí), které ve výrokové logice neanalyzujeme. Jejich pravdivost tedy musí být dána z vnějšku.

Množina pravdivostních hodnot $\{1, 0\}$ $(\{true, false\})$

(i) *Pravdivostní ohodnocení* (valuace) výrokových proměnných z P je zobrazení, které každé výrokové proměnné z P přiřadí pravdivostní hodnotu 1 nebo 0.

38

Je-li dáno pravdivostní ohodnocení v výrokových proměnných, pak lze každé výrokové formuli A jednoznačně přiřadit pravdivostní hodnotu $v(A)$.

Postupujeme indukcí podle složitosti formule A .

$v(A) = v(A)$ je-li A výroková proměnná

$v(\neg A) = 0$ je-li $v(A) = 1$
 $= 1$ je-li $v(A) = 0$

$v(A \& B) = 1$ je-li $v(A) = v(B) = 1$
 $= 0$ jinak

39

$v(A \vee B) = 0$ je-li $v(A) = v(B) = 0$
 $= 1$ jinak

$v(A \rightarrow B) = 0$ je-li $v(A) = 1$ a $v(B) = 0$
 $= 1$ jinak

$v(A \leftrightarrow B) = 1$ je-li $v(A) = v(B) = 0$
 $= 0$ jinak

40

Říkáme, že $v(A)$ je *pravdivostní hodnota* formule A při ohodnocení v .

Formule A je pravdivá při ohodnocení v , je-li $v(A) = 1$, jinak je *nepravdivá*.

Je-li formule A pravdivá při ohodnocení v , říkáme, že v je *model* A a píšeme $v \models A$.

41

Je-li v pravdivostní ohodnocení, A formule, nechť R je množina všech výrokových proměnných ve formuli A .

Snadno se nahlédne, že pravdivostní hodnota formule A při ohodnocení v závisí jenom na pravdivostních hodnotách, které v přiřazuje výrokovým proměnným z R .

42

Tautologie, splnitelné množiny formulí

Nechť A je formule, T je množina formulí.

(i) Říkáme, že A je *tautologie*, jestliže je pravdivá při každém ohodnocení. Píšeme $\models A$.

(ii) Říkáme, že množina formulí T je *splnitelná* jestliže existuje pravdivostní ohodnocení v takové, že každá formule A z T je pravdivá při ohodnocení v . V takovém případě říkáme, že v je *model* T .

43

(iii) Říkáme, že formule A je (*tautologickým*) *důsledkem* množiny formulí T , jestliže každý model množiny T je také modelem A . Píšeme $T \models A$.

44

Příklady

Definice pravdivosti dává možnost rozhodnout o každé formuli, zda je či není tautologií. S tím spojený algoritmus je výpočtově exponenciálně složitý.

$A \vee \neg A$	Zákon vyloučeného třetího
$\neg(A \& \neg A)$	Vyloučení kontradikce
$\neg(A \& B) \leftrightarrow (\neg A \vee \neg B)$	de Morganova pravidla
$\neg(A \vee B) \leftrightarrow (\neg A \& \neg B)$	
$\neg\neg A \leftrightarrow A$	Zákon dvojité negace

45

Snadno se zjistí, že pro libovolné ohodnocení v a libovolné formule A, B , je-li v modelem A a $A \rightarrow B$, potom v je modelem B .

Odtud také plyne, že pro libovolnou množinu formulí T a formuli A , plyne

$$T \models A \quad \text{a} \quad T \models A \rightarrow B \quad \text{implikuje} \quad T \models B$$

46

Formální systém výrokové logiky

- Jazyk / Redukce jazyka
- Axiomy / schemata axiomů
- Odvozovací pravidlo
- Důkazy
- Důkazy z předpokladů
- Věty o úplnosti
- Věta o kompaktnosti

47

Redukce jazyka

Chceme-li úsporně volit axiomy, je výhodné redukovat počet spojek na spojky základní, v našem případě na negaci a implikaci $\neg, \rightarrow$.

Potom

$(A \vee B)$ je zkratka za formuli $(\neg A \rightarrow B)$

$(A \& B)$ je zkratka za formuli $\neg(A \rightarrow \neg B)$

$(A \leftrightarrow B)$ je zkratka za formuli $((A \rightarrow B) \& (B \rightarrow A))$

48

Axiomy

Jsou-li výrazy A , B , C formule, pak každá formule následujících tvarů je axiom.

$$A1 \quad (A \rightarrow (B \rightarrow A))$$

$$A2 \quad (A \rightarrow (B \rightarrow C)) \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow C)]$$

$$A3 \quad (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$$

49

Protože pro každou volbu formulí A , B , C vznikne jedna instance výrazů $A1$, $A2$, $A3$ tedy nový axiom, říkáme, že $A1$, $A2$, $A3$ jsou *schemata axiomů*.

Z jazyka výrokové logiky lze vytvořit nekonečně mnoho formulí, každé schema generuje nekonečně mnoho axiomů.

Formální systém výrokové logiky má tedy tři schemata axiomů a z nich odvozeno mnoho axiomů.

Je-li množina výrokových proměnných spočetná, je spočetná množina všech formulí a množina všech axiomů.

50

Odvozovací pravidlo (modus ponens)

Z formulí A a $A \rightarrow B$ odvodí formuli B .

$$\frac{A \quad A \rightarrow B}{B}$$

51

Důkaz, dokazatelnost

(i) Je-li A říkáme, že konečná posloupnost formulí $A_1, A_2, \dots, A_n$ je důkazem formule A ,

a) Je-li A_n formule A

b) Jestliže pro každé $i, 1 \leq i \leq n$, je formule A_i buď axiom nebo je odvozena z předchozích formulí v důkazu $A_j, 1 \leq j < i$ pravidlem modus ponens.

(ii) Existuje-li důkaz formule A , říkáme, že A je dokazatelná ve výrokové logice nebo, že A je větou výrokové logiky a píšeme $\vdash A$.

52

Jednoduché věty výrokové logiky

(v1) $A \rightarrow A$

Sestrojíme posloupnost formulí, která bude důkazem formule (v1).

$ - A \rightarrow ((A \rightarrow A) \rightarrow A)$	instance A1
$ - (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow [(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)]$	instance A2
$ - (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$	modus ponens
$ - (A \rightarrow (A \rightarrow A))$	instance A1
$ - A \rightarrow A$	modus ponens

53

Důkaz z předpokladů

Nechť T je množina formulí, nechť A je formule.

(i) Říkáme, že posloupnost formulí

$$A_1, A_2, \dots, A_n$$

je *důkaz formule A z (množiny předpokladů) T* , jestliže

a) A_n je formule A

b) a pro každé $i, 1 \leq i \leq n$, je formule A_i axiom nebo prvek T nebo je odvozena z předchozích formulí v důkazu $A_j, 1 \leq j < i$ pravidlem modus ponens.

(ii) Existuje-li důkaz formule A z předpokladů T , říkáme, že *A je dokazatelná z T* a píšeme $T \vdash A$.

54

Věta o dedukci

Nechť T je množina formulí a nechť A, B jsou formule, potom

$$T \vdash A \rightarrow B \text{ právě když } T \cup \{A\} \vdash B$$

55

Poznámky. Místo $T \cup \{A\}$ na pravé straně píšeme T, A . Pravá strana ekvivalence odpovídá tomu, jak se obvykle implikace dokazují.

Věta o dedukci, je větou o existenci důkazů. Existuje-li důkaz tvrzení na levé straně ekvivalence, pak také existuje důkaz tvrzení na pravé straně a naopak.

56

Důkaz

a) Necht' $T \mid -A \rightarrow B$ a necht' $A_1, A_2, \dots, A_n, A \rightarrow B$ je důkaz $A \rightarrow B$ z předpokladů T .

Potom $A_1, A_2, \dots, A_n, A, A \rightarrow B, B$ je důkaz B z předpokladů T, A .

b) Necht' $T \cup \{A\} \mid -B$ a necht' $A \equiv A_0, A_1, A_2, \dots, A_n$ je důkaz B z předpokladů T, A . Omezenou indukcí pro $j, 0 \leq j < n$ dokážeme $T \mid -A \rightarrow A_j$. Tím pro $j=n$ důkaz bude hotov.

57

Budeme rozebírat čtyři případy

b1) $j=0$, potom $\mid -A_0 \rightarrow A$ plyne z (v1).

b2) A_j je axiom výrokové logiky, potom $A_j \rightarrow (A \rightarrow A_j)$ je instancí schematu AI a $A \rightarrow A_j$ odvodíme pomocí pravidla modus ponens.

b3) A_j je předpoklad z T . Postupujeme stejně jako v předešlém případě.

b4) A_j je odvozena z formulí A_i, A_k $i, k < j$. Bez újmy na obecnosti můžeme předpokládat, že A_i je tvaru $A_k \rightarrow A_i$.

58

Podle indukčního předpokladu

$$\begin{aligned} T \mid -A \rightarrow A_k \\ T \mid -A \rightarrow \underbrace{(A_k \rightarrow A_i)}_{A_j} \end{aligned} \quad (1)$$

Ze schematu A2 plyne

$$T \mid -(A \rightarrow \underbrace{(A_k \rightarrow A_i)}_{A_j}) \rightarrow [(A \rightarrow A_k) \rightarrow (A \rightarrow A_i)]$$

Odkud dvojitým použitím pravidla modus ponens a předpokladů (1) dostáváme

$$T \mid -A \rightarrow A_j$$

Pro $j=n$ je věta dokázána.

59

Příklady použití

$$\mid -(A \rightarrow (B \rightarrow C)) \rightarrow (B \rightarrow (A \rightarrow C)) \quad (I)$$

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

$$(A \rightarrow (B \rightarrow C)), B \mid -(A \rightarrow C))$$

$$(A \rightarrow (B \rightarrow C)), B, A \mid -C$$

Ale

$$\frac{A \quad (A \rightarrow (B \rightarrow C))}{(B \rightarrow C)} \quad \frac{B \quad (B \rightarrow C)}{C}$$

Tím je (1) dokázáno. Na pořadí antecedentů v implikaci nezáleží (obrácená implikace k (1) se dokáže stejným způsobem).

60

$$\mid -(A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)] \quad (2)$$

$$(A \rightarrow B) \mid -[(B \rightarrow C) \rightarrow (A \rightarrow C)]$$

$$(A \rightarrow B), (B \rightarrow C) \mid -(A \rightarrow C)$$

$$(A \rightarrow B), (B \rightarrow C), A \mid -C$$

K důkazu (2) stačí dvojnásobným použitím pravidla modus ponens z daných předpokladů dokázat C .

$$\frac{A \quad A \rightarrow B}{B} \quad \frac{B \quad B \rightarrow C}{C}$$

V uvedených příkladech se důkazy opíraly jen o Větu o dedukci a pravidlo modus ponens.

61

Dalších šest pomocných vět výrokové logiky

$$\mid -\neg A \rightarrow (A \rightarrow B) \quad (v2)$$

$$\mid -\neg A \rightarrow (\neg B \rightarrow \neg A) \quad \text{schema } A2$$

$$\neg A \mid -A \rightarrow B \quad A3, MP$$

$$\mid -\neg A \rightarrow (A \rightarrow B) \quad \text{Věta o dedukci}$$

Tím je věta (v2) dokázána.

62

$$\mid -\neg\neg A \rightarrow A \quad (v3)$$

$$\mid -\neg\neg A \rightarrow (\neg A \rightarrow \neg\neg A) \quad (v2)$$

$$\neg\neg A \mid \neg A \rightarrow \neg\neg A \quad VD$$

$$\neg\neg A \mid -\neg\neg A \rightarrow A \quad (A3), MP$$

$$\neg\neg A \mid -A \quad VD$$

$$\mid -\neg\neg A \rightarrow A \quad VD$$

63

Formuli (v3) lze zapsat ve tvaru $\neg A \vee A$ a to je zákon vyloučeného třetího (tertium non datur). Naše logika je tedy klasická, ne intuicionistická.

64

$$\begin{array}{l}
 | - A \rightarrow \neg\neg A \quad (v4) \\
 \hline
 | - \neg\neg\neg A \rightarrow \neg A \quad (v3) \\
 | - A \rightarrow \neg\neg A \quad (A3), MP
 \end{array}$$

65

$$\begin{array}{l}
 | - (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A) \quad (v5) \\
 \hline
 \neg\neg A, A \rightarrow B | - A \quad (v3), MP \\
 \neg\neg A, A \rightarrow B | - B \quad MP \\
 \neg\neg A, A \rightarrow B | - \neg\neg B \quad (v4), MP \\
 A \rightarrow B | - \neg\neg A \rightarrow \neg\neg B \quad VD \\
 A \rightarrow B | - (\neg B \rightarrow \neg A) \quad (A3), MP \\
 | - A \rightarrow B \rightarrow (\neg B \rightarrow \neg A) \quad VD
 \end{array}$$

66

$$\begin{array}{l}
 | - A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B)) \quad (v6) \\
 \hline
 A, A \rightarrow B | - B \quad MP \\
 A | - (A \rightarrow B) \rightarrow B \quad VD \\
 A | - \neg\neg B \rightarrow \neg(A \rightarrow B) \quad (v5), (A3), MP \\
 | - A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B)) \quad VD
 \end{array}$$

67

$$\begin{array}{l}
 | - (\neg A \rightarrow A) \rightarrow A \quad (v7) \\
 \hline
 | - \neg A \rightarrow (\neg A \rightarrow \neg(\neg A \rightarrow A)) \quad (v6) \\
 \neg A | - \neg(\neg A \rightarrow A)) \quad 2 \times VD \\
 | - \neg A \rightarrow \neg(\neg A \rightarrow A) \quad VD \\
 | - (\neg A \rightarrow A) \rightarrow A \quad (A3), MP
 \end{array}$$

68

Dokázali jsme několik pomocných vět výrokové logiky.

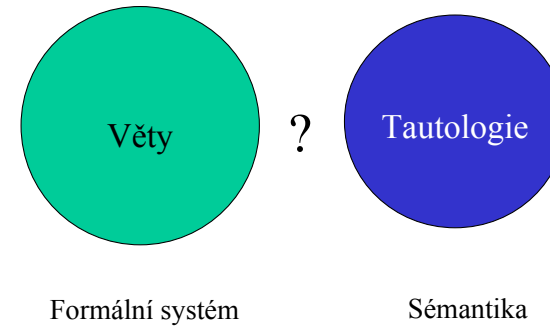
Nyní se budeme zabývat vztahem vět odvoditelných ve formálním systému a jejich sémantikou.

Naším cílem je dokázat *věty o úplnosti*, které dávají dohromady oba pojmy: *věty a tautologie*.

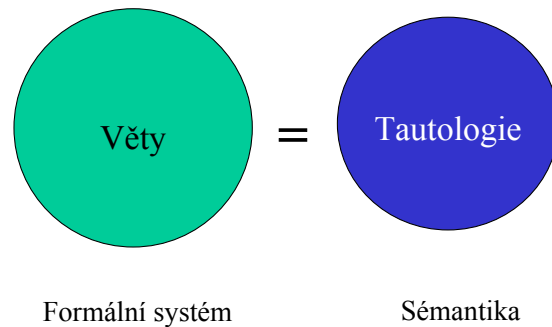
Dokážeme

$$\begin{array}{lll} \vdash A & \text{právě když} & \models A \\ T \vdash A & \text{právě když} & T \models A \end{array}$$

69



70



71

Bezespornost a maximalita

Nechť T je množina formulí

- (i) Říkáme, že T je *sporná*, (nekonzistentní), jestliže libovolná formule A je dokazatelná z předpokladů T , jinak je T *bezesporná* (konzistentní).
- (ii) T je *maximální bezesporná množina*, jestliže je bezesporná a jediná bezesporná množina, která obsahuje T .
- (iii) Množinu všech formulí dokazatelných z T označíme $Con(T)$, tedy

$$Con(T) = \{A \mid T \vdash A\}$$

72

Cvičení

Necht' T a S jsou množiny formulí. Dokažte

- a) $T \subseteq \text{Con}(T)$
- b) Je-li $T \subseteq S$ potom $\text{Con}(T) \subseteq \text{Con}(S)$
- c) $\text{Con}(\text{Con}(T)) = \text{Con}(T)$
- d) Je-li $\perp$ bezsporná, potom $\text{Con}(\perp)$ je také bezsporná

73

Cvičení

Necht' T je maximální bezsporná množina a A, B jsou formule.

- a) je-li $T \vdash A$, potom $A \in T$
- b) Pro každou formuli A platí
 $T \vdash A$ právě když $T \cup \{\neg A\}$ je sporná
- c) T je sporná, právě když $T \vdash p \ \& \ \neg p$ pro nějakou výrokovou proměnnou.

74

- d) pro každou formuli A , právě jedna z formulí
 $A, \neg A$ je prvkem T .

- e) $A \ \& \ B \in T$ právě když $A \in T$ a $B \in T$

- f) $A \vee B \in T$ právě když A nebo B náleží do T

75

Věta (Lindenbaum)

Každou bezspornou množinu formulí T lze rozšířit do maximální bezsporné množiny $S, T \subseteq S$.

76

Důkaz

Uspořádejme všechny formule jazyka do posloupnosti

$$A_0, A_1, A_2, \dots, A_n, \dots$$

na uspořádání formulí nezáleží, důležité je, aby posloupnost byla prostá.

Vytvoříme neklesající posloupnost bezesporných množin

$$T \equiv T_0 \subseteq T_1 \subseteq \dots T_n \subseteq \dots$$

následujícím postupem.

77

Je-li $T \cup \{A_0\}$ bezesporná, definujeme $T_1 = T \cup \{A_0\}$, jinak položíme $T_1 = T$. V α -tém kroku položíme $T_{\alpha+1} = T_\alpha \cup \{A_\alpha\}$ je-li to bezesporná množina, jinak $T_{\alpha+1} = T_\alpha$. Je-li α limitní ordinál položíme $T_\alpha = \bigcup_{\beta < \alpha} T_\beta$.

Nechť S je sjednocení všech množin T_α . Ukážeme, že S je bezesporná množina. Postupujeme sporem.

78

Předpokládejme, že S není bezesporná. Potom existuje důkaz

$$B_0, B_1, \dots, B_n$$

formule $p \& \neg p$, kde p je výroková proměnná. Necht'

$$C_1, C_2, \dots, C_m$$

jsou všechny formule z S , které se vyskytují v uvedeném důkazu. Pak existuje α , takové, že

$$C_1, C_2, \dots, C_m \subseteq T_\alpha$$

To znamená, že T_α je sporná - spor.

79

Zbývá dokázat, že S je maximální bezesporná množina. Předpokládejme, že S' je bezesporná množina a $S \subseteq S'$.

Necht' některá formule A_α z posloupnosti formulí je prvkem S' . Potom $T_\alpha \cup \{A_\alpha\}$ je bezesporná, a tedy

$$T_{\alpha+1} = T_\alpha \cup \{A_\alpha\}$$

Proto $A_\alpha \in S$ a $S=S'$.

80

Věta o bezespornosti a splnitelnosti

Je-li T množina formulí výrokové logiky, potom

T je bezesporná, právě když je splnitelná.

81

Důkaz.

a) Předpokládejme, že T je splnitelná a v je model T .
Tedy $v \models T$.

Ukážeme, že každá formule dokazatelná z předpokladů T , je pravdivá při ohodnocení v . Postupujeme indukcí.

Nechť $A_0, A_1, \dots, A_n$ je důkaz formule A_n z předpokladů T .
Pro libovolné $m, m \leq n$ platí

Je-li A_m axiom výrokové logiky, nebo prvek T , je $v \models A_m$.

82

Je-li A_m odvozena z formulí $A_i, A_i \rightarrow A_m$ pravidlem modus ponens, pak z indukčního předpokladu a korektnosti pravidla modus ponens dostáváme $v \models A_m$. Tedy každá formule dokazatelná z předpokladů T je pravdivá při ohodnocení v .

Protože $p \wedge \neg p$ pro výrokovou proměnnou p není pravdivá při ohodnocení v , není tato formule dokazatelná z T a T je bezesporná množina.

83

b) Nyní předpokládejme, že T je bezesporná. Podle Lindenbaumovy věty, lze T rozšířit do maximální bezesporné nadmnožiny S .

Nechť v je pravdivostní ohodnocení definované vztahem

$$v(p) = 1 \quad \text{právě když} \quad p \in S$$

Pro libovolnou formuli A dokážeme

$$A \in S \quad \text{právě když} \quad v \models A \quad (I)$$

84

Postupujeme indukcí podle složitosti formule A .

Přímo z definice plyne (1) pro výrokové proměnné.

Ze cvičení d) plyne, že platí-li (1) pro B , pak platí i pro $\neg B$.

Ze cvičení f) plyne, že platí-li (1) pro B, C , pak platí i pro $B \rightarrow C$.

Z toho vyplývá, že $v \models S$ a protože $T \subseteq S, v \models T$.

Množina T je tedy splnitelná.

85

Důsledek. Věty o úplnosti.

Je-li T množina formulí, A formule, potom platí

$$(i) \quad T \vdash A \text{ právě když } T \models A$$

$$(ii) \quad \vdash A \text{ právě když } \models A$$

Z (ii) plyne, že

A je větou výrokové logiky, právě když A je tautologie.

86

Důkaz.

$$\begin{aligned} (i) \quad T \vdash A & \text{ právě když } T \cup \{\neg A\} \text{ je sporná} \\ & \text{právě když } T \cup \{\neg A\} \text{ je nesplnitelná} \\ & \text{právě když } T \models A \end{aligned}$$

(ii) Tvrzení je speciálním případem (i) pro $T = \emptyset$.

87

Výroková logika je bezesporná

Z Věty o úplnosti plyne, že ve výrokové logice jsou dokazatelné právě tautologie.

Formule

$$p \ \& \ \neg p$$

není tautologie, a proto není větou výrokové logiky.

Výroková logika je tedy bezesporná.

88

Věta o kompaktnosti.

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

Důsledek.

Je-li $T \models A$

*pak existuje konečná podmnožina $T' \subseteq T$
taková, že $T' \models A$*

89

Důkaz.

a) Je-li T splnitelná, pak je splnitelná i každá její část.

Předpokládejme, že T není splnitelná. Podle věty o splnitelnosti je T sporná. Tedy $T \models p \ \& \ \neg p$ pro nějakou výrokovou proměnnou.

Ale důkaz sporu využívá jen konečnou podmnožinu T' množiny T . Tedy T' je sporná a proto není ani splnitelná.

90

b) Je-li $T \models A$ potom $T \models A$ (1)
potom $T' \models A$

pro konečnou podmnožinu T' množiny T sestávající z formulí, které se použijí v důkazu (1).

a $T' \models A$

První a poslední krok důkazu využívá tvrzení (i) Věty o úplnosti.

91

Normální tvary výrokových formulí

1

Ke každé formuli dovoluje výroková logika sestavit ekvivalentní formuli v určitém standardním tvaru.

Potřebujeme

- Vědět něco o dokazování formulí s odvozenými spojkami.
- Větu o ekvivalenci (kterou jsme mohli dokázat již dříve).
- Normální tvary výrokových formulí. (Jsou dva).

2

Lemma.

- (i) $A \& B \mid - A \quad A \& B \mid - B$
(ii) $A, B \mid - A \& B$

3

Důkaz.

(i) Výraz $A \& B$ je zkratkou za formuli $\neg(A \rightarrow \neg B)$.

Podle (v2) platí

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

odkud

$$\mid - \neg(A \rightarrow \neg B) \rightarrow A \quad (\text{v3}), (\text{v5}), \text{MP}$$

tedy

$$\mid - (A \& B) \rightarrow A$$

Důkaz druhého tvrzení v (i) postupuje stejně, jen se zamění symboly A a B .

4

(ii) Z (v4) dostáváme

$$A, B \mid - \neg\neg B$$

dále z (v6) a Věty o dedukci plyne

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

Celkem

$$A, B \mid - A \& B$$

5

Důsledek.

Uvědomíme-li si, že ekvivalence $A \leftrightarrow B$ je zkratkou za formuli

$$(A \rightarrow B) \& (B \rightarrow A)$$

dostáváme

$$(i) \quad A \leftrightarrow B \mid - A \rightarrow B$$

$$(ii) \quad A \leftrightarrow B \mid - B \rightarrow A$$

$$(iii) \quad A \rightarrow B, B \rightarrow A \mid - B \leftrightarrow A$$

(iv) Je-li $\mid - A \leftrightarrow B$ potom pro libovolnou množinu T platí $T \mid - A$ právě když $T \mid - B$.

6

Důsledek.

$$(i) \quad \mid - A \leftrightarrow (A \& A) \quad (\text{idempotence})$$

$$(ii) \quad \mid - (A \& B) \leftrightarrow (B \& A) \quad (\text{komutativnost})$$

$$(iii) \quad \mid - ((A \& B) \& C) \leftrightarrow (A \& (B \& C)) \\ (\text{asociativnost})$$

$$(iv) \quad \mid - (A_1 \rightarrow \dots (A_n \rightarrow B) \dots) \leftrightarrow ((A_1 \& \dots \& A_n) \rightarrow B)$$

7

Věta o ekvivalenci.

Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $A_1, A_2, \dots, A_n$ formulemi $A'_1, A'_2, \dots, A'_n$.

Je-li

$$\mid - A_1 \leftrightarrow A'_1 \mid - A_2 \leftrightarrow A'_2 \dots \mid - A_n \leftrightarrow A'_n$$

potom

$$\mid - A \leftrightarrow A'$$

8

Důkaz.

Indukcí podle složitosti formule A .

a) A je výroková proměnná nebo některá z formulí $A_j, 1 \leq j \leq n$.

Potom A' je A pokud k výměně nedojde, jinak A' je A_j .

b) A je tvaru $\neg B$. Potom

$$\begin{aligned} &|- B \leftrightarrow B' \\ &|- B \rightarrow B' \\ &|- A' \rightarrow A \end{aligned} \quad (v5)$$

Opačná implikace se dokazuje podobně.

9

c) A je $B \rightarrow C$ a $|- B \leftrightarrow B' \quad |- C \leftrightarrow C'$

Potom

$$\begin{array}{c} \boxed{B' \rightarrow B} \qquad \boxed{C \rightarrow C'} \\ \vdash \neg(B' \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow ((C \rightarrow C') \rightarrow (B' \rightarrow C'))) \end{array}$$

$$\vdash \neg(B \rightarrow C) \rightarrow (B' \rightarrow C')$$

Opačná implikace se dokáže záměnou čárkovaných a nečárkovaných formulí.

10

de Morganova pravidla.

$$(i) \quad \vdash \neg(A \& B) \leftrightarrow (\neg A \vee \neg B)$$

$$(ii) \quad \vdash \neg(A \vee B) \leftrightarrow (\neg A \& \neg B)$$

11

Důkaz.

Z (v3), (v4) a zavedení ekvivalence plyne $\vdash A \leftrightarrow \neg\neg A$.

Užitím věty o ekvivalenci dostáváme

$$\begin{aligned} \vdash \neg(A \& B) &\leftrightarrow \neg\neg(A \rightarrow \neg B) \\ &\leftrightarrow (\neg\neg A \rightarrow \neg B) \\ &\leftrightarrow (\neg A \vee \neg B) \end{aligned}$$

Tvrzení (ii) se dokazuje obdobně.

12

Důsledek.

- (i) $\vdash A \rightarrow (A \vee B) \quad \vdash B \rightarrow (A \vee B)$ (monotonnost)
- (ii) $\vdash A \leftrightarrow (A \vee A)$ (idempotence)
- (iii) $\vdash (A \vee B) \leftrightarrow (B \vee A)$ (komutativnost)
- (iv) $\vdash ((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$ (asociativnost)

13

Důkaz.

(i) Podle zavedení disjunkce je $\vdash (A \vee B) \leftrightarrow (\neg A \rightarrow B)$, proto formule $A \rightarrow (A \vee B)$ je obdobou (v2) a $B \rightarrow (A \vee B)$ je instancí schematu (A1).

(ii) - (iv) Použitím de Morganových pravidel lze tato tvrzení převést na již dokázaná tvrzení o konjunkci.

14

Lemma o důkazu rozbořem případů.

Je-li T množina formulí a A, B, C jsou formule, potom

$$T, (A \vee B) \vdash C \quad \text{právě když} \quad T, A \vdash C \quad \text{a} \quad T, B \vdash C$$

15

Důkaz.

a) Je-li $T, (A \vee B) \vdash C$, stačí dokázat

$$T, A \vdash (A \vee B) \quad \text{a} \quad T, B \vdash (A \vee B)$$

obě tvrzení plynou z monotonnosti disjunkce Větou o dedukci.

b) Platí-li $T, A \vdash C$ a $T, B \vdash C$ podle věty o dedukci a (v5) dostáváme

$$\begin{array}{ll} T, \neg C \vdash \neg \neg A, \neg B & \\ T, \neg C \vdash \neg \neg A \& \neg B & \text{konjunkce} \\ T, \neg C \vdash \neg \neg (A \vee B) & \text{de Morgan} \\ T \vdash \neg \neg C \rightarrow \neg \neg (A \vee B) & \text{VD} \\ T, (A \vee B) \vdash C & \text{(A3), VD} \end{array}$$

16

Distributivnost konjunkce a disjunkce

$$(i) \quad |-(A \vee (B \& C)) \leftrightarrow ((A \vee B) \& (A \vee C))$$

$$(ii) \quad |-(A \& (B \vee C)) \leftrightarrow ((A \& B) \vee (A \& C))$$

17

Důkaz.

(i) $\Rightarrow$ Použijeme důkaz rozbořem případů. Platí

$$A |-(A \vee B) \quad A |-(A \vee C) \quad (\text{monotonnost})$$

Tedy $A |-(A \vee B) \& (A \vee C)$ (konjunkce)

Podobně

$$B \& C |-(B \vee A) \quad B \& C |-(C \vee A) \quad (\text{konjunkce})$$

$$B \& C |-(A \vee B) \quad B \& C |-(A \vee C) \quad (\text{monotonnost})$$

$$B \& C |-(A \vee B) \& (A \vee C) \quad (\text{konjunkce})$$

celkem

$$|-(A \vee (B \& C)) \rightarrow ((A \vee B) \& (A \vee C))$$

18

$\Leftarrow$ Platí

$$(A \vee B) \& (A \vee C) |-(A \vee B), (A \vee C) \quad (\text{konjunkce})$$

Přitom $A \vee B$ je zkratka za implikaci $\neg A \rightarrow B$.

Tedy

$$\neg A, A \vee B |-(B) \quad \neg A, A \vee C |-(C)$$

$$(A \vee B) \& (A \vee C) |-\neg A \rightarrow (B \& C) \quad \text{VD konjunkce}$$

$$|-(A \vee (B \& C)) \rightarrow (A \vee (B \& C)) \quad \text{VD}$$

19

Normální tvary výrokových formulí

Syntax

- *Výrokové proměnné*
- *Literály* výrokové proměnné a jejich negace
- *Klauzule* disjunkce literálů
- *Formule v konjunktivním tvaru* (CNF) konjunkce klauzulí
- *Formule v disjunktivním tvaru* (DNF) disjunkce konjunkcí literálů

20

Příklady

Necht' $p_1, p_2, \dots, p_n, \dots$ jsou výrokové proměnné.

a) $(p_1 \vee \neg p_3 \vee p_6) \& p_1 \& (p_2 \vee p_7)$ je CNF

b) $(p_2 \& \neg p_3 \& \neg p_{10} \& \neg p_1) \vee (\neg p_2 \& \neg p_7)$ je DNF

21

Věta o normálních tvarech.

Ke každé formuli A lze sestrojit formule A_k, A_d v konjunktivním a disjunktivním tvaru, tak že

$$\models A \leftrightarrow A_k \quad a \quad \models A \leftrightarrow A_d$$

22

Důkaz.

a) Je-li A výroková proměnná, pak je v konjunktivním i disjunktivním tvaru.

b) Předpokládejme, že A je $\neg B$ a formule B_k a B_d již byly sestrojeny.

Z předpokladu $\models B \leftrightarrow B_d$

dostáváme $\models \neg B \leftrightarrow \neg B_d$

Předpokládejme, že B_d je tvaru $B_1 \vee B_2 \vee \dots \vee B_n$ kde

$B_i, i \leq n$ je tvaru $L_1^i \& L_2^i \& \dots \& L_{m_i}^i$.

23

z de Morganových pravidel

$$\models \neg B \leftrightarrow (\neg B_1 \& \neg B_2 \& \dots \& \neg B_n)$$

a pro každé $i \leq n$

$$\models \neg B_i \leftrightarrow (\neg L_1^i \vee \neg L_2^i \vee \dots \vee \neg L_{m_i}^i)$$

Označíme-li A_i formuli, která vznikne z pravé strany ekvivalence vynecháním dvojných negací u výrokových proměnných, pak A_i je disjunkce literálů a

$$\models A \leftrightarrow (A_1 \& A_2 \& \dots \& A_n)$$

kde na pravé straně ekvivalence je konjunktivní tvar formule A . Stejným způsobem se z $\neg B_k$ sestrojí disjunktivní tvar formule A .

24

c) předpokládejme, že A je tvaru $B \rightarrow C$ a že disjunktivní a konjunktivní normální tvary podformulí, B, C již byly sestrojeny. Podle zavedení disjunkce

$$\vdash (B \rightarrow C) \leftrightarrow (\neg B \vee C) \quad (1)$$

K sestrojení disjunktivního tvaru formule A stačí sestrojit disjunktivní tvar D formule $\neg B_k$ a formule $D \vee C_d$ je disjunktivním tvarem A .

Konjunktivní tvar formule A sestrojíme pomocí distributivity. Vyjdeme z (1) a z formule $\neg B_d$. K ní sestrojíme konjunktivní tvar $D_1 \& D_2 \& \dots \& D_n$ jako konjunkci klauzulí.

Také C_k je konjunkce klauzulí $E_1 \& E_2 \& \dots \& E_m$.

Tedy

$$\vdash A \leftrightarrow ((D_1 \& D_2 \& \dots \& D_n) \vee (E_1 \& E_2 \& \dots \& E_m))$$

Použijeme distributivnost a po roznásobení na pravé straně dostaneme konjunkci klauzulí tvaru

$$D_i \vee E_j, i, 1 \leq i \leq n, j, 1 \leq j \leq m.$$

Tím je konjunktivní tvar formule A sestrojen.

Predikátová logika

1

Jazyk prvního řádu

Jazyk obsahuje

- (i) **Proměnné** $x, y, z, x_1, x_2, \dots, y', y'', \dots$ neomezeně mnoho
- (ii) **Funkční symboly** $f, g, h, \dots, f_1, f_2, \dots$ každý má svou četnost (počet argumentů) $n \geq 0$.
- (iii) **Predikátové symboly** $p, q, r, \dots, p_1, p_2, \dots$ každý má svou četnost $n > 0$.
- (iv) **Symboly pro logické spojky** $\neg$ negace, $\vee$ disjunkce, $\&$ konjunkce, $\rightarrow$ implikace, $\leftrightarrow$ ekvivalence.
- (v) **Symboly pro kvantifikátory** $\forall$ univerzální $\exists$ existenční.

2

Termy a formule

jsou výrazy jazyka prvního řádu, které mají svůj význam.

Termy popisují (některá) individua.

Formule jsou tvrzeními o individuích.

Definujeme je induktivně.

3

Definice - Termy

(i) Každá proměnná je term.

(ii) Je-li f n -ární funkční symbol a výrazy $t_1, t_2, \dots, t_n$ jsou termy, potom výraz

$$f(t_1, t_2, \dots, t_n)$$

je term.

Termy jsou definovány konečným počtem užití pravidel

(i) a (ii). Tedy jsou to konečná slova.

4

Příklad.

V jazyce aritmetiky jsou následující výrazy termy

$$x \quad x+0 \quad y+S(x) \quad y+S(S(0)) \quad x*y \quad S(0)*S(S(0))$$

Podle definice bychom měli psát

$$x \quad +(x, 0) \quad +(y, S(x)) \quad +(y, S(S(0))) \\ *(x, y) \quad *(S(0), S(S(0)))$$

ale u binárních symbolů se přidržujeme zavedené praxe infixního zápisu.

5

Formule.

- (i) Je-li p n -ární predikátový symbol, potom výraz $p(t_1, t_2, \dots, t_n)$, kde $t_1, t_2, \dots, t_n$ jsou termy, je *(atomická) formule*.
- (ii) Jsou-li výrazy A, B formule, potom výrazy $\neg A, (A \& B), (A \vee B), (A \rightarrow B), a (A \leftrightarrow B)$ jsou také *formule*.
- (iii) Je-li x proměnná a A formule, potom výrazy $(\forall x)A$ a $(\exists x)A$ jsou *formule*.

6

Příklady.

$$x \bullet e = e \bullet x \quad x \bullet e = x \quad (\forall x)(\exists y)(x \bullet y = e) \quad e \bullet e = e$$

$$x \leq S(x) \quad x+x = S(S0)*x \quad x+y \leq x+S(y)$$

$$\underbrace{x \neq 0}_{\neg x=0} \rightarrow (\exists y)(x = S(y)) \quad k \mid x \leftrightarrow (\exists y)(k \bullet y = x)$$

$$(k \mid x \rightarrow (x \mid y \rightarrow (y \mid z \rightarrow k \mid z)))$$

7

Formule a podformule.

Formule

$$x \bullet e = e \bullet x \quad x \bullet e = x \quad e \bullet e = e$$

jsou atomické. Vznikly podle pravidla (i)

Formule

$$(\forall x)(\exists y)(x \bullet y = e) \quad (1)$$

vznikla z formulí

$$\begin{array}{ll} (x \bullet y = e) & (i) \\ (\exists y)(x \bullet y = e) & (iii) \\ (\forall x)(\exists y)(x \bullet y = e) & (iii) \end{array} \quad (2)$$

Říkáme, že formule (2) jsou podformule formule (1).

8

Podtermy, podformule, volné a vázané proměnné.

Nechť t je term a A je formule.

(i) Podslovo s termu t , které je samo termem nazveme *podtermem* termu t .

Podslovo B formule A , které je samo formulí nazveme *podformulí* formule A .

(ii) Daný výskyt proměnné x ve formuli A je vázaný, je-li součástí nějaké podformule tvaru $(\exists x)B$ nebo $(\forall x)B$.
Není-li daný výskyt proměnné x vázaný, říkáme, že je volný.

9

(iii) Říkáme, že proměnná x je volná ve formuli A , má-li tam volný výskyt. Proměnná x je *vázaná* v A , má-li tam vázaný výskyt.

(iv) Formule A je *otevřená*, pokud neobsahuje žádnou vázanou proměnnou. A je *uzavřená*, neobsahuje-li žádnou volnou proměnnou,

Je zřejmé, že otevřená formule neobsahuje žádný kvantifikátor zatím co uzavřená formule váže každou proměnnou nějakým kvantifikátorem .

10

Příklad.

Proměnná může být v téže formuli současně volná i vázaná.

$$(\forall x)((x \bullet e) = x) \rightarrow ((e \bullet x) = x)$$

$\wedge \quad \wedge \quad \wedge \quad \# \quad \#$

$$(x = z) \rightarrow (\exists x)(x = z)$$

11

Sémantika predikátové logiky

Interpretace jazyka je definována množinovou (relační) strukturou M která ke každému symbolu jazyka a k množině proměnných přiřadí množinu individuí.

Relační struktura M obsahuje

- neprázdnou množinu M pro individua.
- zobrazení $f_M : M^n \rightarrow M$ pro n -ární funkční symbol f
- relaci $R_M \subseteq M^n$ pro každý n -ární predikát p

12

Příklady.

a) $M = (M = \{a, b, c\}, \rightarrow_M = \{<a, b>\})$

je interpretací jazyka $L = \{\rightarrow\}$, je to (orientovaný) graf se třemi vrcholy a jednou hranou.

b) $E = (\{e\}, e, \bullet_E)$, kde $\bullet_E : \{e\}^2 \rightarrow \{e\}$ je interpretací jazyka $L = \{e, \bullet\}$ teorie grup. Je to jednoprvková grupa.

c) $N = (N, \theta_N, S_N, \oplus, \otimes)$, kde θ_N je interpretace konstanty 0, S_N interpretuje funkci následníka a $\oplus, \otimes$ interpretují operace součtu a součinu, je interpretací jazyka aritmetiky.

13

Interpretace termů.

Mějme jazyk L a strukturu M , která ho interpretuje. Chceme každému termu přiřadit jeho hodnotu v doméně M struktury M .

a) Proměnné, v termech musíme ohodnotit nejdříve.

Použijeme zobrazení e , které každé proměnné x přiřadí hodnotu $e(x)$ z domény M . Takovému zobrazení říkáme **ohodnocení proměnných**.

b) *Interpretaci termu* t při ohodnocení e označíme $t[e]$.

Definujeme $t[e] = e(x)$ je-li t proměnná x
 $t[e] = f_M(t_1[e], \dots, t_n[e])$, je-li t tvaru $f(t_1 \dots t_n)$.

14

Je zřejmé, že ohodnocení proměnných není absolutní pojem, ale že závisí na struktuře M . Měli bychom proto psát $t[e, M]$. Je-li struktura M dána, píšeme krátce $t[e]$.

Interpretace termu při ohodnocení e závisí jenom na konečně hodnotách e .

Lemma.

Jsou-li všechny proměnné termu t mezi proměnnými

$$x_1, x_2, \dots, x_n$$

a e, e' dvě ohodnocení taková, že $e(x_i) = e'(x_i)$ pro $i, 1 \leq i \leq n$, potom $t[e] = t[e']$.

Důkaz indukci podle složitosti termu t .

15

Tarského definice pravdy

Nechť L je jazyk, M jeho interpretace, e pravdivostní ohodnocení a A je formule jazyka L .

(i) Říkáme, že A je *splněna v M při ohodnocení e* a píšeme

$$M \models A[e]$$

jestliže (indukcí podle složitosti A)

a) A je atomická $A \equiv p(t_1, \dots, t_n)$, kde p není rovnost. Potom

$$M \models A[e], \text{ jestliže } (t_1[e], \dots, t_n[e]) \in p_M$$

16

b) A je atomická, $A \equiv t_1 = t_2$ a $t_1[e] = t_2[e]$.

c) A je tvaru $\neg B$ a $M \models B[e]$.

d) A je tvaru $B \rightarrow C$ a $M \models B[e]$ nebo $M \models C[e]$.

Je-li e ohodnocení proměnných, x je proměnná a m je prvek z domény M , pozmeněné ohodnocení $e(x/m)$ definujeme

$$e(x/m)(y) = \begin{cases} m & \text{je-li } y \equiv x \\ e(y) & \text{je-li } y \not\equiv x \end{cases}$$

17

e) A je tvaru $(\forall x)B$ a $M \models B[e(x/m)]$ pro každé $m \in M$.

f) A je tvaru $(\exists x)B$ a $M \models B[e(x/m)]$ pro nějaké $m \in M$.

(ii) Říkáme, že *formule A je pravdivá v M* a píšeme

$$M \models A$$

je-li A splněna v M při každém ohodnocení proměnných.

18

- Podobně jako u termů, splnění formule při nějakém ohodnocení e závisí jen na ohodnocení $e(x)$ konečně mnoha proměnných.
- z e) a f) vyplývá, že pokud má proměnná jen vázané výskyty, potom splnění formule nezávisí na ohodnocení této formule.
- Je-li formule uzavřená, potom její splnění je pro všechna ohodnocení stejné. Stačí ověřit zda je splněna, či nesplněna při jednom ohodnocení.
- Jinými slovy, je-li uzavřená formule splněna při alespoň jednom ohodnocení, je pravdivá.

19

Říkáme, že formule je *validní (platná)* nebo *logicky pravdivá* a píšeme $\models A$, jestliže je pravdivá při každé interpretaci daného jazyka.

Tedy

$$\models A \text{ právě když } M \models A \text{ pro každou interpretaci } M$$

20

Substituce termů do termů za proměnné

Příklady.

$$t \equiv (x + y) \quad s \equiv (x + x) \quad r \equiv (z * y) \quad q \equiv w$$

$$t_x[s] \equiv ((x + x) + y) \quad t_y[r] \equiv (x + (z * y))$$

$$t_{xy}[s, r] \equiv ((x + x) + (z * y))$$

$$r_z[s] \equiv ((x + x) * y) \quad r_y[q] \equiv (z * w)$$

$$r_{zy}[t_x[s], s_x[q]] \equiv (((x + x) + y) * (w + w))$$

21

Jsou-li $x_1, \dots, x_n$ různé proměnné a $t, t_1, \dots, t_n$ jsou termy, potom symbolicky

$$t_{x_1, \dots, x_n}[t_1, \dots, t_n]$$

označíme výraz, který vznikne z t současným nahrazením každého výskytu proměnné x_i termem t_i pro $i, i \leq n$.

Indukcí podle složitosti termu t se snadno ověří, tímto způsobem vznikne term.

22

Substituce termů do formulí

$$A \equiv \sin^2(\alpha) + \cos^2(\alpha) = 1 \quad B \equiv (\exists z)(x^2 + y^2 = z)$$

$$t \equiv (\pi / 3) \quad s \equiv \sqrt{2} \quad q \equiv a^2 \quad u \equiv \sqrt{x^2 + 1}$$

$$A_\alpha[t] \equiv \sin^2(\pi / 3) + \cos^2(\pi / 3) = 1$$

$$B_x[q] \equiv (\exists z)((a^2)^2 + y^2 = z)$$

$$B_{xy}[s, u] \equiv (\exists z)((\sqrt{2}^2 + \sqrt{x^2 + 1}^2) = z)$$

23

Jsou-li $x_1, \dots, x_n$ různé proměnné A formule a $t_1, \dots, t_n$ jsou termy, potom symbolicky

$$A_{x_1, \dots, x_n}[t_1, \dots, t_n] \quad (1)$$

označíme výraz, který vznikne z A nahrazením každého volného výskytu proměnné x_i termem t_i pro $i, i \leq n$.

Indukcí podle složitosti formule A se snadno ověří, tímto způsobem vznikne formule. Této formulí říkáme *instance formule A*.

24

Substituovatelnost termu do formule

Intuice: formule vypovídá o substituovaných termech „totéž“, co vypovídá o proměnných, za které bylo substituováno.

Varovný příklad.

Mějme formuli

$$A \equiv (\exists y)(x = (y + y)) \quad (1)$$

a term $t \equiv (y + 1)$. Potom instance $A_x[t]$ formule (1)

$$A_x[t] \equiv (\exists y)(y + 1 = y + y)$$

vypovídá něco jiného o termu $(y + 1)$ než vypovídala formule (1) o x .

25

Co se stalo?

Volná proměnná x , za kterou bylo substituováno, byla v podformuli kvantifikátoru, který svázal proměnnou y v termu t .

Říkáme, že term t je substituovatelný do formule A za proměnnou x , jestliže pro každou proměnnou y vyskytující se v t žádná podformule $(\forall y)B, (\exists y)B$ formule A neobsahuje (z hlediska formule A) volný výskyt proměnné x .

Ve dvou případech je snadné substituovatelnost rozpoznat

- je-li formule A otevřená
- žádná proměnná substituovaných termů není vázaná v A .

26

Příklady.

$$A \equiv (x \neq 0) \rightarrow (\forall x)(\forall y)(\exists z)((u + z) > (x + y))$$

$$B \equiv ((\forall x)(\exists y)((y + u) > (x + u)) \rightarrow \neg(\exists y)(\forall x)(y \geq (x + u)))$$

a) substituovatelné

$$t \equiv (u / v + w) \quad s \equiv (v^2 + z^2) \quad r \equiv (v + x)$$

$$A_u[t] \equiv (x \neq 0) \rightarrow (\forall x)(\forall y)(\exists z)((u / v + w) + z) > (x + y))$$

$$A_x[r] \equiv ((v + x) \neq 0) \rightarrow (\forall x)(\forall y)(\exists z)((u + z) > (x + y))$$

Spočítejte

$$A_u[s] \quad B_u[t] \quad B_u[s]$$

27

$$A \equiv (x \neq 0) \rightarrow (\forall x)(\forall y)(\exists z)((u + z) > (x + y))$$

$$B \equiv ((\forall x)(\exists y)((y + u) > (x + u)) \rightarrow \neg(\exists y)(\forall x)(y \geq (x + u)))$$

b) nesubstituovatelné

$$d \equiv x * y \quad e \equiv u + y^2 \quad f \equiv (z + v + w)$$

$$A_u[d] \quad A_u[e]$$

$$B_u[d] \quad B_u[e] \quad B_u[f]$$

Přitom

$$A_x[d] \quad A_x[e] \quad A_x[f] \quad A_u[f]$$

jsou substituovatelné.

28

Úmluva.

Výraz $A_{x,y,z,\dots}[t,s,r\dots]$ budeme používat jen když jsou termy $t,s,r\dots$ substituovatelné za proměnné $x,y,z,\dots$ do formule A .

29

Lemma.

L je jazyk, M jeho interpretace, $x_1, \dots, x_n$ proměnné, $t, t_1, \dots, t_n$ termy a e je ohodnocení proměnných takové, že $t_i[e] = m_i$ pro nějaké individuum $z M$. Potom

$$(i) \quad t_{x_1, x_2, \dots, x_n}[t_1, t_2, \dots, t_n][e] = t[(e/m_1), \dots, (e/m_n)]$$

$$(ii) \quad M \models A_{x_1, \dots, x_n}[t_1, \dots, t_n][e] \text{ právě když}$$

$$M \models A[(e/m_1), \dots, (e/m_n)]$$

30

Formální systém predikátové logiky

Dokazatelnost

31

Redukce jazyka.

- Z logických spojek pracujeme jen s negací a implikací. Ostatní spojky jsou z nich odvozené.
- Univerzální kvantifikátor je základní.
- Existenční kvantifikátor je z něj odvozen vztahem

$$(\exists x)A \text{ je zkratka za formuli } \neg(\forall x)\neg A.$$

32

Axiomy pro logické spojky

Je-li L jazyk 1. řádu a A, B, C jsou formule jazyka L , potom každá formule tvaru

$$A \rightarrow (B \rightarrow A) \quad (A1)$$

$$(A \rightarrow (B \rightarrow C)) \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow C)] \quad (A2)$$

$$(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B) \quad (A3)$$

je axiom.

33

Axiomy predikátové logiky pro spojky jsou „instancemi“ schemat (A1), (A2) a (A3), které vzniknou z axiomů výrokové logiky dosazením libovolných formulí predikátové logiky za výrokové proměnné.

Vezmeme-li v úvahu, že pravidlo modus ponens je také odvozovací pravidlo predikátové logiky, dostáváme

Je-li A větou výrokové logiky a A' vznikne z A dosazením libovolných formulí predikátové logiky za výrokové proměnné formule A , potom A' je větou predikátové logiky.

34

Axiomy pro kvantifikátory.

Schema specifikace. Je-li A formule, x proměnná a t je term, potom formule

$$(\forall x)A \rightarrow A_x[t]$$

je *axiom specifikace* predikátové logiky.

Schema „přeskoku“. Jsou-li A, B formule a je-li x proměnná, která nemá volný výskyt ve formuli A , potom formule

$$(\forall x)(A \rightarrow B) \rightarrow (A \rightarrow (\forall x)B)$$

je axiom predikátové logiky.

35

Odvozovací pravidla.

Modus ponens

$$\frac{A \quad A \rightarrow B}{B}$$

Pravidlo generalizace

$$\frac{A}{(\forall x)A}$$

pro libovolnou proměnnou x .

36

Uvedené axiomy a odvozovací pravidla tvoří
formální systém predikátové logiky bez rovnosti.

Pojem důkazu, důkazu z předpokladů a vět je stejný
jako ve výrokové logice.

Formální systém predikátové logiky s rovností vznikne
z tohoto systému rozšířením jazyka o predikátový
symbol rovnosti '=' a tři schema axiomů rovnosti.

37

Základní věty o kvantifikátorech.

Pravidlo zavedení $\forall$.

Nemá-li proměnná x volný výskyt ve formuli A a

$$|- A \rightarrow B \quad \text{potom} \quad |- A \rightarrow (\forall x)B$$

Pravidlo substituce, Pravidlo zavedení $\exists$.

$$(i) \quad |- A_x[t] \rightarrow (\exists x)A$$

$$(ii) \text{ Je-li } |- A \rightarrow B \text{ a } x \text{ není volná v } B, \text{ potom}$$

$$\text{také} \quad |- (\exists x)A \rightarrow B.$$

38

V Gentzenově stylu můžeme tato pravidla zapsat

$$\frac{A \rightarrow B \quad x \text{ není volná v } A}{A \rightarrow (\forall x)B} \quad \text{Pravidlo zavedení } \forall.$$

$$\frac{}{A_x[t] \rightarrow (\exists x)A} \quad \text{Pravidlo substituce}$$

$$\frac{A \rightarrow B \quad x \text{ není volná v } B}{(\exists x)A \rightarrow B} \quad \text{Pravidlo zavedení } \exists.$$

39

Důkazy.

Pravidlo zavedení $\forall$.

$ - A \rightarrow B$	předpoklad
$ - (\forall x)(A \rightarrow B)$	generalizace
$ - (\forall x)(A \rightarrow B) \rightarrow (A \rightarrow (\forall x)B)$	schema přeskočů
$ - (A \rightarrow (\forall x)B)$	MP

40

Pravidlo substitute.

$$|- (\forall x)\neg A \rightarrow \neg A_x[t]$$

schema specifikace

$$|- \underbrace{\neg(\forall x)\neg A}_{(\exists x)A} \rightarrow \neg A_x[t]$$

(v3), zkratka $\exists$

$$|- A_x[t] \rightarrow (\exists x)A$$

(A3), MP

Pravidlo zavedení $\exists$.

$$|- A \rightarrow B$$

předpoklad

$$|- \neg B \rightarrow \neg A$$

(v5), MP

$$|- \neg B \rightarrow \underbrace{\neg(\forall x)\neg A}_{(\exists x)A}$$

pravidlo $\forall$, (v4)

$$|- (\exists x)A \rightarrow B$$

(A3)

41

Instance formulí.

$$A_{x_1}, \dots, x_n [t_1, \dots, t_n]$$

je instance formule A . $x_1, \dots, x_n$ jsou navzájem různé proměnné, $t_1, \dots, t_n$ jsou (substituovatelné) termy.

Instance vyjadřuje nějaký zvláštní případ tvrzení formule. Do formule dosazujeme všechny termy současně (paralelně).

$$(\exists y)(x < y)$$

$$(\exists y)(l < y)$$

42

Varovný příklad.

$$A \equiv x < y \quad t \equiv x \quad s \equiv y$$

$$A_{xy}[s, t] \equiv y < x$$

$$A_x[s] \equiv y < y \quad ((A_x[s])_y[t]) \equiv x < x$$

$$A_y[t] \equiv x < x \quad ((A_y[t])_x[s]) \equiv y < y$$

43

Věta o instancích.

Je-li A' instance A , potom platí

$$|- A \text{ implikuje } |- A'$$

Je-li dokazatelná formule A , potom je dokazatelná každá její instance.

44

Důkaz.

Indukcí podle počtu substituovaných termů.

Necht' $A' \equiv A_{x_1}, \dots, x_n[t_1, \dots, t_n]$

Je-li $n = 1$ a $A' \equiv A_x[t]$ potom

$ - A$	předpoklad
$ - (\forall x)A$	generalizace
$ - (\forall x)A \rightarrow A_x[t]$	axiom specifikace
$ - A_x[t]$	MP

45

Je-li $n > 1$, necht' $z_1, \dots, z_n$ jsou nové proměnné, které se nevyskytují ani ve formuli A ani v termech $t_1, \dots, t_n$. Potom

$ - A$	předpoklad
$ - A_{x_1}[z_1]$	základ indukce
$ - (A_{x_1}[z_1])_{x_2}[z_2] \equiv A_{x_1 x_2}[z_1, z_2]$	iterace
$\vdots$	
$ - \underbrace{A_{x_1}, \dots, x_n[t_1, \dots, t_n]}_B$	celkem

46

Nyní

$ - B$	mezivýsledek
$ - B_{z_1}[t_1]$	základ indukce
$ - (B_{z_1}[t_1])_{z_2}[t_2] \equiv B_{z_1 z_2}[t_1, t_2]$	iterace
$\vdots$	
$ - \underbrace{B_{x_1}, \dots, z_n[t_1, \dots, t_n]}_{A[t_1, \dots, t_n]}$	celkem

Tedy $| - A' \equiv A_{x_1}, \dots, x_n[t_1, \dots, t_n]$

47

Co nás překvapilo?

Je-li $A \equiv x = 0 \quad t \equiv 3$

potom $A' \equiv A_x[t] \equiv 3 = 0$

Kdyby $| - A$

potom $| - A' \equiv 3 = 0$

Jak ukážeme později formule $A \equiv x = 0$ není dokazatelná.

48

Specifikace a substitute.

Je-li A formule, $x_1, \dots, x_n$ proměnné a $t_1, \dots, t_n$ termy, potom platí

$$(i) \quad (\forall x_1), \dots, (\forall x_n) A \rightarrow A_{x_1, \dots, x_n}[t_1, \dots, t_n]$$

$$(ii) \quad A_{x_1, \dots, x_n}[t_1, \dots, t_n] \rightarrow (\exists x_1), \dots, (\exists x_n) A$$

49

Důkaz. (i) Z axiomu specifikace pro libovolnou formuli C dostáváme

$$|- (\forall x) C \rightarrow C \quad (\equiv C_x[x])$$

iterací

$$|- (\forall x_n) A \rightarrow A$$

$$|- (\forall x_{n-1})(\forall x_n) A \rightarrow (\forall x_n) A$$

$\vdots$

$$|- (\forall x_1), \dots, (\forall x_n) A \rightarrow (\forall x_2), \dots, (\forall x_n) A$$

Složením všech implikací dostaneme

$$|- (\forall x_1), \dots, (\forall x_n) A \rightarrow A$$

Tvrzení (i) je instancí této formule. (ii) se dokáže obdobně iterací Substitučního lemmatu.

50

Uzávěr formule

Jsou-li $x_1, \dots, x_n$ všechny proměnné s volným výskytem ve formuli A v nějakém pořadí, potom formuli

$$(\forall x_1) \dots (\forall x_n) A$$

nazveme *uzávěrem formule A* .

Podle této definice má formule více uzávěrů, podle toho jaké zvolíme pořadí proměnných. Pomocí lemmatu o specifikaci a pravidla zavedení univerzálního kvantifikátoru se dokáže, že *všechny uzávěry jsou ekvivalentní*.

51

Cvičení.

a) Jestliže formule A neobsahuje volně proměnnou x , potom platí

$$|- A \leftrightarrow (\forall x) A$$

$$|- A \leftrightarrow (\exists x) A$$

b)

$$|- (\forall x)(\forall y) A \leftrightarrow (\forall y)(\forall x) A$$

$$|- (\exists x)(\exists y) A \leftrightarrow (\exists y)(\exists x) A$$

c) Je-li π permutace čísel $\{1, \dots, n\}$, potom

$$|- (\forall x_1)(\forall x_2) \dots (\forall x_n) A \leftrightarrow (\forall x_{\pi(1)})(\forall x_{\pi(2)}) \dots (\forall x_{\pi(n)}) A$$

$$|- (\exists x_1)(\exists x_2) \dots (\exists x_n) A \leftrightarrow (\exists x_{\pi(1)})(\exists x_{\pi(2)}) \dots (\exists x_{\pi(n)}) A$$

52

Věta o uzávěru.

Je-li A' uzávěr formule A , potom platí

$$\vdash A \text{ právě když } \vdash A'$$

Důkaz.

- a) Je-li dokazatelné A , potom pravidlem generalizace odvodíme A' .
- b) Je-li dokazatelné A' , použijeme lemma o specifikaci a substituci a A odvodíme pravidlem modus ponens.

53

Lemma o distribuci kvantifikátorů

Je-li $\vdash A \rightarrow B$, potom

$$\vdash (\forall x)A \rightarrow (\forall x)B \quad \text{a} \quad \vdash (\exists x)A \rightarrow (\exists x)B$$

Důkaz.

$\vdash A \rightarrow B$	předpoklad
$\vdash (\forall x)A \rightarrow A$	axiom specifikace
$\vdash (\forall x)A \rightarrow B$	složení implikací
$\vdash (\forall x)A \rightarrow (\forall x)B$	zavedení $\forall$

Druhé tvrzení se dokazuje obdobně pomocí substitučního lemmatu a pravidla $\exists$.

54

Věta o ekvivalenci.

Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $B_1, \dots, B_n$ po řadě formulemi $B'_1, \dots, B'_n$. Je-li

$$\vdash B_1 \leftrightarrow B'_1 \dots \vdash B_n \leftrightarrow B'_n$$

potom

$$\vdash A \leftrightarrow A'$$

55

Důkaz.

Postupujeme indukcí podle složitosti formule A stejně jako u obdobné věty výrokového počtu. Navíc je jen případ, kdy A je tvaru

$$(\forall x)B \text{ nebo } (\exists x)B.$$

Potom A' je tvaru

$$(\forall x)B' \text{ nebo } (\exists x)B'.$$

$\vdash B \leftrightarrow B'$	indukční předpoklad
$\vdash B \rightarrow B' \text{ a } \vdash B' \rightarrow B$	zkratka ekvivalence
$\vdash A \rightarrow A' \text{ a } \vdash A' \rightarrow A$	distribuce kvantifikátorů

Tedy $\vdash A \leftrightarrow A'$.

56

Záměna vázaných proměnných

Vázané proměnné se používají v běžné matematické praxi.

$$\sum_{n=0}^{\infty} 1/n^2 = \sum_{k=0}^{\infty} 1/k^2$$

$$\int_0^{\pi} \sin(\alpha) d\alpha = \int_0^{\pi} \sin(\beta) d\beta$$

Na obou stranách rovnosti je stejné číslo.

57

Říkáme, že *formule A' je variantou formule A* , jestliže A' vznikne z A postupným nahrazením podformulí $(Qx)B$ formulí $(Qy)B_x[y]$, kde y není volná ve formuli B a Q je univerzální nebo existenční kvantifikátor.

Příklad.

$$A \equiv (\forall x)(\exists y) \underbrace{(\forall z)(x < y < z)}_C \quad C \mapsto (\forall w)(x < y < w)$$

$$A_1 \equiv (\forall x) \underbrace{(\exists y)(\forall w)(x < y < w)}_{C_1} \quad C_1 \mapsto (\exists v)(\forall w)(x < v < w)$$

$$A_2 \equiv (\forall x) \underbrace{(\exists v)(\forall w)(x < v < w)}_{C_2} \quad C_2 \mapsto A'$$

$$A' \equiv (\forall u)(\forall v)(\forall w)(u < v < w)$$

58

Věta o variantách

Je-li A' variantou formule A , potom

$$\vdash A \leftrightarrow A'$$

59

Důkaz.

Podle Věty o ekvivalenci stačí dokázat

$$\vdash \neg (Qx)B \leftrightarrow (Qy)B_x[y]$$

za předpokladů uvedených v definici varianty. Důkaz provedeme pro $Q \equiv \forall$.

$$\text{a) } \vdash \neg (\forall x)B \rightarrow B_x[y] \quad \text{axiom specifikace}$$

$$\vdash \neg (\forall x)B \rightarrow (\forall y)B_x[y] \quad \text{pravidlo } \forall$$

60

b) Označme formuli $B_x[y]$ symbolem C . Potom

$|-(\forall y)C \rightarrow C_y[x]$ axiom specifikace

$|-(\forall y)C \rightarrow (\forall x)C_y[x]$ pravidlo $\forall$

protože proměnná x není volná v C a je substituovatelná do C za y . Ale $C_y[x]$ je formule B . tím je dokázána i opačná implikace.

61

Věta o dedukci

Necht' T je množina formulí, A je uzavřená formule a B je libovolná formule. Potom

$$T \mid - A \rightarrow B \quad \text{právě když} \quad T, A \mid - B$$

62

Důkaz.

Implikace zleva do prava se dokazuje zcela stejně jako ve výrokové logice.

Při důkazu zprava do leva, mějme důkaz $B_1, \dots, B_n$ formule B z předpokladů T, A . Indukcí podle délky důkazu dokážeme $T \mid - B_j$ pro všechna j .

Ve výrokové logice jsme rozebrali všechny případy až na ten, kdy je formule B_i odvozena z formule $B_j, j < i$ pravidlem generalizace.

63

To znamená, že B_i je tvaru $(\forall x)B_j$. Z indukčního předpokladu

$$T \mid - A \rightarrow B_j$$

odvodíme

$$T \mid - A \rightarrow \underbrace{(\forall x)B_j}_{B_i}$$

pravidlem zavedení univerzálního kvantifikátoru, protože proměnná x není volná ve formuli A .

Tím je důkaz dokončen.

64

Ve větě o dedukci je předpoklad uzavřenosti formule A příliš omezující.

Stačilo by, kdybychom věděli, že v důkazu formule B z T, A nebylo použito pravidlo generalizace na žádnou proměnnou, která je volná v A .

Jinými slovy, kdybychom věděli, že žádná volná proměnná z A nebyla v důkazu využita.

To by znamenalo, že se taková proměnná chovala v průběhu důkazu jako konstanta.

Dokážeme větu, že proměnné lze za určitých předpokladů nahradit konstantami a později se k těmto proměnným vrátit.

65

Věta o konstantách

Nechť T je množina formulí jazyka L a A je formule jazyka L . Necht' $x_1, \dots, x_n$ jsou proměnné.

Nechť jazyk L' vznikne rozšířením L o nové symboly $c_1, \dots, c_n$ pro konstanty. Potom platí

$$T \mid -_{L'} A_{x_1}, \dots, x_n [c_1, \dots, c_n] \text{ právě když } T \mid -_L A$$

(Přidali jsme nové symboly pro konstanty ale nepřidali jsme o nich žádné axiomy.)

66

Důkaz.

Označme A' formuli $A_{x_1}, \dots, x_n [c_1, \dots, c_n]$.

a) je-li $T \mid -_L A$ potom $T \mid -_{L'} A'$, protože A' je instancí A .

b) je-li $T \mid -_{L'} A'$, necht' $A'_1, \dots, A'_n$ je důkaz A' z T .

Necht' $y_1, \dots, y_n$ jsou nové proměnné, které se nevyskytují v důkazu A' ani v A .

Důkaz $A'_1, \dots, A'_n$ formule A' přeměníme na důkaz $A_1, \dots, A_n$ formule $A_{x_1}, \dots, x_n [y_1, \dots, y_n]$. Formule $A_{x_1}, \dots, x_n [c_1, \dots, c_n]$ bude její instancí.

67

Necht' pro každé i , formule A_i vznikne z formule A'_i nahrazením každého výskytu konstanty c_j proměnnou y_j .

Snadno se přesvědčíme, že $A_1, \dots, A_n$ je důkazem formule $A_{x_1}, \dots, x_n [y_1, \dots, y_n]$ z T . Je-li A'_i axiom predikátové logiky, potom A_i je také axiom predikátové logiky stejného druhu.

Je-li A'_i prvek T , potom A_i je A'_i , protože tato formule neobsahuje nové konstanty.

Je-li A'_i odvozena pravidlem modus ponens nebo generalizace, pak A_i je odvozena stejným pravidlem.

68

Odtud

$$T \mid -_L A_{x_1}, \dots, x_n [y_1, \dots y_n]$$

a formule A je její instancí. Tím je důkaz věty dokončen.

Konstanty a Věta o dedukci.

Chceme-li dokázat implikaci $A \rightarrow B$ z T a A má volné proměnné $x_1, \dots x_n$, rozšíříme jazyk o nové konstanty $c_1, \dots c_n$.

Stačí dokázat

$$T, A_{x_1}, \dots, x_n [c_1, \dots c_n] \mid - B_{x_1}, \dots, x_n [c_1, \dots c_n]$$

a z Věty o dedukci a Věty o konstantách dostaneme

$$T \mid - A \rightarrow B.$$

69

Důsledek.

Je-li A' uzávěr formule A a T je množina formulí, potom

$$T \mid - A, \text{ právě když } T \cup \{\neg A'\} \text{ je sporná}$$

70

Důkaz.

a) je-li $T \mid - A$, z věty o uzávěru dostáváme $T \mid - A'$.

Proto je $T \cup \{\neg A'\}$ sporná.

b) Je-li $T \cup \{\neg A'\}$ je sporná, potom z ní lze dokázat libovolnou formuli, tedy i formuli A' . Podle Věty o dedukci dostáváme $T \mid - \neg A' \rightarrow A'$ a podle věty (v7) výrokové logiky $T \mid - A'$.

71

Cvičení.

a) Jestliže formule A neobsahuje proměnnou x volně, potom

$$\mid - A \leftrightarrow (\forall x)A$$

$$\mid - A \leftrightarrow (\exists x)A$$

$$\mid - (\forall x)A \leftrightarrow (\exists x)A$$

b)

$$\mid - (Qx)(Qy)A \leftrightarrow (Qy)(Qx)A$$

c)

$$\mid - (\exists x)(\forall y)A \rightarrow (\forall y)(\exists x)A$$

72

d)

$$\vdash (\forall x)A \rightarrow (\forall x)(A \rightarrow B)$$

$$\vdash (\exists x)\neg A \vee (\forall x)(\neg A \vee B)$$

$$\vdash (\exists x)\neg A \vee \neg(\exists x)(A \wedge \neg B)$$

e)

$$\vdash (\forall x)(A \& B) \leftrightarrow ((\forall x)(A) \& (\forall x)(B))$$

$$\vdash ((\forall x)(A) \vee (\forall x)(B)) \rightarrow (\forall x)(A \vee B)$$

$$\vdash (\exists x)(A \vee B) \leftrightarrow ((\exists x)(A) \vee (\exists x)(B))$$

$$\vdash (\exists x)(A \& B) \rightarrow ((\exists x)(A) \& (\exists x)(B))$$

f)

$$\vdash (Q_1 x_1) \dots (Q_{i-1} x_{i-1}) (Q_i x_i) (Q_{i+1} x_{i+1}) \dots (Q_j x_j) \dots (Q_n x_n) \leftrightarrow \\ (Q_1 x_1) \dots (Q_{i-1} x_{i-1}) (Q_{i+1} x_{i+1}) \dots (Q_j x_j) \dots (Q_n x_n)$$

Prenexní tvary formulí. Rovnost.

1

Ve výrokové logice jsme pomocí logických spojek sestrojili konjunktivní a disjunktivní normální tvary formulí.

V predikátové logice sestrojíme prenexní normální tvary, které jsou v jistém smyslu jejich nadstavbou.

Budeme požadovat, aby při sestrojení formule, byly kvantifikátory použity až na konec.

To znamená, že za řetězcem kvantifikátorů bude následovat podformule sestrojená jen z výrokových spojek. Chceme-li, ta může být v konjunktivním nebo disjunktivním tvaru.

2

Prenexní tvar formule.

Formule A je v prenexním tvaru, jeli

$$A \equiv (Q_1 x_1)(Q_2 x_2) \dots (Q_n x_n) B$$

kde

(i) $n \geq 0$ a pro každé $i, 1 \leq i \leq n$ je Q_i $\forall$ nebo $\exists$.

(ii) B je otevřená formule a kvantifikované proměnné jsou navzájem různé.

Formule B se nazývá *otevřené jádro* A a posloupnost kvantifikací před B se nazývá *prefix*.

3

Příklady.

a) $(\forall x)(\forall y)(\exists z)(z = (x + y) / 2)$

b) $(\forall x)((x \mid p \rightarrow x = 1) \rightarrow p \text{ je prvočíslo})$

c) $(\exists F)(\forall x)(\forall y)((x \cup y) \in F \leftrightarrow (x \in F \vee y \in F))$

d) $(\forall F)(\forall G)(\forall C)(\forall D)(\forall E)[(F : C \rightarrow D) \rightarrow ((G : D \rightarrow E) \rightarrow \rightarrow (F \circ G : C \rightarrow E))]$

4

Věta o prenexních tvarech

Ke každé formuli A lze sestavit formuli A' , v prenexním tvaru, která je s ní ekvivalentní.

5

Značení.

Je-li Q kvantifikátor, potom značíme

$$\overline{Q} = \begin{cases} \forall & \text{je-li } Q \equiv \exists \\ \exists & \text{je-li } Q \equiv \forall \end{cases}$$

Konstrukce ekvivalentní formule v prenexním tvaru postupuje indukcí podle složitosti dané formule pomocí *prenexních operací*.

Jejich úkolem je vyvést kvantifikátory zevnitř podformulí ven. Až tento proces skončí, máme hledanou prenexní formuli.

6

Lemma. Prenexní operace.

a) v případě potřeby nahradíme nějakou podformuli její variantou (ta je s ní ekvivalentní).

Pro libovolné formule B, C , kvantifikátor Q a proměnnou x platí

$$b) \quad | - \neg(Qx)B \leftrightarrow (\overline{Q}x)\neg B$$

$$c) \quad | - (B \rightarrow (Qx)C) \leftrightarrow (Qx)(B \rightarrow C), \text{ pokud } x \text{ není volná v } B.$$

$$d) \quad | - ((Qx)B \rightarrow C) \leftrightarrow (\overline{Q}x)(B \rightarrow C), \text{ pokud } x \text{ není volná v } C.$$

$$e) \quad | - ((Qx)B \diamond C) \leftrightarrow (Qx)(B \diamond C), \text{ pokud } x \text{ není volná v } C.$$

Symbol $\diamond$ zastupuje konjunkci nebo disjunkci.

7

Důkaz.

b) Je-li $Q \equiv \forall$ dostáváme

$$| - \neg(\forall x)B \leftrightarrow \neg(\underbrace{(\forall x)\neg\neg}_{(\exists x)})B$$

protože B a $\neg\neg B$ jsou ekvivalentní

c) Je-li $Q \equiv \forall$ a proměnná x není volná v B , implikace

$$| - (\forall x)(B \rightarrow C) \rightarrow (B \rightarrow (\forall x)C)$$

je axiom. Abychom dokázali obrácenou implikaci užijeme

$$| - (B \rightarrow (\forall x)C) \rightarrow \underbrace{[(\forall x)C \rightarrow C]}_{\text{axiom specifikace}} \rightarrow (B \rightarrow C)$$

8

c) Je-li $Q \equiv \forall$ a proměnná x není volná v B , implikace

$$\vdash \neg (\forall x)(B \rightarrow C) \rightarrow (B \rightarrow (\forall x)C)$$

je axiom. Abychom dokázali obrácenou implikaci užijeme

$$\vdash \neg (B \rightarrow (\forall x)C) \rightarrow [\underbrace{((\forall x)C \rightarrow C)}_{\text{axiom specifikace}} \rightarrow (B \rightarrow C)]$$

$$\vdash \neg (B \rightarrow (\forall x)C) \rightarrow (B \rightarrow C) \quad \text{MP}$$

Na konec pravidlem zavedení $\forall$ dostaneme druhou implikaci protože B neobsahuje x volně.

9

Abychom dokázali tvrzení pro $Q \equiv \exists$ uvědomme si, že ze zavedení disjunkce plyne

$$\vdash \neg (B \rightarrow (\exists x)C) \leftrightarrow (\neg B \vee (\exists x)C) \quad (1)$$

Máme tedy dokázat

$$\vdash \neg (\neg B \vee (\exists x)C) \rightarrow (\exists x)(B \rightarrow C) \quad (2)$$

Podle věty o důkazu rozbořem případů máme dokázat

$$\vdash \neg (\exists x)C \rightarrow (\exists x)(B \rightarrow C) \quad (3)$$

a

$$\vdash \neg \neg B \rightarrow (\exists x)(B \rightarrow C) \quad (4)$$

10

Důkaz (3).

$$\vdash \neg C \rightarrow (B \rightarrow C) \quad \text{axiom (A1)}$$

$$\vdash \neg (\exists x)C \rightarrow (\exists x)(B \rightarrow C) \quad \text{distribuce kvantifikátorů}$$

Důkaz (4).

$$\vdash \neg (B \rightarrow C) \rightarrow (\exists x)(B \rightarrow C) \quad \text{substituční lemma}$$

$$\vdash \neg \neg B \rightarrow (B \rightarrow C) \quad (\vee 2)$$

$$\vdash \neg \neg B \rightarrow (\exists x)(B \rightarrow C) \quad \text{složení implikací, MP}$$

11

Tím, že jsme dokázali (3) a (4), jsme podle věty o důkazu rozbořem případů dokázali (2) a podle (1) i jednu implikaci případu c). Dokážeme opačnou implikaci.

$$\vdash \neg (C \rightarrow \exists x C) \quad \text{substituční lemma}$$

$$\vdash \neg (B \rightarrow C) \rightarrow \neg [(C \rightarrow \exists x C) \rightarrow (B \rightarrow (\exists x)C)]$$

skládání implikací

$$\vdash \neg (B \rightarrow C) \rightarrow (B \rightarrow (\exists x)C) \quad \text{MP}$$

$$\vdash \neg (\exists x)(B \rightarrow C) \rightarrow (B \rightarrow (\exists x)C) \quad \text{pravidlo } \exists$$

protože B neobsahuje x volně. Tím je případ c) dokázán pro oba kvantifikátory.

12

Při důkazu tvrzení c) pro existenční kvantifikátor, byla použita věta o důkazu rozbořem případů. Ale ta byla dokázána jen ve výrokové logice. V jejím důkazu se používá věta o dedukci, a to v obou směrech.

Při pečlivém provedení důkazu c) je třeba požadovat, aby

$$B \vdash (\exists x)C$$

byly uzavřené formule. Tohoto požadavku lze dosáhnout použitím věty o konstantách.

13

d) $Q \equiv \forall$

$\vdash ((\forall x)B \rightarrow C) \leftrightarrow (\neg C \rightarrow \neg(\forall x)B)$	tautologie
$\leftrightarrow (\neg C \rightarrow \neg(\forall x)\neg\neg B)$	ekvivalence
$\leftrightarrow (\neg C \rightarrow (\exists x)\neg B)$	operace b)
$\leftrightarrow (\exists x)(\neg C \rightarrow \neg B)$	operace c)
$\leftrightarrow (\exists x)(B \rightarrow C)$	tautologie

Pro $Q \equiv \exists$ se důkaz dělá obdobně.

14

e) důkaz prenexní operace pro konjunci a disjunci se převede na předchozí operace a) - d) rozepsáním zkratk.

15

Důkaz Věty

se provádí indukcí podle složitosti formule A .

- (i) je-li A atomická, pak je v prenexním tvaru a A' je A .
- (ii) je-li A tvaru $\neg B$ a B' je prenexní tvar B , A' se sestrojí pomocí operace b).
- (iii) je-li A tvaru $B \rightarrow C$ a B', C' jsou prenexní tvary B a C , potom podle věty o variantách (operace a)), přejmenujeme vázané proměnné tak, aby žádná volná proměnná B' nebyla vázaná v C' a naopak.

Platí

$$\vdash A \leftrightarrow (B' \rightarrow C')$$

a A' se sestrojí pomocí c) a d).

16

Příklady.

Nechť proměnná x není volná ve formuli B a proměnná y se nevyskytuje v B ani v C .

a) Prenexní operace pro ekvivalenci

$$(B \leftrightarrow (\forall x)C)$$

$$(B \rightarrow (\forall x)C) \& ((\forall y)C_x[y] \rightarrow B) \quad \text{ekvivalence, varianta}$$

$$(\forall x)(B \rightarrow C) \& (\exists y)(C_x[y] \rightarrow B) \quad \text{operace e)}$$

$$(\forall x)(\exists y)[(B \rightarrow C) \& (C_x[y] \rightarrow B)] \quad \text{operace c), d)}$$

17

b) Prenexní tvar v aritmetice.

$$(\exists x)(x = y) \rightarrow (\exists x)(x = 0 \vee \neg(\exists y)(y < 0)) \quad (o)$$

$$(\exists x)(x = y) \rightarrow (\exists u)(u = 0 \vee \neg(\exists v)(v < 0)) \quad (a)$$

$$(\exists x)(x = y) \rightarrow (\exists u)(u = 0 \vee (\forall v)\neg(v < 0)) \quad (b)$$

$$(\exists x)(x = y) \rightarrow (\exists u)(\forall v)(u = 0 \vee \neg(v < 0)) \quad (e)$$

$$(\forall x)(\exists u)(\forall v)[(x = y) \rightarrow (u = 0 \vee \neg(v < 0))] \quad (c), (d)$$

Pořadí prenexních operací není deterministické, toto je jiný prenexní tvar formule (o).

$$(\exists u)(\forall x)(\forall v)[(x = y) \rightarrow (u = 0 \vee \neg(v < 0))]$$

18

Predikátová logika s rovností.

19

Schema axiomů identity.

Je-li x proměnná, pak následující formule je *axiom identity*

$$x = x \quad (R1)$$

{Leibnitzův axiom}

20

Schema axiomů rovnosti pro funkce.

Je-li f n -ární funkční symbol, $x_1, x_2, \dots, x_n$ a $y_1, y_2, \dots, y_n$ jsou proměnné, potom následující formule je *axiom rovnosti pro funkce*.

$$x_1 = y_1 \rightarrow \dots x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \quad (R2)$$

21

Schema axiomů rovnosti pro predikáty.

Je-li p n -ární predikátový symbol, $x_1, x_2, \dots, x_n$ a $y_1, y_2, \dots, y_n$ jsou proměnné, potom následující formule je *axiom rovnosti pro predikáty*.

$$x_1 = y_1 \rightarrow \dots x_n = y_n \rightarrow p(x_1, \dots, x_n) \rightarrow p(y_1, \dots, y_n) \quad (R3)$$

22

Elementární vlastnosti rovnosti.

O rovnosti se předpokládá, že je *reflexivní*, *symetrická* a *tranzitivní*.

Reflexivnost je dána axiomem (R1). Dokážeme nejprve symetrii, tedy

$$|- x = y \rightarrow y = x \quad (1)$$

pro libovolné proměnné x, y .

$$|- x = y \rightarrow \boxed{x = x} \rightarrow \boxed{x = x} \rightarrow y = x \quad (2)$$

$$|- x_1 = y_1 \rightarrow x_2 = y_2 \rightarrow x_1 = x_2 \rightarrow y_1 = y_2 \quad (R3)$$

$$|- x = y \rightarrow y = x \quad (2), (R1), MP$$

Tím je dokázáno (1).

23

Tranzitivnost

$$x = y \rightarrow y = z \rightarrow x = z \quad (3)$$

$$|- y = x \rightarrow z = z \rightarrow y = z \rightarrow x = z \quad (R3)$$

Pro kontrolu

$$|- x_1 = y_1 \rightarrow x_2 = y_2 \rightarrow x_1 = x_2 \rightarrow y_1 = y_2 \quad (R3)$$

$$|- y = x \rightarrow y = z \rightarrow x = z \quad (R1), (R3), MP$$

Formule (3) se odvodí složením poslední implikace s implikací (1).

24

Základní věta o rovnosti.

Necht' T je množina formulí a $t_1, \dots, t_n, s_1, \dots, s_n$ jsou termy pro, které platí

$$T \mid -t_1 = s_1, \dots, -t_n = s_n \quad (5)$$

(i) Je-li t term a term s z něj vznikne záměnou některých výskytů termů t_i odpovídajícími termy s_i , potom

$$T \mid -t = s \quad (6)$$

(ii) Je-li A' formule, která vznikne z formule A záměnou některých výskytů termů t_i odpovídajícími termy s_i , ne však bezprostředně za kvantifikátorem, potom

$$T \mid -A' = A \quad (7)$$

25

Důkaz.

(i) Indukcí podle složitosti termu t . Je-li t proměnná nebo některý z termů t_i a term s vznikne záměnou celého termu t termem s , potom (6) je jedním z předpokladů (5).

Je-li term t tvaru $f(r_1, \dots, r_k)$ a term s tvaru $f(r'_1, \dots, r'_k)$ z indukčního předpokladu dostáváme

$$T \mid -r_1 = r'_1, \dots, -r_n = r'_n \quad (8)$$

$$\mid -r_1 = r'_1 \rightarrow \dots r_k = r'_k \rightarrow \underbrace{f(x_1, \dots, x_k)}_t = \underbrace{f(r'_1, \dots, r'_k)}_s \quad (R2)$$

odkud tvrzení (i) odvodíme pravidlem modus ponens.

Tvrzení (ii) se dokazuje obdobně.

26

Důsledek.

Jsou-li $t, t_1, \dots, t_n, s_1, \dots, s_n$ termy, A formule, potom platí

$$(i) \mid -t_1 = s_1 \rightarrow \dots t_n = s_n \rightarrow t[t_1, \dots, t_n] = t[s_1, \dots, s_n]$$

$$(ii) \mid -t_1 = s_1 \rightarrow \dots t_n = s_n \rightarrow (A[t_1, \dots, t_n] \leftrightarrow A[s_1, \dots, s_n])$$

Je-li navíc x proměnná, která není obsažena v termu t , potom

$$(iii) \mid -A_x[t] \leftrightarrow (\forall x)(x = t \rightarrow A)$$

$$(iv) \mid -A_x[t] \leftrightarrow (\exists x)(x = t \ \& \ A)$$

27

Pravdivost a dokazatelnost

Vztah formálního systému a sémantiky predikátové logiky

1

Teorie prvního řádu.

Je-li L jazyk prvního řádu a T množina jeho formulí, říkáme, že T je *teorie prvního řádu s jazykem L* .

Formulím z množiny T říkáme *speciální axiomy teorie T* .

Predikátová logika je zvláštním případem teorie prvního řádu, která nemá žádné speciální axiomy.

2

Modely teorií.

(i) Je-li T teorie s jazykem L a M je interpretace jazyka L , říkáme, že *M je modelem teorie T* a píšeme $M \models T$, jestliže každý speciální axiom teorie T , tedy každá formule z T je pravdivá v M .

(ii) Říkáme, že *formule A je sémantickým důsledkem teorie (množiny) T* a píšeme $T \models A$, jestliže A je pravdivá v každém modelu teorie T .

3

Příklady.

(a) *Teorie (ostrého) uspořádání* má jazyk s rovností, který obsahuje jediný speciální symbol, binární predikát $<$ a dva speciální axiomy

$$\neg(x < x)$$

$$x < y \rightarrow (y < z \rightarrow x < z)$$

každý model této teorie je částečně uspořádaná množina.

(b) přidáme-li ještě axiom $x < y \vee x = y \vee y < x$, dostaneme *teorii (ostrého) lineárního uspořádání*. Každý model této teorie je lineárně uspořádaná množina.

4

(c) Teorie okruhů, oborů integrity a těles. Necht'

$$L = \{0, 1, +, *\}$$

je jazyk s rovností, kde $0, 1$ jsou konstanty a $+, *$ jsou binární funkční symboly pro operace sčítání a násobení.

Teorie komutativních okruhů s jednotkou má tyto speciální axiomy pro sčítání

$$x + (y + z) = (x + y) + z \quad (\text{o1})$$

$$x + 0 = x \quad 0 + x = x \quad (\text{o2})$$

$$(\exists y)(x + y = 0 \ \& \ y + x = 0) \quad (\text{o3})$$

$$x + y = y + x \quad (\text{o4})$$

5

a pro násobení

$$1 * x = x \quad x * 1 = x \quad (\text{o5})$$

$$x * (y * z) = (x * y) * z \quad (\text{o6})$$

$$x * y = y * x \quad (\text{o7})$$

$$x * (y + z) = (x * y) + (x * z) \quad (\text{o8})$$

přidáme-li axiom

$$x * y = 0 \rightarrow (x = 0 \vee y = 0) \quad (\text{i1})$$

dostaneme *Teorii oborů integrity*. Přidáme-li k teorii okruhů dva axiomy

$$0 \neq 1 \quad (\text{t1})$$

$$x \neq 0 \rightarrow (\exists y)(y * x = 1) \quad (\text{t2})$$

dostaneme *Teorii těles*.

6

(d) Jazyk *elementární aritmetiky* obsahuje rovnost a speciální symboly $0, S, +, *$ kde

- 0 je konstanta pro nejmenší přirozené číslo,
- S je unární funkční symbol pro následující přirozené číslo $S(x) = x + 1$,
- $+$ a $*$ jsou binární funkční symboly pro operace sčítání a násobení.

7

Elementární aritmetika má tyto speciální axiomy

$$S(x) \neq 0$$

$$S(x) = S(y) \rightarrow x = y$$

$$x \neq 0 \rightarrow (\exists y)(S(y) = x)$$

$$x + 0 = x$$

$$x + S(y) = S(x + y)$$

$$x * 0 = 0$$

$$x * S(y) = (x * y) + x$$

8

Interpretace $\mathcal{N}$, jejíž doménou jsou přirozená čísla,

$$0_{\mathcal{N}} = 0$$

$$S_{\mathcal{N}}(x) = x + 1 = (x \cup \{x\})$$

$$x +_{\mathcal{N}} y = x + y = (x \oplus y) \quad \text{ordinální součet}$$

$$x *_{\mathcal{N}} y = x * y = (x \otimes y) \quad \text{ordinální součin}$$

Se nazývá *standardní model aritmetiky*.

9

Věta o korektnosti.

Je-li T teorie, A formule T , potom platí

$$T \vdash A \Rightarrow T \models A$$

Speciálně

$$\vdash A \Rightarrow \models A$$

$\{\Rightarrow\}$ není implikace v jazyku T , zastupuje slova "jestliže ... potom "...}

10

Lemma.

Axiomy predikátové logiky jsou validní formule.

Důkaz. Necht' L je jazyk predikátové logiky a A jeho formule. Necht' M je libovolná interpretace jazyka L , e je pravdivostní ohodnocení v M . Probereme jednotlivé axiomy.

(a) A je případ axiomu A' výrokové logiky. Podle věty o úplnosti výrokové logiky je A' tautologie.

Jsou-li $p_1, \dots, p_n$ všechny výrokové proměnné fomule A' a $A_1, \dots, A_n$ jsou formule, které v A vystupují na jejich místě, pak $M \models A[e]$ nezávisle na pravdivosti $M \models A_i[e]$ $i, 1 \leq i \leq n$.

11

(b1) A je případ axiomu specifikace tvaru $(\forall x)B \rightarrow B_x[t]$. Je-li $M \models (\forall x)B[e]$, potom implikace A je pravdivá.

Naopak, je-li $M \models (\forall x)B[e]$, potom $M \models (\forall x)B[e(x/m)]$, pro libovolný prvek m z domény M , speciálně pro $t[e]$. potom $M \models (B_x[t])[e]$. Axiom specifikace je pravdivý v M .

(b2) A je případ axiomu přeskočkovu tvaru

$$(\forall x)(B \rightarrow C) \rightarrow (B \rightarrow (\forall x)C) \quad (1)$$

kde proměnná x není volná v B . Jako v předchozím případě, není-li pravdivý předpoklad implikace, potom A je pravdivá v M při ohodnocení e .

12

Předpokládejme, že $M \models (\forall x)(B \rightarrow C)[e]$, tedy pro libovolné m z domény M podle definice splňování platí

$$M \models (B \rightarrow C)[e(x/m)].$$

to znamená, že buď je formule B pravdivá při ohodnocení $e(x/m)$ nebo totéž musí platit pro formuli C .

Protože formule B neobsahuje proměnnou x volně, je pravdivá při ohodnocení $e(x/m)$ právě když je pravdivá při ohodnocení e . Přitom $M \models C[e(x/m)]$ to znamená, že $M \models (\forall x)C[e]$, a tedy $M \models (B \rightarrow (\forall x)C)[e]$.

Tím je pravdivost (a validnost) (1) dokázána.

13

(c) Necht' A je axiom rovnosti pro funkce

$$x_1 = y_1 \rightarrow \dots x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \quad (2)$$

Je zřejmé, že nebude-li některá z rovností $x_i = y_i$ některá splněna při ohodnocení e , potom nebude splněn axiom (2).

Předpokládejme, že tom u tak není, to znamená, že

$$e(x_1) = e(y_1) \dots e(x_n) = e(y_n) \quad (3)$$

Potom

$$M \models (f(x_1, \dots, x_n) = f(y_1, \dots, y_n))[e] \Leftrightarrow \\ \Leftrightarrow f_M(e(x_1), \dots, e(x_n)) = f_M(e(y_1), \dots, e(y_n))$$

a z (3) plyne $M \models A[e]$

Validnost axiomu rovnosti pro predikáty se dokazuje podobně.

14

Důkaz věty o korektnosti.

Předpokládejme, že $T \vdash A$ a že $A_1, \dots, A_n \equiv A$ je důkaz A v teorii T . Necht' M je libovolný model T .

Budeme postupovat indukcí podle důkazu formule A . Předpokládejme, že A_i je taková, že pro všechny formule $A_j, 1 \leq j < i$ již bylo dokázáno $M \models A_j$.

Dokážeme

$$M \models A_i. \quad (1)$$

Rozebereme několik případů

15

(a) A_i je axiom predikátové logiky. Pak je to validní formule a (1) platí.

(b) A_i je axiom T . Potom (1) platí protože M je model T .

(c) A_i je odvozena z formulí $A_j, A_k, 1 \leq j, k < i$ pravidlem modus ponens. Předpokládejme, že platí

$$A_k \equiv A_j \rightarrow A_i.$$

Z indukčního předpokladu dostáváme $M \models A_j$ a $M \models A_k$.

Z korektnosti pravidla modus ponens také $M \models A_i$.

16

(c) A_i je odvozena z formule $A_j, 1 \leq j < i$ pravidlem generalizace. Tedy $A_i \equiv (\forall x) A_j$ pro nějakou proměnnou x .

necht' e je libovolné ohodnocení. Z indukčního předpokladu plyne $M \models A_j$, tedy také $M \models A_j[e]$.

Speciálně

$$M \models A_j[e(x/m)]$$

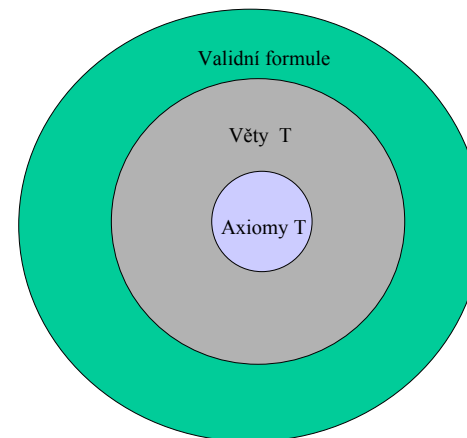
odkud

$$M \models \underbrace{((\forall x) A_j)}_{A_i}[e]$$

protože e bylo libovolné ohodnocení, dostáváme

$$M \models A_i.$$

Tím je věta o korektnosti dokázána.



Věta o úplnosti.

1

Věta o úplnosti. (Gödel 1930)

Nechť T je teorie s jazykem L .

(i) je-li A libovolná formule jazyka L , potom platí

$$T \mid - A \quad \text{právě když} \quad T \models A$$

(ii) Teorie T je bezesporná, právě když má model.

2

Pozorování.

Věta o korektnosti dává polovinu z každého tvrzení Věty o úplnosti.

Samotná věta o korektnosti je implikací zleva doprava v tvrzení (i),

zatím co

její důsledek je implikací zprava doleva v tvrzení (ii).

3

Lemma.

Ve Větě o úplnosti druhé tvrzení implikuje první.

Důkaz. Předpokládejme, že platí (ii). Nechť T je teorie, A formule jazyka teorie T .

Víme

$$T \mid - A \quad \text{právě když} \quad T \cup \{\neg \text{uzávěr}(A)\} \text{ je sporná}$$

Podle (ii) to znamená, že teorie $T \cup \{\neg \text{uzávěr}(A)\}$ nemá model. Tedy v každém modelu teorie T je pravdivá (uzavřená) formule $\text{uzávěr}(A)$ a také A .

Tím je tvrzení (i) dokázáno.

4

Větu o úplnosti dokážeme, podaří-li se nám dokázat, že každá bezesporná teorie má model. Metoda, kterou použijeme není původní Gödelova, ale pochází od L. Henkina.

Mějme bezespornou teorii T s jazykem L . Naším úkolem je sestavit její model, tedy strukturu M , která má neprázdné universum M a která v něm interpretuje všechny funkční a predikátové symboly teorie T .

Přitom T nám poskytuje jenom syntaktický materiál v podobě jazyka, axiomů a vět. Z něj musíme strukturu M vytvořit. Navíc máme užitečný předpoklad, že T je bezesporná teorie.

5

Kanonická struktura M .

- **Universum M** = $\{t \mid t \text{ je term bez proměnných}\}$
- **Funkční symboly** (nepotřebujeme ohodnocení proměnných). Je-li $t_1, \dots, t_n \in M$ a f je n -ární funkční symbol, jeho realizaci f_M definujeme následovně
- **Predikátové symboly**. Je-li p n -ární predikátový symbol, jeho interpretace p_M se definuje takto

$$f_M(t_1, \dots, t_n) = f(t_1, \dots, t_n) \in M$$

$$(t_1, \dots, t_n) \in p_M \text{ právě když } T \vdash p(t_1, \dots, t_n)$$

6

Pokud jazyk L neobsahuje predikát rovnosti, je lehké ověřit indukcí podle složitosti termu, že $t[e] = t$ pro každý prvek t univerza a každé ohodnocení proměnných e .

Potom pro každou atomickou formuli $A \equiv p(t_1, \dots, t_n)$ bez proměnných (a každé ohodnocení e) platí

$$\begin{aligned} M \models A &\Leftrightarrow M \models A[e] \\ &\Leftrightarrow (t_1, \dots, t_n) \in p_M \\ &\Leftrightarrow T \vdash A \end{aligned} \quad (1)$$

Sémantika atomických formulí bez proměnných je tedy dána větami teorie T .

7

Sémantika se trochu zkomplikuje, pokud jazyk L obsahuje predikát rovnosti. Je-li například T aritmetika, může se stát, že

$$T \vdash \underbrace{S(0) + S(0)}_t = \underbrace{S(S(0))}_s$$

ale

$$M \not\models \underbrace{S(0) + S(0)}_t = \underbrace{S(S(0))}_s \text{ protože } t \neq s$$

Struktura M považuje termy t, s za dvě různá individua.

8

Zde pomůžte faktorizace. Víme, že predikát rovnosti definuje na množině všech termů, tedy i na univerzu M , struktury M , reflexivní, symetrickou a tranzitivní relaci, tedy relaci ekvivalence, označme ji $\approx$ a definujme

$$t \approx s \text{ právě když } T \models t = s$$

Místo termů samotných pracujeme s třídami ekvivalence $[t] = \{s \in M \mid s \approx t\}$ a s univerzem $M/\approx$.

Potom hodnotou termu t ve struktuře M je $[t]$.

Platí

$$[t] = [s] \text{ právě když } T \models t = s$$

9

Tedy

$$\begin{aligned} M \models t = s &\Leftrightarrow [t] = [s] \\ &\Leftrightarrow T \models t = s \end{aligned}$$

definujeme-li pro funkční symboly f

$$f_M([t_1], \dots, [t_n]) = [f(t_1, \dots, t_n)] \quad (2)$$

a ostatní predikáty p , $p_M \subseteq (M/\approx)^n$ předpisem

$$([t_1], \dots, [t_n]) \in p_M \text{ právě když } T \models p(t_1, \dots, t_n) \quad (3)$$

dostáváme následující tvrzení.

10

Lemma.

Nechť M je kanonická struktura pro L . Nechť A je atomická formule bez proměnných jazyka L . Potom platí

$$M \models A \Leftrightarrow T \models A \quad (4)$$

11

Důkaz

probíhá úplně stejně, jako u předchozího tvrzení (1), jenom je třeba ověřit, že definice f_M a p_M jsou korektní, tedy že (2) a (3) nezávisí na volbě termů $s_i \in [t_i]$.

Interpretaci f_M funkčního symbolu f jsme definovali předpisem (2).

Nechť $s_l \in [t_l], \dots, s_n \in [t_n]$ pro libovolné $i, 1 \leq i \leq n$ (5) platí

$$\begin{aligned} s_i \in [t_i] &\Leftrightarrow s_i \approx t_i \\ &\Leftrightarrow T \models s_i = t_i \end{aligned} \quad (6)$$

12

z (5) a (6) dostáváme

$$T \mid - s_i = t_i \quad \text{pro} \quad i, 1 \leq i \leq n \quad (7)$$

vezměme axiom rovnosti pro f .

$$s_1 = t_1 \rightarrow \dots \rightarrow s_n = t_n \rightarrow f(s_1, \dots, s_n) = f(t_1, \dots, t_n)$$

Potom

$$T \mid - f(s_1, \dots, s_n) = f(t_1, \dots, t_n) \quad \text{MP, (7)}$$

Tedy

$$[f(s_1, \dots, s_n)] = [f(t_1, \dots, t_n)]$$

a definice f_M je korektní. Stejným způsobem bychom dokázali, že korektní je i definice p_M .

13

Naším cílem je dokázat stejnou větu (4) pro každou uzavřenou formuli A . Potom struktura $\mathbf{M}$ bude modelem teorie T .

Pro libovolný axiom B teorie T a jeho uzávěr A , dostáváme $T \mid - A$ a podle (4) také $\mathbf{M} \models A$. Z definice splňování potom $\mathbf{M} \models B$.

14

Další postup

- Větu o úplnosti dokážeme jen pro některé teorie (úplné a Henkinovy)
- Ukážeme, že každou bezespornou teorii lze rozšířit do teorie s požadovanými vlastnostmi.
- Ukážeme, že model rozšíření nějaké teorie lze redukovat do modelu výchozí teorie.
- Tím sestrojíme model libovolné bezesporné teorie.

15

Dvě definice.

Nechť T je teorie s jazykem L .

(i) Říkáme, že T je **úplná teorie**, je-li bezesporná a pro libovolnou uzavřenou formuli A jazyka L je jedna z formulí A a $\neg A$ dokazatelná v T .

(ii) Říkáme, že T je **Henkinova teorie**, jestliže pro libovolnou uzavřenou formuli tvaru $(\exists x)B$ existuje konstanta c , taková, že

$$T \mid - (\exists x)B \rightarrow B_x[c]$$

16

Věta o kanonickém modelu.

Je-li T úplná a Henkinova teorie, potom kanonická struktura M pro T je modelem T .

17

Důkaz.

Pro každou uzavřenou formuli A ukážeme

$$M \models A \Leftrightarrow T \vdash A \quad (4)$$

a) pro uzavřené atomické formule jsme to již dokázali.

b) je-li A tvaru $\neg B$, potom

$$\begin{aligned} M \models A &\Leftrightarrow M \not\models B \\ &\Leftrightarrow T \not\vdash B && \text{indukční předpoklad} \\ &\Leftrightarrow T \vdash \neg B && \text{úplnost } T \\ &\Leftrightarrow T \vdash \neg A \end{aligned}$$

18

c) je-li A tvaru $B \rightarrow C$, potom

$$\begin{aligned} M \models A &\Leftrightarrow M \not\models B \text{ nebo } M \models C \\ &\Leftrightarrow T \not\vdash B \text{ nebo } T \vdash C && \text{indukční předpoklad} \\ &\Leftrightarrow T \vdash \neg B \text{ nebo } T \vdash C && \text{úplnost } T \\ &\Leftrightarrow T \vdash \neg A && \{\text{cvičení}\} \end{aligned}$$

19

d) Je-li A uzavřená formule tvaru $(\exists x)B$, potom

$$\begin{aligned} M \models A &\Leftrightarrow M \models B(x/[t]) \quad \text{pro nějaký term } t \text{ bez proměnných} \\ &\Leftrightarrow M \models B_x[t] \quad \text{pro nějaký term } t \text{ bez proměnných} \\ &\Leftrightarrow T \vdash B_x[t] \quad \text{pro nějaký term } t \text{ bez proměnných} \\ &\Leftrightarrow T \vdash A \end{aligned}$$

20

Rozeberme ještě podrobněji poslední ekvivalenci.

$$A \equiv (\exists x)B$$

T je Henkinova, existuje tedy konstanta c , taková, že

$$T \mid - (\exists x)B \rightarrow B_x[c] \quad (5)$$

Tím je implikace zdola nahoru dokázána. Obrácená implikace je instancí lemmatu o substituci.

Tím je věta o kanonickém modelu dokázána a první krok na cestě k důkazu věty o úplnosti máme za sebou.

21

Co jsme již dosáhli

- Větu o úplnosti dokážeme jen pro některé teorie (úplné a Henkinovy)
- Ukážeme, že každou bezespornou teorii lze rozšířit do teorie s požadovanými vlastnostmi.
- Ukážeme, že model rozšíření nějaké teorie lze redukovat do modelu výchozí teorie.
- Tím sestojíme model libovolné bezesporné teorie.

22

Jak rozšířit teorii: dva způsoby

- Necht' L a L' jsou jazyky, necht' T je teorie s jazykem L a T' je teorie s jazykem L' .
- **Definice.** Říkáme, že *jazyk L' je rozšířením jazyka L* , jestliže každý symbol jazyka L je symbolem jazyka L' stejného významu a stejné četnosti.
- **Definice.** Říkáme, že *teorie T' je rozšířením teorie T* , jestliže L' je rozšířením L a každý axiom teorie T je větou teorie T' .
- **Definice.** Říkáme, že *T' je konzervativní rozšíření T* , je-li to rozšíření a pro každou formuli A jazyka L platí

$$T' \mid - A \Rightarrow T \mid - A.$$

23

Pozorování.

- (i) je-li T' rozšířením teorie T a T' je bezesporná, potom T je také bezesporná.
- (ii) je-li T' konzervativní rozšíření T , potom T je bezesporná, právě když je bezesporná teorie T' .

24

Věta. (Henkin)

Ke každé teorii T lze sestrojit konzervativní rozšíření T_H , které je Henkinovou teorií.

25

Důkaz.

Teorii T_H sestrojíme postupným přidáváním axiomů tak, aby byla splněna podmínka (5) z definice Henkinovy teorie.

Položme $T \equiv T_0$, $L \equiv L_0$ a pro libovolnou uzavřenou formuli

$$(\exists x)B$$

přidejme do jazyka L_0 novou speciální konstantu

$$c_{(\exists x)B} \quad (6)$$

a do teorie T_0 axiom

$$(\exists x)B \rightarrow B_x[c_{(\exists x)B}] \quad (7)$$

Budeme říkat, že konstanta (6) přísluší k axiomu (7).

26

Tak vytvoříme rozšíření L_1 jazyka L_0 a rozšíření T_1 teorie T_0 .

Tento postup je třeba iterovat. Formule $(\exists x)B$ jazyka teorie T_1 může obsahovat konstantu $c_{(\exists x)B}$ z T_1 k níž nepatří žádný axiom

$$(\exists x)B \rightarrow B_x[c_{(\exists x)B}].$$

Proto konstanty (6) teorie T_1 nazveme Henkinovými konstantami prvního řádu a k nim příslušné axiomy (7) také nazveme Henkinovými axiomy prvního řádu.

Opakujeme-li stejný postup s uzavřenými existenčními formulami teorie T_1 sestrojíme rozšíření L_2 jazyka L_1 a rozšíření T_2 teorie T_1 . Tak získáme Henkinovy konstanty a axiomy druhého řádu.

27

Postupně vytvoříme posloupnost rozšíření jazyků

$$L \equiv L_0 \subset L_1 \subset \dots \subset L_n \subset L_{n+1} \subset \dots$$

a teorií

$$T \equiv T_0 \subset T_1 \subset \dots \subset T_n \subset T_{n+1} \subset \dots$$

Položíme-li

$$L_H = \bigcup_{n=0}^{\infty} L_n \quad T_H = \bigcup_{n=0}^{\infty} T_n$$

potom jazyk L_H obsahuje Henkinovy konstanty všech řádů a v teorii T_H jsou všechny k nim příslušné axiomy. Tedy T_H je Henkinova teorie.

Zbývá dokázat, že je to konzervativní rozšíření teorie T .

28

Necht' A je formule jazyka L , která je větou T_H .

Necht'

$$B_1, B_2, \dots, B_n \quad (8)$$

jsou všechny Henkinovy axiomy z důkazu A . Potom

$$T, B_1, B_2, \dots, B_n \vdash A$$

protože (8) jsou uzavřené formule, z Věty o dedukci dostáváme

$$T \vdash B_1 \rightarrow B_2 \rightarrow \dots \rightarrow B_n \rightarrow A \quad (9)$$

Bez újmy na obecnosti můžeme předpokládat, že B_1 je axiom příslušný k Henkinově konstantě maximálního řádu.

29

Tedy řád konstanty příslušející k axiomu B_1 je větší nebo roven řádům všech konstant příslušejících k formulím

$$B_2, \dots, B_n$$

Předpokládejme, že B_1 je tvaru

$$(\exists x)D \rightarrow D_x[c_{(\exists x)D}].$$

Podle předpokladu o řádech Henkinových konstant, $c_{(\exists x)D}$ není obsažena ve formulích $B_2, \dots, B_n$ a tím méně v teorii T . Můžeme použít větu o konstantách a nahradíme uvedenou Henkinovu konstantu novou proměnnou w .

30

Z (9) dostaneme

$$T \vdash ((\exists x)D \rightarrow D_x[w]) \rightarrow \underbrace{(B_2 \rightarrow \dots \rightarrow (B_n \rightarrow A))}_{\text{neobsahuje } w}$$

pravidlem zavedení $\exists$

$$T \vdash (\exists w) \underbrace{((\exists x)D \rightarrow D_x[w])}_{\text{není } w} \rightarrow (B_2 \rightarrow \dots \rightarrow (B_n \rightarrow A))$$

prenexní operací

$$T \vdash ((\exists x)D \rightarrow (\exists w)D_x[w]) \rightarrow (B_2 \rightarrow \dots \rightarrow (B_n \rightarrow A))$$

z Věty o variantách plyne

$$\vdash ((\exists x)D \rightarrow (\exists w)D_x[w])$$

$$T \vdash B_2 \rightarrow \dots \rightarrow B_n \rightarrow A \quad \text{MP}$$

$\vdots$

$$T \vdash A \quad \text{dostaneme opakováním stejného postupu}$$

31

Věta (Lindenbaum)

Každou bezespornou teorii T lze rozšířit do úplné teorie S se stejným jazykem jako T .

32

Důkaz.

Je-li dána bezesporná teorie T s jazykem L , podle Věty o uzavěru můžeme předpokládat, že všechny axiomy T jsou uzavřené formule.

Úplné rozšíření T_U teorie T sestojíme jako maximální bezesporné rozšíření T s jazykem L .

Postupujeme stejným způsobem jako u obdobné věty Výrokové logiky, jenom místo všech formulí očíslovujeme jen formule uzavřené.

33

Uspořádejme všechny uzavřené formule jazyka L do posloupnosti

$$A_0, A_1, A_2, \dots, A_n, \dots$$

na uspořádání formulí nezáleží, důležité je, aby posloupnost byla prostá.

Vytvoříme neklesající posloupnost teorií se stejným jazykem

$$T \equiv T_0 \subseteq T_1 \subseteq \dots T_n \subseteq \dots$$

následujícím postupem.

34

Je-li $T \cup \{A_0\}$ bezesporná, definujeme $T_1 = T \cup \{A_0\}$, jinak položíme $T_1 = T$. V α -tém kroku položíme $T_{\alpha+1} = T_\alpha \cup \{A_\alpha\}$ je-li to bezesporná teorie, jinak $T_{\alpha+1} = T_\alpha$. Je-li α limitní ordinál položíme $T_\alpha = \bigcup_{\beta < \alpha} T_\beta$.

Necht' T_U je sjednocení všech teorií T_α .

Stejným způsobem jako v Lindenbaumově větě ve Výrokové logice se ověří, že S je bezesporná maximální množina uzavřených formulí teorie T .

35

Ukážeme, že T_U je úplná teorie. Postupujeme sporem. Necht' T_U není úplná a existuje uzavřená formule A taková, že

$$T_U \not\models A \quad \text{a} \quad T_U \not\models \neg A$$

Protože $\neg A$ není větou T_U , nemůže být ani prvkem T_U . Navíc A také není dokazatelná v T_U , to znamená, že

$$T_U \cup \{\neg A\}$$

je bezesporná a T_U je její vlastní podmnožinou. To je ve sporu s maximalitou množiny T_U . Teorie T_U je tedy úplná.

36

Redukce a expanze struktur

Definice. Je-li L' rozšíření jazyka L , potom

(i) je-li M' interpretace jazyka L' , *redukce struktury M' do jazyka L* , kterou označíme $M'|L$, vznikne z M' vynecháním těch zobrazení a relací, které interpretují funkční a predikátové symboly, které nejsou v jazyce L .

(ii) je-li M interpretace jazyka L a M' interpretace L' , *říkáme, že M' je expanzí M* , jestliže $M = M'|L$.

Po všimněme si, že redukce a expanze mají stejné univerzum.

37

Lemma.

Nechť T' je rozšíření teorie T , která má jazyk L . Je-li M' model teorie T' potom reduct $M = M'|L$ je model teorie T .

38

Důkaz lemmatu.

M je reduct M' , mají tedy stejné univerzum a také stejnou množinu ohodnocení proměnných. Obě struktury interpretují stejně všechny funkční a predikátové symboly jazyka L .

(i) Nechť t je libovolný term jazyka L . Indukcí podle složitosti termu t se pro každé ohodnocení e dokáže, že interpretace (hodnota) $t[e]$ je stejná v obou strukturách.

39

(ii) je-li A formule jazyka L , potom se indukcí podle složitosti formule A dokáže pro každé ohodnocení e

$$M \models A[e] \Leftrightarrow M' \models A[e]$$

tedy také

$$M \models A \Leftrightarrow M' \models A$$

(iii) je-li A axiom teorie T , pak je větou teorie T' a podle věty o korektnosti je $M' \models A$ tedy také $M \models A$. To znamená, že M je model T .

40

Dosavadní výsledky můžeme shrnout takto

- Je-li dána bezesporná teorie T ,
- umíme sestrojit konservativní rozšíření T^* teorie T , které je Henkinovou teorií.
- Protože T je podle předpokladu bezesporná a T^* je její konzervativní rozšíření, je také T^* bezesporná.
- Můžeme, tedy sestrojit úplné rozšíření T^{**} teorie T^*
- Přitom T^{**} má stejný jazyk jako T^* je tedy Henkinova.
- Máme tedy úplnou Henkinovu teorii T^{**} , která je rozšířením teorie T . Podle Věty o kanonickém modelu má model M' .
- redukt $M = M' \upharpoonright L$ je model teorie T .

41

Věta o kompaktnosti.

Teorie T má model, právě když každý její konečný fragment $T' \subseteq T$ má model.

{spolu s Větou o úplnosti patří k několika větám, které charakterizují logiku prvního řádu.}

42

Důkaz.

Podle Věty o úplnosti má libovolná teorie S model, právě když je bezesporná.

(i) je-li bezesporná T pak je bezesporný každý její fragment a má tedy model.

(ii) je-li naopak bezesporný každý konečný fragment $T' \subseteq T$ pak je bezesporná i teorie T , protože důkaz sporu by se odehrál v nějakém konečném fragmentu T' . To znamená, že má-li každý konečný fragment teorie T model, pak T má také model.

43

Důsledek.

Je-li T teorie s jazykem L , A je libovolná formule jazyka L , potom

$$T \models A \iff T' \models A$$

pro nějaký konečný fragment $T' \subseteq T$.

44

Důkaz.

Podle věty o úplnosti

$$T \models A \Leftrightarrow T \vdash A$$

a důkaz formule A používá jen konečně mnoho axiomů teorie T .

45

Dva příklady.

a) Je nutné v logice prvního řádu popisovat teorii těles charakteristiky 0 nekonečným počtem axiomů?

Nechť T je teorie těles s jazykem $L = \{0, 1, +, \cdot\}$ s rovnostmi. Je-li x proměnná, termy

$$x, (x+x), (x+(x+x)), \dots, \underbrace{(x+(x+(x+\dots(x+x)\dots)))}_{n \text{ krát } x}, \dots$$

budeme označovat zkratkami

$$1 * x, 2 * x, 3 * x \dots n * x, \dots$$

a budeme jim říkat *přirozené násobky* x .

46

Připomeňme, že přirozená čísla nemusí být prvky každého tělesa a přirozený násobek imituje součin jako opakované přičítání.

Výraz $p * x$ může zastupovat term značné délky.

Pokud v nějakém tělese platí formule

$$p * 1 = 0 \tag{1}$$

pro nějaké nenulové p říkáme, že těleso má konečnou charakteristiku a nejmenší nenulové p , pro které platí (1) nazveme charakteristikou tělesa.

47

Pokud pro žádné nenulové p neplatí (1), říkáme, že těleso má charakteristiku 0.

Přidáme-li k teorii těles axiomy

$$p * 1 \neq 0 \tag{2}$$

pro všechna nenulová p , dostaneme rozšíření T' , které axiomatizuje tělesa charakteristiky nula.

Je přirozené položit si otázku, zda je možné nekonečnou množinu axiomů (2) nahradit konečně mnoha, a tedy jedním axiomem.

Odpověď je negativní.

48

Předpokládejme, že by nekonečné schema axiomů (2) bylo možné nahradit jedinou formulí A jazyka L .

Potom A je pravdivá ve všech tělesech charakteristiky 0 a v žádném tělese konečné charakteristiky.

Dostáváme $T' \models A$ a podle důsledku Věty o kompakt-nosti existuje konečný fragment T'' teorie T' takový, že $T'' \models A$.

49

Přitom T'' obsahuje jenom konečně mnoho axiomů (2). Je-li r největší z čísel v těchto axiomech, A platí v každém tělese konečné charakteristiky větší než r .

To je spor, protože algebra ukazuje, že existují tělesa libovolně velké konečné charakteristiky.

Nekonečnou množinu axiomů (2) nelze v logice prvního řádu nahradit jedním axiomem.

50

b) Je standardní model aritmetiky N jediným modelem aritmetiky (až na isomorfismus) ?

V Peanově aritmetice druhého řádu ANO.

V Peanově aritmetice prvního řádu NE.

Obě aritmetiky se liší celkovým rámcem, do kterého jsou zasazeny. Aritmetika druhého řádu je teorie v logice druhého řádu.

Aritmetika prvního řádu je teorie v logice prvního řádu.

51

Snad nejvíce se obě teorie liší ve vyjádření principu indukce.

Peanova aritmetika prvního řádu vznikne z Elementární aritmetiky přidáním *schematu axiomů indukce*:

pro každou formuli A a proměnnou x je následující formule *axiom indukce*.

$$A_x[0] \rightarrow ((\forall x)(A \rightarrow A_x[S(x)]) \rightarrow (\forall x)A) \quad (3)$$

Snadno se ověří, že standardní model (elementární) aritmetiky je také modelem Peanovy aritmetiky prvního řádu.

52

Peanova aritmetika druhého řádu (náznak)

$x, y, z, \dots$ proměnné pro čísla

$X, Y, Z, \dots$ proměnné pro množiny

$\in$ predikát náležení

Axiom indukce

$$(\forall X)[0 \in X \rightarrow ((\forall x)(x \in X \rightarrow S(x) \in X) \rightarrow (\forall x)(x \in X))]$$

Schema indukce (3) zachycuje jen spočetně mnoho instancí Axiomu indukce pro množiny, které jsou definovatelné pomocí formulí prvního řádu.

53

Ukážeme, že z Věty o kompaktnosti plyne, že existují modely Peanovy aritmetiky prvního řádu, které nejsou izomorfní se standardním modelem N . Takové modely nazýváme nestandardní.

Pro každé přirozené číslo n budeme definovat term $\overline{n}$ následovně.

$$\begin{aligned}\overline{0} &= 0 \\ \overline{1} &= S(0) \\ &\vdots \\ \overline{n+1} &= \underbrace{S(S(S(\dots S(0)\dots))}_{n+1 \text{ krát}}\end{aligned}$$

Tyto termy se nazývají *numerály*. Každé individuum standardního modelu je interpretací nějakého numerálu.

54

K jazyku Peanovy aritmetiky přidáme novou konstantu c a axiomy

$$\begin{aligned}\overline{0} &\neq c \\ \overline{1} &\neq c \\ &\vdots \\ \overline{n+1} &\neq c \\ &\vdots\end{aligned}\tag{4}$$

Tak vznikne rozšíření P_c Peanovy aritmetiky P . Přitom každý konečný fragment $T \subseteq P_c$ má model, který vznikne expanzí standardního modelu N .

T obsahuje jen konečně mnoho axiomů (4), konstantu c interpretujeme za všemi numerály z fragmentu T .

55

Podle Věty o kompaktnosti má teorie P_c model M' . Jeho redukcí do jazyka Peanovy aritmetiky dostaneme model M Peanovy aritmetiky, který není izomorfní se standardním modelem N .

M obsahuje individuum, které není interpretací žádného numerálu. Protože individua, která odpovídají numerálům tvoří počáteční úsek M , takové individuum má nekonečně předchůdců jako žádné individuum v N .

Proto N a M nejsou izomorfní.

56

Cvičení.

a) Ukažte, že žádná teorie prvního řádu T necharakterizuje třídu všech konečných interpretací svého jazyka. To znamená, že pro žádnou teorii T neplatí

$$M \models T \iff M \text{ je konečná struktura pro } T$$

[Návod. Sporem. Předpokládejte, že T má uvedenou vlastnost.

Rozšiřte jazyk o spočetně mnoho konstant

$$c_0, c_1, c_2, \dots, c_n, \dots \quad n \geq 0$$

a přidejte množinu S axiomů tvaru $c_i \neq c_j$ pro $i \neq j$.

Necht' $T' = T \cup S$. pomocí věty o kompaktnosti ukažte, že T' má nějaký model M' . Jeho redukt do T je potom nekonečný model T .]

b) Ukažte, že žádná teorie prvního řádu necharakterizuje třídu všech dobrých uspořádání.

[Návod. Sporem. Předpokládejte, že T má u vedenou vlastnost.

Podobně jako v a) přidejte spočetně mnoho konstant a k nim axiomy, které postulují nekonečnou klesající posloupnost. Pomocí věty o kompaktnosti ukažte, že takové rozšíření má nějaký model. Jeho reduktem je model T , který není dobrým uspořádáním.]

Vývoj teorií prvního řádu

Rozšiřování teorií

1

Teorie mají svou historii.

- Jejich formální systémy začínají axiomy.
- Ty jsou formulovány úsporně a v co nejjednodušším jazyku.
- S rozvíjením teorie přibývají nové pojmy.
- Konstanty, operace, predikáty.
- Ty jsou zaváděny pomocí formulí.
- Ukážeme, že nové pojmy mají pomocný charakter.
- Jejich definováním vznikne konzervativní rozšíření.
- Definované symboly lze eliminovat a tak se vrátit k původnímu jazyku.

2

Užitečné lemma

Nechť L' je rozšířením jazyka L a nechť T je teorie s jazykem L a T' teorie s jazykem L' .

(i) T' je rozšířením T , právě když redukt $M'|L$ každého modelu M' teorie T' je modelem T .

(ii) Je-li T' rozšířením T a každý model M teorie T lze expandovat do modelu M' teorie T' , potom T' je konzervativní rozšíření T .

3

Důkaz.

(i) Je-li T' rozšířením T , potom podle lemmatu o redukci a expanzi je redukt každého modelu teorie T' do L modelem teorie T .

Naopak nechť redukt každého modelu teorie T' do L je modelem teorie T .

Nechť A je axiom T a M' je libovolný model T' . Protože $M'|L$ je modelem T , $M'|L \models A$ a tedy $M' \models A$.

Formule A je tedy pravdivá v každém modelu teorie T' .

Podle věty o úplnosti je A větou T' . To znamená, že teorie T' je rozšířením T .

4

(ii) Necht' T' je rozšířením T a A je formule jazyka L , která je větou teorie T' .

Necht' M je libovolný model teorie T a M' je jeho expanze do modelu teorie T' . Potom podle Věty o korektnosti

$$M' \models A$$

odkud také

$$M \models M'|L \models A$$

Ukázali jsme, že formule A je pravdivá v každém modelu M teorie T . Podle Věty o úplnosti je A také větou T .

To znamená, že T' je konzervativní rozšíření T .

5

Rozšíření teorie o definici predikátu.

Motivace.

V aritmetice můžeme definovat predikát dělitelnosti

$$k \mid n \leftrightarrow (\exists s)(s * k = n)$$

Výraz $k \mid n$ čteme „ k dělí n “ nebo „ k je dělitelem n “.

Na levé straně ekvivalence je definovaný predikát a na pravé straně je definující formule.

6

Věta o definici predikátu.

Necht' T je teorie s jazykem L , necht' $x_1, \dots, x_n$ jsou proměnné.

Necht' D je formule jazyka L , taková, že všechny její volné proměnné jsou mezi $x_1, \dots, x_n$.

Necht' jazyk L' vznikne z L přidáním nového n -árního predikátového symbolu p a necht' rozšíření T' teorie T vznikne přidáním axiomu

$$p(x_1, \dots, x_n) \leftrightarrow D \quad (1)$$

Potom T' je konzervativní rozšíření T a nově definovaný symbol lze z každé formule B' jazyka L' eliminovat tak, že pro upravenou formuli B platí

$$T' \vdash B \leftrightarrow B'$$

7

Důkaz.

Nejprve ukážeme, že definovaný symbol lze eliminovat.

Necht' B' je libovolná formule jazyka L' . Zvolme variantu D' definující formule z (1) takovou, že žádná proměnná formule B' není vázaná v D' . Potom podle věty o variantách v definici (1) můžeme zaměnit D' za D .

Ve formuli B' nahradíme každou podformuli

formulí $p(t_1, \dots, t_n)$

potom $D'_{x_1 x_2 \dots x_n} [t_1, t_2, \dots, t_n]$

$$T' \vdash p(t_1, t_2, \dots, t_n) \leftrightarrow D'_{x_1 x_2 \dots x_n} [t_1, t_2, \dots, t_n] \quad (2)$$

8

Poslední ekvivalence je instancí varianty definujícího axiomu (1).

Ve formuli B' jsme nahrazovali některé atomické formule ekvivalentními formulemi. Pro výslednou formuli B podle Věty o ekvivalenci platí

$$T'|-B \leftrightarrow B'$$

Tím je možnost eliminace dokázána.

K důkazu konzervativnosti T' stačí pro libovolnou formuli B' jazyka L' ukázat

$$T'|-B' \Rightarrow T|-B \quad (3)$$

kde B vznikla z B' eliminováním definovaného predikátu. Speciálně, je-li B' z jazyka L , pak B a B' jsou totožné formule a (3) má tvar

$$T'|-B \Rightarrow T|-B$$

Tím bude konzervativnost dokázána.

Nechť $B'_1, \dots, B'_m$ je důkaz B' z T' . Necht' pro každé i formule B_i vznikne z B'_i eliminací definovaného predikátu.

Ukážeme, že každá formule B_i je větou teorie T . Postupujeme indukcí podle důkazu. Uvažujeme tyto případy.

a) B'_i je axiom predikátové logiky kromě axiomu rovnosti pro p . Potom B_i je axiom stejného druhu.

b) B'_i je axiom rovnosti pro p , tedy

$$x_1 = y_1 \rightarrow \dots \rightarrow x_n = y_n \rightarrow p(x_1, \dots, x_n) \rightarrow p(y_1, \dots, y_n)$$

potom B_i je tvaru

$$x_1 = y_1 \rightarrow \dots \rightarrow x_n = y_n \rightarrow D[x_1, \dots, x_n] \rightarrow D[y_1, \dots, y_n]$$

a to je důsledek Věty o rovnosti.

c) Je-li B'_i axiom z T' pak je buď z T a není co dokazovat, nebo je to definující axiom (1). V tomto případě je B_i tvaru $D \leftrightarrow D$ a to je instance Věty o variantách.

d) Je-li B'_i odvozena pravidlem modus ponens nebo pravidlem generalizace, pak B_i je odvozena stejným pravidlem z odpovídajících formulí.

Ukázali jsme, že každá formule B_i a tedy i formule B je větou T . Tím je (3) dokázáno a důkaz je uzavřen.

Rozšíření teorie o funkční symboly.

Dva způsoby rozšíření teorie o nový funkční symbol, podle toho s jakou určitostí jsou dány funkční hodnoty.

Příklad.

a) Řekneme-li „necht’ p je nějaké prvočíslo $p > x$ “, *zavádíme funkci* $f(x)$, formulí, která určí množinu možných hodnot a $f(x)$ vybere jednu z nich, ale nám nezáleží na tom, kterou.

b) Řekneme-li „necht’ p je nejmenší prvočíslo p , $p > x$ “, definujeme hodnotu p jednoznačně. V takovém případě *definujeme funkci* $f(x) = p$ formulí, která definuje hodnotu funkce jednoznačně.

13

Oba postupy mají své oprávnění.

Zavedení funkčního symbolu je jedinou možností v situaci, kdy umíme dokázat, že pro každou hodnotu argumentu je množina možných hodnot neprázdná, ale neumíme z nich žádnou jednoznačně definovat.

Definice funkčního symbolu odpovídá situaci, kdy se nám to podaří.

14

Věta o zavedení funkčního symbolu.

Necht’ T je teorie s jazykem L , necht’ formule

$$(\exists y)A \quad (4)$$

jazyka L má všechny volné proměnné mezi $x_1, \dots, x_n$.

Necht’ T' vznikne z T rozšířením jazyka o nový funkční n -ární symbol f a přidáním axiomu

$$A_y[f(x_1, \dots, x_n)] \quad (5)$$

Potom T' je konzervativním rozšířením teorie T .

15

K důkazu věty použijeme jeden důsledek axiomu výběru z teorie množin: Větu o dobrém uspořádání.

Připomeňme, že množina m je dobře uspořádaná relací $<$ jestliže každá neprázná podmnožina m' má nejmenší prvek vzhledem k $<$.

Věta o dobrém uspořádání.

Na každé množině existuje relace dobrého uspořádání.

16

Důkaz Věty o zavedení funkčního symbolu.

T' je rozšíření T , konzervativnost dokážeme tím, že libovolný model T budeme expandovat do modelu T' .

Nechť M je libovolný model T , nechť $<$ je relace dobrého uspořádání na jeho univerzu M .

Podle předpokladu je formule (4) větou teorie T , to znamená, že je pravdivá v M při každém ohodnocení proměnných e . Mějme takové ohodnocení e , nechť

$$e(x_1) = m_1, \dots, e(x_n) = m_n$$

17

Podle definice splňování existuje alespoň jedno individuum m takové, že $M \models A[e(y/m)]$. přitom m závisí na individuích $m_1, \dots, m_n$. množinu všech takových m označme

$$F(m_1, \dots, m_n) = \{m \mid M \models A[e(y/m)]\}$$

je to neprázdná množina individuí a protože uspořádání $<$ je dobré, má tato množina nejmenší prvek

$$\min(F(m_1, \dots, m_n))$$

Nyní můžeme definovat interpretaci $f_{M'}$ nového funkčního symbolu f předpisem

$$f_{M'}(m_1, \dots, m_n) = (\min(F(m_1, \dots, m_n)))$$

18

Je-li M' expanze modelu M přidáním interpretace $f_{M'}$ funkčního symbolu f , je zřejmé, že axiom (5) je pravdivý v M' .

Každý model T jsme expandovali do modelu T' , tedy T' je konzervativní rozšíření T .

Poznámka.

Důkaz věty se opíral o charakteristiku konzervativního rozšíření pomocí modelů. Modely teorií jsou množinové struktury, většinou nekonečné. Proto se takovým důkazům říká nefinitní.

Finitní důkaz této věty se opírá o Herbrandovu větu, která je mimo rámec této přednášky.

19

Aplikace: Skolemova věta.

Říkáme, že T je *otevřená teorie*, jestliže všechny axiomy z T jsou otevřené formule.

Věta (Skolem)

K libovolné teorii T lze sestavit otevřenou teorii T' , která je konzervativním rozšířením T .

20

Idea důkazu.

Věta o zavedení funkčního symbolu ukazuje, že pomocí zavedených funkčních symbolů lze eliminovat existenční kvantifikátory. {s univerzálními si poradíme podle věty o uzávěru}

Několik definic.

(i) říkáme, že *formule A je univerzální (existenční)*, je-li v prenexním tvaru a všechny kvantifikátory jsou univerzální (existenční).

(ii) Teorie T a S se stejným jazykem *jsou ekvivalentní*, jestliže mají stejné věty. Píšeme $T \equiv S$.

21

Podle Věty o úplnosti jsou dvě teorie ekvivalentní, právě když mají stejné modely.

Teorie T a S jsou ekvivalentní, právě když každý axiom z T je větou S a naopak.

22

Skolemova varianta formule.

Je-li A uzavřená formule v prenexním tvaru, indukcí podle počtu existenčních kvantifikátorů sestrojíme uzavřenou univerzální formuli A_S takovou, že $\vdash A_S \rightarrow A$.

(i) je-li A univerzální, A_S je A .

(ii) je-li A tvaru

$$(\forall x_1) \dots (\forall x_n)(\exists y)B \quad n \geq 0$$

necht' f je nový n -ární funkční symbol, definujeme formuli A°

$$(\forall x_1) \dots (\forall x_n)B_y[f(x_1, \dots, x_n)]$$

23

Pokud formule A° není otevřená, stejným postupem sestrojíme formuli $A^{\circ\circ} \dots$ až po konečném počtu kroků sestrojíme formuli A_S .

K sestrojení Skolemovy varianty potřebujeme rozšířit jazyk o konečně mnoho nových funkčních symbolů.

Podle substitučního lemmatu platí

$$\vdash A^\circ \rightarrow A \quad \text{a tedy} \quad \vdash A_S \rightarrow A \quad (7)$$

24

K důkazu Skolemovy věty zavedeme čtyři teorie, z nichž ta poslední bude otevřeným konzervativním rozšířením T .

T_1 je teorie se stejným jazykem jako T a její axiomy jsou uzávěry prenexních tvarů formulí z T . Z věty o prenexním tvaru a věty o uzávěru plyne, že teorie T a T_1 jsou ekvivalentní.

25

T_2 vznikne z T_1 tak, že ke každému axiomu A z T přidáme jeho Skolemovu variantu A_s . Potom T_2 je konzervativní rozšíření T_1 . Je-li A axiom z T_1 , potom přidáním axiomu A° vznikne podle věty o zavedení funkčního symbolu konzervativní rozšíření T_1 . Opakováním tohoto postupu dostaneme konzervativní rozšíření přidáním A_s .

T_3 vznikne z T_2 vynecháním všech axiomů teorie T_2 . Podle (7) jsou obě teorie ekvivalentní.

T_4 vznikne z T_3 nahrazením každého axiomu (je to univerzální formule) jeho otevřeným jádrem. Podle věty o uzávěru jsou obě teorie ekvivalentní.

26

Vytvořili jsme následující situaci

$$T \equiv T_1 \Rightarrow T_2 \equiv T_3 \equiv T_4$$

kde T_4 je otevřená teorie a je konzervativním rozšířením teorie T .

Tím je Skolemova věta dokázána.

27

Věta o definici funkčního symbolu.

Nechť L je jazyk, $x_1, \dots, x_n, y$ různé proměnné. Nechť T je teorie s jazykem L a D formule jazyka L s volnými proměnnými mezi $x_1, \dots, x_n, y$.

Nechť platí

$$T \models (\exists y)D \quad (8)$$

$$T \models D \rightarrow (D_y[t] \rightarrow y = t) \quad (9)$$

Nechť T' vznikne z T přidáním nového n -árního funkčního symbolu f a definujícího axiomu

$$y = f(x_1, \dots, x_n) \leftrightarrow D \quad (10)$$

28

Potom T' je konzervativní rozšíření teorie T a definovaný symbol lze eliminovat. To znamená, že ke každé formuli A' jazyka teorie T' lze sestrojít formuli A jazyka L , takovou, že

$$T' \vdash A \leftrightarrow A' \quad (11)$$

Důkaz je rozdělen do dvou kroků

- Nejprve dokážeme eliminovatelnost symbolu f
- potom konzervativnost rozšíření T'

29

a) eliminovatelnost. Všechny výskyty symbolu f najdeme už v atomických podformulích. Stačí dokázat (11) jen pro atomické formule a obecný případ plyne z věty o ekvivalenci.

Nechť A' je formule jazyka teorie T' . Při eliminaci postupujeme indukcí podle počtu výskytů symbolu f v A' .

Pokud f nemá výskyt v A' pak A je A' . V opačném případě uvažujeme některý z nejvnitřnějších výskytů f v A' , tedy term

$$f(t_1, \dots, t_n)$$

kde $t_1, \dots, t_n$ již neobsahují f .

30

Potom A' je tvaru

$$B'_z[f(t_1, \dots, t_n)]$$

kde B' má o jeden výskyt f méně než A' . Můžeme předpokládat, že proměnná z se nevyskytuje ani v A' ani v definující formuli D .

Podle indukčního předpokladu již umíme sestrojít formuli B jazyka L (tedy bez symbolu f) takovou, že

$$T' \vdash B \leftrightarrow B' \quad (11')$$

Pro definici formule A nechť D' je varianta definující formule D , která neváže žádnou proměnnou formule A' .

31

Nyní můžeme A definovat takto

$$A \equiv (\exists z)(D'_{x_1 x_2 \dots x_n y}[t_1, \dots, t_n, z] \& B)$$

Potom A je formule teorie T a ukážeme, že platí ekvivalence (11).

Z definujícího axiomu a věty o variantách dostáváme

$$T' \vdash z = f(t_1, \dots, t_n) \leftrightarrow D'_{x_1 x_2 \dots x_n y}[t_1, \dots, t_n, z]$$

a z (11') a věty o ekvivalenci dostaneme

$$T' \vdash (\exists z)(z = f(t_1, \dots, t_n) \& B') \leftrightarrow A$$

odkud pomocí vět o rovnosti

$$T' \vdash \underbrace{B'_z[f(t_1, \dots, t_n)]}_{A'} \leftrightarrow A$$

Tím je (11) dokázáno.

32

Zbývá dokázat konzervativnost rozšíření. Užijeme větu o zavedení funkčního symbolu.

Nechť S je teorie, která vznikne z T přidáním stejného funkčního symbolu f a axiomu

$$D_y[f(x_1, \dots, x_n)] \quad (12)$$

S je konzervativním rozšířením T , protože vznikla zavedením funkčního symbolu. Ukážeme, že S a T' jsou ekvivalentní.

K tomu stačí ukázat, že (12) je větou T' a definující axiom (10) je větou S .

33

a) (12) je větou T' . Vezměme instanci definujícího axiomu (10) a dostáváme

$$T' \vdash f(x_1, \dots, x_n) = f(x_1, \dots, x_n) \leftrightarrow D_y[f(x_1, \dots, x_n)]$$

Použitím axiomu identity a pravidla MP, potom

$$T' \vdash \underbrace{D_y[f(x_1, \dots, x_n)]}_{(12)}$$

b) (10) je větou S . Vyjdeme z této věty o rovnosti

$$\vdash y = f(x_1, \dots, x_n) \rightarrow (D \leftrightarrow D_y[f(x_1, \dots, x_n)])$$

odkud prostředky výrokové logiky

$$\vdash \neg D_y[f(x_1, \dots, x_n)] \rightarrow (y = f(x_1, \dots, x_n) \rightarrow D)$$

34

Z axiomu (12) a MP pak

$$S \vdash \neg y = f(x_1, \dots, x_n) \rightarrow D$$

Opačnou implikaci odvodíme z axiomu jednoznačnosti (9). Uvědomme si, že S je rozšířením T .

Záměnou prvních dvou členů implikace odvodíme

$$S \vdash \neg D_y[f(x_1, \dots, x_n)] \rightarrow (D \rightarrow y = f(x_1, \dots, x_n))$$

Z axiomu (12) a MP pak

$$S \vdash \neg D \rightarrow y = f(x_1, \dots, x_n)$$

Ukázali jsem, že T' a S jsou ekvivalentní teorie, tedy T' je konzervativní rozšíření T .

35

Cvičení.

Jeli-li T' rozšíření teorie T o definice, pak ke každému modelu M teorie T existuje jednoznačně určená expanze M' modelu M , která je modelem T' .

36

Definice funkčního symbolu termem.

Častým případem definice funkčního symbolu je definice „předpisem“ v podobě termu.

Definující formule D je tvaru $y = t$, kde všechny proměnné termu t jsou mezi $x_1, \dots, x_n$.

V takovém případě jsou podmínky existence a jednoznačnosti snadno dokazatelné jen v predikátové logice.

Existence $\vdash \underbrace{D_y[t]}_{t=t} \rightarrow (\exists y)D$ tedy $\vdash (\exists y)D$.

Jednoznačnost $\vdash y = t \rightarrow t' = t \rightarrow y = t'$ je důsledkem symetrie a tranzitivnosti rovnosti.

37

Přirozené násobky a numerály byly zavedeny pomocí termů. Můžeme se na ně dívat nejen jako na zkratky, ale jako na definované funkční symboly.

Definice.

Říkáme, že T' je rozšířením teorie T o definice jestliže T' vznikne z T konečným počtem rozšíření o definice funkcí a a predikátů.

V takovém případě je T' konzervativním rozšířením T a ke každé formuli A' teorie T' existuje formule A teorie T taková, že

$$T' \vdash A \leftrightarrow A'$$

38

Nerozhodnutelnost, neúplnost

Meze formální metody

1

V následujícím výkladu nebudeme mít k dispozici všechny prostředky nutné k provedení důkazů, pokusíme se je alespoň přiblížit.

Výsledky, které chceme uvést jsou natolik důležité, že patří k základnímu kurzu predikátové logiky, uvedeme je alespoň bez důkazů.

Nejprve uvedeme některé pojmy.

2

(Částečné) *rekursivní funkce* tvoří třídu „efektivně (algoritmicky) vyčíslitelných“ funkcí

$$f : N^k \rightarrow N \quad k \geq 1$$

zobrazující (podmnožiny) množiny uspořádaných k -tic přirozených čísel do množiny přirozených čísel pro nějaké k .

Tato třída má přesnou definici v teorii rekurze.

3

Množina k -tic přirozených čísel je rekursivní, když je rekursivní její charakteristická funkce. Pokud má taková množina nějaký vztah k logice, říkáme také, že taková množina je rozhodnutelná.

Přibližně řečeno, množina A je rekursivní, když umíme algoritmicky rozpoznat její prvky.

Budeme pracovat s jazyky, které mají konečně, nebo spočetně speciálních symbolů, nejčastěji s jazykem aritmetiky. Takové jazyky budeme nazývat *spočetné*.

4

Předpokládejme, že L je spočetný jazyk a že jeho speciální symboly umíme efektivně očíslovat přirozenými čísly.

Používáme slovo 'efektivně' místo 'rekurzivně', protože jsme rekurzivní funkce zavedli na přirozených číslech a ne na symbolech.

Ve většině případů budeme uvažovat jen jazyky s konečně mnoha speciálními symboly.

Dá se ukázat, že v takovém případě lze každé formuli A efektivně přiřadit přirozené číslo $\#A$, její kód.

5

Nerozhodnutelnost predikátové logiky.

Věta (Church)

Necht' L je spočetný jazyk prvního řádu takový, že

- obsahuje alespoň jednu konstantu a alespoň jeden funkční symbol četnosti $k > 0$.
- pro každé přirozené číslo n obsahuje spočetně mnoho predikátových symbolů.

Potom množina

$$\{ \#A \mid A \text{ je uzavřená formule a } L \models A \}$$

není rozhodnutelná.

6

Předchozí věta byla formulována k určitému důkazu, k nerozhodnutelnosti stačí daleko méně speciálních symbolů.

Věta.

Necht' L je jazyk prvního řádu bez rovnosti, který obsahuje alespoň dva binární predikáty,

potom predikátová logika s jazykem L je nerozhodnutelná.

7

Tři axiomatizace aritmetiky

Jazyk $L = \{0, S, +, *, \leq\}$

Robinsonova aritmetika Q .

$$Q1 \quad S(x) \neq 0$$

$$Q6 \quad x * 0 = 0$$

$$Q2 \quad S(x) = S(y) \rightarrow x = y$$

$$Q7 \quad x * S(y) = (x * y) + x$$

$$Q3 \quad x \neq 0 \rightarrow (\exists y)(x = S(y)) \quad Q8 \quad x \leq y \leftrightarrow (\exists z)(z + x = y)$$

$$Q4 \quad x + 0 = x$$

$$Q5 \quad x + S(y) = S(x + y)$$

8

Peanova aritmetika P (prvního řádu)

Má axiomy $Q1, Q2, Q4 - Q8$ a *schema indukce*

Pro každou formuli A a každou proměnnou x je následující formule axiom indukce.

$$A_x[0] \rightarrow \{(\forall x)(A \rightarrow A_x[S(x)]) \rightarrow (\forall x)A\}$$

Dá se ukázat, že v Peanově aritmetice je dokazatelný axiom $Q3$, takže Peanova aritmetika je rozšířením Robinsonovy aritmetiky.

Dá se také dokázat, že axiomatika Peanovy aritmetiky je rekursivní.

9

Úplná aritmetika.

Je-li N standardní model aritmetiky, *Úplná aritmetika* má za axiomy všechny uzavřené formule pravdivé v N .

$$Th(N) = \{ A \mid A \text{ je uzavřená formule } N \models A \}$$

Této teorii se také říká *Pravdivá aritmetika*, protože je axiomatizovaná všemi formulemi, které jsou pravdivé ve standardním modelu N .

Množině formulí $Th(N)$ se říká *teorie modelu N* .

10

Máme tři axiomatizace aritmetiky $Q, P, Th(N)$, všechny v jazyku $L = \{0, S, +, *, \}\}$. Je zřejmé, že

$$Q \subseteq P \subseteq Th(N)$$

kde inkluze znamená rozšíření.

- Q má konečně mnoho axiomů, je tedy rekursivně axiomatizovatelná.
- P má spočetně axiomů. Dá se ukázat, že kódy axiomů schematu indukce tvoří rekursivní množinu, spolu s dalšími konečně mnoha axiomy je P rekursivně axiomatizovatelná.
- $Th(N)$ podle důkazu není rekursivně axiomatizovatelná.

11

Je-li T teorie s jazykem aritmetiky, můžeme definovat množinu kódů vět teorie T

$$Thm(T) = \{ \#A \mid A \text{ je uzavřená formule, } T \models A \}$$

Podle věty o uzávěru stačí se omezit na uzavřené formule.

Definice.

Říkáme, že *teorie T je rozhodnutelná*, je-li množina $Thm(T)$ (kódů) vět rekursivní. Jinak je *teorie nerozhodnutelná*.

12

Věta o nerozhodnutelnosti aritmetiky (Church)

Je-li T bezesporné rozšíření Robinsonovy aritmetiky Q , potom T je nerozhodnutelná teorie.

13

Věta o neúplnosti aritmetiky. (Gödel, Rosser)

Je-li T bezesporné, rekurzivně axiomatizovatelné rozšíření Robinsonovy aritmetiky Q , potom T není úplná teorie.

14

Označení.

Je-li T bezesporné, rekurzivně axiomatizovatelné rozšíření Peanovy aritmetiky P a A formule, píšeme

$\ulcorner A$ jako zkratku za formuli $Thm(T)(\#A)$

$Con(T)$ jako zkratku za formuli $\neg \ulcorner 0=1$

$Con(T)$ čteme T je bezesporná (konzistentní).

15

Druhá věta o neúplnosti.

Necht' T je bezesporné rekurzivně axiomatizovatelné rozšíření Peanovy aritmetiky P , potom

$$T \nmid \vdash Con(T)$$

16

Poznámka.

Předpokládejme, že Peanova aritmetika je bezesporná.
Protože

$$P \nmid \text{Con}(P)$$

podle věty o úplnosti existuje model $M \models P$,
takový, že $M \models \text{Proof}(d, \# 0=1)$, kde d je číslo
důkazu formule $0 = 1$. Takové číslo musí být
nestandardní.

17

Shepherdsonova hříčka aneb kouzlo nestandardních důkazů.

Předpokládejme, že jsme v nějakém nestandardním modelu
 P , kde existuje nestandardní číslo.

Nechť A je libovolná formule, potom posloupnost
 $A \rightarrow (A \rightarrow A), A \rightarrow (A \rightarrow A) \dots; \dots (A \rightarrow A), A, (A \rightarrow A), A, \dots$

vypadá jako důkaz (libovolné) formule A .

Ale není to důkaz, protože takovou posloupnost formulí
nelze kódovat žádným přirozeným číslem daného modelu.

18

Zermelo-Fraenkelova teorie množin ZF

má jazyk prvního řádu s rovností, obsahuje Peanovu
aritmetiku, má rekuzivní množinu axiomů, tedy je-li
ZF bezesporná, pak

$$ZF \nmid \text{Con}(ZF)$$

Můžeme, proto očekávat jen důkazy relativní
bezespornosti

$$\text{Con}(ZF) \rightarrow \text{Con}(ZFC)$$

19