Predikátová logika

Jazyk prvního řádu

Jazyk obsahuje

(i) Proměnné $x, y, z, x_1, x_2, \ldots y', y'', \ldots$ neomezeně mnoho

(ii) Funkční symboly $f, g, h, \ldots, f_1, f_2 \cdots$ každý má svou četnost (počet argumentů) $n \geq 0$.

(iii)Predikátové symboly $p, q, r, \ldots p_1, p_2, \cdots$ 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.

Termy a formule

jsou výrazy jazyka prvního řádu, které mají svůj význam.

Termy popisují (některá) individua.

Formule jsou tvrzeními o individuích.

Definujeme je induktivně.

Definice - Termy

(i) Každá proměnná je term.

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

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

je term.

Termy jsou definovány konečným počtem užití pravidel (i) a (ii). Tedy jsou to konečná slova.

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.

Formule.

(i) Je-li p n-ární predikátový symbol,

potom výraz $p(t_1, t_2, \ldots t_n)$, kde $t_1, t_2, \ldots t_n$ jsou termy, je *(atomická) formule.*

(ii) Jsou-li výrazy A, B formule, potom výrazy

$\neg A, \quad (A \,\&\, B), \quad (A \vee B), \quad (A \rightarrow B), \quad a \quad (A \leftrightarrow B)$

jsou také *formule.*

(iii) Je-li x proměnná a A formule, potom výrazy

$(\forall x)A \quad a \quad (\exists x)A$

jsou *formule.*

Příklady.

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

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

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

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

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

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

vznikla z formulí

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

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

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.

(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 vázan ou 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 .

Příklad.

Proměnná může být v téže formuli současně volná i vázaná.

$$\underset{\wedge}{(\forall x)}((\underset{\wedge}{x} \bullet \underset{\wedge}{e}) = \underset{\wedge}{x}) \rightarrow ((\underset{\#}{e} \bullet \underset{\#}{x}) = x)$$

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

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 $f_M : M^n \to M$ pro n-ární funkční symbol f
- relaci $p_M \subseteq M^n$ pro každý n-ární predikát p

Příklady.

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

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

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

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

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 $t[\mathrm{e}] = e(x)$ je-li t proměnná x

$t[e] = f_M(t_1[e], \ldots t_n[e])$, je-li t tvaru $f(t_1 \ldots t_n)$.

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

$$x_1, x_2, \ldots x_n$$

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 indukcí podle složitosti termu t.

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 $A \equiv p(t_1, \ldots t_n)$, kde p není rovnost. Potom

$$M \models A[e], \quad \textit{jestliže} \quad (t_1[e], \ldots t_n[e]) \in p_M$$

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

c) A je tvaru $\neg B$ *a* $M \not\models B[e]$.

d) A je tvaru $B \to C$ *a* $M \not\models B[e]$ *nebo* $M \models C[e]$.

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

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

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.

• 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.

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

Tedy

$\models A$ *právě když* $M \models A$ *pro každou interpretaci* M

Substituce termů do termů za proměnné

Příklady.

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

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

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

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

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

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

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

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.

Substituce termů do formulí

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

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

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

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

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

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

$$A_{x_1, \ldots, x_n}[t_1, \ldots t_n] \qquad (1)$$

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 formuli říkáme *instance formule A.*

Substituovatelnost termu do formule

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

Varovný příklad.

Mějme formuli

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

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.

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.

Přříklady.

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

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

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

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

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

b) nesubstituovatelné

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

$$A_u[d] \qquad A_u[e]$$

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

Přitom

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

jsou substituovatelné.

Úmluva.

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

Lemma.

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

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

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

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

Formální systém predikátové logiky

Dokazatelnost

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

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

Axiomy pro logické spojky

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

$$A \to (B \to A) \qquad \text{(A1)}$$

$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \qquad \text{(A2)}$$

$$(\neg B \to \neg A) \to (A \to B) \qquad \text{(A3)}$$

je axiom.

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.

Axiomy pro kvantifikátory.

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

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

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

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

je axiom predikátové logiky.

Odvozovací pravidla.

Modus ponens

$$\frac{A \qquad A \to B}{B}$$

Pravidlo generalizace

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

pro libovolnou proměnnou x.

Uvedené axiomy 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.

Základní věty o kvantifikátorech.

Pravidlo zavedení $\forall$.

Nemá-li proměnná x volný výskyt ve formuli A a

$$\vdash A \to B \quad \text{potom} \quad \vdash A \to (\forall x)B$$

Pravidlo substituce, Pravidlo zavedení $\exists$.

(*i*) $\vdash A_x[t] \to (\exists x)A$

(ii) Je-li $\vdash A \to B$ a x není volná v B, potom také $\vdash (\exists x)A \to B$.

V Gentzenově stylu můžeme tato pravidla zapsat

$$\frac{A \to B \quad x \text{ není volná v } A}{A \to (\forall x)B}$$

Pravidlo zavedení $\forall$.

$$\frac{}{A_x[t] \to (\exists x)A}$$

Pravidlo substituce

$$\frac{A \to B \quad x \text{ není volná v } B}{(\exists x)A \to B}$$

Pravidlo zavedení $\exists$.

Důkazy.

Pravidlo zavedení $\forall$.

$\vdash A \to B$	předpoklad
$\vdash \boxed{(\forall x)(A \to B)}$	generalizace
$\vdash \boxed{(\forall x)(A \to B)} \to (A \to (\forall x)B)$	schema přeskoku
$\vdash (A \to (\forall x)B)$	MP

Pravidlo substituce.

$$\vdash (\forall x)\neg A \rightarrow \neg A_x[t]$$ schema specifikace

$$\vdash \neg\underbrace{\neg(\forall x)\neg A}_{(\exists x)A} \rightarrow \neg A_x[t]$$ (v3), zkratka $\exists$

$$\vdash A_x[t] \rightarrow (\exists x)A$$ (A3), MP

Pravidlo zavedení $\exists$.

$$\vdash A \rightarrow B$$ předpoklad

$$\vdash \neg B \rightarrow \neg A$$ (v5), MP

$$\vdash \neg B \rightarrow \underbrace{\neg\neg(\forall x)\neg}_{(\exists x)} A$$ pravidlo $\forall$, (v4)

$$\vdash (\exists x)A \rightarrow B$$ (A3)

Instance formulí.

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

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

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

$(\exists y)(x < y)$ $(\exists y)(1 < y)$

Varovný příklad.

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

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

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

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

Věta o instancích.

Je-li A' instance A, potom platí

$$\vdash A \text{ implikuje } \vdash A'$$

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

Důkaz.

Indukcí podle počtu substituovaných termů.

Nechť $A' \equiv A_{x_1, \ldots, x_n}[t_1, \ldots t_n]$

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

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

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

$\vdash A$ předpoklad

$\vdash A_{x_1}[z_1]$ základ indukce

$\vdash (A_{x_1}[z_1])_{x_2}[z_2] \equiv A_{x_1 x_2}[z_1, z_2]$ iterace

$\vdots$

$\vdash \underbrace{A_{x_1, \ldots, x_n}[z_1, \ldots z_n]}_{B}$ celkem

Nyní

$$\vdash B$$ mezivýsledek

$$\vdash B_{z_1}[t_1]$$ základ indukce

$$\vdash (B_{z_1}[t_1])_{z_2}[t_2] \equiv B_{z_1 z_2}[t_1, t_2]$$ iterace

$$\vdots$$

$$\vdash \underbrace{B_{x_1}, \ldots, {}_{z_n}[t_1, \ldots t_n]}_{A[t_1,\ldots,t_n]}$$ celkem

Tedy $$\vdash A' \equiv A_{x_1}, \ldots, {}_{x_n}[t_1, \ldots t_n]$$

Co nás překvapilo?

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

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

Kdyby $\vdash A$

potom $\vdash A' \equiv 3 = 0$

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

Specifikace a substituce.

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

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

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

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

$$\vdash (\forall x)C \to C \quad (\equiv C_x[x])$$

iterací

$$\vdash (\forall x_n)A \to A$$

$$\vdash (\forall x_{n-1})(\forall x_n)A \to (\forall x_n)A$$

$$\vdots$$

$$\vdash (\forall x_1), \ldots, (\forall x_n)A \to (\forall x_2), \ldots, (\forall x_n)A$$

Složením všech implikací dostaneme

$$\vdash (\forall x_1), \ldots, (\forall x_n)A \to A$$

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

Uzávěr formule

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

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

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.*

Cvičení.

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

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

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

b)

$$\vdash (\forall x)(\forall y)A \leftrightarrow (\forall y)(\forall x)A$$

$$\vdash (\exists x)(\exists y)A \leftrightarrow (\exists y)(\exists x)A$$

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

$$\vdash (\forall x_1)(\forall x_2)\ldots(\forall x_n)A \leftrightarrow (\forall x_{\pi(1)})(\forall x_{\pi(2)})\ldots(\forall x_{\pi(n)})A$$

$$\vdash (\exists x_1)(\exists x_2)\ldots(\exists x_n)A \leftrightarrow (\exists x_{\pi(1)})(\exists x_{\pi(2)})\ldots(\exists x_{\pi(n)})A$$

Věta o uzávěru.

Je-li A' uzávěr formule A, potom platí

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

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.

Lemma o distribuci kvantifikátorů

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

$$\vdash (\forall x)A \to (\forall x)B \quad a \quad \vdash (\exists x)A \to (\exists x)B$$

Důkaz.

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

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

Věta o ekvivalenci.

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

$$\vdash B_1 \leftrightarrow B_1' \ldots \vdash B_n \leftrightarrow B_n'$$

potom

$$\vdash A \leftrightarrow A'$$

Důkaz.

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

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

Potom A' je tvaru

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

Dostáváme

$\vdash B \leftrightarrow B'$ indukční předpoklad

$\vdash B \rightarrow B'$ a $\vdash B' \rightarrow B$ zkratka ekvivalence

$\vdash A \rightarrow A'$ a $\vdash A' \rightarrow A$ distribuce kvantifikatorů

Tedy $\vdash A \leftrightarrow A'$.

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.

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

Příklad.

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

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

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

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

Věta o variantách

Je-li A' variantou formule A, potom

$$\vdash A \leftrightarrow A'$$

Důkaz.

Podle Věty o ekvivalenci stačí dokázat

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

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

a) $\vdash (\forall x)B \rightarrow B_x[y]$ axiom specifikace

$\vdash (\forall x)B \rightarrow (\forall y)B_x[y]$ pravidlo $\forall$

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

$$\vdash (\forall y)C \to C_y[x] \qquad \text{axiom specifikace}$$

$$\vdash (\forall y)C \to (\forall x)C_y[x] \qquad \text{pravidlo } \forall$$

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.

Věta o dedukci

Nechť T je množina formulí, A je uzavřená formule a B je libovolná formule. Potom

$$T \vdash A \to B \quad \text{právě když} \quad T, A \vdash B$$

Důkaz.

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

Při důkazu zprava do leva, mějme důkaz $B_1, \ldots, B_n$ 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.

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

$$T \mid\!- A \to B_j$$

odvodíme

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

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

Tím je důkaz dokončen.

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.

Věta o konstantách

Nechť T je množina formulí jazyka L a A je formule jazyka L. Nechť $x_1, \ldots x_n$ jsou proměnné.

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

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

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

Důkaz.

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

a) je-li $T \vdash_L A$ potom $T \vdash_L A'$, protože A' je instancí A.

b) je-li $T \vdash_{L'} A'$, nechť $A'_1,\ldots,A'_n$ je důkaz A' z T.
Nechť $y_1,\ldots y_n$ jsou nové proměnné, které se nevyskytují v důkazu A' ani v A.

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

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

Snadno se přesvědčíme, že $A_1, \ldots, A_n$ je důkazem formule $A_{x_1}, \ldots, {}_{x_n}[y_1, \ldots y_n]$ 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.

Odtud

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

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

Konstanty a Věta o dedukci.

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

Stačí dokázat

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

a z Věty o dedukci a Věty o konstantách dostaneme

$$T \mid\!- A \to B.$$

Důsledek.

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

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

Důkaz.

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

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 $T \vdash \neg A' \rightarrow A'$ a podle věty (v7) výrokové logiky $T \vdash A'$.

Cvičení.

a) Jestliže formule A neobsahuje proměnnou x volně, potom

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

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

$\vdash (\forall x) A \leftrightarrow (\exists x) A$

b)

$\vdash (Qx)(Qy) A \leftrightarrow (Qy)(Qx) A$

c)

$\vdash (\exists x)(\forall y) A \rightarrow (\forall y)(\exists x) A$

d)

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

$$|- (\exists x) \neg A \vee (\forall x)(\neg A \vee B)$$

$$|- (\exists x) \neg A \vee \neg (\exists x)(A \wedge \neg B)$$

e)

$$|- (\forall x)(A \,\&\, B) \leftrightarrow ((\forall x)(A) \,\&\, (\forall x)(B))$$

$$|- ((\forall x)(A) \vee (\forall x)(B)) \rightarrow (\forall x)(A \vee B)$$

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

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

f)

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

Prenexní tvary formulí. Rovnost.

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.

Prenexní tvar formule.

Formule A *je v prenexním tvaru*, jeli

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

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.*

Příklady.

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

$b)\quad (\forall x)((x \mid p \rightarrow x = 1) \rightarrow p \ je \ prvočíslo)$

$c)\quad (\exists \mathsf{F})(\forall x)(\forall y)((x \cup y) \in \mathsf{F} \leftrightarrow (x \in \mathsf{F} \vee y \in \mathsf{F}))$

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

$\rightarrow (F \circ G : C \rightarrow E))]$

Věta o prenexních tvarech

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

Značení.

Je-li Q kvantifikátor, potom značíme

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

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.

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

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

$c)\quad \vdash (B \to (Qx)C) \leftrightarrow (Qx)(B \to C)$, *pokud* x *není vo*ln*á v* B.

$d)\quad \vdash ((Qx)B \to C) \leftrightarrow (\overline{Q}x)(B \to C)$, *pokud* x *není vo*ln*á v* C.

$e)\quad \vdash ((Qx)B \lozenge C) \leftrightarrow (Qx)(B \lozenge C)$, *pokud* x *není vo*ln*á v* C.

Symbol $\lozenge$ zastupuje konjunkci nebo disjunkci.

Důkaz.

b) Je-li $Q \equiv \forall$ dostáváme

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

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

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

$$\vdash (\forall x)(B \to C) \to (B \to (\forall x)C)$$

je axiom. Abychom dokázali obrácenou implikaci užijeme

$$\vdash (B \to (\forall x)C) \to [\underbrace{((\forall x)C \to C)}_{\textit{axiom specifikace}} \to (B \to C)]$$

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

$$\vdash (\forall x)(B \to C) \to (B \to (\forall x)C)$$

je axiom. Abychom dokázali obrácenou implikaci užijeme

$$\vdash (B \to (\forall x)C) \to [\underbrace{((\forall x)C \to C)}_{\textit{axiom specifikace}} \to (B \to C)]$$

$$\vdash (B \to (\forall x)C) \to (B \to C)] \qquad \text{MP}$$

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

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

$$\vdash (B \to (\exists x)C) \leftrightarrow (\neg B \vee (\exists x)C) \qquad (1)$$

Máme tedy dokázat

$$\vdash (\neg B \vee (\exists x)C) \to (\exists x)(B \to C) \qquad (2)$$

Podle věty o důkazu rozborem případů máme dokázat

$$\vdash (\exists x)C \to (\exists x)(B \to C) \qquad (3)$$

a

$$\vdash \neg B \to (\exists x)(B \to C) \qquad (4)$$

Důkaz (3).

$\vdash C \to (B \to C)$ axiom (A1)

$\vdash (\exists x) C \to (\exists x)(B \to C)$ distribuce kvantifikátorů

Důkaz (4).

$\vdash \boxed{(B \to C)} \to (\exists x)(B \to C)$ substituční lemma

$\vdash \neg B \to \boxed{(B \to C)}$ (v2)

$\vdash \neg B \to (\exists x)(B \to C)$ složení implikací, MP

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

$\vdash \boxed{C \to \exists x\, C}$ substituční lemma

$\vdash (B \to C) \to [\boxed{(C \to \exists x\, C)} \to (B \to (\exists x) C)]$

skládání implikací

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

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

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

Při důkazu tvrzení c) pro existenční kvantifikátor, byla použita věta o důkazu rozborem 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

$$B \quad a \quad (\exists x)C$$

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

d) $Q \equiv \forall$

$$\begin{aligned}
&\vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to \neg(\forall x)B) && \text{tautologie}\\
&\leftrightarrow (\neg C \to \neg(\forall x)\neg\neg B) && \text{ekvivalence}\\
&\leftrightarrow (\neg C \to (\exists x)\neg B) && \text{operace b)}\\
&\leftrightarrow (\exists x)(\neg C \to \neg B) && \text{operace c)}\\
&\leftrightarrow (\exists x)(B \to C) && \text{tautologie}
\end{aligned}$$

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

e) důkaz prenexní operace pro konjunkci a disjunkci se převede na předchozí operace a) - d) rozepsáním zkratek.

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 $B \to C$ 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

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

a A' se sestrojí pomocí c) a d).

Příklady.

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

a) Prenexní operace pro ekvivalenci

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

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

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

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

b) Prenexní tvar v aritmetice.

$$(\exists x)(x = y) \to (\exists x)(x = 0 \vee \neg(\exists y)(y < 0)) \qquad \text{(o)}$$

$$(\exists x)(x = y) \to (\exists u)(u = 0 \vee \neg(\exists v)(v < 0)) \qquad \text{(a)}$$

$$(\exists x)(x = y) \to (\exists u)(u = 0 \vee (\forall v)\neg(v < 0)) \qquad \text{(b)}$$

$$(\exists x)(x = y) \to (\exists u)(\forall v)(u = 0 \vee \neg(v < 0)) \qquad \text{(e)}$$

$$(\forall x)(\exists u)(\forall v)[(x = y) \to (u = 0 \vee \neg(v < 0))] \qquad \text{(c), (d)}$$

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

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

Predikátová logika s rovností.

Schema axiomů identity.

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

$$x = x \qquad \text{(R1)}$$

{Leibnitzův axiom}

Schema axiomů rovnosti pro funkce.

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

$$x_1 = y_1 \rightarrow \ldots x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \qquad \text{(R2)}$$

Schema axiomů rovnosti pro predikáty.

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

$$x_1 = y_1 \rightarrow \ldots x_n = y_n \rightarrow p(x_1, \ldots, x_n) \rightarrow p(y_1, \ldots, y_n) \qquad \text{(R3)}$$

Elementární vlastnosti rovnosti.

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

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

$$\vdash x = y \to y = x \qquad (1)$$

pro libovolné proměnné x, y.

$$\vdash x = y \to \boxed{x = x} \to \boxed{x = x} \to y = x \qquad (2)$$

$$\vdash x_1 = y_1 \to x_2 = y_2 \to x_1 = x_2 \to y_1 = y_2 \quad (R3)$$

$$\vdash x = y \to y = x \qquad (2),(R1),MP$$

Tím je dokázáno (1).

Tranzitivnost

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

$$\vdash y = x \rightarrow z = z \rightarrow y = z \rightarrow x = z \qquad (R3)$$

Pro kontrolu

$$\vdash x_1 = y_1 \rightarrow x_2 = y_2 \rightarrow x_1 = x_2 \rightarrow y_1 = y_2 \qquad (R3)$$

$$\vdash y = x \rightarrow y = z \rightarrow x = z \qquad (R1),(R3), MP$$

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

Základní věta o rovnosti.

Nechť T je množina formulí a $t_1, \ldots, t_n, \quad s_1, \ldots, s_n$ jsou termy pro, které platí

$$T \mid\!- t_1 = s_1, \ldots, \mid\!- t_n = s_n \qquad (5)$$

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

$$T \mid\!- t = s \qquad (6)$$

(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

$$T \mid\!- A' = A \qquad (7)$$

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 $f(r_1, \ldots, r_k)$ a term s tvaru $f(r'_1, \ldots, r'_k)$ z indukčního předpokladu dostáváme

$$T \mid\!- r_1 = r'_1, \ldots, \mid\!- r_n = r'_n \qquad (8)$$

$$\mid\!- r_1 = r'_1 \rightarrow \ldots r_k = r'_k \rightarrow \underbrace{f(x_1, \ldots, x_k)}_{t} = \underbrace{f(r'_1, \ldots, r'_k)}_{s} \quad \text{(R2)}$$

odkud tvrzení (i) odvodíme pravidlem modus ponens.

Tvrzení (ii) se dokazuje obdobně.

Důsledek.

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

(i) $\vdash t_1 = s_1 \to \ldots t_n = s_n \to t[t_1, \ldots, t_n] = t[s_1, \ldots, s_n]$

(ii) $\vdash t_1 = s_1 \to \ldots t_n = s_n \to (A[t_1, \ldots, t_n] \leftrightarrow A[s_1, \ldots, s_n])$

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

(iii) $\vdash A_x[t] \leftrightarrow (\forall x)(x = t \to A)$

(iv) $\vdash A_x[t] \leftrightarrow (\exists x)(x = t \,\&\, A)$

Pravdivost a dokazatelnost

Vztah formálního systému a sémantiky predikátové logiky

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.

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.

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.

(c) Teorie okruhů, oborů integrity a těles. Nechť

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

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

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

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

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

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

a pro násobení

$$1 * x = x \qquad x * 1 = x \tag{o5}$$

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

$$x * y = y * x \tag{o7}$$

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

přidáme-li axiom

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

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

$$0 \neq 1 \tag{t1}$$

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

dostaneme *Teorii těles.*

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

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

Elementární aritmetika má tyto speciální axiomy

$$S(x) \neq 0$$

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

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

$$x + 0 = x$$

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

$$x * 0 = 0$$

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

Interpretace N , jejíž doménou jsou přirozená čísla,

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

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

$$x +_{\mathrm{N}} y = x + y = (x \oplus y) \qquad \textit{ordinální součet}$$

$$x *_{\mathrm{N}} y = x * y = (x \otimes y) \qquad \textit{ordinální součin}$$

Se nazývá *standardní model aritmetiky.*

Věta o korektnosti.

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

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

Speciálně

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

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

Lemma.

Axiomy predikátové logiky jsou validní formule.

Důkaz. Nechť L je jazyk predikátové logiky a A jeho formule. Nechť 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 $p_1, \ldots, p_n$ všechny výrokové proměnné fomule A' a $A_1, \ldots, A_n$ jsou formule, které v A vystupují na jejich místě, pak $M \models A[e]$ nezávisle na pravdivosti $M \models A_i[e]$ $i, 1 \leq i \leq n$.

(b1) A je případ axiomu specifikace tvaru $(\forall x)B \to B_x[t]$.
Je-li $M \not\models (\forall x)B[e]$, 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 přeskoku tvaru

$$(\forall x)(B \to C) \to (B \to (\forall x)C) \qquad (1)$$

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.

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

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

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 $e(x/\mathrm{m})$ 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 $M \models (B \to (\forall x)C)[e]$.

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

(c) Nechť A je axiom rovnosti pro funkce

$$x_1 = y_1 \rightarrow \ldots x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \qquad (2)$$

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

$$e(x_1) = e(y_1) \ldots e(x_n) = e(y_n) \qquad (3)$$

Potom

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

$$\Leftrightarrow f_M(e(x_1), \cdots e(x_n)) = f_M(e(y_1), \cdots e(y_n))$$

a z (3) plyne

$$M \models A[e]$$

Validnost axiomu rovnosti pro predikáty se dokazuje podobně.

Důkaz věty o korektnosti.

Předpokládejme, že $T \mid\!- A$ a že $A_1, \ldots, A_n \equiv A$ je důkaz A v teorii T. Nechť 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

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

Rozebereme několik případů

(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 $M \models A_i$.

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

nechť e je li bovolné ohodnocení. Z i ndukčního před pokladu plyne $M \models A_j$, tedy také $M \models A_j[e]$. Speciálně

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

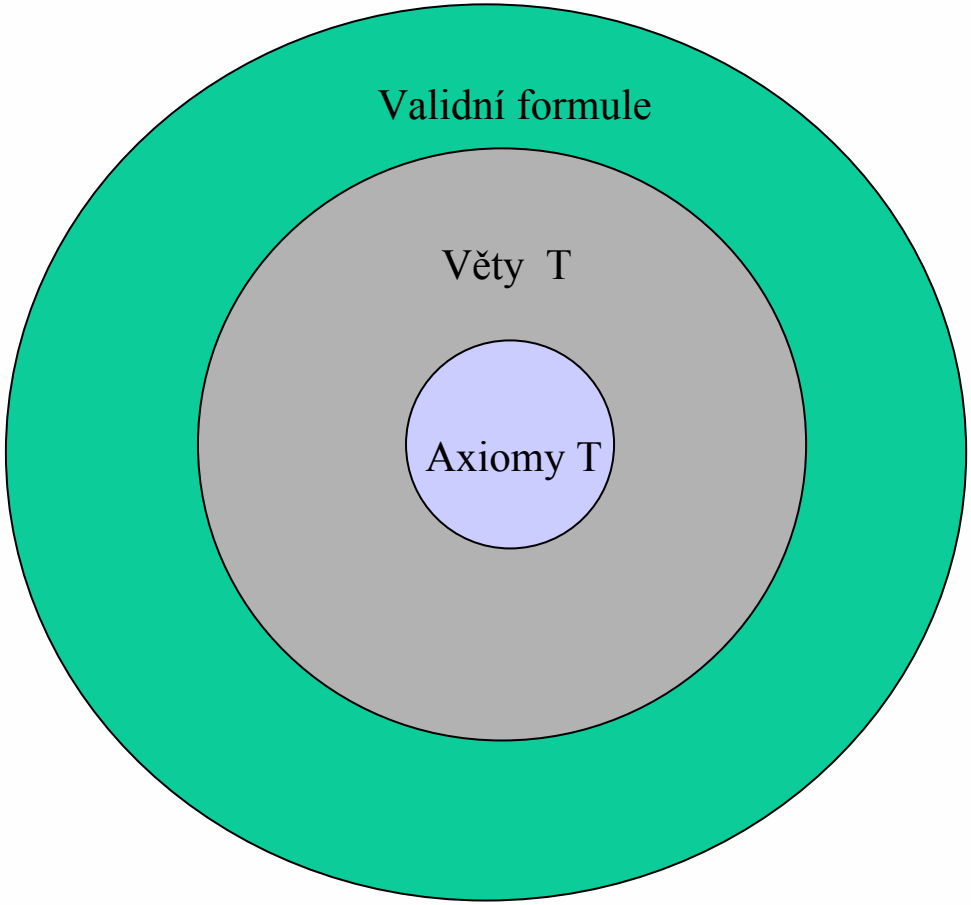
odkud

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

protože e bylo libovolné ohodnocení, dostáváme

$$M \models A_i.$$

Tím je věta o korektnosti dokázána.


Validní formule
Věty T
Axiomy T

Věta o úplnosti.

Věta o úplnosti. (Gödel 1930)

Nechť T je teorie s jazykem L.

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

$$T \vdash A \quad \textit{právě když} \quad T \models A$$

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

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).

Lemma.

Ve Větě o úplnosti druhé tvrzení implikuje první.

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

Víme

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

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

Tím je tvrzení (i) dokázáno.

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 sestrojit 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.

Kanonická struktura M .

- Universum M = {t | t je term bez proměnných}
- Funkční symboly (nepotřebujeme ohodnocení proměnných). Je-li $t_1, \ldots, t_n \in \mathrm{M}$ a f je n-ární funkční symbol, jeho realizaci f_M definujeme následovně

$$f_M(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) \in \mathrm{M}$$

- Predikátové symboly. Je-li p n-ární predikátový symbol, jeho interpretace p_M se definuje takto

$$(t_1, \ldots, t_n) \in p_M \quad \textit{právě když} \quad T \mid\!- p(t_1, \ldots, t_n)$$

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 $A \equiv p(t_1, \ldots, t_n)$ bez proměnných (a každé ohodnocení e) platí

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

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

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

$$M \not\models \underbrace{S(0)+S(0)}_{t} = \underbrace{S(S(0))}_{s} \quad \textit{protože} \quad t \not\equiv s$$

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

Zde pomůže 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

$$t \approx s \quad \textit{právě když} \quad T \mid\!- t = s$$

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

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

Platí

$$[t] = [s] \quad \textit{právě když} \quad T \mid\!- t = s$$

Tedy

$$M \models t = s \quad \Leftrightarrow \quad [t] = [s]$$
$$\Leftrightarrow \quad T \vdash t = s$$

definujeme-li pro funkční symboly f

$$f_M([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)] \qquad (2)$$

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

$$([t_1], \ldots, [t_n]) \in p_M \quad \textit{právě když} \quad T \vdash p(t_1, \ldots, t_n) \qquad (3)$$

dostáváme následující tvrzení.

Lemma.

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

$$M \models A \quad \Leftrightarrow \quad T \vdash A \tag{4}$$

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 $s_1 \in [t_1], \ldots, s_n \in [t_n]$ pro libovolné $i, 1 \le i \le n$ (5) platí

$$\begin{aligned} s_i \in [t_i] &\Leftrightarrow s_i \approx t_i \\ &\Leftrightarrow T \mid\!- s_i = t_i \end{aligned} \qquad (6)$$

z (5) a (6) dostáváme

$$T \mid\!- s_i = t_i \quad \text{pro} \quad i, 1 \le i \le n \tag{7}$$

vezměme axiom rovnosti pro f.

$$s_1 = t_1 \to \ldots \to s_n = t_n \to f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)$$

Potom

$$T \mid\!- f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \qquad \text{MP, (7)}$$

Tedy

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

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

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

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

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.

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

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

Věta o kanonickém modelu.

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

Důkaz.

Pro každou uzavřenou formuli A ukážeme

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

a) pro uzavřené atomické formule jsme to již dokázali.

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

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

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

$M \models A \quad \Leftrightarrow \quad M \not\models B$ *nebo* $M \models C$

$\Leftrightarrow \quad T \not\vdash B$ *nebo* $T \vdash C$ indukční předpoklad

$\Leftrightarrow \quad T \vdash \neg B$ *nebo* $T \vdash C$ úplnost T

$\Leftrightarrow \quad T \vdash A$ {cvičení}

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

$$M \models A \quad \Leftrightarrow \quad M \models B(x/[t]) \qquad \text{pro nějaký term } t \text{ bez proměnných}$$

$$\Leftrightarrow \quad M \models B_x[t] \qquad \text{pro nějaký term } t \text{ bez proměnných}$$

$$\Leftrightarrow \quad T \vdash B_x[t] \qquad \text{pro nějaký term } t \text{ bez proměnných}$$

$$\Leftrightarrow \quad T \vdash A$$

Rozeberme ještě podrobněji poslední ekvivalenci.

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

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

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

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.

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 sestrojíme model libovolné bezesporné teorie.

Jak rozšířit teorii: dva způsoby

- Nechť L a L' jsou jazyky, nechť 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

$$T' \vdash A \quad \Rightarrow \quad T \vdash A.$$

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'.

Věta. (Henkin)

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

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

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

a do teorie T_0 axiom

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

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

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 formulemi 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.

Postupně vytvoříme posloupnost rozšíření jazyků

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

a teorií

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

Položíme-li

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

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.

Nechť A je formule jazyka L, která je větou T_H.

Nechť

$$B_1, B_2, \ldots, B_n \tag{8}$$

jsou všechny Henkinovy axiomy z důkazu A. Potom

$$T, B_1, B_2, \ldots, B_n \mid\!- A$$

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

$$T \mid\!- B_1 \to B_2 \to \quad \ldots \quad \to B_n \to A \tag{9}$$

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

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

$$B_2, \ldots, B_n$$

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 $B_2, \ldots, B_n$ a tím méně v teorii T. Můžeme použít větu o konstantách a nahradíme uvedenou Henkinovu konstantu novou proměnnou w.

Z (9) dostaneme

$$T \mid\!- ((\exists x)D \to D_x[w]) \to \underbrace{(B_2 \to \ldots \to (B_n \to A)\ldots)}_{\text{neobsahuje } w}$$

pravidlem zavedení $\exists$

$$T \mid\!- (\exists w)((\underbrace{\exists x)D}_{\text{není } w} \to D_x[w]) \to (B_2 \to \ldots \to (B_n \to A)\ldots)$$

prenexní operací

$$T \mid\!- ((\exists x)D \to (\exists w)D_x[w]) \to (B_2 \to \ldots \to (B_n \to A)\ldots)$$

z Věty o variantách plyne

$$\mid\!- ((\exists x)D \to (\exists w)D_x[w]))$$

$$T \mid\!- B_2 \to \ldots \to B_n \to A \qquad \text{MP}$$

$$\vdots$$

$$T \mid\!- A$$

dostaneme opakováním stejného postupu

Věta (Lindenbaum)

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

Důkaz.

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

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

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

Uspořádejme všechny uzavřené formule jazyka L do posloupnosti

$$A_0, A_1, A_2, \ldots, A_n, \ldots$$

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

Vytvoříme neklesající posloupnost teorií se stejným jazykem

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

následujícím postupem.

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 $T_\alpha = \bigcup_{\beta<\alpha} T_\beta$.

Nechť 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.

Ukážeme, že T_U je úplná teorie. Postupujeme sporem. Nechť T_U není úplná a existuje uzavřená formule A taková, že

$$T_U \nvdash A \quad a \quad T_U \nvdash \neg A$$

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.

Redukce a expanze struktur

Definice. Je-li L' rozšíření jazyka L, potom

(i) je-li M' je 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.

Lemma.

Nechť T' je rozšíření teorie T, která má jazyk L. Je-li M' model teorie T' potom redukt $M = M' | L$ je model teorie T.

Důkaz lemmatu.

M je redukt 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.

(ii) je-li A formule jazyka L, potom se indukcí podle složitosti formule A dokáže pro každé ohodnocení e

$$M \models A[e] \quad \Leftrightarrow \quad M' \models A[e]$$

tedy také

$$M \models A \quad \Leftrightarrow \quad M' \models A$$

(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.

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 $M = M' | L$ je model teorie T.

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.}

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.

Důsledek.

Je-li T teorie s jazykem L, A je libovolná formule jazyka L, potom

$$T \models A \quad \Leftrightarrow \quad T' \models A$$

pro nějaký konečný fragment $T' \subseteq T$.

Důkaz.

Podle věty o úplnosti

$$T \models A \quad \Leftrightarrow \quad T \vdash A$$

a důkaz formule A používá jen konečně mnoho axiomů teorie T.

Dva příklady.

a) Je nutné v logice prvního řádu popisovat teorii těles charakteristiky 0 nekonečným počtem axiomů?

Nechť T je teorie těles s jazykem $L = \{0, 1, +, \bullet\}$ s rovností. Je-li x proměnná, termy

$$x,\ (x+x),\ (x+(x+x)),\ \ldots,\ \underbrace{(x+(x+(x+\ldots(x+x)\ldots)))}_{n \text{ krát } x},\ \ldots$$

budeme označovat zkratkami

$$1 * x,\ 2 * x,\ 3 * x \ldots n * x, \ldots$$

a budeme jim říkat *přirozené násobky x.*

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

$$p * 1 = 0 \qquad (1)$$

pro nějaké nenulové p říkáme, že těleso má konečnou charakteristiku a nejmenší nenulové p, pro které platí (1) nazveme charakteristikou tělesa.

Pokud pro žádné nenulové p neplatí (1), říkáme, že těleso má charakteristiku 0.

Přidáme-li k teorii těles axiomy

$$p * 1 \neq 0 \qquad (2)$$

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.

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 kompaktnosti existuje konečný fragment T'' teorie T' takový, že $T'' \models A$.

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.

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.

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.*

$$A_x[0] \rightarrow ((\forall x)(A \rightarrow A_x[S(x)]) \rightarrow (\forall x)A) \qquad (3)$$

Snadno se ověří, že standardní model (elementární) aritmetiky je také modelem Peanovy aritmetiky prvního řádu.

Peanova aritmetika druhého řádu (náznak)

$x, y, z, \ldots$	proměnné pro čísla
$X, Y, Z, \ldots$	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.

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.

$$\overline{0} = 0$$

$$\overline{1} = S(0)$$

$$\vdots$$

$$\overline{n+1} = \underbrace{S(S(S(\ldots S(0)\ldots))}_{n+1 \text{ krát}}$$

Tyto termy se nazývají *numerály*. Každé individuum standardního modelu je interpretací nějakého numerálu.

K jazyku Peanovy aritmetiky přidáme novou konstantu c a axiomy

$$\begin{aligned} &\bar{0} \neq c \\ &\bar{1} \neq c \\ &\vdots \\ &\overline{n+1} \neq c \\ &\vdots \end{aligned} \qquad (4)$$

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.

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.

Cvičení.

a) Ukažte, že žádná teorie prvního řádu T necharakterizuje třídu všech konečných interpretací svého jazyka. To znamená, že pro žádnou teorii T neplatí

$$M \models T \quad \Leftrightarrow \quad M \text{ je konečná struktura pro } T$$

[Návod. Sporem. Předpokládejte, že T má uvedenou vlastnost.

Rozšiřte jazyk o spočetně mnoho konstant

$$c_0, c_1, c_2, \ldots, c_n, \ldots \qquad n \geq 0$$

a přidejte množinu S axiomů tvaru $c_i \neq c_j$ *pro* $i \neq j$.

Nechť $T' = T \cup S.$ 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

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.

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.

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.

(ii) Nechť T' je rozšířením T a A je formule jazyka L, která je větou teorie T'.

Nechť 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

$$M = M' \mid L \models A$$

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.

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.

Věta o definici predikátu.

Nechť T je teorie s jazykem L, nechť $x_1, \ldots, x_n$ jsou proměnné.

Nechť D je formule jazyka L, taková, že všechny její volné proměnné jsou mezi $x_1, \ldots, x_n$.

Nechť jazyk L' vznikne z L přidáním nového n-árního predikátového symbolu p a nechť rozšíření T' teorie T vznikne přidáním axiomu

$$p(x_1, \ldots, x_n) \leftrightarrow D \qquad (1)$$

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

$$T' \vdash B \leftrightarrow B'$$

Důkaz.

Nejprve ukážeme, že definovaný symbol lze eliminovat.

Nechť 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 $$p(t_1, \ldots, t_n)$$

$$D'_{x_1 x_2 \ldots x_n}[t_1, t_2, \ldots t_n]$$

potom $$T' \vdash p(t_1, t_2, \ldots t_n) \leftrightarrow D'_{x_1 x_2 \ldots x_n}[t_1, t_2, \ldots t_n] \qquad (2)$$

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

$$T' \vdash B \leftrightarrow B'$$

Tím je možnost eliminace dokázána.

K důkazu konzervativnosti T' stačí pro libovolnou formuli B' jazyka L' ukázat

$$T' \vdash B' \quad \Rightarrow \quad T \vdash B \tag{3}$$

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

$$T' \vdash B \quad \Rightarrow \quad T \vdash B$$

Tím bude konzervativnost dokázána.

Nechť $B'_1, \ldots, B'_m$ je důkaz B' z T'. Nechť 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

$$x_1 = y_1 \to \ldots \to x_n = y_n \to p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n)$$

potom B_i je tvaru

$$x_1 = y_1 \to \ldots \to x_n = y_n \to D'[x_1, \ldots, x_n] \to D'[y_1, \ldots, y_n]$$

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 „nechť p je nějaké prvočíslo $p > x$“, *zavádíme funkci* $f(x)$, formulí, která určí množinu možných hodnot a $f(x)$ vyberere jednu z nich, ale nám nezáleží na tom, kterou.

b) Řekneme-li „nechť 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.

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.

Věta o zavedení funkčního symbolu.

Nechť T je teorie s jazykem L, nechť formule

$$(\exists y)A \tag{4}$$

jazyka L má všechny volné proměnné mezi $x_1, \ldots, x_n$.

Nechť T' vznikne z T rozšířením jazyka o nový funkční n-ární symbol f a přidáním axiomu

$$A_y[f(x_1, \ldots, x_n)] \tag{5}$$

Potom T' je konzervativním rozšířením teorie T.

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.

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

$$e(x_1) = m_1, \ldots, e(x_n) = m_n$$

Podle definice splňování existuje alespoň jedno individuum m takové, že $M \models A[e(y/m)]$. přitom m závisí na individuích $m_1, \ldots, m_n$. množinu všech takových m označme

$$F(m_1, \ldots, m_n) = \{m \mid M \models A[e(y/m)]\}$$

je to neprázdná množina individuí a protože uspořádání $<$ je dobré, má tato množina nejmenší prvek

$$\min(F(m_1, \ldots, m_n))$$

Nyní můžeme definovat interpretaci $f_{M'}$ nového funkčního symbolu f předpisem

$$f_{M'}(m_1, \ldots, m_n) = (\min(F(m_1, \ldots, m_n))$$

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.

Aplikace: Skolemova věta.

Říkáme, že T je *otevřená teorie,* jestliže všechny axiomy z T jsou otevřené formule.

Věta (Skolem)

K libovolné teorii T lze sestrojit otevřenou teorii T', která je konzervativním rozšířením T.

Idea důkazu.

Věta o zavedení funkčního symbolu ukazuje, že pomocí zavedených funkčních symbolů lze elimino-vat 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 $T \equiv S$.

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.

Skolemova varianta formule.

Je-li A uzavřená formule v prenexním tvaru, indukcí podle počtu existenčních kvantifikátorů sestrojíme uzavřenou univerzální formuli A_S takovou, že $\vdash A_S \to A$.

(i) je-li A univerzální, A_S je A.

(ii) je-li A tvaru

$$(\forall x_1) \ldots (\forall x_n)(\exists y)B \qquad\qquad n \geq 0$$

nechť f je nový n-ární funkční symbol, definujeme formuli A°

$$(\forall x_1) \ldots (\forall x_n)B_y[f(x_1, \ldots, x_n)]$$

Pokud formule A° není otevřená, stejným postupem sestrojíme formuli $A^{\circ\circ}$ ... 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

$$\vdash A^\circ \to A \quad \textit{a tedy} \quad \vdash A_S \to A \tag{7}$$

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.

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.

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.

Věta o definici funkčního symbolu.

Nechť L je jazyk, $x_1, \ldots, x_n, y$ různé proměnné. Nechť T je teorie s jazykem L a D formule jazyka L s volnými proměnnými mezi $x_1, \ldots, x_n, y$.

Nechť platí

$$T \vdash (\exists y) D \tag{8}$$

$$T \vdash D \rightarrow (D_y[t] \rightarrow y = t) \tag{9}$$

Nechť T' vznikne z T přidáním nového n-árního funkčního symbolu f a definujícího axiomu

$$y = f(x_1, \ldots, x_n) \leftrightarrow D \tag{10}$$

Potom T' je konzervativní rozšíření teorie T a definovaný symbol lze eliminovat. To znamená, že ke každé formuli A' jazyka teorie T' lze sestrojit formuli A jazyka L, takovou, že

$$T' \vdash A \leftrightarrow A' \tag{11}$$

Důkaz je rozdělen do dvou kroků

- Nejprve dokážeme eliminovatelnost symbolu f
- potom konzervativnost rozšíření T'

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

$$f(t_1, \ldots, t_n)$$

kde $t_1, \ldots, t_n$ již neobsahují f.

Potom A' je tvaru

$$B'_z[f(t_1, \ldots, t_n)]$$

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 sestrojit formuli B jazyka L (tedy bez symbolu f) takovou, že

$$T' \vdash B \leftrightarrow B' \qquad (11')$$

Pro definici formule A nechť D' je varianta definující formule D, která neváže žádnou proměnnou formule A'.

Nyní můžeme A definovat takto

$$A \equiv (\exists z)(D'_{x_1 x_2 \ldots x_n y}[t_1, \ldots, t_n, z] \,\&\, B)$$

Potom A je formule teorie T a ukážeme, že platí ekvivalence (11).

Z definujícího axiomu a věty o variantách dostáváme

$$T' \vdash z = f(t_1, \ldots, t_n) \leftrightarrow D'_{x_1 x_2 \ldots x_n y}[t_1, \ldots, t_n, z]$$

a z (11′) a věty o ekvivalenci dostaneme

$$T' \vdash (\exists z)(z = f(t_1, \ldots, t_n) \,\&\, B') \leftrightarrow A$$

odkud pomocí vět o rovnosti

$$T' \vdash \underbrace{B'_z[f(t_1, \ldots, t_n)]}_{A'} \leftrightarrow A$$

Tím je (11) dokázáno.

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

$$D_y[f(x_1, \ldots, x_n)] \qquad (12)$$

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.

a) (12) je větou T'. Vezměme instanci definujícího axiomu (10) a dostáváme

$$T' \vdash f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \leftrightarrow D_y[f(x_1, \ldots, x_n)]$$

Použitím axiomu identity a pravidla MP, potom

$$T' \vdash \underbrace{D_y[f(x_1, \ldots, x_n)]}_{(12)}$$

b) (10) je větou S. Vyjdeme z této věty o rovnosti

$$\vdash y = f(x_1, \ldots, x_n) \rightarrow (D \leftrightarrow D_y[f(x_1, \ldots, x_n)])$$

odkud prostředky výrokové logiky

$$\vdash D_y[f(x_1, \ldots, x_n)] \rightarrow (y = f(x_1, \ldots, x_n) \rightarrow D)$$

Z axiomu (12) a MP pak

$$S \mid\!- y = f(x_1, \ldots, x_n) \rightarrow D$$

Opačnou implikaci odvodíme z axiomu jednoznačnosti (9). Uvědomme si, že S je rozšířením T.

Záměnou prvních dvou členů implikace odvodíme

$$S \mid\!- D_y[f(x_1, \ldots, x_n)] \rightarrow (D \rightarrow y = f(x_1, \ldots, x_n))$$

Z axiomu (12) a MP pak

$$S \mid\!- D \rightarrow y = f(x_1, \ldots, x_n)$$

Ukázali jsem, že T' a S jsou ekvivalentní teorie, tedy T' je konzervativní rozšíření T.

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'.

Definice funkčního symbolu termem.

Častým případemdefinice funkčního symbolu je definice „předpisem“ v podobě termu.

Definující formule D je tvaru $y = t$, kde všechny proměnné termu t jsou mezi $x_1, \ldots, x_n$.

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.

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 tako vá, že

$$T' \vdash A \leftrightarrow A'$$

Nerozhodnutelnost, neúplnost

Meze formální metody

V následujícím výkladu nebudeme mít k disposici 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.

(*Částečné*) *rekursivní funkce* tvoří třídu „efektivně (algoritmicky) vyčíslitelných“ funkcí

$$f : N^k \to N \quad k \geq 1$$

zobrazující (podmnožiny) množiny uspořádaných k-tic přirozených čísel do množiny přirozených čísel pro nějaké k.

Tato třída má přesnou definici v teorii rekurze.

Množina k-tic přirozených čísel je rekurzivní, když je rekurzivní její charakteristická funkce. Pokud má taková množina nějaký vztah k logice, říkáme také, že taková množina je rozhodnutelná.

Přibližně řečeno, množina A je rekurzivní, 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*.

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.

Nerozhodnutelnost predikátové logiky.

Věta (Church)

Nechť 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.

Předchozí věta byla formulována k určitému důkazu, k nerozhodnutelnosti stačí daleko méně speciálních symbolů.

Věta.

Nechť L je jazyk prvního řádu bez rovnosti, který obsahuje alespoň dva binární predikáty,

potom predikátová logika s jazykem L je nerozhodnutelná.

Tři axiomatizace aritmetiky

Jazyk $L = \{0, S, +, *, \}$

Robinsonova aritmetika Q.

$Q1$ $S(x) \neq 0$

$Q2$ $S(x) = S(y) \rightarrow x = y$

$Q3$ $x \neq 0 \rightarrow (\exists y)(x = S(y))$

$Q4$ $x + 0 = x$

$Q5$ $x + S(y) = S(x + y)$

$Q6$ $x * 0 = 0$

$Q7$ $x * S(y) = (x * y) + x$

$Q8$ $x \leq y \leftrightarrow (\exists z)(z + x = y)$

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.

Úplná aritmetika.

Je-li N standardní model aritmetiky, *Úplná aritmetika* má za axiomy všechny uzavřené formule pravdivé v N.

$$Th(N) = \{ A \mid A \text{ je uzavřená formule} \quad N \models A \}$$

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.

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 rekurzivní množinu, spolu s dalšími konečně mnoha axiomy je P rekurzivně axiomatizovatelná.

- $Th(N)$ podle důkazu není rekurzivně axiomatizovatelná.

Je-li T teorie s jazykem aritmetiky, můžeme definovat množinu kódů vět teorie T

$$Thm\,(T) = \{\, \#A \mid A \text{ je uzavřená formule, } T \vdash A \,\}$$

Podle věty o uzávěru stačí se omezit na uzavřené formule.

Definice.

Říkáme, že *teorie T je rozhodnutelná*, je-li množina $Thm(T)$ (kódů) vět rekurzivní. Jinak je *teorie nerozhodnutelná*.

Věta o nerozhodnutelnosti aritmetiky (Church)

Je-li T bezesporné rozšíření Robinsonovy aritmetiky Q, potom T je nerozhodnutelná teorie.

Věta o neúplnosti aritmetiky. (Gödel, Rosser)

Je-li T bezesporné, rekurzivně axiomatizovatelné rozšíření Robinsonovy aritmetiky Q, potom T není úplná teorie.

Označení.

Je-li T bezesporné, rekurzivně axiomatizovatelné rozšíření Peanovy aritmetiky P a A formule, píšeme

$\Box A$ jako zkratku za formuli $Thm(T)(\#A)$

Con(T) jako zkratku za formuli $\neg\Box(0=1)$

$Con(T)$ čteme T je bezesporná (konzistentní).

Druhá věta o neúplnosti.

Nechť T je bezesporné rekurzivně axiomatizovatelné rozšíření Peanovy aritmetiky P, potom

$$T \nvdash Con(T)$$

Poznámka.

Předpokládejme, že Peanova aritmetika je bezesporná. Protože

$$P \nvdash Con(P)$$

podle věty o úplnosti existuje model $M \models P$, takový, že $M \models Proof(d, \#\,0=1)$, kde d je číslo důkazu formule $0 = 1$. Takové číslo musí být nestandardní.

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

$$A \to (A \to A),\ A \to (A \to A) \ldots ; \ldots (A \to A),\ A,\ (A \to A),\ A, \ldots$$

vypadá jako důkaz (libovolné) formule A .

Ale není to důkaz, protože takovou posloupnost formulí nelze kódovat žádným přirozeným číslem daného modelu.

Zermelo-Fraenkelova teorie množin ZF

má jazyk prvního řádu s rovností, obsahuje Peanovu aritmetiku, má rekuzivní množinu axiomů, tedy je-li ZF bezesporná, pak

$$ZF \nvdash Con(ZF)$$

Můžeme, proto očekávat jen důkazy relativní bezespornosti

$$Con(ZF) \rightarrow Con(ZFC)$$