Matematická logika

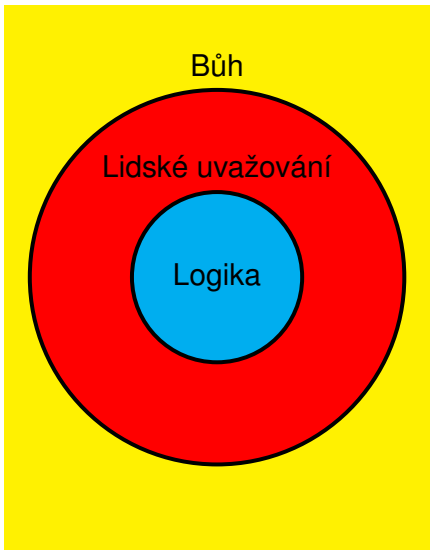
Materiály ke kurzu MA007

Poslední modifikace: březen 2024

Antonín Kučera

http://www.fi.muni.cz/usr/kucera/teaching.html

Logika.



- *Logika* (z řeckého $\lambda o \gamma o \varsigma$) zkoumá způsob vyvozování závěrů z předpokladů.
- V běžné řeči se „logikou“ označuje myšlenková cesta, která vedla k daným závěrům.
- Logika nezkoumá lidské myšlení (psychologie) ani obecné hranice lidského poznání (epistemologie).
- *„Může všemohoucí Bůh stvořit kámen, který sám nedokáže uzvednout?“*

Logika. Neformální, formální, matematická.

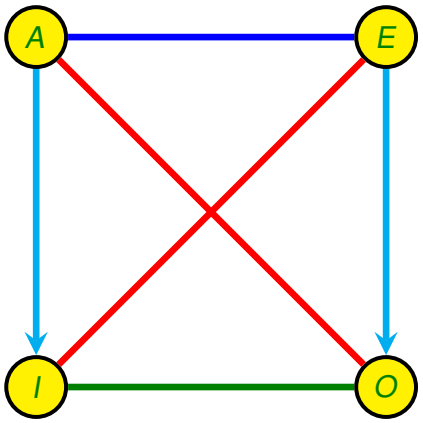
- *Neformální* logika studuje problematiku správné argumentace v přirozeném jazyce.
- *Formální* logika definuje a studuje abstraktní *odvozovací pravidla* (tj. *„formy úsudků“*), jejichž platnost nezávisí na významu pojmů, které v nich vystupují.
- Pojmem *matematická logika* se obvykle myslí dvě různé oblasti výzkumu:
  - aplikace poznatků z oblasti formální logiky na matematiku (např. snaha „vnořit“ matematiku do logiky ve formě konečného systému axiomů a odvozovacích pravidel);
  - aplikace matematických struktur a technik ve formální logice (např. teorie modelů, teorie důkazů, apod.)

Aristotelova logika.

- Považován za zakladatele formální logiky.
- Zavedl a prozkoumal pojem *sylogismu*.
- Aristoteles zkoumal také pravdivostní módy a položil tak základy modální logiky.

Aristoteles (384-322 př. Kr.)

Aristotelova logika. Logický čtverec.

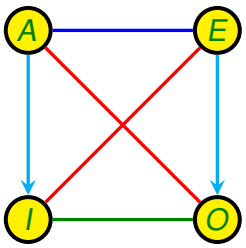


Nechť S a P jsou *neprázdné* vlastnosti. Aristoteles rozlišuje následující základní *kategorická tvrzení*:

- A „*všechna S jsou P*“
- E „*žádná S nejsou P*“
- I „*některá S jsou P*“
- O „*některá S nejsou P*“

Mnemonika: AffIrmo—nEgO
(tvrdím—popírám)

Aristotelova logika. Logický čtverec. (2)



- A a O jsou kontradiktorická, tj. nemohou být současně pravdivá ani současně nepravdivá. I a E jsou rovněž kontradiktorická.
- A a E jsou kontrární, tj. mohou být současně nepravdivá ale ne současně pravdivá.
- I a O jsou subkontrární, tj. mohou být současně pravdivá ale ne současně nepravdivá.
- I je subalterní (podřízené) A, tj. I je pravdivé jestliže A je pravdivé, a současně A je nepravdivé jestliže I je nepravdivé. Podobně O je subalterní E.

Aristotelova logika. Sylogismy.

- Sylogismy jsou jednoduché úsudky tvaru

  Hlavní premisa
  Vedlejší premisa
  $\therefore$ *Závěr*

- Obě premisy i závěr jsou kategorická tvrzení tvaru A, E, I, O obsahující dohromady právě tři vlastnosti S, M, P, kde
  - hlavní premisa obsahuje P a M;
  - vedlejší premisa obsahuje S a M;
  - závěr je tvaru S z P.
- Lze tedy rozlišit následující čtyři *formy* sylogismů:

I:	II:	III:	IV:
M x P	P x M	M x P	P x M
S y M	S y M	M y S	M y S
$\therefore S$ z P	$\therefore S$ z P	$\therefore S$ z P	$\therefore S$ z P

- Celkem tedy existuje $4 \cdot 4^3 = 256$ sylogismů.

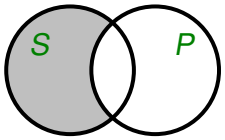
Aristotelova logika. Sylogismy. (2)

- Jen 24 sylogismů je *platných*:

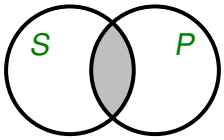
  „Barbara, Celarent, Darii, Ferioque prioris
  Cesare, Camestres, Festino, Baroco secundae
  Tertia grande sonans recitat Darapti, Felapton
  Disamis, Datisi, Bocardo, Ferison. Quartae
  Sunt Bamalip, Calames, Dimatis, Fesapo, Fresison.“

  - Forma I: AAA, EAE, AII, EIO (Barbara, Celarent, Darii, Ferioque), AAI, EAO (subalterní módy);
  - Forma II: EAE, AEE, EIO, AOO, (Cesare, Camestres, Festino, Baroco), AEO, EAO (subalterní módy);
  - Forma III: AAI, EAO, IAI, AII, OAO, EIO (Darapti, Felapton, Disamis, Datisi, Bocardo, Ferison);
  - Forma IV: AAI, AEE, IAI, EAO, EIO (Bamalip, Calemes, Dimatis, Fesapo, Fresison), AEO (subalterní mód).
- O (ne)platnosti sylogismů se lze snadno přesvědčit pomocí *Vennových diagramů* (John Venn, 1834–1923).

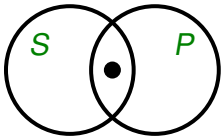
Aristotelova logika. Platnost sylogismů.



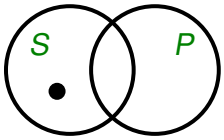
A
(všechna *S* jsou *P*)



E
(žádná *S* nejsou *P*)



I
(některá *S* jsou *P*)



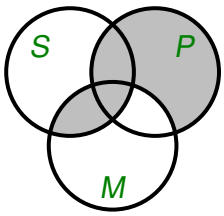
O
(některá *S* nejsou *P*)

- šedé oblasti jsou prázdné;
- symbol „•“ označuje neprázdné oblasti;
- bílé oblasti mohou být prázdné i neprázdné.

Aristotelova logika. Platnost sylogismů. (2)

- Uvažme nyní např. *AEE* sylogismus druhé formy (Camestres):

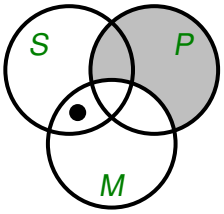
Všechna P jsou M
Žádná S nejsou M
∴ *Žádná S nejsou P*

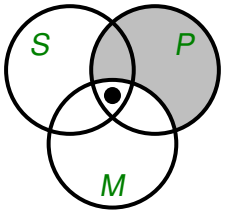


Tento sylogismus je tedy platný.

- Pro *AIO* sylogismus druhé formy dostáváme:

Všechna P jsou M
Některá S jsou M
∴ *Některá S nejsou P*



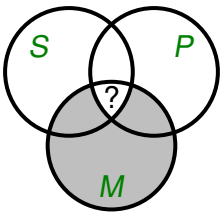


Druhý diagram podává protipříklad, sylogismus platný není.

Aristotelova logika. Platnost sylogismů. (3)

Rozeberme ještě *AAI* sylogismus třetí formy (Darapti):

Všechna M jsou P
Všechna M jsou S
$\therefore$ *Některá S jsou P*



Tento sylogismus je v Aristotelově logice považován za *platný*. Je však třeba použít předpoklad, že každá vlastnost je *neprázdná*. Tento předpoklad ale přináší jisté problémy:

Všechny skleněné hory jsou skleněné.
Všechny skleněné hory jsou hory.
$\therefore$ *Některé hory jsou skleněné.*

Hlavní i vedlejší premisa jsou na intuitivní úrovni pravdivá tvrzení, závěr však nikoliv.

Booleova „algebra logiky“.

George Boole (1815–1864)

- Aplikoval algebraické techniky při formalizaci procesu odvozování. Nalezl souvislost mezi algebrou a sylogismy.
- Booleova „algebra logiky“ se chová podobně jako algebra čísel. Násobení odpovídá logické spojce *„a současně“*, sčítání logické spojce *„nebo“*, apod. (Odtud pocházejí pojmy *„logický součin“* a *„logický součet“*.).

Algebra logiky. Motivační příklad.

Uvažme následující sylogismus:

Všechna S *jsou* M
Žádná M *nejsou* P
$\therefore$ *Žádná* S *nejsou* P

Pokud vlastnosti identifikujeme se soubory objektů univerza, pro které platí, můžeme uvedený sylogismus přepsat na

$$\begin{aligned} & S \subseteq M \\ & M \cap P = 0 \\ \therefore\ & S \cap P = 0 \end{aligned}$$

a dále na

$$\begin{aligned} & S \cap M' = 0 && (1) \\ & M \cap P = 0 && (2) \\ \therefore\ & S \cap P = 0 && (3) \end{aligned}$$

Pokusme se nyní „odvodit“ (3) z (1) a (2):

Algebra logiky. Motivační příklad. (2)

- Z toho, že $S \cap M' = 0$ a $0 \cap X = 0$ pro libovolné X dostáváme
  $(S \cap M') \cap P = 0$ (4)
- Podobně z (2) plyne $(M \cap P) \cap S = 0$ (5).
- Ze (4), (5) a faktu, že $0 \cup 0 = 0$, plyne
  $((S \cap M') \cap P) \cup ((M \cap P) \cap S) = 0$ (6)
- Užitím asociativity a komutativity $\cup$ a $\cap$ dostáváme z (6)
  $((S \cap P) \cap M') \cup ((S \cap P) \cap M) = 0$ (7)
- Nyní podle distributivního zákona lze (7) přepsat na
  $(S \cap P) \cap (M' \cup M) = 0$ (8)
- Jelikož $X \cup X' = 1$ a $X \cap 1 = X$ pro libovolné X, dostáváme z (8)
  $S \cap P = 0$

  což bylo dokázat.

Algebra logiky. Motivační příklad. (3)

V předchozím příkladu jsme k dokázání sylogismu použili symbolickou manipulaci se symboly S, M a P podle následujících *algebraických identit* (tj. nezabývali jsme se tím, jaký mají symboly $\cup$, $\cap$, 0, 1, a $'$ *význam*).

$$
\begin{aligned}
X \cup X &= X & \qquad X \cup X' &= 1 \\
X \cap X &= X & \qquad X \cap X' &= 0 \\
X \cup Y &= Y \cup X & \qquad X'' &= X \\
X \cap Y &= Y \cap X & \qquad X \cup 1 &= 1 \\
X \cup (Y \cup Z) &= (X \cup Y) \cup Z & \qquad X \cap 1 &= X \\
X \cap (Y \cap Z) &= (X \cap Y) \cap Z & \qquad X \cup 0 &= X \\
X \cap (X \cup Y) &= X & \qquad X \cap 0 &= 0 \\
X \cup (X \cap Y) &= X & \qquad (X \cup Y)' &= X' \cap Y' \\
X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) & \qquad (X \cap Y)' &= X' \cup Y' \\
X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z)
\end{aligned}
$$

Algebra logiky. Motivační příklad. (4)

- Tyto identity definují algebraickou strukturu, které se později začalo říkat *Booleva algebra* (případně *Booleův svaz*).
- V původní Booleově notaci se
  - místo $X \cap Y$ píše $X.Y$ (případně jen XY);
  - místo $X \cup Y$ píše $X + Y$;
  - místo X' píše $1 - X$.

  V této notaci pak identity dostávají číselnou podobu a Boole sám se pokoušel převést další číselné konstrukce (např. dělení, ale i Taylorův rozvoj) do své „algebry logiky“. Tyto úvahy však již byly zcela mylné.

Algebra logiky. Dva základní problémy.

- Podle Boolea je každý sylogismus možné zapsat ve tvaru

$$\begin{aligned} F_1(P,M,A) &= 0 \\ F_2(S,M,B) &= 0 \\ \therefore\ F(S,P,C) &= 0 \end{aligned}$$

kde $F_1(P,M,A)$, $F_2(S,M,B)$, $F(S,P,C)$ jsou vhodné výrazy vytvořené ze symbolů 0, 1, $\cup$, $\cap$, $'$ a symbolů v závorkách.

- Symboly A, B, C plní roli „blíže neurčených vlastností“ při přepisu kategorických tvrzení I a O. Např. „některá S jsou P“ Boole vyjádřil pomocí rovnosti $S \cap A = P \cap A$, tj. $(S \cap A) \cap (P \cap A)' = 0$, kde A je blíže neurčená vlastnost. Tento postup *není* zcela korektní.

Algebra logiky. Dva základní problémy. (2)

- Boole uvážil obecnější úsudky tvaru

$$\begin{aligned} F_1(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0 \\ &\vdots \\ F_k(A_1,\ldots,A_m,B_1,\ldots,B_n) &= 0 \\ \therefore\ F(B_1,\ldots,B_n) &= 0 \end{aligned}$$

- Cílem jeho snah bylo vyvinout metodu, která umožní
  - zjistit, zda je daný úsudek *pravdivý*;
  - nalézt *nejobecnější* závěr (F) pro dané předpoklady ($F_1,\ldots,F_k$).

Algebra logiky. Booleova metoda.

Definice 1

Nechť $\vec{A} = A_1, \ldots, A_n$. $\vec{A}$-konstituent je výraz tvaru $\ell_1 \cap \cdots \cap \ell_n$, kde ℓ_i je buď A_i nebo A_i'.

Věta 2

Pro každé $F(X_1, \cdots, X_n)$ platí

$$F(X_1, \cdots, X_n) = \bigcup_{\vec{v} \in \{0,1\}^n} F(\vec{v}) \cap \ell_1(\vec{v}) \cap \cdots \cap \ell_n(\vec{v})$$

kde $\ell_i(\vec{v})$ je buď X_i nebo X_i' podle toho, zda je $\vec{v}_i$ rovno 1 nebo 0.

Příklad 3

Nechť $F(A, B) = (A \cup B') \cap (A' \cup B)$. Pak

$$\begin{aligned} F(A,B) &= (F(0,0) \cap A' \cap B') \cup (F(0,1) \cap A' \cap B) \\ &\quad \cup (F(1,0) \cap A \cap B') \cup (F(1,1) \cap A \cap B) \\ &= (1 \cap A' \cap B') \cup (0 \cap A' \cap B) \cup (0 \cap A \cap B') \cup (1 \cap A \cap B) \\ &= (A' \cap B') \cup (A \cap B) \end{aligned}$$

Algebra logiky. Řešení 1. problému.

Věta 4

Úsudek

$$\begin{aligned} F_1(A_1, \ldots, A_m, B_1, \ldots, B_n) &= 0 \\ &\vdots \\ F_k(A_1, \ldots, A_m, B_1, \ldots, B_n) &= 0 \\ \therefore \quad F(B_1, \ldots, B_n) &= 0 \end{aligned}$$

je platný, právě když každý $\vec{A}, \vec{B}$-konstituent výrazu F je $\vec{A}, \vec{B}$-konstituentem některého F_i.

Algebra logiky. Řešení 1. problému. (2)

Příklad 5

Uvažme opět sylogismus

$$\begin{array}{rcl} S \cap M' & = & 0 \\ M \cap P & = & 0 \\ \therefore \quad S \cap P & = & 0 \end{array}$$

Pak $\vec{A} = M$ a $\vec{B} = S, P$. Uvažme $\vec{A}, \vec{B}$-konstituenty jednotlivých výrazů:

$$\begin{array}{rcl} S \cap M' & : & M' \cap S \cap P,\ M' \cap S \cap P' \\ M \cap P & : & M \cap S \cap P,\ M \cap S' \cap P \\ S \cap P & : & M \cap S \cap P,\ M' \cap S \cap P \end{array}$$

Podle *věty 4* je tento úsudek pravdivý.

Algebra logiky. Řešení 2. problému.

- Nechť $\vec{A} = A_1, \ldots, A_m$, $\vec{B} = B_1, \ldots, B_n$. Uvažme předpoklady tvaru

$$F_1(\vec{A}, \vec{B}) = 0, \cdots, F_k(\vec{A}, \vec{B}) = 0$$

- Cílem je nalézt nejobecnější závěr tvaru $F(\vec{B}) = 0$. Označme

$$E(\vec{A}, \vec{B}) = F_1(\vec{A}, \vec{B}) \cup \cdots \cup F_k(\vec{A}, \vec{B})$$

Algebra logiky. Řešení 2. problému. (2)

Věta 6

Nejobecnější závěr $F(\vec{B}) = 0$, který plyne z $E(\vec{A}, \vec{B}) = 0$, je tvaru

$$F(\vec{B}) \quad = \quad \bigcap_{\vec{v} \in \{0,1\}^m} E(\vec{v}, \vec{B})$$

Příklad 7

Nejobecnější závěr $F(S, P)$ plynoucí z předpokladů $S \cap M' = 0$ a $M \cap P = 0$ je tvaru

$$\begin{aligned} F(S,P) &= ((S \cap 0') \cup (0 \cap P)) \cap ((S \cap 1') \cup (1 \cap P)) \\ &= S \cap P \end{aligned}$$

Výstavba formálních logických systémů.

- Potřebujeme znát jisté pojmy a umět myslet (*metaúroveň*).
  - Musí být např. jasné, co myslíme symbolem, konečnou posloupností, atd.
  - Metapojmy a formální pojmy se bohužel často „značí“ stejně. Tím vzniká (nesprávný) dojem, že formální pojmy jsou definovány pomocí „sebe sama“ (typickým příkladem je *důkaz* nebo *množina*).
  - Co všechno si lze na metaúrovni dovolit? (*potenciální* vs. *aktuální* nekonečno).
- Základní kroky:
  - Vymezení užívaných symbolů (abeceda).
  - Syntaxe formulí.
  - Sémantika (zde se objeví pojem *pravdivost*).
  - Odvozovací systém (zde se objeví pojem *dokazatelnost*).

Výroková logika. Syntaxe.

Definice 8

Abecedu výrokové logiky tvoří následující symboly:

- *znaky pro výrokové proměnné* $A, B, C, \ldots$, *kterých je spočetně mnoho;*
- *logické spojky* $\wedge$, $\vee$, $\rightarrow$, $\neg$
- *závorky* (*a*)

Výroková logika. Syntaxe. (2)

Definice 9

Formule výrokové logiky je slovo φ *nad abecedou výrokové logiky, pro které existuje vytvořující posloupnost, tj. konečná posloupnost slov* $\psi_1, \cdots, \psi_k$, *kde* $k \geq 1$, ψ_k *je* φ, *a pro každé* $1 \leq i \leq k$ *má slovo* ψ_i *jeden z následujících tvarů:*

- *výroková proměnná,*
- $\neg\psi_j$ *pro nějaké* $1 \leq j < i$,
- $(\psi_j \circ \psi_{j'})$ *pro nějaká* $1 \leq j, j' < i$, *kde* $\circ$ *je jeden ze symbolů* $\wedge$, $\vee$, $\rightarrow$.

Složitost výrokové formule φ *je nejmenší* ℓ *takové, že existuje vytvořující posloupnost pro* φ *délky právě* ℓ.

Výroková logika. Syntaxe. (3)

Příklady:

- $A, B, (A \wedge B)$
- $B, A, (A \wedge B)$
- $B, C, (C \rightarrow B), A, (A \wedge (B \vee B)), (A \wedge B)$
- $A, B, A \wedge B$

Výroková logika. Syntaxe. (4)

Poznámka 10

V dalším textu budeme často vynechávat v zápisech formulí *vnější* závorky. Např. místo $(A \vee \neg B)$ budeme psát $A \vee \neg B$. Po zavedení *sémantiky* výrokové logiky budeme často vynechávat i další dvojice závorek v případě, kdy vzniklá *syntaktická* nejednoznačnost nepovede k *sémantické* nejednoznačnosti.

Výroková logika. Sémantika.

Definice 11

Pravdivostní ohodnocení (valuace) je zobrazení v, které každé výrokové proměnné přiřadí hodnotu 0 nebo 1.

Metamatematickou indukcí ke složitosti formule lze každou valuaci v jednoznačně rozšířit na všechny výrokové formule:

- $v(A)$ je již definováno;
- $v(\neg\psi) = \begin{cases} 0 & \text{jestliže } v(\psi) = 1; \\ 1 & \text{jinak.} \end{cases}$
- $v(\psi_1 \wedge \psi_2) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 0 \text{ nebo } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$
- $v(\psi_1 \vee \psi_2) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 0 \text{ a současně } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$
- $v(\psi_1 \to \psi_2) = \begin{cases} 0 & \text{jestliže } v(\psi_1) = 1 \text{ a současně } v(\psi_2) = 0; \\ 1 & \text{jinak.} \end{cases}$

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Výroková logika. Sémantika. (2)

Definice 12

- *Výroková formule* φ *je*
  - *pravdivá (resp. nepravdivá) při valuaci* v*, pokud* $v(\varphi) = 1$ *(resp.* $v(\varphi) = 0$*);*
  - *splnitelná, jestliže existuje valuace* v *taková, že* $v(\varphi) = 1$*;*
  - *tautologie (také (logicky) pravdivá), jestliže* $v(\varphi) = 1$ *pro každou valuaci* v*.*
- *Soubor* T *výrokových formulí je splnitelný, jestliže existuje valuace* v *taková, že* $v(\varphi) = 1$ *pro každé* φ *z* T*.*
- *Formule* φ *a* ψ *jsou ekvivalentní, psáno* $\varphi \approx \psi$*, jestliže pro každou valuaci* v *platí, že* $v(\varphi) = v(\psi)$*.*

Výroková logika. Sémantika. (3)

Příklad 13

- Formule $A \wedge B$ je pravdivá při valuaci v_1, kde $v_1(A) = v_1(B) = 1$, a nepravdivá při valuaci v_2, kde $v_2(A) = 0$. Jde tedy o splnitelnou formuli, která není tautologií.
- Pro každou formuli φ platí, že φ je tautologie právě když $\neg\varphi$ není splnitelná.
- Nechť φ, ψ, ξ jsou výrokové formule. Pak:

$$\begin{array}{rcl} \varphi \wedge \psi & \approx & \psi \wedge \varphi \\ \varphi \wedge (\psi \wedge \xi) & \approx & (\varphi \wedge \psi) \wedge \xi \\ \varphi \wedge (\psi \vee \xi) & \approx & (\varphi \wedge \psi) \vee (\varphi \wedge \xi) \\ \neg(\varphi \wedge \psi) & \approx & \neg\varphi \vee \neg\psi \\ \neg\neg\varphi & \approx & \varphi \end{array}$$

Výroková logika. Sémantika. (4)

Poznámka 14

„Identity“ z posledního bodu *příkladu 13* umožňují dále zpřehlednit zápis formulí. Např. místo $(A \vee B) \vee C$ můžeme (nejednoznačně) psát $A \vee B \vee C$. Tato nejednoznačnost nevede k problémům, neboť příslušné definice a tvrzení „fungují“ pro libovolné možné uzávorkování.

Poznámka 15

V teorii *výpočetní složitosti* se dokazuje, že problém zda daná výroková formule φ je splnitelná (resp. tautologie) je *NP-úplný* (resp. *co-NP-úplný*). Otázka, zda existuje efektivní (polynomiální) algoritmus pro uvedené problémy, je ekvivalentní otázce zda $P = NP$.

Definice 16

Formule φ je tautologickým důsledkem souboru formulí T, psáno $T \models \varphi$, jestliže $v(\varphi) = 1$ pro každou valuaci v takovou, že $v(\psi) = 1$ pro každou formuli ψ ze souboru T. Jestliže $T \models \varphi$ pro prázdný soubor T, píšeme krátce $\models \varphi$.

Výroková logika. Pravdivostní tabulky.

Někdy se sémantika výrokových spojek definuje „předem“ pomocí *pravdivostních tabulek*:

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

X	Y	$X \to Y$
0	0	1
0	1	1
1	0	0
1	1	1

X	$\neg X$
0	1
1	0

Pojmy „pravdivostní tabulka“ a „výroková spojka“ je možné dále zobecnit a uvážit formální logické systémy budované na obecnějším základu:

Definice 17

Výroková funkce je funkce $F : \{0,1\}^n \to \{0,1\}$, kde $n \geq 1$.

Výroková logika. Systém $\mathcal{L}(F_1, \cdots, F_k)$.

Definice 18

Nechť $F_1, \cdots, F_k$ je konečný soubor výrokových funkcí. Definujeme formální logický systém $\mathcal{L}(F_1, \cdots, F_k)$, kde

- *Abeceda je tvořena znaky pro výrokové proměnné, závorkami a znaky $\mathcal{F}_1, \cdots, \mathcal{F}_k$ pro uvedené výrokové funkce.*
- *V definici vytvořující posloupnosti formule (viz definice 9) požadujeme, aby ψ_i bylo buď výrokovou proměnnou nebo tvaru $\mathcal{F}_j(\psi_{j_1}, \cdots, \psi_{j_n})$, kde $1 \leq j_1, \cdots, j_n < i$ a n je arita F_j.*
- *Valuace rozšíříme z výrokových proměnných na formule předpisem $v(\mathcal{F}(\psi_1, \cdots, \psi_n)) = F(v(\psi_1), \cdots, v(\psi_n))$*

Poznámka 19

Ve smyslu *definice 18* je dosud uvažovaný systém výrokové logiky systémem $\mathcal{L}(\wedge, \vee, \to, \neg)$. Dříve zavedené sémantické pojmy (splnitelnost, pravdivost, atd.) se opírají pouze o pojem valuace a „fungují“ tedy v *libovolném* systému $\mathcal{L}(F_1, \cdots, F_k)$.

Výroková logika. Systém $\mathcal{L}(F_1, \cdots, F_k)$. (2)

Pro účely následující definice zvolme libovolné (ale dále pevné) lineární uspořádání $\sqsubseteq$ na souboru všech výrokových proměnných.

Definice 20

Nechť φ je formule $\mathcal{L}(F_1, \cdots, F_k)$ a nechť $X_1, \cdots, X_n$ je vzestupně uspořádaná posloupnost (vzhledem k $\sqsubseteq$) všech výrokových proměnných, které se ve φ vyskytují. Formule φ jednoznačně určuje výrokovou funkci $F_\varphi : \{0,1\}^n \to \{0,1\}$ danou předpisem $F_\varphi(\vec{u}) = v_{\vec{u}}(\varphi)$, kde $v_{\vec{u}}$ je valuace definovaná takto:

- $v_{\vec{u}}(X_i) = \vec{u}(i)$ *pro každé* $1 \leq i \leq n$,
- $v_{\vec{u}}(Y) = 0$ *pro ostatní* Y.

Výroková logika. Systém $\mathcal{L}(F_1, \cdots, F_k)$. (3)

Příklad:

- Nechť $\varphi \equiv X \to (Y \wedge Z)$. Pak F_φ je následující funkce:

X	Y	Z	F_φ
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Výroková logika. Systém $\mathcal{L}(F_1, \cdots, F_k)$. (4)

Definice 21

Systém $\mathcal{L}(F_1, \cdots, F_k)$ je plnohodnotný, jestliže pro každou výrokovou funkci F existuje formule φ systému $\mathcal{L}(F_1, \cdots, F_k)$ taková, že $F = F_\varphi$.

Výroková logika. Plnohodnotnost.

Věta 22

Systém $\mathcal{L}(\wedge, \vee, \neg)$ je plnohodnotný.

Důkaz. Nechť $F : \{0,1\}^n \to \{0,1\}$ je výroková funkce a nechť $\vec{u}_1, \cdots, \vec{u}_k$ jsou všechny vektory z $\{0,1\}^n$, pro které nabývá F hodnoty 1. Pokud žádný takový vektor není (tj. $k = 0$), klademe $\varphi = X_1 \wedge \neg X_1 \wedge X_2 \wedge \cdots \wedge X_n$. Jinak

$$\varphi = \bigvee_{i=1}^{k} \ell_1(u_i) \wedge \cdots \wedge \ell_n(u_i)$$

kde $\ell_j(u_i)$ je buď X_j nebo $\neg X_j$ podle toho, zda $u_i(j) = 1$ nebo $u_i(j) = 0$. Nyní se lehce ověří, že $F = F_\varphi$. □

Výroková logika. Plnohodnotnost. (2)

- Uvažme následující výrokové funkce:

X	Y	$X \curlywedge Y$
0	0	1
0	1	0
1	0	0
1	1	0

X	Y	$X \mid Y$
0	0	1
0	1	1
1	0	1
1	1	0

X	Y	Z	$\odot(X,Y,Z)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

- Funkce $\curlywedge$ se nazývá *Schröderův* operátor. Platí $\varphi \curlywedge \psi \approx \neg(\varphi \vee \psi)$.
- Funkce $\mid$ se nazývá *Shefferův* operátor. Platí $\varphi \mid \psi \approx \neg(\varphi \wedge \psi)$.

Výroková logika. Plnohodnotnost. (3)

Následující systémy výrokové logiky jsou plnohodnotné:

- $\mathcal{L}(\wedge,\vee,\neg)$ *Věta 22*.
- $\mathcal{L}(\wedge,\neg)$ $\varphi \vee \psi \approx \neg(\neg\varphi \wedge \neg\psi)$
- $\mathcal{L}(\vee,\neg)$ $\varphi \wedge \psi \approx \neg(\neg\varphi \vee \neg\psi)$
- $\mathcal{L}(\rightarrow,\neg)$ $\varphi \vee \psi \approx \neg\varphi \rightarrow \psi$
- $\mathcal{L}(\curlywedge)$ $\neg\varphi \approx \varphi \curlywedge \varphi$, $\varphi \vee \psi \approx (\varphi \curlywedge \psi) \curlywedge (\varphi \curlywedge \psi)$
- $\mathcal{L}(\mid)$ $\neg\varphi \approx \varphi \mid \varphi$, $\varphi \wedge \psi \approx (\varphi \mid \psi) \mid (\varphi \mid \psi)$
- $\mathcal{L}(\odot)$ $\neg\varphi \approx \odot(\varphi,\varphi,\varphi)$,
  $\varphi \rightarrow \psi \approx \odot(\varphi,\odot(\varphi,\varphi,\varphi),\odot(\varphi,\psi,\odot(\varphi,\varphi,\varphi)))$

Následující systémy plnohodnotné nejsou:

- $\mathcal{L}(\wedge)$, $\mathcal{L}(\vee)$, $\mathcal{L}(\rightarrow)$, $\mathcal{L}(\neg)$, atd.

Výroková logika. Shefferovské spojky.

Definice 23

Výroková funkce F je Shefferovská jestliže $\mathcal{L}(F)$ je plnohodnotný systém.

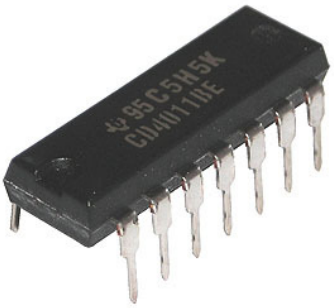
Věta 24

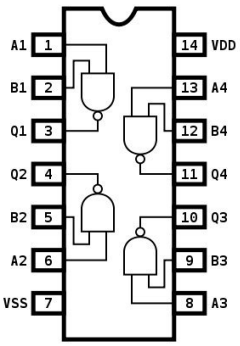
- *Nechť $S(n)$ značí počet všech Shefferovských funkcí arity $n \geq 1$. Pak $S(n) = 2^{(2^{n-1}-1)}(2^{(2^{n-1}-1)} - 1)$. (Pro $n = 1, 2, 3, 4, 5, \ldots$ dostáváme postupně $0, 2, 56, 16256, 1073709056, \ldots$)*
- *Jelikož $\lim_{n\to\infty} \frac{S(n)}{2^{2^n}} = 1/4$, je (pro velká n) zhruba čtvrtina ze všech výrokových funkcí arity n Shefferovská.*

Výroková logika. Shefferovské spojky. (2)

Poznámka 25

Výsledky o Shefferovských funkcích nalézají uplatnění při výrobě logických obvodů; na „podkladové desce“ se např. vytvoří hustá síť binárních |-hradel. Obvody různé funkce se pak realizují jejich vhodným propojením.





Integrovaný obvod 4011 CMOS se čtyřmi |-hradly.

Výroková logika. Normální formy.

Definice 26

- *Literál* je formule tvaru X nebo $\neg X$, kde X je výroková proměnná;
- *Klauzule* je formule tvaru $\ell_1 \vee \cdots \vee \ell_n$, kde $n \geq 1$ a každé ℓ_i je literál.
- *Duální klauzule* je formule tvaru $\ell_1 \wedge \cdots \wedge \ell_n$, kde $n \geq 1$ a každé ℓ_i je literál.
- Formule v *konjunktivním* normálním tvaru (CNF) je formule tvaru $C_1 \wedge \cdots \wedge C_m$, kde $m \geq 1$ a každé C_i je klauzule.
- Formule v *disjunktivním* normálním tvaru je formule tvaru $C_1 \vee \cdots \vee C_m$, kde $m \geq 1$ a každé C_i je duální klauzule.

Okamžitým důsledkem *věty 22* je následující:

Věta 27

Pro každou formuli φ existuje ekvivalentní formule v disjunktivním normálním tvaru.

Výroková logika. Normální formy. (2)

Věta 28

Pro každou formuli φ existuje ekvivalentní formule ψ v konjunktivním normálním tvaru.

Důkaz. Nechť $F_\varphi : \{0,1\}^n \to \{0,1\}$ je výroková funkce určená formulí φ (viz *definice 20*) a nechť $\vec{u}_1, \cdots, \vec{u}_k$ jsou všechny vektory z $\{0,1\}^n$, pro které nabývá F_φ hodnoty 0. Pokud žádný takový vektor není (tj. $k = 0$), klademe $\psi = X_1 \vee \neg X_1 \vee X_2 \vee \cdots \vee X_n$. Jinak

$$\psi = \bigwedge_{i=1}^{k} \ell_1(u_i) \vee \cdots \vee \ell_n(u_i)$$

kde $\ell_j(u_i)$ je buď X_j nebo $\neg X_j$ podle toho, zda $u_i(j) = 0$ nebo $u_i(j) = 1$. Nyní se lehce ověří, že $\varphi \approx \psi$. □

Výroková logika. Normální formy. (3)

Příklad 29

Formuli $(A \to B) \wedge (B \to C) \wedge (C \to A)$ lze v CNF reprezentovat jako

- $(\neg A \vee B) \wedge (\neg B \vee C) \wedge (\neg C \vee A)$

nebo

- $(\neg A \vee C) \wedge (\neg C \vee B) \wedge (\neg B \vee A)$.

CNF tedy *není* určena jednoznačně až na pořadí klauzulí a literálů.

Výroková logika. Věta o kompaktnosti.

Věta 30 (o kompaktnosti)

Nechť T je soubor formulí výrokové logiky. T je splnitelný právě když každá konečná část T je splnitelná.

Důkaz. Směr „$\Rightarrow$“ je triviální. Dokážeme „$\Leftarrow$“. Pokud je T konečný, jsme hotovi ihned. Jinak nechť $\varphi_1, \varphi_2, \ldots$ je posloupnost všech formulí z T. Pro každé $i \geq 1$ definujeme:

- $F_i = \{\varphi_1, \ldots, \varphi_i\}$,
- v_i je splňující valuace pro F_i (taková existuje, neboť F_i je konečná část T).

Nechť $X_1, X_2, \ldots$ je nekonečná posloupnost všech výrokových proměnných. Pro každé $i \geq 0$ induktivně zadefinujeme nekonečnou rostoucí posloupnost α_i přirozených čísel splňující následující podmínky:

- Všechny valuace v_j takové, že j se vyskytuje v α_i, souhlasí na všech proměnných $X_1, \ldots, X_i$.
- α_{i+1} je posloupností vybranou z α_i.

Výroková logika. Věta o kompaktnosti. (2)

Stačí položit

- $\alpha_0 = 1, 2, 3, 4, \ldots$
- Nechť β je podposloupnost α_i složená ze všech čísel j takových, že $v_j(X_{i+1}) = 1$. Pokud je β nekonečná, pak $\alpha_{i+1} = \beta$. Jinak je α_{i+1} podposloupnost α_i složená ze všech čísel j takových, že $v_j(X_{i+1}) = 0$.

Nechť v je valuace definovaná předpisem $v(X_i) = v_j(X_i)$, kde j je (libovolný) index z α_i. Ukážeme, že v je splňující valuace pro T. Buď $\varphi_k \in T$ libovolná (nadále pevná) formule. Nechť všechny výrokové proměnné obsažené ve φ_k jsou mezi $\{X_1, \ldots, X_\ell\}$. . Buď j číslo z α_ℓ takové, že $j \geq k$. Pak $\varphi_k \in F_j$ a valuace v souhlasí s valuací v_j na všech proměnných z $\{X_1, \ldots, X_\ell\}$. Jelikož $v_j(\varphi_k) = 1$, platí také $v(\varphi_k) = 1$. □

Výroková logika. Věta o kompaktnosti. (3)

Užitím *věty 30* lze snadno dokázat řadu dalších tvrzení.

- *Graf* $\mathcal{G}$ je dvojice (U, H), kde U je nejvýše spočetný soubor *uzlů* a H je areflexivní a symetrická relace na U.
- *Podgraf* grafu $\mathcal{G}$ je graf $\mathcal{G}' = (U', H')$, kde $U' \subseteq U$ a $H' \subseteq H$.
- Graf $\mathcal{G} = (U, H)$ je *k-obarvitelný* jestliže existuje funkce $f : U \to \{1, \cdots, k\}$ taková, že $f(u) \neq f(v)$ pro každé $(u, v) \in H$.

Výroková logika. Věta o kompaktnosti. (4)

Věta 31

Graf $\mathcal{G} = (U, H)$ je k-obarvitelný právě když každý konečný podgraf $\mathcal{G}$ je k-obarvitelný.

Důkaz. Nechť $B_{u,i}$ je výroková proměnná pro každý uzel u a každé $1 \leq i \leq k$. Buď T soubor tvořený následujícími formulemi:

- $B_{u,1} \vee \cdots \vee B_{u,k}$ pro každý uzel u;
- $B_{u,i} \rightarrow \neg B_{u,j}$ pro každý uzel u a každé $1 \leq i, j \leq k$, kde $i \neq j$;
- $B_{u,i} \rightarrow \neg B_{v,i}$ pro každé $(u, v) \in H$ a $1 \leq i \leq k$.

Platí následující pozorování:

- Graf $\mathcal{G}$ je k-obarvitelný právě když soubor T je splnitelný.
- Každý konečný podgraf $\mathcal{G}$ je k-obarvitelný právě když každý konečný podsoubor T je splnitelný.

Nyní stačí aplikovat *větu 30*. □

Logika $\mathcal{L}(\rightarrow, \neg)$. Odvozovací systém.

- Odvozovací systém je konečný soubor *pravidel*, která umožňují z daného souboru formulí (třeba i prázdného) odvodit další formuli.
- Odvozovací pravidla jsou definována na základě syntaxe formulí, nikoliv jejich sémantiky.
- Jestliže je formule φ odvoditelná ze souboru formulí T, píšeme $T \vdash \varphi$.
- Daný odvozovací systém je
  - *korektní*, jestliže $T \vdash \varphi$ implikuje $T \models \varphi$;
  - *úplný*, jestliže $T \models \varphi$ implikuje $T \vdash \varphi$.

Logika $\mathcal{L}(\rightarrow, \neg)$. Odvozovací systém. (2)

V této části se soustředíme na $\mathcal{L}(\rightarrow, \neg)$. Uvažme následující odvozovací systém pro $\mathcal{L}(\rightarrow, \neg)$ (Lukasiewicz, 1928):

Schémata axiómů:

- A1: $\varphi \rightarrow (\psi \rightarrow \varphi)$
- A2: $(\varphi \rightarrow (\psi \rightarrow \xi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \xi))$
- A3: $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

Odvozovací pravidlo:

- MP: Z φ a $\varphi \rightarrow \psi$ odvoď ψ. (modus ponens)

Logika $\mathcal{L}(\rightarrow, \neg)$. Odvozovací systém. (3)

Definice 32

Buď T soubor formulí.

- *Důkaz formule ψ z předpokladů T je konečná posloupnost formulí $\varphi_1, \cdots, \varphi_k$, kde φ_k je ψ a pro každé φ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:*
  - *φ_i je prvek T;*
  - *φ_i je instancí jednoho ze schémat A1–A3;*
  - *φ_i vznikne aplikací pravidla MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.*
- *Formule ψ je dokazatelná z předpokladů T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ z předpokladů T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme, že ψ je dokazatelná a píšeme $\vdash \psi$.*

Logika $\mathcal{L}(\rightarrow, \neg)$. Odvozovací systém. (4)

Příklad 33

Pro libovolnou formuli φ platí $\vdash \varphi \rightarrow \varphi$.

Důkaz. Následující posloupnost formulí je důkazem $\varphi \rightarrow \varphi$.

1)	$(\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)) \rightarrow ((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi))$	$A2$
2)	$\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)$	$A1$
3)	$(\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi)$	MP na 2), 1)
4)	$\varphi \rightarrow (\varphi \rightarrow \varphi)$	$A1$
5)	$\varphi \rightarrow \varphi$	MP na 4), 3)

□

Logika $\mathcal{L}(\rightarrow, \neg)$. Odvozovací systém. (5)

Příklad 34

Pro libovolné formule φ, ψ platí $\{\varphi, \neg\varphi\} \vdash \psi$.

Důkaz. Následující posloupnost formulí je důkazem ψ z $\{\varphi, \neg\varphi\}$:

1)	$\neg\varphi \rightarrow (\neg\psi \rightarrow \neg\varphi)$	$A1$
2)	$\neg\varphi$	předpoklad
3)	$\neg\psi \rightarrow \neg\varphi$	MP na 2), 1)
4)	$(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$	$A3$
5)	$\varphi \rightarrow \psi$	MP na 3), 4)
6)	φ	předpoklad
7)	ψ	MP na 6), 5)

□

Výroková logika. Věta o dedukci.

Věta 35 (o dedukci)

Nechť φ, ψ jsou formule a T soubor formulí. Pak $T \cup \{\psi\} \vdash \varphi$ právě když $T \vdash \psi \to \varphi$.

Důkaz.

„$\Leftarrow$“: Nechť $\xi_1, \cdots, \xi_k$ je důkaz formule $\psi \to \varphi$ z předpokladů T. Pak $\xi_1, \cdots, \xi_k, \psi, \varphi$ je důkaz formule φ z předpokladů $T \cup \{\psi\}$ (poslední formule vznikne aplikací MP na ψ a ξ_k).

„$\Rightarrow$“: Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ z předpokladů $T \cup \{\psi\}$. Metaindukcí k j dokážeme, že $T \vdash \psi \to \xi_j$ pro každé $1 \leq j \leq k$.

- $j = 1$. Je-li ξ_1 instance axiómu nebo formule z T, platí $T \vdash \xi_1$. K důkazu ξ_1 z T nyní připojíme formule $\xi_1 \to (\psi \to \xi_1)$, $\psi \to \xi_1$. První formule je instancí A1, druhá aplikací MP na ξ_1 a první formuli. Máme tedy důkaz $\psi \to \xi_1$ z T.
  Je-li ξ_1 formule ψ, platí $T \vdash \psi \to \psi$ podle *příkladu 33*.
- *Indukční krok:* Je-li formule ξ_j instancí axiómu nebo prvek $T \cup \{\psi\}$, postupujeme stejně jako výše (místo ξ_1 použijeme ξ_j).
  Je-li ξ_j výsledkem aplikace MP na ξ_m, ξ_n, kde $1 \leq m, n < j$, je ξ_n tvaru $\xi_m \to \xi_j$. Podle I.P. navíc platí $T \vdash \psi \to \xi_m$ a $T \vdash \psi \to (\xi_m \to \xi_j)$. Důkazy $\psi \to \xi_m$ a $\psi \to (\xi_m \to \xi_j)$ z T nyní zřetězíme za sebe a připojíme následující formule:

Výroková logika. Věta o dedukci. (2)

- $(\psi \to (\xi_m \to \xi_j)) \to ((\psi \to \xi_m) \to (\psi \to \xi_j))$
- $(\psi \to \xi_m) \to (\psi \to \xi_j)$
- $\psi \to \xi_j$

První formule je instancí A2, další dvě vzniknou aplikací MP. Máme tedy důkaz formule $\psi \to \xi_j$ z T.

□

Výroková logika. Věta o korektnosti.

Věta 36 (o korektnosti)

Nechť φ je formule a T soubor formulí. Jestliže $T \vdash \varphi$, pak $T \models \varphi$.

Důkaz. Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ z T. Indukcí vzhledem k j dokážeme, že $T \models \xi_j$ pro každé $1 \leq j \leq k$. (Stačí ověřit, že každá instance A1–A3 je tautologie, a že jestliže $T \models \psi$ a $T \models \psi \to \xi$, pak také $T \models \xi$). □

Výroková logika. Věta o úplnosti.

Lema 37

Nechť φ, ψ jsou formule. Pak

(a) $\vdash \neg\varphi \to (\varphi \to \psi)$

(b) $\vdash \neg\neg\varphi \to \varphi$

(c) $\vdash \varphi \to \neg\neg\varphi$

(d) $\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$

(e) $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$

(f) $\vdash (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$

Výroková logika. Věta o úplnosti. (2)

Důkaz.

- (a): Podle *příkladu 34* platí $\{\varphi, \neg\varphi\} \vdash \psi$, proto $\vdash \neg\varphi \to (\varphi \to \psi)$ opakovaným užitím věty o dedukci.
- (b): Platí

1)	$\vdash \neg\neg\varphi \to (\neg\varphi \to \neg\neg\neg\varphi)$	podle (a)
2)	$\{\neg\neg\varphi\} \vdash \neg\varphi \to \neg\neg\neg\varphi$	věta o dedukci
3)	$\vdash (\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$	$A3$
4)	$\{\neg\neg\varphi\} \vdash \neg\neg\varphi \to \varphi$	MP na 2), 3)
5)	$\{\neg\neg\varphi\} \vdash \varphi$	věta o dedukci
6)	$\vdash \neg\neg\varphi \to \varphi$	věta o dedukci

- (c): Platí

1)	$\vdash \neg\neg\neg\varphi \to \neg\varphi$	podle (b)
2)	$\vdash (\neg\neg\neg\varphi \to \neg\varphi) \to (\varphi \to \neg\neg\varphi)$	$A3$
3)	$\vdash \varphi \to \neg\neg\varphi$	MP na 1), 2)

Výroková logika. Věta o úplnosti. (3)

- (d): Platí

1)	$\{\varphi \to \psi\} \vdash \varphi \to \psi$	
2)	$\{\neg\neg\varphi\} \vdash \varphi$	podle (b) a věty o dedukci
3)	$\{\varphi \to \psi, \neg\neg\varphi\} \vdash \psi$	MP na 2), 1)
4)	$\vdash \psi \to \neg\neg\psi$	podle (c)
5)	$\{\varphi \to \psi, \neg\neg\varphi\} \vdash \neg\neg\psi$	MP na 3), 4)
6)	$\{\varphi \to \psi\} \vdash \neg\neg\varphi \to \neg\neg\psi$	věta o dedukci
7)	$\vdash (\neg\neg\varphi \to \neg\neg\psi) \to (\neg\psi \to \neg\varphi)$	$A3$
8)	$\{\varphi \to \psi\} \vdash \neg\psi \to \neg\varphi$	MP na 6), 7)
9)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	věta o dedukci

- (e): Platí

1)	$\{\varphi, \varphi \to \psi\} \vdash \psi$	
2)	$\{\varphi\} \vdash (\varphi \to \psi) \to \psi$	věta o dedukci
3)	$\vdash ((\varphi \to \psi) \to \psi) \to (\neg\psi \to \neg(\varphi \to \psi))$	podle (d)
4)	$\{\varphi\} \vdash \neg\psi \to \neg(\varphi \to \psi)$	MP na 2), 3)
5)	$\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$	věta o dedukci

Výroková logika. Věta o úplnosti. (4)

- (f): Platí

1)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi))$	podle (d)
2)	$\{\varphi \to \psi, \neg\psi\} \vdash \neg\varphi$	2x MP na 1)
3)	$\{\varphi \to \psi, \neg\psi, \neg\varphi \to \psi\} \vdash \psi$	MP na 2), $\neg\varphi \to \psi$
4)	$\{\varphi \to \psi, \neg\varphi \to \psi\} \vdash \neg\psi \to \psi$	věta o dedukci
5)	$\vdash \neg\psi \to (\neg\psi \to \neg(\neg\psi \to \psi))$	podle (e)
6)	$\{\neg\psi\} \vdash \neg(\neg\psi \to \psi)$	2x věta o dedukci
7)	$\vdash \neg\psi \to \neg(\neg\psi \to \psi)$	věta o dedukci
8)	$\vdash (\neg\psi \to \neg(\neg\psi \to \psi)) \to ((\neg\psi \to \psi) \to \psi)$	$A3$
9)	$\vdash (\neg\psi \to \psi) \to \psi$	MP na 7), 8)
10)	$\{\varphi \to \psi, \neg\varphi \to \psi\} \vdash \psi$	MP na 4), 9)
11)	$\vdash (\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$	2x věta o dedukci

□

Výroková logika. Věta o úplnosti. (5)

Definice 38

Nechť v je valuace a φ formule. Jestliže $v(\varphi) = 1$, označuje symbol φ^v formuli φ. Jinak φ^v označuje formuli $\neg\varphi$.

Lema 39 (A. Church)

Nechť v je valuace, φ formule, a $\{X_1, \cdots, X_k\}$ konečný soubor výrokových proměnných, kde všechny proměnné vyskytující se ve φ jsou mezi $\{X_1, \cdots, X_k\}$. Pak $\{X_1^v, \cdots, X_k^v\} \vdash \varphi^v$.

Důkaz. Indukcí ke složitosti φ.

- Je-li $\varphi = X$, pak X je mezi $\{X_1, \cdots, X_k\}$ a tedy $\{X_1^v, \cdots, X_k^v\} \vdash X^v$.
- Je-li $\varphi = \neg\psi$, kde $\{X_1^v, \cdots, X_k^v\} \vdash \psi^v$, rozlišíme dvě možnosti:
  - $v(\psi) = 0$. Pak $\psi^v = \neg\psi$ a $\varphi^v = \neg\psi$, není co dokazovat.
  - $v(\psi) = 1$. Pak $\psi^v = \psi$ a $\varphi^v = \neg\neg\psi$. Podle *lematu 37 (c)* platí $\vdash \psi \to \neg\neg\psi$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \neg\neg\psi$ užitím MP.

Výroková logika. Věta o úplnosti. (6)

- Je-li $\varphi = \psi \to \xi$, kde $\{X_1^v, \cdots, X_k^v\} \vdash \psi^v$ a $\{X_1^v, \cdots, X_k^v\} \vdash \xi^v$ rozlišíme následující možnosti:
  - $v(\psi \to \xi) = 1$. Máme tedy dokázat, že $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$.
    - Jestliže $v(\psi) = 0$, platí $\{X_1^v, \cdots, X_k^v\} \vdash \neg\psi$. Podle *lematu 37 (a)* dále platí $\vdash \neg\psi \to (\psi \to \xi)$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$ užitím MP.
    - Jestliže $v(\xi) = 1$, platí $\{X_1^v, \cdots, X_k^v\} \vdash \xi$. Podle A1 platí $\vdash \xi \to (\psi \to \xi)$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \psi \to \xi$ užitím MP.
  - $v(\psi \to \xi) = 0$. Pak $\{X_1^v, \cdots, X_k^v\} \vdash \psi$ a $\{X_1^v, \cdots, X_k^v\} \vdash \neg\xi$. Máme dokázat, že $\{X_1^v, \cdots, X_k^v\} \vdash \neg(\psi \to \xi)$. Podle *lematu 37 (e)* platí $\vdash \psi \to (\neg\xi \to \neg(\psi \to \xi))$, proto $\{X_1^v, \cdots, X_k^v\} \vdash \neg(\psi \to \xi)$ opakovaným užitím MP.

□

Výroková logika. Věta o úplnosti. (7)

Věta 40 (o úplnosti)

Nechť φ je formule a T soubor formulí. Jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Důkaz. Nejprve uvážíme případ, kdy T je *prázdný* soubor. Nechť φ je tautologie a $X_1, \cdots, X_k$ všechny výrokové proměnné, které se ve φ vyskytují.

- Podle Churchova lematu platí $\{X_1^v, \cdots, X_k^v\} \vdash \varphi$ pro *libovolné* v.
- Ukážeme, že všechny X_i^v lze postupně „eliminovat“, až dostaneme důkaz φ z prázdného souboru formulí.

Předpokládejme, že pro dané $0 \leq n < k$ jsme již prokázali, že

$$\{X_1^v, \cdots, X_n^v, X_{n+1}^v\} \vdash \varphi$$

pro *libovolné* v. Dokážeme, že pak také $\{X_1^u, \cdots, X_n^u\} \vdash \varphi$ pro libovolné u.

Výroková logika. Věta o úplnosti. (8)

Buď tedy u libovolná valuace. Nechť u_1, u_2 jsou valuace definované takto:

- $u_1(X_{n+1}) = 1$, $u_2(X_{n+1}) = 0$
- pro každé $Y \neq X_{n+1}$ platí $u_1(Y) = u_2(Y) = u(Y)$.

Platí

1)	$\{X_1^u, \cdots, X_n^u, X_{n+1}\} \vdash \varphi$	předpoklad pro $v = u_1$
2)	$\{X_1^u, \cdots, X_n^u, \neg X_{n+1}\} \vdash \varphi$	předpoklad pro $v = u_2$
3)	$\{X_1^u, \cdots, X_n^u\} \vdash X_{n+1} \to \varphi$	věta o dedukci na 1)
4)	$\{X_1^u, \cdots, X_n^u\} \vdash \neg X_{n+1} \to \varphi$	věta o dedukci na 2)
5)	$\vdash (X_{n+1} \to \varphi) \to ((\neg X_{n+1} \to \varphi) \to \varphi)$	podle *lematu 37 (f)*
6)	$\{X_1^u, \cdots, X_n^u\} \vdash \varphi$	2x MP na 5) s využitím 3), 4)

Výroková logika. Věta o úplnosti. (9)

Nyní uvážíme obecný případ. Buď T *libovolný* soubor formulí a φ formule taková, že $T \models \varphi$. Podle věty o kompaktnosti existuje konečný soubor $\{\psi_1, \cdots, \psi_n\}$ formulí z T takový, že $\{\psi_1, \cdots, \psi_n\} \models \varphi$. Lehce se ověří, že

$$\models \psi_1 \to (\psi_2 \to (\psi_3 \to \cdots (\psi_n \to \varphi) \cdots))$$

Podle předchozího bodu tedy platí

$$\vdash \psi_1 \to (\psi_2 \to (\psi_3 \to \cdots (\psi_n \to \varphi) \cdots))$$

Po n aplikacích věty o dedukci dostáváme $\{\psi_1, \cdots, \psi_n\} \vdash \varphi$, tedy také $T \vdash \varphi$. □

Výroková logika. Historické poznámky.

- Výroková logika nebyla rozvíjena samostatně, ale jako součást složitějších formálních systémů.
- *Gottlob Frege* (1848–1925) položil základy predikátové logiky a zavedl „moderní“ odvozovací systém. „Výrokový fragment“ tohoto systému vypadá takto (verze z roku 1879):
  - 1: $P \to (Q \to P)$
  - 2: $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
  - 3: $(P \to (Q \to R)) \to (Q \to (P \to R))$
  - 4: $(P \to Q) \to (\neg Q \to \neg P)$
  - 5: $\neg\neg P \to P$
  - 6: $P \to \neg\neg P$
  - Odvozovací pravidla: MP a substituce

  Fregeho výsledky byly vědeckou komunitou ignorovány zhruba 20 let.

Výroková logika. Historické poznámky. (2)

- Giuseppe Peano (1858-1932) doporučil na mezinárodním matematickém kongresu v Paříži (rok 1900) mladému *Bertrandu Russellovi* (1872-1970) studovat Fregeho práce. Russell v roce 1901 objevil inkonzistenci ve Fregeho systému (Russellův paradox), současně plně docenil Fregeho myšlenky. V letech 1910-1913 byla publikována třídílná *Principia Mathematica* (autoři Whitehead, Russell). Tato monografie měla hluboký vliv na vývoj logiky v následujících desetiletích. Věnována byla Fregemu. Pro fragment výrokové logiky byly použity následující axiómy a odvozovací pravidla:
  - 1: $(P \vee P) \to P$
  - 2: $Q \to (P \vee Q)$
  - 3: $(P \vee Q) \to (Q \vee P)$
  - 4: $(P \vee (Q \vee R)) \to (Q \vee (P \vee R))$
  - 5: $(Q \to R) \to ((P \vee Q) \to (P \vee R))$
  - Odvozovací pravidla: MP a substituce

Výroková logika. Historické poznámky. (3)

- V roce 1917 nalezl Jean Nicod následující zjednodušení axiomatického systému z *Principia Mathematica*:
  - 1: $(P \vee P) \rightarrow P$
  - 2: $P \rightarrow (P \vee Q)$
  - 4: $(P \vee (Q \vee R)) \rightarrow (Q \vee (P \vee R))$
  - 5: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
  - Odvozovací pravidla: MP a substituce

Výroková logika. Historické poznámky. (4)

- Ve stejném roce publikoval Henry Sheffer následující axiomatický systém založený na Shefferově operátoru:
  - Axióm: $(P|(Q|R))|((S|(S|S))|((U|Q)|((P|U)|(P|U))))$
  - Odvozovací pravidla: substituce a „z F a $F|(G|H)$ odvoď H“
- David Hilbert (1862–1943) a Wilhelm Ackermann (1896-1962) publikovali v roce 1928 následující systém:
  - 1: $(P \vee P) \rightarrow P$
  - 2: $P \rightarrow (P \vee Q)$
  - 4: $(P \vee Q) \rightarrow (Q \vee P)$
  - 5: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
  - Odvozovací pravidla: MP a substituce
- V roce 1927 navrhl John von Neumann (1903-1957) aplikovat substituci pouze na axiómy. Vznikly systémy založené na *schématech axiómů*.

Výroková logika. Historické poznámky. (5)

- Jan Lukasiewicz (1878–1956) prezentoval svůj odvozovací systém (použitý v přednášce) v roce 1928.
- Další odvozovací systémy:
  - V roce 1947 zjednodušili Götling a Rasiowa systém z *Principia Mathematica* do následující podoby:
    - 1: $(P \vee P) \rightarrow P$
    - 2: $P \rightarrow (P \vee Q)$
    - 3: $(Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow (P \vee R))$
    - Odvozovací pravidla: MP a substituce
  - V roce 1953 prezentoval Meredith systém s jediným schématem a jediným odvozovacím pravidlem:
    - Schéma axiómu: $((((\varphi \rightarrow \psi) \rightarrow (\neg\varrho \rightarrow \neg\xi)) \rightarrow \varrho) \rightarrow \gamma) \rightarrow ((\gamma \rightarrow \varphi) \rightarrow (\xi \rightarrow \varphi))$
    - Odvozovací pravidlo: MP

Predikátová logika. Vznik a vývoj.

- *Predikátová logika* (také *logika prvního řádu*) se opírá o pojem *vlastnosti* (tj. *predikátu*). Umožňuje formulovat tvrzení o vlastnostech objektů s využitím *kvantifikátorů*.
- Např. Aristotelova logika je z dnešního pohledu fragmentem predikátové logiky.
- Formule prvního řádu byly součástí Fregeho systému, později se objevily ve 3. dílu Schröderovy monografie *Algebra der Logik* (1910) a monografii *Principia Mathematica* (Whitehead, Russel).
- Logika prvního řádu byla definována jako samostatný systém až v monografii Hilberta a Ackermanna *Grundzügen der theoretischen Logik* (1928).

Predikátová logika. Syntaxe.

Definice 41

Jazyk (stejně jako jazyk s rovností) je systém predikátových symbolů a funkčních symbolů, kde u každého symbolu je dána jeho četnost (arita), která je nezáporným celým číslem. Jazyk bez rovnosti musí obsahovat alespoň jeden predikátový symbol.

Poznámka 42

- Predikáty arity nula v jistém smyslu odpovídají *výrokovým proměnným*, funkční symboly arity nula jsou symboly pro *konstanty*.
- Predikátovým a funkčním symbolům se také říká *mimologické symboly*. Jazyk je tedy plně určen mimologickými symboly.
- Rozdíl mezi *jazykem* a *jazykem s rovností* se projeví v tom, že do predikátové logiky pro jazyk s rovností přidáme speciální logický symbol $=$ jehož sémantika bude definována speciálním způsobem.

Predikátová logika. Syntaxe. (2)

Příklad 43

- Jazyk *teorie množin* je jazykem s rovností, který obsahuje jeden predikátový symbol $\in$ arity 2.
- Jazyk *teorie pologrup* je jazykem s rovností, který obsahuje jeden funkční symbol „$\cdot$“ arity 2.

Definice 44

Abecedu predikátové logiky pro jazyk $\mathcal{L}$ tvoří následující symboly:

- *Znaky pro proměnné $x, y, z, \ldots$, kterých je spočetně mnoho*
- *Mimologické symboly, tj. predikátové a funkční symboly jazyka $\mathcal{L}$.*
- *Je-li $\mathcal{L}$ jazyk s rovností, obsahuje abeceda speciální znak $=$ pro rovnost.*
- *Logické spojky $\rightarrow$ a $\neg$.*
- *Symbol $\forall$ pro univerzální kvantifikátor.*
- *Čárka , a závorky (a).*

Predikátová logika. Syntaxe. (3)

Definice 45

Termem jazyka $\mathcal{L}$ je slovo t nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $t_1, \cdots, t_k$, kde $k \geq 1$, t_k je t, a pro každé $1 \leq i \leq k$ má slovo t_i jeden z následujících tvarů:

- *proměnná,*
- *$f(t_{i_1}, \cdots, t_{i_n})$, kde $1 \leq i_1, \cdots, i_n < k$, f je funkční symbol jazyka $\mathcal{L}$, a n je arita f.*

Term je uzavřený, jestliže neobsahuje proměnné.

Poznámka 46

U binárních funkčních symbolů (a později také predikátů) dovolíme pro větší čitelnost infixový zápis. U funkčních (a predikátových) symbolů arity nula budeme psát c místo $c()$.

Predikátová logika. Syntaxe. (4)

Příklad 47

- $(x \cdot y) \cdot z$ je termem jazyka pologrup (v prefixové notaci $\cdot(\cdot(x, y), z)$)
- $0 + (S(0) + S(S(0)))$ je termem jazyka $0, S, +$, kde 0, S a $+$ jsou po řadě funkční symboly arity nula, jedna a dva.

Predikátová logika. Syntaxe. (5)

Definice 48

Formule predikátového počtu jazyka $\mathcal{L}$ *je slovo* φ *nad abecedou predikátové logiky pro jazyk* $\mathcal{L}$, *pro které existuje vytvořující posloupnost slov* $\psi_1, \cdots, \psi_k$, *kde* $k \geq 1$, ψ_k *je* φ, *a pro každé* $1 \leq i \leq k$ *má slovo* ψ_i *jeden z následujících tvarů:*

- $P(t_1, \cdots, t_n)$, *kde* P *je predikátový symbol jazyka* $\mathcal{L}$ *arity* n *a* $t_1, \cdots, t_n$ *jsou termy jazyka* $\mathcal{L}$.
- $t_1 = t_2$, *je-li* $\mathcal{L}$ *jazyk s rovností a* t_1, t_2 *jsou termy jazyka* $\mathcal{L}$.
- $\neg\psi_j$ *pro nějaké* $1 \leq j < i$,
- $(\psi_j \to \psi_{j'})$ *pro nějaká* $1 \leq j, j' < i$,
- $\forall x\, \psi_j$, *kde* x *je proměnná a* $1 \leq j < i$.

Predikátová logika. Syntaxe. (6)

Poznámka 49

Ve zbytku přednášky budeme používat následující „zkratky“:

- $\exists x\, \varphi$ značí $\neg\forall x\, \neg\varphi$
- $\varphi \vee \psi$ značí $\neg\varphi \to \psi$
- $\varphi \wedge \psi$ značí $\neg(\varphi \to \neg\psi)$.
- $\varphi \leftrightarrow \psi$ značí $(\varphi \to \psi) \wedge (\psi \to \varphi)$, kde symbol $\wedge$ dále „rozvineme“ podle předchozího bodu.

Příklady formulí:

- $\forall x\, P(x, y) \wedge \exists x\, (P(x, x) \vee Q(c))$
- $\forall x\, \exists x\, (P(x, x) \vee \forall y\, \forall x\, Q(x))$

Predikátová logika. Syntaxe. (7)

Definice 50

Každý výskyt proměnné ve formuli predikátového počtu je buď volný nebo vázaný podle následujícího induktivního předpisu:

- *Ve formuli tvaru* $P(t_1, \cdots, t_n)$ *nebo* $t_1 = t_2$ *jsou všechny výskyty proměnných volné.*
- *Výrokové spojky nemění charakter výskytů proměnných, tj. je-li daný výskyt proměnné ve formuli* ψ *volný (resp. vázaný), je odpovídající výskyt ve formulích* $\neg\psi$, $\varphi \to \psi$, $\psi \to \varphi$ *rovněž volný (resp. vázaný).*
- *Ve formuli* $\forall x\, \psi$ *je každý výskyt proměnné* x *(včetně výskytu za kvantifikátorem) vázaný; byl-li výskyt proměnné různé od* x *volný (resp. vázaný) ve formuli* ψ*, je odpovídající výskyt ve formuli* $\forall x\, \psi$ *rovněž volný (resp. vázaný).*

Příklady (volné výskyty jsou červené):

- $\forall x\, P(x, y) \vee \forall y\, P(x, y)$
- $\forall x\, (P(x, y) \vee \forall y\, P(x, y))$

Predikátová logika. Syntaxe. (8)

Definice 51

- *Proměnná se nazývá volnou (resp. vázanou) ve formuli, má-li v ní volný (resp. vázaný) výskyt.*
- *Formule je uzavřená (také sentence), jestliže v ní žádná proměnná nemá volný výskyt.*
- *Zápis* $\varphi(x_1, \cdots, x_n)$ *značí, že všechny volné proměnné ve formuli* φ *jsou mezi* $x_1, \cdots, x_n$ *(nemusí nutně platit, že každá z těchto proměnných je volná ve* φ*).*
- *Univerzální uzávěr formule* φ *je formule tvaru* $\forall\, x_1 \cdots \forall\, x_n\, \varphi$*, kde* $x_1, \cdots, x_n$ *jsou právě všechny volné proměnné formule* φ*.*

Predikátová logika. Substituce.

Definice 52

Term t je substituovatelný za proměnnou x ve formuli φ, jestliže žádný výskyt proměnné v termu t se nestane vázaným po provedení substituce termu t za každý volný výskyt proměnné x ve formuli φ. Je-li t substituovatelný za x ve φ, značí zápis $\varphi(x/t)$ formuli, která vznikne nahrazením každého volného výskytu x ve φ termem t.

Příklady:

- Term $y+3$ je substituovatelný za x ve formuli $\exists z\, x{+}y{=}z$
- Term $y+z$ není substituovatelný za x ve formuli $\exists z\, x{+}y{=}z$
- $(P(x,y) \wedge \forall x\, P(x,y))(x/3)$ je formule $P(3,y) \wedge \forall x\, P(x,y)$
- $P(x,y)(x/y)(y/x)$ je formule $P(x,x)$

Predikátová logika. Substituce. (2)

Definice 53

Nechť φ je formule a $t_1, \cdots, t_n$ termy, které jsou v uvedeném pořadí substituovatelné za proměnné $x_1, \cdots, x_n$ ve φ (předpokládáme, že $x_1, \cdots, x_n$ jsou různé). Symbol $\varphi(x_1/t_1, \cdots, x_n/t_n)$ značí formuli, která vznikne „simultánním nahrazením“ každého volného výskytu x_i termem t_i pro každé $1 \leq i \leq n$. Přesněji, $\varphi(x_1/t_1, \cdots, x_n/t_n)$ je formule $\varphi(x_1/z_1)\cdots(x_n/z_n)(z_1/t_1)\cdots(z_n/t_n)$, kde $z_1, \cdots, z_n$ jsou (různé) proměnné, které se nevyskytují v $t_1, \cdots, t_n$ ani mezi $x_1, \cdots, x_n$.

Příklad:

- $P(x,y)(x/y, y/x)$ je formule $P(y,x)$

Predikátová logika. Realizace jazyka.

Definice 54

Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je zadána

- *neprázdným souborem M, nazývaným univerzem (případně nosičem). Prvky univerza nazýváme individui.*
- *přiřazením, které každému n-árnímu predikátovému symbolu P přiřadí n-ární relaci $P_{\mathcal{M}}$ na M*
- *přiřazením, které každému m-árnímu funkčnímu symbolu přiřadí funkci $f_{\mathcal{M}} : M^m \to M$.*

Ohodnocení je zobrazení přiřazující proměnným prvky univerza M.

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Predikátová logika. Realizace jazyka. (2)

Definice 55

Realizaci termu t při ohodnocení e v relizaci $\mathcal{M}$, psáno $t^{\mathcal{M}}[e]$ (případně jen $t[e]$, je-li $\mathcal{M}$ jasné z kontextu), definujeme induktivně takto:

- $x[e] = e(x)$
- $f(t_1, \cdots, t_m)[e] = f_{\mathcal{M}}(t_1[e], \cdots, t_m[e])$
  (pro $m = 0$ je na pravé straně uvedené definující rovnosti $f_{\mathcal{M}}(\emptyset)$).

Predikátová logika. Realizace jazyka. (3)

Definice 56 (A. Tarski)

Buď $\mathcal{M}$ realizace $\mathcal{L}$, e ohodnocení a φ formule predikátového počtu jazyka $\mathcal{L}$. Ternární vztah $\mathcal{M} \models \varphi[e]$ definujeme indukcí ke složitosti φ:

- $\mathcal{M} \models P(t_1, \cdots, t_m)[e]$ *právě když* $(t_1[e], \cdots, t_m[e]) \in P_{\mathcal{M}}$.
- *Jestliže $\mathcal{L}$ je jazyk s rovností, definujeme $\mathcal{M} \models (t_1 = t_2)[e]$ právě když $t_1[e]$ a $t_2[e]$ jsou stejná individua.*
- $\mathcal{M} \models \neg\psi[e]$ *právě když není* $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models (\psi \to \xi)[e]$ *právě když* $\mathcal{M} \models \xi[e]$ *nebo není* $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models \forall x\, \psi[e]$ *právě když* $\mathcal{M} \models \psi[e(x/a)]$ *pro každý prvek a univerza M (kde $[e(x/a)]$ je funkce, která pro x vrací a a pro ostatní argumenty stejnou hodnotu jako e).*

Jestliže $\mathcal{M} \models \varphi[e]$, říkáme, že φ je pravdivá v $\mathcal{M}$ při ohodnocení e. Jestliže $\mathcal{M} \models \varphi[e]$ pro každé e, je φ pravdivá v $\mathcal{M}$, psáno $\mathcal{M} \models \varphi$.

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Predikátová logika. Realizace jazyka. (4)

Příklad 57

Buď $\mathcal{L}$ jazyk s jedním unárním predikátem P a $\mathcal{M}$ jeho realizace nad univerzem $M = \{a, b\}$, kde $P_{\mathcal{M}} = \{a\}$. Pak

- Platí $\mathcal{M} \models \exists x\, (P(x) \to (P(x) \wedge \neg P(x)))$
- Neplatí $\mathcal{M} \models P(x) \to \forall x\, P(x)$
- Neplatí $\mathcal{M} \models (\forall x\, P(x) \to \forall x\, \neg P(x)) \to \forall x\, (P(x) \to \neg P(x))$

Predikátová logika. Lema o substituci.

Podmínka substituovatelnosti je klíčová pro důkaz následujícího tvrzení, které využijeme v důkazu *věty 78*.

Lema 58 (O substituci)

Nechť φ je formule jazyka a $\mathcal{L}$ a t term substituovatelný za x ve φ. Pak pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ a ohodnocení e platí $\mathcal{M} \models \varphi[e(x/t[e])]$ právě když $\mathcal{M} \models \varphi(x/t)[e]$.

Důkaz. Indukcí ke složitosti φ.

- $\mathcal{M} \models P(t_1, \ldots, t_m)[e(x/t[e])]$ právě když $(t_1[e(x/t[e])], \ldots, t_m[e(x/t[e])]) \in P_{\mathcal{M}}$ právě když $(t_1(x/t)[e], \ldots, t_m(x/t)[e]) \in P_{\mathcal{M}}$ právě když $\mathcal{M} \models P(t_1(x/t), \ldots, t_m(x/t))[e]$ právě když $\mathcal{M} \models P(t_1, \ldots, t_m)(x/t)[e]$.
- Jestliže $\mathcal{L}$ je jazyk s rovností, platí $\mathcal{M} \models (t_1 = t_2)[e(x/t[e])]$ právě když $t_1[e(x/t[e])]$ a $t_2[e(x/t[e])]$ jsou stejná individua. Jelikož $t_1[e(x/t[e])]$ a $t_1(x/t)[e]$ jsou stejná individua a rovněž $t_2[e(x/t[e])]$ a $t_2(x/t)[e]$ jsou stejná individua, platí $\mathcal{M} \models (t_1 = t_2)[e(x/t[e])]$ právě když $\mathcal{M} \models ((t_1 = t_2)(x/t))[e]$.

Predikátová logika. Lema o substituci. (2)

- $\mathcal{M} \models \neg\psi[e(x/t[e])]$ právě když $\mathcal{M} \not\models \psi[e(x/t[e])]$ právě když (I.P.) $\mathcal{M} \not\models \psi(x/t)[e]$ právě když $\mathcal{M} \models \neg\psi(x/t)[e]$.
- $\mathcal{M} \models (\psi \to \xi)[e(x/t[e])]$ právě když $\mathcal{M} \models \xi[e(x/t[e])]$ nebo $\mathcal{M} \not\models \psi[e(x/t[e])]$ právě když (I.P.) $\mathcal{M} \models \xi(x/t)[e]$ nebo $\mathcal{M} \not\models \psi(x/t)[e]$ právě když $\mathcal{M} \models (\psi(x/t) \to \xi(x/t))[e]$ právě když $\mathcal{M} \models (\psi \to \xi)(x/t)[e]$.
- $\mathcal{M} \models \forall y\, \psi[e(x/t[e])]$ právě když pro každý prvek a univerza M platí $\mathcal{M} \models \psi[e(x/t[e])(y/a)]$. Jelikož t je substituovatelný za x, proměnná y se v termu t nevyskytuje. Ohodnocení $e(x/t[e])(y/a)$ je tedy přesně stejné jako ohodnocení $e(y/a)(x/t[e(y/a)])$. Proto pro libovolné a platí $\mathcal{M} \models \psi[e(x/t[e])(y/a)]$ právě když pro libovolné a platí $\mathcal{M} \models \psi[e(y/a)(x/t[e(y/a)])]$. Podle I.P. je druhá podmínka ekvivalentní tomu, že pro libovolné a platí $\mathcal{M} \models \psi(x/t)[e(y/a)]$, což nastává právě když $\mathcal{M} \models \forall y\, \psi(x/t)$.

□

Predikátová logika. Teorie.

Definice 59

Buď $\mathcal{L}$ jazyk (příp. jazyk s rovností).

- *Teorie (s jazykem $\mathcal{L}$) je soubor T formulí predikátového počtu jazyka $\mathcal{L}$. Prvky T se nazývají axiómy teorie T.*
- *Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je model teorie T, psáno $\mathcal{M} \models T$, jestliže $\mathcal{M} \models \varphi$ pro každé φ z T.*
- *Teorie je splnitelná, jestliže má model.*
- *Je-li $\mathcal{M}$ realizace jazyka $\mathcal{L}$, pak $Th(\mathcal{M})$ označuje teorii tvořenou právě všemi uzavřenými formulemi, které jsou v $\mathcal{M}$ pravdivé.*
- *Formule φ je sémantickým důsledkem teorie T, psáno $T \models \varphi$, jestliže φ je pravdivá v každém modelu teorie T.*

Predikátová logika. Teorie. (2)

Příklad 60

Uvažme jazyk s rovností obsahující jeden binární funkční symbol "$\cdot$" a jednu konstantu 1. Nechť T je tvořena následujícími formulemi:

- $\forall x \forall y \forall z \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $\forall x \;\; (x \cdot 1 = x) \wedge (1 \cdot x = x)$
- $\forall x \exists y \;\; (x \cdot y = 1) \wedge (y \cdot x = 1)$

Pak formule $\forall x \forall y \;\; (x \cdot y) = (y \cdot x)$ není sémantickým důsledkem T, zatímco formule $x \cdot (1 \cdot y) = (1 \cdot x) \cdot y$ ano.

Predikátová logika. Odvozovací systém.

- Schémata *výrokových axiómů*:
  - P1: $\varphi \to (\psi \to \varphi)$
  - P2: $(\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi))$
  - P3: $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$
- Schéma *axiómu specifikace*:
  - P4: $\forall x\, \varphi \to \varphi(x/t)$, kde t je substituovatelný za x ve φ.
- Schéma *axiómu distribuce*:
  - P5: $(\forall x\, (\varphi \to \psi)) \to (\varphi \to \forall x\, \psi)$, kde x nemá volný výskyt ve φ.
- Odvozovací pravidla:
  - MP: Z φ a $\varphi \to \psi$ odvoď ψ. (*modus ponens*)
  - GEN: Z φ odvoď $\forall x\, \varphi$. (*generalizace*)

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Predikátová logika. Odvozovací systém. (2)

Je-li $\mathcal{L}$ jazyk s rovností, přidáme dále následující *axiómy rovnosti*:

- R1: $x = x$
- R2: $(x_1{=}y_1 \wedge \cdots \wedge x_n{=}y_n \wedge P(x_1, \cdots, x_n)) \to P(y_1, \cdots, y_n)$, kde P je predikátový symbol arity n.
- R3: $(x_1{=}y_1 \wedge \cdots \wedge x_m{=}y_m) \to (f(x_1, \cdots, x_m){=}f(y_1, \cdots, y_m))$, kde f je funkční symbol arity m.

Predikátová logika. Odvozovací systém. (3)

Definice 61

Buď T teorie jazyka $\mathcal{L}$. Důkaz formule ψ v teorii T je konečná posloupnost formulí $\varphi_1, \cdots, \varphi_k$, kde φ_k je ψ a pro každé φ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:

- *φ_i je prvek T;*
- *φ_i je instancí jednoho ze schémat P1–P5;*
- *$\mathcal{L}$ je jazyk s rovností a φ_i je instancí jednoho ze schémat R1–R3;*
- *φ_i vznikne aplikací MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.*
- *φ_i vznikne aplikací GEN na formuli φ_m pro vhodné $1 \leq m < i$.*

Predikátová logika. Odvozovací systém. (4)

Definice 62

Buď T teorie jazyka $\mathcal{L}$.

- *Formule ψ je dokazatelná v teorii T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ v T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme že ψ je dokazatelná a píšeme $\vdash \psi$.*
- *Formule ψ je vyvratitelná v teorii T, jestliže $T \vdash \neg\psi$*
- *Teorie T je sporná (též inkonzistentní), jestliže každá formule predikátové logiky jazyka $\mathcal{L}$ je v T dokazatelná.*
- *Teorie je bezesporná (též konzistentní), jestliže není nekonzistentní.*

Poznámka 63

Jelikož pro libovolné formule φ, ψ platí $\{\varphi, \neg\varphi\} \vdash \psi$ (Příklad 34), je teorie T sporná právě když $T \vdash \varphi$ a $T \vdash \neg\varphi$ pro nějakou formuli φ.

Predikátová logika. Důkazy.

Poznámka 64 (Princip dosazení do tautologie výrokového počtu)

Je-li φ tautologií $\mathcal{L}(\neg, \rightarrow)$, ve které nahradíme výrokové proměnné formulemi predikátové logiky tak, že daná výroková proměnná je nahrazena vždy *touž* formulí, obdržíme formuli predikátové logiky, která je dokazatelná v odvozovacím systému predikátové logiky pouze pomocí P1–P3 a MP.

Poznámka 65 (Neplatnost „obecné“ věty o dedukci)

Za předpokladu korektnosti odvozovacího systému pro predikátovou logiku neplatí $\vdash \varphi \rightarrow \forall x\, \varphi$. Platí ovšem $\{\varphi\} \vdash \forall x\, \varphi$. Proto *obecně neplatí*, že $T \models \varphi \rightarrow \psi$ právě když $T \cup \{\varphi\} \models \psi$.

Predikátová logika. Věta o dedukci.

Věta 66 (o dedukci)

Nechť T je teorie jazyka $\mathcal{L}$, ψ uzavřená formule jazyka $\mathcal{L}$ a φ (libovolná) formule jazyka $\mathcal{L}$. Pak $T \vdash \psi \rightarrow \varphi$ právě když $T \cup \{\psi\} \vdash \varphi$.

Důkaz. Důkaz je velmi podobný důkazu *věty 35*:

„$\Rightarrow$“: Nechť $\xi_1, \cdots, \xi_k$ je důkaz formule $\psi \rightarrow \varphi$ v T. Pak $\xi_1, \cdots, \xi_k, \psi, \varphi$ je důkaz φ v $T \cup \{\psi\}$ (poslední formule vznikne aplikací MP na ψ a ξ_k).

„$\Leftarrow$“: Nechť $\xi_1, \cdots, \xi_k$ je důkaz φ v $T \cup \{\psi\}$. Metaindukcí k j dokážeme, že $T \vdash \psi \rightarrow \xi_j$ pro každé $1 \leq j \leq k$.

- $j = 1$. Je-li ξ_1 instance axiómu nebo formule z T, platí $T \vdash \xi_1$. K důkazu ξ_1 z T nyní připojíme formule $\xi_1 \rightarrow (\psi \rightarrow \xi_1)$, $\psi \rightarrow \xi_1$. První formule je instancí P1, druhá aplikací MP na ξ_1 a první formuli. Máme tedy důkaz $\psi \rightarrow \xi_1$ v T. Je-li ξ_1 formule ψ, platí $T \vdash \psi \rightarrow \psi$ podle *příkladu 33* a *poznámky 64*.
- *Indukční krok:* Je-li formule ξ_j instancí axiómu nebo prvek $T \cup \{\psi\}$, postupujeme stejně jako výše (místo ξ_1 použijeme ξ_j).

Predikátová logika. Věta o dedukci. (2)

- Je-li ξ_j výsledkem aplikace MP na ξ_m, ξ_n, kde $1 \leq m, n < j$, je ξ_n tvaru $\xi_m \to \xi_j$. Podle I.P. navíc platí $T \vdash \psi \to \xi_m$ a $T \vdash \psi \to (\xi_m \to \xi_j)$. Důkazy $\psi \to \xi_m$ a $\psi \to (\xi_m \to \xi_j)$ v T nyní zřetězíme za sebe a připojíme následující formule:
  - $(\psi \to (\xi_m \to \xi_j)) \to ((\psi \to \xi_m) \to (\psi \to \xi_j))$
  - $(\psi \to \xi_m) \to (\psi \to \xi_j)$
  - $\psi \to \xi_j$

  První formule je instancí P2, další dvě vzniknou aplikací MP. Máme tedy důkaz formule $\psi \to \xi_j$ v T.
- Je-li ξ_j výsledkem aplikace GEN na ξ_m, kde $1 \leq m < j$, je ξ_j tvaru $\forall x\, \xi_m$. Podle I.P. platí $T \vdash \psi \to \xi_m$. K tomuto důkazu nyní stačí připojit formule
  - $\forall x\, (\psi \to \xi_m)$
  - $\forall x\, (\psi \to \xi_m) \to (\psi \to \forall x\, \xi_m)$
  - $\psi \to \forall x\, \xi_m$.

  První vznikne aplikací GEN, druhá je instancí P5, třetí vznikne aplikací MP. Dostaneme tak důkaz formule $\psi \to \xi_j$ v T. □

Predikátová logika. Kvantifikace.

Lema 67

Pro každé formule φ a ψ platí:

1. $\vdash (\forall x\, (\varphi \to \psi)) \leftrightarrow (\varphi \to \forall x\, \psi)$, *pokud x není volná ve formuli φ;*
2. $\vdash (\forall x\, (\varphi \to \psi)) \leftrightarrow (\exists x\, \varphi \to \psi)$, *pokud x není volná ve formuli ψ;*
3. $\vdash (\exists x\, (\varphi \to \psi)) \leftrightarrow (\varphi \to \exists x\, \psi)$, *pokud x není volná ve formuli φ;*
4. $\vdash (\exists x\, (\varphi \to \psi)) \leftrightarrow (\forall x\, \varphi \to \psi)$, *pokud x není volná ve formuli ψ.*

Důkaz. Pozorování:

(a) Jestliže $\vdash \varphi \to \psi$ a současně $\vdash \psi \to \varphi$, pak $\vdash \varphi \leftrightarrow \psi$. To plyne z toho, že $(A \to B) \to ((B \to A) \to (A \leftrightarrow B))$ je výroková tautologie (viz *poznámka 64*).

(b) (tranzitivita implikace). Jestliže $T \vdash \varphi \to \xi$ a současně $T \vdash \xi \to \psi$, pak $T \vdash \varphi \to \psi$. Stačí použít *poznámku 64* a tautologii $(A \to C) \to ((C \to B) \to (A \to B))$.

Predikátová logika. Kvantifikace. (2)

(c) Nechť $\varphi(x)$, $\psi(x)$ jsou formule. Pak $\vdash \forall x\,(\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$, neboť

1)	$\vdash \forall x\,(\varphi \to \psi) \to (\varphi \to \psi)$	*P*4
2)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	výr. tautologie
3)	$\vdash \forall x\,(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	tranz. impl. na 1), 2)
4)	$\forall x\,(\varphi \to \psi) \vdash \neg\psi \to \neg\varphi$	věta o dedukci
5)	$\forall x\,(\varphi \to \psi) \vdash \forall x\,(\neg\psi \to \neg\varphi)$	GEN
6)	$\vdash \forall x\,(\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$	věta o dedukci

Predikátová logika. Kvantifikace. (3)

Tvrzení 1.–4. teď dokážeme za předpokladu, že $\varphi(x)$ a $\psi(x)$. Obecná podoba vyplyne užitím věty konstantách (viz dále).

1. Platí $\vdash (\forall x\,(\varphi \to \psi)) \to (\varphi \to \forall x\,\psi)$, neboť tato formule je instancí P5. Důkaz opačné implikace vypadá takto:

1)	$\vdash \forall x\,\psi \to \psi$	*P*4
2)	$\vdash (\forall x\,\psi \to \psi) \to ((\varphi \to \forall x\,\psi) \to (\varphi \to \psi))$	$(A \to B) \to ((C \to A) \to (C \to B))$ je tautologie, viz *pozn. 64*
3)	$\vdash (\varphi \to \forall x\,\psi) \to (\varphi \to \psi)$	MP na 1), 2)
4)	$\varphi \to \forall x\,\psi \vdash \varphi \to \psi$	věta o dedukci
5)	$\varphi \to \forall x\,\psi \vdash \forall x\,(\varphi \to \psi)$	*GEN*
6)	$\vdash (\varphi \to \forall x\,\psi) \to (\forall x\,(\varphi \to \psi))$	věta o dedukci

Predikátová logika. Kvantifikace. (4)

2. Nejprve ukážeme, že $\vdash \forall x\,(\varphi \to \psi) \to (\exists x\,\varphi \to \psi)$.

1)	$\vdash \forall x\,(\neg\psi \to \neg\varphi) \to (\neg\psi \to \forall x\,\neg\varphi)$	podle 1.
2)	$\vdash \forall x\,(\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$	podle (c)
3)	$\vdash \forall x\,(\varphi \to \psi)) \to (\neg\psi \to \forall x\,\neg\varphi)$	tranz. impl. na 2), 1)
4)	$\vdash (\neg\psi \to \forall x\,\neg\varphi) \to (\neg\forall x\,\neg\varphi \to \psi)$	taut. $(\neg B \to A) \to (\neg A \to B)$
5)	$\vdash \forall x\,(\varphi \to \psi) \to (\neg\forall x\,\neg\varphi \to \psi)$	tranz. impl. na 3), 4)
6)	$\vdash \forall x\,(\varphi \to \psi) \to (\exists x\,\varphi \to \psi)$	reformulace

Nyní opačný směr $\vdash (\exists x\,\varphi \to \psi) \to \forall x\,(\varphi \to \psi)$:

1)	$\vdash (\neg\psi \to \forall x\,\neg\varphi) \to \forall x\,(\neg\psi \to \neg\varphi)$	podle 1.
2)	$\vdash (\neg\forall x\,\neg\varphi \to \psi) \to (\neg\psi \to \forall x\,\neg\varphi)$	taut. $(\neg B \to A) \to (\neg A \to B)$
3)	$\vdash (\neg\forall x\,\neg\varphi \to \psi) \to \forall x\,(\neg\psi \to \neg\varphi)$	tranz. impl. na 1), 2)
4)	$\exists x\,\varphi \to \psi \vdash \forall x\,(\neg\psi \to \neg\varphi)$	věta o dedukci
5)	$\exists x\,\varphi \to \psi \vdash \neg\psi \to \neg\varphi$	P4 a MP
6)	$\exists x\,\varphi \to \psi \vdash \varphi \to \psi$	$(\neg A \to \neg B) \to (B \to A)$ a MP
7)	$\exists x\,\varphi \to \psi \vdash \forall x\,(\varphi \to \psi)$	GEN
8)	$\vdash (\exists x\,\varphi \to \psi) \to \forall x\,(\varphi \to \psi)$	věta o dedukci

Predikátová logika. Věta o korektnosti.

Věta 68

Nechť T je teorie a φ formule jazyka teorie T. Jestliže $T \vdash \varphi$, pak $T \models \varphi$.

Důkaz. Stačí ověřit následující tvrzení:

- Je-li ψ instancí jednoho ze schémat P1–P5 (příp. také R1–R3, pokud jazyk teorie T je jazyk s rovností) a $\mathcal{M}$ je model T, pak $\mathcal{M} \models \psi$.
- Je-li $\mathcal{M}$ model T a ψ, ξ formule jazyka teorie T, kde $\mathcal{M} \models \psi$ a $\mathcal{M} \models \psi \to \xi$, pak $\mathcal{M} \models \xi$.
- Je-li $\mathcal{M}$ model T a ψ formule jazyka teorie T, kde $\mathcal{M} \models \psi$, pak $\mathcal{M} \models \forall x\,\psi$.

Metaindukcí vzhledem k i je pak již triviální ukázat, že je-li $\psi_1, \cdots, \psi_k$ důkaz formule φ v T a $\mathcal{M}$ je model T, pak $\mathcal{M} \models \psi_i$ pro každé $1 \le i \le k$. □

Predikátová logika. Úplnost (úvod).

Lema 69

Následující tvrzení jsou ekvivalentní:

1. *Pro každou teorii T a pro každou formuli φ jazyka teorie T platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.*
2. *Každá bezesporná teorie má model.*

Důkaz.

(1. $\Rightarrow$ 2.) Buď T bezesporná teorie. Pak existuje formule φ jazyka teorie T, která není v T dokazatelná (tj. $T \nvdash \varphi$). Obměnou 1. pak ale dostáváme, že φ není sémantickým důsledkem T (tj. $T \not\models \varphi$). To znamená, že existuje takový model T, kde není pravdivá φ. Zejména má tedy T model.

Predikátová logika. Úplnost (úvod). (2)

(2. $\Rightarrow$ 1.) Užitím 2. dokážeme obměnu 1. Nechť tedy $T \nvdash \varphi$, a nechť $\overline{\varphi}$ je univerzální uzávěr φ. Ukážeme, že $T \cup \{\neg\overline{\varphi}\}$ je bezesporná; pak podle 2. má $T \cup \{\neg\overline{\varphi}\}$ model, tedy $T \not\models \varphi$.
$T \cup \{\neg\overline{\varphi}\}$ je bezesporná: Předpokládejme naopak, že $T \cup \{\neg\overline{\varphi}\}$ je sporná. Pak

1)	$T \cup \{\neg\overline{\varphi}\} \vdash \overline{\varphi}$	$T \cup \{\neg\overline{\varphi}\}$ je sporná
2)	$T \vdash \neg\overline{\varphi} \to \overline{\varphi}$	věta o dedukci
3)	$\vdash (\neg\overline{\varphi} \to \overline{\varphi}) \to \overline{\varphi}$	$(\neg A \to A) \to A$ je tautologie, viz *pozn. 64*
4)	$T \vdash \overline{\varphi}$	MP na 2), 3)
5)	$T \vdash \varphi$	opakovaně P4 a MP

Obdrželi jsme tedy spor s tím, že $T \nvdash \varphi$.

□

Predikátová logika. Úplnost (úvod). (3)

Cílem dalšího postupu je dokázat, že každá bezesporná teorie má model. Tato konstrukce obsahuje dva základní obraty:

- Zavede se pojem *kanonické struktury* pro danou teorii T. Tato struktura obecně *není* modelem T. Ukážeme, že pokud T vyhovuje dalším podmínkám (je *henkinovská* a *úplná*), pak kanonická struktura *je* modelem T.
- Ukážeme, že každou bezespornou teorii je možné vhodným způsobem *rozšířit* tak, aby byla henkinovská a úplná.

Predikátová logika. Rozšíření teorie.

Definice 70

- *Teorie S je rozšíření teorie T, jestliže jazyk teorie S obsahuje jazyk teorie T a v teorii S jsou dokazatelné všechny axiómy teorie T.*
- *Rozšíření S teorie T se nazývá konzervativní, jestliže každá formule jazyka teorie T, která je dokazatelná v S, je dokazatelná i v T.*
- *Teorie S a T jsou ekvivalentní, jestliže S je rozšířením T a současně T je rozšířením S.*

Příklad 71

- Teorie komutativních grup je nekonzervativní rozšíření teorie grup.
- Teorie grup je nekonzervativní rozšíření teorie monoidů (tvrzení $\forall x \, \exists y \; x \cdot y = 1$ nelze dokázat v teorii monoidů).
- Gödel-Bernaysova teorie tříd je konzervativním rozšířením Zermelo-Fraenkelovy teorie množin.

Predikátová logika. Věta o konstantách.

Věta 72 (o konstantách)

Nechť S je rozšíření T vzniklé obohacením jazyka teorie T o novou konstantu c (nové axiómy nepřidáváme). Pak pro každou formuli φ jazyka teorie T a každou proměnnou x platí, že $T \vdash \varphi$ právě když $S \vdash \varphi(x/c)$.

Důkaz.

$\Rightarrow$: K důkazu φ v T připojíme formule $\forall x\,\varphi, \quad \forall x\,\varphi \to \varphi(x/c), \quad \varphi(x/c)$ a obdržíme tak důkaz formule $\varphi(x/c)$ v S.

$\Leftarrow$: Nechť $\psi_1, \cdots, \psi_k$ je důkaz $\varphi(x/c)$ v S. Nechť y je proměnná, která se nevyskytuje v tomto důkazu. Indukcí k i ukážeme, že pro každé $1 \le i \le k$ je $\psi_1(c/y), \cdots, \psi_i(c/y)$ důkaz v T (kde $\psi_j(c/y)$ označuje formuli, která vznikne z ψ_j nahrazením kostanty c proměnnou y). Rozlišíme tyto možnosti:

- Je-li ψ_i instancí P1–P5 (příp. R1–R3), je také $\psi_i(c/y)$ instancí téhož schématu.
- Je-li ψ_i axióm teorie T, pak se v ψ_i nevyskytuje c a formule ψ_i a $\psi_i(c/y)$ jsou tedy totožné.
- Jestliže ψ_i vyplývá z ψ_j a ψ_m pomocí MP, je ψ_m tvaru $\psi_j \to \psi_i$ a formule $\psi_m(c/y)$ je tedy formulí $\psi_j(c/y) \to \psi_i(c/y)$. Takže formule $\psi_i(c/y)$ vyplývá z $\psi_j(c/y)$ a $\psi_m(c/y)$ pomocí MP.

Predikátová logika. Věta o konstantách. (2)

- Jestliže ψ_i vyplývá z ψ_j pomocí GEN, je ψ_i tvaru $\forall x\,\psi_j$. Stačí si uvědomit, že $(\forall x\,\psi_j)(c/y)$ je tatáž formule jako $\forall x\,(\psi_j(c/y))$, neboť x a y jsou různé.

Ukázali jsme, že $T \vdash \varphi(x/c)(c/y)$. Dále

1)	$T \vdash \varphi(x/y)$	$\varphi(x/y)$ je totéž co $\varphi(x/c)(c/y)$
2)	$T \vdash \forall y\,\varphi(x/y)$	GEN
3)	$\vdash \forall y\,\varphi(x/y) \to (\varphi(x/y)(y/x))$	$P4$
4)	$T \vdash \varphi(x/y)(y/x)$	MP na 2), 3)
5)	$T \vdash \varphi$	$\varphi(x/y)(y/x)$ je totéž co φ

□

Predikátová logika. Henkinovské teorie.

Definice 73

- *Teorie T je henkinovská, jestliže pro každou formuli φ jazyka teorie T s jednou volnou proměnnou x existuje v jazyce teorie T konstanta c taková, že $T \vdash \exists x\, \varphi \to \varphi(x/c)$.*
- *Teorie T je úplná, jestliže je bezesporná a pro každou uzavřenou formuli φ jejího jazyka platí buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.*

Predikátová logika. Henkinovské teorie. (2)

Věta 74 (o henkinovské konstantě)

Buď T teorie a $\varphi(x)$ formule jejího jazyka. Je-li S rozšíření T, které vznikne přidáním nové konstanty c_φ a formule $\exists x\, \varphi \to \varphi(x/c_\varphi)$, pak S je konzervativní rozšíření T.

Důkaz. Nejprve ukážeme, že pro libovolnou formuli $\xi(x)$ platí $\vdash \exists x\xi \to \exists y\xi(x/y)$:

1)	$\{\forall y\neg\xi(x/y)\} \vdash \forall y\neg\xi(x/y)$	
2)	$\{\forall y\neg\xi(x/y)\} \vdash \neg\xi(x/y)(y/x)$	P4 a MP
3)	$\{\forall y\neg\xi(x/y)\} \vdash \neg\xi$	přepis
4)	$\{\forall y\neg\xi(x/y)\} \vdash \forall x\neg\xi$	GEN
5)	$\vdash \forall y\neg\xi(x/y) \to \forall x\neg\xi$	dedukce
6)	$\vdash \exists x\xi \to \exists y\xi(x/y)$	taut. $(A \to B) \to (\neg B \to \neg A)$ a MP.

Predikátová logika. Henkinovské teorie. (3)

Nechť R značí teorii vzniklou pouhým přidáním konstanty c_φ k T. Nechť ψ je formule jazyka teorie T taková, že $S \vdash \psi$. Nechť y je proměnná, která se nevyskytuje ani ve φ, ani v ψ. Platí:

1)	$S \vdash \psi$	předpoklad
2)	$R \vdash (\exists x\varphi \to \varphi(x/c_\varphi)) \to \psi$	$S = R \cup \{\exists x\varphi \to \varphi(x/c_\varphi)\}$ a dedukce
3)	$T \vdash (\exists x\varphi \to \varphi(x/y)) \to \psi$	věta o konstantách
4)	$T \vdash \forall y((\exists x\varphi \to \varphi(x/y)) \to \psi)$	GEN
5)	$T \vdash \exists y(\exists x\varphi \to \varphi(x/y)) \to \psi$	*lema 67 (2)* a MP
6)	$\vdash (\exists x\varphi \to \exists y\varphi(x/y)) \to \exists y(\exists x\varphi \to \varphi(x/y))$	*lema 67 (3)*
7)	$T \vdash (\exists x\varphi \to \exists y\varphi(x/y)) \to \psi$	tranz. implikace
8)	$\vdash \exists x\varphi \to \exists y\varphi(x/y)$	dokázáno výše
9)	$T \vdash \psi$	MP

□

Predikátová logika. Henkinovské teorie. (4)

Věta 75 (o henkinovském rozšíření)

Ke každé teorii existuje henkinovská teorie, která je jejím konzervativním rozšířením.

Důkaz. Buď T teorie. Pro každé $n \geq 0$ definujeme teorii T_n takto:

- $T_0 = T$. Teorie T_{i+1} vznikne z T_i tak, že pro každou formuli $\varphi(x)$ jazyka teorie T_i přidáme novou konstantu c_φ a formuli $\exists x\varphi \to \varphi(x/c_\varphi)$.

Metaindukcí vzhledem k n ukážeme, že T_n je konzervativní rozšíření T.

- Pro $n = 0$ není co dokazovat. V indukčním kroku si stačí uvědomit, že je-li $T_{i+1} \vdash \psi$, může být v důkazu formule ψ použito jen *konečně mnoho* axiómů $\xi_1, \cdots, \xi_k$, které nepatří do T_i. Užitím věty o henkinovské konstantě k-krát po sobě dostáváme $T_i \vdash \psi$, proto $T \vdash \psi$ podle I.P.

Uvažme teorii $S = \bigcup_{n=0}^{\infty} T_n$. Teorie S je konzervativní rozšíření T, neboť každý důkaz v S používá jen konečně mnoho axiómů a je tedy důkazem v nějaké T_m. Teorie S je zjevně henkinovská. □

Predikátová logika. Henkinovské teorie. (5)

V následující větě využíváme princip maximality (*Zornovo lema*), který říká následující:

> *Nechť $(A, \leq)$ je uspořádaná množina. Jestliže pro každý řetězec B obsažený v A existuje v A horní závora, pak $(A, \leq)$ má maximální prvek.*

Zornovo lema je ekvivalentní s *axiomem výběru*.

Predikátová logika. Henkinovské teorie. (6)

Věta 76 (o zúplňování teorií)

Ke každé bezesporné teorii existuje její rozšíření se stejným jazykem, které je úplnou teorií.

Důkaz. Buď T bezesporná teorie. Uvažme uspořádanou množinu $(\mathcal{T}, \subseteq)$, kde $\mathcal{T}$ je soubor všech bezesporných teorií obsahujících T. Nechť B je řetězec obsažený v $\mathcal{T}$ a nechť C je sjednocením všech prvků B. Pak C je horní závora B v $\mathcal{T}$. Zde je třeba ověřit, že C je skutečně bezesporná teorie (a tedy prvek $\mathcal{T}$): pokud by C byla sporná, existuje v ní důkaz kontradikce. Tento důkaz ale používá jen *konečně mnoho* axiómů, proto je důkazem i v nějaké teorii $K \in B$, tedy K je sporná, spor.

Predikátová logika. Henkinovské teorie. (7)

Podle Zornova lematu tedy existuje *maximální* bezesporná teorie $\mathcal{U}$ obsahující T. Dokážeme, že $\mathcal{U}$ je úplná. Pokud není, existuje uzavřená formule φ taková, že $\mathcal{U} \nvdash \varphi$ a současně $\mathcal{U} \nvdash \neg\varphi$. Zejména tedy $\varphi, \neg\varphi \notin \mathcal{U}$. Z maximality $\mathcal{U}$ plyne, že teorie $\mathcal{U} \cup \{\varphi\}$ i $\mathcal{U} \cup \{\neg\varphi\}$ jsou sporné, platí tedy $\mathcal{U} \cup \{\varphi\} \vdash \neg\varphi$ a $\mathcal{U} \cup \{\neg\varphi\} \vdash \varphi$. Proto také $\mathcal{U} \vdash \varphi \to \neg\varphi$ a $\mathcal{U} \vdash \neg\varphi \to \varphi$ (užitím věty o dedukci). Z toho dostáváme $\mathcal{U} \vdash \psi \wedge \neg\psi$ pro libovolné ψ, neboť $(A \to \neg A) \to ((\neg A \to A) \to (\psi \wedge \neg\psi))$ je výroková tautologie (použijeme 2x MP). Tedy $\mathcal{U}$ je sporná, spor.

Pokud je jazyk teorie T konečný nebo spočetný, lze se použití Zornova lematu snadno vyhnout. Dokazovaná věta pak žádnou formu axiómu výběru nevyužívá. □

Predikátová logika. Kanonická struktura.

Definice 77

Buď T teorie, kde jazyk teorie T obsahuje alespoň jednu konstantu. Kanonická struktura teorie T je realizace $\mathcal{M}$ jazyka teorie T, kde

- *univerzum M je tvořeno všemi uzavřenými termy jazyka teorie T;*
- *relizace funkčního symbolu f arity n je funkce $f_{\mathcal{M}}$, která uzavřeným termům $t_1, \cdots, t_n$ přiřadí uzavřený term $f(t_1, \cdots, t_n)$;*
- *realizace predikátového symbolu P arity m je predikát $P_{\mathcal{M}}$ definovaný takto: $(t_1, \cdots, t_m) \in P_{\mathcal{M}}$ platí právě když $T \vdash P(t_1, \cdots, t_m)$.*

Predikátová logika. Kanonická struktura. (2)

Věta 78 (o kanonické struktuře)

Nechť T je úplná henkinovská teorie, a nechť jazyk teorie T je jazykem bez rovnosti. Pak kanonická struktura teorie T je modelem T.

Důkaz. Nechť $\mathcal{M}$ je kanonická struktura teorie T. Ukážeme, že pro libovolnou formuli φ jazyka teorie T platí následující:

- Jestliže $\hat{\varphi}$ je uzavřená instance formule φ, pak $T \vdash \hat{\varphi}$ právě když $\mathcal{M} \models \hat{\varphi}$.

Jelikož lze (bez újmy na obecnosti) předpokládat, že prvky T jsou *uzavřené* formule, plyne z výše uvedeného, že $\mathcal{M}$ je model T.

Indukcí ke struktuře φ:

- $\varphi \equiv P(t_1, \cdots, t_n)$. Buď $P(t'_1, \cdots, t'_n)$ libovolná uzavřená instance. Podle definice kanonické struktury $\mathcal{M} \models P(t'_1, \cdots, t'_n)$ právě když $T \vdash P(t'_1, \cdots, t'_n)$.

Predikátová logika. Kanonická struktura. (3)

- $\varphi \equiv \neg\psi$. Buď $\neg\hat{\psi}$ libovolná uzavřená instance. Jelikož $\hat{\psi}$ je uzavřená instance ψ, podle IP platí $T \vdash \hat{\psi}$ právě když $\mathcal{M} \models \hat{\psi}$. Dále $T \vdash \neg\hat{\psi}$ právě když $T \nvdash \hat{\psi}$ (T je bezesporná) právě když $\mathcal{M} \not\models \hat{\psi}$ (IP) právě když $\mathcal{M} \models \neg\hat{\psi}$.
- $\varphi \equiv \psi \to \xi$. Každá uzavřená instance této formule je tvaru $\hat{\psi} \to \hat{\xi}$, kde $\hat{\psi}$ je uzavřená instance ψ a $\hat{\xi}$ je uzavřená instance ξ.
  - Nechť $T \vdash \hat{\psi} \to \hat{\xi}$. Jelikož $\hat{\psi}$ je uzavřená formule a T je uplná, platí buď $T \vdash \hat{\psi}$ nebo $T \vdash \neg\hat{\psi}$. V prvém případě dále $T \vdash \hat{\xi}$ (MP) a užitím IP celkem dostáváme $\mathcal{M} \models \hat{\psi}$ a $\mathcal{M} \models \hat{\xi}$. Proto také $\mathcal{M} \models \hat{\psi} \to \hat{\xi}$. V druhém případě $T \nvdash \hat{\psi}$ (T je bezesporná), proto $\mathcal{M} \not\models \hat{\psi}$ (IP), tudíž $\mathcal{M} \models \hat{\psi} \to \hat{\xi}$.
  - Nechť $\mathcal{M} \models \hat{\psi} \to \hat{\xi}$. Pak buď $\mathcal{M} \not\models \hat{\psi}$ nebo $\mathcal{M} \models \hat{\xi}$. V prvém případě $T \nvdash \hat{\psi}$ podle IP, tudíž $T \vdash \neg\hat{\psi}$ neboť T je úplná. Proto $T \vdash \hat{\psi} \to \hat{\xi}$ užitím tautologie $\neg A \to (A \to B)$ a MP.
    V druhém případě $T \vdash \hat{\xi}$, proto $T \vdash \hat{\psi} \to \hat{\xi}$ užitím tautologie $A \to (B \to A)$ a MP.

Predikátová logika. Kanonická struktura. (4)

- $\varphi \equiv \forall x\, \psi$. Pokud x nemá volný výskyt v ψ, má uzavřená instance formule $\forall x\, \psi$ tvar $\forall x\, \hat{\psi}$, kde $\hat{\psi}$ je uzavřená instance ψ. Pak $\mathcal{M} \models \forall x\, \hat{\psi}$ právě když $\mathcal{M} \models \hat{\psi}$ právě když $T \vdash \hat{\psi}$ (užitím IP) právě když $T \vdash \forall x\, \hat{\psi}$.

  Pokud x má volný výskyt v ψ, má uzavřená instance formule $\forall x\, \psi$ tvar $\forall x\, \bar{\psi}$, kde x je jediná volná proměnná formule $\bar{\psi}$.

  - Nechť $T \vdash \forall x\, \bar{\psi}$. Dokážeme, že $\mathcal{M} \models \forall x\, \bar{\psi}$. Buď e libovolné ohodnocení a t libovolný prvek univerza (uzavřený term). Podle *Lematu 58* platí, že $\mathcal{M} \models \bar{\psi}[e(x/t)]$ právě když $\mathcal{M} \models \bar{\psi}(x/t)[e]$ (zde využíváme i toho, že $t[e] = t$). Dále $\mathcal{M} \models \bar{\psi}(x/t)[e]$ právě když $\mathcal{M} \models \bar{\psi}(x/t)$, neboť formule $\bar{\psi}(x/t)$ je uzavřená. Podle I.P. platí $\mathcal{M} \models \bar{\psi}(x/t)$ pravě když $T \vdash \bar{\psi}(x/t)$. Jelikož $T \vdash \forall x\, \bar{\psi}$, platí také $T \vdash \bar{\psi}(x/t)$ užitím P4 a MP.
  - Nechť $T \nvdash \forall x\, \bar{\psi}$. Pak také $T \nvdash \forall x\, \neg\neg\bar{\psi}$ (kdyby $T \vdash \forall x\, \neg\neg\bar{\psi}$, dostaneme dále $T \vdash \neg\neg\bar{\psi}$ (P4 a MP) a $T \vdash \bar{\psi}$ (tautologie $\neg\neg A \to A$ a MP), $T \vdash \forall x\, \bar{\psi}$ (GEN), spor).
    Jelikož $T \nvdash \forall x \neg\neg\bar{\psi}$, platí $T \vdash \neg\forall x \neg\neg\bar{\psi}$ neboť T je úplná. Tedy $T \vdash \exists x \neg\bar{\psi}$. Jelikož T je henkinovská, platí $T \vdash \exists x \neg\bar{\psi} \to \neg\bar{\psi}(x/c)$. Tedy $T \vdash \neg\bar{\psi}(x/c)$ a proto $T \nvdash \bar{\psi}(x/c)$ neboť T je bezesporná. Podle IP $\mathcal{M} \not\models \bar{\psi}(x/c)$, tedy $\mathcal{M} \not\models \bar{\psi}[e]$, kde $e(x) = c$ (užitím *Lematu 58*). Proto $\mathcal{M} \not\models \forall x \bar{\psi}$.

□

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Predikátová logika. Kanonická struktura. (5)

Věta 79

Nechť T je úplná henkinovské teorie, a nechť jazyk teorie T je jazykem s rovností. Pak T má model.

Důkaz. Buď S teorie (s jazykem bez rovnosti), která vznikne rozšířením T o nový binární predikátový symbol $=$ a axiomy R1–R3. Symbol $=$ v teorii S je tedy *mimologický* a může být realizován „jakkoliv“. Axiomy R1–R3 jsou v S „normální“ axiómy. Stačí nám ukázat, že S má takový model, kde $=$ je realizován jako identita. Takový model pak jistě bude i modelem T (kde $=$ je chápáno jako logický symbol).

Predikátová logika. Kanonická struktura. (6)

Buď $\mathcal{M}$ kanonická struktura teorie S, a nechť $\sim$ je realizace $=$ v S (tj. $t_1 \sim t_2$ právě když $S \vdash t_1 = t_2$). Dokážeme, že $\sim$ je nutně ekvivalence:

- reflexivita: $S \vdash x{=}x$ (R1), $S \vdash \forall x\, x{=}x$ (GEN), $S \vdash \forall x\, x{=}x \to t{=}t$ (P4), $S \vdash t{=}t$ (MP). Tedy $t \sim t$.
- symetrie: nechť $s \sim t$, tj. $S \vdash s{=}t$. Platí $S \vdash (x_1{=}y_1 \wedge x_2{=}y_2) \to (x_1{=}x_2 \to y_1{=}y_2)$ (R2, $=$ hraje i roli P). Užitím GEN, P4 a MP dostaneme $S \vdash (s{=}t \wedge s{=}s) \to (s{=}s \to t{=}s)$. Užitím MP dostaneme $S \vdash t{=}s$.
- Tranzitivita: podobně.

Predikátová logika. Kanonická struktura. (7)

Nyní již můžeme definovat strukturu $\mathcal{O}$ pro jazyk teorie S:

- Nosičem $\mathcal{O}$ jsou třídy rozkladu nosiče $\mathcal{M}$ podle $\sim$.
- Funkční symbol f arity n je realizován takto:

$$f_{\mathcal{O}}([t_1], \cdots, [t_n]) = [f_{\mathcal{M}}(t_1, \cdots, t_n)]$$

- Predikátový symbol P arity m je realizován takto:

$$P_{\mathcal{O}}([t_1], \cdots, [t_m]) \text{ právě když } P_{\mathcal{M}}(t_1, \cdots, t_m)$$

Korektnost této definice (tj. nezávislost na volbě reprezentantů) se dokáže pomocí R1–R3 podobným stylem jako výše. Snadno se ověří, že realizací uzavřeného termu t ve struktuře $\mathcal{O}$ je $[s]$ právě když $S \vdash s{=}t$. To znamená, že predikátový symbol $=$ je v $\mathcal{O}$ realizován jako identita.

Predikátová logika. Kanonická struktura. (8)

Zbývá ukázat, že $\mathcal{O}$ je modelem S. Podobně jako ve *větě 78* budeme chtít prokázat, že pro libovolnou formuli $\varphi(x_1, \ldots, x_n)$ jazyka teorie S platí:

- Jestliže $t_1, \cdots, t_n$ jsou uzavřené termy jazyka teorie S, pak $S \vdash \varphi(x_1/t_1, \cdots, x_n/t_n)$ právě když $\mathcal{O} \models \varphi(x_1/[t_1], \cdots, x_n/[t_n])$.

Jelikož S je henkinovská a úplná, platí podle *věty 78*

- $S \vdash \varphi(x_1/t_1, \cdots, x_n/t_n)$ právě když $\mathcal{M} \models \varphi(x_1/t_1, \cdots, x_n/t_n)$

Stačí tedy ukázat, že

- $\mathcal{M} \models \varphi(x_1/t_1, \cdots, x_n/t_n)$ právě když $\mathcal{O} \models \varphi(x_1/[t_1], \cdots, x_n/[t_n])$

To lze lehce provést indukcí ke struktuře φ. □

Predikátová logika. Věta o úplnosti.

Kurt Gödel (1906–1978)

Věta 80 (o úplnosti, Kurt Gödel)

Každá bezesporná teorie má model. Pro každou teorii T a každou formuli jejího jazyka tedy platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Důkaz. Jde o jednoduchý důsledek předchozích vět. □

Predikátová logika. Věta o kompaktnosti.

Věta 81

Teorie T má model, právě když každá její podteorie s konečně mnoha axiómy (a s minimálním jazykem, v němž jsou tyto axiómy formulovatelné) má model.

Důkaz. Směr „$\Rightarrow$“ je triviální. Pro opačnou implikaci stačí ukázat, že T je bezesporná (pak T má model podle věty o úplnosti). Kdyby T byla sporná, existoval by důkaz formule $\psi \wedge \neg\psi$ v T. Tento důkaz je konečný, využívá tedy jen konečně mnoho axiómů T, které tvoří spornou podteorii T, spor. □

Predikátová logika. Löwenheimova-Skolemova věta.

Poznámka 82

Z důkazu *věty 75* plyne, že každá bezesporná teorie *s jazykem bez rovnosti* má model kardinality $\max\{|\mathcal{L}|, \aleph_0\}$ (při rozšíření teorie na henkinovskou bylo přidáno $|\mathcal{L}| \cdot \aleph_0$ nových konstant). Toto pozorování *neplatí* pro teorie s jazykem s rovností (např. pro $T = \{\forall x\, x{=}c\}$). Nicméně lze dokázat následující:

Věta 83

Nechť T je teorie a nechť pro každé $n \in \mathbb{N}$ existuje model teorie T, jehož nosič má mohutnost alespoň n. Pak T má nekonečný model.

Důkaz. Je-li jazyk teorie T jazykem bez rovnosti, plyne tvrzení ihned z *poznámky 82*. Jinak pro každé $n \in \mathbb{N}$ definujeme formuli $\varphi_n \equiv \forall x_1 \cdots \forall x_n \exists y\ x_1 \neq y \wedge \cdots \wedge x_n \neq y$ a teorii $S_n = T \cup \{\varphi_1, \cdots, \varphi_n\}$. Podle předpokladu věty má každá S_n model. Podle věty o kompaktnosti má proto model i teorie $\bigcup_{i=1}^{\infty} S_n$. Tento model je nutně nekonečný a je i modelem teorie T. □

Predikátová logika. Löwenheimova-Skolemova věta. (2)

Věta 84 (Löwenheimova-Skolemova)

Nechť T je teorie s jazykem L, která má nekonečný model. Nechť κ je nekonečný kardinál takový, že $\kappa \geq |\mathcal{L}|$. Pak T má model mohutnosti κ.

Důkaz. Nechť $\mathcal{M}$ je nekonečný model T. Jazyk $\mathcal{L}$ rozšíříme o systém $\{c_i \mid i < \kappa\}$ nových konstant a k T přidáme axiómy $\{c_i \neq c_j \mid i, j < \kappa\}$. Obdržíme tak teorii T'. Nechť K je konečná část T', a nechť $c_1, \cdots, c_n$ jsou všechny nově přidané konstanty, které se vyskytují ve formulích teorie K (takových konstant je jen konečně mnoho). Pokud tyto konstanty realizujeme navzájem různými prvky nosiče $\mathcal{M}$, obdržíme model teorie K. Každá konečná část T' je tedy splnitelná. Podle věty o kompaktnosti má tedy model i teorie T'. Nosič tohoto model ale nutně obsahuje alespoň κ navzájem různých individuí. □

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Predikátová logika. Löwenheimova-Skolemova věta. (3)

Poznámka 85

Löwenheimova-Skolemova věta říká, že teorie prvního řádu nedokáží definovat mohutnost modelu. Není tedy možné dosáhnout toho, aby teorie prvního řádu s nekonečným modelem měla jediný model až na izomorfismus. To lze vynutit pouze za cenu přidání axiómů v logice vyššího řádu (typicky monadické logiky druhého řádu). Pro tyto logiky ovšem zpravidla neplatí věta o úplnosti. Příkladem je obecně užívaná axiomatická definice reálných čísel, která má až na izomorfismus jediný model a obsahuje (druhořádový) axiom existence supréma ohraničené množiny.

Predikátová logika. Löwenheimova-Skolemova věta. (4)

Poznámka 86 (Skolemův paradox)

Jelikož teorie množin je teorie prvního řádu, která nemá konečný model, podle Löwenheimovy-Skolemovy platí, že má-li teorie množin nějaký model (tj. je-li bezesporná), pak má také (meta)spočetný model $\mathcal{M}$. Tento fakt je velmi kontraintuitivní, neboť každý model teorie množin musí obsahovat „obrazy“ veškerých množin, jejichž existence je zaručena axiómy teorie množin. Zejména $\mathcal{M}$ musí obsahovat „obrazy“ prvního nekonečného ordinálu ω a množiny 2^ω všech podmnožin ω. Oba tyto obrazy jsou z „vnějšího (meta) pohledu na $\mathcal{M}$“ spočetné, z „vnitřního“ pohledu samotného $\mathcal{M}$ ovšem 2^ω spočetná není. V každém modelu teorie množin totiž platí, že neexistuje množina, která je bijekcí mezi ω a 2^ω, neboť tento fakt lze z teorie množin dokázat. Ani v $\mathcal{M}$ tedy taková bijekce neexistuje. Zdánlivý rozpor vzniká pouze na základě toho, že obrazy metapojmů „spočetná množina“, „bijekce“, atd., v modelu $\mathcal{M}$ nejsou takové, jaké intuitivně očekáváme.

Věta o neúplnosti. Úvod.

- *Jazyk aritmetiky* je jazyk s rovností obsahující konstantu 0, unární funkční symbol S a dva binární funkční symboly $*$ a $+$.
- Význačnou realizací jazyka aritmetiky je $(\mathbb{N}_0, *, +)$, kde univerzem je soubor všech nezáporných celých čísel, 0 je realizováno jako nula, S jako funkce následníka, $*$ jako násobení, $+$ jako sčítání. (Relační predikáty jako $<, \leq$ lze snadno definovat.)
- Jedním ze základních kroků *Hilbertova programu* formalizace matematiky mělo být vytvoření *rekurzivní a úplné* teorie T jazyka aritmetiky.
- Slovem „úplné“ se myslí, že $T \vdash \varphi$ právě když $\varphi \in Th(\mathbb{N}_0, *, +)$ (Tj. formule dokazatelné v T jsou právě formule pravdivé v $(\mathbb{N}_0, *, +)$).
- Slovo „rekurzívní“ intuitivně znamená, že musí být „mechanicky ověřitelné“, zda daná posloupnost symbolů je či není důkazem v T (možných formalizací tohoto pojmu je více).
- Z Gödelových výsledků plyne, že taková teorie neexistuje.

Věta o neúplnosti. Turingův stroj.

Alan Turing (1912–1954)

- Definoval pojem Turingova stroje a s jeho pomocí ukázal, že problém pravdivosti formulí prvního řádu je *nerozhodnutelný*.
- Považován za zakladatele informatiky (jako vědy).
- Turingův stroj je matematickým modelem „hloupého odvozovače“, který má k dispozici papír, tužku a gumu, a který si pamatuje konečně mnoho schémat axiómů.
- Význam Turingova stroje coby modelu reálných výpočetních zařízení se projevil až v druhé polovině 20. století.

Věta o neúplnosti. Turingův stroj. (2)

- Je-li Σ konečná *abeceda*, značí symbol Σ^* soubor všech konečných slov složených z prvků Σ. *Jazyk* nad abecedou Σ je podmnožina Σ^*.
- *Turingův stroj* je matematický model výpočetního zařízení, které je vybaveno konečně-stavovou *řídící jednotkou* („hlava odvozovače“), jednosměrně nekonečnou *pracovní páskou* („papír“), a čtecí/zápisovou hlavou („tužka/guma“).
- Na začátku výpočtu je na pásce zapsáno konečné *vstupní slovo* nad *vstupní abecedou*, hlava je na nejlevější pozici, a stavová jednotka je v počátečním stavu.
- Stroj na základě svého momentálního kontrolního stavu a symbolu pod čtecí hlavou provede „výpočetní krok“, tj. změní svůj kontrolní stav, nahradí symbol pod čtecí hlavou jiným symbolem *páskové abecedy*, a posune čtecí hlavu vlevo nebo vpravo.
- Výpočet se zastaví, pokud stroj dojde do konfigurace, jejíž kontrolní stav je *akceptující* nebo *zamítající*. Pro některá slova může stroj také *nezastavit* (cyklit).
- Vstupní slovo je *akceptované* strojem M, jestliže M po konečně mnoha krocích dojde do akceptující konfigurace. Soubor všech vstupních slov, která M akceptuje, tvoří *jazyk akceptovaný daným strojem*, označovaný $L(M)$.

Věta o neúplnosti. Vlastnosti jazyků.

- Jazyk $L \subseteq \Sigma^*$ je *rekurzivně vyčíslitelný*, jestliže $L = L(M)$ pro nějaký Turingův stroj M. Jazyk $L \subseteq \Sigma^*$ je *rekurzivní*, jestliže $L = L(M)$ pro nějaký Turingův stroj M, který zastaví pro *každé* vstupní slovo. Jednoduché pozorování je, že jazyk $L \subseteq \Sigma^*$ je rekurzivní právě když L i $\overline{L}$ jsou rekurzivně vyčíslitelné (kde $\overline{L} = \Sigma^* \setminus L$).
- Uvažme soubor *všech* Turingových strojů se vstupní abecedou $\{0,1\}$. Bez újmy na obecnosti lze předpokládat, že kontrolní stavy a symboly páskové abecedy *každého* takového stroje jsou prvky nějaké fixní spočetné množiny. Pak *každý* Turingův stroj M se vstupní abecedou $\{0,1\}$ lze jednoznačně zapsat jako slovo $code(M) \in \{0,1\}^*$. Navíc lze předpokládat, že *každé* $u \in \{0,1\}^*$ je kódem nějakého stroje M_u se vstupní abecedou $\{0,1\}$.
- Uvažme jazyk $Accept = \{u \in \{0,1\}^* \mid M_u \text{ akceptuje } u\}$.
- Lze snadno (i když technicky) dokázat, že $Accept$ je rekurzivně vyčíslitelný (lze zkonstruovat stroj U, který pro dané vstupní slovo $u \in \{0,1\}^*$ „simuluje“ výpočet stroje M_u na slově u).
- Ukážeme, že $Accept$ *není rekurzivní*. Podle jednoho z předchozích bodů pak jazyk $\overline{Accept}$ *není rekurzivně vyčíslitelný*.

Věta o neúplnosti. Jazyk *Accept*.

Věta 87

Jazyk $Accept$ není rekuzivní.

Důkaz. Předpokládejme, že $Accept$ je rekurzivní. Pak také $\overline{Accept}$ je rekurzivní, tj. existuje Turingův stroj M se vstupní abecedou $\{0,1\}$, který zastaví pro každé vstupní slovo a $L(M) = \overline{Accept}$. Nechť $v = code(M)$. Platí $v \in L(M)$?

- Ano. Pak $v \notin L(M_v) = L(M)$, spor.
- Ne. Pak $v \in L(M_v) = L(M)$, spor.

Z předpokladu existence stroje M se nám podařilo odvodit spor. Stroj M tedy *neexistuje*. □

Poznámka 88

V důkazu předchozí věty se objevuje určitá forma *autoreference* (stroj M zkoumá „sám sebe“ tak, že analyzuje svůj vlastní kód). Každý známý důkaz věty o neúplnosti se o nějakou formu autoreference opírá.

Věta o neúplnosti. Redukce.

Definice 89

Redukce jazyka $L_1 \subseteq \Sigma_1^*$ *na jazyk* $L_2 \subseteq \Sigma_2^*$ *je zobrazení* $f : \Sigma_1^* \to \Sigma_2^*$ *splňující následující podmínky:*

- *Pro každé slovo* $w \in \Sigma_1^*$ *platí* $w \in L_1$ *právě když* $f(w) \in L_2$.
- f *je vypočitatelné, tj. existuje Turingův stroj* M*, který pro každé vstupní slovo* $w \in \Sigma_1^*$ *zastaví v akceptujícím stavu a na výstupní pásku zapíše slovo* $f(w)$.

Věta 90

Nechť existuje redukce f *jazyka* L_1 *na jazyk* L_2*. Platí:*

- *Jestliže* L_2 *je rekurzivní (resp. rekurzivně vyčíslitelný), pak také* L_1 *je rekurzivní (resp. rekurzivně vyčíslitelný).*
- *Jestliže* L_1 *není rekurzivní (resp. není rekurzivně vyčíslitelný), pak také* L_1 *není rekurzivní (resp. není rekurzivně vyčíslitelný).*
- *Redukce* f *je rovněž redukcí jazyka* $\overline{L_1}$ *na jazyk* $\overline{L_2}$.

Věta o neúplnosti. Minského stroj.

Definice 91

Minského stroj $\mathcal{M}$ *se dvěma čítači* c, d *je konečná posloupnost očíslovaných instrukcí tvaru*

$$1 : Com_1; \quad \cdots \quad \mathtt{m} : Com_m; \quad \mathtt{m{+}1} : \mathtt{Halt}$$

kde každá instrukce Com_i *je jednoho ze dvou typů:*

I: $\mathtt{i} : \mathtt{inc\ x;\ goto\ u}$

II: $\mathtt{i} : \mathtt{if\ x = 0\ then\ goto\ u\ else\ dec\ x;\ goto\ v}$

kde $\mathtt{x} \in \{c, d\}$, $1 \leq \mathtt{u} \leq m{+}1$ *a* $1 \leq \mathtt{v} \leq m{+}1$.

Věta o neúplnosti. Minského stroj. (2)

- Konfigurace stroje $\mathcal{M}$ je trojice $\langle \ell, c, d \rangle$, kde $\ell \in \{1, \ldots, m{+}1\}$ je číslo následující instrukce a $c, d \in \mathbb{N}_0$ jsou momentální hodnoty čítačů.
- Krok výpočtu $\mathcal{M}$ je binární relace $\mapsto$ na konfiguracích $\mathcal{M}$, kde $\langle \ell, c, d \rangle \mapsto \langle \ell', c', d' \rangle$ právě když provedením Com_ℓ pro hodnoty čítačů c, d stroj $\mathcal{M}$ změní hodnoty čítačů na c', d' a odskočí na instrukci ℓ'.
- Stroj $\mathcal{M}$ zastaví, pokud existuje konečná posloupnost konfigurací $\langle \ell_0, c_0, d_0 \rangle, \ldots, \langle \ell_k, c_k, d_k \rangle$, kde $\langle \ell_0, c_0, d_0 \rangle = \langle 1, 0, 0 \rangle$, $\ell_k = m{+}1$, a pro každé $0 \leq i < k$ platí $\langle \ell_i, c_i, d_i \rangle \mapsto \langle \ell_{i+1}, c_{i+1}, d_{i+1} \rangle$.
- Zápis každého Minského stroje je konečné slovo nad fixní konečnou abecedou Σ. Navíc každé slovo $w \in \Sigma^*$ lze chápat jako zápis nějakého Minského stroje $\mathcal{M}_w$.
- Nechť $\mathit{Halt} = \{w \in \Sigma^* \mid \mathcal{M}_w \text{ zastaví}\}$.

Věta o neúplnosti. Minského stroj. (3)

Věta 92 (Minsky)

Jazyk Halt není rekurzivní (a tudíž $\overline{\mathit{Halt}}$ není rekurzivně vyčíslitelný).

Idea důkazu. Jazyk *Accept* se redukuje na jazyk *Halt*. Nejprve se ukáže, že Turingův stroje je možné simulovat strojem se dvěma zásobníky, do kterých se ukládá obsah pásky nalevo/napravo od čtecí hlavy. Následně se provede simulace zásobníku dvěma čítači. Turingův stroj lze tedy simulovat Minského strojem se čtyřmi čítači. Čtyři čítače lze ovšem simulovat pomocí dvou. Navíc lze předpokládat, že jejich iniciální hodnota je nula, neboť pomocí instrukcí typu I je možné iniciální hodnotu snadno změnit na libovolnou danou konstantu. □

Věta o neúplnosti. Rekurzivní teorie.

- Každou formuli jazyka aritmetiky je možné zapsat jako slovo nad abecedou $\{v, +, *, 0, S, (,), \forall, \rightarrow, \neg, =, \#\}$. Různé proměnné zapisujeme jako řetězce složené z v různé délky (např. místo x, y, z můžeme psát v, vv, vvv apod.).
- Podobně můžeme i každou *konečnou* posloupnost formulí zapsat jako slovo nad výše uvedenou abecedou, kde symbol $\#$ použijeme pro oddělení jednotlivých formulí.

Definice 93

Teorie T jazyka aritmetiky je rekurzivní, jestliže jazyk tvořený zápisy všech důkazů v T je rekurzivní.

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Věta o neúplnosti. Rekurzivní teorie. (2)

Lze snadno (i když technicky) dokázat, že např. Peanovy axiómy tvoří rekurzivní teorii. Definici rekurzivity teorie lze samozřejmě rozšířit i na teorie nad jinými jazyky. Rekurzivní teorie odpovídají (na intuitivní úrovni) právě teoriím, které umožňují „mechanické odvozování“. Triviální pozorování o rekurzivních teoriích podává následující věta.

Věta 94

Nechť T je rekurzivní teorie jazyka aritmetiky. Pak jazyk tvořený všemi formulemi dokazatelnými v T je rekurzivně vyčíslitelný.

Věta o neúplnosti. Jazyk *Valid*.

- Nechť *Valid* resp. *Provable* jsou jazyky nad abecedou $\{v, +, *, 0, S, (,), \forall, \rightarrow, \neg, =\}$ obsahující zápisy všech formulí jazyka aritmetiky, které jsou *pravdivé* v realizaci $(\mathbb{N}_0, *, +)$ resp. *dokazatelné* z nějaké pevně zvolené teorie jazyka aritmetiky, která je korektní a rekurzivní.
- Zjevně *Provable* $\subseteq$ *Valid*, neboť uvažovaná teorie je korektní.
- Naším cílem je ukázat, že tato inkluze je *vlastní*, tj. že existují formule pravdivé v $(\mathbb{N}_0, *, +)$, které nejsou z uvažované teorie dokazatelné.
- Jelikož jazyk *Provable* je podle *věty 94* rekurzivně vyčislitelný, stačí ukázat, že *Valid* není rekurzivně vyčislitelný.

Věta o neúplnosti. Gödelův predikát β.

Z hlediska důkazu věty o neúplnosti je jednou z podstatných vlastností přirozených čísel jejich schopnost „kódovat“ *libovolně dlouhé* konečné posloupnosti přirozených čísel.

- Definujeme 4-ární predikát β na nezáporných celých číslech předpisem

$$\beta(a, b, i, x) \iff x = a \bmod (1 + b(1 + i))$$

- Buď $\mathcal{S}$ nekonečná posloupnost nezáporných celých čísel, $a, b \in \mathbb{N}_0$. Řekneme, že $\mathcal{S}$ *splňuje* β (pro dané a a b), jestliže pro každé $i \in \mathbb{N}_0$ platí $\beta(a, b, i, \mathcal{S}(i))$.
- Pro každé $a, b \in \mathbb{N}_0$ existuje *jediná* posloupnost splňující β; tou je posloupnost $\mathcal{S}_{a,b}$ daná předpisem $\mathcal{S}_{a,b}(i) = a \bmod (1 + b(1 + i))$.
- Predikát β je vyjádřitelný v jazyce aritmetiky, neboť $x = a \bmod b$ lze napsat jako $a \geq 0 \ \wedge \ b \geq 0 \ \wedge \ \exists k \left(k \geq 0 \ \wedge \ k * b \leq a \ \wedge \ (k + 1) * b > a \ \wedge \ x = a - (k * b) \right)$

Věta o neúplnosti. Gödelův predikát β. (2)

Věta 95

Pro každou konečnou posloupnost $n_0, \cdots, n_k$ nezáporných celých čísel existují $n, m \in \mathbb{N}_0$ taková, že $n_j = \mathcal{S}_{n,m}(j)$ pro každé $0 \leq j \leq k$. To znamená, že pro každé $0 \leq j \leq k$ platí $\beta(n, m, j, x) \iff x = n_j$.

Důkaz. (osnova)

- Nechť $m = (\max\{k, n_0, \cdots, n_k\})!$ Čísla $p_i = 1 + m(1 + i)$, kde $0 \leq i \leq k$, jsou navzájem nesoudělná a $n_i < p_i$ pro každé $0 \leq i \leq k$.
- Dále pro každé $0 \leq i \leq k$ definujeme $c_i = p_0 \cdot \cdots \cdot p_k / p_i$. Nyní pro každé $0 \leq i \leq k$ existuje přesně jedno d_i, $0 \leq d_i \leq p_i$, takové, že $(c_i \cdot d_i) \bmod p_i = 1$
- Definujeme

$$n = \sum_{i=0}^{k} c_i \cdot d_i \cdot n_i$$

Pro každé $0 \leq i \leq k$ platí $n_i = n \bmod p_i$, což je tvrzení věty.

□

Věta o neúplnosti. Důkaz.

Věta 96

Jazyk Valid není rekurzivně vyčíslitelný.

Důkaz. Jazyk $\overline{Halt}$ zredukujeme na jazyk *Valid*. Buď $w \in \Sigma^*$ libovolné slovo nad abecedou jazyka *Halt*, a nechť

$$\mathcal{M}_w \quad \equiv \quad 1 : \mathrm{Com}_1; \quad \cdots \quad \mathtt{m} : \mathrm{Com}_m; \quad \mathtt{m{+}1} : \mathtt{Halt}$$

je Minského stroj se dvěma čítači kódovaný slovem w. Redukce $f(w)$ vrací formuli tvaru $\neg\Psi_w$, kde Ψ_w vyjadřuje, že $\mathcal{M}_w$ zastaví.

Stroj $\mathcal{M}_w$ zastaví, právě když existuje $k \in \mathbb{N}_0$ a posloupnost konfigurací $\langle \ell_0, c_0, d_0 \rangle, \ldots, \langle \ell_k, c_k, d_k \rangle$ taková, že

1. $\langle \ell_0, c_0, d_0 \rangle = \langle 1, 0, 0 \rangle$,
2. $\ell_k = m{+}1$,
3. pro každé $0 \leq i < k$ platí $\langle \ell_i, c_i, d_i \rangle \mapsto \langle \ell_{i+1}, c_{i+1}, d_{i+1} \rangle$.

Věta o neúplnosti. Důkaz. (2)

Jelikož posloupnost konfigurací je posloupností přirozených čísel, můžeme pomocí predikátu β uvedenou podmínku zapsat následovně:

$$\exists k\ \exists a\ \exists b \quad \mathit{INIT}(a,b) \ \wedge\ \mathit{HALTING}(a,b,k) \ \wedge\ \Big(\forall i\ 0{\leq}i{<}k \rightarrow \mathit{STEP}(a,b,i)\Big)$$

kde jednotlivé podformule vyjadřují následující:

- „Posloupnost $\mathcal{S}_{a,b}$ začíná zápisem konfigurace $\langle 1,0,0\rangle$“.

  $$\mathit{INIT}(a,b) \quad\equiv\quad \beta(a,b,0,1) \wedge \beta(a,b,1,0) \wedge \beta(a,b,2,0)$$

- „Konfigurace $\langle \ell_k, c_k, d_k\rangle$ v posloupností $\mathcal{S}_{a,b}$ splňuje $\ell_k = m{+}1$“.

  $$\mathit{HALTING}(a,b,k) \quad\equiv\quad \beta(a,b,k*3,m{+}1)$$

Věta o neúplnosti. Důkaz. (3)

- „Platí $\langle \ell_i, c_i, d_i\rangle \mapsto \langle \ell_{i+1}, c_{i+1}, d_{i+1}\rangle$“. Formule $\mathit{STEP}(a,b,i)$ je definována takto:

$$\begin{aligned}&\forall \ell\ \forall c\ \forall d\ \forall \ell'\ \forall c'\ \forall d'\\ &\Big(\ \beta(a,b,i{*}3,\ell) \ \wedge\ \beta(a,b,i{*}3{+}1,c) \ \wedge\ \beta(a,b,i{*}3{+}2,d)\\ &\quad\ \beta(a,b,i{*}3{+}3,\ell') \ \wedge\ \beta(a,b,i{*}3{+}4,c') \ \wedge\ \beta(a,b,i{*}3{+}5,d')\ \Big)\\ &\rightarrow\ \bigwedge_{j=1}^{m} \mathit{COM}_j\end{aligned}$$

  kde COM_j je definována následovně:

  - Jestliže $\mathrm{Com}_j \equiv$ `j : inc c; goto u`, pak COM_j je formule

    $$(\ell{=}j) \rightarrow (c'{=}c{+}1 \wedge d'{=}d \wedge \ell'{=}u)$$

  - Jestliže $\mathrm{Com}_j \equiv$ `j : inc d; goto u`, pak COM_j je formule

    $$(\ell{=}j) \rightarrow (d'{=}d{+}1 \wedge c'{=}c \wedge \ell'{=}u)$$

Věta o neúplnosti. Důkaz. (4)

- Jestliže $\mathrm{Com}_j \equiv$ `j : if c = 0 then goto u else dec c; goto v`, pak COM_j je formule

$$(\ell{=}j) \rightarrow \Big(\big(c{=}0 \rightarrow (c'{=}c \wedge \ell'{=}u)\big) \wedge \big(c{\geq}1 \rightarrow (c'{=}c{-}1 \wedge \ell'{=}v)\big) \wedge d'{=}d\Big)$$

- Jestliže $\mathrm{Com}_j \equiv$ `j : if d = 0 then goto u else dec d; goto v`, pak COM_j je formule

$$(\ell{=}j) \rightarrow \Big(\big(d{=}0 \rightarrow (d'{=}d \wedge \ell'{=}u)\big) \wedge \big(d{\geq}1 \rightarrow (d'{=}d{-}1 \wedge \ell'{=}v)\big) \wedge c'{=}c\Big)$$

□

Věta o neúplnosti. Důkaz. (5)

Triviálním důsledkem *věty 94* a *věty 96* je následující:

Věta 97 (o neúplnosti)

Neexistuje žádná rekurzivní teorie jazyka aritmetiky, ve které jsou dokazatelné právě všechny formule pravdivé v realizaci $(\mathbb{N}_0, +, *)$. Specielně pro každou korektní rekurzivní teorii T (tj. takovou teorii, která umožnuje dokázat pouze formule pravdivé v $(\mathbb{N}_0, +, *)$) nutně existuje formule platná v $(\mathbb{N}_0, +, *)$, která není v T dokazatelná.

Věta 97 bývá v literatuře také označována jako *první věta o neúplnosti*. Původní Gödelova formulace této věty (a zejména její důkaz) vypadá odlišně.

Pravdivost a splnitelnost.

- Otázku, zda existuje mechanický postup (algoritmus), který rozhodne, zda je dané matematické tvrzení pravdivé nebo ne (tzv. Entscheidungsproblem) formuloval David Hilbert v roce 1928.
- Pokud za matematicky správná tvrzení považujeme formule φ jazyka teorie množin takové, že $ZF \models \varphi$, je jazyk tvořený všemi správnými tvrzeními rekurzivně vyčislitelný, neboť $ZF \models \varphi$ právě když $ZF \vdash \varphi$ a ZF je rekurzivní teorie.
- Alan Turing publikoval v roce 1936 práci *„On Computable Numbers, with an Application to the Entscheidungsproblem“*, kde zavedl pojem Turingova stroje a ukázal, že jazyk tvořený predikátovými tautologiemi (nad jistým fixním konečným systémem predikátových a funkčních symbolů) není rekurzivní.
- Kurt Gödel publikoval větu a úplnosti v roce 1930 a dvě věty o neúplnosti v roce 1931, kdy Turingovy výsledky neexistovaly. Jednoduché důkazy první Gödelovy věty o neúplnosti (jako ten prezentovaný na přednášce) se objevily později.

Pravdivost a splnitelnost. (2)

- Nechť $\mathcal{L} = \{0, S, Reach\}$, kde 0 a S jsou funkční symboly arity nula resp. jedna, a $Reach$ je predikátový symbol arity tři.
- Nechť $Tautologies$ je jazyk tvořený zápisy všech formulí φ predikátové logiky nad $\mathcal{L}$, které jsou tautologiemi, tj. platí $\models \varphi$.
- Ukážeme, že $Tautologies$ *není rekurzivní*.

Pravdivost a splnitelnost. (3)

Věta 98

Jazyk Tautologies není rekurzivní.

Důkaz. Jazyk *Halt* zredukujeme na jazyk *Tautologies*. Buď $w \in \Sigma^*$ libovolné slovo nad abecedou jazyka *Halt*, a nechť

$$\mathcal{M}_w \quad \equiv \quad 1 : \mathrm{Com}_1; \quad \cdots \quad \mathtt{m} : \mathrm{Com}_m; \quad \mathtt{m{+}1} : \mathtt{Halt}$$

je Minského stroj se dvěma čítači kódovaný slovem w. Redukce $f(w)$ vrací formuli Ψ_w, kde $\models \Psi_w$ právě když $\mathcal{M}_w$ zastaví.

- Každému $k \in \mathbb{N}_0$ přiřadíme (nulární) term $[k] \equiv S(S(\ldots S(0)\ldots)$, kde S je použito k-krát.
- Predikát $\mathit{Reach}(\ell, c, d)$ vyjadřuje, že konfigurace $\langle \ell, c, d \rangle$ je dosažitelná z počáteční konfigurace $\langle 1, 0, 0 \rangle$.
- Pro každé $i \in \{1, \ldots m\}$ sestrojíme formuli φ_i, která říká „je-li $\langle i, c, d \rangle$ dosažitelná konfigurace, pak je dosažitelná i konfigurace $\langle i', c', d' \rangle$, kde $\langle i, c, d \rangle \mapsto \langle i', c', d' \rangle$“.

Pravdivost a splnitelnost. (4)

Pak

$$\Psi_w \quad \equiv \quad \left(\mathit{Reach}([1],[0],[0]) \wedge \bigwedge_{i=1}^{m} \varphi_i \right) \rightarrow \exists c \, \exists d \, \mathit{Reach}([m{+}1], c, d)$$

Formule φ_i jsou definovány takto:

- Jestliže $\mathrm{Com}_i \equiv \mathtt{i} : \mathtt{inc\ c;\ goto\ u}$, pak

$$\varphi_i \quad \equiv \quad \forall c \, \forall d \; \mathit{Reach}([i], c, d) \rightarrow \mathit{Reach}([u], S(c), d)$$

- Jestliže $\mathrm{Com}_i \equiv \mathtt{i} : \mathtt{inc\ d;\ goto\ u}$, pak

$$\varphi_i \quad \equiv \quad \forall c \, \forall d \; \mathit{Reach}([i], c, d) \rightarrow \mathit{Reach}([u], c, S(d))$$

- Jestliže $\mathrm{Com}_i \equiv \mathtt{i} : \mathtt{if\ c = 0\ then\ goto\ u\ else\ dec\ c;\ goto\ v}$, pak $\varphi_i \equiv \psi_i \wedge \xi_i$, kde

$$\psi_i \quad \equiv \quad \forall d \;\; \mathit{Reach}([i], [0], d) \rightarrow \mathit{Reach}([u], [0], d)$$
$$\xi_i \quad \equiv \quad \forall c \, \forall d \;\; \mathit{Reach}([i], S(c), d) \rightarrow \mathit{Reach}([v], c, d)$$

Pravdivost a splnitelnost. (5)

- Jestliže $\mathrm{Com}_i \equiv \mathtt{i : if\ d = 0\ then\ goto\ u\ else\ dec\ d;\ goto\ v}$, pak $\varphi_i \equiv \psi_i \wedge \xi_i$, kde

$$\psi_i \equiv \forall c\ \mathit{Reach}([i], c, [0]) \rightarrow \mathit{Reach}([u], c, [0])$$
$$\xi_i \equiv \forall c\, \forall d\ \mathit{Reach}([i], c, S(d)) \rightarrow \mathit{Reach}([v], c, d)$$

Dokážeme, že $\mathcal{M}_w$ zastaví právě když $\models \Psi_w$.

($\Rightarrow$) Buď $\mathcal{U}$ realizace $\mathcal{L}$ taková, že $\mathcal{U} \models \mathit{Reach}([1], [0], [0]) \wedge \bigwedge_{i=1}^{m} \varphi_i$. Z konstrukce formulí φ_i ihned plyne, že pro libovolnou dosažitelnou konfiguraci $\langle \ell, c, d \rangle$ stroje $\mathcal{M}_w$ platí $\mathcal{U} \models \mathit{Reach}([\ell], [c], [d])$. Jelikož $\mathcal{M}_w$ zastaví, platí $\mathcal{U} \models \mathit{Reach}([m{+}1], [c'], [d'])$ pro nějaké $c', d' \in \mathbb{N}_0$. Celkem $\mathcal{U} \models \Psi_w$.

($\Leftarrow$) Nechť $\mathcal{M}_w$ nezastaví. Uvažme realizaci nad univerzem $\mathbb{N}_0$, kde 0 je realizováno jako nula, S jako přičtení jedničky, a $\mathit{Reach}_{\mathbb{N}_0}(\ell, c, d)$ právě když je konfigurace $\langle \ell, c, d \rangle$ dosažitelná. Jelikož $\mathcal{M}_w$ nezastaví, pro každé $c, d \in \mathbb{N}_0$ platí, že predikát $\mathit{Reach}_{\mathbb{N}_0}(m{+}1, c, d)$ není splněn. Zjevně $\mathbb{N}_0 \models \mathit{Reach}([1], [0], [0]) \wedge \bigwedge_{i=1}^{m} \varphi_i$, ale $\mathbb{N}_0 \not\models \Psi_w$. □

Pravdivost a splnitelnost. (6)

- Pro každou uzavřenou formuli Φ platí, že $\models \Phi$ právě když $\neg\Phi$ není splnitelná. Okamžitým důsledkem věty 98 je následující:

Věta 99

Nechť Satisfiable je jazyk tvořený zápisy všech formulí predikátové logiky nad jazykem $\mathcal{L} = \{0, S, \mathit{Reach}\}$, které jsou splnitelné. Pak Satisfiable není rekurzivně vyčislitelný.

Pravdivost a splnitelnost. (7)

- Uvažme jazyk (s rovností) $\mathcal{L}' = \{0, S, Reach'\}$, kde $Reach'$ je predikátový symbol arity 4. Užitím techniky z důkazu Věty 98 lze snadno dokázat následující:

Věta 100 (Boris Trachtenbrot)

Nechť Fsatisfiable je jazyk tvořený zápisy všech formulí predikátové logiky nad jazykem $\mathcal{L}'$, které jsou konečně splnitelné. Pak Fsatisfiable není rekurzivní.

Důkaz. [Osnova] Jazyk *Halt* zredukujeme na jazyk *Fsatisfiable*. Pro daný Minského stroj $\mathcal{M}$ sestrojíme formuli tvaru

$$\Psi \equiv Reach'([1],[0],[0],[0]) \wedge \bigwedge_{i=1}^{m} \varphi_i$$
$$\wedge \; Reach'(x_1,x_2,x_3,y) \rightarrow (S(y) \neq 0 \wedge \forall z (y \neq z \rightarrow S(y) \neq S(z)))$$

kde formule φ_i jsou definovány stejně jako v důkazu věty 98 s tím rozdílem, že poslední argument $Reach'$ se vždy „zvětší o jedničku“ pomocí S. Snadno se ověří, že $\mathcal{M}$ zastaví právě když Ψ má konečný model. □

Pravdivost a splnitelnost. (8)

- Jazyk *Fsatisfiable* je rekurzivně vyčislitelný, jeho doplněk tedy rekurzivně vyčislitelný není.
- Formule Φ predikátového počtu je konečně-pravdivá, psáno $\models_f \Phi$, právě když Φ je pravdivá ve všech konečných realizacích svého jazyka.
- Uzavřená formule Φ je konečně-pravdivá právě když $\neg\Phi$ není konečně-splnitelná. Proto jazyk *Ftautologies* tvořený zapisy všech konečně-pravdivých formulí predikátové logiky nad jazykem $\mathcal{L}'$ není rekurzivně vyčislitelný.
- Důsledkem věty 100 je tedy to, že neexistuje žádný odvozovací systém s vlastností $\vdash \varphi$ právě když $\models_f \varphi$, dokonce ani pro fixní jazyk $\mathcal{L}'$.

Druhá věta o neúplnosti. Úvod

- Původní Gödelova formulace 1. věty o neúplnosti se týkala třídy teorií, které vzniknou „primitivně rekurzivním rozšířením“ jedné fixní teorie (varianty Peanovy aritmetiky).
- Důkaz je založen na konstrukci pravdivé formule, jejíž intuitivní význam je „já nejsem dokazatelná“.
- Pomocí vytvořeného aparátu je možné kódovat metatvrzení o Peanově aritmetice jako formule jazyka aritmetiky. Jedním takovým metatvrzením je *bezespornost*. Druhá Gödelova věta o neúplnosti říká, že tato formule není v Peanově aritmetice dokazatelná.
- Klíčové obraty celé konstrukce si nyní naznačíme. V této části se slovem „formule“ myslí *formule jazyka aritmetiky*.

První věta o neúplnosti. Gödelův důkaz

Jedním z pokusů o vytvoření rekurzivní a úplné teorie aritmetiky byl následující systém nazývaný *Peanova aritmetika* (seznam Peanových axiómů bývá v literatuře uváděn v různých podobách):

- $\forall x\ S(x) \neq 0$
- $\forall x \forall y\ S(x){=}S(y) \rightarrow x{=}y$
- $\forall x\ x{+}0 = x$
- $\forall x \forall y\ x{+}S(y) = S(x{+}y)$
- $\forall x\ x{*}0 = 0$
- $\forall x \forall y\ x{*}S(y) = (x{*}y) + x$
- $(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(S(x)))) \rightarrow \forall x\, \varphi(x)$, kde φ je formule s jednou volnou proměnnou x.

První věta o neúplnosti. Gödelův důkaz (2)

Původní formulace Gödelovy věty uveřejněná v práci *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I* z roku 1931 je tato:

Satz VI

Zu jeder ω-widerspruchsfreien rekursiven Klasse χ von Formeln gibt es rekursive Klassenzeichen r, so daß weder v Gen r noch Neg(v Gen r) zu Flg(χ) gehört (wobei v die freie Variable aus r ist).

Tuto formulaci lze (o něco čitelněji) přepsat následovně:

Věta 101

Nechť T je teorie splňující následující podmínky:

- *Jazyk teorie T je stejný jako jazyk odvozovacího systému P.*
- *T obsahuje axiómy systému P a navíc nějaký primitivně rekurzivní soubor dalších axiómů.*
- *T je ω-konzistentní.*

Pak T je neúplná, tj. existuje sentence φ taková, že $T \nvdash \varphi$ a současně $T \nvdash \neg\varphi$.

První věta o neúplnosti. Gödelův důkaz (3)

- Odvozovací systém P je variantou odvozovacího systému z Principia Mathematica k němuž jsou přidány „aritmetické“ axiómy podobné Peanově aritmetice.
- Teorie je T je ω-konzistentní pokud neexistuje žádná formule $\varphi(x)$ taková, že současně platí
  - $T \vdash \exists x.\varphi(x)$,
  - $T \vdash \neg\varphi[x/k]$ pro každé $k \in \mathbb{N}_0$.

  Každá korektní teorie, která umožňuje dokázat pouze formule platné v $\mathbb{N}_0$, je ω-konzistentní. Původní formulace Gödelovy věty se ovšem vyhýbá „sémantickým“ pojmům.

První věta o neúplnosti. Gödelův důkaz (4)

Nechť *PA* značí teorii Peanovy aritmetiky, a nechť $\mathbb{N}_0$ značí realizaci $(\mathbb{N}_0, +, *)$ jazyka aritmetiky. Formule jsou konečná slova nad abecedou $\{v, +, *, 0, S, (,), \forall, \rightarrow, \neg, =\}$ a lze je tedy kódovat *čísly* stejným způsobem jako konfigurace Turingových strojů. Pro každou formuli φ označíme symbolem $\lceil \varphi \rceil$ číslo, které je jejím kódem.

Lema 102 (Gödelovo lema o pevném bodě)

Pro každou formuli $\psi(x)$ existuje uzavřená formule τ taková, že $PA \vdash \tau \leftrightarrow \psi(\lceil \tau \rceil)$. (Formule τ říká „ψ platí pro můj kód“.)

Důkaz. (osnova) Pro libovolnou fixní proměnnou x_0 lze sestrojit formuli $SUBST(x, y, z)$, která říká následující:

- „Číslo z je kódem formule, kterou získáme substitucí proměnné x_0 za konstantu s hodnotou x ve formuli s kódem y.“

Např. $SUBST(5, \lceil \varphi(x_0) \rceil, 413)$ je pravdivá právě když $\lceil \varphi(5) \rceil = 413$. Konstrukce formule $SUBST(x, y, z)$ je technická; lze použít podobný přístup jako při konstrukci formule *ACOMP* v důkazu *věty 96*.

První věta o neúplnosti. Gödelův důkaz (5)

Nyní definujeme

- $\sigma(x) \equiv \forall y\,(SUBST(x, x, y) \rightarrow \psi(y))$
- $\tau \equiv \sigma(\lceil \sigma(x_0) \rceil)$

Ověřme, že τ má požadovanou vlastnost:

- $\tau \equiv \sigma(\lceil \sigma(x_0) \rceil) \equiv \forall y\,(SUBST(\lceil \sigma(x_0) \rceil, \lceil \sigma(x_0) \rceil, y) \rightarrow \psi(y))$
- $\mathbb{N}_0 \models \forall y\,(SUBST(\lceil \sigma(x_0) \rceil, \lceil \sigma(x_0) \rceil, y) \rightarrow \psi(y))$ právě když $\mathbb{N}_0 \models \forall y\,(y = \lceil \sigma(\lceil \sigma(x_0) \rceil) \rceil \rightarrow \psi(y))$
- $\forall y\,(y = \lceil \sigma(\lceil \sigma(x_0) \rceil) \rceil \rightarrow \psi(y)) \equiv \forall y\,(y = \lceil \tau \rceil \rightarrow \psi(y))$
- $\mathbb{N}_0 \models \forall y\,(y = \lceil \tau \rceil \rightarrow \psi(y))$ právě když $\mathbb{N}_0 \models \psi(\lceil \tau \rceil)$

Předchozí argument se opírá o *sémantickou* ekvivalenci jistých formulí; ekvivalence těchto formulí je ale ve skutečnosti *dokazatelná v PA*. Např.

$$PA \vdash (\forall y\,(y = \lceil \tau \rceil \rightarrow \psi(y))) \leftrightarrow \psi(\lceil \tau \rceil)$$

což je třeba v posledním bodu. Proto $PA \vdash \tau \leftrightarrow \psi(\lceil \tau \rceil)$. □

První věta o neúplnosti. Gödelův důkaz (6)

Věta 103 (První věta o neúplnosti, Gödelova)

Lze sestrojit uzavřenou formuli ϱ, která je pravdivá v $\mathbb{N}_0$, ale není dokazatelná v PA.

Důkaz. (osnova) Ukáže se, že i důkazy (tj. konečné posloupnosti formulí) je možné kódovat čísly, a že existuje formule $PROOF(x, y)$, která říká, že x je kódem důkazu (v PA) pro formuli s kódem y. Dokazatelnost v PA lze pak zapsat formulí

- $PROVABLE(y) \equiv \exists x\, PROOF(x, y)$

Pak pro každou uzavřenou formuli φ platí

- $PA \vdash \varphi$ právě když $\mathbb{N}_0 \models PROVABLE(\ulcorner\varphi\urcorner)$

Dále lze ukázat

- $PA \vdash \varphi$ právě když $PA \vdash PROVABLE(\ulcorner\varphi\urcorner)$

Směr „$\Leftarrow$“ plyne ihned z korektnosti PA (indukcí se snadno ukáže, že jestliže $PA \vdash \varphi$, pak $\mathbb{N}_0 \models \varphi$). Opačný směr je výrazně pracnější.

První věta o neúplnosti. Gödelův důkaz (7)

Nyní stačí aplikovat *lema 102* na formuli $\neg PROVABLE(x)$. Dostaneme tak sentenci ϱ takovou, že platí

- $PA \vdash \varrho \leftrightarrow \neg PROVABLE(\ulcorner\varrho\urcorner)$

Formule ϱ tedy říká *„já nejsem dokazatelná“*, přičemž toto tvrzení je v PA dokazatelné.
Z korektnosti PA dostáváme, že

- $\mathbb{N}_0 \models \varrho \leftrightarrow \neg PROVABLE(\ulcorner\varrho\urcorner)$

Pak ale musí platit $\mathbb{N}_0 \models \varrho$; kdyby totiž $\mathbb{N}_0 \models \neg\varrho$, dostaneme $\mathbb{N}_0 \models PROVABLE(\ulcorner\varrho\urcorner)$, proto $PA \vdash \varrho$ a tedy $\mathbb{N}_0 \models \varrho$, spor.

Jelikož $\mathbb{N}_0 \models \varrho$, platí $\mathbb{N}_0 \models \neg PROVABLE(\ulcorner\varrho\urcorner)$, tedy $\mathbb{N}_0 \not\models PROVABLE(\ulcorner\varrho\urcorner)$, proto $PA \nvdash \varrho$.

Formule ϱ je tedy pravdivá v $\mathbb{N}_0$, ale není dokazatelná v PA. □

Druhá věta o neúplnosti. Tvrzení o *PA* v *PA*.

Pozorování:

- Důkaz *věty 103* se opírá o možnost vyjádřit jistá *metatvrzení* o formulích aritmetiky a teorii *PA* jako formule aritmetiky. Typicky lze takto vyjádřit tvrzení, která se týkají *dokazatelnosti*.
  - Metatvrzení „$PA \vdash \varphi$“ lze vyjádřit formulí $PROVABLE(\ulcorner\varphi\urcorner)$. Dokonce platí $PA \vdash \varphi$ právě když $PA \vdash PROVABLE(\ulcorner\varphi\urcorner)$.
  - I metatvrzení „$PA \vdash \varphi$ právě když $PA \vdash PROVABLE(\ulcorner\varphi\urcorner)$“ lze vyjádřit v *PA* pomocí formule

    $$PROVABLE(\ulcorner\varphi\urcorner) \leftrightarrow PROVABLE(\ulcorner PROVABLE(\ulcorner\varphi\urcorner)\urcorner)$$

    I tato formule je v *PA* dokazatelná.
  - *Bezespornost* teorie *PA* lze vyjádřit formulí $CONSIS \equiv \neg PROVABLE(\ulcorner\xi \wedge \neg\xi\urcorner)$, kde ξ je (nějaká) formule.

Druhá věta o neúplnosti. Tvrzení o *PA* v *PA*. (2)

- Jsou ale i metatvrzení o formulích aritmetiky, která jako formule aritmetiky výjádřit *nelze*. Typicky se jedná o tvrzení týkající se *pravdivosti*.
  - Tvrzení „$\mathbb{N}_0 \models \varphi$“ jako formuli aritmetiky vyjádřit nelze: Předpokládejme naopak, že existuje formule $TRUE(x)$ taková, že $\mathbb{N}_0 \models \varphi$ právě když $\mathbb{N}_0 \models TRUE(\ulcorner\varphi\urcorner)$. Pak podle *lematu 102* existuje sentence τ taková, že $\mathbb{N}_0 \models \tau$ právě když $\mathbb{N}_0 \models \neg TRUE(\ulcorner\tau\urcorner)$. Ovšem podle výše uvedeného platí $\mathbb{N}_0 \models \tau$ právě když $\mathbb{N}_0 \models TRUE(\ulcorner\tau\urcorner)$, což je spor.

Druhá věta o neúplnosti. Důkaz.

Úvahy o vyjádřitelnosti některých vlastností teorie *PA* formulemi aritmetiky hrají klíčovou roli v důkazu následujícího tvrzení:

Věta 104 (2. věta o neúplnosti, Gödelova)

Formule CONSIS není v PA dokazatelná. (Obecněji: v „dostatečně silné“ teorii lze dokázat její vlastní bezespornost jen v případě, že je tato teorie sporná.)

Důkaz. (osnova) Nechť ϱ je formule zkonstruovaná v důkazu *věty 103* (která o sobě říká, že je nedokazatelná). Uvažme následující metatvrzení:

- „Jestliže $PA \vdash \varrho$, pak platí $PA \vdash PROVABLE(\ulcorner\varrho\urcorner)$ a současně $PA \vdash \neg PROVABLE(\ulcorner\varrho\urcorner)$“

Toto tvrzení je nejen pravdivé, ale lze ho vyjádřit formulí aritmetiky, která je navíc *dokazatelná* v *PA*:

- $PA \vdash PROVABLE(\ulcorner\varrho\urcorner) \rightarrow (PROVABLE(\ulcorner PROVABLE(\ulcorner\varrho\urcorner)\urcorner) \wedge PROVABLE(\ulcorner\neg PROVABLE(\ulcorner\varrho\urcorner)\urcorner))$

Proto platí také $PA \vdash PROVABLE(\ulcorner\varrho\urcorner) \rightarrow \neg CONSIS$.

Druhá věta o neúplnosti. Důkaz. (2)

Obměnou uvedeného tvrzení dostáváme

- $PA \vdash CONSIS \rightarrow \neg PROVABLE(\ulcorner\varrho\urcorner)$

Kdyby $PA \vdash CONSIS$, platilo by také $PA \vdash \neg PROVABLE(\ulcorner\varrho\urcorner)$ (aplikací MP). Už dříve jsme ale ukázali (viz důkaz *věty 103*), že

- $PA \vdash \varrho \leftrightarrow \neg PROVABLE(\ulcorner\varrho\urcorner)$

Další aplikací MP tedy dostáváme $PA \vdash \varrho$, spor. □

Na intuitivní úrovni: druhá věta o neúplnosti říká, že bezespornost „dostatečně silné“ teorie (např. teorie množin) *nelze v této teorii dokázat*. Jediná možnost je použít *metaargumenty*, tj. zdůvodnit bezespornost dané teorie pomocí teorie „vyšší“. Ani bezespornost této vyšší teorie není ovšem možno prokázat v ní samé. Na nějaké úrovni nám prostě nezbývá, než v bezespornost *uvěřit*, resp. ji *předpokládat*. Gödelovy výsledky o neúplnosti mají tedy i svůj *epistemologický* význam.

Automatické dokazování.

- Odvozovací systémy pro logiky s implikací a negací založené na pravidle *modus ponens* (tzv. *Hilbertovské systémy*) reflektují styl lidského uvažování a vznikly v souvislosti se snahou o formalizaci matematiky.
- Hilbertovské systémy *nejsou* příliš vhodné jako základ pro *automatické* dokazování formulí výrokového nebo predikátového počtu. Z tohoto pohledu jsou výrazně výhodnější odvozovací systémy založené na *rezoluci*.
- Pro každou teorii T a každou *uzavřenou* formuli φ jejího jazyka platí $T \models \varphi$ právě když $T \cup \{\neg\varphi\}$ není splnitelná. Místo $T \models \varphi$ tedy můžeme prokazovat *nesplnitelnost* teorie $T \cup \{\neg\varphi\}$.

Rezoluční metoda. Výrokový počet.

- Každou formuli φ výrokového počtu lze ekvivalentně zapsat v *konjunktivní normální formě CNF*, tj. jako formuli tvaru $C_1 \wedge \cdots \wedge C_n$, kde každé C_i je *klauzule*, tj. disjunkce *literálů* tvaru $\ell_1 \vee \cdots \vee \ell_m$, kde literál je buď výroková proměnná nebo negace výrokové proměnné (viz *věta 28*).
- Pro naše účely je vhodnější definovat klauzule jako konečné *soubory* literálů (vyhneme se tak formálním problémům, které by vznikly při možnosti opakovat v klauzuli tentýž literál několikrát).

Rezoluční metoda. Výrokový počet. (2)

Definice 105

- *Literál* je výroková proměnná nebo její negace.
- *Klauzule* je konečný soubor literálů. Prázdná klauzule se značí symbolem $\square$.

Notace:

- Klauzuli $\{\ell_1, \ldots, \ell_n\}$ zapisujeme také jako $\ell_1 \vee \ldots \vee \ell_n$, kde na pořadí literálů nezáleží. Jsou-li C_1 a C_2 klauzule, pak symbolem $C_1 \vee C_2$ označujeme klauzuli $C_1 \cup C_2$. Místo $C \vee \{\ell\}$ píšeme jen $C \vee \ell$
- Konečný soubor klauzulí $\{C_1, \ldots, C_n\}$ zapisujeme také jako $C_1 \wedge \cdots \wedge C_n$, kde na pořadí klauzulí nezáleží.

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Rezoluční metoda. Výrokový počet. (3)

Definice 106

- *Nechť ν je valuace.*
  - *Klauzule C je pravdivá (splněná) při valuaci ν, jestliže existuje literál $\ell \in C$ takový, že $\nu(\ell) = 1$. V opačném případě je C nepravdivá (nesplněná) při ν.*
  - *Soubor klauzulí Γ je pravdivý (splněný) při valuaci ν, jestliže každá klauzule $C \in \Gamma$ je při ν splněná. V opačném případě je Γ je nepravdivý (nesplněný) při ν.*
- *Klazule je splnitelná, pokud existuje valuace, při které je splněna. V opačném případě je nesplnitelná (prázdná klauzule $\square$ je tedy nesplnitelná).*
- *Soubor klauzulí Γ je splnitelný, pokud existuje valuace, při které je splněn. V opačném případě je nesplnitelný.*

Rezoluční metoda. Výrokový počet. (4)

Rezoluční odvozovací pravidlo: Z klauzulí tvaru $C_1 \vee A$ a $C_2 \vee \neg A$, kde $A \notin C_1$ a $\neg A \notin C_2$, odvoď klauzuli $C_1 \vee C_2$.

Lema 107

Nechť Γ je soubor klauzulí a nechť C je klauzule, která vznikne aplikací rezoluce na (nějaké) dvě klauzule z Γ. Je-li Γ splnitelný, pak také $\Gamma \wedge C$ je splnitelný.

Důkaz. Předpokládejme, že C vzniklo pomocí rezoluce ze dvou klauzulí tvaru $C_1 \vee A$ a $C_2 \vee \neg A$, které patří do Γ (tj. $C = C_1 \vee C_2$. Jelikož Γ je splnitelné, existuje valuace ν taková, že $C_1 \vee A$ i $C_2 \vee \neg A$ jsou při ν splněny. Přitom ale buď $\nu(A) = 0$ nebo $\nu(\neg A) = 0$, tedy alespoň jedna z klauzulí C_1 a C_2 je při ν splněna. Proto je při ν splněna i klauzule $C = C_1 \vee C_2$. □

Matematická logika
Antonín Kučera
Úvod
Aristotelova logika
Logický čtverec
Sylogismy
Booleova algebra logiky
Dva zákl. problémy
Výroková logika
Syntaxe
Sémantika
Plnohodnotnost
Kompaktnost
Odvozovací systém
Predikátová logika
Syntaxe
Sémantika
Odvozovací systém
Věta o úplnosti
Věta o neúplnosti
Turingův stroj
Důkaz věty o neúplnosti
Pravdivost a splnitelnost
2. věta o neúplnosti
Automatické dokazování

Rezoluční metoda. Výrokový počet. (5)

Definice 108

Buď Γ soubor klauzulí a C klauzule. Rezoluční důkaz klauzule C ze souboru předpokladů Γ je konečná posloupnost klauzulí $C_1, \ldots, C_n$ taková, že

- $C_n = C$.
- *Každé C_i je buď prvkem Γ nebo vzniklo z předchozích klauzulí pomocí pravidla rezoluce.*

Jestliže existuje rezoluční důkaz C ze souboru Γ, píšeme $\Gamma \vdash C$.

Rezoluční metoda. Výrokový počet. (6)

Věta 109

Nechť Γ je soubor klauzulí. Pak Γ je nesplnitelný právě když $\Gamma \vdash \square$.

Důkaz.

$\Leftarrow$: Jelikož $\Gamma \vdash \square$, existuje konečná posloupnost klauzulí $C_1, \ldots, C_n$, která je důkazem $\square$ z Γ. Podle lematu 107 platí, že je-li soubor $\Gamma \wedge C_1 \wedge \cdots \wedge C_n$ nesplnitelný, pak je nesplnitelný také soubor Γ. Ovšem soubor $\Gamma \wedge C_1 \wedge \cdots \wedge C_n$ je zjevně nesplnitelný, neboť obsahuje klauzuli $C_n = \square$.

$\Rightarrow$: Nechť Γ je nesplnitelný soubor klauzulí, a nechť m je počet všech navzájem různých literálů, které jsou obsaženy v klauzulích souboru Γ. Indukcí k m dokážeme, že $\Gamma \vdash \square$.

- $m = 0$. Jelikož Γ je nesplnitelný, musí obsahovat alespoň jednu klauzuli. Přitom jediná klauzule, kterou Γ může obsahovat, je prázdná klauzule $\square$. Platí tedy $\Gamma = \{\square\}$ a tudíž $\Gamma \vdash \square$.
- Nechť se v klauzulích souboru Γ vyskytuje právě $m+1$ navzájem různých literálů. Jelikož Γ je nesplnitelný, musí existovat výroková proměnná A taková, že literály A i $\neg A$ jsou obsaženy v nějaké klauzuli souboru Γ (ne nutně ve stejné). V opačném případě by totiž existovala splňující valuace ν pro Γ, kde
  - $\nu(A) = 1$ pro všechny výrokové proměnné A, kde A je obsaženo v nějaké klauzuli souboru Γ,

Rezoluční metoda. Výrokový počet. (7)

  - $\nu(A) = 0$ pro všechny výrokové proměnné A, kde $\neg A$ je obsaženo v nějaké klauzuli souboru Γ.

Uvažme tedy literály A, $\neg A$, které se vyskytují v klauzulích souboru Γ. Nechť $\Gamma = C_1 \wedge \cdots \wedge C_n$, a nechť

- $\Gamma^A = C_1^A \wedge \cdots \wedge C_n^A$, kde $C_i^A = C_i \setminus \{A\}$,
- $\Gamma^{\neg A} = C_1^{\neg A} \wedge \cdots \wedge C_n^{\neg A}$, kde $C_i^{\neg A} = C_i \setminus \{\neg A\}$.

Soubory Γ^A i $\Gamma^{\neg A}$ jsou nesplnitelné, jinak by Γ byl splnitelný. Podle indukčního předpokladu tedy platí $\Gamma^A \vdash \square$ a $\Gamma^{\neg A} \vdash \square$. Je ihned vidět, že pokud v důkazu $\square$ z Γ^A vždy použijeme klauzuli C_i místo klauzule C_i^A, dostaneme důkaz buď prázdné klauzule nebo klauzule $\{A\}$ z Γ. V prvním případě jsme ihned hotovi, v druhém případě aplikujeme stejné pozorování na důkaz $\square$ z $\Gamma^{\neg A}$. Při použití C_i místo $C_i^{\neg A}$ tak obdržíme buď důkaz $\square$ z Γ (a jsme hotovi), nebo důkaz klauzule $\{\neg A\}$ z Γ. Pokud $\Gamma \vdash \{A\}$ a $\Gamma \vdash \{\neg A\}$, platí rovněž $\Gamma \vdash \square$, neboť uvedené důkazy stačí zřetězit za sebe a aplikovat rezoluční odvozovací pravidlo na $\{A\}$ a $\{\neg A\}$.

$\square$

Rezoluční metoda. Predikátový počet.

- Ukážeme, že každou formuli φ predikátové logiky je možné algoritmicky převést na formuli tvaru

$$\bar{\varphi} \quad = \quad \forall x_1 \cdots \forall x_n \; C_1 \wedge \cdots \wedge C_n \,.$$

  Každá *klauzule* C_i je konečnou disjunkcí *literálů* tvaru $P(t_1, \ldots, t_k)$ nebo $\neg P(t_1, \ldots, t_k)$, kde k je arita P a $t_1, \ldots, t_k$ jsou termy, v nichž se mohou vyskytovat proměnné $x_1, \ldots, x_n$ (a žádné další).
- Formule $\bar{\varphi}$ obecně *není* ekvivalentní formuli φ a může být vytvořena nad bohatším jazykem obsahujícím nové funkční symboly. Nicméně platí, že φ je splnitelná právě když $\bar{\varphi}$ je splnitelná.
- Rezoluční odvozovací pravidlo

Rezoluční metoda. Predikátový počet. (2)

Buď φ formule predikátové logiky.

1. Odstraníme veškeré výrokové spojky mimo $\wedge$, $\vee$ a $\neg$.
2. Všechny negace „posuneme“ až k predikátovým symbolům, eliminujeme násobné negace.
3. Přejmenujeme proměnné tak, aby
   - žádná proměnná neměla současně volný a vázaný výskyt;
   - proměnné použité bezprostředně za kvantifikátory byly po dvou různé.
4. Přesuneme všechny kvantifikátory vlevo před formuli při zachování jejich pořadí.
5. Provedeme Skolemizaci existenčních kvantifikátorů.
6. Opakovaně použijeme distributivní zákon pro $\wedge$ a $\vee$.