Matematická logika
Přednáška č. 12

RNDr. Kateřina Trlifajová PhD.

katerina.trlifajova@fit.cvut.cz

Katedra aplikované matematiky
Fakulta informačních technologií
České vysoké učení technické v Praze

BI-MLO, ZS 2015/2016

Sémantika vs. syntax

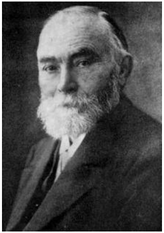
Sémantika:

- Zabýváme se významem tvrzení
- Pravdivost je definována pomocí ohodnocení - pravdivostní tabulky, tautologie, kontradikce, logický důsledek, ekvivalence.

Syntax:

- Formule je posloupnost symbolů.
- Dokazatelnost je definována syntakticky. Důkaz je posloupnost formulí, které jsou vytvářeny podle přesných pravidel.
- Hledáme formální odvozovací systém, v němž z co nejméně formulí (axiomů) dokážeme všechny tautologie.

Gottlob Frege



David Hilbert

Jazyk výrokové logiky

Víme, že všechny formule můžeme vyjádřit pouze pomocí $\neg, \Rightarrow$.

Definice

Jazyk výrokové logiky obsahuje:

- množinu prvotních formulí $A, B, C, \ldots$,
- logické spojky $\neg, \Rightarrow$,
- závorky (,).

Definice

I. Prvotní formule je **výroková formule**.

II. Jsou-li A, B výrokové formule, pak jsou i $\neg A, (A \Rightarrow B)$ výrokové formule.

III. Každá výroková formule vznikne konečným užitím pravidel I. a II.

Ostatní logické spojky zavedeme později, jako zkratky:

$A \vee B \leftrightharpoons \neg A \Rightarrow B$; $A \wedge B \leftrightharpoons \neg(A \Rightarrow \neg B)$; $A \Leftrightarrow B \leftrightharpoons \neg\big((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow A)\big)$

Hilbertovský výrokový kalkul

Definice

Hilbertův axiomatický systém výrokové logiky se skládá z **Hilbertových axiomů:**

(H1) $A \Rightarrow (B \Rightarrow A)$

(H2) $\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)$

(H3) $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$

kde A, B, C jsou libovolné formule a odvozovacího pravidla **modus ponens**:

- Z A
- a $A \Rightarrow B$
- odvodíme B.

Poznámka: Axiomy představují schéma formulí. Za axiom považujeme jakoukoli jejich instanci.

- $E \Rightarrow (G \Rightarrow E)$ (H1)
- $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (H1)
- $(\neg(F \Rightarrow \neg G) \Rightarrow \neg G) \Rightarrow (G \Rightarrow (F \Rightarrow \neg G))$ (H3)
- $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ (H2)

Důkaz v Hilbertově kalkulu

Definice

Posloupnost formulí $A_1, \ldots A_n$ nazýváme **důkazem formule** A, jestliže A_n je A a pro každé A_i, $1 \leq i \leq n$, platí

i) A_i je axiom nebo

ii) A_i vznikne z předchozích A_j, $j \leq i$, pravidlem modus ponens.

Existuje-li důkaz formule A, píšeme $\vdash A$ a říkáme, že formule A **je dokazatelná**.

Příklad

Dokážeme $\vdash (E \Rightarrow G) \Rightarrow (E \Rightarrow E)$.

Důkaz

- $\vdash E \Rightarrow (G \Rightarrow E)$ (H1)
- $\vdash \big(E \Rightarrow (G \Rightarrow E)\big) \Rightarrow \big((E \Rightarrow G) \Rightarrow (E \Rightarrow E)\big)$ (H2)
- $\vdash (E \Rightarrow G) \Rightarrow (E \Rightarrow E)$ (MP)

$\square$

Důkaz

Lemma 1

$\vdash A \Rightarrow A.$

Poznámka: $A \Rightarrow A$ je vlastně $\neg A \vee A$, *princip vyloučeného třetího*.

Důkaz

- $\vdash A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ (H1)
- $\vdash (A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ (H2)
- $\vdash (A \Rightarrow (A \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ (MP)
- $\vdash A \Rightarrow (A \Rightarrow A)$ (H1)
- $\vdash A \Rightarrow A$ (MP)

$\square$

Korektnost

Věta o korektnosti I.

Je-li $\vdash A$*, pak* A *je tautologie.*

Důkaz

Indukcí podle délky důkazu:

(i) Všechny axiomy jsou tautologie:

(H1) $A \Rightarrow (B \Rightarrow A) \models\!\!\!\dashv \neg A \vee \neg B \vee A$
(H2) $\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)$
(H3) $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B) \models\!\!\!\dashv (B \vee \neg A) \Rightarrow (\neg A \vee B)$

(ii) *Modus ponens* je korektní, z tautologií odvodí tautologii: Jsou-li $A, A \Rightarrow B$ tautologie, pak pro každé ohodnocení v platí, že $v(A) = 1$ a $v(A \Rightarrow B) = 1$, nutně tedy i $v(B) = 1$. B je tedy tautologie.

□

Všechny kroky důkazu jsou tedy tautologie.

Důkaz z teorie

Definice

Posloupnost formulí $A_1, \ldots A_n$ je **důkazem formule** A **z teorie** T, jestliže A_n je A a pro každé A_i, $1 \leq i \leq n$, platí, že

i) A_i je axiom nebo

ii) A_i vznikne z předchozích A_j, $j \leq i$ pravidlem modus ponens nebo

iii) A_i je formule teorie T.

Píšeme $T \vdash A$ a říkáme, že formule A **je dokazatelná v teorii** T.

Poznámky:

- $\{A\} \vdash A$ přímo z definice, píšeme $A \vdash A$ (FT)
- Jestliže $T \vdash B$, pak $T \cup \{A\} \vdash B$, píšeme $T, A \vdash B$.
- Jestliže $\vdash B$, pak $T \vdash B$.
- $T \vdash A \Rightarrow A$

Důkazy

Lemma 2

$B \vdash A \Rightarrow B.$

Důkaz

- $\vdash B \Rightarrow (A \Rightarrow B)$ (H1)
- $B \vdash B$ (FT)
- $B \vdash A \Rightarrow B$ (MP)

$\square$

Lemma 3

$\neg A \vdash A \Rightarrow B$

Důkaz

- $\neg A \vdash \neg A$ (FT)
- $\vdash \neg A \Rightarrow (\neg B \Rightarrow \neg A)$ (H1)
- $\neg A \vdash (\neg B \Rightarrow \neg A)$ (MP)
- $\vdash (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$ (H3)
- $\neg A \vdash (A \Rightarrow B)$ (MP)

$\square$

Korektnost

Věta o korektnosti II.

Je-li $T \vdash A$, *pak* $T \models A$.

Důkaz

Indukcí podle délky důkazu:

(i) Všechny axiomy jsou tautologie. Formule obsažené v nějaké teorii jsou jejími logickými důsledky.

(ii) V indukčním kroku užijeme *modus ponens*, což je korektní: nechť $T \models A$ a $T \models A \Rightarrow B$, tedy v každém ohodnocení v, které splňuje T, je pravdivé A a $A \Rightarrow B$, tedy je pravdivé i B. Je tedy $T \models B$.

□

Věta o úplnosti

Věta o úplnosti

Formule A je dokazatelná, právě když A je tautologie,
$\vdash A$ *právě když* $\models A$.

Důkaz

$\Rightarrow$: Je-li A dokazatelná, pak A je tautologie. = Věta o korektnosti.
To jsme již dokázali.

$\Leftarrow$: Dokazovat nebudeme. $\square$

Věta o úplnosti (silná podoba)

Věta o úplnosti II

Formule A je dokazatelná v teorii T, právě když A je tautologickým důsledkem T,
$T \vdash A$ právě když $T \models A$

Důkaz

$\Rightarrow$: Jestliže $T \vdash A$, pak $T \models A$. Již jsme dokázali (věta o korektnosti).
$\Leftarrow$: Nechť $T \models A$. Potom:

- $S \models A$ pro nějakou konečnou $S = \{A_1, A_2, \ldots A_n\} \subseteq T$ (věta o kompaktnosti),
- $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \models A$, právě když $\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow A$,
- $((A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow A) \Dashv\models (\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \vee A)$
  $\Dashv\models (\neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n \vee A) \Dashv\models (A_1 \Rightarrow (A_2 \Rightarrow \ldots \Rightarrow (A_n \Rightarrow A) \ldots))$
- $\models A_1 \Rightarrow (A_2 \Rightarrow \ldots \Rightarrow (A_n \Rightarrow A) \ldots)$,
- $\vdash A_1 \Rightarrow (A_2 \Rightarrow \ldots \Rightarrow (A_n \Rightarrow A) \ldots)$ (věta o úplnosti),
- $A_1, A_2, \ldots A_n \vdash A$ (n krát věta o dedukci),
- $S \vdash A$,
- $T \vdash A$.

$\square$

Bezespornost

Definice

Teorie T je **sporná** (nekonsistentní) právě, když existuje formule A taková, že $T \vdash A$ a $T \vdash \neg A$.

Teorie T je **bezesporná (konsistentní)** právě, když není sporná.

Věta o bezespornosti

Teorie T je bezesporná, právě když je splnitelná.

Dokážeme, že teorie T je sporná, právě když není splnitelná.

Důkaz věty o bezespornosti

Důkaz

Následující tvrzení jsou ekvivalentní:

- T je sporná.
- Existuje B tak, že $T \vdash B$ a $T \vdash \neg B$ (přímo z definice).
- Existuje B tak, že $T \models B$ a $T \models \neg B$ (věta o úplnosti).
- Existují konečné $S_1, S_2 \subseteq T$ tak, že $S_1 \models B$ a $S_2 \models \neg B$ (věty o kompaktnosti).
- Označíme-li $S = S_1 \cup S_2$, pak platí $S \models B$ a $S \models \neg B$.
- $S \models \bot$ (věta o resoluci)
- $S \subseteq T$ není splnitelná.
- T není splnitelná (věta o kompaktnosti).

□

Bezespornost

Věta

T je sporná, právě když každá formule A je v T dokazatelná.

Důkaz

$\Leftarrow$: Je-li dokazatelná každá formule, pak jistě je dokazatelná nejaká formule i její negace.

$\Rightarrow$: Nechť T je sporná, tj. existuje formule B tak, že $T \vdash B$ a $T \vdash \neg B$.
Pro libovolnou formuli A platí:

- $\vdash \neg B \Rightarrow (B \Rightarrow A)$ (L5))
- $T \vdash \neg B$ (předpoklad)
- $T \vdash B \Rightarrow A$ (MP)
- $T \vdash B$ (předpoklad)
- $T \vdash A$ (MP) □

Hilbertovský predikátový kalkulus

Definice

Nechť A, B, C jsou formule predikátové logiky, x je proměnná, t je term

(H1) $A \Rightarrow (B \Rightarrow A)$.

(H2) $\big(A \Rightarrow (B \Rightarrow C)\big) \Rightarrow \big((A \Rightarrow B) \Rightarrow (A \Rightarrow C)\big)$.

(H3) $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$.

(H4) $(\forall x)A \Rightarrow A(x/t)$, kde t je term substituovatelný za x.

(H5) $(\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$, kde x nemá volný výskyt v A.

Odvozovací pravidla:

- **Modus ponens** (MP): Z formulí $A, A \Rightarrow B$ odvoď formuli B.
- **Pravidlo generalizace** (Gen): Pro libovolnou proměnnou x odvoď z A formuli $(\forall x)A$.

Věta o korektnosti

Věta

Nechť T je teorie a A je formule predikátové logiky. Potom platí, že je-li A dokazatelná, pak A je logicky platná, tj.

$$\vdash A, \text{ pak } \models A.$$

Důkaz

Dokazujeme indukcí podle délky důkazu A podobně jako ve VL.

(1) Axiomy (H1) – (H3) jsou logicky platné, jedná se o instance tautologií VL.

(2) Axiom (H4) $(\forall x)A \Rightarrow A(x/t)$, kde t je substituovatelný za x, je logicky platná formule.

(3) Axiom (H5) $(\forall x)(A \Rightarrow B) \Rightarrow (A \Rightarrow (\forall x)B)$, kde x nemá volný výskyt v A, také.

(4) Pomocí *modus ponens* odvodíme z log.platných formulí opět log. platné formule, viz VL.

(5) Pravidlem *generalizace* z $\vdash A$ odvodíme $\vdash (\forall x)A(x)$. To je korektní, neboť podle věty o uzávěru platí $\models A(x)$, právě když $\models (\forall x)A(x)$.

$\square$

Věta o korektnosti II

Věta

Nechť T je teorie a A je formule predikátové logiky. Platí, že je-li A dokazatelná, pak A je logicky platná, tj. jestliže

$$T \vdash A, \text{ pak } T \models A.$$

Důkaz

Dokazujeme indukcí podle délky důkazu A.

(1) Každý axiom je logicky pravdivá formule, tedy platí v každé interpretaci při každém ohodnocení, a tudíž i $T \models A$.

(2) Pravidlem **modus ponens** odvozujeme z logických důsledků opět logické důsledky, stejně jako ve VL.

Jestliže A bylo odvozeno pravidlem **generalizace** z B, tedy A je $(\forall x)B$, a $T \models B$, pak v každém modelu $\mathcal{M}$ teorie T platí $\mathcal{M} \models B$. Protože T je množina uzavřených formulí, platí pro každé ohodnocení e, že $\mathcal{M} \models B[e]$. Tedy platí i $\mathcal{M} \models (\forall x)B$. Tudíž $T \models (\forall x)B$.

(3) Jestliže $A \in T$, pak $T \models A$, neboť $A \models A$.

$\square$

Bezespornost a model

Věta

Jestliže T má model, potom je bezesporná.

Důkaz

Plyne z věty o korektnosti. Nechť $\mathcal{M}$ je model T a A je libovolná uzavřená formule stejného jazyka. Kdyby $T \vdash A$ a $T \vdash \neg A$, pak by $T \models A$ a $T \models \neg A$, tedy i $\mathcal{M} \models A$ a $\mathcal{M} \models \neg A$, ale to je spor! $\square$

Příklad: Teorie částečného uspořádání, lineárního uspořádání, teorie grup mají model. Jsou tedy bezesporné.

Věta

Teorie T je bezesporná, potom má model.

Model musíme zkonstruovat, což je technicky náročnější a tím se zde nebudeme zabývat.

Věta o úplnosti

Věta

Je-li T teorie a A je formule, pak A je dokazatelná v T, právě když A je logickým důsledkem T.

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

Důkaz

Označujeme $A^{(\forall)}$ je uzávěr formule A, $\neg A^{(\forall)}$ je negace uzávěru A, resp. $\neg(A^{(\forall)})$.

- $T \vdash A$ právě tehdy, když $T, \neg A^{(\forall)}$ nemá model.
  - $\Rightarrow$: Nechť $T \vdash A$. Podle pravidla generalizace platí $T \vdash A^{(\forall)}$. Zároveň ale $T, \neg A^{(\forall)} \vdash \neg A^{(\forall)}$. Proto je $T, \neg A^{(\forall)}$ sporná a tedy nemá model.
  - $\Leftarrow$: Jestliže $T, \neg A^{(\forall)}$ nemá model, pak je sporná, tedy v ní dokážeme cokoli, například $A^{(\forall)}$. Platí tedy $T, \neg A^{(\forall)} \vdash A^{(\forall)}$ a také $T, A^{(\forall)} \vdash A^{(\forall)}$. Podle věty o neutrální formuli tedy $T \vdash A^{(\forall)}$. Podle (H4) a (MP) z toho plyne, že $T \vdash A$.
- $T \models A$, právě když $T, \neg A^{(\forall)}$ nemá model.
  - $\Rightarrow$: Nechť tedy $T \models A$. Kdyby $\mathcal{M}$ byl model $T, \neg A^{(\forall)}$, pak též $\mathcal{M} \models T$ a $\mathcal{M} \models \neg A^{(\forall)}$. Také $\mathcal{M} \models A$, a tedy i $\mathcal{M} \models A^{(\forall)}$. To je spor, a proto $T, \neg A^{(\forall)}$ nemá model.
  - $\Leftarrow$: Nechť $T, \neg A^{(\forall)}$ nemá model. Nechť $T \not\models A$. Pak existuje $\mathcal{M} \models T$ takový, že $\mathcal{M} \not\models A$, tudíž i $\mathcal{M} \not\models A^{(\forall)}$. Tedy $\mathcal{M} \models \neg A^{(\forall)}$. $\mathcal{M}$ je modelem $\mathcal{M} \models T, \neg A^{(\forall)}$.

Rekapitulace

Věta

Nechť T je teorie, A je formule výrokové logiky. Následující tvrzení jsou ekvivalentní:

i) *T je bezesporná (konsistentní).*

ii) *T je splnitelná.*

iii) *T má model.*

iv) *Existuje formule, která z T není dokazatelná.*

Neboli následující tvrzení jsou ekvivalentní:

i) *T je sporná (nekonsistentní).*

ii) *T není splnitelná.*

iii) *T nemá model.*

iv) *Každá formule je dokazatelná z T.*