Vlastnosti formálních důkazových metod a systémů

Šárka Vavrečková

Ústav informatiky
Filozoficko-Přírodovědecká fakulta
Slezské univerzity, Opava

Co je to logika?

- Souhrn postupů k vyvozování závěrů neodporujících myšlenkám již přijatým za správné, postupů analyzujících myšlenky, o jejichž správnosti jsme přesvědčeni (hypotéz).

Co je to logika?

- Souhrn postupů k vyvozování závěrů neodporujících myšlenkám již přijatým za správné, postupů analyzujících myšlenky, o jejichž správnosti jsme přesvědčeni (hypotéz).
- Logika je věda o správném usuzování.

Co je to logika?

- formální logika,

Co je to logika?

- formální logika,
- matematická logika,

Co je to logika?

- formální logika,
- matematická logika,
- výroková logika, predikátová logika prvního řádu,

Co je to logika?

- formální logika,
- matematická logika,
- výroková logika, predikátová logika prvního řádu,
- filozofická logika,

Co je to logika?

- formální logika,
- matematická logika,
- výroková logika, predikátová logika prvního řádu,
- filozofická logika,
- klasické kontra neklasické logiky:
  - vícehodnotová (nejen *true/false*),
  - fuzzy logika,
  - pravděpodobnostní logika,
  - modální logiky, temporální logika, atd.
- atd.

Paradoxy

Paradoxy (antinomie, spory) – s využitím běžných prostředků (zdánlivě) dojdeme k opaku toho, z čeho jsme vycházeli.

Paradoxy

Paradoxy (antinomie, spory) – s využitím běžných prostředků (zdánlivě) dojdeme k opaku toho, z čeho jsme vycházeli.

David Hilbert – začátkem 20. století vytýčil *program formalizace vědy*, který měl kromě jiného i odstranit paradoxy, účelem bylo vytvořit *formální systémy* pro vědní obory.

Využití logiky v informatice

- znalostní a expertní systémy,

Využití logiky v informatice

- znalostní a expertní systémy,
- umělá inteligence,

Využití logiky v informatice

- znalostní a expertní systémy,
- umělá inteligence,
- logické programování (Prolog, Fuzzy Prolog, Templog, Chronolog, Temporal Prolog, Merkur atd.),

Využití logiky v informatice

- znalostní a expertní systémy,
- umělá inteligence,
- logické programování (Prolog, Fuzzy Prolog, Templog, Chronolog, Temporal Prolog, Merkur atd.),
- analýza přirozeného jazyka,

Využití logiky v informatice

- znalostní a expertní systémy,
- umělá inteligence,
- logické programování (Prolog, Fuzzy Prolog, Templog, Chronolog, Temporal Prolog, Merkur atd.),
- analýza přirozeného jazyka,
- důkazové metody, myšlení :-)

Důkazové metody

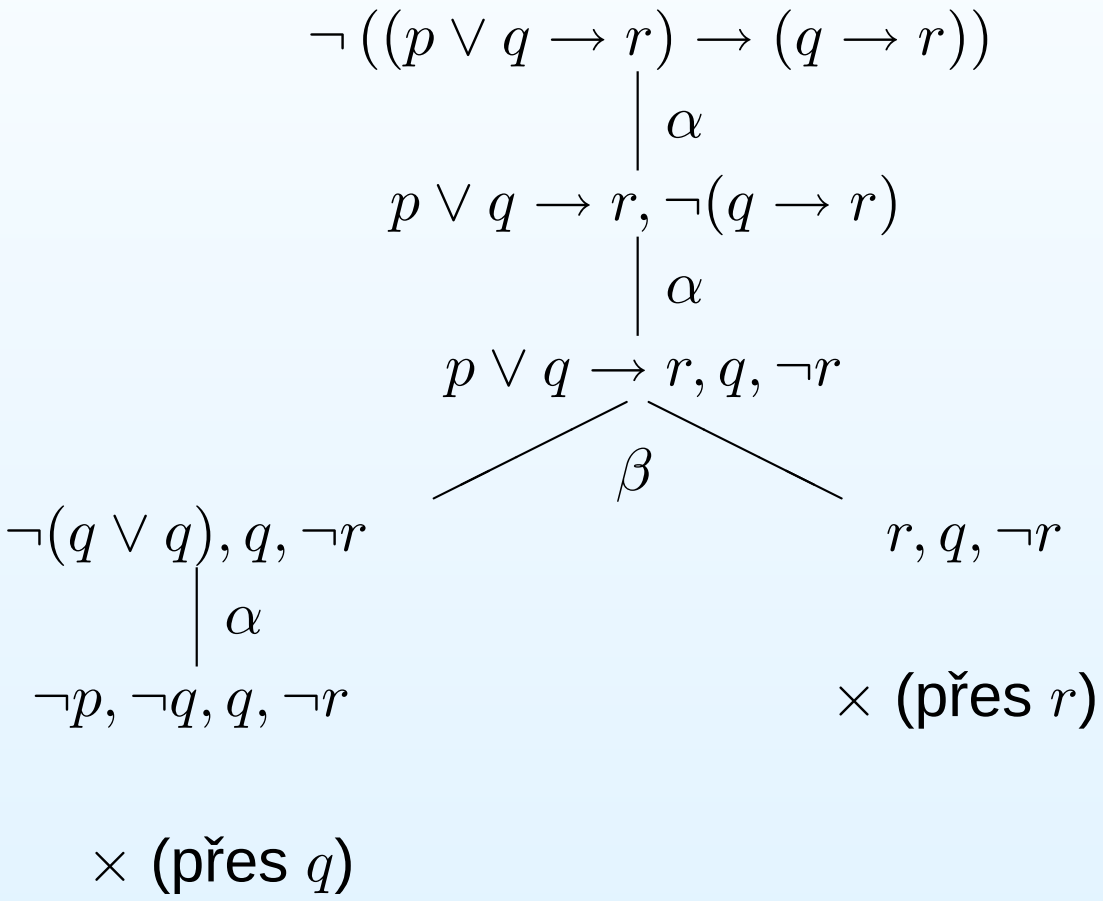
1. Sémantické – vyhodnocujeme podle sémantické hodnoty prvků formule, pracujeme s pravdivostními hodnotami (dosazumeme, prověřujeme různá ohodnocení):
   - sémantická tabulka,
   - sémantický strom (Quinův algoritmus).

Důkazové metody

1. Sémantické – vyhodnocujeme podle sémantické hodnoty prvků formule, pracujeme s pravdivostními hodnotami (dosazumeme, prověřujeme různá ohodnocení):
   - sémantická tabulka,
   - sémantický strom (Quinův algoritmus).
2. Syntaktické – řídíme se výhradně podle syntaktické struktury formule, netestujeme podle dosazených hodnot:
   - sémantické tablo,
   - rezoluce.

Sémantické tablo

Dokažte větu $\boxed{p \vee q \to r \models q \to r}$



Nepřímá rezoluce

Dokažte větu $\boxed{\{p \vee q, p \rightarrow r, q \rightarrow s\} \models r \vee s}$

Nepřímá rezoluce

Dokažte větu $\boxed{\{p \vee q, p \rightarrow r, q \rightarrow s\} \models r \vee s}$

Znegujeme: $(p \vee q)\&(p \rightarrow r)\&(q \rightarrow s)\&\neg(r \vee s)$.

Nepřímá rezoluce

Dokažte větu $\boxed{\{p \vee q, p \to r, q \to s\} \models r \vee s}$

Znegujeme: $(p \vee q)\&(p \to r)\&(q \to s)\&\neg(r \vee s)$.

Rezoluční odvozovací pravidlo je $A \vee B,\ \neg B \vee C \models A \vee C$

Nepřímá rezoluce

Dokažte větu $\{p \vee q, p \rightarrow r, q \rightarrow s\} \models r \vee s$

Znegujeme: $(p \vee q)\&(p \rightarrow r)\&(q \rightarrow s)\&\neg(r \vee s)$.

Rezoluční odvozovací pravidlo je $A \vee B,\ \neg B \vee C \models A \vee C$

1.	$p \vee q$	
2.	$\neg p \vee r$	
3.	$\neg q \vee s$	
4.	$\neg r$	*první konjunkt negace závěru*
5.	$\neg s$	*druhý konjunkt negace závěru*
6.	$\neg p$	R(2,4)
7.	q	R(1,6)
8.	s	R(3,7)
9.	$\square$	R(5,8)

Deduktivní úsudek

zapisujeme schématem $P_1, P_2, \ \ldots, P_n \models Z$, kde

- $P_1, P_2, \ \ldots, P_n, Z$ jsou tvrzení,
- $P_1, P_2, \ \ldots, P_n$ nazýváme *předpoklady* (premisy),
- Z je *závěr*.

Deduktivní úsudek

zapisujeme schématem $P_1, P_2, \ \ldots, P_n \models Z$, kde

- $P_1, P_2, \ \ldots, P_n, Z$ jsou tvrzení,
- $P_1, P_2, \ \ldots, P_n$ nazýváme *předpoklady* (premisy),
- Z je *závěr*.

Platný deduktivní úsudek:

- Z platnosti předpokladů usuzujeme na platnost závěru.

Deduktivní úsudek

zapisujeme schématem $P_1, P_2, \ \ldots, P_n \models Z$, kde

- $P_1, P_2, \ \ldots, P_n, Z$ jsou tvrzení,
- $P_1, P_2, \ \ldots, P_n$ nazýváme *předpoklady* (premisy),
- Z je *závěr*.

Platný deduktivní úsudek:

- Z platnosti předpokladů usuzujeme na platnost závěru.
- Ve všech případech, kdy jsou platné zároveň všechny předpoklady, musí být platný i závěr (tedy nesmí nastat situace, ve které by všechny předpoklady byly pravdivé a závěr nepravdivý).

Deduktivní úsudek

zapisujeme schématem $P_1, P_2, \ \ldots, P_n \models Z$, kde

- $P_1, P_2, \ \ldots, P_n, Z$ jsou tvrzení,
- $P_1, P_2, \ \ldots, P_n$ nazýváme *předpoklady* (premisy),
- Z je *závěr*.

Platný deduktivní úsudek:

- Z platnosti předpokladů usuzujeme na platnost závěru.
- Ve všech případech, kdy jsou platné zároveň všechny předpoklady, musí být platný i závěr (tedy nesmí nastat situace, ve které by všechny předpoklady byly pravdivé a závěr nepravdivý).
- „Ve všech případech“ může znamenat například ve výrokové logice „při všech možných ohodnoceních výrokových symbolů“.

Deduktivní úsudek

Větu *nesmí nastat situace, ve které by všechny předpoklady byly pravdivé a závěr nepravdivý* můžeme symbolicky přepsat jako

$$\neg\left(P_1 \& P_2 \& \ldots \& P_n \& \neg Z\right)$$
$$\neg\left(\left(P_1 \& P_2 \& \ldots \& P_n\right) \& \neg Z\right)$$
$$\left(P_1 \& P_2 \& \ldots \& P_n\right) \rightarrow Z$$

Deduktivní úsudek

Větu *nesmí nastat situace, ve které by všechny předpoklady byly pravdivé a závěr nepravdivý* můžeme symbolicky přepsat jako

$$\neg\left(P_1 \& P_2 \& \ldots \& P_n \& \neg Z\right)$$
$$\neg\left(\left(P_1 \& P_2 \& \ldots \& P_n\right) \& \neg Z\right)$$
$$\left(P_1 \& P_2 \& \ldots \& P_n\right) \rightarrow Z$$

Zapisujeme $P_1, P_2, \ldots, P_n \models Z$.

Odvozovací pravidlo

Odvozovací pravidlo je metoda, kterou lze použít pro odvození jednoho tvrzení z jiných. Musí splňovat vlastnosti deduktivního úsudku, tedy zachovávat platnost (závěr odvozený z platných předpokladů musí být také platný).

Definice důkazu

Důkaz tvrzení T z předpokladů $P_1, P_2, \ldots, P_n$ je taková posloupnost tvrzení $B_1, B_2, \ldots, B_m$, kde $B_m = T$ a každý její člen $B_i, 1 \leq i \leq m$ je:

- jeden z předpokladů P_j nebo
- vznikl uplatněním některého odvozovacího pravidla daného formálního systému na předchozí členy posloupnosti.

Věta o důkazech

Nechť dokazovaná formule F je ve tvaru $A \rightarrow B$. Pak platí:

$$
\begin{array}{rcll}
(A \rightarrow B) & \Leftrightarrow & (\neg B \rightarrow \neg A\ ) & \textit{Nepřímý důkaz} \\
(F \leftrightarrow true) & \Leftrightarrow & (\neg F \leftrightarrow false) & \textit{Důkaz sporem} \\
((A \rightarrow B) \leftrightarrow true) & \Leftrightarrow & ((A\ \&\neg B) \leftrightarrow false) &
\end{array}
$$

Všechny tyto vztahy jsou dokazatelné například sémantickou tabulkou.

Důkazy

1. Zda daná formule je tautologií.
2. Jestli daný závěr vyplývá ze zadaných předpokladů.
3. Co by mohlo vyplývat ze zadaných předpokladů.

Důkazy

1. Zda daná formule je tautologií.
2. Jestli daný závěr vyplývá ze zadaných předpokladů.
3. Co by mohlo vyplývat ze zadaných předpokladů.

Důkazy dělíme na:

- *Přímé* – z množiny předpokladů odvozujeme závěr podle daných odvozovacích pravidel.
- *Nepřímé* – formuli popřeme a dokážeme, že tato negace je kontradikce, tedy dojdeme ke sporu, jde o důkaz sporem.

Logické systémy

Stavební kameny – *axiomy*,

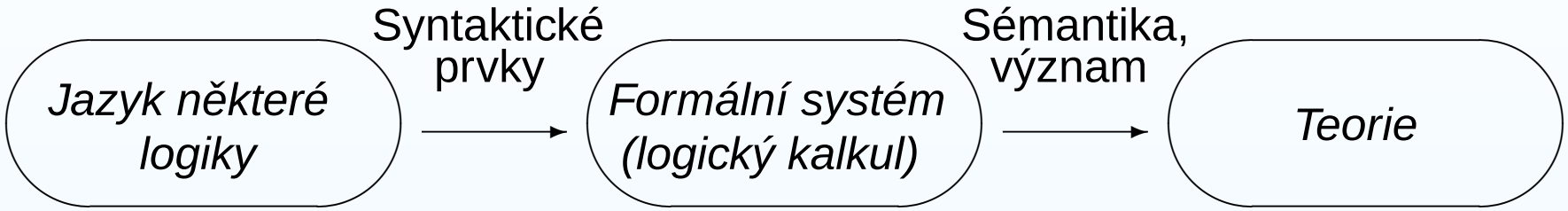
Metody – *odvozovací pravidla* (syntaktická)

Odvozená tvrzení – *věty*, *teorémy*

Znak $\models$ značí logické vyplývání, u formálních systémů budeme pro tytéž účely používat znak $\vdash$ – symbol pro dokazatelnost.

Formální systém nad daným formálním jazykem je množina tvrzení formulovaných v tomto jazyce.

Logické systémy



výroková,
predikátová,
. . .

Hilbertovský,
Gentzenovský,
přirozené dedukce,
. . .

teorie uspořádání,
teorie grup,
různ. fyzikální teorie,
. . .

Formální systémy

- axiomatické
- předpokladové

Formální systémy

Axiomatický systém je určen

- jazykem (obvykle výroková nebo predikátová logika, příp. s omezením spojek),
- logickými axiomy,
- odvozovacími pravidly.

Předpokladový formální systém je určen

- jazykem,
- dedukčními pravidly.

Speciální axiomy

jsou tvrzení, která považujeme za platná v rámci této teorie (tj. v zamýšlené interpretaci), ale nemusí být platná v každé interpretaci

$$\exists n \forall x (x \cdot n = x \ \ \& \ n \cdot x = x)$$

Speciální axiomy

jsou tvrzení, která považujeme za platná v rámci této teorie (tj. v zamýšlené interpretaci), ale nemusí být platná v každé interpretaci

$$\exists n \forall x (x \cdot n = x \ \ \& \ n \cdot x = x)$$

Teorii vytvoříme tak, že k vybranému formálnímu systému přidáme speciální axiomy, tedy odvozovací (deduktivní) pravidla můžeme používat na logické axiomy, již odvozené věty a speciální axiomy.

Vlastnosti důkazových metod

U metod sémantické analýzy vyžadujeme tyto vlastnosti:

- sémantická korektnost,
- sémantická úplnost.

Vlastnosti formálních systémů

U formálních systémů jsou obvykle důležité tyto vlastnosti:

- sémantická korektnost,
- sémantická úplnost,
- bezespornost.

Užitečnou vlastností je také minimálnost. U formálních systémů se vyžaduje především korektnost a bezespornost.

Definice

Korektnost:

Důkazová metoda je sémanticky korektní, je-li každá pomocí ní dokazatelná formule logicky platná (tedy pokud lze formuli dokázat pomocí této metody, musí být logicky platná).

Úplnost:

Důkazová metoda je sémanticky úplná, lze-li pomocí ní dokázat všechny logicky platné formule.

Vztah korektnost–úplnost

M – metoda, jejíž korektnost a úplnost zkoumáme,
$\mathcal{F}_M$ – množina všech formulí dokazatelných metodou M,
$\mathcal{P}$ – množina všech logicky platných formulí.

Vztah korektnost–úplnost

M – metoda, jejíž korektnost a úplnost zkoumáme,
$\mathcal{F}_M$ – množina všech formulí dokazatelných metodou M,
$\mathcal{P}$ – množina všech logicky platných formulí.

Množinově:

Korektnost: $\mathcal{F}_M \subseteq \mathcal{P}$
Úplnost: $\mathcal{F}_M \supseteq \mathcal{P}$

Zároveň korektní a úplná: $\mathcal{F}_M \cong \mathcal{P}$

Vztah korektnost–úplnost

M – metoda, jejíž korektnost a úplnost zkoumáme,
$\mathcal{F}_M$ – množina všech formulí dokazatelných metodou M,
$\mathcal{P}$ – množina všech logicky platných formulí.

Množinově:

Korektnost: $\mathcal{F}_M \subseteq \mathcal{P}$
Úplnost: $\mathcal{F}_M \supseteq \mathcal{P}$

Zároveň korektní a úplná: $\mathcal{F}_M \cong \mathcal{P}$

Pomocí implikací:

Korektnost: $\mathcal{F}_M \longrightarrow \mathcal{P}$
Úplnost: $\mathcal{F}_M \longleftarrow \mathcal{P}$

Zároveň korektní a úplná: $\mathcal{F}_M \longleftrightarrow \mathcal{P}$