Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2015/2016

5. prednáška

Hilbertovský a tablový kalkul

21. marca 2016

Obsah 5. prednášky

Kalkul

Kalkul je systém odvodzovacích pravidiel.
Odvodzovacie pravidlo je $(n+1)$-tica formúl zapisovaná

$$\text{(R)} \quad \frac{A_1 \ \cdots \ A_n}{A}$$

Formuly $A_1, \ldots, A_n$ nazývame *premisami* pravidla (R).
Formulu A nazývame *záver* pravidla (R).
Pravidlo bez premís ($n = 0$) nazývame *axióma* a namiesto

$$\frac{}{A}$$

ho zapisujeme iba A.

Hilbertovský kalkul — axiómy a pravidlo

Definícia

Hilbertovský kalkul sa skladá z axióm vytvorených podľa nasledujúcich *schém axióm* pre všetky formuly A, B, C:

(A1) $(A \to (B \to A))$
(A2) $((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$
(A3) $((\neg A \to \neg B) \to (B \to A))$

(A4) $((A \wedge B) \to A)$, $((A \wedge B) \to B)$
(A5) $(A \to (B \to (A \wedge B)))$
(A6) $((A \to (A \vee B))$, $(B \to (A \vee B))$
(A7) $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$

a pravidla *modus ponens*:

(MP) $$\frac{A \quad (A \to B)}{B}$$

pre všetky formuly A a B.

Hilbertovský kalkul — dôkaz

Definícia

(Formálnym) dôkazom z množiny predpokladov S je postupnosť formúl $Y_1, Y_2, \ldots, Y_n$, v ktorej každá formula Y_i je

- predpoklad z množiny S, alebo
- záver odvodzovacieho pravidla, ktorého premisy sa nachádzajú v postupnosti pred Y_i, teda špeciálne
  - Y_i je axióma, inštancia jednej zo schém (A1)–(A7), alebo
  - existujú $j < i$ a $k < i$ také, že Y_i je záver pravidla (MP) pre formuly Y_j a $Y_k = (Y_j \to Y_i)$.

Dôkazom formuly X z S je taký dôkaz z S, ktorého posledným členom je X.
Formula X je *dokázateľná* z množiny predpokladov S (skrátene $S \vdash X$) vtt, keď existuje dôkaz X z S.

(Švejdar, 2002, §1.3)

Príklad dôkazu v hilbertovskom kalkule

Príklad

Nájdime dôkaz formuly $Z = (X \to X)$ (pre ľubovoľnú formulu X) z $\{\}$:

$Y_1 = (X \to (X \to X))$ inštancia (A1) pre $A = B = X$

$Y_2 = (X \to ((X \to X) \to X))$ inšt. (A1) pre $A = X$, $B = (X \to X)$

$Y_3 = ((X \to ((X \to X) \to X)) \to ((X \to (X \to X)) \to (X \to X)))$ inšt. (A2) pre $A = C = X$, $B = (X \to X)$

$Y_4 = ((X \to (X \to X)) \to (X \to X))$ záver (MP) pre Y_2 a Y_3

$Y_5 = (X \to X)$ záver (MP) pre Y_1 a Y_4

Veta o dedukcii

Veta (o dedukcii)

$S \cup \{X\} \vdash Y$ *vtt* $S \vdash (X \to Y)$

Dôkaz.

($\Leftarrow$) Nech $Y_1, \ldots, Y_n$ je dôkaz $(X \to Y)$ z S. Potom $Y_1, \ldots, Y_n, X, Y$ je dôkaz Y z $S \cup \{X\}$.
($\Rightarrow$) Nech $Y_1, \ldots, Y_n$ je dôkaz Y z $S \cup \{X\}$. Úplnou indukciou na k dokážeme, že $S \vdash (X \to Y_k)$.
Báza: Nech $k = 1$. Y_1 nemohla byť odvodená pravidlom (MP), takže je buď axióma, alebo patrí do S, alebo je X. V prvých dvoch prípadoch je postupnosť Y_1, $(Y_1 \to (X \to Y_1))$, $(Y_1 \to (X \to Y_1))$, $(X \to Y_1)$ dôkazom $(X \to Y_1)$. V treťom prípade použijeme dôkaz z predchádzajúceho príkladu.
Ind. krok: Nech $k > 1$ a platí IP: pre všetky $j < k$ máme $S \vdash (X \to Y_j)$.
Ak Y_k je axióma, patrí do S, alebo je X, postupujeme ako pre $k = 1$.
Ak je Y_k záverom pravidla (MP) pre Y_i a $Y_j = (Y_i \to Y_k)$, tak $i, j < k$ a platí pre ne IP. Teda existuje dôkaz $A_1, \ldots, A_a$ formuly $A_a = (X \to Y_i)$ z S a dôkaz $B_1, \ldots, B_b$ formuly $B_b = (X \to (Y_i \to Y_k))$ z S. Dôkazom formuly $(X \to Y_k)$ potom je: $A_1, \ldots, A_a, B_1, \ldots, B_b, ((X \to (Y_i \to Y_k)) \to ((X \to Y_i) \to (X \to Y_k)))$, $((X \to Y_i) \to (X \to Y_k))$, $(X \to Y_k)$. □

Korektnosť a úplnosť hilbertovského kalkulu

Veta

Pre každú množinu formúl S a každú formulu X platí:

(korektnosť) *ak je X dokázateľná z S, tak X výrokovologicky vyplýva z S;*

(úplnosť) *ak X výrokovologicky vyplýva z S, tak X je dokázateľná z S.*

Korektnosť (angl. soundness) hilbertovského kalkulu vyplýva matematickou indukciou na dĺžku dôkazu z korektnosti pravidiel: Ak S je množina výrokových formúl a

$$\frac{A_1 \quad \cdots \quad A_n}{A}$$

je pravidlo (axióma alebo (MP)), potom ak $A_1, \ldots, A_n$ súčasne vyplývajú z S, tak aj A vyplýva z S.

Dôkaz tautológie sporom

V slovenčine

Príklad

Je formula $X = (p \to (q \to (p \land q)))$ tautológia?
Dokážme tvrdenie sporom: Zoberme ľubovoľné ohodnotenie v a predpokladajme (1) $v \not\models (p \to (q \to (p \land q)))$.
Potom podľa definície spĺňania (2) $v \models p$ a (3) $v \not\models (q \to (p \land q))$, teda opäť podľa definície spĺňania (4) $v \models q$ a (5) $v \not\models (p \land q)$.
Z faktu (5) dostávame, že (6) $v \not\models p$ alebo (7) $v \not\models q$. Nevieme, ktorá z týchto možností platí pre v, ale môžeme ich predpokladať *nezávisle od seba*:

- Nech platí (6), teda $v \not\models p$. To je však v spore s faktom (2).
- Nech platí (7). To je v spore s faktom (4).

V oboch prípadoch sme dospeli k sporu a ďalšie možnosti nie sú.
Preto $v \models X$.

Dôkaz tautológie sporom

Notácia

Príklad

Predchádzajúcu úvahu môžeme stručne zapísať, ak sa dohodneme, že:

- **F**X označuje, že X je vo v nesplnená;
- **T**X 1označuje, že X je vo v splnená;
- ak z niektorého z predchádzajúcich faktov vyplýva priamo z definície spĺňania nový fakt, zapíšeme ho do ďalšieho riadka;
- ak z niektorého faktu vyplýva, že platí fakt F_1 alebo fakt F_2, rozdelíme úvahu na dve nezávislé *vetvy*, pričom prvá začne faktom F_1 a druhá faktom F_2;
- ak nastane spor, pridáme riadok so symbolom $*$.

Dôkaz tautológie sporom

Použitím notácie

Príklad

$$
\begin{array}{lllll|llll}
(1) & & & \multicolumn{6}{c}{\mathbf{F}(p \to (q \to (p \land q)))} & \\
(2) & & & \multicolumn{6}{c}{\mathbf{T}p} & \text{z } (1) \\
(3) & & & \multicolumn{6}{c}{\mathbf{F}(q \to (p \land q))} & \text{z } (1) \\
(4) & & & \multicolumn{6}{c}{\mathbf{T}q} & \text{z } (3) \\
(5) & & & \multicolumn{6}{c}{\mathbf{F}(p \land q)} & \text{z } (3) \\
(6) & \mathbf{F}p & \text{z } (5) & & & (7) & \mathbf{F}q & & \text{z } (5) \\
 & * & \text{medzi } (2) \text{ a } (6) & & & & * & & \text{medzi } (4) \text{ a } (7)
\end{array}
$$

Splĺňanie a priame podformuly

Pozorovanie

Nech v je ľubovoľné ohodnotenie výrokových premenných. Nech X a Y sú ľubovoľné formuly.

1. 1.1 *Ak v splĺňa $\neg X$, tak v nesplĺňa X.*
   1.2 *Ak v nesplĺňa $\neg X$, tak v splĺňa X.*
2. 2.1 *Ak v splĺňa $(X \land Y)$, tak v splĺňa X a v splĺňa Y.*
   2.2 *Ak v nesplĺňa $(X \land Y)$, tak v nesplĺňa X alebo v nesplĺňa Y.*
3. 3.1 *Ak v splĺňa $(X \lor Y)$, tak v splĺňa X alebo v splĺňa Y.*
   3.2 *Ak v nesplĺňa $(X \lor Y)$, tak v nesplĺňa X a v nesplĺňa Y.*
4. 4.1 *Ak v splĺňa $(X \to Y)$, tak v nesplĺňa X alebo v splĺňa Y.*
   4.2 *Ak v nesplĺňa $(X \to Y)$, tak v splĺňa X a v nesplĺňa Y.*

Označené formuly a ich sémantika

Definícia

Nech X je formula výrokovej logiky. Postupnosti symbolov $\mathbf{T}X$ a $\mathbf{F}X$ nazývame *označenými formulami*.

Definícia

Nech v je ohodnotenie výrokových premenných a X je formula. Potom

- v spĺňa $\mathbf{T}X$ vtt v spĺňa X;
- v spĺňa $\mathbf{F}X$ vtt v nespĺňa Y.

Tablové pravidlá

Predchádzajúce pozorovanie a definície umožňujú formulovať pravidlá:

$$\frac{\alpha}{\begin{array}{c}\alpha_1\\ \alpha_2\end{array}} \qquad \frac{\beta}{\beta_1 \mid \beta_2}$$

$$\frac{\mathbf{T}(X \land Y)}{\begin{array}{c}\mathbf{T}X\\ \mathbf{T}Y\end{array}} \qquad \frac{\mathbf{F}(X \land Y)}{\mathbf{F}X \mid \mathbf{F}Y} \qquad \frac{\mathbf{T}\neg X}{\mathbf{F}X}$$

$$\frac{\mathbf{F}(X \lor Y)}{\begin{array}{c}\mathbf{F}X\\ \mathbf{F}Y\end{array}} \qquad \frac{\mathbf{T}(X \lor Y)}{\mathbf{T}X \mid \mathbf{T}Y} \qquad \frac{\mathbf{F}\neg X}{\mathbf{T}X}$$

$$\frac{\mathbf{F}(X \to Y)}{\begin{array}{c}\mathbf{T}X\\ \mathbf{F}Y\end{array}} \qquad \frac{\mathbf{F}(X \to Y)}{\mathbf{T}X \mid \mathbf{T}Y}$$

Tablové pravidlá — jednotný zápis

Označenými formulami typu A sú formuly v tvare $\mathbf{T}(X \land Y)$, $\mathbf{F}(X \lor Y)$, $\mathbf{F}(X \to Y)$, $\mathbf{T}\neg X$, $\mathbf{F}\neg X$.
Označenými formulami typu B sú formuly v tvare $\mathbf{F}(X \land Y)$, $\mathbf{T}(X \lor Y)$, $\mathbf{T}(X \to Y)$.

α	α_1	α_2
$\mathbf{T}(X \land Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{F}(X \lor Y)$	$\mathbf{F}X$	$\mathbf{F}Y$
$\mathbf{F}(X \to Y)$	$\mathbf{T}X$	$\mathbf{F}Y$
$\mathbf{T}\neg X$	$\mathbf{F}X$	$\mathbf{F}X$
$\mathbf{F}\neg X$	$\mathbf{T}X$	$\mathbf{T}X$

$$\frac{\alpha}{\begin{array}{c}\alpha_1\\ \alpha_2\end{array}}$$

β	β_1	β_2
$\mathbf{F}(X \land Y)$	$\mathbf{F}X$	$\mathbf{F}Y$
$\mathbf{T}(X \lor Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{T}(X \to Y)$	$\mathbf{F}X$	$\mathbf{T}Y$

$$\frac{\beta}{\beta_1 \mid \beta_2}$$

Tablo pre formulu

Definícia

Analytické tablo pre označenú formulu X (skrátene *tablo pre* X) je binárny strom, ktorého vrcholy obsahujú označené formuly a je skonštruovaný podľa nasledovných rekurzívnych pravidiel:

- Strom s jediným vrcholom obsahujúcim X (koreň) je tablom pre X.
- Nech $\mathcal{T}$ je tablo pre X a y je nejaký jeho list. Potom tablom pre X je aj každé rozšírenie $\mathcal{T}$ pomocou ktorejkoľvek z nasledujúcich operácií:
  - A: Ak sa na vetve π_y (ceste z koreňa do y) vyskytuje nejaká označená formula α, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci α_1 alebo α_2.
  - B: Ak sa na vetve π_y vyskytuje nejaká označená formula β, tak ako deti y pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.

Uzavretosť

Definícia

Vetva π tabla $\mathcal{T}$ je *uzavretá* vtt obsahuje označené formuly $\mathbf{F}X$ a $\mathbf{T}X$ pre nejakú formulu X. Inak je π *otvorená*.

Tablo $\mathcal{T}$ je *uzavreté* vtt každá jeho vetva je uzavretá.
Naopak, $\mathcal{T}$ je *otvorené* vtt aspoň jedna jeho vetva je otvorená.

Korektnosť tablového kalkulu

Veta (Korektnosť tablovej metódy)

Nech X je formula a $\mathcal{T}$ je uzavreté tablo pre $\mathbf{F}X$.
Potom X je tautológia.

Pozorovanie

Formula X je tautológia vtt $\mathbf{F}X$ je nesplniteľná.

Veta

Nech $\mathcal{T}$ je uzavreté tablo pre označenú formulu X.
Potom X je nesplniteľná.

Dôsledok korektnosti pre splniteľnosť

Pozorovanie

Nech $S = \{A_1, \ldots, A_n\}$ *je konečná množina formúl a* X *je formula. Potom* X *vyplýva z* S *vtt formula* $((\bigwedge_{i=1}^{n} A_i) \to X)$ *je tautológia.*

Tvrdenie

Nech $S = \{A_1, \ldots, A_n\}$ *je konečná množina formúl a* X *je formula.*
Nech $\mathcal{T}$ *je uzavreté tablo pre* $\mathbf{F}((\bigwedge_{i=1}^{n} A_i) \to X)$*.*
Potom X *vyplýva z* S*.*

Literatúra

SMULLYAN, R. M. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.

ŠVEJDAR, V. *Logika: neúplnost, složitost, nutnost*. Academia, 2002. Prístupné aj na `http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf`.