Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2016/2017

5. prednáška

Hilbertovský a tablový kalkul

20. marca 2017

Obsah 5. prednášky

1. Výroková logika
   - Kalkuly
   - Hilbertovský kalkul
   - Tablový kalkul
     - Korektnosť

Organizačné poznámky

Konzultačné hodiny
streda 13:10–14:30
na I-16 (Kľuka) a I-7 (Šiška k praktickým cvičeniam)

Midterm
- piatok 7. apríla o 12:30 v A
- (pondelok 10. apríla o 18:10 v A)

Vysvetľovanie riešení
Vysvetľujte svoj postup, odvolávajte sa na definície, dajte najavo, že chápete súvislosť medzi definovanými pojmami, ktoré sa nachádzajú v zadaní a technikou, ktorú používate na vyriešenie úlohy

Domáce úlohy
Ohodnotené a okomentované riešenia na cvičeniach
Konzultácie po cvičeniach alebo počas konzult. hodín

Usudzovacie pravidlá

- Na úvodnej prednáške sme *usudzovacie pravidlo* neformálne zadefinovali ako *vzor (šablóna) úsudkov*, napríklad:

$$\left.\begin{array}{l}\text{Ak } A\text{, tak } B.\\ A.\end{array}\right\}\ \text{vzory premís}$$
$$\overline{\phantom{\text{Ak } A\text{, tak } B.}}$$
$$B. \qquad\qquad \text{vzor záveru}$$

- Úsudok získame dosadením výrokov (alebo výrokových foriem) na príslušné miesta v pravidle
- Teraz sa pokúsime:
  - formálne zadefinovať pravidlá,
  - ukázať, ako pravidlami budujeme *dôkazy* vyplývania,
  - diskutovať, či sú správne a či môžeme dokázať všetky vyplývania

Kalkul

Neformálne definície:

- *Odvodzovacie pravidlo* je množina $(n+1)$-tíc formúl, zapisovaných

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

  vytvorená substitúciou do jednej vzorovej $(n+1)$-tice.
  Formuly $A_1, \ldots, A_n$ nazývame *premisami* pravidla (R).
  Formulu A nazývame *záver* pravidla (R).
- Pravidlo bez premís $(n = 0)$ nazývame *schéma axióm* a namiesto

$$\frac{}{A}$$

  ho zapisujeme iba A.
- *Kalkul* je systém odvodzovacích pravidiel.

V.3.10 Hilbertovský kalkul

Hilbertovský kalkul — axiómy a pravidlo

Definícia 3.66

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) $((A \land B) \to A)$, $((A \land B) \to B)$
(A5) $(A \to (B \to (A \land B)))$
(A6) $((A \to (A \lor B))$, $(B \to (A \lor B))$
(A7) $((A \to C) \to ((B \to C) \to ((A \lor B) \to C)))$

a pravidla *modus ponens*:

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

pre všetky formuly A a B.

Hilbertovský kalkul — dôkaz

Definícia 3.67

(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 3.68

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

$Y_1 = (X \to (X \to X))$ 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 3.69 (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 treťom prípade použijeme dôkaz $(X \to X)$ z predchádzajúceho príkladu 3.68. V prvých dvoch prípadoch je postupnosť $Y_1, (Y_1 \to (X \to Y_1)), (X \to Y_1)$ dôkazom $(X \to Y_1)$.
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: $A_1, \ldots, A_a, B_1, \ldots, B_b, ((X \to (Y_i \to Y_k)) \to ((X \to Y_i) \to (X \to Y_k))), ((X \to Y_i) \to (X \to Y_k)), (X \to Y_k)$. $\square$

Dokazovanie s vetou o dedukcii

Príklad 3.70

Ukážme $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
(pre ľubovoľné formuly A, B a C).
Podľa vety o dedukcii máme $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
vtt $\{(A \to B)\} \vdash ((B \to C) \to (A \to C))$ vtt
$\{(A \to B), (B \to C)\} \vdash (A \to C)$ vtt $\{(A \to B), (B \to C), A\} \vdash C$.
Posledný dôkaz nájdeme veľmi ľahko:

$Y_1 =$	A	predpoklad
$Y_2 =$	$(A \to B)$	predpoklad
$Y_3 =$	B	(MP) pre Y_1 a Y_2
$Y_4 =$	$(B \to C)$	predpoklad
$Y_5 =$	C	(MP) pre Y_3, Y_4

Podľa úvodnej úvahy teda $\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
(ale nevieme, ako tento dôkaz presne vyzerá).

Dokazovanie s vetou o dedukcii

Príklad 3.71

Ukážme $\{\} \vdash (\neg X \to (X \to Y))$ (pre ľubovoľné formuly X a Y).

$Y_1 = (\neg X \to (\neg Y \to \neg X))$ (A1) pre $A = \neg X$, $B = \neg Y$

$Y_2 = ((\neg Y \to \neg X) \to (X \to Y))$ (A3) pre $A = Y$, $B = X$

$\vdots$ dôkaz z príkladu 3.70

$$Y_n = \big((\neg X \to (\neg Y \to \neg X)) \to \\ (((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y)))\big)$$

$Y_{n+1} = (((\neg Y \to \neg X) \to (X \to Y)) \to (\neg X \to (X \to Y)))$ (MP) pre Y_1 a Y_n

$Y_{n+2} = (\neg X \to (X \to Y))$ (MP) pre Y_2 a Y_{n+1}

Korektnosť a úplnosť hilbertovského kalkulu

Veta 3.72

Pre každú množinu formúl S a každú formulu X platí:

(korektnosť) *ak je X dokázateľná z S ($S \vdash X$), tak X výrokovologicky vyplýva z S ($S \models X$);*

(úplnosť) *ak X výrokovologicky vyplýva z S ($S \models X$), tak X je dokázateľná z S ($S \vdash X$).*

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.
Úplnosť (angl. completeness) je komplikovanejšia.

Vyskúšajte si V.1

Ukážte $\{\} \vdash (\neg\neg X \to X)$.

(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) $((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$

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

$S \cup \{X\} \vdash Y$ vtt $S \vdash (X \to Y)$
$\{\} \vdash (X \to X)$
$\{\} \vdash ((A \to B) \to ((B \to C) \to (A \to C)))$
$\{\} \vdash (\neg X \to (X \to Y))$

V.3.11 Tablový kalkul

Dôkaz tautológie sporom

V slovenčine

Príklad 3.73

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 3.74

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

- $\mathbf{F}X$ označuje, že v nespĺňa X;
- $\mathbf{T}X$ označuje, že v spĺňa X;
- 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 3.75

(1)			$\mathbf{F}(p \to (q \to (p \wedge q)))$			
(2)			$\mathbf{T}p$			z (1)
(3)			$\mathbf{F}(q \to (p \wedge q))$			z (1)
(4)			$\mathbf{T}q$			z (3)
(5)			$\mathbf{F}(p \wedge q)$			z (3)
(6)	$\mathbf{F}p$	z (5)		(7)	$\mathbf{F}q$	z (5)
	$*$	medzi (2) a (6)			$*$	medzi (4) a (7)

Splĺňanie a priame podformuly

Pozorovanie 3.76

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

1. T) *Ak v splĺňa $\neg X$, tak v nesplĺňa X.*
   F) *Ak v nesplĺňa $\neg X$, tak v splĺňa X.*
2. T) *Ak v splĺňa $(X \land Y)$, tak v splĺňa X a v splĺňa Y.*
   F) *Ak v nesplĺňa $(X \land Y)$, tak v nesplĺňa X alebo v nesplĺňa Y.*
3. T) *Ak v splĺňa $(X \lor Y)$, tak v splĺňa X alebo v splĺňa Y.*
   F) *Ak v nesplĺňa $(X \lor Y)$, tak v nesplĺňa X a v nesplĺňa Y.*
4. T) *Ak v splĺňa $(X \to Y)$, tak v nesplĺňa X alebo v splĺňa Y.*
   F) *Ak v nesplĺňa $(X \to Y)$, tak v splĺňa X a v nesplĺňa Y.*

Označené formuly a ich sémantika

Definícia 3.77

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

Definícia 3.78

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.

Dohoda

Pre označené formuly budeme používať veľké písmená zo začiatku a konca abecedy s horným indexom $+$ a prípadne s dolnými indexmi, napr. A^+, X_7^+.
Pre množiny označených formúl budeme používať písmená S, T s horným indexom $+$ a prípadne s dolnými indexmi, napr. S^+, T_3^+.

Tablové pravidlá

Podľa pozorovania 3.76 a definície 3.78 môžeme sformulovať pravidlá pre označené formuly:

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

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

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

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

Jednotný zápis označených formúl — α

Definícia 3.79 (Jednotný zápis označených formúl typu α)

Označená formula A^+ je typu α, ak má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y.
Takéto formuly budeme označovať písmenom α;
α_1 bude označovať príslušnú označenú formulu zo stredného stĺpca
a α_2 príslušnú formulu z pravého stĺpca.

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

Pozorovanie 3.80 (Zostručnené vďaka jednotnému zápisu)

Nech v je ľubovoľné ohodnotenie výrokových premenných.
Ak v spĺňa α, tak v spĺňa α_1 a v spĺňa α_2.

Jednotný zápis označených formúl — β

Definícia 3.81 (Jednotný zápis označených formúl typu β)

Označená formula B^+ je typu β, ak má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y.
Takéto formuly budeme označovať písmenom β;
β_1 bude označovať príslušnú označenú formulu zo stredného stĺpca a β_2 príslušnú formulu z pravého stĺpca.

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

Pozorovanie 3.82 (Zostručnené vďaka jednotnému zápisu)

Nech v je ľubovoľné ohodnotenie výrokových premenných.
Ak v spĺňa β, tak v spĺňa β_1 alebo v spĺňa β_2.

Tablo pre množinu označených formúl

Definícia 3.83

Analytické tablo pre množinu označených formúl S^+ (skrátene *tablo pre* S^+) je binárny strom, ktorého vrcholy obsahujú označené formuly a ktorý je skonštruovaný podľa nasledovných rekurzívnych pravidiel:

- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+.
- Nech $\mathcal{T}$ je tablo pre S^+ a y je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* $\mathcal{T}$ ktoroukoľvek z 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.
  - Ax: Ako jediné dieťa y pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Uzavretosť

Definícia 3.84

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 3.85 (Korektnosť tablového kalkulu)

Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Potom je množina S^+ nesplniteľná.

Dôsledok 3.86

Nech S je množina formúl a X je formula.
Ak existuje uzavreté tablo pre $\{\mathbf{T}A \mid A \in S\} \cup \{\mathbf{F}X\}$ (skr. $S \vdash X$), tak X vyplýva z S ($S \vDash X$).

Pozorovanie 3.87

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

Dôsledok 3.88

Nech X je formula a existuje uzavreté tablo pre $\{\mathbf{F}X\}$ (skr. $\vdash X$). Potom X je tautológia ($\vDash X$).

Literatúra

Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.

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

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