Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2017/2018

6. prednáška

Korektné pravidlá
Rezolvencia

26. marca 2018

Obsah 6. prednášky

2.8

Tablový kalkul

2.8.5 Nové korektné pravidlá

Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

- Na dokázanie *korektnosti* tablového kalkulu stačilo, aby mali pravidlá vlastnosť:

  Nech v je ohodnotenie. Ak v spĺňa premisu (a množinu S^+),
  tak spĺňa oba (α) závery/aspoň jeden (β) záver.

  - Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
  - Netreba opačnú implikáciu (ak *v* spĺňa oba/jeden záver, tak spĺňa premisu).
- Na dôkaz *úplnosti* stačili pravidlá (S^+), α, β,
  pretože stačia na vybudovanie úplného tabla.

Nové pravidlo

Čo sa stane, ak pridáme nové pravidlo, napríklad disjunktívny sylogizmus:

$$\frac{\mathbf{T}(A \vee B) \quad \mathbf{F}\,A}{\mathbf{T}\,B} \quad ? \qquad (\mathrm{DS}_1)$$

Upravíme definíciu priameho rozšírenia:

Úprava definície tabla

(…) 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** …
- ⋮
- DS_1: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(A \vee B)$ a $\mathbf{F}\,A$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}\,B$.

Nové pravidlo vs. korektnosť a úplnosť

- Pravidlo (DS_1) je *korektné*:
  Nech v je ľubovoľné ohodnotenie.
  Ak v spĺňa $\mathbf{T}(A \lor B)$ a $\mathbf{F}\,A$, tak v spĺňa $\mathbf{T}\,B$.
  Keďže $v \models \mathbf{T}(A \lor B)$, tak $v \models (A \lor B)$, teda $v \models A$ alebo $v \models B$.
  Pretože ale $v \models \mathbf{F}\,A$, tak $v \not\models A$. Takže $v \models B$.
- Preto stále dokážeme lemu K1 (**??**):

  > *Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných.*
  > *Ak v spĺňa S^+ a v spĺňa $\mathcal{T}$,*
  > *tak v spĺňa aj každé priame rozšírenie $\mathcal{T}$.*

  Z nej dokážeme K2 a vetu o korektnosti
- Pridanie pravidla neohrozuje úplnosť
  (doterajšími pravidlami stále vybudujeme úplné tablo).

Nové pravidlá vo všeobecnosti

Definícia 2.82 (Tablové pravidlo a jeho korektnosť)

Nech n a k sú prirodzené čísla, $n \geq 0$, $k > 0$, nech $P_1^+, \dots, P_n^+, C_1^+, \dots, C_k^+$ sú označené formuly nad výrokovými premennými $\{q_1, \dots, q_m\}$.

Tablové pravidlo R je množina dvojíc n-tíc a k-tic označených formúl

$$R = \left\{ \begin{array}{c|c|c} \multicolumn{3}{c}{P_1^+{}_{[q_1|X_1,\dots,q_m|X_m]} \quad \cdots \quad P_n^+{}_{[q_1|X_1,\dots,q_m|X_m]}} \\ \hline C_1^+{}_{[q_1|X_1,\dots,q_m|X_m]} & \dots & C_k^+{}_{[q_1|X_1,\dots,q_m|X_m]} \end{array} \;\middle|\; X_1, \dots, X_m \in \mathcal{E} \right\},$$

ktoré vzniknú súčasnou substitúciou formúl $X_1, \dots, X_m$ za premenné $q_1, \dots, q_m$ v označených formulách $P_1^+, \dots, P_n^+, C_1^+, \dots, C_k^+$.
Prvky hornej n-tice nazývame ***premisy***, prvky dolnej k-tice nazývame ***závery***.
Každý prvok R nazývame ***inštancia*** pravidla R.

Tablové pravidlo R je ***korektné*** (tiež *zdravé* z angl. *sound*) vtt pre každé ohodnotenie výrokových premenných v platí, že ak v spĺňa *všetky* premisy $P_1^+, \dots, P_n^+$, tak v spĺňa *niektorý* záver $C_1^+, \dots, C_k^+$.

Nové pravidlá vo všeobecnosti

Úprava definície tabla

(...)

- ...
- 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:

  $\vdots$

  R: Ak sa pre nejakú inštanciu pravidla R na vetve π_y nachádzajú *všetky* premisy $P_1^+, \ldots, P_n^+$, tak k uzlu y pripojíme k nových vrcholov obsahujúcich postupne závery $C_1^+, \ldots, C_k^+$.

2.9

Rezolvencia vo výrokovej logike

Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.
Je nasledujúce pravidlo korektné?

$$\frac{(A \longrightarrow B) \qquad (B \longrightarrow C)}{(A \longrightarrow C)}$$

Nahraďme implikácie disjunkciami:

$$\frac{(\neg A \lor B) \qquad (\neg B \lor C)}{(\neg A \lor C)}$$

Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 2.83

Rezolvenčný princíp (***rezolvencia***, angl. *resolution principle*) je pravidlo

$$\frac{(k_1 \lor \cdots \lor p \lor \cdots \lor k_m) \qquad (\ell_1 \lor \cdots \lor \neg p \lor \cdots \lor \ell_n)}{(k_1 \lor \cdots \lor k_m \lor \ell_1 \lor \cdots \lor \ell_n)}$$

pre ľubovoľnú výrokovú premennú p
a ľubovoľné literály $k_1, \ldots, k_m, \ell_1, \ldots, \ell_n$.

Klauzulu $(k_1 \lor \cdots \lor k_m \lor \ell_1 \lor \cdots \lor \ell_n)$ nazývame ***rezolventou*** klauzúl $(k_1 \lor \cdots \lor p \lor \cdots \lor k_m)$ a $(\ell_1 \lor \cdots \lor \neg p \lor \cdots \lor \ell_n)$.

Tvrdenie 2.84

Rezolvencia je korektné pravidlo, teda
rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.

Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

$$\frac{(\neg p \lor q) \quad (\neg q \lor r)}{(\neg p \lor r)} \qquad \frac{(p \to q) \quad (q \to r)}{(p \to r)} \qquad \text{(tranzitivita } \to\text{)}$$

$$\frac{(\neg p \lor \ell) \quad p}{\ell} \qquad \frac{(p \to \ell) \quad p}{\ell} \qquad \text{(modus ponens)}$$

$$\frac{(\neg p \lor q) \quad \neg q}{\neg p} \qquad \frac{(p \to q) \quad \neg q}{\neg p} \qquad \text{(modus tolens)}$$

Pozorovania o rezolvencii

- Rezolvencia s jednotkovou klauzulou skráti druhú klauzulu:

$$\frac{\neg q \quad (p \lor q \lor \neg r)}{(p \lor \neg r)}$$

- Nie každý logický dôsledok sa dá odvodiť rezolvenciou:
  $\{p, q\} \models (p \lor q)$

Pozorovania o rezolvencii

- Ak rezolvencia odvodí **prázdnu klauzulu**

$$\frac{\neg p \quad p}{\square},$$

premisy **nie sú súčasne splniteľné**

- Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch, ale je **nekorektné urobiť to naraz**:

$$\frac{(\neg p \lor q) \quad (p \lor \neg q)}{(q \lor \neg q)} \qquad \frac{(\neg p \lor q) \quad (p \lor \neg q)}{(\neg p \lor p)} \qquad \cancel{\frac{(\neg p \lor q) \quad (p \lor \neg q)}{\square}}$$

Prečo?
Lebo $\{(\neg p \lor q), (p \lor \neg q)\}$ je splniteľná
$(v_1 = \{p \mapsto t, q \mapsto t\}, v_2 = \{p \mapsto f, q \mapsto f\})$,
ale $\square$ je nesplniteľná

Problematické prípady

- Opakovaným aplikovaním rezolvencie môžeme odvodzovať ďalšie dôsledky

Príklad 2.85

Z množiny $S = \{(\neg p \lor r), (\neg q \lor r), (p \lor q)\}$ odvodíme $(r \lor r)$:

1. $(\neg p \lor r)$ predpoklad z S
2. $(\neg q \lor r)$ predpoklad z S
3. $(p \lor q)$ predpoklad z S
4. $(r \lor q)$ rezolventa (1) a (3)
5. $(r \lor r)$ rezolventa (2) a (4)

- Klauzula $(r \lor r)$ je evidentne ekvivalentná s r; r sa ale z množiny S iba rezolvenciou odvodiť nedá
- Preto potrebujeme ešte ***pravidlo idempotencie***:

$$\frac{(k_1 \lor \cdots \lor \ell \lor \cdots \lor \ell \lor \cdots \lor k_n)}{(k_1 \lor \ell \lor \cdots \lor k_n)}$$

Rezolvenčné odvodenie a zamietnutie

Definícia 2.86

Rezolvenčné odvodenie z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \dots, C_n, \dots$, ktorej každý člen C_i je:

- prvkom S alebo
- rezolventou dvoch predchádzajúcich klauzúl C_j a C_k pre $j < i$ a $k < i$, alebo
- záverom pravidla idempotencie pre nejakú predchádzajúcu klauzulu C_j, $j < i$.

Zamietnutím (angl. *refutation*) množiny klauzúl S je konečné rezolvenčné odvodenie, ktorého posledným prvkom je prázdna klauzula $\square$.

Definícia 2.87

Množinu klauzúl budeme nazývať aj ***klauzálna teória***.

Korektnosť a úplnosť rezolvencie

Veta 2.88 (Korektnosť rezolvencie)

Nech S je množina klauzúl.
Ak existuje zamietnutie S, tak S je nesplniteľná.

Veta 2.89 (Úplnosť rezolvencie)

Nech S je množina klauzúl.
Ak S je nesplniteľná, tak existuje zamietnutie S.

2.10 Späť k dôkazom o vyplývaní

Konzultácie a termín pre 6. sadu úloh

- Ak chcete
  - získať spätnú väzbu na riešenie nehodnotených úloh,
  - poradiť sa o riešení aktuálnej sady úloh (teoretických aj praktických),
  - poradiť sa o obsahu prednášok,
  - dať nám spätnú väzbu na obsah alebo formu vyučovania predmetu,

  využívajte **konzultačné hodiny**:

  streda od 13:10 do 14:30 v I-7 alebo I-16

- Riešenie **6. sady úloh** odovzdajte

  najneskôr vo štvrtok 5. apríla 2018 o 13:00
  v kancelárii **I-7 alebo I-16**

Uvažovanie o vyplývaní

Cvičenie 2.90

sada úloh 3, úloha 3 Nech X a Y sú ľubovoľné výrokové formuly, nech T je ľubovoľná výroková teória.

Dokážte alebo vyvráťte:

- **c** Ak $T \models \neg X$, tak $T \not\models X$.
- **d** Ak $T \not\models X$, tak $T \models \neg X$.
- **e** $T \models (X \rightarrow Y)$ vtt $T \cup \{X\} \models Y$.

su03/3c) Ak $T \models \neg X$, tak $T \not\models X$

Riešenie 2.90 (c)

Zoberme ľub. teóriu T a formulu X také, že $T \models \neg X$. *Aby* tvrdenie platilo:

- musí $T \not\models X$, teda (podľa definície vyplývania)
- *nesmie* byť pravda, že *každé* ohodnotenie spĺňajúce T spĺňa aj X, teda
- musí *existovať* ohodnotenie, ktoré *spĺňa* T a nespĺňa X, teda
- T musí byť *splniteľná*. Predpoklad $T \models \neg X$ to však nezaručuje: $T \models \neg X$ platí aj pre nesplniteľnú T (a vtedy dokonca pre ľubovoľnú X).

Tvrdenie teda **neplatí** a vieme ho vyvrátiť konkrétnym kontrapríkladom:

- Zoberme $T = \{(p \land \neg p)\}$ a $X = p$.
- Pre ľubovoľné ohodnotenie v platí $v \not\models T$, teda platia aj implikácie:
  i. ak $v \models T$, tak $v \models \neg X$, ii. ak $v \models T$, tak $v \models X$,
  lebo ich antecedenty sú nepravdivé.
- Ich zovšeobecnením dostávame: i. $T \models \neg X$ a ii. $T \models X$.

su03/3d) Ak $T \not\models X$, tak $T \models \neg X$

Riešenie 2.90 (d)

Zoberme ľubovoľnú teóriu T a formulu X také, že $T \not\models X$.

- Aby tvrdenie platilo, musí $T \models \neg X$, teda
- *každé* ohodnotenie v spĺňajúce T musí spĺňať aj $\neg X$.
- Podľa predpokladu a definície vyplývania *existuje* ohodnotenie v také, že $v \models T$ a $v \not\models X$, teda aj $v \models \neg X$.
- Ale to *nestačí na to*, aby pre *ľubovoľné* ohodnotenie v', ktoré spĺňa T, tiež platilo $v' \not\models X$ a teda aj $v' \models \neg X$.

Tvrdenie teda **neplatí** a vieme ho vyvrátiť konkrétnym kontrapríkladom:

- Zoberme $T = \{p\}$ a $X = q$.
- Pre ohod. $v = \{p \mapsto t, q \mapsto f\}$ máme $v \models T$ a $v \not\models X$, preto $T \not\models X$.
- Pre ohod. $v = \{p \mapsto t, q \mapsto t\}$ máme $v \models T$ a $v \not\models \neg X$, preto $T \not\models \neg X$.
- Teda $T \not\models X$ a $T \not\models \neg X$.

su03/3e) $T \models (X \to Y)$ vtt $T \cup \{X\} \models Y$

Riešenie 2.90 (e, smer $\Rightarrow$)

Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \models (X \to Y)$, teda pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \to Y)$.
Aby (e$\Rightarrow$) platilo, musí $T \cup \{X\} \models Y$, teda
pre každé ohodnotenie v musí platiť, že $(*)$ ak $v \models T \cup \{X\}$, tak $v \models Y$.

Zoberme teda ľubovoľné ohodnotenie v.

- Ak $v \not\models T \cup \{X\}$, vlastnosť $(*)$ platí, lebo jej antecedent je nepravdivý.
- Ak $v \models T \cup \{X\}$, tak $v \models T$ a $T \models X$ a musíme ukázať, že $v \models Y$.
  - Z $v \models T$ a predpokladu, vyplýva, že $v \models (X \to Y)$, teda
  - (a) $v \not\models X$ alebo (b) $v \models Y$ podľa definície spĺňania.
  - Podľa $T \models X$ prípad (a) nenastáva,
  - takže $v \models Y$.

  Vlastnosť $(*)$ teda platí aj v tomto prípade.

Ďalšie možnosti nie sú. Môžeme teda zovšeobecniť, že $T \cup \{X\} \models Y$, č.b.t.d.

su03/3e) $T \models (X \to Y)$ vtt $T \cup \{X\} \models Y$

Riešenie 2.90 (e, smer $\Leftarrow$)

Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \cup \{X\} \models Y$, teda pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \to Y)$.
Aby (e$\Leftarrow$) platilo, musí $T \models (X \to Y)$, teda
pre každé ohodnotenie v musí platiť, že $(*)$ ak $v \models T$, tak $v \models (X \to Y)$.

Zoberme teda ľubovoľné ohodnotenie v.

- Ak $v \not\models T$, vlastnosť $(*)$ platí.
- Ak $v \models T$, musíme ukázať, že $v \models (X \to Y)$.
  - Ak $v \not\models X$, tak $v \models (X \to Y)$, a teda $(*)$ platí.
  - Ak $v \models X$, tak $v \models T \cup \{X\}$, teda podľa predpokladu $v \models Y$. Preto $v \models (X \to Y)$. Vlastnosť $(*)$ teda znova platí.

Ďalšie možnosti nie sú. Môžeme teda zovšeobecniť, že $T \models (X \to Y)$, č.b.t.d.

Problémy v dôkazoch (1)

Používanie pojmov *splnenie* a *vyplývanie*

- ✅ ohodnotenie v spĺňa formulu X
- ✅ formula X je splnená v ohodnotení v
- ✅ $v \models X$
- ⛔ formula X spĺňa ohodnotenie v
- ✅ ohodnotenie v spĺňa teóriu T
- ✅ teória T je splnená v ohodnotení v
- ✅ $v \models T$
- ⛔ teória T spĺňa ohodnotenie v

- ✅ z teórie T vyplýva formula X
- ✅ formula X vyplýva z teórie T
- ✅ formula X je (logickým) dôsledkom teórie T
- ✅ teória T má (logický) dôsledok X
- ✅ $T \models X$
- ⛔ z ohodnotenia v vyplýva…
- ⛔ z formuly X vyplýva teória T

Problémy v dôkazoch (2)

Ignorovanie pojmov a ich definícií

- Niektorí úplne ignorovali, že pojmy vyplývanie a splnenie majú presný dohodnutý význam
- Hovorili o pravdivosti bez ohodnotenia alebo o vyplývaní bez teórie

Definície pojmov a ich negovanie

- Z T vyplýva X ($T \models X$) vtt
  - ✅ pre **všetky** ohodnotenia v, **ak** $v \models T$, **tak** $v \models X$
  - ✅ **každý** model v teórie T spĺňa X
  - ⛔ pre **všetky** ohodnotenia v, $v \models T$ **a** $v \models X$
  - ⛔ **existuje** ohodnotenie v také, že $v \models T$ **a** $v \models X$
  - ⛔ **existuje** ohodnotenie v také, že **ak** $v \models T$, **tak** $v \models X$
- Z T **ne**vyplýva X ($T \not\models X$) vtt
  - ✅ **existuje** ohodnotenie v také, že $v \models T$ a $v \not\models X$
  - ✅ **existuje** model v teórie T, ktorý nespĺňa X
  - ⛔ ...

Problémy v dôkazoch (3)

Skríženie pojmov splnenia a vyplývania

- **Vyplývanie z teórie ($T \models X$) sa správa *inak* ako splnenie formuly ohodnotením ($v \models X$)**
  - $v \models \neg X$ vtt $v \not\models X$
    priamo z definície splnenia formuly ohodnotením
  - $T \models \neg X$ vtt $T \not\models X$
    neplatí ani v jednom smere (videli sme pred chvíľou)
- Symbol $\models$ sa (žiaľ) používa pre oba pojmy

Skoky v uvažovaní veľké a nezdôvodnené

- Ak $T \models (X \rightarrow Y)$, tak $T \not\models X$ alebo $T \models Y$.
- Ak $T \not\models X$ alebo $T \models Y$, tak $T \models (X \rightarrow Y)$.
- Ak $v \not\models T$, tak T je nesplniteľná.

Problémy v dôkazoch (4)

- **Neuvedomenie si toho, čo treba dokázať**
  Rozoberú sa možnosti vyplývajúce z predpokladov,
  ale nezistí sa, či platí požadovaný záver
- **Uvažovanie v kruhu**
  Použitie toho, čo máme dokázať, na zdôvodnenie nejakého kroku
- Snaha uvažovať **naraz o všetkých modeloch/ohodnoteniach**
- 1. Vyslovte jasne, akú vlastnosť majú mať všetky ohodnotenia
  2. **Zoberte jedno ohodnotenie, o ktorom nič nepredpokladáte („ľubovoľné")**
  3. **Overte**, či má za každých okolností požadovanú vlastnosť
  4. **Zovšeobecnite**, že požadovanú vlastnosť majú všetky ohodnotenia
- Snaha uvažovať **súbežne o viacerých možnostiach**
- **Uvažujte prípady postupne a oddelene,**
  vyčerpajte všetky možnosti

Problémy v dôkazoch (5)

Uvažovanie o formulách a teóriách, akoby to boli výrokové premenné

- Ohodnotenie v priraďuje t alebo f iba výrokovej premennej ($v(p) = t$, $v(p) = f$, $\cancel{v(\boldsymbol{X}) = t}$, $\cancel{v(X \land Y) = t}$, $\cancel{v(\boldsymbol{T}) = t}$)
- Formula X je v ohodnotení v splnená ($v \models X$) alebo nesplnená ($v \not\models X$)
- Teória T je v ohodnotení v splnená ($v \models T$) alebo nesplnená ($v \not\models T$)

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.