Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2016/2017

6. prednáška

Úplnosť tabiel, korektné pravidlá
Výroková rezolvencia

3. apríla 2017

Obsah 6. prednášky

3.11 Tablový kalkul

3.11.1
Korektnosť tabiel — opakovanie a dokončenie

Splĺňanie formúl typov α a β

Pozorovanie 3.80 (Stručne vďaka jednotnému zápisu)

Nech v je ľubovoľné ohodnotenie výrokových premenných. Potom v splĺňa α vtt v splĺňa α_1 a v splĺňa α_2.

Pozorovanie 3.82 (Stručne vďaka jednotnému zápisu)

Nech v je ľubovoľné ohodnotenie výrokových premenných. Potom v splĺňa β vtt v splĺňa β_1 alebo v splĺňa 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 $A^+ \in S^+$.

Nič iné nie je tablom pre S^+.

Korektnosť tablového kalkulu

Lema 3.91 (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 $\mathcal{T}$.

Lema 3.92 (K2)

Nech S^+ je množina označených formúl, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie. Ak v spĺňa S^+, tak v spĺňa $\mathcal{T}$.

Veta 3.86 (Korektnosť tablového kalkulu)

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

Korektnosť — dôkaz

Dôkaz vety o korektnosti.

Sporom: Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+. Nech v je ohodnotenie, ktoré spĺňa S^+. Potom podľa lemy K2 v spĺňa tablo $\mathcal{T}$, teda v spĺňa niektorú vetvu π v $\mathcal{T}$. Pretože $\mathcal{T}$ je uzavreté, aj vetva π je uzavretá, teda π obsahuje označené formuly $\mathbf{T}X$ a $\mathbf{F}X$ pre nejakú formulu X. Ale $v \models \mathbf{T}X$ vtt $v \models X$ a $v \models \mathbf{F}X$ vtt $v \not\models X$, čo je spor. $\square$

3.11.2
Tablový dôkaz splniteľnosti

Otvorené tablo a splniteľnosť

Čo ak nevieme nájsť uzavreté tablo pre nejakú množinu ozn. formúl?

Definícia 3.93 (Úplná vetva a úplné tablo)

Nech S^+ je množina označených formúl a $\mathcal{T}$ je tablo pre S^+.
Vetva π v table $\mathcal{T}$ je *úplná* vtt má všetky nasledujúce vlastnosti:

- pre každú ozn. formulu α, ktorá sa vyskytuje na π, sa aj obidve α_1 a α_2 vyskytujú na π,
- pre každú ozn. formulu β, ktorá sa vyskytuje na π, sa aspoň jedna z ozn. formúl β_1 alebo β_2 vyskytuje na π.
- každá $X^+ \in S^+$ sa vyskytuje na π.

Tablo $\mathcal{T}$ je *úplné* vtt každá vetva je buď úplná alebo uzavretá.

Príklad 3.94

Vybudujme úplné tablo pre $\mathbf{F}X$, kde
$X = (((p \lor q) \land (r \lor p)) \to (p \land (q \lor r)))$.

Lema 3.95 (o existencii úplného tabla)

Nech S^+ je konečná množina označených formúl.
Potom existuje úplné tablo pre S^+.

Dôkaz.

Vybudujme tablo $\mathcal{T}_0$ pre S^+ tak, že do koreňa vložíme niektorú formulu z S^+ a opakovaním operácie Ax postupne doplníme ostatné.
Potom tablo postupne rozširujeme tak, že vyberieme ľubovoľný list y tabla $\mathcal{T}_i$, ktorého vetva π_y je otvorená a nie je úplná. Potom nastane aspoň jedna z možností:

- Na π_y sa nachádza nejaká formula α, ale nenachádza sa niektorá z formúl α_1 a α_2.
- Na π_y sa nachádza nejaká formula β, ale nenachádza sa ani jedna z formúl β_1 a β_2.

Ak platí prvá alebo obe možnosti, aplikujeme operáciu A. Ak platí druhá možnosť, aplikujeme operáciu B. Získame tablo $\mathcal{T}_{i+1}$, s ktorým proces opakujeme. Tento proces po konečnom počte krokov (prečo?) vytvorí nejaké tablo $\mathcal{T}_n$, v ktorom už neexistuje vetva, ktorá by bola otvorená a nebola úplná. Teda každá vetva v $\mathcal{T}_n$ je buď uzavretá alebo úplná, čiže $\mathcal{T}_n$ je úplné. $\square$

3.11.3
Hintikkova lema

Nadol nasýtené množiny a Hintikkova lemma

Definícia 3.96

Množina označených formúl S^+ sa nazýva *nadol nasýtená* vtt platí:

(H$_0$) v S^+ sa nevyskytujú naraz $\mathbf{T}p$ a $\mathbf{F}p$ pre žiadnu výrokovú premennú p;

(H$_1$) ak $\alpha \in S^+$, tak $\alpha_1 \in S^+$ a $\alpha_2 \in S^+$;

(H$_2$) ak $\beta \in S^+$, tak $\beta_1 \in S^+$ alebo $\beta_2 \in S^+$.

Pozorovanie 3.97

Nech π je úplná otvorená vetva nejakého tabla $\mathcal{T}$.
Potom množina všetkých formúl na π je nadol nasýtená.

Lema 3.98 (Hintikkova)

Každá nadol nasýtená množina S^+ je splniteľná.

Dôkaz Hintikkovej lemy.

Chceme vytvoriť ohodnotenie v, ktoré splní všetky formuly z S^+.
Definujme v pre každú výrokovú premennú p takto:

- ak $\mathbf{T}p \in S^+$: $v(p) = t$,
- ak $\mathbf{F}p \in S^+$: $v(p) = f$,
- ak ani $\mathbf{T}p$ ani $\mathbf{F}p$ nie sú v S^+, tak $v(p) = t$.

v je korektne definované vďaka H_0.
Indukciou na stupeň formuly dokážeme, že v spĺňa všetky formuly z S^+:

- v očividne spĺňa všetky označené výrokové premenné z S^+.
- $X^+ \in S^+$ je buď α alebo β:
  - Ak X^+ je α, potom obidve α_1, $\alpha_2 \in S^+$ (H_1), sú nižšieho stupňa X^+, a teda podľa indukčného predpokladu sú splnené pri v, preto v spĺňa aj α (podľa pozorovania 3.80).
  - Ak X^+ je β, potom aspoň jedna z β_1, β_2 je v S^+ (H_2). Nech je to ktorákoľvek, je nižšieho stupňa ako X^+, teda podľa IP ju v spĺňa, a preto v spĺňa β (podľa pozorovania 3.82). $\square$

3.11.4
Úplnosť

Úplnosť

Úplnosť kalkulu neformálne znamená, že je dostatočne silný, aby sa v ňom dali dokázať všetky dôsledky teórií.

Veta 3.99 (o úplnosti)

Nech S^+ je konečná nesplniteľná množina označených formúl. Potom existuje uzavreté tablo pre S^+.

Dôsledok 3.100

Nech S je konečná teória a X je formula. Ak $S \models X$, tak $S \vdash X$.

Dôsledok 3.101

Nech X je formula. Ak $\models X$, tak $\vdash X$.

Úplnosť platí aj pre nekonečné množiny, ale dôkaz je ťažší.

Úplnosť — dôkaz

Dôkaz vety o úplnosti.

Zoberme ľubovoľnú konečnú nesplniteľnú množinu označených formúl S^+.
Podľa lemy o existencii úplného tabla vieme pre S^+ nájsť úplné tablo $\mathcal{T}$, teda také, že každá vetva je buď uzavretá alebo úplná.
Ak by niektorá vetva bola otvorená, potom musí byť úplná, a teda nadol uzavretá. Podľa Hintikkovej lemy by bola splniteľná. Pretože obsahuje všetky formuly z S^+, bola by aj S^+splniteľná, čo je spor s nesplniteľnosťou S^+.
Preto musia byť všetky vetvy tabla $\mathcal{T}$ uzavreté. □

3.11.5 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 (Ax), α, β, pretože stačia na vybudovanie úplného tabla.

Nové pravidlo

Čo sa stane, ak pridáme nové pravidlo, napr.

$$\frac{\mathbf{T}(A \lor B) \quad \mathbf{F}A}{\mathbf{T}B} \quad (\lor_1) \quad ?$$

Upravíme definíciu priameho rozšírenia:

Úprava definície 3.83

(...) 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: ...

⋮

$\lor_1$: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(A \lor B)$ a $\mathbf{F}A$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}B$.

Nové pravidlo vs. korektnosť a úplnosť

- Pravidlo $(\vee_1)$ je *korektné*:
  Nech v je ľubovoľné ohodnotenie. Ak v spĺňa $\mathbf{T}(A \vee B)$ a $\mathbf{F}A$, tak v spĺňa $\mathbf{T}B$.
  Keďže v spĺňa $\mathbf{T}(A \vee B)$, v spĺňa A alebo v spĺňa B.
  Pretože ale v spĺňa $\mathbf{F}A$, nespĺňa A. Takže v musí spĺňať B.
- Preto stále dokážeme lemu K1 (3.91):

  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 3.102 (Tablové pravidlo a jeho korektnosť)

Tablové pravidlo je množina dvojíc zapisovaných:

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \mid \ldots \mid C_k^+} \quad (R)$$

tvorených n-ticou (označených) formúl, ktoré nazývame *premisy*, a k-ticou (označených) formúl, ktoré nazývame *závery*, pričom $n \geq 0$ a $k > 0$.

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

Nové pravidlá vo všeobecnosti

Úprava definície 3.83

(...)

- ...
- 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 na vetve π_y nachádzajú *všetky* premisy $P_1^+, \ldots, P_n^+$, tak k uzlu y pripojíme k nových vrcholov obsahujúcich postupne závery $C_1^+, \ldots, C_k^+$.

3.12
Rezolvencia vo výrokovej logike

Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.
Je nasledujúce pravidlo korektné?

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

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 3.103

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

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

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

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

Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

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

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

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

Rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.

Pozorovania o rezolvencii

- Rezolvencia s jednotkovou klauzulou skráti druhú klauzulu:

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

- Ak rezolvencia odvodí **prázdnu klauzulu**

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

  premisy **nie sú súčasne splniteľné**
- Nie každý logický dôsledok sa dá odvodiť rezolvenciou: $\{p, q\} \models (p \lor q)$
- Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch, ale je **nekorektné urobiť to naraz**:

$$\frac{(\neg p \lor q) \; (p \lor \neg q)}{(q \lor \neg q)} \quad \frac{(\neg p \lor q) \; (p \lor \neg q)}{(\neg p \lor p)} \quad \cancel{\frac{(\neg p \lor q) \; (p \lor \neg q)}{\Box}}$$

Problematické prípady

- Opakovaným aplikovaním rezolvencie môžeme odvodzovať ďalšie dôsledky

Príklad 3.104

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 (2)
(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 3.105

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

- prvkom S,
- rezolventou dvoch predchádzajúcich klauzúl C_j a C_k, t.j., $j < i$ a $k < i$,
- 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 $\square$.

Korektnosť a úplnosť rezolvencie

Veta 3.106 (Korektnosť rezolvencie)

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

Veta 3.107 (Úplnosť rezolvencie)

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

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.