# Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2018/2019

# 7. prednáška

## Úplnosť tabiel
## Korektné pravidlá
## Výroková rezolvencia

1. apríla 2019

# Obsah 7. prednášky

2 Výroková logika
- Tablový kalkul
  - Tablový dôkaz splniteľnosti
  - Hintikkova lema
  - Úplnosť
  - Nové korektné pravidlá
- Rezolvencia vo výrokovej logike

2.9

# Tablový kalkul

2.9.2

# Tablový dôkaz splniteľnosti

# Úplná vetva a tablo

## Definícia 2.93 (Úplná vetva a úplné tablo)

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

- pre každú označenú formulu $\alpha$, ktorá sa vyskytuje na $\pi$, sa *obidve* označené formuly $\alpha_1$ a $\alpha_2$ vyskytujú na $\pi$;
- pre každú označenú formulu $\beta$, ktorá sa vyskytuje na $\pi$, sa *aspoň jedna* z označených formúl $\beta_1, \beta_2$ vyskytuje na $\pi$;
- *každá* $X^+ \in S^+$ sa vyskytuje na $\pi$.

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

## Lema 2.95 (o existencii úplného tabla)

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

## 2.9.3

# Hintikkova lema

# Nadol nasýtené množiny a Hintikkova lemma

## Definícia 2.96

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

- **H₀** v $S^+$ sa nevyskytujú naraz $\mathbf{T}\,p$ a $\mathbf{F}\,p$ pre žiadnu výrokovú premennú $p$;
- **H₁** ak $\alpha \in S^+$, tak $\alpha_1 \in S^+$ a $\alpha_2 \in S^+$;
- **H₂** ak $\beta \in S^+$, tak $\beta_1 \in S^+$ alebo $\beta_2 \in S^+$.

## Pozorovanie 2.97

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

## Lema 2.98 (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 $\mathrm{H}_0$.
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 $\alpha$ alebo $\beta$:
  - Ak $X^+$ je $\alpha$, potom obidve $\alpha_1, \alpha_2 \in S^+$ ($\mathrm{H}_1$), sú nižšieho stupňa $X^+$, a teda podľa indukčného predpokladu sú splnené pri $v$, preto $v$ spĺňa aj $\alpha$ (podľa pozorovania 2.81).
  - Ak $X^+$ je $\beta$, potom aspoň jedna z $\beta_1, \beta_2$ je v $S^+$ ($\mathrm{H}_2$). Nech je to ktorákoľvek, je nižšieho stupňa ako $X^+$, teda podľa IP ju $v$ spĺňa, a preto $v$ spĺňa $\beta$ (podľa pozorovania 2.83). □

# 2.9.4
# Úplnosť

# Úplnosť

*Úplnosť* kalkulu neformálne:
Ak je nejaké tvrdenie pravdivé, tak existuje jeho dôkaz v kalkule.

## Veta 2.99 (o úplnosti)

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

## Dôsledok 2.100

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

## Dôsledok 2.101

*Nech $X$ je formula. Ak $\vDash X$, 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. □

2.9.5

# 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 ($\alpha$) závery/aspoň jeden ($\beta$) 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 ($S^+$), $\alpha$, $\beta$, pretože stačia na vybudovanie úplného tabla.

# Nové pravidlo

Čo sa stane, ak pridáme nové pravidlo, napríklad modus ponens:

$$\frac{\mathbf{T}(A \to B) \quad \mathbf{T}\,A}{\mathbf{T}\,B} \quad ? \tag{MP}$$

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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:

- $\alpha$ ...

⋮

- MP Ak sa na vetve $\pi_y$ nachádzajú *obe* formuly $\mathbf{T}(A \to B)$ a $\mathbf{T}\,A$, tak ako jediné dieťa $y$ pripojíme nový vrchol obsahujúci $\mathbf{T}\,B$.

# Nové pravidlo vs. korektnosť a úplnosť

**Korektnosť** tabiel s (MP)

- Pri dôkaze lemy 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 $\mathcal{T}$.*

  využijeme

## Tvrdenie 2.102 (Korektnosť pravidla (MP))

*Nech $v$ je ľubovoľné ohodnotenie. Ak $v$ spĺňa $\mathbf{T}(A \to B)$ a $\mathbf{T}\,A$, tak $v$ spĺňa $\mathbf{T}\,B$.*

## Dôkaz.

Keďže $v \models \mathbf{T}(A \to B)$, tak $v \models (A \to B)$, teda $v \not\models A$ alebo $v \models B$.
Pretože ale $v \models \mathbf{T}\,A$, tak $v \models A$. Takže $v \models B$. $\square$

- Dôkaz lemy K2 a samotnej vety o korektnosti — bez zmeny

**Úplnosť** — bez zmeny, úplné tablo vybudujú základné pravidlá

# Nové pravidlá vo všeobecnosti

## Definícia 2.103 (Tablové pravidlo a jeho korektnosť)

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

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

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

ktoré vzniknú súčasnou substitúciou formúl $X_1, \ldots, X_m$ za premenné $q_1, \ldots, q_m$ v označených formulách $P_1^+, \ldots, P_n^+, C_1^+, \ldots, C_k^+$.
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 $P_1^+, \ldots, P_n^+$, tak $v$ spĺňa *niektorý* záver $C_1^+, \ldots, C_k^+$.

# 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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:

  ⋮

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

2.10

# 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 2.104

***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 2.105

*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:

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

- 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**:

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

  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 2.106

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

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

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

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

# Rezolvenčné odvodenie a zamietnutie

## Definícia 2.107

***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 $S$ 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 2.108

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

# Korektnosť a úplnosť rezolvencie

**Veta 2.109 (Korektnosť rezolvencie)**

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

**Veta 2.110 (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.