Korektnosť a úplnosť výrokovologických tabiel

5. prednáška

Logika pre informatikov a Úvod do matematickej logiky

Ján Kľuka, Ján Mazák, Jozef Šiška

Letný semester 2024/2025

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Obsah 5. prednášky

Rekapitulácia a plán

Minulý týždeň:

- Sformalizovali sme dôkazy sporom pomocou tabiel.
- Vyslovili, ale nedokázali tvrdenie o korektnosti tabiel:
  uzavreté tablo dokazuje výrokovologickú nesplniteľnosť
- a dôsledky pre dokazovanie vyplývania a tautológií.

Dnes:

- Dokážeme korektnosť tabiel.
- Preskúmame, čo vedia tablá povedať o splniteľnosti.
- Dokážeme úplnosť tabiel.

Dôkazy a výrokovologické tablá

Dôkazy a výrokovologické tablá

Výrokovologické tablá – opakovanie

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

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 induktívnych pravidiel:

- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+.

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

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

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

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 induktívnych 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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:
  - **α**: 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.

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

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 induktívnych 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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:
  - **α**: 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.
  - **β**: Ak sa na vetve π_y (ceste z koreňa do 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.

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

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 induktívnych 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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:
  - $\boldsymbol{\alpha}$: 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.
  - $\boldsymbol{\beta}$: Ak sa na vetve π_y (ceste z koreňa do 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.
  - $\boldsymbol{S^+}$: Ako jediné dieťa y pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Definícia 5.13 (Tablo pre množinu označených formúl [Smullyan, 1979])

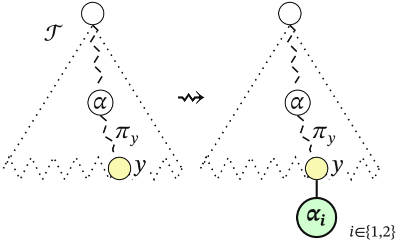
Analytické tablo pre množinu označených formúl S^+ (skrátene ***tablo pre S^+***) je binárny strom, ktorého vrcholy obsahujú označené formuly a ktorý je skonštruovaný podľa nasledovných induktívnych pravidiel:

- 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*** $\mathcal{T}$ ktorýmkoľvek z pravidiel:
  - $\boldsymbol{\alpha}$: 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.
  - $\boldsymbol{\beta}$: Ak sa na vetve π_y (ceste z koreňa do 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.
  - $\boldsymbol{S^+}$: Ako jediné dieťa y pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Nič iné nie je tablom pre S^+.

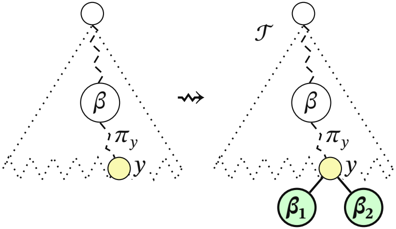
Tablá a tablové pravidlá

Pôvodné tablo **Možné priame rozšírenie** **Pravidlá a označené formuly v nich**



$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2}$$

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

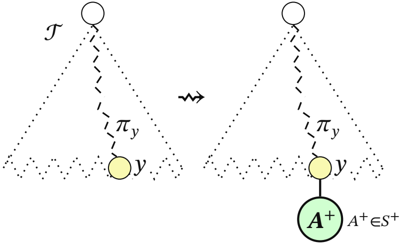


$$\frac{\beta}{\beta_1 \mid \beta_2}$$

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

Legenda: y je list v table $\mathcal{T}$, π_y je cesta od koreňa k y

Tablá a tablové pravidlá (pokračovanie)

Pôvodné tablo	Možné priame rozšírenie	Pravidlá a označené formuly v nich	
		$\dfrac{}{A^+}$	$A^+ \in S^+$

Legenda: y je list v table $\mathcal{T}$, π_y je cesta od koreňa k y

Uzavretosť a otvorenosť vetvy a tabla

Definícia 5.14

Vetvou tabla $\mathcal{T}$ je každá cesta od koreňa $\mathcal{T}$ k niektorému listu $\mathcal{T}$.

Označená formula X^+ sa *vyskytuje na vetve* π v $\mathcal{T}$
vtt X^+ sa nachádza v niektorom vrchole na π.
Skrátene to budeme zapisovať $X^+ \in \mathrm{formulas}(\pi)$.

Tablo $\sim$ dôkaz sporom. Vetvenie $\sim$ rozbor možných prípadov.

$\Longrightarrow$ Spor musí nastať vo všetkých vetvách.

Definícia 5.15

Vetva π tabla $\mathcal{T}$ je *uzavretá* vtt na π sa súčasne vyskytujú 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.

Príklad — vetvy a uzavretosť

Príklad 5.16 (Vetvy a uzavretosť)

Určme vetvy v table a zistime, či sú uzavreté a či je uzavreté tablo:

1. $\mathbf{T}(\mathrm{p}(A) \to (\mathrm{p}(B) \land \mathrm{p}(C)))$ $\quad S^+$
2. $\mathbf{T}((\mathrm{p}(B) \lor \mathrm{p}(D)) \to \mathrm{p}(E))$ $\quad S^+$
3. $\mathbf{T}(\mathrm{p}(F) \to \neg\mathrm{p}(E))$ $\quad S^+$
4. $\mathbf{F}(\mathrm{p}(A) \to \neg\mathrm{p}(F))$ $\quad S^+$
5. $\mathbf{T}\,\mathrm{p}(A)$ $\quad \alpha 4$
6. $\mathbf{F}\,\neg\mathrm{p}(F)$ $\quad \alpha 4$
7. $\mathbf{T}\,\mathrm{p}(F)$ $\quad \alpha 6$
8. $\mathbf{F}\,\mathrm{p}(F)$ $\quad \beta 3$
   $*7, 8$
9. $\mathbf{T}\,\neg\mathrm{p}(E)$ $\quad \beta 3$
10. $\mathbf{F}\,\mathrm{p}(E)$ $\quad \alpha 9$
11. $\mathbf{F}\,\mathrm{p}(A)$ $\quad \beta 1$
    $*5, 11$
12. $\mathbf{T}(\mathrm{p}(B) \land \mathrm{p}(C))$ $\quad \beta 1$
13. $\mathbf{T}\,\mathrm{p}(B)$ $\quad \alpha 12$
14. $\mathbf{F}(\mathrm{p}(B) \lor \mathrm{p}(D))$ $\quad \beta 2$
15. $\mathbf{T}\,\mathrm{p}(E)$ $\quad \beta 2$
    $*10{,}15$

Dôkazy a výrokovologické tablá

Korektnosť tabiel

Korektnosť tablového kalkulu

Veta 5.17 (Korektnosť tablového kalkulu [Smullyan, 1979])

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

Dôsledok 5.18

*Nech S je výrokovologická teória, X je výrokovologická formula a nech **X je výrokovologicky dokázateľná z S** (skrát. $S \vdash_{\mathrm{p}} X$), t.j., nech existuje uzavreté tablo pre množinu označených formúl $\{\mathbf{T}\,A \mid A \in S\} \cup \{\mathbf{F}\,X\}$. Potom z S výrokovologicky vyplýva X ($S \vDash_{\mathrm{p}} X$).*

Dôsledok 5.19

*Nech X je výrokovologická formula a nech **X je výrokovologicky dokázateľná** (skrát. $\vdash_{\mathrm{p}} X$), t.j., nech existuje uzavreté tablo pre množinu označených formúl $\{\mathbf{F}\,X\}$. Potom X je tautológia ($\vDash_{\mathrm{p}} X$).*

Korektnosť — idea dôkazu

Aby sme dokázali korektnosť tabiel, dokážeme postupne dve lemy:

K1: Ak máme tablo pre splniteľnú množinu S^+
s aspoň jednou splniteľnou vetvou,
tak každé jeho **priame rozšírenie** má tiež splniteľnú vetvu.

K2: Každé tablo pre splniteľnú množinu S^+
má aspoň jednu splniteľnú vetvu.

Z toho ľahko sporom dokážeme, že množina, pre ktorú sme našli uzavreté tablo je nesplniteľná.

Korektnosť — pravdivosť priameho rozšírenia tabla

Všimnime si:

Vetva sa správa ako konjunkcia svojich označených formúl — všetky musia byť naraz pravdivé.

Tablo sa správa ako disjunkcia vetiev — niektorá musí byť pravdivá.

Definícia 5.20

Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+, nech π je vetva tabla $\mathcal{T}$ a nech v je výrokovologické ohodnotenie pre $\mathcal{L}$. Potom:

- ***vetva π je pravdivá vo v*** ($v \models_p \pi$) vtt vo v sú pravdivé **všetky** označené formuly vyskytujúce sa na vetve π.
- ***tablo $\mathcal{T}$ je pravdivé vo v*** ($v \models_p \mathcal{T}$) vtt **niektorá** vetva v table $\mathcal{T}$ je pravdivá.

Korektnosť — pravdivosť priameho rozšírenia tabla

Pomocou predchádzajúcej definície sformulujeme lemu K1 takto:

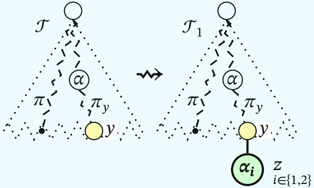
Lema 5.21 (K1)

Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a nech v je výrokovologické ohodnotenie pre $\mathcal{L}$.
Ak S^+ a $\mathcal{T}$ sú pravdivé vo v,
tak aj každé priame rozšírenie $\mathcal{T}$ je pravdivé vo v.

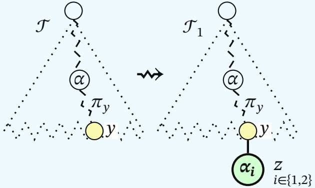
Dôkaz lemy K1.

Nech $v \models_p S^+$ a nech $\mathcal{T}$ je pravdivé vo v. Potom je pravdivá niektorá vetva v $\mathcal{T}$. Zoberme jednu takú vetvu a označme ju π. Nech $\mathcal{T}_1$ je priame rozšírenie $\mathcal{T}$. Nastáva jeden z prípadov:

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom α, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom z obsahuje α_1 alebo α_2 pre nejakú formulu α na vetve π_y.



Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.



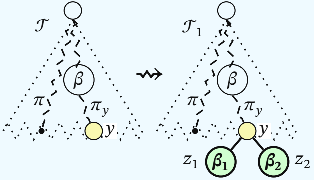
Ak $\pi = \pi_y$, tak α je pravdivá vo v, pretože α je na π. Potom aj α_1 a α_2 sú pravdivé vo v (pozorovanie 5.8). Vetva π_z v table $\mathcal{T}_1$ rozširuje vetvu π pravdivú vo v o vrchol z obsahujúci ozn. formulu α_1 alebo α_2 pravdivú vo v. Preto π_z je pravdivá vo v, a teda aj tablo $\mathcal{T}_1$ je pravdivé vo v.

Pozorovanie 5.8:
$v \models_p \alpha$ vtt
$v \models_p \alpha_1$ a $v \models_p \alpha_2$.

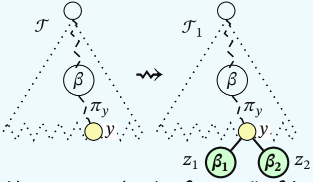
Dôkaz lemy K1.

Nech $v \models_p S^+$ a nech $\mathcal{T}$ je pravdivé vo v. Potom je pravdivá niektorá vetva v $\mathcal{T}$. Zoberme jednu takú vetvu a označme ju π. Nech $\mathcal{T}_1$ je priame rozšírenie $\mathcal{T}$. Nastáva jeden z prípadov:

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom β, pridaním detí z_1 a z_2 nejakému listu y v $\mathcal{T}$, pričom z_1 obsahuje β_1 a z_2 obsahuje β_2 pre nejakú formulu β na vetve π_y.



Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.



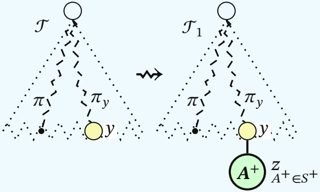
Ak $\pi = \pi_y$, tak $v \models_p \beta$, pretože β je na π. Potom $v \models_p \beta_1$ alebo $v \models_p \beta_2$ (poz. 5.11).
Ak $v \models_p \beta_1$,
tak $v \models_p \pi_{z_1}$, a teda $v \models_p \mathcal{T}_1$.
Ak $v \models_p \beta_2$,
tak $v \models_p \pi_{z_2}$, a teda $v \models_p \mathcal{T}_1$.

Pozorovanie 5.11:
$v \models_p \beta$ vtt
$v \models_p \beta_1$ alebo $v \models_p \beta_2$.

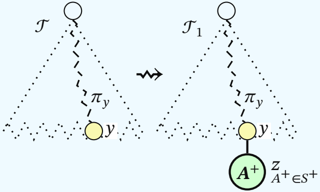
Dôkaz lemy K1.

Nech $v \models_p S^+$ a nech $\mathcal{T}$ je pravdivé vo v. Potom je pravdivá niektorá vetva v $\mathcal{T}$. Zoberme jednu takú vetvu a označme ju π. Nech $\mathcal{T}_1$ je priame rozšírenie $\mathcal{T}$. Nastáva jeden z prípadov:

- $\mathcal{T}_1$ vzniklo z $\mathcal{T}$ pravidlom S^+, pridaním nového dieťaťa z nejakému listu y v $\mathcal{T}$, pričom z obsahuje formulu $A^+ \in S^+$.



Ak $\pi \neq \pi_y$, tak $\mathcal{T}_1$ obsahuje π, a teda aj $\mathcal{T}_1$ je pravdivé vo v.



Ak $\pi = \pi_y$, tak π_z v table $\mathcal{T}_1$ je pravdivá vo v, pretože je rozšírením vetvy π pravdivej vo v o vrchol z obsahujúci formulu A^+ pravdivú vo v (pretože $v \models_p S^+$ a $A^+ \in S^+$). Preto tablo $\mathcal{T}_1$ je pravdivé vo v. $\square$

Korektnosť — pravdivosť množiny a tabla pre ňu

Lema 5.22 (K2)

Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a nech v je ohodnotenie pre $\mathcal{L}$.
Ak S^+ je pravdivá vo v, tak aj $\mathcal{T}$ je pravdivé vo v.

Dôkaz lemy K2.

Nech S^+ je množina označených formúl, nech v je ohodnotenie a nech $v \models_p S^+$. Úplnou indukciou na počet vrcholov tabla $\mathcal{T}$ dokážeme, že vo v je pravdivé každé tablo $\mathcal{T}$ pre S^+.

Ak má $\mathcal{T}$ jediný vrchol, tento vrchol obsahuje formulu $A^+ \in S^+$, ktorá je pravdivá vo v. Preto je pravdivá jediná vetva v $\mathcal{T}$, teda aj $\mathcal{T}$.

Ak $\mathcal{T}$ má viac ako jeden vrchol, je priamym rozšírením nejakého tabla $\mathcal{T}_0$, ktoré má o 1 alebo o 2 vrcholy menej ako $\mathcal{T}$.
Podľa indukčného predpokladu je $\mathcal{T}_0$ pravdivé vo v.
Podľa lemy K1 je potom vo v pravdivé aj $\mathcal{T}$. $\square$

Dôkaz vety o korektnosti 5.17.

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

Sporom: Predpokladajme, že existuje ohodnotenie, v ktorom je S^+ pravdivá. Označme ho v.

Potom podľa lemy K2 je vo v pravdivé tablo $\mathcal{T}$, teda vo v je pravdivá niektorá vetva π v $\mathcal{T}$.

Pretože $\mathcal{T}$ je uzavreté, aj vetva π je uzavretá. Na π sa teda nachádzajú označené formuly $\mathbf{T}\,X$ a $\mathbf{F}\,X$ pre nejakú formulu X.

Pretože π je pravdivá vo v, musia byť vo v pravdivé všetky formuly na nej. Ale $v \models_{\mathrm{p}} \mathbf{T}\,X$ vtt $v \models_{\mathrm{p}} X$ a $v \models_{\mathrm{p}} \mathbf{F}\,X$ vtt $v \not\models_{\mathrm{p}} X$.

Teda $\mathbf{T}\,X$ a $\mathbf{F}\,X$ nemôžu byť obe pravdivé, čo je spor. $\square$

Dôkazy a výrokovologické tablá

Testovanie nesplniteľnosti, splniteľnosti a falzifikovateľnosti

Úplná vetva a tablo

Príklad 5.23

Zistime tablom, či

$$\{((\mathtt{rychly}(\mathtt{p}) \lor \mathtt{spravny}(\mathtt{p})) \land (\mathtt{citatelny}(\mathtt{p}) \lor \mathtt{rychly}(\mathtt{p})))\}$$
$$\vDash_{\mathrm{p}} (\mathtt{rychly}(\mathtt{p}) \land (\mathtt{spravny}(\mathtt{p}) \lor \mathtt{citatelny}(\mathtt{p}))).$$

Vybudujeme tablo pre množinu označených formúl:

$$S^+ = \{\mathbf{T}((\mathtt{rychly}(\mathtt{p}) \lor \mathtt{spravny}(\mathtt{p})) \land (\mathtt{citatelny}(\mathtt{p}) \lor \mathtt{rychly}(\mathtt{p}))),$$
$$\mathbf{F}(\mathtt{rychly}(\mathtt{p}) \land (\mathtt{spravny}(\mathtt{p}) \lor \mathtt{citatelny}(\mathtt{p})))\}$$

Podarí sa nám ho uzavrieť?

Úplná vetva a tablo

Nech v príklade tablové pravidlá používame akokoľvek,

- **nenájdeme uzavreté** tablo, ale
- ak pravidlá nepoužívame opakovane na rovnakú formulu v rovnakej vetve, po čase **vybudujeme úplné** a **otvorené** tablo.

Definícia 5.24 (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 označenú formulu α, ktorá sa vyskytuje na π, sa **obidve** označené formuly α_1 a α_2 vyskytujú na π;
- pre každú označenú formulu β, ktorá sa vyskytuje na π, sa **aspoň jedna** z označených formúl β_1, β_2 vyskytuje na π;
- **každá** $X^+ \in S^+$ sa vyskytuje na π.

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

Otvorené tablo a splniteľnosť

Z otvoreného a úplného tabla pre S^+ môžeme vytvoriť ohodnotenie v:

1. nájdeme otvorenú vetvu π,
2. pre každý atóm A
   - ak sa na π nachádza $\mathbf{T}\,A$, definujeme $v(A) = t$;
   - ak sa na π nachádza $\mathbf{F}\,A$, definujeme $v(A) = f$;
   - inak definujeme $v(A)$ ľubovoľne.

V tomto v je pravdivá π, a preto je v ňom pravdivá aj S^+ (všetky formuly z S^+ sa vyskytujú na π, lebo π je úplná).

Otázka

- Dá sa vždy nájsť úplné tablo pre S^+?
- Naozaj sa z úplného otvoreného tabla dá vytvoriť model S^+?

Existencia úplného tabla

Lema 5.25 (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 spravidla S^+ 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 pravidlo α.
Ak platí iba druhá možnosť, aplikujeme pravidlo β.
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. $\square$

Dôkazy a výrokovologické tablá

Úplnosť

Nadol nasýtené množiny a Hintikkova lemma

Definícia 5.26

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

H$_0$: v S^+ sa nevyskytujú naraz $\mathbf{T}\,A$ a $\mathbf{F}\,A$
pre žiaden predikátový atóm A;

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 5.27

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

Lema 5.28 (Hintikkova)

Každá nadol nasýtená množina S^+ je splniteľná.

Dôkaz Hintikkovej lemy.

Chceme dokázať, že existuje ohodnotenie v, v ktorom sú pravdivé všetky označené formuly z S^+. Definujme v pre každý predikátový atóm A takto:

$$v(A) = \begin{cases} t, & \text{ak } \mathbf{T}\, A \in S^+; \\ f, & \text{ak } \mathbf{F}\, A \in S^+; \\ t, & \text{ak ani } \mathbf{T}\, A \text{ ani } \mathbf{F}\, A \text{ nie sú v } S^+. \end{cases}$$

v je korektne definované vďaka H_0 (každému atómu priradí t alebo f, žiadnemu nepriradí obe).

Indukciou na stupeň formuly dokážeme, že vo v sú pravdivé všetky formuly z S^+:

1° Všetky označené predikátové atómy (formuly stupňa 0) z S^+ sú pravdivé vo v.

2° Nech $X^+ \in S^+$ a nech platí IP: Vo v sú pravdivé všetky formuly z S^+ nižšieho stupňa ako X^+. X^+ je buď α alebo β:

Ak X^+ je α, potom obidve $\alpha_1, \alpha_2 \in S^+$ (H_1), sú nižšieho stupňa ako X^+,
a teda podľa indukčného predpokladu sú pravdivé vo v,
preto (podľa poz. 5.8) je v ňom pravdivá aj α.

Ak X^+ je β, potom aspoň jedna z β_1, β_2 je v S^+ (H_2). Nech je to ktorákoľvek,
má nižší stupeň ako X^+, teda podľa IP je pravdivá vo v,
a preto (podľa poz. 5.11) je vo v pravdivá aj β. □

Úplnosť

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

Veta 5.29 (o úplnosti tablového kalkulu [Smullyan, 1979])

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

Dôsledok 5.30

Nech S je konečná teória a X je formula.
Ak $S \models_{\mathrm{p}} X$, tak $S \vdash_{\mathrm{p}} X$.

Dôsledok 5.31

Nech X je formula. Ak $\models_{\mathrm{p}} X$, tak $\vdash_{\mathrm{p}} X$.

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 nasýtená. 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. $\square$

Dôkazy a výrokovologické tablá

Nové korektné pravidlá

Problémy so základnými pravidlami

Základné tablové pravidlá sú jednoduché, ľahko overiteľné a analytické — z (ne)pravdivosti zloženej formuly odvodzujú (ne)pravdivosť jej priamych podformúl.

Nie sú ale úplne pohodlné ani prirodzené, hlavne β.

Príklad 5.32

Dokážme, že pre všetky formuly A, B, C, X, Y, Z:

$$\{(A \to C), (B \to C), (C \to X), (C \to Y), ((X \land Y) \to Z)\} \vdash_{\mathrm{p}} ((A \lor B) \to Z)$$

Všimnime si:

- časté použitia pravidla β na implikáciu, kde sa jedna vetva ihneď uzavrie;
- opakovanie jedného podstromu dôkazu.

Riešenie príkladu 5.32

Tablo pre

$$S^+ = \{\, \mathbf{T}(A \to C), \mathbf{T}(B \to C), \mathbf{T}(C \to X), \mathbf{T}(C \to Y), \mathbf{T}((X \land Y) \to Z),$$
$$\mathbf{F}((A \lor B) \to Z)\}$$

1. $\mathbf{T}\,(A \to C)$	S^+
2. $\mathbf{T}\,(B \to C)$	S^+
3. $\mathbf{T}\,(C \to X)$	S^+
4. $\mathbf{T}\,(C \to Y)$	S^+
5. $\mathbf{T}\,((X \land Y) \to Z)$	S^+
6. $\mathbf{F}\,((A \lor B) \to Z)$	S^+
7. $\mathbf{T}\,(A \lor B)$	$\alpha 6$
8. $\mathbf{F}\,Z$	$\alpha 6$

- 9. $\mathbf{F}\,(X \land Y)\ \beta 5$
  - 10. $\mathbf{T}\,A\ \beta 7$
    - 11. $\mathbf{F}\,A\ \beta 1$ — $*\ 10, 11$
    - 12. $\mathbf{T}\,C\ \beta 1$
      - 13. $\mathbf{F}\,C\ \beta 3$ — $*\ 12, 13$
      - 14. $\mathbf{T}\,X\ \beta 3$
        - 15. $\mathbf{F}\,C\ \beta 4$ — $*\ 12, 15$
        - 16. $\mathbf{T}\,Y\ \beta 4$
          - 17. $\mathbf{F}\,X\ \beta 9$ — $*\ 14, 17$
          - 18. $\mathbf{F}\,Y\ \beta 9$ — $*\ 16, 18$
  - 19. $\mathbf{T}\,B\ \beta 7$
    - 20. $\mathbf{F}\,B\ \beta 2$ — $*\ 19, 20$
    - 21. $\mathbf{T}\,C\ \beta 2$
      - 22. $\mathbf{F}\,C\ \beta 3$ — $*\ 21, 22$
      - 23. $\mathbf{T}\,X\ \beta 3$
        - 24. $\mathbf{F}\,C\ \beta 4$ — $*\ 21, 24$
        - 25. $\mathbf{T}\,Y\ \beta 4$
          - 26. $\mathbf{F}\,X\ \beta 9$ — $*\ 23, 26$
          - 27. $\mathbf{F}\,Y\ \beta 9$ — $*\ 25, 27$
- 28. $\mathbf{T}\,Z\ \beta 5$ — $*\ 8, 28$

Odstránenie problémov — nové pravidlá

Keby tablový kalkul obsahoval napríklad veľmi prirodzené pravidlá *modus ponens*, *modus tolens* a *rez*:

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{T}\,X}{\mathbf{T}\,Y} \qquad \text{(MP)}$$

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{F}\,Y}{\mathbf{F}\,X} \qquad \text{(MT)}$$

$$\frac{}{\mathbf{T}\,X \mid \mathbf{F}\,X} \qquad \text{(cut)}$$

dôkaz v príklade by sa dal sprehľadniť a odstránila by sa duplicita.

Riešenie príkladu 5.32 s modus ponens a modus tolens

1.	$\mathbf{T}(A \to C)$	S^+
2.	$\mathbf{T}(B \to C)$	S^+
3.	$\mathbf{T}(C \to X)$	S^+
4.	$\mathbf{T}(C \to Y)$	S^+
5.	$\mathbf{T}((X \land Y) \to Z)$	S^+
6.	$\mathbf{F}((A \lor B) \to Z)$	S^+
7.	$\mathbf{T}(A \lor B)$	$\alpha 6$
8.	$\mathbf{F}Z$	$\alpha 6$
9.	$\mathbf{F}(X \land Y)$	MT 5, 8

<table>
<tr>
<td colspan="2">10. $\mathbf{T}A$ $\beta 7$
11. $\mathbf{T}C$ MP 1, 10
12. $\mathbf{T}X$ MP 3, 11
13. $\mathbf{T}Y$ MP 4, 11</td>
<td colspan="2">16. $\mathbf{T}B$ $\beta 7$
17. $\mathbf{T}C$ MP 2, 16
18. $\mathbf{T}X$ MP 3, 17
19. $\mathbf{T}Y$ MP 4, 17</td>
</tr>
<tr>
<td>14. $\mathbf{F}X$ $\beta 9$
$*$ 12, 14</td>
<td>15. $\mathbf{F}Y$ $\beta 9$
$*$ 13, 15</td>
<td>20. $\mathbf{F}X$ $\beta 9$
$*$ 18, 20</td>
<td>21. $\mathbf{F}Y$ $\beta 9$
$*$ 19, 21</td>
</tr>
</table>

Riešenie príkladu 5.32 s rezom, modus ponens a modus tolens

1.	$\mathbf{T}(A \to C)$	S^+
2.	$\mathbf{T}(B \to C)$	S^+
3.	$\mathbf{T}(C \to X)$	S^+
4.	$\mathbf{T}(C \to Y)$	S^+
5.	$\mathbf{T}((X \land Y) \to Z)$	S^+
6.	$\mathbf{F}((A \lor B) \to Z)$	S^+
7.	$\mathbf{T}(A \lor B)$	$\alpha 6$
8.	$\mathbf{F}\,Z$	$\alpha 6$
9.	$\mathbf{F}(X \land Y)$	MT $5, 8$

<table>
<tr>
<td colspan="2">10. $\mathbf{T}\,C$ cut
11. $\mathbf{T}\,X$ MP $3, 10$
12. $\mathbf{T}\,Y$ MP $4, 10$</td>
<td colspan="2">15. $\mathbf{F}\,C$ cut</td>
</tr>
<tr>
<td>13. $\mathbf{F}\,X$ $\beta 9$
$* \; 11, 13$</td>
<td>14. $\mathbf{F}\,Y$ $\beta 9$
$* \; 12, 14$</td>
<td>16. $\mathbf{T}\,A$ $\beta 7$
17. $\mathbf{T}\,C$ MP $1, 16$
$* \; 15, 17$</td>
<td>18. $\mathbf{T}\,B$ $\beta 7$
19. $\mathbf{F}\,B$ MT $2, 15$
$* \; 18, 19$</td>
</tr>
</table>

Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

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

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2}$$

$$\frac{\beta}{\beta_1 \mid \beta_2} \qquad \frac{}{A^+}\ A^+ \in S^+$$

Nech v je ľubovoľné ohodnotenie, v ktorom je pravdivá S^+.
Ak je vo v pravdivá premisa, tak je vo v pravdivý aspoň jeden záver.

- Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
- Netreba opačnú implikáciu (ak je vo v pravdivý aspoň jeden záver, tak je vo v pravdivá premisa).

Na dôkaz **úplnosti** stačili pravidlá (S^+), α, β, pretože stačia na vybudovanie úplného tabla.

Nové pravidlo

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

$$\frac{\mathbf{T}(X \to Y) \quad \mathbf{T}\, X}{\mathbf{T}\, Y} \quad ? \tag{MP}$$

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:

α: $\cdots$

$\vdots$

MP: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(X \to Y)$ a $\mathbf{T}\, X$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}\, Y$.

Nové pravidlo vs. korektnosť a úplnosť

Korektnosť tabiel s MP:

Pri dôkaze lemy K1

> *Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+ a v je ohodnotenie pre $\mathcal{L}$. Ak sú S^+ a $\mathcal{T}$ pravdivé vo v, tak je vo v pravdivé aj každé priame rozšírenie tabla $\mathcal{T}$.*

využijeme

Tvrdenie 5.33 (Korektnosť pravidla MP)

Nech X a Y sú ľubovoľné formuly a v je ľubovoľné ohodnotenie. Ak sú vo v pravdivé $\mathbf{T}(X \to Y)$ a $\mathbf{T}\, X$, tak je vo v pravdivá $\mathbf{T}\, Y$.

Dôkaz.

Keďže $v \models_p \mathbf{T}(X \to Y)$, tak $v \models_p (X \to Y)$, teda $v \not\models_p X$ alebo $v \models_p Y$. Pretože ale $v \models_p \mathbf{T}\, X$, tak $v \models_p X$. Takže $v \models_p Y$, a teda $v \models_p \mathbf{T}\, Y$. $\square$

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

Úplnosť — bez zmeny, úplné tablo vybudujú základné pravidlá.

Tablové pravidlá vo všeobecnosti — problém

Zadefinovať vo všeobecnosti, čo je pravidlo a kedy je korektné, nie je také jednoduché.

Potrebujeme zachytiť, že pravidlo:

- má premisy, ktoré nejaký tvar a zdieľajú nejaké podformuly, napr. moduls tolens (MT) má premisy $\mathbf{T}(X \to Y)$ a $\mathbf{F}\,Y$;
- odvodzuje z nich závery, ktoré tiež zdieľajú podformuly s premisami, napr. $\mathbf{F}\,X$ (alebo medzi sebou v prípade rezu).

pre všetky možné zdieľané podformuly, v našom príklade X a Y.

Tablové pravidlá vo všeobecnosti — vzor

Pravidlo sa dá predstaviť nasledovne:

Pravidlo má vzor — dvojicu tvorenú vzormi premís a záverov, kde spoločné podformuly predstavujú konkrétne atómy, napr. vzor pravidla MT:

$$\frac{\mathbf{T}(\mathrm{p}(\mathrm{c}) \to \mathrm{q}(\mathrm{c})) \quad \mathbf{F}\,\mathrm{q}(\mathrm{c})}{\mathbf{F}\,\mathrm{p}(\mathrm{c})}$$

Tablové pravidlá vo všeobecnosti — inštancia

Každý konkrétny prípad — inštancia pravidla vznikne substitúciou ľubovoľných formúl za atómy vo vzore:

$$\frac{\begin{array}{c}\mathbf{T}(\mathtt{p}(\mathtt{c}) \to \mathtt{q}(\mathtt{c}))[\mathtt{p}(\mathtt{c})|(\mathtt{sedan}(\mathtt{a}) \land \mathtt{biely}(\mathtt{a})),\ \mathtt{q}(\mathtt{c})|\mathtt{kupi}(\mathtt{B},\mathtt{a})]\\ \mathbf{F}\,\mathtt{q}(\mathtt{c})[\mathtt{p}(\mathtt{c})|(\mathtt{sedan}(\mathtt{a}) \land \mathtt{biely}(\mathtt{a})),\ \mathtt{q}(\mathtt{c})|\mathtt{kupi}(\mathtt{B},\mathtt{a})]\end{array}}{\mathbf{F}\,\mathtt{p}(\mathtt{c})[\mathtt{p}(\mathtt{c})|(\mathtt{sedan}(\mathtt{a}) \land \mathtt{biely}(\mathtt{a})),\ \mathtt{q}(\mathtt{c})|\mathtt{kupi}(\mathtt{B},\mathtt{a})]}$$

$$= \frac{\begin{array}{c}\mathbf{T}((\mathtt{sedan}(\mathtt{a}) \land \mathtt{biely}(\mathtt{a})) \to \mathtt{kupi}(\mathtt{B},\mathtt{a}))\\ \mathbf{F}\,\mathtt{kupi}(\mathtt{B},\mathtt{a})\end{array}}{\mathbf{F}(\mathtt{sedan}(\mathtt{a}) \land \mathtt{biely}(\mathtt{a}))}$$

Tablové pravidlá vo všeobecnosti — pravidlo

Samotné pravidlo je množina všetkých inštancií vzoru:

$$\mathsf{MT} = \left\{ \frac{\begin{array}{c}\mathbf{T}(\mathtt{p}(\mathtt{c}) \to \mathtt{q}(\mathtt{c}))_{[\mathtt{p}(\mathtt{c})|X,\ \mathtt{q}(\mathtt{c})|Y]} \\ \mathbf{F}\,\mathtt{q}(\mathtt{c})_{[\mathtt{p}(\mathtt{c})|X,\ \mathtt{q}(\mathtt{c})|Y]}\end{array}}{\mathbf{F}\,\mathtt{p}(\mathtt{c})_{[\mathtt{p}(\mathtt{c})|X,\ \mathtt{q}(\mathtt{c})|Y]}} \;\middle|\; X, Y \in \mathcal{E}_{\mathcal{L}} \right\}$$

Samozrejme, *konkrétne* pravidlo vieme zapísať aj bez substitúcie:

$$\mathsf{MT} = \left\{ \frac{\mathbf{T}(X \to Y) \quad \mathbf{F}\,Y}{\mathbf{F}\,X} \;\middle|\; X, Y \in \mathcal{E}_{\mathcal{L}} \right\}$$

Tablové pravidlá vo všeobecnosti

Definícia 5.34 (Vzor tablového pravidla)

Nech $n \geq 0$ a $k > 0$ sú prirodzené čísla, nech $P_1^+, \ldots, P_n^+$, $C_1^+, \ldots, C_k^+$ sú označené formuly.

Dvojicu tvorenú n-ticou $(P_1^+, \ldots, P_n^+)$ a k-ticou $(C_1^+, \ldots, C_k^+)$ a zapisovanú

$$\begin{array}{c}
P_1^+ \quad \cdots \quad P_n^+ \\
\hline
\begin{array}{c|c|c} C_1^+ & \cdots & C_k^+ \end{array}
\end{array}$$

nazývame ***vzorom tablového pravidla***.

Označené formuly $P_1^+, \ldots, P_n^+$ nazývame ***vzory premís***, označené formuly $C_1^+, \ldots, C_k^+$ nazývame ***vzory záverov***.

Definícia 5.35 (Tablové pravidlo a jeho inštancia)

Nech

$$\begin{array}{c|c|c} P_1^+ & \cdots & P_n^+ \\ \hline C_1^+ & \cdots & C_k^+ \end{array}$$

je vzor tablového pravidla a $a_1, \ldots, a_m$ sú všetky atómy, ktoré sa vyskytujú v označených formulách $P_1^+, \ldots, P_n^+, C_1^+, \ldots, C_k^+$.

Tablové pravidlo R je množina

$$R = \left\{ \begin{array}{c|c|c} P_1^+ {}_{[a_1|X_1,\ldots,a_m|X_m]} & \cdots & P_n^+ {}_{[a_1|X_1,\ldots,a_m|X_m]} \\ \hline C_1^+ {}_{[a_1|X_1,\ldots,a_m|X_m]} & \cdots & C_k^+ {}_{[a_1|X_1,\ldots,a_m|X_m]} \end{array} \middle| X_1, \ldots, X_m \in \mathcal{E}_{\mathcal{L}} \right\},$$

Každý prvok množiny R nazývame *inštanciou* pravidla R.

Keď už vieme, čo je pravidlo, môžeme povedať, kedy je korektné:

Definícia 5.36 (Tablové pravidlo a jeho korektnosť)

Tablové pravidlo R je *korektné* vtt
pre každú inštanciu pravidla R

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \;\middle|\; \cdots \;\middle|\; C_k^+}$$

a pre každé ohodnotenie v platí, že
ak sú vo v pravdivé **všetky** premisy $P_1^+, \ldots, P_n^+$,
tak je vo v pravdivý **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:

  $\vdots$

  ***R*:** Ak sa pre nejakú inštanciu pravidla R

$$\begin{array}{c|c|c} P_1^+ & \cdots & P_n^+ \\ \hline C_1^+ & \cdots & C_k^+ \end{array}$$

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

Príklad: korektnosť rezu

To, že rez

$$\begin{array}{c|c} \hline \mathbf{T}\,X & \mathbf{F}\,X \end{array}$$

je korektné pravidlo, dokážeme veľmi ľahko:

Tvrdenie 5.37 (Korektnosť pravidla rezu)

Nech X je ľubovoľná formula a v je ľubovoľné ohodnotenie.
Potom je vo v pravdivý niektorý zo záverov pravidla rezu
$\mathbf{T}\,X$ *alebo* $\mathbf{F}\,X$.

Dôkaz.

Formula X je vo v buď pravdivá alebo nepravdivá.
V prvom prípade $v \models_{\mathrm{p}} \mathbf{T}\,X$. V druhom prípade $v \models_{\mathrm{p}} \mathbf{F}\,X$.
Teda v oboch prípadoch platí, že vo v je pravdivý niektorý zo záverov $\mathbf{T}\,X$ alebo $\mathbf{F}\,X$ pravidla rezu. $\square$

Príklad: zložitejšie pravidlá

Príklady zložitejších pravidiel:

- Viacnásobné pravidlá β :

$$\frac{\mathbf{T}(A_1 \lor A_2 \lor \cdots \lor A_n)}{\mathbf{T}\,A_1 \mid \mathbf{T}\,A_2 \mid \cdots \mid \mathbf{T}\,A_n} \qquad \frac{\mathbf{F}(A_1 \land A_2 \land \cdots \land A_n)}{\mathbf{F}\,A_1 \mid \mathbf{F}\,A_2 \mid \cdots \mid \mathbf{F}\,A_n}$$

- Pravidlo konštruktívnej dilemy:

$$\frac{\mathbf{T}(P \to Q) \quad \mathbf{T}(R \to S) \quad \mathbf{T}(P \lor R)}{\mathbf{T}\,Q \quad\mid\quad \mathbf{T}\,S}$$

Zistite, či sú tieto pravidlá korektné.

Dôkazy a výrokovologické tablá

Iné dokazovacie systémy

Materiál z nasledujúcich slajdov slúži na ilustráciu historických súvislostí a rozšírenie všeobecného prehľadu. Ak ho nepreberáme aj inde, netreba sa ho učiť na skúšku ani na písomky.

Ukážeme si niekoľko iných dokazovacích systémov pre výrokovú logiku a porovnáme ich navzájom.

Hilbertov kalkul

Schémy axióm:

A1. $\varphi \to (\psi \to \varphi)$

A2. $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

A3. $((\neg\psi \to \neg\varphi) \to (\varphi \to \psi))$

Odvodzovacie pravidlo:

$$\frac{\varphi \quad \varphi \to \psi}{\psi} \qquad \text{modus ponens, MP}$$

Korektnosť: Všetky axiómy sú tautológie, MP je korektné pravidlo.

FOL: Áno, pridať 2 axiómy a 2 pravidlá pre kvantifikátory.

Hilbertov kalkul: príklad dôkazu

Dokážeme $p \to p$.

1. $(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$ A2
2. $p \to ((p \to p) \to p)$ A1
3. $(p \to (p \to p)) \to (p \to p)$ MP(2,1)
4. $p \to (p \to p)$ A1
5. $p \to p$ MP(4,3)

- Dôkaz je neprimerane dlhý a zahŕňa formuly podstatne zložitejšie ako dokazovaná. Odkiaľ ich vziať?

Hilbertov kalkul vs. tablá

- *Korektnosť Hilbertovho kalkulu:*
  Každá formula v dôkaze je splnená v každej štruktúre
  (lebo je to tautológia či dôsledok MP).
  Korektnosť je tak zjavná, priam triviálna.
- Naopak pri tablách je korektnosť komplikovaná: tablo dáva zmysel len ako celok, jednotlivé formuly v ňom sú bezvýznamné, nevieme nič povedať o ich splniteľnosti (dokonca niektoré vetvy obsahujú spor, ale to je opäť vlastnosť celej vety, nie jednotlivých formúl na nej).
- *Korektnosť tablového kalkulu:*
  Množina S^+ je splniteľná vtt existuje vetva, v ktorej sú v nejakej štruktúre splnené všetky formuly naraz.
- Tieto (červene vyznačené) invarianty sa zachovajú aj po pridaní kvantifikátorov.

Hilbertov kalkul vs. tablá

Pri *úplnosti* je to zase naopak:

- Pre tablá je pomerne zjavná — tablo rozbije formulu na atómy a ak by pre tautológiu X nebol v nejakej vetve tabla pre $\mathbf{F}\,X$ spor, priamo si z vetvy prečítame ohodnotenie atómov, v ktorom by X nebola splnená.
- Pre Hilbertov kalkul vôbec nevidno, prečo by práve uvedené axiómy boli postačujúce. Príklad podobnej sady axióm, ktorá nie je úplná:

  A1. $\varphi \to (\psi \to \varphi)$
  A2. $\neg\varphi \to (\varphi \to \psi)$
  A3. $\neg\neg\varphi \to \varphi$

Sekventový kalkul

Sekvent je zápis v tvare $\Gamma \vdash \Delta$. Intuitívne:
ak platia všetky formuly z Γ, potom platí aspoň jedna formula z Δ.

Základné pravidlá:

- Identita (Ax): $\varphi \vdash \varphi$
- Oslabenie: $\dfrac{\Gamma \vdash \Delta}{\Gamma, \varphi \vdash \Delta}$, $\quad \dfrac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}$
- Kontrakcia: $\dfrac{\Gamma, \varphi, \varphi \vdash \Delta}{\Gamma, \varphi \vdash \Delta}$, $\quad \dfrac{\Gamma \vdash \Delta, \varphi, \varphi}{\Gamma \vdash \Delta, \varphi}$
- Výmena: $\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \psi, \varphi \vdash \Delta}$, $\quad \dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \psi, \varphi}$
- Pravidlá pre log. spojky, napr. $\to_L$: $\dfrac{\Gamma \vdash \varphi \quad \psi, \Gamma' \vdash \Delta}{\Gamma, \Gamma', \varphi \to \psi \vdash \Delta}$

Korektnosť: Všetky pravidlá zachovávajú pravdivosť.
FOL: Áno, pridať 4 pravidlá pre kvantifikátory.

Sekventový kalkul: príklad dôkazu

Dokážeme sekvent $p,\ p \to q \vdash q$.

$$\dfrac{\dfrac{}{p \vdash p}\,(\mathrm{Ax}) \qquad \dfrac{}{q \vdash q}\,(\mathrm{Ax})}{p,\ p \to q \vdash q}\,(\to_L)$$

Pri použití $\to_L$ máme $\Gamma = p, \Gamma' = \emptyset, \varphi = p, \psi = q, \Delta = q$.

- Nutnosť pravidiel pre výmenu a kontrakciu naznačuje nepríjemnosti pri používaní.
- Dokazované formuly postupne skladáme z jednoduchších častí, nevyskytuje sa použitie „uhádnutých“ dlhých formúl ako pri Hilbertovom kalkule.
- Dôkazy v niektorých variantoch sekventového kalkulu vyzerajú ako tablo obrátené hore nohami.

Sekventový kalkul: teória typov

- Sekventový kalkul sa využíva v teórii typov. Množina Γ reprezentuje typy existujúcich premenných, t.j. kontext, v rámci ktorého uvažujeme o typoch nových premenných.
- Ukážka pravidiel:

$$\frac{\Gamma \vdash f : A \to B \quad \Gamma \vdash a : A}{\Gamma \vdash f(a) : B} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash (\lambda x.t) : A \to B}$$

- Typy v programovacích jazykoch sú netriviálny problém: napr. šablóny v C++ sú turingovsky úplné (v čase kompilácie).
- Funkcionálne jazyky ako Haskell sú cenené pre ľahkú dokázateľnosť správnosti programov. Súčasťou tých dôkazov je presné a dokázateľne korektné uvažovanie o typoch premenných.

Rezolvencia

Rezolvencia operuje nad klauzulami (disjunkciami literálov) a odvodzuje nové klauzuly, kým nenájde spor (prázdnu klauzulu).

Dve pravidlá:

$$\frac{(A \vee C_1 \vee C_2) \qquad (\neg A \vee B_1 \vee B_2)}{C_1 \vee C_2 \vee B_1 \vee B_2} \qquad \frac{A \vee A \vee C_1 \vee C_2}{A \vee C_1 \vee C_2}$$

Rezolvenciou možno znížiť počet klauzúl či boolovských premenných (atómov vo formulách), čo naznačuje, ako postupovať pri dôkaze nesplniteľnosti množiny formúl.

Korektnosť: Rezolvenčné pravidlo zachováva pravdivosť.
FOL: Áno, pomocou skolemizácie a unifikácie.

Rezolvencia: príklad dôkazu

Dokážeme nesplniteľnosť množiny

$$\{A \vee B, \qquad \neg A, \qquad \neg B\}.$$

1. Rezolvujeme $A \vee B$ s $\neg A$, dostaneme B.
2. Rezolvujeme B s $\neg B$, dostávame prázdnu klauzulu, tá je nesplniteľná.

- Vstup pre rezolvenciu je „umelý“, keďže všetko treba prepísať do klauzúl.
- Aj dôkaz je tak dosť neprirodzený a nekopíruje originálnu formalizáciu.

Dokazovacie systémy

Existujú iné typy dokazovacích systémov, najmä dvoch druhov:

- Historické, sú prekonané alebo sa neujali, napr. aristotelovské sylogizmy či existenciálne grafy (obrázkový systém, Peirce 1882). Vlastne každý veľký logik v minulosti vymyslel vlastný systém, keďže sme nemali žiadne štandardy.
- Moderné z posledných cca 20 rokov, budúcnosť nejasná.

Pre **výrokovú** logiku sú všetky dokazovacie systémy úplné (ak je niečo pravda, existuje dôkaz) a dôkaz vieme algoritmicky nájsť.

Pre **predikátovú** logiku (s kvantifikátormi) sa dajú použiť všetky okrem SAT solverov. Stále sú úplné, ale dôkaz nemožno algoritmicky hľadať. Tu je veľký priestor pre umelú inteligenciu.

Dokazovacie systémy

Používané dokazovacie systémy sa dajú zhruba zhrnúť do dvoch skupín:

- **hilbertovské**: „veľa axióm, málo pravidiel“ (bežne len MP), dôkazy sú dlhé, pôsobia umelo a neintuitívne;
- **gentzenovské**: „veľa pravidiel, málo axióm“ (ideálne žiadne), dôkazy sú kratšie a priamočiarejšie (ale štrukturálne zložitejšie, vetvenie miesto lineárnosti) — tablá, prirodzená dedukcia, sekventový kalkul.

Rezolvencia a SAT solvery sú skôr gentzenovské (nemajú axiómy), ale sú zamerané na výpočtový výkon, nie prirodzenosť, priamočiarosť či prehľadnosť dôkazov.

Pre trénovanie AI má prehľadnosť a generalizovateľnosť veľkú hodnotu aj z hľadiska počítačového spracovania, nielen pre ľudské pochopenie. Napr. AlphaProof sa učil na miliónoch vygenerovaných dôkazov neveľmi zaujímavých geometrických tvrdení v Lean.

História

1900	Hilbertov program (hľadanie úplnej sady axióm)
1920s	hilbertovský systém (Hilbert, Ackermann)
1930s	prirodzená dedukcia a sekventový kalkul (Gentzen)
1950s	tablo (Beth, Smullyan)
1965	rezolvencia (Robinson)
1970s	Prolog (SLD-rezolvencia, orientovaná na cieľ)
1980s	tablá pre modálnu logiku (musí/môže byť)
1990s	tablá na vrchole popularity
2000s	ústup tabiel, rezolvencia pre FOL s rovnosťou (dokazovač Vampire), SAT solvery pre výrokovú logiku
2010s	SMT solvery (SAT + aritmetika + polia, nie kvantifikátory), dominujú vo verifikácii programov
2020s	Lean (based on type theory), AI proof search

Literatúra

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