Výroková a predikátová logika - III

Petr Gregor

KTIML MFF UK

ZS 2015/2016

Teorie

Neformálně, teorie je popis "světa", na který vymezujeme svůj diskurz.

- Výroková *teorie* nad jazykem $\mathbb{P}$ je libovolná množina T výroků z $\mathrm{VF}_{\mathbb{P}}$. Výrokům z T říkáme *axiomy* teorie T.
- *Model teorie* T nad $\mathbb{P}$ je ohodnocení $v \in M(\mathbb{P})$ (tj. model jazyka), ve kterém platí všechny axiomy z T, značíme $v \models T$.
- *Třída modelů* T je $M^{\mathbb{P}}(T) = \{v \in M(\mathbb{P}) \mid v \models \varphi$ pro každé $\varphi \in T\}$.

  Např. pro teorii $T = \{p,\ \neg p \vee \neg q,\ q \rightarrow r\}$ nad $\mathbb{P} = \{p, q, r\}$ je

$$M^{\mathbb{P}}(T) = \{(1,0,0), (1,0,1)\}$$

- Je-li teorie T konečná, lze ji nahradit *konjunkcí* jejích axiomů.
- Zápis $M(T, \varphi)$ značí $M(T \cup \{\varphi\})$.

Sémantika vzhledem k teorii

Sémantické pojmy zobecníme vzhledem k teorii, respektive k jejím modelům.

Nechť T je teorie nad $\mathbb{P}$. Výrok φ nad $\mathbb{P}$ je

- *pravdivý v T* (*platí v T*), pokud platí v každém modelu T, značíme $T \models \varphi$, Říkáme také, že φ je (sémantickým) *důsledkem* teorie T.
- *lživý v T* (*sporný v T*), pokud neplatí v žádném modelu teorie T,
- *nezávislý v T*, pokud platí v nějakém modelu teorie T a neplatí v jiném,
- *splnitelný v T* (*konzistentní s T*), pokud platí v nějakém modelu T.

Výroky φ a ψ jsou *ekvivalentní v T* (*T-ekvivalentní*), psáno $\varphi \sim_T \psi$, pokud každý model teorie T je modelem φ právě když je modelem ψ.

Poznámka Jsou-li všechny axiomy teorie T pravdivé (tautologie), např. pro $T = \emptyset$, všechny pojmy vzhledem k T se shodují s původními (logickými) pojmy.

Důsledek teorie

Důsledek teorie T nad $\mathbb{P}$ je množina $\theta^{\mathbb{P}}(T)$ všech výroků pravdivých v T, tj.

$$\theta^{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid T \models \varphi\}.$$

Tvrzení *Pro každé dvě teorie $T \subseteq T'$ a výroky $\varphi, \varphi_1, \ldots, \varphi_n$ nad $\mathbb{P}$ platí*

(1) $T \subseteq \theta^{\mathbb{P}}(T) = \theta^{\mathbb{P}}(\theta^{\mathbb{P}}(T)) \subseteq \theta^{\mathbb{P}}(T')$,

(2) $\varphi \in \theta^{\mathbb{P}}(\{\varphi_1, \ldots, \varphi_n\})$ *právě když* $\models (\varphi_1 \wedge \ldots \wedge \varphi_n) \rightarrow \varphi$.

Důkaz Dle definic, $T \models \varphi \;\Leftrightarrow\; M(T) \subseteq M(\varphi)$ a $M(T') \subseteq M(T) = M(\theta(T))$.

(1)
$$\begin{aligned} \varphi \in T \;\Rightarrow\; M(T) \subseteq M(\varphi) \;&\Leftrightarrow\; T \models \varphi \;\Leftrightarrow\; \varphi \in \theta(T) \;\Leftrightarrow \\ M(\theta(T)) \subseteq M(\varphi) \;&\Leftrightarrow\; \theta(T) \models \varphi \;\Leftrightarrow\; \varphi \in \theta(\theta(T)) \;\Rightarrow \\ M(T') \subseteq M(\varphi) \;&\Leftrightarrow\; T' \models \varphi \;\Leftrightarrow\; \varphi \in \theta(T') \end{aligned}$$

Část (2) plyne obdobně z $M(\varphi_1, \ldots, \varphi_n) = M(\varphi_1 \wedge \ldots \wedge \varphi_n)$ a $\models \psi \rightarrow \varphi$ právě když $M(\psi) \subseteq M(\varphi)$. $\square$

Vlastnosti teorií

Výroková teorie T nad $\mathbb{P}$ je *(sémanticky)*

- *sporná*, jestliže v ní platí $\perp$ (spor), jinak je *bezesporná* (*splnitelná*),
- *kompletní*, jestliže není sporná a každý výrok je v ní pravdivý či lživý, tj. žádný výrok v ní není nezávislý,
- *extenze* teorie T' nad $\mathbb{P}'$, jestliže $\mathbb{P}' \subseteq \mathbb{P}$ a $\theta^{\mathbb{P}'}(T') \subseteq \theta^{\mathbb{P}}(T)$, o extenzi T teorie T' řekneme, že je *jednoduchá*, pokud $\mathbb{P} = \mathbb{P}'$, a *konzervativní*, pokud $\theta^{\mathbb{P}'}(T') = \theta^{\mathbb{P}}(T) \cap \mathrm{VF}_{\mathbb{P}'}$,
- *ekvivalentní* s teorií T', jestliže T je extenzí T' a T' je extenzí T,

Pozorování *Nechť T a T' jsou teorie nad $\mathbb{P}$. Teorie T je (sémanticky)*

1. *bezesporná, právě když má model,*
2. *kompletní, právě když má jediný model,*
3. *extenze T', právě když $M^{\mathbb{P}}(T) \subseteq M^{\mathbb{P}}(T')$,*
4. *ekvivalentní s T', právě když $M^{\mathbb{P}}(T) = M^{\mathbb{P}}(T')$.*

Algebra výroků

Nechť T je bezesporná teorie nad $\mathbb{P}$. Na množině $\mathrm{VF}_{\mathbb{P}}/\!\sim_T$ lze zadefinovat operace $\neg$, $\wedge$, $\vee$, $\perp$, $\top$ (korektně) pomocí reprezentantů, např.

$$[\varphi]_{\sim_T} \wedge [\psi]_{\sim_T} = [\varphi \wedge \psi]_{\sim_T}$$

Pak $AV^{\mathbb{P}}(T) = \langle \mathrm{VF}_{\mathbb{P}}/\!\sim_T, \neg, \wedge, \vee, \perp, \top \rangle$ je *algebra výroků* vzhledem k T.

Jelikož $\varphi \sim_T \psi \;\Leftrightarrow\; M(T,\varphi) = M(T,\psi)$, je $h([\varphi]_{\sim_T}) = M(T,\varphi)$ korektně definovaná prostá funkce $h\colon \mathrm{VF}_{\mathbb{P}}/\!\sim_T \to \mathcal{P}(M(T))$ a platí

$$\begin{aligned} h(\neg[\varphi]_{\sim_T}) &= M(T) \setminus M(T,\varphi) \\ h([\varphi]_{\sim_T} \wedge [\psi]_{\sim_T}) &= M(T,\varphi) \cap M(T,\psi) \\ h([\varphi]_{\sim_T} \vee [\psi]_{\sim_T}) &= M(T,\varphi) \cup M(T,\psi) \\ h([\perp]_{\sim_T}) = \emptyset, &\quad h([\top]_{\sim_T}) = M(T) \end{aligned}$$

Navíc h je *na*, pokud $M(T)$ je *konečná*.

Důsledek Je-li T bezesporná nad konečnou $\mathbb{P}$, je $AV^{\mathbb{P}}(T)$ Booleova algebra *izomorfní* s (konečnou) potenční algebrou $\underline{\mathcal{P}}(M(T))$ via h.

Analýza teorií nad konečně prvovýroky

Nechť T je bezesporná teorie nad $\mathbb{P}$, kde $|\mathbb{P}| = n \in \mathbb{N}^+$ a $m = |M^{\mathbb{P}}(T)|$. Pak

- neekvivalentních výroků (popř. teorií) nad $\mathbb{P}$ je 2^{2^n},
- neekvivalentních výroků nad $\mathbb{P}$ pravdivých (lživých) v T je $2^{2^n - m}$,
- neekvivalentních výroků nad $\mathbb{P}$ nezávislých v T je $2^{2^n} - 2.2^{2^n - m}$,
- neekvivalentních jednoduchých extenzí teorie T je 2^m, z toho sporná 1,
- neekvivalentních kompletních jednoduchých extenzí teorie T je m,
- T-neekvivalentních výroků nad $\mathbb{P}$ je 2^m,
- T-neekvivalentních výroků nad $\mathbb{P}$ pravdivých (lživých) (v T) je 1,
- T-neekvivalentních výroků nad $\mathbb{P}$ nezávislých (v T) je $2^m - 2$.

Důkaz Díky bijekci $\mathrm{VF}_{\mathbb{P}}/\sim$ resp. $\mathrm{VF}_{\mathbb{P}}/\sim_T$ s $\mathcal{P}(M(\mathbb{P}))$ resp. $\mathcal{P}(M^{\mathbb{P}}(T))$ stačí zjistit počet podmnožin s vhodnou vlastností. $\square$

Formální dokazovací systémy

Naším cílem je přesně formalizovat pojem důkazu jako syntaktické procedury.

Ve *(standardních)* formálních dokazovacích systémech,

- důkaz je konečný objekt, může vycházet z axiomů dané teorie,
- $T \vdash \varphi$ značí, že φ je *dokazatelná* z T,
- pokud důkaz dané formule existuje, lze ho nalézt *"algoritmicky"*,
  (Je-li T *"rozumně zadaná"*.)

Od formálního dokazovacího systému obvykle očekáváme, že bude

- *korektní*, tj. každá formule φ dokazatelná z teorie T je v T pravdivá,
- nejlépe i *úplný*, tj. každá formule φ pravdivá v T je z T dokazatelná.

Příklady formálních dokazovacích systémů (kalkulů): tablo metody, *Hilbertovské systémy, Gentzenovy systémy, systémy přirozené dedukce*.

Tablo metoda - úvod

Budeme předpokládat, že jazyk je pevný a spočetný, tj. množina prvovýroků $\mathbb{P}$ je spočetná. Pak každá teorie nad $\mathbb{P}$ je spočetná.

Hlavní rysy tablo metody *(neformálně)*

- tablo pro danou formuli φ je binární značkovaný strom reprezentující vyhledávání *protipříkladu* k φ, tj. modelu teorie, ve kterém φ neplatí,
- formule má důkaz, pokud každá větev příslušného tabla selže, tj. nebyl nalezen protipříklad, v tom případě bude (systematické) tablo konečné,
- pokud protipříklad existuje, v (dokončeném) tablu bude větev, která ho poskytuje, tato větev může být i nekonečná.

Úvodní příklady

- $F(((p \to q) \to p) \to p)$
  - $T((p \to q) \to p)$
    - Fp
      - $T((p \to q) \to p)$
        - $F(p \to q)$
          - $F(p \to q)$
            - Tp
              - Fq
                - $\otimes$
        - Tp
          - $\otimes$

- $F((\neg q \vee p) \to p)$
  - $T(\neg q \vee p)$
    - Fp
      - $T(\neg q \vee p)$
        - $T(\neg q)$
          - $T(\neg q)$
            - Fq
        - Tp
          - $\otimes$

Komentář k příkladům

Vrcholy tabla jsou značeny *položkami*. Položka je formule s *příznakem* T / F, který reprezentuje předpoklad, že formule v nějakém modelu platí / neplatí. Je-li tento předpoklad u položky správný, je správný i v nějaké větvi pod ní.

V obou příkladech jde o dokončená (systematická) tabla z prázdné teorie.

- Vlevo je *tablo důkaz* pro $((p \to q) \to p) \to p$. Všechny větve tabla *"selhaly"*, značeno $\otimes$, neboť je na nich dvojice $T\varphi$, $F\varphi$ pro nějaké φ *(protipříklad tedy nelze nalézt)*. Formule má důkaz, píšeme
$$\vdash ((p \to q) \to p) \to p$$
- Vpravo je (dokončené) tablo pro $(\neg q \vee p) \to p$. Levá větev *"neselhala"* a je dokončená (není třeba v ní pokračovat) *(ta poskytuje protipříklad* $v(p) = v(q) = 0$*)*.

Atomická tabla

Atomické tablo je jeden z následujících (položkami značkovaných) stromů, kde p je libovolná výroková proměnná a φ, ψ jsou libovolné výrokové formule.

Tp	Fp	$\begin{array}{c} T(\varphi \wedge \psi) \\ \mid \\ T\varphi \\ \mid \\ T\psi \end{array}$	$\begin{array}{ccc} & F(\varphi \wedge \psi) & \\ / & & \backslash \\ F\varphi & & F\psi \end{array}$	$\begin{array}{ccc} & T(\varphi \vee \psi) & \\ / & & \backslash \\ T\varphi & & T\psi \end{array}$	$\begin{array}{c} F(\varphi \vee \psi) \\ \mid \\ F\varphi \\ \mid \\ F\psi \end{array}$
$\begin{array}{c} T(\neg\varphi) \\ \mid \\ F\varphi \end{array}$	$\begin{array}{c} F(\neg\varphi) \\ \mid \\ T\varphi \end{array}$	$\begin{array}{ccc} & T(\varphi \rightarrow \psi) & \\ / & & \backslash \\ F\varphi & & T\psi \end{array}$	$\begin{array}{c} F(\varphi \rightarrow \psi) \\ \mid \\ T\varphi \\ \mid \\ F\psi \end{array}$	$\begin{array}{ccc} & T(\varphi \leftrightarrow \psi) & \\ / & & \backslash \\ T\varphi & & F\varphi \\ \mid & & \mid \\ T\psi & & F\psi \end{array}$	$\begin{array}{ccc} & F(\varphi \leftrightarrow \psi) & \\ / & & \backslash \\ T\varphi & & F\varphi \\ \mid & & \mid \\ F\psi & & T\psi \end{array}$

Pomocí atomických tabel a pravidel, jak tabla rozvinout (prodloužit), formálně zadefinujeme všechna tabla (popíšeme jejich konstrukci).

Tablo

Konečné tablo je binární, položkami značkovaný strom daný předpisem

(i) každé atomické tablo je konečné tablo,

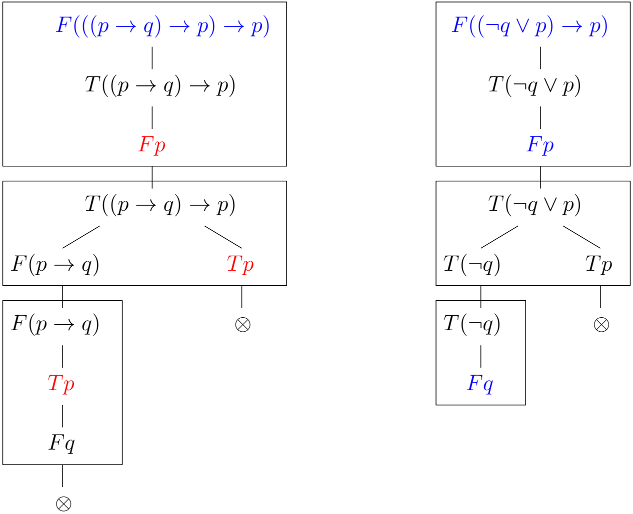
(ii) je-li P položka na větvi V konečného tabla τ a τ' vznikne z τ připojením atomického tabla pro P na konec větve V, je τ' rovněž konečné tablo,

(iii) každé konečné tablo vznikne konečným užitím pravidel (i), (ii).

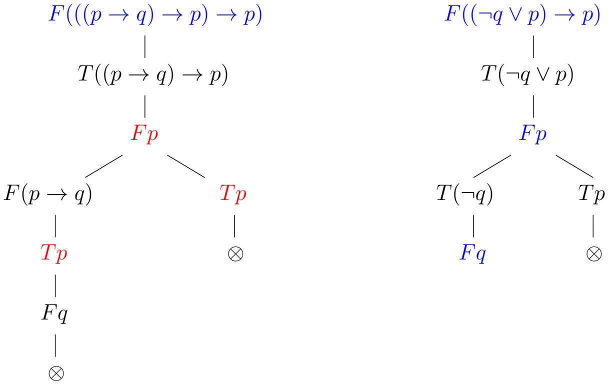
Tablo je posloupnost $\tau_0, \tau_1, \ldots, \tau_n, \ldots$ (konečná i nekonečná) konečných tabel takových, že τ_{n+1} vznikne z τ_n pomocí pravidla (ii), formálně $\tau = \cup\tau_n$.

Poznámka *Není předepsané, jak položku P a větev V pro krok (ii) vybírat. To specifikujeme až v systematických tablech.*

Konstrukce tabla



Konvence



Položku, dle které tablo prodlužujeme, nebudeme na větvi znovu zobrazovat.

Poznámka *Její zopakování bude potřeba později v predikátové logice.*

Tablo důkaz

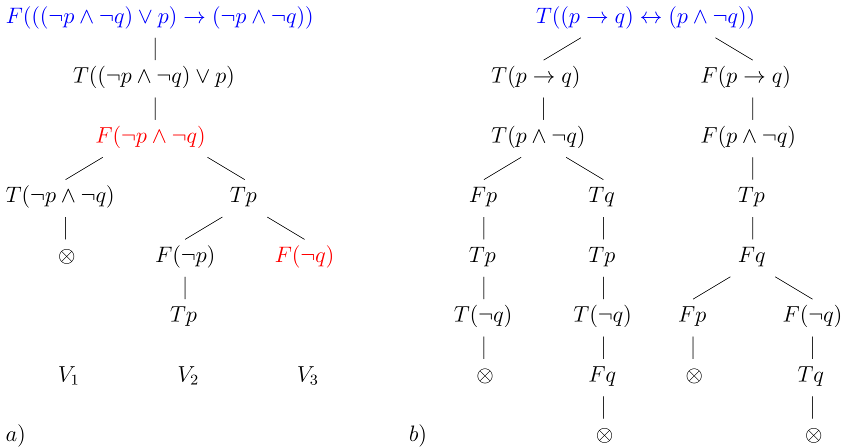
Nechť P je položka na větvi V tabla τ. Řekneme, že

- položka P je *redukovaná* na V, pokud se na V vyskytuje jako kořen atomického tabla, tj. při konstrukci τ již došlo k jejímu rozvoji na V,
- větev V je *sporná*, obsahuje-li položky $T\varphi$ a $F\varphi$ pro nějakou formuli φ, jinak je *bezesporná*. Větev V je *dokončená*, je-li sporná nebo je každá její položka redukovaná na V,
- tablo τ je *dokončené*, pokud je každá jeho větev dokončená, a je *sporné*, pokud je každá jeho větev sporná.

Tablo důkaz (*důkaz tablem*) výrokové formule φ je sporné tablo s položkou $F\varphi$ v kořeni. φ je *(tablo) dokazatelná*, píšeme $\vdash \varphi$, má-li tablo důkaz.

Obdobně, *zamítnutí* formule φ *tablem* je sporné tablo s položkou $T\varphi$ v kořeni. Formule φ je *(tablo) zamítnutelná*, má-li zamítnutí tablem, tj. $\vdash \neg\varphi$.

Příklady



a) $F(\neg p \wedge \neg q)$ neredukovaná na V_1, V_1 sporná, V_2 je dokončená, V_3 není,

b) zamítnutí tablem výrokové formule φ: $(p \to q) \leftrightarrow (p \wedge \neg q)$, tedy $\vdash \neg\varphi$.

Tablo z teorie

Jak do důkazu přidat axiomy dané teorie T?

Konečné tablo z teorie T je zobecnění konečného tabla přidáním pravidla

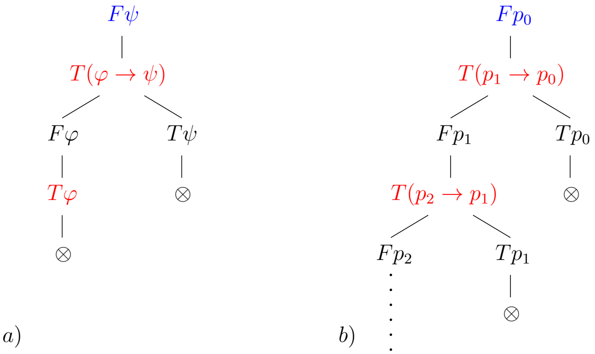
(ii)' je-li V větev konečného tabla (z T) a $\varphi \in T$, pak připojením $T\varphi$ na konec V vznikne (také) konečné tablo z T.

Přidáním dodatku *"z teorie T"* přirozeně zobecníme další pojmy

- *tablo z teorie* T je posloupnost $\tau_0, \tau_1, \ldots, \tau_n, \ldots$ konečných tabel z T takových, že τ_{n+1} vznikne z τ_n pomocí (ii) či (ii)', formálně $\tau = \cup\tau_n$,
- *tablo důkaz* formule φ *z teorie* T je sporné tablo z T s $F\varphi$ v kořeni, Má-li φ tablo důkaz z T, je *(tablo) dokazatelná z* T, píšeme $T \vdash \varphi$.
- *zamítnutí* formule φ *tablem z teorie* T je sporné tablo z T s $T\varphi$ v kořeni.

Narozdíl od předchozích definic, u tabla z teorie T je větev V *dokončená*, je-li sporná, nebo je každá její položka redukovaná na V a navíc obsahuje $T\varphi$ pro každé $\varphi \in T$.

Příklady tabla z teorie



a) Tablo důkaz formule ψ z teorie $T = \{\varphi, \varphi \to \psi\}$, tedy $T \vdash \psi$.

b) Dokončené tablo pro formuli p_0 z teorie $T = \{p_{n+1} \to p_n \mid n \in \mathbb{N}\}$.
Všechny větve jsou dokončené, nejlevější větev je bezesporná a nekonečná. Poskytuje (jediný) model teorie T, ve kterém p_0 neplatí.