

# Výroková a predikátová logika - III

Petr Gregor

KTIML MFF UK

ZS 2020/21

# Horn-SAT

- *Jednotková klauzule* je klauzule obsahující jediný literál,
- *Hornova klauzule* je klauzule obsahující **nejvýše** jeden pozitivní literál,  
$$\neg p_1 \vee \dots \vee \neg p_n \vee q \sim (p_1 \wedge \dots \wedge p_n) \rightarrow q$$
- *Hornův výrok* je konjunkcí Hornových klauzulí,
- *Horn-SAT* je problém splnitelnosti daného Hornova výroku.

## Algoritmus

- ① *obsahuje-li  $\varphi$  dvojici jednotkových klauzulí  $l$  a  $\bar{l}$ , není splnitelný,*
- ② *obsahuje-li  $\varphi$  jednotkovou klauzuli  $l$ , nastav  $l$  na 1, odstraň všechny klauzule obsahující  $l$ , odstraň  $\bar{l}$  ze všech klauzulí a opakuj od začátku,*
- ③ *neobsahuje-li  $\varphi$  jednotkovou klauzuli, je splnitelný ohodnocením 0 všech zbývajících proměnných.*

Krok (2) se nazývá *jednotková propagace*.

# Jednotková propagace

$$(\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg r \vee \neg s) \wedge (\neg t \vee s) \wedge s$$

$$v(s) = 1$$

$$(\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge \neg r$$

$$v(\neg r) = 1$$

$$(\neg p \vee q) \wedge (\neg p \vee \neg q)$$

*Takže t  
nemění výsledek díky  
S je ho de potřeba nastavit*

$$v(p) = v(q) \Rightarrow v(t) = 0$$

**Pozorování** Necht'  $\varphi^l$  je výrok získaný z  $\varphi$  **jednotkovou propagací**. Pak  $\varphi^l$  je splnitelný, právě když  $\varphi$  je splnitelný.

**Důsledek** Algoritmus je korektní (řeší Horn-SAT).

**Důkaz** Korektnost 1. kroku je zřejmá, v 2. kroku plyne z pozorování, v 3. kroku díky **Hornově tvaru**, neboť každá zbývající klauzule obsahuje negativní literál.

**Poznámka** Přímočará implementace vyžaduje kvadratický čas, při vhodné reprezentaci v paměti lze dosáhnout lineárního času (vzhledem k délce  $\varphi$ ).

# Teorie

*Neformálně, teorie je popis “světa”, na který vymezujeme svůj diskurz.*

- Výroková **teorie** nad jazykem  $\mathbb{P}$  je libovolná množina  $T$  výroků z  $\text{VF}_{\mathbb{P}}$ .  
Výrokům z  $T$  říkáme **axiomy** teorie  $T$ . *příravní 0 a 1 kvadraticky prvočíslo*
- **Model teorie**  $T$  nad  $\mathbb{P}$  je ohodnocení  $v \in M(\mathbb{P})$  (tj. model jazyka),  
ve kterém platí všechny axiomy z  $T$ , značíme  $v \models T$ . *všechny modely*
- **Třída modelů**  $T$  je  $M^{\mathbb{P}}(T) = \{v \in M(\mathbb{P}) \mid v \models \varphi \text{ pro každé } \varphi \in T\}$ . *co znamená ohodnocení teorie*

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  $\varphi$  nad  $\mathbb{P}$  je

- **pravdivý v  $T$  (platí v  $T$ )**, pokud platí v každém modelu  $T$ , značíme  $T \models \varphi$ ,  
Říkáme také, že  $\varphi$  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  $\varphi$  a  $\psi$  jsou **ekvivalentní v  $T$  ( $T$ -ekvivalentní)**, psáno  $\varphi \sim_T \psi$ , pokud každý model teorie  $T$  je modelem  $\varphi$  právě když je modelem  $\psi$ .

**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.

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

*↔ axiomy, které platí v teorii  $T$  (tedy ve všech modelech  $T$  teorie)*

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

⊙  $T \subseteq \theta^{\mathbb{P}}(T) = \theta^{\mathbb{P}}(\theta^{\mathbb{P}}(T)),$

⊙  $T \subseteq T' \Rightarrow \theta^{\mathbb{P}}(T) \subseteq \theta^{\mathbb{P}}(T'),$  *množství vzhledem ke inkluzi*

⊙  $\varphi \in \theta^{\mathbb{P}}(\{\varphi_1, \dots, \varphi_n\}) \Leftrightarrow \models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \varphi.$  *↔ vždy rozšířím axiomy teorie, tak všechno co platilo v  $T$ , musí platit i v  $T'$*

**Důkaz** Snadno z definic, neboť  $T \models \varphi \Leftrightarrow M(T) \subseteq M(\varphi)$  a navíc

⊙  $M(\theta(T)) = M(T),$  *↔ obrácení inkluze!*

⊙  $T \subseteq T' \Rightarrow M(T') \subseteq M(T),$  *↔ vždycky musí všechny axiomy  $T'$  splnit všechny v  $T$*

⊙  $\models \psi \rightarrow \varphi \Leftrightarrow M(\psi) \subseteq M(\varphi), M(\varphi_1 \wedge \dots \wedge \varphi_n) = M(\varphi_1, \dots, \varphi_n). \quad \square$

# Vlastnosti teorií

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

*ve správné je např.: všechno platné.  
Z jedné lži má plyne celádiv.*

- **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,

*všechno, co přišlo v původní teorii,  
i v té rozšířené*

- **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  $\theta^{\mathbb{P}'}(T') = \theta^{\mathbb{P}}(T) \cap \text{VF}_{\mathbb{P}'}$ ,

*výroků původního jazyka.  
Nové výroky již budou v rozšířeného jazyka  $\mathbb{P}$ .*

- **ekvivalentní** s teorií  $T'$ , jestliže  $T$  je extenzí  $T'$  a  $T'$  je extenzí  $T$ ,

*$T = \{p\} = \mathbb{P}$   $T' = \{p, r\} = \mathbb{P}$ . Jde o konzervativní extenzi.*

**Pozorování** Necht'  $T$  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  $M^{\mathbb{P}}(T) = M^{\mathbb{P}}(T')$ .

*protože musí platit všechny axiomy  
pokud by jich bylo více, musel by existovat provýrok, co v jednom je True, v druhém False, tedy musí být nezávislý, pokud ota modely platí.*

$1) \iff 2) \iff 3) \iff 4)$   
 $\iff \theta(T) \subseteq \theta(T')$

1) pokud  $\forall \phi \in \theta(T)$ , pak  $\phi \in M^{\mathbb{P}}(T) \supseteq M^{\mathbb{P}}(T')$ , tedy platí na modelech  $T'$ , tudíž i na modelech  $T$ . Tudíž musí platit i na  $\theta(T)$ .  
 2) Mějme odůvodnění ve  $M^{\mathbb{P}}(T)$ . Mějme  $\forall \phi \in M^{\mathbb{P}}(T')$ , ten patří  $\theta(T)$ . Tak patří i do  $\theta(T)$ . Tudíž v musí platit i v  $M^{\mathbb{P}}(T)$

# Algebra výroků

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

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

*- Tohle je třída*

*Tohle je nově vzniklá třída.*

Pak  $AV^{\mathbb{P}}(T) = \langle \text{VF}_{\mathbb{P}} / \sim_T, \neg, \wedge, \vee, \perp, \top \rangle$  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  $h: \text{VF}_{\mathbb{P}} / \sim_T \rightarrow \mathcal{P}(M(T))$  a platí

$$h(\neg[\varphi]_{\sim_T}) = M(T) \setminus M(T, \varphi)$$

$$h([\varphi]_{\sim_T} \wedge [\psi]_{\sim_T}) = M(T, \varphi) \cap M(T, \psi)$$

$$h([\varphi]_{\sim_T} \vee [\psi]_{\sim_T}) = M(T, \varphi) \cup M(T, \psi)$$

$$h([\perp]_{\sim_T}) = \emptyset, \quad h([\top]_{\sim_T}) = M(T)$$

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  $2^{2^n}$ , *→ kolik je možných podmnožin modelu.  $2^n = \#$  možných označení  $2^x = \#$  podmnožin*
- neekvivalentních výroků nad  $\mathbb{P}$  pravdivých (lživých) v  $T$  je  $2^{2^n - m}$ ,
- neekvivalentních výroků nad  $\mathbb{P}$  nezávislých v  $T$  je  $2^{2^n} - 2 \cdot 2^{2^n - m}$ , *pravdivých lživých*
- neekvivalentních jednoduchých extenzí teorie  $T$  je  $2^m$ , *vybíráme podmnožiny*, z toho sporná **1**,
- neekvivalentních kompletních jednoduchých extenzí teorie  $T$  je  $m$ , *vybíráme signatury*
- $T$ -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  $\text{VF}_{\mathbb{P}} / \sim$  resp.  $\text{VF}_{\mathbb{P}} / \sim_T$  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  $\varphi$  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  $\varphi$  dokazatelná z teorie  $T$  je v  $T$  pravdivá,
- nejlépe i *úplný*, tj. každá formule  $\varphi$  pravdivá v  $T$  je z  $T$  dokazatelná.

Příklady formálních dokazovacích systémů (kalkulů): *tablo metody*,

*Hilbertovské systémy*, *Gentzenovy systémy*, *systémy přirozené dedukce*.

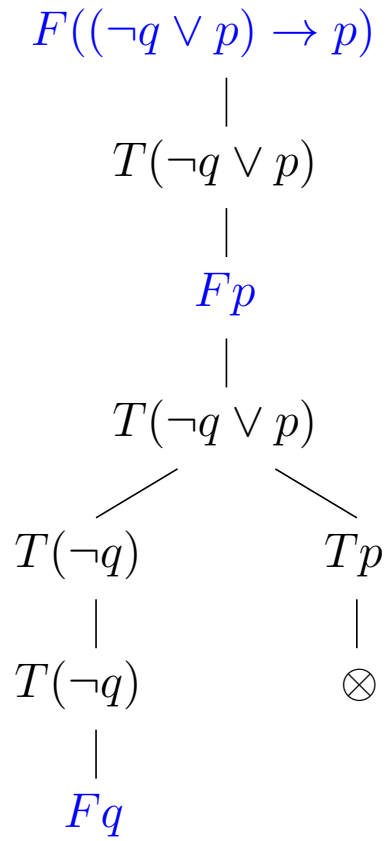
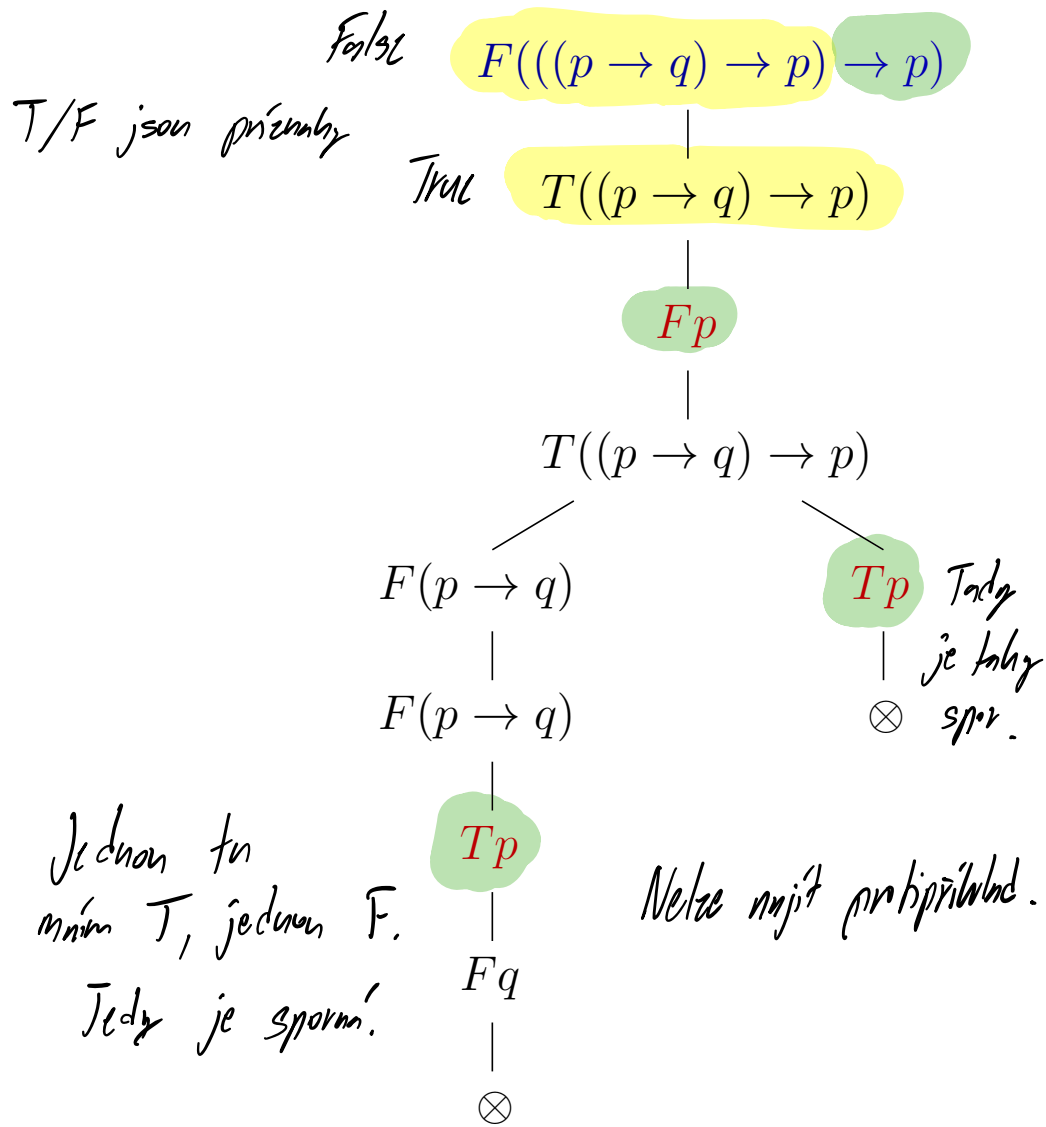
# Tablo metoda - úvod

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  $\varphi$  je binární značkový strom reprezentující vyhledávání **protipříkladu** k  $\varphi$ , tj. modelu teorie, ve kterém  $\varphi$  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



# 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  $((p \rightarrow q) \rightarrow p) \rightarrow p$ . Všechny větve tabla “selhaly”, značeno  $\otimes$ , neboť je na nich dvojice  $T\varphi, F\varphi$  pro nějaké  $\varphi$  (*protipříklad tedy nelze nalézt*). Formule má důkaz, píšeme

$$\vdash ((p \rightarrow q) \rightarrow p) \rightarrow p$$

- Vpravo je (dokončené) tablo pro  $(\neg q \vee p) \rightarrow p$ . 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  $\varphi, \psi$  jsou libovolné výrokové formule.

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

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

# Tablo

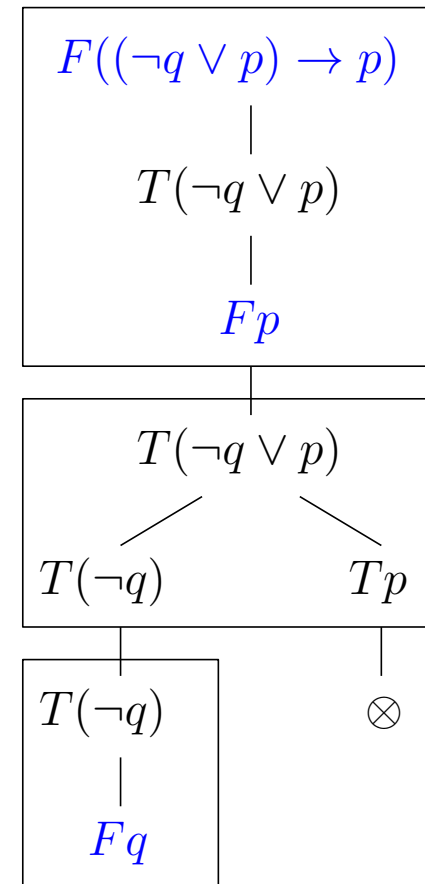
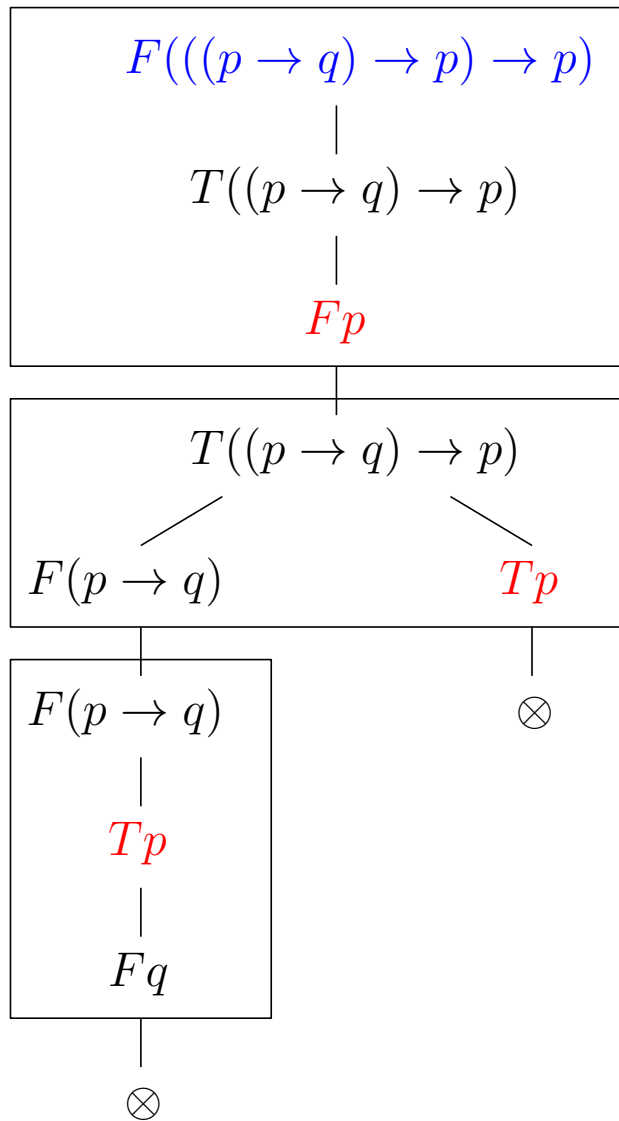
**Konečné tablo** je binární, položkami značkový strom daný předpisem

- (i) každé atomické tablo je konečné tablo,
- (ii) je-li  $P$  položka na větvi  $V$  konečného tabla  $\tau$  a  $\tau'$  vznikne z  $\tau$  **připojením** atomického tabla pro  $P$  na **konec větve**  $V$ , je  $\tau'$  rovněž konečné tablo,
- (iii) každé konečné tablo vznikne **konečným** užitím pravidel (i), (ii).

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

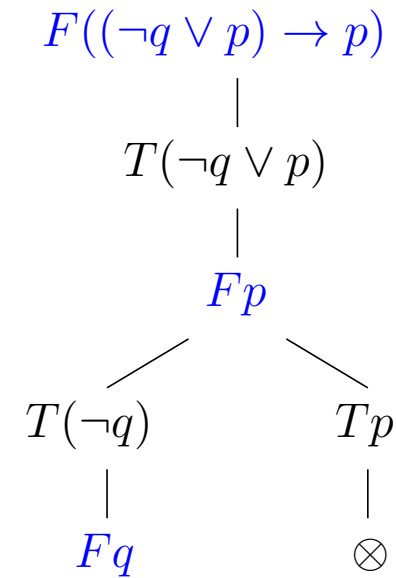
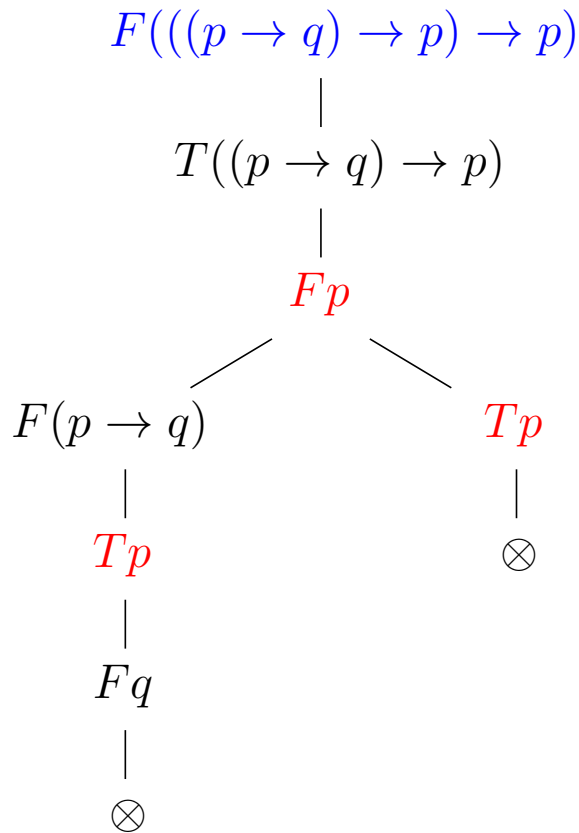
**Poznámka** *Není předepsané, jak položku  $P$  a větev  $V$  pro krok (ii) vybírat. To specifikujeme až v **systematických** tablech.*

# Konstrukce tabla





# Konvence



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

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

# Tablo důkaz

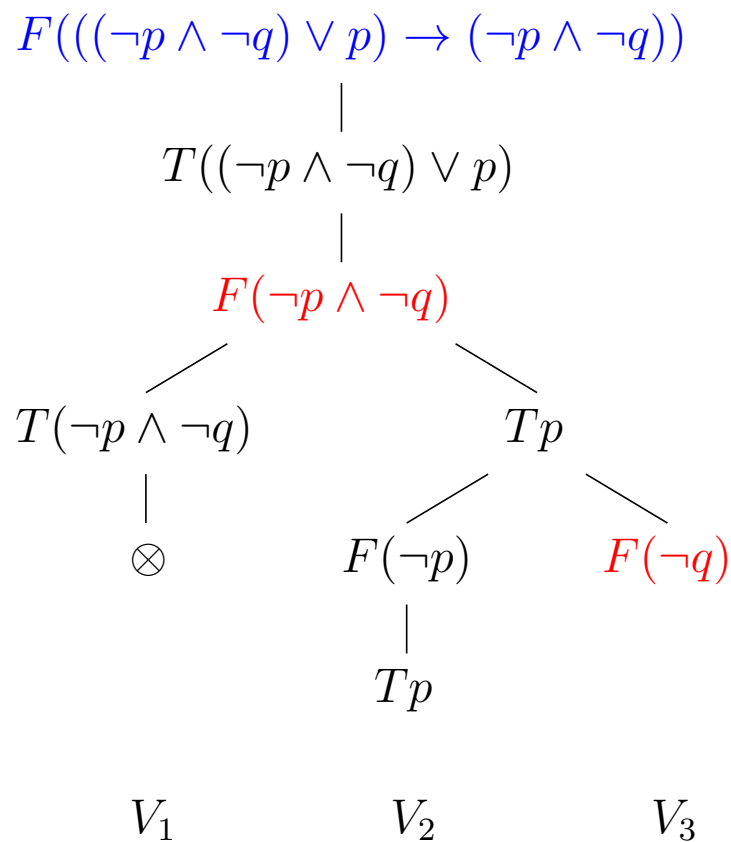
Nechť  $P$  je položka na větvi  $V$  tabla  $\tau$ . Řekneme, že

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

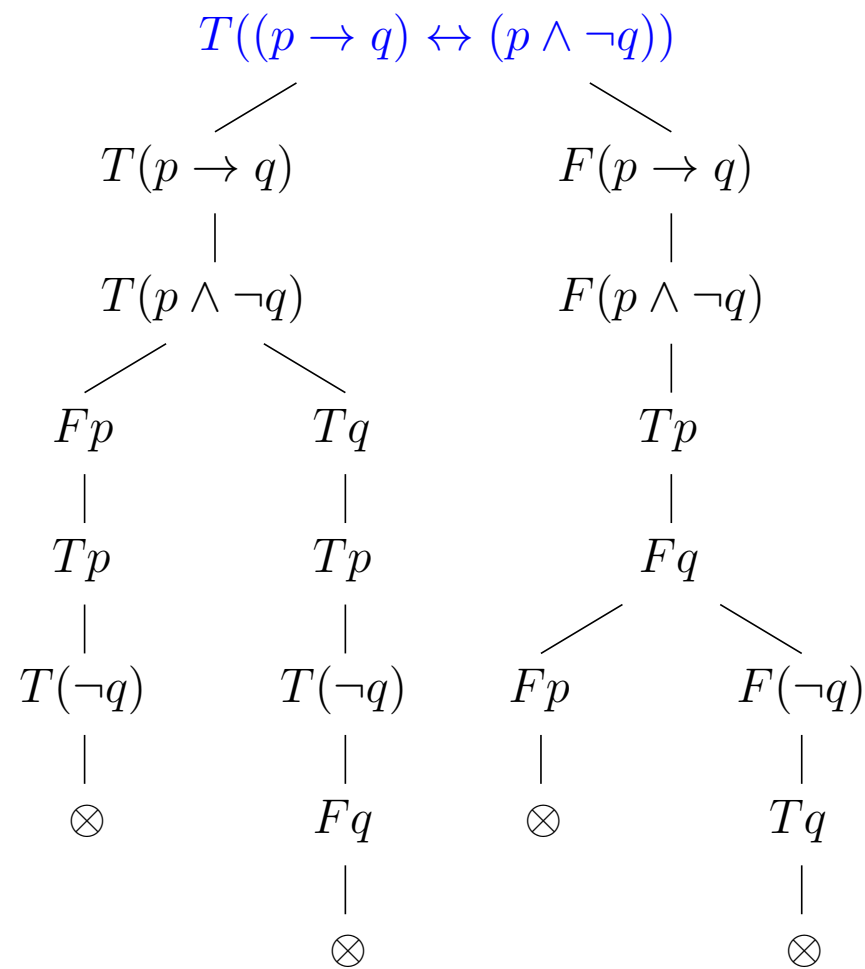
*Tablo důkaz* (*důkaz tablem*) výrokové formule  $\varphi$  je *sporné tablo* s položkou  $F\varphi$  v kořeni.  $\varphi$  je (*tablo*) *dokazatelná*, píšeme  $\vdash \varphi$ , má-li tablo důkaz.

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

# Příklady



a)



b)

- 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  $\varphi: (p \rightarrow q) \leftrightarrow (p \wedge \neg q)$ , tedy  $\vdash \neg\varphi$ .