Čtvrtá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Čtvrtá přednáška

Program

- úvod do tablo metody
- tablo důkaz
- korektnost a úplnost

Materiály

Zápisky z přednášky, Sekce 4.1-4.6 z Kapitoly 4

Kapitola 4: Metoda analytického tabla

4.1 Formální dokazovací systémy

Formální dokazovací systém

chceme zjistit, zda výrok platí [$T \models \varphi$], a to čistě syntakticky, aniž bychom se zabývali sémantikou: najít (formální) důkaz [$T \vdash \varphi$]

důkaz je konečný syntaktický objekt vycházející z φ a axiomů T

dokazování lze dělat algoritmicky (pokud máme algoritmický přístup k axiomům T, která může být nekonečná), a lze rychle algoritmicky ověřit, zda je daný objekt opravdu korektní důkaz

- korektnost: "co dokážu, platí" $T \vdash \varphi \ \Rightarrow\ T \models \varphi$
- úplnost: "dokážu vše, co platí" $T \models \varphi \ \Rightarrow\ T \vdash \varphi$

(korektnost je nutná, úplnost ne: rychlý dokazovací systém může být praktický i když není úplný)

ukážeme si: *tablo metodu*, *hilbertovský kalkulus*, *rezoluční metodu*

nutný předpoklad: jazyk musí být spočetný (potom i T je spočetná)

4.2 Úvod do tablo metody

Tablo metoda neformálně

nejprve případ $T = \emptyset$, tedy dokazujeme, že φ platí *v logice*

tablo je strom představující hledání protipříkladu (modelu $v \not\models \varphi$), když všechny větve selžou, máme důkaz (sporem)

labely: položky $\mathrm{T}\psi, \mathrm{F}\psi$ (určují, zda na dané větvi platí výrok ψ)

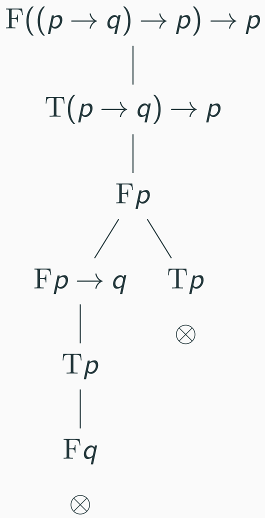
kořen $\mathrm{F}\varphi$, dále rozvíjíme redukcí položek (podle struktury výroků v nich), aby platil invariant:

Každý model, který se *shoduje* s položkou v kořeni (tj. ve kterém neplatí φ), se musí *shodovat* i s některou větví tabla (tj. splňovat všechny požadavky vyjádřené položkami na této větvi).

je-li na větvi $\mathrm{T}\psi$ a zároveň $\mathrm{F}\psi$, potom selhala (je sporná), pokud všechny větve selhaly, je tablo sporné, je to důkaz $T \vdash \varphi$

pokud nějaká větev neselhala a je dokončená (vše na ní zredukované), lze z ní zkonstruovat model, ve kterém φ neplatí

Příklad: tablo důkaz $((p \to q) \to p) \to p$



- důkaz sporem: v kořeni příznak F
- redukujeme položku tvaru $\mathrm{F}\varphi_1 \to \varphi_2$:
- pokud $v \not\models \varphi_1 \to \varphi_2$, nutně $v \models \varphi_1$ a zároveň $v \not\models \varphi_2$
- proto na větev připojíme položky $\mathrm{T}(p \to q) \to p$ a $\mathrm{F}p$, invariant platí
- redukce položky $\mathrm{T}(p \to q) \to p$: model se shoduje s $\mathrm{F}(p \to q)$ nebo s $\mathrm{T}p$, rozvětvi!
- redukce $\mathrm{F}(p \to q)$: připoj $\mathrm{T}p$ a $\mathrm{F}q$
- všechny větve sporné, protipříklad neexistuje, tedy máme tablo důkaz, píšeme: $\vdash ((p \to q) \to p) \to p$

Příklad: tablo pro $\mathrm{F}(\neg q \vee p) \to p$

$$\mathrm{F}(\neg q \vee p) \to p$$

$$\mathrm{T}\neg q \vee p$$

$$\mathrm{F}p$$

$$\mathrm{T}\neg q \qquad \mathrm{T}p$$

$$\mathrm{F}q \qquad \otimes$$

$$\checkmark$$

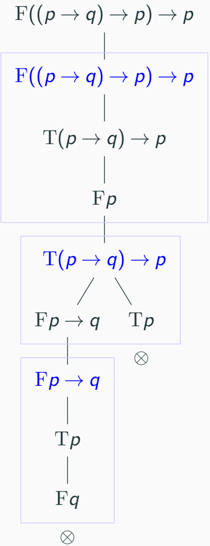
- tablo je dokončené, ale není sporné
- tedy nejde o důkaz
- levá větev dává protipříklad: model $v = (0, 0)$ ve kterém výrok neplatí
- invariant říká, že existuje-li protipříklad, shoduje se s některou větví
- tato větev nemůže být sporná
- tak se dokáže korektnost tablo metody

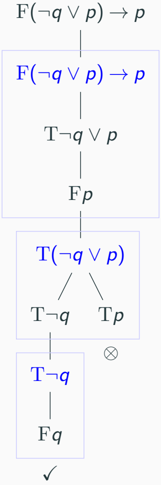
Poznámky

- Jak redukujeme položky?
  - Připojíme příslušné atomické tablo (viz následující slide) na konec všech bezesporných větví procházejících vrcholem.
- Co když dokazujeme v nějaké teorii T?
  - Připojíme položky $\mathrm{T}\alpha$ pro (všechny) axiomy $\alpha \in T$.
- Co když je T nekonečná?
  - Tablo může být nekonečné.
  - Ale vyjde-li sporné, lze sestrojit jiné, které je konečné a také sporné. ("Existuje-li důkaz, existuje konečný důkaz.")

Atomická tabla

	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
True	$\begin{array}{c} \mathrm{T}\neg\varphi \\ \vert \\ \mathrm{F}\varphi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi \wedge \psi \\ \vert \\ \mathrm{T}\varphi \\ \vert \\ \mathrm{T}\psi \end{array}$	$\begin{array}{ccc} & \mathrm{T}\varphi \vee \psi & \\ / & & \backslash \\ \mathrm{T}\varphi & & \mathrm{T}\psi \end{array}$	$\begin{array}{ccc} & \mathrm{T}\varphi \rightarrow \psi & \\ / & & \backslash \\ \mathrm{F}\varphi & & \mathrm{T}\psi \end{array}$	$\begin{array}{ccc} & \mathrm{T}\varphi \leftrightarrow \psi & \\ / & & \backslash \\ \mathrm{T}\varphi & & \mathrm{F}\varphi \\ \vert & & \vert \\ \mathrm{T}\psi & & \mathrm{F}\psi \end{array}$
False	$\begin{array}{c} \mathrm{F}\neg\varphi \\ \vert \\ \mathrm{T}\varphi \end{array}$	$\begin{array}{ccc} & \mathrm{F}\varphi \wedge \psi & \\ / & & \backslash \\ \mathrm{F}\varphi & & \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \vee \psi \\ \vert \\ \mathrm{F}\varphi \\ \vert \\ \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \rightarrow \psi \\ \vert \\ \mathrm{T}\varphi \\ \vert \\ \mathrm{F}\psi \end{array}$	$\begin{array}{ccc} & \mathrm{F}\varphi \leftrightarrow \psi & \\ / & & \backslash \\ \mathrm{T}\varphi & & \mathrm{F}\varphi \\ \vert & & \vert \\ \mathrm{F}\psi & & \mathrm{T}\psi \end{array}$





konvence: kořeny atomických tabel (modře) nezakreslujeme

O stromech

- strom je $T \neq \emptyset$ s částečným uspořádáním $<_T$, které má nejmenší prvek (kořen) a množina předků libovolného vrcholu je dobře uspořádaná (každá její neprázdná podmnožina má nejmenší prvek, to zakáže nekonečné klesající řetězce předků)
- větev je maximální lineárně uspořádaná podmnožina T.
- uspořádaný strom má navíc lineární uspořádání $<_L$ množiny synů každého vrcholu (říkáme mu pravolevé, $<_T$ je stromové)
- označkovaný strom má navíc funkci $\mathrm{label}\colon T \to \mathrm{Labels}$

Königovo lemma: Nekonečný, konečně větvící strom má nekonečnou větev.

4.3 Tablo důkaz

Formální definice tabla

- položka je nápis $\mathrm{T}\varphi$ nebo $\mathrm{F}\varphi$, kde φ je nějaký výrok
- konečné tablo z teorie T je uspořádaný, položkami označkovaný strom zkonstruovaný aplikací konečně mnoha následujících pravidel:
  - jednoprvkový strom s libovolnou položkou je tablo z teorie T
  - pro libovolnou položku P na libovolné větvi V můžeme na konec větve V připojit atomické tablo pro položku P
  - na konec libovolné větve můžeme připojit položku $\mathrm{T}\alpha$ pro libovolný axiom $\alpha \in T$
- tablo z teorie T je buď konečné, nebo i nekonečné: v tom případě je spočetné a definujeme ho jako $\tau = \bigcup_{i \geq 0} \tau_i$, kde:
  - τ_i jsou konečná tabla z T
  - τ_0 je jednoprvkové tablo
  - τ_{i+1} vzniklo z τ_i v jednom kroku
- tablo pro položku P je tablo, které má položku P v kořeni

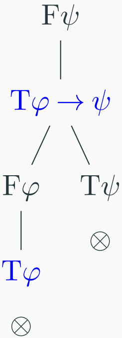
Dokončené a sporné tablo

- Tablo je sporné, pokud je každá jeho větev sporná.
- Větev je sporná, pokud obsahuje položky $\mathrm{T}\psi$ a $\mathrm{F}\psi$ pro nějaký výrok ψ, jinak je bezesporná.
- Tablo je dokončené, pokud je každá jeho větev dokončená.
- Větev je dokončená, pokud je sporná, nebo
  - každá její položka je na této větvi redukovaná,
  - a zároveň obsahuje položku $\mathrm{T}\alpha$ pro každý axiom $\alpha \in T$.
- Položka P je redukovaná na větvi V procházející touto položkou, pokud
  - je tvaru $\mathrm{T}p$ resp. $\mathrm{F}p$ pro nějaký prvovýrok $p \in \mathbb{P}$,
  - nebo se vyskytuje na V jako kořen atomického tabla (byť ho podle konvence nezakreslujeme), tj., typicky, při konstrukci tabla již došlo k jejímu rozvoji na V.

Tablo důkaz a tablo zamítnutí

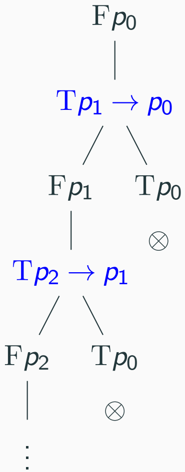
- tablo důkaz výroku φ z teorie T je sporné tablo z teorie T s položkou $\mathrm{F}\varphi$ v kořeni
- pokud existuje, je φ (tablo) dokazatelný z T, píšeme $T \vdash \varphi$
- podobně, tablo zamítnutí je sporné tablo s $\mathrm{T}\varphi$ v kořeni
- existuje-li, je φ (tablo) zamítnutelný z T, tj. platí $T \vdash \neg\varphi$

Příklad: tablo důkaz



- tablo důkaz výroku ψ z $T = \{\varphi, \varphi \to \psi\}$
- položky vycházející z axiomů jsou modře
- ukázali jsme tedy $T \vdash \psi$
- φ, ψ jsou libovolné pevně dané výroky
- tím jsme dokázali tzv. větu o dedukci

Příklad: dokončené tablo, které není sporné



- dokončené tablo pro výrok p_0 z teorie $T = \{p_{n+1} \to p_n \mid n \in \mathbb{N}\}$.
- nejlevější větev je dokončená a bezesporná
- sestává z položek $\mathrm{T}p_{i+1} \to p_i$ a $\mathrm{F}p_i$ pro všechna $i \in \mathbb{N}$
- shoduje se s modelem $v = (0, 0, \dots)$, tj. $v : \mathbb{P} \to \{0, 1\}$ kde $v(p_i) = 0$ pro vš. i
- máme protipříklad ukazující, že $T \not\models p_0$

4.4 Konečnost a systematičnost důkazů

Konečnost a systematičnost důkazů

Dokážeme:

- existuje-li tablo důkaz, existuje i konečný tablo důkaz
- existuje algoritmus, který umí vždy zkonstruovat dokončené tablo, tzv. systematické tablo
- tento algoritmus tedy zkonstruuje tablo důkaz, pokud existuje

  (zde potřebujeme *korektnost* a *úplnost*, ty dokážeme později)

  (pokud tablo důkaz neexistuje, algoritmus se nemusí zastavit)

Dokončení tabla: v čem je problém?

Pro konečnou T je snadné zkonstruovat dokončené tablo:

- na začátku použijeme všechny axiomy
- při redukci položek se výroky v nich zkracují
- stačí nedělat zbytečné kroky

Pro nekonečnou T bychom ale mohli zkonstruovat nekonečné tablo, a přitom:

- nikdy nepoužít některý axiom, nebo
- nikdy se nedostat k redukci některé položky

Myšlenka systematického tabla: na všechny se dostane, střídáme

- redukce následující položky (po úrovních, zleva doprava) na všech bezesporných větvích, které jí procházejí
- přidání následujícího axiomu na všechny bezesporné větve (T je spočetná, axiomy libovolně očíslujeme)

Definice systematického tabla

Systematické tablo z teorie $T = \{\alpha_1, \alpha_2, \dots\}$ pro položku R je tablo $\tau = \bigcup_{i \geq 0} \tau_i$, kde τ_0 je jednoprvkové tablo s položkou R, a pro každé $i \geq 0$:

- buď P nejlevější položka v co nejmenší úrovni, která není redukovaná na nějaké bezesporné větvi procházející P
- nejprve definujeme τ_i' jako tablo vzniklé z τ_i připojením atomického tabla pro P na každou bezespornou větev procházející P
- pokud taková položka P neexistuje, potom $\tau_i' = \tau_i$
- tablo τ_{i+1} vznikne z τ_i' připojením $\mathrm{T}\alpha_{i+1}$ na každou bezespornou větev
- to v případě, že $i < |T|$, jinak (je-li T konečná a už jsme použili všechny axiomy) definujeme $\tau_{i+1} = \tau_i'$

Dokončenost systematického tabla

Lemma: Systematické tablo je dokončené.

Důkaz: Jsou všechny větve dokončené?

- Sporné větve jsou dokončené z definice.
- Bezesporná větev:
  - obsahuje $\mathrm{T}\alpha_i$ pro všechna i (připojeno v i-tém kroku)
  - každá položka je na ní zredukovaná (leží-li v hloubce d, dostali jsme se k ní nejdéle v kroku $i = 2^{d+1} - 1$)
- Tedy i všechny bezesporné větve jsou dokončené. $\square$

Konečnost sporu

Věta (Konečnost sporu): Je-li $\tau = \bigcup_{i \geq 0} \tau_i$ sporné tablo, potom existuje $n \in \mathbb{N}$ takové, že τ_n je sporné konečné tablo.

Důkaz: Buď S množina všech vrcholů, nad kterými (ve stromovém uspořádání) není spor, tj. dvojice položek $\mathrm{T}\psi$, $\mathrm{F}\psi$.

- Kdyby byla S nekonečná: Podle Königova lemmatu pro podstrom τ na množině S máme nekonečnou, bezespornou větev v S. To ale dává i bezespornou větev v τ, což je spor.
- Množina S je tedy konečná, celá leží v hloubce $\leq d$ pro nějaké $d \in \mathbb{N}$. Každý vrchol na úrovni $d + 1$ už má nad sebou spor.
- Zvolme n tak, že τ_n už obsahuje všechny vrcholy τ z prvních $d + 1$ úrovní. Potom každá větev tabla τ_n je sporná. $\square$

Důsledky konečnosti sporu

Tedy: Pokud neprodlužujeme už sporné větve (např. pro systematické tablo), potom sporné tablo je konečné.

Důsledek (Konečnost důkazů): Pokud $T \vdash \varphi$, potom existuje i konečný tablo důkaz φ z T.

Důkaz: Platí $\tau = \tau_n$, neboť sporné tablo už neměníme. $\square$

Důsledek (Systematičnost důkazů): Pokud $T \vdash \varphi$, potom systematické tablo je (konečným) tablo důkazem φ z T.

Důkaz bude až v příští sekci, chybí nám dvě fakta:

- je-li φ dokazatelná z T, potom v T platí (Věta o korektnosti)
- pokud by systematické tablo mělo bezespornou větev, šel by z ní vyrobit protipříklad (to je klíč k důkazu Věty o úplnosti)1

4.5 Korektnost a úplnost

Korektnost a úplnost

Nyní ukážeme, že dokazatelnost je totéž, co platnost, tj. pro každou teorii T a výrok φ:

$$T \vdash \varphi \ \Leftrightarrow \ T \models \varphi$$

Rozdělíme na dvě implikace:

- $T \vdash \varphi \ \Rightarrow \mathrm{T} \models \varphi$ (korektnost) *"co jsme dokázali, platí"*
- $T \models \varphi \ \Rightarrow \mathrm{T} \vdash \varphi$ (úplnost) *"co platí, lze dokázat"*

Korektnost: pomocné lemma

Model v se shoduje

- s položkou P, pokud $P = \mathrm{T}\varphi$ a $v \models \varphi$, nebo $P = \mathrm{F}\varphi$ a $v \not\models \varphi$
- s větví V, pokud se shoduje s každou položkou na této větvi

Lemma: Shoduje-li se model teorie T s položkou v kořeni tabla z teorie T, potom se shoduje s některou větví.

Důkaz: Indukcí podle kroků i při konstrukci tabla $\tau = \bigcup_{i\geq 0} \tau_i$ najdeme posloupnost větví $V_0 \subseteq V_1 \subseteq \ldots$ takovou, že:

- V_i je větev v tablu τ_i shodující se s modelem v
- V_{i+1} je prodloužením V_i

Hledaná větev v τ je potom $V = \bigcup_{i\geq 0} V_i$.

Báze indukce: Model v se shoduje s kořenem τ, tj. s (jednoprvkovou) větví V_0 v τ_0.

Pokračování důkazu pomocného lemmatu

Indukční krok:

Pokud τ_{i+1} vzniklo z τ_i bez prodloužení V_i, definujeme $V_{i+1} = V_i$.

Pokud τ_{i+1} vzniklo připojením $\mathrm{T}\alpha$ (pro axiom $\alpha \in T$) na konec V_i, definujeme V_{i+1} jako tuto prodlouženou větev. Protože $v \models T$, máme i $v \models \alpha$, tedy v se shoduje i s novou položkou.

Nechť τ_{i+1} vzniklo připojením atomického tabla pro položku P na konec V_i. Protože se v shoduje s P (která leží na V_i), shoduje se i s kořenem připojeného atomického tabla, a proto se shoduje i s některou z jeho větví. (Ověříme si pro všechna atomická tabla.) Definujeme V_{i+1} jako prodloužení V_i o tuto větev atomického tabla. $\square$

Věta o korektnosti [tablo metody ve výrokové logice]

Věta (O korektnosti): Je-li výrok φ tablo dokazatelný z teorie T, potom je φ pravdivý v T, tj. $T \vdash \varphi \Rightarrow \mathrm{T} \models \varphi$.

Myšlenka důkazu: Protipříklad by se shodoval s některou z větví tablo důkazu, ty jsou ale všechny sporné.

Důkaz: Sporem, nechť $T \not\models \varphi$, tj. existuje $v \in \mathrm{M}(T)$, že $v \not\models \varphi$.

Protože je $T \vdash \varphi$, existuje tablo důkaz φ z T, což je sporné tablo z T s položkou $\mathrm{F}\varphi$ v kořeni.

Model v se shoduje s kořenem $\mathrm{F}\varphi$, tedy podle Lemmatu se shoduje s nějakou větví V. Všechny větve jsou ale sporné. Takže na V jsou $\mathrm{T}\psi$ a $\mathrm{F}\psi$ (pro nějaký výrok ψ), a model v se s těmito položkami shoduje. Máme $v \models \psi$ a zároveň $v \not\models \psi$, což je spor. $\square$

Úplnost: pomocné lemma

chceme selže-li dokazování, dostaneme bezespornou, dokončenou větev v tablu z T s $\mathrm{F}\varphi$ v kořeni; ukážeme, že dává protipříklad:

Kanonický model pro bezespornou, dokončenou větev V je model

$$v(p) = \begin{cases} 1 \text{ pokud se na } V \text{ vyskytuje položka } \mathrm{T}p \\ 0 \text{ jinak} \end{cases}$$

Lemma: Kanonický model pro (bezespornou, dokončenou) větev V se shoduje s V.

(tento model tedy musí splňovat všechny axiomy T, ale protože se shoduje s položkou $\mathrm{F}\varphi$ v kořeni, neplatí v něm výrok φ)

Důkaz pomocného lemmatu

Důkaz: Indukcí podle struktury výroků v položkách. Báze indukce:

- je-li $P = \mathrm{T}p$ pro prvovýrok p, máme $v(p) = 1$, shoduje se
- je-li $P = \mathrm{F}p$, potom na V nemůže být $\mathrm{T}p$ (byla by sporná), máme tedy $v(p) = 0$, shoduje se

Indukční krok: rozebereme dva případy, ostatní jsou obdobné

- $P = \mathrm{T}\varphi \wedge \psi$. Protože je V dokončená, je na ní P redukovaná. To znamená, že se na V vyskytují i položky $\mathrm{T}\varphi$ a $\mathrm{T}\psi$. Podle indukčního předpokladu se s nimi v shoduje: $v \models \varphi$ a $v \models \psi$. Takže platí i $v \models \varphi \wedge \psi$ a v se shoduje s P.
- $P = \mathrm{F}\varphi \wedge \psi$. Protože je P na V redukovaná, vyskytuje se na V položka $\mathrm{F}\varphi$ nebo položka $\mathrm{F}\psi$. Platí tedy $v \not\models \varphi$ nebo $v \not\models \psi$, z čehož plyne $v \not\models \varphi \wedge \psi$ a v se shoduje s P. $\square$

Věta o úplnosti (+ důkaz systematičnosti)

Věta (O úplnosti): Je-li výrok φ pravdivý v teorii T, potom je tablo dokazatelný z T, tj. $T \models \varphi \;\Rightarrow \mathrm{T} \vdash \varphi$.

Důkaz: Ukážeme, že libovolné dokončené (např. systematické) tablo z T s $\mathrm{F}\varphi$ v kořeni je nutně sporné, tedy je tablo důkazem.

Sporem: Není-li sporné, má bezespornou (dokončenou) větev V, a dle Lemmatu se s ní kanonický model pro V shoduje.

Protože je V dokončená, obsahuje $\mathrm{T}\alpha$ pro všechny axiomy T. Model v tedy splňuje všechny axiomy a máme $v \models T$.

Protože se ale v shoduje i s položkou $\mathrm{F}\varphi$ v kořeni, máme $v \not\models \varphi$, což dává protipříklad, a máme $T \not\models \varphi$, spor. $\square$

Dokázali jsme i Důsledek o systematičnosti důkazů: Z důkazu vidíme, že i systematické tablo pro položku $\mathrm{F}\varphi$ je nutně sporné, a je tedy tablo důkazem. $\square$

4.6 Důsledky korektnosti a úplnosti

$\vdash = \models$

Syntaktickou analogií důsledků jsou teorémy:

$$\mathrm{Thm}_{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid T \vdash \varphi\}$$

Z korektnosti a úplnosti okamžitě dostáváme:

- $T \vdash \varphi$ právě když $T \models \varphi$
- $\mathrm{Thm}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(T)$

Všude můžeme nahradit ‘platnost’ pojmem ‘dokazatelnost’. Např:

- T je sporná, je-li v ní dokazatelný spor (tj. $T \vdash \bot$)
- T je kompletní, je-li pro každý výrok buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$, ale ne obojí (jinak by byla sporná)

Věta (O dedukci): $T, \varphi \vdash \psi$ právě když $T \vdash \varphi \to \psi$.

Důkaz: Stačí dokázat: $T, \varphi \models \psi \Leftrightarrow T \models \varphi \to \psi$. To je snadné. $\square$