

Výroková a predikátová logika - I

Petr Gregor

KTIML MFF UK

ZS 2021/22

K čemu je logika?

Pro **matematiky**: *“matematika o matematice”*.

Pro **informatiky**:

- formální specifikace (viz spor EU vs. Microsoft),
- testování software i hardware (formální verifikace, model checking),
- deklarativní programování (např. Prolog),
- složitost (Booleovské funkce, obvody, rozhodovací stromy),
- vyčíslitelnost (nerozhodnutelnost, věty o neúplnosti),
- umělá inteligence (automatické odvozování, rezoluce),
- univerzální nástroje: SAT a SMT řešiče (SAT modulo theory),
- návrh databází (konečné relační struktury, Datalog), ...

Koncepce přednášky

- **klasická logika**

- + výroková logika (nejprve samostatně)
- + predikátová logika
- + teorie modelů, nerozhodnutelnost, neúplnost

- **logika pro informatiky**

- + tablo metoda namísto Hilbertovského kalkulu
- + dokazování jako forma výpočtu (systematické hledání protipříkladu)
- + rezoluce v predikátové logice, unifikace, “pozadí” Prologu
- + důraz na algoritmické otázky
- + omezení na spočetné jazyky

Doporučená literatura

• Knihy

- ▶ A. Nerode, R. A. Shore, *Logic for Applications*, Springer, 2nd edition, 1997.
- ▶ P. Pudlák, *Logical Foundations of Mathematics and Computational Complexity - A Gentle Introduction*, Springer, 2013.
- ▶ V. Švejdar, *Logika, neúplnost, složitost a nutnost*, Academia, Praha, 2002.
- ▶ A. Sochor, *Klasická matematická logika*, UK v Praze - Karolinum, 2001.
- ▶ W. Hodges, *Shorter Model Theory*, Cambridge University Press, 1997.
- ▶ W. Rautenberg, *A concise introduction to mathematical logic*, Springer, 2009.

• Elektronické zdroje

- ▶ J. Miček, *Výroková a predikátová logika*, skripta k přednášce, 2012. [[www](#)]
- ▶ P. Štěpánek, *Meze formální metody*, skripta k přednášce, 2000. [[pdf](#)]
- ▶ M. Pilát, *Propositional and Predicate Logic*, lecture notes, 2017. [[pdf](#)]
- ▶ slidy k přednášce

Trocha historie

- **Aristotelés** (384-322 př.n.l.) - **sylogismy**, např.
z *‘žádný Q není R ’* a *‘každý P je Q ’* odvod *‘žádný P není R ’*.
- **Eukleidés: Základy** (asi 330 př.n.l.) - **axiomatický** přístup ke geometrii
*“Pro každou přímku p a bod x , který neleží na p , existuje
přímka skrze x neprotínající p .”* (5. postulát)
- **Descartes: Geometrie** (1637) - **algebraizace** geometrie
- **Leibniz** - sen o *“lingua characteristica”* a *“calculus ratiocinator”* (1679-90)
- **De Morgan** - zavedení **logických spojek** (1847)
$$\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$$
$$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$$
- **Boole** - výrok jako binární funkce, **algebraizace** logiky (1847)
- **Schröder** - sémantika predikátové logiky, koncept **modelu** (1890-1905)

Trocha historie - teorie množin

- **Cantor** - intuitivní **teorie množin** (1878), např. **princip zahrnutí**
“Pro každou vlastnost $\varphi(x)$ existuje množina $\{x \mid \varphi(x)\}$.”
- **Frege** - logika s **kvantifikátory** a **predikáty**, pojem důkazu jako **odvození**,
axiomatická teorie množin (1879, 1884)
- **Russel** - Fregeho teorie množin je **sporná** (1903)

Pro $a = \{x \mid \neg(x \in x)\}$ je $a \in a$?

- **Russel, Whitehead** - teorie typů (1910-13)
- **Zermelo** (1908), **Fraenkel** (1922) - *standardní* teorie množin **ZFC**, např.
“Pro každou vlastnost $\varphi(x)$ a množinu y existuje množina $\{x \in y \mid \varphi(x)\}$.”
- **Bernays** (1937), **Gödel** (1940) - teorie množin založená na **třídách**, např.
“Pro každou množinovou vlastnost $\varphi(x)$ existuje třída $\{x \mid \varphi(x)\}$.”

Trocha historie - algoritmizace

- Hilbert - **kompletní** axiomatizace Euklidovské geometrie (1899),
formalismus - striktní odproštění se od významu, mechaničnost
“... musí být možné místo o bodu, přímce a rovině mluvit
o stole, židli a pultu.” (Grundlagen der Geometrie)
- Brouwer - **intuicionismus**, důraz na **konstruktivní** důkazy
“Matematické tvrzení je myšlenková konstrukce ověřitelná intuicí.”
- Post - **úplnost** výrokové logiky (1921)
- Gödel - **úplnost** predikátové logiky (1930), věty o **neúplnosti** (1931)
- Kleene, Post, Church, Turing - formalizace pojmu **algoritmus**,
existence algoritmicky **nerozhodnutelných** problémů (1936)
- Robinson - **rezoluční** metoda (1965)
- Kowalski; Colmerauer, Roussel - **Prolog** (1972)

Jazyk matematiky

Logika formalizuje pojem **důkazu** a **pravdivosti** matematických tvrzení.

Lze ji postupně rozčlenit dle prostředků jazyka.

- **logické spojky**

výroková logika

Umožňují vytvářet složená tvrzení ze základních.

- **proměnné pro individua, funkční a relační symboly, kvantifikátory** *1. řádu*

Tvrzení o individuích, jejich vlastnostech a vztazích. Teorii množin, která je “světem” (téměř) celé matematiky, lze popsat jazykem 1. řádu.

V jazyce vyšších řádů máme navíc

- **proměnné pro množiny individuí (i relace a funkce)**

logika 2. řádu

- **proměnné pro množiny množin individuí, atd.**

logika 3. řádu

- ...

Příklady tvrzení v jazycích různých řádů

- “Nebude-li pršet, nezmoknem. A když bude pršet, zmokneme, na sluníčku zase uschneme.”

výrok

$$(\neg p \rightarrow \neg z) \wedge (p \rightarrow (z \wedge u))$$

- “Existuje nejmenší prvek.”

1. řádu

$$\exists x \forall y (x \leq y)$$

- Axiom indukce.

2. řádu

$$\forall X ((X(0) \wedge \forall x (X(x) \rightarrow X(x+1))) \rightarrow \forall x X(x))$$

- “Libovolné sjednocení otevřených množin je otevřená množina.”

3. řádu

$$\forall \mathcal{X} \forall Y ((\forall X (\mathcal{X}(X) \rightarrow \mathcal{O}(X)) \wedge \forall x (Y(x) \leftrightarrow \exists X (\mathcal{X}(X) \wedge X(x)))) \rightarrow \mathcal{O}(Y))$$

Syntax a sémantika

Budeme studovat vztahy mezi syntaxí a sémantikou:

- *syntax*: symboly, pravidla vytváření termů a formulí, odvozovací pravidla, dokazovací systém, důkaz, dokazatelnost,
- *sémantika*: přiřazení významu, struktury, modely, splnitelnost, pravdivost.

V logice zavedeme pojem *důkazu* jako přesný syntaktický koncept.

Formální dokazovací systém je

- *korektní*, pokud každé dokazatelné tvrzení je pravdivé,
- *úplný*, pokud každé pravdivé tvrzení je dokazatelné.

Uvidíme, že predikátová logika (1. řádu) má dokazovací systémy, které jsou korektní a zároveň úplné. Pro logiky vyšších řádů to neplatí.

Paradoxy

“Paradoxy” jsou inspirací k přesnému zadefinování základů logiky.

- *paradox krétana*

Krétan řekl: “Všichni krétané jsou lháři.”

- *paradox holiče*

V městě žije holič, jenž holí všechny, kteří se neholí sami.

Holí sám sebe?

- *paradox lháře*

Tato věta je lživá.

- *Berryho paradox*

Výraz “nejmenší přirozené číslo, které nelze definovat méně než jedenácti slovy” ho definuje pomocí deseti slov.

Výroková a predikátová logika - II

Petr Gregor

KTIML MFF UK

ZS 2021/22

Jazyk

Výroková logika je “*logikou spojek*”. Vycházíme z (neprázdnej) množiny $\mathbb{P}$ *výrokových proměnných* (*prvovýroků*). Např.

$$\mathbb{P} = \{p, p_1, p_2, \dots, q, q_1, q_2, \dots\}$$

Obvykle budeme předpokládat, že $\mathbb{P}$ je spočetná.

Jazyk výrokové logiky (nad $\mathbb{P}$) obsahuje *symbols*

- výrokové proměnné z $\mathbb{P}$
- logické spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- závorky $(,)$

Jazyk je tedy určen množinou $\mathbb{P}$. Říkáme, že logické spojky a závorky jsou *logické symbols*, zatímco výrokové proměnné jsou *mimologické symbols*.

Budeme používat i *konstantní* symbols $\top$ (pravda), $\perp$ (spor), jež zavedeme jako *zkratky* za $p \vee \neg p$, resp. $p \wedge \neg p$, kde p je pevný prvovýrok z $\mathbb{P}$.

Formule

Výrokové formule (**výroky**) (nad $\mathbb{P}$) jsou dány indukčním předpisem

- (i) každá výroková proměnná z $\mathbb{P}$ je výrokovou formulí,
- (ii) jsou-li φ, ψ výrokové formule, pak rovněž

$$(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi)$$

jsou výrokové formule,

- (iii) každá výroková formule vznikne **konečným** užitím pravidel (i), (ii).

- Výrokové formule jsou tedy (dobře vytvořené) **konečné posloupnosti** symbolů jazyka (**řetězce**).
- Výrokovou formuli, která je součástí jiné výrokové formule φ nazveme **podformulí** (**podvýrokem**) φ .
- Množinu všech výrokových formulí nad $\mathbb{P}$ značíme **$\mathbf{VF}_{\mathbb{P}}$** .
- Množinu všech výrokových proměnných s výskytem ve φ značíme **$\mathbf{var}(\varphi)$** .

Konvence zápisu

Zavedení (obvyklých) *priorit* logických spojek umožňuje v **zkráceném zápisu** vypouštět závorky okolo podvýroku vzniklého spojkou s **vyšší** prioritou.

(1) $\rightarrow, \leftrightarrow$

(2) $\wedge, \vee$

(3) $\neg$

Rovněž vnější závorky můžeme vynechat. Např.

$((\neg p) \wedge q) \rightarrow (\neg(p \vee (\neg q)))$ lze zkrátit na $\neg p \wedge q \rightarrow \neg(p \vee \neg q)$

Poznámka Nerespektováním priorit může vzniknout **nejednoznačný** zápis nebo dokonce jednoznačný zápis **neekvivalentní** formule.

Další možnosti zjednodušení zápisu vyplývají ze sémantických vlastností spojek (**asociativita** $\vee, \wedge$).

Vytvořující strom

Vytvořující strom je konečný **uspořádaný strom**, jehož vrcholy jsou označeny výroky dle následujících pravidel

- listy (a jen listy) jsou označeny prvovýroky,
- je-li vrchol označen $(\neg\varphi)$, má jediného syna označeného φ ,
- je-li vrchol označen $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ nebo $(\varphi \leftrightarrow \psi)$, má dva syny, přičemž **levý** syn je označen φ a **pravý** je označen ψ .

Vytvořující strom výroku φ je vytvořující strom s kořenem označeným φ .

Tvrzení Každý výrok má jednoznačně určený vytvořující strom.

Důkaz Snadno indukci dle počtu vnoření závorek (odpovídající hloubce vytvořujícího stromu). $\square$

Poznámka Takovéto důkazy nazýváme důkazy indukci **dle struktury formule**.

Sémantika

- Uvažujeme pouze **dvouhodnotovou** logiku.
- Prvovýroky reprezentují atomická tvrzení, jejich význam je určen přiřazením **pravdivostní hodnoty** 0 (*nepravda*) nebo 1 (*pravda*).
- Sémantika logických spojek je dána jejich **pravdivostními tabulkami**.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Ty **jednoznačně** určují hodnotu každého výroku z hodnot prvovýroků.

- K výrokům tedy můžeme také přiřadit "**pravdivostní tabulky**". Říkáme, že **reprezentují** Booleovské funkce (až na určení pořadí proměnných).
- Booleovská funkce** je n -ární operace na $\{0, 1\}$, tj. $f: \{0, 1\}^n \rightarrow \{0, 1\}$.

Hodnota výroku

- **Ohodnocení** prvovýroků je funkce $v: \mathbb{P} \rightarrow \{0, 1\}$.
- **Hodnota** $\bar{v}(\varphi)$ výroku φ při ohodnocení v je dána induktivně

$$\begin{aligned}
 \bar{v}(p) &= v(p) \text{ jestliže } p \in \mathbb{P} & \bar{v}(\neg\varphi) &= \neg_1(\bar{v}(\varphi)) \\
 \bar{v}(\varphi \wedge \psi) &= \wedge_1(\bar{v}(\varphi), \bar{v}(\psi)) & \bar{v}(\varphi \vee \psi) &= \vee_1(\bar{v}(\varphi), \bar{v}(\psi)) \\
 \bar{v}(\varphi \rightarrow \psi) &= \rightarrow_1(\bar{v}(\varphi), \bar{v}(\psi)) & \bar{v}(\varphi \leftrightarrow \psi) &= \leftrightarrow_1(\bar{v}(\varphi), \bar{v}(\psi))
 \end{aligned}$$

kde $\neg_1, \wedge_1, \vee_1, \rightarrow_1, \leftrightarrow_1$ jsou Booleovské funkce dané tabulkami.

Tvrzení Hodnota výroku φ závisí pouze na ohodnocení $\text{var}(\varphi)$.

Důkaz Snadno indukci dle struktury formule. $\square$

Poznámka Jelikož funkce $\bar{v}: \text{VF}_{\mathbb{P}} \rightarrow \{0, 1\}$ je jednoznačnou **extenzí** funkce v , můžeme psát v místo $\bar{v}$ aniž by došlo k nedorozumění.

Sémantické pojmy

Výrok φ nad $\mathbb{P}$ je

- **splněn** (*platí*) **při ohodnocení** $v: \mathbb{P} \rightarrow \{0, 1\}$, pokud $\bar{v}(\varphi) = 1$.
Pak v je **splňující ohodnocení** výroku φ , značíme $v \models \varphi$.
- **pravdivý** ((logicky) **platí, tautologie**), pokud $\bar{v}(\varphi) = 1$ pro každé $v: \mathbb{P} \rightarrow \{0, 1\}$, tj. φ je splněn při každém ohodnocení, značíme $\models \varphi$.
- **lživý** (*sporný*), pokud $\bar{v}(\varphi) = 0$ pro každé $v: \mathbb{P} \rightarrow \{0, 1\}$, tj. $\neg\varphi$ je pravdivý.
- **nezávislý**, pokud $\bar{v}_1(\varphi) = 0$ a $\bar{v}_2(\varphi) = 1$ pro nějaká $v_1, v_2: \mathbb{P} \rightarrow \{0, 1\}$, tj. φ není ani pravdivý ani lživý.
- **splnitelný**, pokud $\bar{v}(\varphi) = 1$ pro nějaké $v: \mathbb{P} \rightarrow \{0, 1\}$, tj. φ není lživý.

Výroky φ a ψ jsou (logicky) **ekvivalentní**, psáno $\varphi \sim \psi$, pokud $\bar{v}(\varphi) = \bar{v}(\psi)$ pro každé $v: \mathbb{P} \rightarrow \{0, 1\}$, tj. výrok $\varphi \leftrightarrow \psi$ je pravdivý.

Modely

Předchozí definice ekvivalentně přeformulujeme v terminologii modelů.

Model jazyka $\mathbb{P}$ je ohodnocení $v: \mathbb{P} \rightarrow \{0, 1\}$. Třída všech modelů jazyka $\mathbb{P}$ se značí $M(\mathbb{P})$, tedy $M(\mathbb{P}) = \{v \mid v: \mathbb{P} \rightarrow \{0, 1\}\} = \mathbb{P}^2$. Výrok φ nad $\mathbb{P}$ (je)

- **platí v modelu** $v \in M(\mathbb{P})$, pokud $\bar{v}(\varphi) = 1$. Pak v je **model výroku** φ , značíme $v \models \varphi$ a $M^{\mathbb{P}}(\varphi) = \{v \in M(\mathbb{P}) \mid v \models \varphi\}$ je **třída modelů** φ .
- **pravdivý** ((logicky) **platí, tautologie**), pokud platí v každém modelu (jazyka), značíme $\models \varphi$.
- **lživý** (**sporný**), pokud nemá model.
- **nezávislý**, pokud platí v nějakém modelu a neplatí v jiném.
- **splnitelný**, pokud má model.

Výroky φ a ψ jsou (logicky) **ekvivalentní**, psáno $\varphi \sim \psi$, pokud mají stejné modely.

Univerzálnost spojek

Jazyk výrokové logiky obsahuje *základní* spojky $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

Můžeme zavést obecně n -ární spojku pro libovolnou Booleovu funkci. Např.

$p \downarrow q$ “*ani p ani q* ” (NOR, Peirceova spojka)

$p \uparrow q$ “*ne (p a q)*” (NAND, Shefferova spojka)

Množina spojek je *univerzální*, pokud lze každou Booleovskou funkci reprezentovat nějakým z nich (dobře) vytvořeným výrokem.

Tvrzení $\{\neg, \wedge, \vee\}$ je univerzální.

Důkaz Funkci $f: \{0, 1\}^n \rightarrow \{0, 1\}$ reprezentuje výrok $\bigvee_{v \in f^{-1}[1]} \bigwedge_{i=1}^n p_i^{v_i}$, kde $p_i^{v_i}$ značí prvovýrok p_i pokud $v_i = 1$, jinak výrok $\neg p_i$. Pro $f^{-1}[1] = \emptyset$ zvolíme výrok $\perp$. $\square$

Tvrzení $\{\neg, \rightarrow\}$ je univerzální.

Důkaz $(p \wedge q) \sim \neg(p \rightarrow \neg q)$, $(p \vee q) \sim (\neg p \rightarrow q)$. $\square$

CNF a DNF

- **Literál** je prvvýrok nebo jeho negace. Je-li p prvvýrok, označme p^0 literál $\neg p$ a p^1 literál p . Je-li l literál, označme $\bar{l}$ literál **opačný** k l .
- **Klauzule** je disjunkce literálů, **prázdnou klauzulí** rozumíme $\perp$.
- Výrok je v **konjunktivně normálním tvaru (CNF)**, je-li konjunkcí klauzulí. **Prázdným výrokem v CNF** rozumíme $\top$.
- **Elementární konjunkce** je konjunkce literálů, **prázdnou konjunkcí** je $\top$.
- Výrok je v **disjunktivně normálním tvaru (DNF)**, je-li disjunkcí elementárních konjunktí. **Prázdným výrokem v DNF** rozumíme $\perp$.

Poznámka Klauzule nebo elementární konjunkce je zároveň v CNF i DNF.

Pozorování Výrok v CNF je pravdivý, právě když každá jeho klauzule obsahuje dvojici opačných literálů. Výrok v DNF je splnitelný, právě když aspoň jedna jeho elementární konjunkce neobsahuje dvojici opačných literálů.

Převod tabulkou

Tvrzení Necht' $K \subseteq {}^{\mathbb{P}}2$ pro $\mathbb{P}$ konečné. Označme $\overline{K} = {}^{\mathbb{P}}2 \setminus K$. Pak

$$M^{\mathbb{P}}\left(\bigvee_{v \in K} \bigwedge_{p \in \mathbb{P}} p^{v(p)}\right) = K = M^{\mathbb{P}}\left(\bigwedge_{v \in \overline{K}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}}\right)$$

Důkaz První rovnost plyne z $\overline{w}(\bigwedge_{p \in \mathbb{P}} p^{v(p)}) = 1$ právě když $w = v$, kde $w: \mathbb{P} \rightarrow \{0, 1\}$. Druhá obdobně z $\overline{w}(\bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}}) = 1$ právě když $w \neq v$. $\square$

Např. $K = \{(1, 0, 0), (1, 1, 0), (0, 1, 0), (1, 1, 1)\}$ **namodelujeme**

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

Důsledek Každý výrok je ekvivalentní nějakému výroku v CNF/DNF.

Důkaz Hodnota výroku φ závisí pouze na ohodnocení jeho proměnných, kterých je konečně. Lze tedy použít tvrzení pro $K = M^{\mathbb{P}}(\varphi)$ a $\mathbb{P} = \text{var}(\varphi)$. $\square$

Převod úpravami

Tvrzení *Nechť φ' je výrok vzniklý z výroku φ nahrazením některých výskytů podvýroku ψ za výrok ψ' . Jestliže $\psi \sim \psi'$, pak $\varphi \sim \varphi'$.*

Důkaz Snadno indukcí dle struktury formule. $\square$

$$(1) (\varphi \rightarrow \psi) \sim (\neg\varphi \vee \psi), \quad (\varphi \leftrightarrow \psi) \sim ((\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi))$$

$$(2) \neg\neg\varphi \sim \varphi, \quad \neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi), \quad \neg(\varphi \vee \psi) \sim (\neg\varphi \wedge \neg\psi)$$

$$(3) (\varphi \vee (\psi \wedge \chi)) \sim ((\psi \wedge \chi) \vee \varphi) \sim ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$$

$$(3)' (\varphi \wedge (\psi \vee \chi)) \sim ((\psi \vee \chi) \wedge \varphi) \sim ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$$

Tvrzení *Každý výrok lze pomocí (1), (2), (3)/(3)' převést na CNF / DNF.*

Důkaz Snadno indukcí dle struktury formule. $\square$

Tvrzení *Nechť výrok φ obsahuje pouze spojky $\neg, \wedge, \vee$. Pak pro výrok φ^* vzniklý z φ záměnou $\wedge$ a $\vee$ a znegováním všech literálů platí $\neg\varphi \sim \varphi^*$.*

Důkaz Snadno indukcí dle struktury formule. $\square$

Problém splnitelnosti a řešiče

- Problém **SAT**: Je daná výroková formule splnitelná?
- *Příklad Lze šachovnici bez dvou protilehlých rohů perfektně pokrýt kostkami domina?*

Snadno vytvoříme výrokovou formuli, která je **splnitelná**, právě když to lze. Pak ji můžeme zkusit ověřit pomocí nějakého SAT řešiče.

- Nejlepší řešiče pro SAT: www.satcompetition.org.
- Řešič v ukázce: [Glucose](#), formát pro CNF soubory: [DIMACS](#).
- Obecnější otázka: *Lze celou matematiku převést do logických formulí?*
AI, strojové dokazování, [Peano: Formulario](#) (1895-1908), [Mizar system](#)
- *Proč to lidé (většinou) nedělají?*
Jak vyřešíme uvedený příklad *elegantněji*? V čem náš postup spočívá?

2-SAT

- Výrok je v ***k*-CNF**, je-li v CNF a každá jeho klauzule má **nejvýše** k literálů.
- ***k*-SAT** je následující problém (pro pevné $k > 0$)

INSTANCE: Výrok φ v k -CNF.

OTÁZKA: Je φ splnitelný?

Zatímco už pro $k = 3$ jde o **NP-úplný** problém, ukážeme, že 2-SAT lze řešit v **lineárním** čase (vzhledem k délce φ).

Vynecháme implementační detaily (výpočetní model, reprezentace v paměti) a využijeme následující znalosti, viz [ADS I].

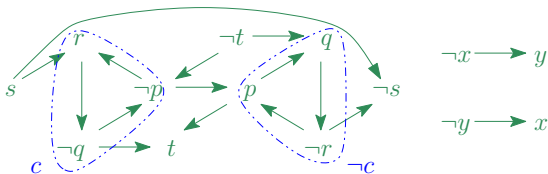
Tvrzení Rozklad orientovaného grafu (V, E) na silně souvislé komponenty lze nalézt v čase $\mathcal{O}(|V| + |E|)$.

- Orientovaný graf G je **silně souvislý**, pokud pro každé dva vrcholy u a v existují v G orientované cesty jak z u do v , tak i z v do u .
- Silně souvislá **komponenta** grafu G je **maximální** silně souvislý podgraf G .

Implikační graf

Implikační graf výroku φ v 2-CNF je orientovaný graf G_φ , v němž

- vrcholy jsou proměnné výroku φ nebo jejich negace,
- klauzuli $l_1 \vee l_2$ výroku φ reprezentujeme dvojicí hran $\overline{l_1} \rightarrow l_2$, $\overline{l_2} \rightarrow l_1$,
- klauzuli l_1 výroku φ reprezentujeme hranou $\overline{l_1} \rightarrow l_1$.



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

Tvrzení φ je splnitelný, právě když žádná silně souvislá komponenta v G_φ neobsahuje dvojici opačných literálů.

Důkaz Každé splňující ohodnocení ohodnotí všechny literály ze stejné komponenty stejně. Implikace zleva doprava tedy platí.

Nalezení ohodnocení

Naopak, označme G_φ^* graf vzniklý z G_φ **kontrakcí** silně souvislých komponent.

Pozorování G_φ^* je *acyklický*, má tedy *topologické uspořádání* $<$.

- Orientovaný graf je *acyklický*, neobsahuje-li orientovaný *cyklus*.
- Lineární uspořádání $<$ vrcholů orientovaného grafu je *topologické*, pokud $p < q$ pro každou hranu z p do q .

Nyní pro každou komponentu v rostoucím pořadí dle $<$, nejsou-li její literály dosud ohodnocené, nastav je na 0 a literály v opačné komponentě na 1.

Zbývá ukázat, že takto získané ohodnocení v splňuje φ . Kdyby ne, existovaly by v G_φ^* hrany $p \rightarrow q$ a $\bar{q} \rightarrow \bar{p}$ s $v(p) = 1$ a $v(q) = 0$. To je ve sporu s pořadím nastavení komponent na 0 resp. 1, neboť $p < q$ a $\bar{q} < \bar{p}$. $\square$

Důsledek 2-SAT je řešitelný v lineárním čase.

Horn-SAT

- **Jednotková klauzule** je klauzule obsahující jediný literál,
- **Hornova klauzule** je klauzule obsahující **nejvýše** jeden pozitivní literál,

$$\neg p_1 \vee \dots \vee \neg p_n \vee q \quad \sim \quad (p_1 \wedge \dots \wedge p_n) \rightarrow q$$

- **Hornův výrok** je konjunkcí Hornových klauzulí,
- **Horn-SAT** je problém splnitelnosti daného Hornova výroku.

Algoritmus

- (1) *obsahuje-li φ dvojici jednotkových klauzulí l a $\bar{l}$, není splnitelný,*
- (2) *obsahuje-li φ 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 φ jednotkovou klauzuli, je splnitelný ohodnocením 0 všech zbývajících proměnných.*

Krok (2) se nazývá **jednotková propagace**.

Jednotková propagace

$$\begin{array}{ll}
 (\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg r \vee \neg s) \wedge (\neg t \vee s) \wedge s & v(s) = 1 \\
 (\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge \neg r & v(\neg r) = 1 \\
 (\neg p \vee q) \wedge (\neg p \vee \neg q) & v(p) = v(q) = v(t) = 0
 \end{array}$$

Pozorování Necht' φ^l je výrok získaný z φ *jednotkovou propagací*. Pak φ^l je splnitelný, právě když φ 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 zbývajících klauzule obsahuje negativní literál.

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

Výroková a predikátová logika - III

Petr Gregor

KTIML MFF UK

ZS 2021/22

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 .
- **Model teorie** T nad $\mathbb{P}$ je ohodnocení $\nu \in M(\mathbb{P})$ (tj. model jazyka), ve kterém platí všechny axiomy z T , značíme $\nu \models T$.
- **Třída modelů** T je $M^{\mathbb{P}}(T) = \{\nu \in M(\mathbb{P}) \mid \nu \models \varphi \text{ pro každé } \varphi \in T\}$.

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.

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

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

- (1) $T \subseteq \theta^{\mathbb{P}}(T) = \theta^{\mathbb{P}}(\theta^{\mathbb{P}}(T))$,
- (2) $T \subseteq T' \Rightarrow \theta^{\mathbb{P}}(T) \subseteq \theta^{\mathbb{P}}(T')$,
- (3) $\varphi \in \theta^{\mathbb{P}}(\{\varphi_1, \dots, \varphi_n\}) \Leftrightarrow \models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \varphi$.

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

- (1) $M(\theta(T)) = M(T)$,
- (2) $T \subseteq T' \Rightarrow M(T') \subseteq M(T)$,
- (3) $\models \psi \rightarrow \varphi \Leftrightarrow M(\psi) \subseteq M(\varphi), M(\varphi_1 \wedge \dots \wedge \varphi_n) = M(\varphi_1, \dots, \varphi_n)$. □

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 $\theta^{\mathbb{P}'}(T') = \theta^{\mathbb{P}}(T) \cap \text{VF}_{\mathbb{P}'}$,
- *ekvivalentní* s teorií T' , jestliže T je extenzí T' a T' je extenzí T ,

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

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.

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

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** $\mathcal{P}(M(T))$ 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 $2^{2^n} - 2 \cdot 2^{2^n - m}$,
- 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 $\text{VF}_{\mathbb{P}}/\sim$ 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 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.

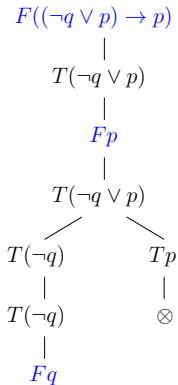
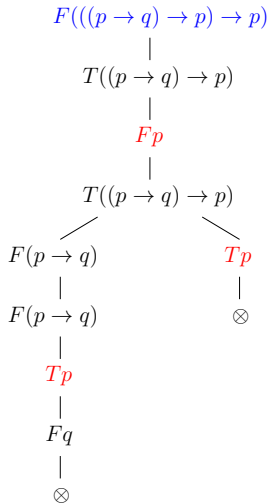
Tablo metoda - úvod

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 značkový 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



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 φ (*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

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

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

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

Tablo

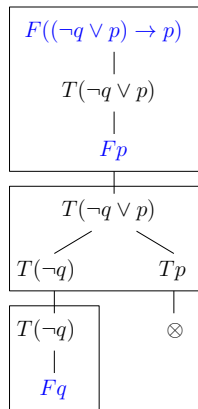
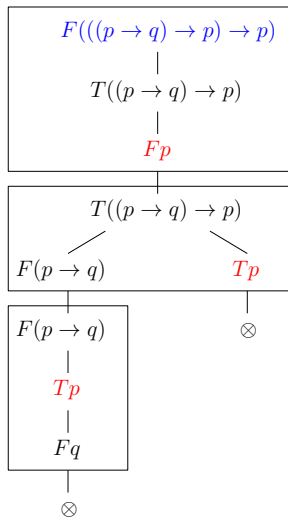
Konečné tablo je binární, položkami značkový strom daný předpisem

- (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).

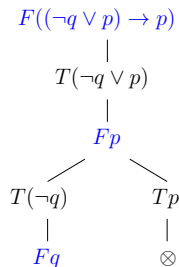
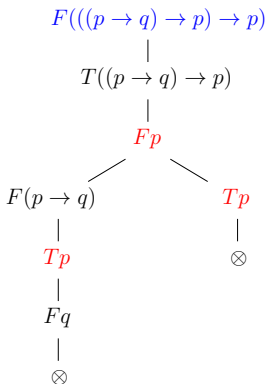
Tablo je posloupnost $\tau_0, \tau_1, \dots, \tau_n, \dots$ (konečná i nekonečná) konečných tabel takových, že τ_{n+1} vznikne z τ_n pomocí pravidla (ii), formálně $\tau = \cup \tau_n$.

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

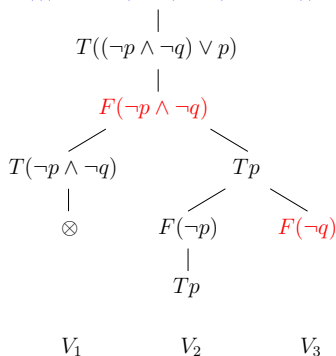
- položka P je *redukována* na V , pokud se na V *vyskytuje* jako kořen atomického tabla, tj. při konstrukci τ již došlo k jejímu rozvoji na V ,
- větev V je *sporná*, obsahuje-li položky $T\varphi$ a $F\varphi$ pro nějakou formuli φ , jinak je *bezesporná*. Větev V je *dokončená*, je-li sporná nebo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

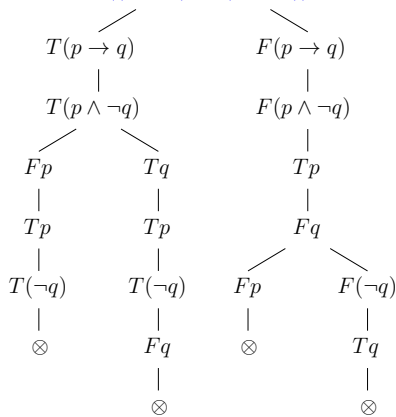
Příklady

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



a)

$$T((p \rightarrow q) \leftrightarrow (p \wedge \neg q))$$



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

Tablo z teorie

Jak do důkazu přidat axiomy dané teorie T ?

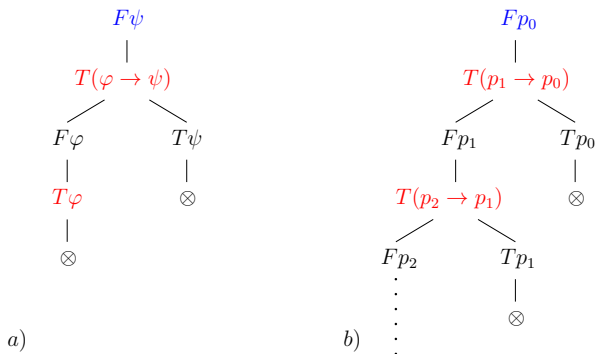
Konečné tablo z teorie T je **zobecnění** konečného tabla přidáním pravidla (ii)' je-li V větev konečného tabla (z T) a $\varphi \in T$, pak připojením $T\varphi$ na konec V vznikne (také) konečné tablo z T .

Přidáním dodatku “z teorie T ” přirozeně zobecníme další pojmy

- **tablo z teorie** T je posloupnost $\tau_0, \tau_1, \dots, \tau_n, \dots$ 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 redukována na V a navíc obsahuje $T\varphi$ pro každé $\varphi \in T$.

Příklady tabla z teorie



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

b) **Dokončené** tablo pro formuli p_0 z teorie $T = \{p_{n+1} \rightarrow p_n \mid n \in \mathbb{N}\}$.

Všechny větve jsou dokončené, nejlevější větev je **bezesporná** a nekonečná. Poskytuje (jediný) model teorie T , ve kterém p_0 neplatí.

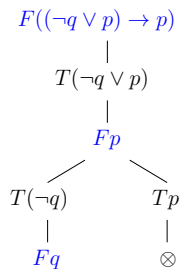
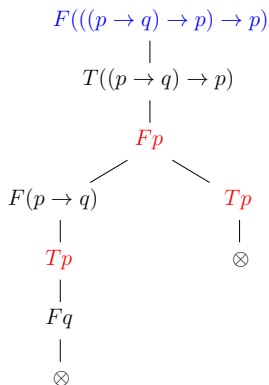
Výroková a predikátová logika - IV

Petr Gregor

KTIML MFF UK

ZS 2021/22

Tablo - příklady



Atomická tabla

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

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

Tablo z teorie

Jak do důkazu přidat axiomy dané teorie?

Konečné tablo z teorie T je binární, položkami značkový 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,
- (ii)' je-li V větev konečného tabla (z T) a $\varphi \in T$, pak připojením $T\varphi$ na konec V vznikne (rovněž) konečné tablo z T .
- (iii) každé konečné tablo vznikne **konečným** užitím pravidel (i), (ii), (ii)'.

Tablo z teorie T je posloupnost $\tau_0, \tau_1, \dots, \tau_n, \dots$ konečných tabel z T takových, že τ_{n+1} vznikne z τ_n pomocí pravidla (ii) či (ii)', formálně $\tau = \cup \tau_n$.

Tablo důkaz z teorie

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

- položka P je **redukována** 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 ,
- větev V je **dokončená**, je-li sporná, nebo je každá její položka redukována na V a **navíc** obsahuje $T\varphi$ pro každé $\varphi \in T$,
- tablo τ je **dokončené**, pokud je každá jeho větev dokončená, a je **sporné**, pokud je každá jeho větev sporná.

Tablo důkaz formule φ **z teorie** T je sporné tablo z T s $F\varphi$ v kořeni,

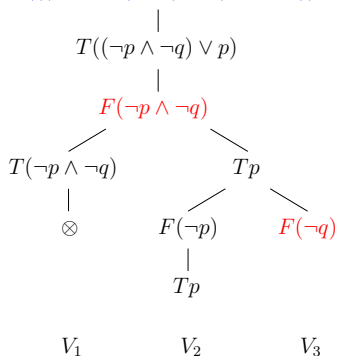
Má-li φ tablo důkaz z T , je **(tablo) dokazatelná z T** , píšeme $T \vdash \varphi$.

Zamítnutí formule φ **tablem z teorie** T je sporné tablo z T s $T\varphi$ v kořeni.

Formule φ je **(tablo) zamítnutelná z T** , má-li zamítnutí tablem z T , tj. $T \vdash \neg\varphi$.

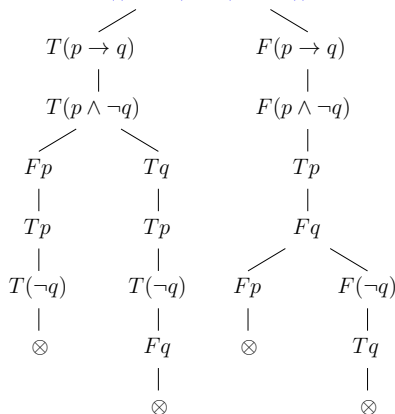
Příklady

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



a)

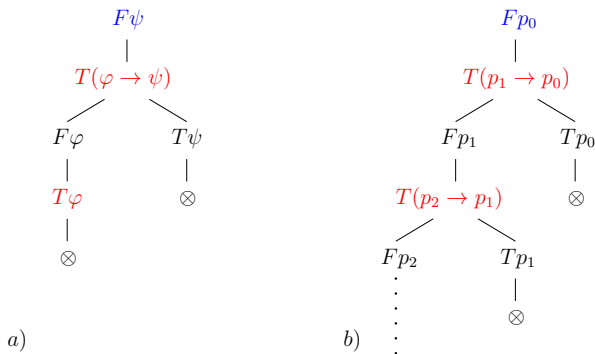
$$T((p \rightarrow q) \leftrightarrow (p \wedge \neg q))$$



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

Příklady tabla z teorie



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

b) **Dokončené** tablo pro formuli p_0 z teorie $T = \{p_{n+1} \rightarrow p_n \mid n \in \mathbb{N}\}$.

Všechny větve jsou dokončené, nejlevější větev je **bezesporná** a nekonečná. Poskytuje (jediný) model teorie T , ve kterém p_0 neplatí.

Systematické tablo

Popíšeme systematickou konstrukci, jež povede vždy k **dokončenému** tablu.

Nechť R je položka a $T = \{\varphi_0, \varphi_1, \dots\}$ je (konečná či nekonečná) teorie.

- (1) Za τ_0 vezmi atomické tablo pro R . Dokud to lze, aplikuj následující kroky.
- (2) Nechť P je **nejlevější** položka v co **nejmenší** úrovni již daného tabla τ_n , která není redukována na nějaké bezesporné větvi procházející **skrze** P .
- (3) Za τ'_n vezmi tablo vzniklé z τ_n přidáním atomického tabla pro P na každou bezespornou větev skrze P . (Neexistuje-li P , vezmi $\tau'_n = \tau_n$.)
- (4) Za τ_{n+1} vezmi tablo vzniklé z τ'_n přidáním $T\varphi_n$ na každou bezespornou větev neobsahující $T\varphi_n$. (Neexistuje-li φ_n , vezmi $\tau_{n+1} = \tau'_n$.)

Systematické tablo z teorie T pro položku R je výsledkem uvedené konstrukce, tj. $\tau = \cup \tau_n$.

Systematické tablo - dokončenost

Tvrzení Pro každou teorii T a položku R je systematické tablo τ **dokončené**.

Důkaz Necht' $\tau = \cup \tau_n$ je systematické tablo z $T = \{\varphi_0, \varphi_1, \dots\}$ s R v kořeni.

- Je-li větev v v τ bezesporná, je i každý její prefix v v τ_n bezesporný.
- Je-li položka P neredukovaná na větvi v v τ , je neredukovaná na každém jejím prefixu v v τ_n (na němž leží).
- Do úrovně každé položky P (včetně její) je v τ jen konečně položek.
- Kdyby P byla neredukovaná na nějaké bezesporné větvi τ , přišla by na ní řada v nějakém kroku (2) a byla by zredukována krokem (3).
- Každá $\varphi_n \in T$ bude dle (4) nejpozději v τ_{n+1} na každé bezesporné větvi.
- Tedy systematické tablo τ obsahuje pouze dokončené větve. $\square$

Konečnost důkazů

Lemma (König) *Každý nekonečný, konečně větvící se strom obsahuje nekonečnou větev.*

Tvrzení *Je-li $\tau = \cup \tau_n$ sporné tablo, je τ_n sporné **konečné** tablo pro nějaké n .*

Důkaz

- Nechť S je množina vrcholů stromu τ , jenž nad sebou neobsahují spor, tj. mezi předky nemají dvojici $T\varphi, F\varphi$ pro žádné φ .
- Kdyby S byla nekonečná, dle **Königova lemmatu** by podstrom τ na vrcholech S obsahoval nekonečnou větev, tedy by τ nebylo sporné tablo.
- Jelikož je S konečné, všechny vrcholy z S leží do úrovně m pro nějaké m .
- Tedy každý vrchol v úrovni $m + 1$ má nad sebou spor. Zvolme n tak, že τ_n se shoduje s τ do úrovně $m + 1$. Pak každá větev v τ_n je sporná. $\square$

Důsledek *Je-li systematické tablo τ důkazem (z teorie T), je τ konečné.*

Důkaz Při jeho konstrukci se prodlužují jen bezesporné větve. $\square$

Korektnost

Řekneme, že položka P se **shoduje** s ohodnocením v , pokud P je $T\varphi$ a $\bar{v}(\varphi) = 1$ nebo pokud P je $F\varphi$ a $\bar{v}(\varphi) = 0$. Větev V tabla se shoduje s v , shoduje-li se s v každá položka na V .

Lemma *Nechť v je model teorie T , který se shoduje s položkou v kořeni tabla $\tau = \cup \tau_n$ z T . Pak v tablu τ existuje větev shodující se s v .*

Důkaz Indukcí nalezneme posloupnost $V_0, V_1, \dots$ takovou, že pro každé n je V_n větev v τ_n shodující se s v a V_n je obsažena ve V_{n+1} .

- Ověřením atomických tabel snadno zjistíme, že základ indukce platí.
- Pokud τ_{n+1} vznikne z τ_n bez prodloužení V_n , položíme $V_{n+1} = V_n$.
- Vznikne-li τ_{n+1} z τ_n připojením $T\varphi$ k V_n pro nějaké $\varphi \in T$, nechť V_{n+1} je tato větev. Jelikož v je model φ , shoduje se V_{n+1} s v .
- Jinak τ_{n+1} vznikne z τ_n prodloužením V_n o atomické tablo nějaké položky P na V_n . Jelikož se P shoduje s v a tvrzení platí pro atomická tabla, lze požadovanou větev V_{n+1} v τ_{n+1} nalézt. $\square$

Věta o korektnosti

Ukážeme, že tablo metoda ve výrokové logice je *korektní*.

Věta Pro každou teorii T a formuli φ , je-li φ tablo dokazatelná z T , je φ pravdivá v T , tj. $T \vdash \varphi \Rightarrow T \models \varphi$.

Důkaz

- Necht' φ je tablo dokazatelná z teorie T , tj. existuje sporné tablo τ s položkou $F\varphi$ v kořeni.
- Pro spor předpokládejme, že φ není pravdivá v T , tj. existuje model v teorie T , ve kterém φ neplatí (*protipříklad*).
- Jelikož se položka $F\varphi$ shoduje s v , dle předchozího lemmatu v tablu τ existuje větev shodující se s v .
- To ale není možné, neboť každá větev tabla τ je sporná, tj. obsahuje dvojici $T\psi, F\psi$ pro nějaké ψ . $\square$

Úplnost

Ukážeme, že bezesporná větev v dokončeném tablu poskytuje *protipříklad*.

Lemma Nechť V je *bezesporná* větev *dokončeného* tablu τ . Pro následující ohodnocení v výrokových proměnných platí, že V se *shoduje* s v .

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

Důkaz Indukcí dle struktury formule v položce vyskytující se na V .

- Je-li položka Tp na V , kde p je prvovýrok, je $\bar{v}(p) = 1$ dle definice v .
- Je-li položka Fp na V , není Tp na V , jinak by V byla sporná, tedy $\bar{v}(p) = 0$ dle definice v .
- Je-li $T(\varphi \wedge \psi)$ na V , je $T\varphi$ a $T\psi$ na V , neboť τ je dokončené. Dle indukčního předpokladu je $\bar{v}(\varphi) = \bar{v}(\psi) = 1$, tedy $\bar{v}(\varphi \wedge \psi) = 1$.
- Je-li $F(\varphi \wedge \psi)$ na V , je $F\varphi$ nebo $F\psi$ na V , neboť τ je dokončené. Dle indukčního předpokladu je $\bar{v}(\varphi) = 0$ nebo $\bar{v}(\psi) = 0$, tedy $\bar{v}(\varphi \wedge \psi) = 0$.
- Pro ostatní spojky obdobně jako v předchozích dvou případech. □

Věta o úplnosti

Ukážeme, že tablo metoda ve výrokové logice je i **úplná**.

Věta Pro každou teorii T a formuli φ , je-li φ pravdivá v T , je φ tablo dokazatelná z T , tj. $T \models \varphi \Rightarrow T \vdash \varphi$.

Důkaz Nechť φ je pravdivá v T . Ukážeme, že libovolné **dokončené** tablo (např. **systematické**) τ z teorie T s položkou $F\varphi$ v kořeni je **sporné**.

- Kdyby ne, nechť V je nějaká bezesporná větev tabla τ .
- Dle předchozího lemmatu existuje ohodnocení v prvvýroků takové, že V se shoduje s v , speciálně s $F\varphi$, tj. $\bar{v}(\varphi) = 0$.
- Jelikož větev V je dokončená, obsahuje $T\psi$ pro každé $\psi \in T$.
- Tedy v je modelem teorie T (neboť větev V se shoduje s v).
- To je ale ve sporu s tím, že φ platí v každém modelu teorie T .

Tedy tablo τ je důkazem φ z T . $\square$

Vlastnosti teorií

Zavedeme syntaktické varianty již definovaných sémantických pojmů.

Nechť T je teorie nad $\mathbb{P}$. Je-li φ dokazatelná z T , řekneme, že φ je **věta** (*teorém*) teorie T . Množinu vět teorie T označme

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

Řekneme, že teorie T je

- **sporná**, jestliže je v T dokazatelný $\perp$ (spor), jinak je **bezesporná**,
- **kompletní**, jestliže není sporná a každá formule je v ní dokazatelná či zamítnutelná, tj. $T \vdash \varphi$ či $T \vdash \neg\varphi$ pro každé $\varphi \in \text{VF}_{\mathbb{P}}$,
- **extenze** teorie T' nad $\mathbb{P}'$, jestliže $\mathbb{P}' \subseteq \mathbb{P}$ a $\text{Thm}^{\mathbb{P}'}(T') \subseteq \text{Thm}^{\mathbb{P}}(T)$, o extenzi T teorie T' řekneme, že je **jednoduchá**, pokud $\mathbb{P} = \mathbb{P}'$, a **konzervativní**, pokud $\text{Thm}^{\mathbb{P}'}(T') = \text{Thm}^{\mathbb{P}}(T) \cap \text{VF}_{\mathbb{P}'}$,
- **ekvivalentní** s teorií T' , jestliže T je extenzí T' a T' je extenzí T .

Důsledky

Z korektnosti a úplnosti tablo metody vyplývá, že předchozí pojmy se shodují se svými sémantickými variantami.

Důsledek Pro každou teorii T a formule φ, ψ nad $\mathbb{P}$,

- $T \vdash \varphi$ právě když $T \models \varphi$,
- $\text{Thm}^{\mathbb{P}}(T) = \theta^{\mathbb{P}}(T)$,
- T je sporná, právě když není splnitelná, tj. nemá model,
- T je kompletní, právě když je sémanticky kompletní, tj. má právě jeden model,
- $T, \varphi \vdash \psi$ právě když $T \vdash \varphi \rightarrow \psi$ (Věta o dedukci).

Poznámka Větu o dedukci lze dokázat přímo, transformací příslušných tabel.

Věta o kompaktnosti

Věta *Teorie má model, právě když každá její **konečná** část má model.*

Důkaz 1 Implikace zleva doprava je zřejmá. Pokud teorie T nemá model, je sporná, tj. je z ní dokazatelný $\perp$ systematickým tablem τ . Jelikož je τ konečné, je $\perp$ dokazatelný z nějaké konečné $T' \subseteq T$, tj. T' nemá model. $\square$

Poznámka *Tento důkaz je založen na konečnosti důkazu, korektnosti a úplnosti. Uved'me ještě druhý, přímý důkaz (pomocí **Königova lemmatu**).*

Důkaz 2 Nechť $T = \{\varphi_i \mid i \in \mathbb{N}\}$. Uvažme strom S na konečných binárních posloupnostech σ uspořádaných prodloužením. Přičemž $\sigma \in S$, právě když existuje ohodnocení v **prodlužující** σ takové, že $v \models \varphi_i$ pro každé $i \leq \text{lth}(\sigma)$.

Pozorování *S má nekonečnou větev, právě když T má model.*

Jelikož $\{\varphi_i \mid i \in n\} \subseteq T$ má model pro každé $n \in \mathbb{N}$, bude každá úroveň v S neprázdná. Tedy S je nekonečný, navíc binární, a dle Königova lemmatu obsahuje nekonečnou větev. $\square$

Aplikace kompaktnosti

Graf (V, E) je ***k-obarvitelný***, pokud existuje $c: V \rightarrow \{1, \dots, k\}$ takové, že $c(u) \neq c(v)$ pro každou hranu $\{u, v\} \in E$.

Věta *Spočetně nekonečný graf $G = (V, E)$ je k -obarvitelný, právě když každý jeho konečný podgraf je k -obarvitelný.*

Důkaz Implikace zleva doprava je zřejmá. Nechť každý konečný podgraf v G je k -obarvitelný. Vezměme $\mathbb{P} = \{p_{u,i} \mid u \in V, 1 \leq i \leq k\}$ a teorii T s axiomy

$$\begin{array}{ll} p_{u,1} \vee \dots \vee p_{u,k} & \text{pro všechna } u \in V, \\ \neg(p_{u,i} \wedge p_{u,j}) & \text{pro všechna } u \in V, 1 \leq i < j \leq k, \\ \neg(p_{u,i} \wedge p_{v,i}) & \text{pro všechna } \{u, v\} \in E, 1 \leq i \leq k. \end{array}$$

Platí, že G je k -obarvitelný, právě když T má model. Dle věty o kompaktnosti stačí dokázat, že každá konečná $T' \subseteq T$ má model. Nechť G' je podgraf na vrcholech u takových, že $p_{u,i}$ se vyskytuje v T' pro nějaké i . Jelikož G' je k -obarvitelný dle předpokladu, má T' model. $\square$

Hilbertovský kalkul

- základní logické spojky: $\neg$, $\rightarrow$ (ostatní z nich odvozené)
- logické axiomy** (schémata logických axiomů):

$$(i) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(ii) \quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$$

$$(iii) \quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

kde φ , ψ , χ jsou libovolné formule (daného jazyka).

- odvozovací pravidlo:**

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi} \quad (\text{modus ponens})$$

Důkaz (Hilbertova stylu) formule φ v teorii T je **konečná** posloupnost

$\varphi_0, \dots, \varphi_n = \varphi$ formulí taková, že pro každé $i \leq n$

- φ_i je logický axiom nebo $\varphi_i \in T$ (axiom teorie), nebo
- φ_i lze odvodit z předchozích formulí pomocí odvozovacího pravidla.

Poznámka Volba axiomů a odvozovacích pravidel se v může v různých dokazovacích systémech Hilbertova stylu lišit.

Příklad a korektnost

Formule φ je **dokazatelná** v T , má-li důkaz z T , značíme $T \vdash_H \varphi$.

Je-li $T = \emptyset$, značíme $\vdash_H \varphi$. Např. pro $T = \{\neg\varphi\}$ je $T \vdash_H \varphi \rightarrow \psi$ pro každé ψ .

- | | | |
|----|---|-----------------------|
| 1) | $\neg\varphi$ | axiom z T |
| 2) | $\neg\varphi \rightarrow (\neg\psi \rightarrow \neg\varphi)$ | logický axiom (i) |
| 3) | $\neg\psi \rightarrow \neg\varphi$ | modus ponens z 1), 2) |
| 4) | $(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$ | logický axiom (iii) |
| 5) | $\varphi \rightarrow \psi$ | modus ponens z 3), 4) |

Věta Pro každou teorií T a formuli φ , $T \vdash_H \varphi \Rightarrow T \models \varphi$.

Důkaz

- Je-li $\varphi \in T$ nebo logický axiom, je $T \models \varphi$ (logické axiomy jsou tautologie),
- jestliže $T \models \varphi$ a $T \models \varphi \rightarrow \psi$, pak $T \models \psi$, tj. modus ponens je **korektní**,
- tedy každá formule vyskytující se v důkazu z T platí v T . □

Poznámka Platí i **úplnost**, tj. $T \models \varphi \Rightarrow T \vdash_H \varphi$ pro každou teorií T a formuli φ .

Výroková a predikátová logika - V

Petr Gregor

KTIML MFF UK

ZS 2021/22

Rezoluční metoda - úvod

Hlavní rysy **rezoluční metody** (*neformálně*)

- je základem mnoha různých systémů, např. interpret Prologu, SAT řešiče, systémy pro automatické dokazování / verifikování, ...
- předpokládá formule v **CNF** (převod obecně “*drahý*”),
- pracuje s **množinovou reprezentací** formulí,
- má jediné odvozovací pravidlo, tzv. **rezoluční pravidlo**,
- nemá žádné explicitní axiomy (či atomická tabla), ale jisté axiomy jsou skryty “*uvnitř*”,
- obdobně jako u tablo metody, jde o **zamítací** proceduru, tj. snaží se ukázat, že daná formule (či teorie) je **nesplnitelná**,
- má různé varianty lišící se např. podmínkami pro použití rezolučního pravidla.

Množinová reprezentace (formulí v CNF)

- **Literál** l je výroková proměnná nebo její negace. $\bar{l}$ značí **opačný** literál k l .
- **Klauzule** C je konečná množina literálů ("tvořících disjunci"). **Prázdná klauzule** se značí $\square$, není nikdy splněna (neobsahuje splněný literál).
- **Formule** S je množina (i **nekonečná**) klauzulí ("tvořících konjunki"). **Prázdná formule** $\emptyset$ je vždy splněna (neobsahuje nesplněnou klauzuli). Nekonečné formule reprezentují nekonečné teorie (konjunktí axiomů).
- (**Částečné**) **ohodnocení** $\mathcal{V}$ je libovolná **konzistentní** množina literálů, tj. neobsahující dvojici opačných literálů. Ohodnocení $\mathcal{V}$ je **totální**, obsahuje-li pozitivní či negativní literál od každé výrokové proměnné.
- $\mathcal{V}$ **splňuje** S , značíme $\mathcal{V} \models S$, pokud $C \cap \mathcal{V} \neq \emptyset$ pro každé $C \in S$.

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

$$S = \{ \{ \neg p, q \}, \{ \neg p, \neg q, r \}, \{ \neg r, \neg s \}, \{ \neg t, s \}, \{ s \} \} \quad \text{a}$$

$$\mathcal{V} \models S \quad \text{pro} \quad \mathcal{V} = \{ s, \neg r, \neg p \}$$

Rezoluční pravidlo

Nechť C_1 , C_2 jsou klauzule a $l \in C_1$, $\bar{l} \in C_2$ pro nějaký literál l . Pak z C_1 a C_2 odvod' **přes literál** l klauzuli (tzv. **rezolventu**)

$$C = (C_1 \setminus \{l\}) \cup (C_2 \setminus \{\bar{l}\}).$$

Např. z klauzulí $\{p, q, r\}$ a $\{\neg p, \neg q\}$ lze odvodit rezolventu $\{q, \neg q, r\}$ přes literál p nebo $\{p, \neg p, r\}$ přes literál q .

Pozorování Rezoluční pravidlo je **korektní**, tj. pro libovolné ohodnocení $\mathcal{V}$,

$$\mathcal{V} \models C_1 \text{ a } \mathcal{V} \models C_2 \quad \Rightarrow \quad \mathcal{V} \models C.$$

Poznámka Rezoluční pravidlo je speciální případ **pravidla řezu**

$$\frac{\varphi \vee \psi, \neg \varphi \vee \chi}{\psi \vee \chi}$$

kde φ , ψ , χ jsou libovolné formule.

Rezoluční důkaz

- **rezoluční důkaz** (*odvození*) klauzule C z formule S je **konečná** posloupnost $C_0, \dots, C_n = C$ taková, že pro každé $i \leq n$ je $C_i \in S$ nebo je C_i rezolventou nějakých dvou předchozích klauzulí (i stejných),
- klauzule C je (rezolucí) **dokazatelná** z S , psáno $S \vdash_R C$, pokud má rezoluční důkaz z S ,
- **zamítnutí** formule S je rezoluční důkaz $\square$ z S ,
- S je (rezolucí) **zamítnutelná**, pokud $S \vdash_R \square$.

Věta (korektnost) *Je-li S rezolucí zamítnutelná, je S nesplnitelná.*

Důkaz Nechť $S \vdash_R \square$. Kdyby $\mathcal{V} \models S$ pro nějaké ohodnocení $\mathcal{V}$, z korektnosti rezolučního pravidla by $\mathcal{V}$ splňovalo každou klauzuli v rezolučním důkazu z S , tedy by platilo i $\mathcal{V} \models \square$, což není možné. ■

Rezoluční strom a uzávěr

Rezoluční strom klauzule C z formule S je **konečný** binární strom s vrcholy označenými klauzulemi takový, že

- (i) kořen je označen C ,
- (ii) listy jsou označeny klauzulemi z S ,
- (iii) každý **vnitřní** vrchol je označen rezolventou z klauzulí v jeho synech.

Pozorování C má rezoluční strom z S právě když $S \vdash_R C$.

Rezoluční uzávěr $\mathcal{R}(S)$ formule S je nejmenší induktivní množina definovaná

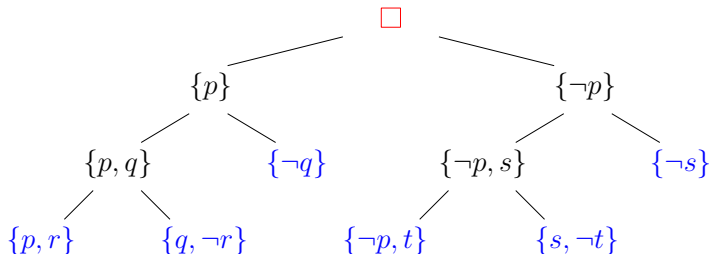
- (i) $C \in \mathcal{R}(S)$ pro každé $C \in S$,
- (ii) jsou-li $C_1, C_2 \in \mathcal{R}(S)$ a C je rezolventa C_1, C_2 , je zároveň $C \in \mathcal{R}(S)$.

Pozorování $C \in \mathcal{R}(S)$ právě když $S \vdash_R C$.

Poznámka Všechny pojmy o rezolučních důkazech lze tedy ekvivalentně zavést pomocí rezolučních stromů či uzávěrů.

Příklad

Formule $((p \vee r) \wedge (q \vee \neg r) \wedge (\neg q) \wedge (\neg p \vee t) \wedge (\neg s) \wedge (s \vee \neg t))$ je nespelnitelná, neboť pro $S = \{\{p, r\}, \{q, \neg r\}, \{\neg q\}, \{\neg p, t\}, \{\neg s\}, \{s, \neg t\}\}$ je $S \vdash_R \square$.



Rezoluční uzávěr S je

$$\mathcal{R}(S) = \{\{p, r\}, \{q, \neg r\}, \{\neg q\}, \{\neg p, t\}, \{\neg s\}, \{s, \neg t\}, \{p, q\}, \{\neg r\}, \{r, t\}, \\ \{q, t\}, \{\neg t\}, \{\neg p, s\}, \{r, s\}, \{t\}, \{q\}, \{q, s\}, \square, \{\neg p\}, \{p\}, \{r\}, \{s\}\}.$$

Redukce dosazením

Nechť S je formule a l je literál. Označme

$$S^l = \{C \setminus \{\bar{l}\} \mid l \notin C \in S\}.$$

Pozorování

- S^l je ekvivalentní formuli, jež vznikne dosazením konstanty $\top$ (true, 1) za literály l a konstanty $\perp$ (false, 0) za literály $\bar{l}$ ve formuli S ,
- S^l neobsahuje v žádné klauzuli literál l ani $\bar{l}$,
- jestliže $\{\bar{l}\} \in S$, pak $\square \in S^l$.

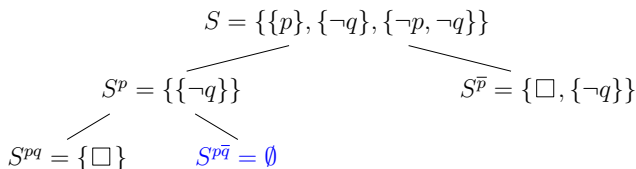
Lemma S je splnitelná, právě když S^l nebo $S^{\bar{l}}$ je splnitelná.

Důkaz ($\Rightarrow$) Nechť $\mathcal{V} \models S$ pro nějaké $\mathcal{V}$ a předpokládejme (búno), že $\bar{l} \notin \mathcal{V}$.

- Pak $\mathcal{V} \models S^l$, neboť pro $l \notin C \in S$ je $\mathcal{V} \setminus \{l, \bar{l}\} \models C$ a tudíž $\mathcal{V} \models C \setminus \{\bar{l}\}$.
- Naopak ($\Leftarrow$) předpokládejme (búno), že $\mathcal{V} \models S^l$ pro nějaké $\mathcal{V}$.
- Jelikož se l ani $\bar{l}$ nevyskytuje v S^l , je i $\mathcal{V}' \models S^l$ pro $\mathcal{V}' = (\mathcal{V} \setminus \{\bar{l}\}) \cup \{l\}$.
- Pak $\mathcal{V}' \models S$, neboť pro $C \in S$ obsahující l máme $l \in \mathcal{V}'$ a pro $C \in S$ neobsahující l je $\mathcal{V}' \models (C \setminus \{\bar{l}\}) \in S^l$. ■

Strom dosazení

Postupnou redukci literálů dosazením lze reprezentovat binárním stromem.



Důsledek S není splnitelná, právě když každá větev obsahuje $\square$.

Poznámka Jelikož S může být nekonečná nad spočetným jazykem, strom může být nekonečný. Je-li ale S nespjitelná, dle **věty o kompaktnosti** existuje konečná část $S' \subseteq S$, která je nespjitelná. Pak po redukci všech literálů vyskytujících se v S' bude $\square$ v každé větvi po konečně mnoha krocích.

Úplnost rezoluce

Věta Je-li *konečná* S nespílitelná, je rezolucí zamítnutelná, tj. $S \vdash_R \square$.

Důkaz Indukcí dle počtu proměnných v S ukážeme, že $S \vdash_R \square$.

- Nemá-li nespílitelná S žádnou proměnnou, je $S = \{\square\}$ a tedy $S \vdash_R \square$,
- Necht' l je literál vyskytující se v S . Dle lemmatu, S^l a $S^{\bar{l}}$ jsou nespílitelné.
- Jelikož S^l a $S^{\bar{l}}$ mají méně proměnných než S , dle indukčního předpokladu existují rezoluční stromy T^l a $T^{\bar{l}}$ pro odvození $\square$ z S^l resp. $S^{\bar{l}}$.
- Je-li každý list T^l z S , je T^l rezolučním stromem $\square$ z S , tj. $S \vdash_R \square$.
- Pokud ne, **doplněním** literálu $\bar{l}$ do každého listu, jenž není z S , (a do všech vrcholů nad ním) získáme rezoluční strom $\{\bar{l}\}$ z S .
- Obdobně získáme rezoluční strom $\{l\}$ z S **doplněním** l ve stromu $T^{\bar{l}}$,
- Rezolucí jejich kořenů $\{\bar{l}\}$ a $\{l\}$ získáme rezoluční strom $\square$ z S . ■

Důsledek Je-li S nespílitelná, je rezolucí zamítnutelná, tj. $S \vdash_R \square$.

Důkaz Plyne z předchozího užitím věty o kompaktnosti.

Lineární rezoluce - úvod

Rezoluční metodu můžeme značně omezit (bez ztráty úplnosti).

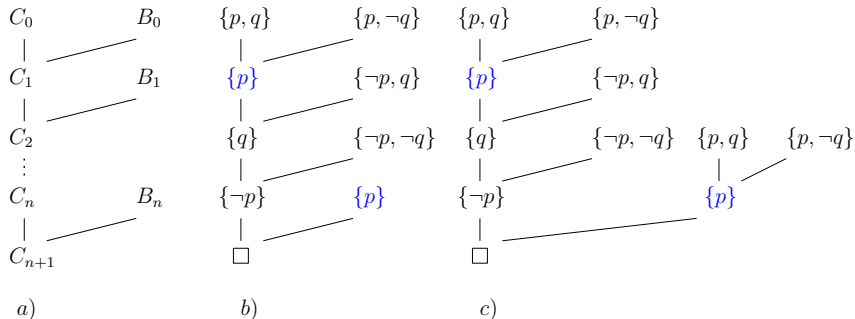
- **Lineární důkaz** (rezolucí) klauzule C z formule S je konečná posloupnost dvojic $(C_0, B_0), \dots, (C_n, B_n)$ taková, že $C_0 \in S$ a pro každé $i \leq n$
 - $B_i \in S$ nebo $B_i = C_j$ pro nějaké $j < i$, a
 - C_{i+1} je rezolventa C_i a B_i , kde $C_{n+1} = C$.
- C_0 zveme **počáteční** klauzule, C_i **centrální** klauzule, B_i **boční** klauzule.
- C je **lineárně dokazatelná** z S , psáno $S \vdash_L C$, má-li lineární důkaz z S .
- **Lineární zamítnutí** S je lineární důkaz $\square$ z S .
- S je **lineárně zamítnutelná**, pokud $S \vdash_L \square$.

Pozorování *Je-li S lineárně zamítnutelná, je S nesplnitelná.*

Důkaz Každý lineární důkaz lze transformovat na (korektní) rezoluční důkaz.

Poznámka *Platí i úplnost, tj. je-li S nesplnitelná, je S lineárně zamítnutelná.*

Příklad lineární rezoluce



a) obecný tvar lineární rezoluce,

b) pro $S = \{\{p, q\}, \{p, \neg q\}, \{\neg p, q\}, \{\neg p, \neg q\}\}$ je $S \vdash_L \square$,

c) transformace lineárního důkazu na rezoluční důkaz.

LI-rezoluce

Pro Hornovy formule můžeme lineární rezoluci dál omezit.

- **Hornova formule** je množina (i nekonečná) Hornových klauzulí.
- **Hornova klauzule** je klauzule obsahující nejvýše jeden pozitivní literál.
- **Fakt** je (Hornova) klauzule $\{p\}$, kde p je pozitivní literál.
- **Pravidlo** je (Hornova) klauzule s právě jedním pozitivním a aspoň jedním negativním literálem. Pravidla a fakta jsou **programové klauzule**.
- **Cíl** je neprázdná (Hornova) klauzule bez pozitivního literálu.

Pozorování Je-li Hornova formule S nespílitelná a $\square \notin S$, obsahuje fakt i cíl.

Důkaz Neobsahuje-li fakt (cíl), je splnitelná nastavením všech proměnných na 0 (resp. na 1). ■

LI-rezoluce (linear input) z formule S je lineární rezoluce z S , ve které je každá boční klauzule B_i ze (vstupní) formule S .

Je-li klauzule C dokazatelná LI-rezolucí z S , píšeme $S \vdash_{LI} C$.

Úplnost LI-rezoluce pro Hornovy formule

Věta Je-li Hornova T splnitelná a $T \cup \{G\}$ nespjitelná pro cíl G , lze $\square$ odvodit LI-rezolucí z $T \cup \{G\}$ začínající G .

Důkaz Dle věty o kompaktnosti můžeme předpokládat, že T je konečná.

- Postupujeme indukcí dle počtu proměnných v T .
- Dle pozorování, T obsahuje fakt $\{p\}$ pro nějakou proměnnou p .
- Dle lemmatu je $T' = (T \cup \{G\})^p = T^p \cup \{G^p\}$ nespjitelná, přičemž $G^p = G \setminus \{\bar{p}\}$.
- Je-li $G^p = \square$, je $G = \{\bar{p}\}$ a tedy $\square$ je rezolventa G a $\{p\} \in T$.
- Jinak, jelikož T^p je splnitelná (stejným ohodnocením, které splňuje T) a má méně proměnných, dle indukčního předpokladu lze $\square$ odvodit LI-rezolucí z T' začínající G^p .
- **Doplněním** literálu $\bar{p}$ do všech listů, jež nejsou v $T \cup \{G\}$, a všech vrcholů pod ním získáme LI-odvození $\{\bar{p}\}$ z $T \cup \{G\}$ začínající v G .
- Závěrečnou rezolucí pomocí faktu $\{p\} \in T$ získáme $\square$. ■

Příklad LI-rezoluce

$$T = \{\{p, \neg r, \neg s\}, \{r, \neg q\}, \{q, \neg s\}, \{s\}\}, \quad G = \{\neg p, \neg q\}$$

$$T^s = \{\{p, \neg r\}, \{r, \neg q\}, \{q\}\}$$

$$T^{sq} = \{\{p, \neg r\}, \{r\}\}$$

$$T^{sqr} = \{\{p\}\} \quad G^{sq} = \{\neg p\} \quad \{p, \neg r\}$$

$$G^{sqr} = \{\neg p\} \quad \{p\}$$

$$G^{sqrp} = \square$$

$$T^{sqr}, G^{sqr} \vdash_{LI} \square$$

$$\begin{array}{c} \{p, \neg r\} \\ | \quad / \\ \{\neg r\} \quad \{r\} \\ | \quad / \\ \square \end{array}$$

$$T^{sq}, G^{sq} \vdash_{LI} \square$$

$$G^s = \{\neg p, \neg q\} \quad \{p, \neg r\}$$

$$\begin{array}{c} \{p, \neg r\} \\ | \quad / \\ \{\neg q, \neg r\} \quad \{r, \neg q\} \\ | \quad / \\ \{\neg q\} \quad \{q\} \\ | \quad / \\ \square \end{array}$$

$$T^s, G^s \vdash_{LI} \square$$

$$G = \{\neg p, \neg q\} \quad \{p, \neg r, \neg s\}$$

$$\begin{array}{c} \{p, \neg r, \neg s\} \\ | \quad / \\ \{\neg q, \neg r, \neg s\} \quad \{r, \neg q\} \\ | \quad / \\ \{\neg q, \neg s\} \quad \{q, \neg s\} \\ | \quad / \\ \{\neg s\} \quad \{s\} \\ | \quad / \\ \square \end{array}$$

$$T, G \vdash_{LI} \square$$

Program v Prologu

(Výrokový) **program** (v Prologu) je Hornova formule obsahující pouze programové klauzule, tj. fakta nebo pravidla.

<i>pravidlo</i>	$p :- q, r.$	$q \wedge r \rightarrow p$	$\{p, \neg q, \neg r\}$	
	$p :- s.$	$s \rightarrow p$	$\{p, \neg s\}$	
	$q :- s.$	$s \rightarrow q$	$\{q, \neg s\}$	
<i>fakt</i>	$r.$	r	$\{r\}$	
	$s.$	s	$\{s\}$	<i>program</i>
<i>dotaz</i>	$?- p, q.$		$\{\neg p, \neg q\}$	<i>cíl</i>

Zajímá nás, zda daný **dotaz** vyplývá z daného programu.

Důsledek Pro každý program P a dotaz $(p_1 \wedge \dots \wedge p_n)$ je ekvivalentní, zda

- (1) $P \models p_1 \wedge \dots \wedge p_n$,
- (2) $P \cup \{\neg p_1, \dots, \neg p_n\}$ je nespílitelná,
- (3) $\square$ lze odvodit LI-rezolucí z $P \cup \{G\}$ začínající cílem $G = \{\neg p_1, \dots, \neg p_n\}$.

Rezoluce v Prologu

1) S klauzulemi interpret pracuje jako s *uspořádanými seznamy literálů*.

LD-rezoluce (linear definite) je LI-rezoluce, při které v každém kroku rezolventa aktuálního cíle $(\neg p_1, \dots, \neg p_{i-1}, \neg p_i, \neg p_{i+1}, \dots, \neg p_n)$ a boční klauzule $(p_i, \neg q_1, \dots, \neg q_m)$ je $(\neg p_1, \dots, \neg p_{i-1}, \neg q_1, \dots, \neg q_m, \neg p_{i+1}, \dots, \neg p_n)$.

Pozorování Každý LI-důkaz lze transformovat na LD-důkaz stejné klauzule ze stejné formule se stejnou počáteční klauzulí (cílem).

2) Výběr literálu z cílové klauzule, přes který se rezolvuje, je určen daným *selekčním pravidlem* $\mathcal{R}$. Typicky, “vyber první literál z aktuálního cíle”.

SLD-rezoluce (selection) dle $\mathcal{R}$ je LD-rezoluce, při které se v kroku (C_i, B_i) rezolvuje přes literál $\mathcal{R}(C_i)$.

Pozorování Každý LD-důkaz lze transformovat na SLD-důkaz stejné klauzule ze stejné formule se stejnou počáteční klauzulí (cílem).

Důsledek SLD-rezoluce je *úplná* pro dotazy nad programy v Prologu.

Prohledávací SLD-strom

Dosud není určen výběr programové klauzule pro rezoluci s aktuálním cílem.

SLD-strom programu P a cíle G pro selekční pravidlo $\mathcal{R}$ je strom s vrcholy označenými cíly takový, že kořen je označen G a je-li nějaký vrchol označen G' , má tolik synů, kolik je **možností** rezolucí G' s programovými klauzulemi v P dle literálu $\mathcal{R}(G')$. Synové jsou označeni příslušnými rezolventami.

$p :- q, r.$ (1)

$p :- s.$ (2)

$q.$ (3)

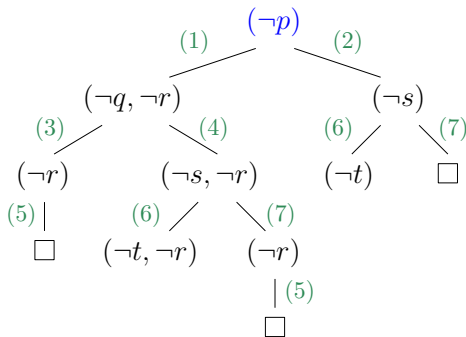
$q :- s.$ (4)

$r.$ (5)

$s :- t.$ (6)

$s.$ (7)

$?- p.$



Závěrečné poznámky

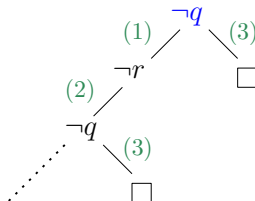
- Interpret Prologu **prochází** SLD-strom, způsob není předepsán.
- Implementace, které používají **DFS**, nezachovávají úplnost.

$q :- r.$ (1)

$r :- q.$ (2)

$q.$ (3)

$?- q.$



- Jistou kontrolu nad prohledáváním poskytuje **!**, tzv. **řez**.
- Při povolení **negace** nastanou potíže se sémantikou programů.
- Síla rezoluční metody bude více patrná v predikátové logice.

Výroková a predikátová logika - VI

Petr Gregor

KTIML MFF UK

ZS 2021/22

Predikátová logika

Zabývá se tvrzeními o individuích, jejich vlastnostech a vztazích.

“Je inteligentní a její otec zná pana rektora.”

$$I(x) \wedge Z(o(x), r)$$

- x je **proměnná**, reprezentuje individuum,
- r je **konstantní symbol**, reprezentuje konkrétní individuum,
- o je **funkční symbol**, reprezentuje funkci,
- I, Z jsou **relační (predikátové) symboly**, reprezentují relace (vlastnost “*být inteligentní*” a vztah “*znát*”).

“Funkce f je na (surjektivní).”

$$(\forall x)(\exists y)(f(y) = x)$$

- $(\forall x)$ je **všeobecný (univerzální) kvantifikátor** proměnné x ,
- $(\exists y)$ je **existenční kvantifikátor** proměnné y ,
- $=$ je (binární) **relační symbol**, reprezentuje identickou relaci.

Jazyk

Jazyk 1. řádu obsahuje

- **proměnné** $x, y, z, \dots, x_0, x_1, \dots$ (spočetně mnoho), množinu všech proměnných značíme **Var**,
- **funkční symboly** $f, g, h, \dots$, včetně **konstantních symbolů** $c, d, \dots$, což jsou nulární funkční symboly,
- **relační (predikátové) symboly** $P, Q, R, \dots$, případně symbol $=$ (**rovnost**) jako speciální relační symbol,
- **kvantifikátory** $(\forall x), (\exists x)$ pro každou proměnnou $x \in \text{Var}$,
- **logické spojky** $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- **závorky** $(,)$

Každý funkční i relační symbol S má danou **aritu** (**četnost**) $\text{ar}(S) \in \mathbb{N}$.

***Poznámka** Oproti výrokové logice nemáme (explicitně) výrokové proměnné, lze je zavést jako nulární relační symboly.*

Signatura jazyka

- Proměnné, kvantifikátory, logické spojky a závorky jsou *logické symboly*, zatímco funkční a relační symboly (kromě případné rovnosti) jsou *mimologické symboly*. Rovnost (*obvykle*) uvažujeme zvlášť.
- *Signatura* je dvojice $\langle \mathcal{R}, \mathcal{F} \rangle$ disjunktních množin relačních a funkčních symbolů s danými aritami, přičemž žádný z nich není rovnost. Signatura tedy určuje všechny mimologické symboly.
- *Jazyk* je dán signaturou $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a uvedením, zda jde o jazyk s rovností či bez rovnosti. Jazyk musí obsahovat alespoň jeden relační symbol (mimologický nebo rovnost).

Poznámka Význam symbolů není v jazyce určen, např. symbol $+$ nemusí reprezentovat standardní sčítání.

Příklady jazyků

Jazyk obvykle uvádíme výčtem mimologických symbolů s případným upřesněním, zda jde o funkční či relační symboly a jakou mají aritu.

Následující příklady jazyků jsou všechny s **rovností**.

- $L = \langle \rangle$ je jazyk **čisté** rovnosti,
- $L = \langle c_i \rangle_{i \in \mathbb{N}}$ je jazyk spočetně mnoha konstant,
- $L = \langle \leq \rangle$ je jazyk **uspořádání**,
- $L = \langle E \rangle$ je jazyk teorie **grafů**,
- $L = \langle +, -, 0 \rangle$ je jazyk teorie **grup**,
- $L = \langle +, -, \cdot, 0, 1 \rangle$ je jazyk teorie **těles**,
- $L = \langle -, \wedge, \vee, 0, 1 \rangle$ je jazyk **Booleových algeber**,
- $L = \langle S, +, \cdot, 0, \leq \rangle$ je jazyk **aritmetiky**,

kde c_i , 0, 1 jsou konstantní symboly, S , $-$ jsou unární funkční symboly, $+$, $\cdot$, $\wedge$, $\vee$ jsou binární funkční symboly, E , $\leq$ jsou binární relační symboly.

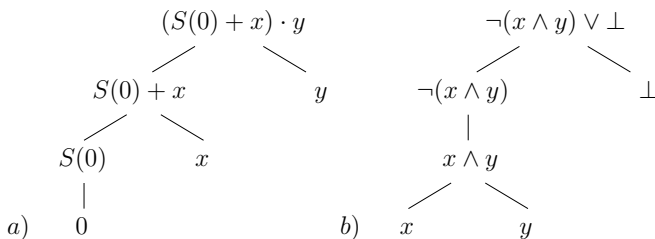
Termy

Jsou výrazy reprezentující hodnoty (složených) funkcí.

Termy jazyka L jsou dány indukčním předpisem

- (i) každá proměnná nebo konstantní symbol je term,
 - (ii) je-li f funkční symbol jazyka L s aritou $n > 0$ a $t_1, \dots, t_n$ jsou termy, pak je i výraz $f(t_1, \dots, t_n)$ term,
 - (iii) každý term vznikne **konečným** užitím pravidel (i), (ii).
- **Konstantní (ground) term** je term bez proměnných, např. $f(0) + 1$.
 - Množinu všech termů jazyka L značíme Term_L .
 - Termu, jenž je součástí jiného termu t , říkáme **podterm** termu t .
 - Strukturu termu můžeme reprezentovat jeho **vytvěřujícím stromem**.
 - U binárních funkčních symbolů často používáme **infixního** zápisu, např. píšeme $(x + y)$ namísto $+(x, y)$.

Příklady termů



- a) Vytvořující strom termu $(S(0) + x) \cdot y$ jazyka aritmetiky.
- b) Výrokové formule se spojkami $\neg$, $\wedge$, $\vee$, případně s konstantami $\top$, $\perp$ lze chápat jako termy jazyka Booleových algeber.

Atomické formule

Jsou nejjednodušší formule.

- **Atomická formule** jazyka L je výraz $R(t_1, \dots, t_n)$, kde R je n -ární relační symbol jazyka L a $t_1, \dots, t_n$ jsou termy jazyka L .
- Množinu všech atomických formulí jazyka L značíme $\mathbf{AFm}_L$.
- Strukturu atomické formule můžeme reprezentovat **vytvorujícím stromem** z vytvorujících podstromů jejích termů.
- U binárních relačních symbolů často používáme **infixního** zápisu, např.
 $t_1 = t_2$ namísto $=(t_1, t_2)$ či $t_1 \leq t_2$ namísto $\leq(t_1, t_2)$.
- *Příklady atomických formulí*

$$Z(o(x), r), \quad x \cdot y \leq (S(0) + x) \cdot y, \quad \neg(x \wedge y) \vee \perp = \perp.$$

Formule

Formule jazyka L jsou výrazy dané induktivním předpisem

- (i) každá atomická formule jazyka L je formule,
 - (ii) jsou-li φ, ψ formule, pak i následující výrazy jsou formule
$$(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi),$$
 - (iii) je-li φ formule a x proměnná, jsou výrazy $((\forall x)\varphi)$ a $((\exists x)\varphi)$ formule.
 - (iv) každá formule vznikne **konečným** užitím pravidel (i), (ii), (iii).
- Množinu všech formulí jazyka L značíme **Fm_L**.
 - Formulí, jež je součástí jiné formule φ , nazveme **podformule** formule φ .
 - Strukturu formule můžeme reprezentovat jejím **vytvěřujícím stromem**.

Konvence zápisu

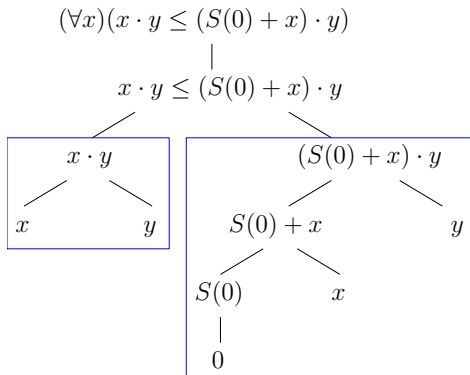
- Zavedení *priorit* binárních funkčních symbolů např. $+$, $\cdot$ umožňuje při *infixním* zápisu vypouštět závorky okolo podtermu vzniklého symbolem *vyšší* priority, např. $x \cdot y + z$ reprezentuje term $(x \cdot y) + z$.
- Zavedení *priorit* logických spojek a kvantifikátorů umožňuje vypouštět závorky okolo podformule vzniklé spojkou s *vyšší* prioritou.

$$(1) \rightarrow, \leftrightarrow \quad (2) \wedge, \vee \quad (3) \neg, (\forall x), (\exists x)$$

- Okolo podformulí vzniklých $\neg, (\forall x), (\exists x)$ lze závorky vypustit vždy.
- Můžeme vypustit závorky i okolo $(\forall x)$ a $(\exists x)$ pro každé $x \in \text{Var}$.
- Rovněž vnější závorky můžeme vynechat.

$$\begin{aligned} & (((\neg((\forall x)R(x))) \wedge ((\exists y)P(y))) \rightarrow (\neg(((\forall x)R(x)) \vee (\neg((\exists y)P(y))))) \\ & \neg(\forall x)R(x) \wedge (\exists y)P(y) \rightarrow \neg((\forall x)R(x) \vee \neg(\exists y)P(y)) \end{aligned}$$

Příklad formule



Vytvořující strom formule $(\forall x)(x \cdot y \leq (S(0) + x) \cdot y)$.

Výskyt proměnné

Nechť φ je formule a x je proměnná.

- **Výskyt** proměnné x ve φ je list vytvořujícího stromu φ označený x .
- Výskyt x ve φ je **vázaný**, je-li součástí nějaké podformule ψ začínající kvantifikátorem $(\forall x)$ nebo $(\exists x)$. Není-li výskyt vázaný, je **volný**.
- Proměnná x je **volná** ve φ , pokud má volný výskyt ve φ .
Je **vázaná** ve φ , pokud má vázaný výskyt ve φ .
- Proměnná x může být zároveň volná i vázaná ve φ . Např. ve formuli

$$(\forall x)(\exists y)(x \leq y) \vee x \leq z.$$

- Zápis $\varphi(x_1, \dots, x_n)$ značí, že $x_1, \dots, x_n$ jsou všechny volné proměnné ve formuli φ .

Poznámka Uvidíme, že pravdivostní hodnota formule (při dané interpretaci symbolů) závisí pouze na ohodnocení volných proměnných.

Otevřené a uzavřené formule

- Formule je *otevřená*, neobsahuje-li žádný kvantifikátor. Pro množinu OFm_L všech otevřených formulí jazyka L platí $\text{AFm}_L \subsetneq \text{OFm}_L \subsetneq \text{Fm}_L$.
- Formule je *uzavřená* (*sentence*), pokud nemá žádnou volnou proměnnou, tj. všechny výskyty proměnných jsou vázané.
- Formule může být otevřená i uzavřená zároveň, pak všechny její termy jsou konstantní.

$x + y \leq 0$	<i>otevřená</i> , $\varphi(x, y)$
$(\forall x)(\forall y)(x + y \leq 0)$	<i>uzavřená (sentence)</i> ,
$(\forall x)(x + y \leq 0)$	<i>ani otevřená, ani uzavřená</i> , $\varphi(y)$
$1 + 0 \leq 0$	<i>otevřená i uzavřená</i>

***Poznámka** Uvidíme, že sentence má při dané interpretaci symbolů pevný význam, tj. její pravdivostní hodnota nezávisí na ohodnocení proměnných.*

Instance

Když do formule za volnou proměnnou x **dosadíme** term t , požadujeme, aby vzniklá formule *říkala (nově) o termu t “totéž”, co předtím říkala o proměnné x .*

$\varphi(x)$	$(\exists y)(x + y = 1)$	“existuje prvek $1 - x$ ”
pro $t = 1$ lze $\varphi(x/t)$	$(\exists y)(1 + y = 1)$	“existuje prvek $1 - 1$ ”
pro $t = y$ nelze	$(\exists y)(y + y = 1)$	“1 je dělitelné 2”

- Term t je **substituovatelný** za proměnnou x ve formuli φ , pokud po současném nahrazení všech volných výskytů x za t nevznikne ve φ žádný vázaný výskyt proměnné x .
- Pak vzniklou formuli značíme $\varphi(x/t)$ a zveme ji **instance** formule φ vzniklá **substitucí** termu t za proměnnou x do φ .
- t není substituovatelný za x do φ , právě když x má volný výskyt v nějaké podformuli φ začínající $(\forall y)$ nebo $(\exists y)$ pro nějakou proměnnou y z t .
- **Konstantní** termy jsou substituovatelné vždy.

Varianty

Kvantifikované proměnné lze (za *určitých* podmínkách) přejmenovat tak, že vznikne ekvivalentní formule.

Nechť $(Qx)\psi$ je podformule ve φ , kde Q značí $\forall$ či $\exists$, a y je proměnná, tž.

- 1) y je *substituovatelná* za x do ψ , a
- 2) y nemá *volný* výskyt v ψ .

Nahrazením podformule $(Qx)\psi$ za $(Qy)\psi(x/y)$ vznikne *varianta* formule φ *v podformuli* $(Qx)\psi$. Postupnou variací jedné či více podformulí ve φ vznikne *varianta* formule φ . *Např.*

$$(\exists x)(\forall y)(x \leq y)$$

$$(\exists u)(\forall v)(u \leq v)$$

$$(\exists y)(\forall y)(y \leq y)$$

$$(\exists x)(\forall x)(x \leq x)$$

je formule φ ,

je varianta φ ,

není varianta φ , neplatí 1),

není varianta φ , neplatí 2).

Struktury - příklady

- $\mathcal{S} = \langle S, \leq \rangle$ **uspořádaná** množina, kde $\leq$ je reflexivní, antisymetrická, tranzitivní binární relace na S ,
- $G = \langle V, E \rangle$ neorientovaný **graf** bez smyček, kde V je množina *vrcholů*, E je ireflexivní, symetrická binární relace na V (*sousednost*),
- $\mathbb{Z}_p = \langle \mathbb{Z}_p, +, -, 0 \rangle$ **grupa** sčítání celých čísel modulo p ,
- $\mathbb{Q} = \langle \mathbb{Q}, +, -, \cdot, 0, 1 \rangle$ **těleso** racionálních čísel.
- $\mathcal{P}(X) = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ **potenční algebra** nad množinou X ,
- $\mathbb{N} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ standardní model **aritmetiky** (přirozených čísel),
- konečné automaty a další modely výpočtu,
- relační databáze, ...

Struktura pro jazyk

Nechť $L = \langle \mathcal{R}, \mathcal{F} \rangle$ je jazyk a A je neprázdná množina.

- *Realizace (interpretace) relačního symbolu* $R \in \mathcal{R}$ na A je libovolná relace $R^A \subseteq A^{\text{ar}(R)}$. Realizace rovnosti na A je relace Id_A (identita).
- *Realizace (interpretace) funkčního symbolu* $f \in \mathcal{F}$ na A je libovolná funkce $f^A : A^{\text{ar}(f)} \rightarrow A$. Realizace *konstantního* symbolu je tedy prvek z A .

Struktura jazyka L (*L-struktura*) je trojice $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$, kde

- A je neprázdná množina, zvaná *doména (univerzum)* struktury $\mathcal{A}$,
- $\mathcal{R}^A = \langle R^A \mid R \in \mathcal{R} \rangle$ je *soubor* realizací relačních symbolů (relací),
- $\mathcal{F}^A = \langle f^A \mid f \in \mathcal{F} \rangle$ je *soubor* realizací funkčních symbolů (funkcí).

Strukturu pro jazyk L nazýváme také *model jazyka* L . Třída všech modelů jazyka L se značí $M(L)$. Např. *struktury pro jazyk* $L = \langle \leq \rangle$ jsou

$\langle \mathbb{N}, \leq \rangle$, $\langle \mathbb{Q}, > \rangle$, $\langle X, E \rangle$ pokud $X \neq \emptyset$, $\langle \mathcal{P}(X), \subseteq \rangle$.

Hodnota termu

Nechť t je term jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ je struktura pro L .

- *Ohodnocení proměnných* v množině A je funkce $e: \text{Var} \rightarrow A$.
- *Hodnota* $t^{\mathcal{A}}[e]$ termu t ve struktuře $\mathcal{A}$ při ohodnocení e je dána induktivním předpisem

$$x^{\mathcal{A}}[e] = e(x) \quad \text{pro každé } x \in \text{Var},$$

$$(f(t_1, \dots, t_n))^{\mathcal{A}}[e] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e]) \quad \text{pro každé } f \in \mathcal{F}.$$

- Speciálně, pro konstantní symbol c je $c^{\mathcal{A}}[e] = c^{\mathcal{A}}$.
- Je-li t *konstantní* term, jeho hodnota v $\mathcal{A}$ nezávisí na ohodnocení e .
- Hodnota termu v $\mathcal{A}$ závisí pouze na ohodnocení jeho proměnných.

Např. hodnota termu $x + 1$ ve struktuře $\mathcal{N} = \langle \mathbb{N}, \cdot, 3 \rangle$ při ohodnocení e , pro které $e(x) = 2$, je $(x + 1)^{\mathcal{N}}[e] = 6$.

Hodnota atomické formule

Nechť φ je **atomická** formule tvaru $R(t_1, \dots, t_n)$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ je struktura pro L .

- **Hodnota** $H_{at}^{\mathcal{A}}(\varphi)[e]$ formule φ ve struktuře $\mathcal{A}$ při ohodnocení e je

$$H_{at}^{\mathcal{A}}(R(t_1, \dots, t_n))[e] = \begin{cases} 1 & \text{pokud } (t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e]) \in R^A, \\ 0 & \text{jinak.} \end{cases}$$

přičemž $=^{\mathcal{A}}$ je Id_A , tj. $H_{at}^{\mathcal{A}}(t_1 = t_2)[e] = 1$ pokud $t_1^{\mathcal{A}}[e] = t_2^{\mathcal{A}}[e]$, jinak 0.

- Je-li φ sentence, tj. všechny její termy jsou **konstantní**, její hodnota v $\mathcal{A}$ nezávisí na ohodnocení e .
- Hodnota φ v $\mathcal{A}$ závisí pouze na ohodnocení jejích (volných) proměnných.

Např. hodnota formule φ tvaru $x + 2 \leq 2$ ve struktuře $\mathcal{N} = \langle \mathbb{N}, +, 2, \leq \rangle$ při ohodnocení e je $H_{at}^{\mathcal{N}}(\varphi)[e] = 1$ právě když $e(x) = 0$.

Hodnota formule

Hodnota $H^{\mathcal{A}}(\varphi)[e]$ formule φ ve struktuře $\mathcal{A}$ při ohodnocení e je

$H^{\mathcal{A}}(\varphi)[e] = H_{at}^{\mathcal{A}}(\varphi)[e]$ pokud φ je atomická,

$$H^{\mathcal{A}}(\neg\varphi)[e] = \neg_1(H^{\mathcal{A}}(\varphi)[e])$$

$$H^{\mathcal{A}}(\varphi \wedge \psi)[e] = \wedge_1(H^{\mathcal{A}}(\varphi)[e], H^{\mathcal{A}}(\psi)[e])$$

$$H^{\mathcal{A}}(\varphi \vee \psi)[e] = \vee_1(H^{\mathcal{A}}(\varphi)[e], H^{\mathcal{A}}(\psi)[e])$$

$$H^{\mathcal{A}}(\varphi \rightarrow \psi)[e] = \rightarrow_1(H^{\mathcal{A}}(\varphi)[e], H^{\mathcal{A}}(\psi)[e])$$

$$H^{\mathcal{A}}(\varphi \leftrightarrow \psi)[e] = \leftrightarrow_1(H^{\mathcal{A}}(\varphi)[e], H^{\mathcal{A}}(\psi)[e])$$

$$H^{\mathcal{A}}((\forall x)\varphi)[e] = \min_{a \in A}(H^{\mathcal{A}}(\varphi)[e(x/a)])$$

$$H^{\mathcal{A}}((\exists x)\varphi)[e] = \max_{a \in A}(H^{\mathcal{A}}(\varphi)[e(x/a)])$$

kde $\neg_1, \wedge_1, \vee_1, \rightarrow_1, \leftrightarrow_1$ jsou Booleovské funkce dané tabulkami a $e(x/a)$ pro $a \in A$ značí ohodnocení získané z e nastavením $e(x) = a$.

Pozorování $H^{\mathcal{A}}(\varphi)[e]$ závisí pouze na ohodnocení *volných* proměnných ve φ .

Platnost při ohodnocení

Formule φ **je pravdivá (platí) ve struktuře $\mathcal{A}$ při ohodnocení e** , pokud $H^{\mathcal{A}}(\varphi)[e] = 1$. Pak píšeme $\mathcal{A} \models \varphi[e]$, v opačném případě $\mathcal{A} \not\models \varphi[e]$. Platí

$\mathcal{A} \models \neg\varphi[e]$	$\Leftrightarrow$	$\mathcal{A} \not\models \varphi[e]$
$\mathcal{A} \models (\varphi \wedge \psi)[e]$	$\Leftrightarrow$	$\mathcal{A} \models \varphi[e]$ a $\mathcal{A} \models \psi[e]$
$\mathcal{A} \models (\varphi \vee \psi)[e]$	$\Leftrightarrow$	$\mathcal{A} \models \varphi[e]$ nebo $\mathcal{A} \models \psi[e]$
$\mathcal{A} \models (\varphi \rightarrow \psi)[e]$	$\Leftrightarrow$	jestliže $\mathcal{A} \models \varphi[e]$, pak $\mathcal{A} \models \psi[e]$
$\mathcal{A} \models (\varphi \leftrightarrow \psi)[e]$	$\Leftrightarrow$	$\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$
$\mathcal{A} \models (\forall x)\varphi[e]$	$\Leftrightarrow$	$\mathcal{A} \models \varphi[e(x/a)]$ pro každé $a \in A$
$\mathcal{A} \models (\exists x)\varphi[e]$	$\Leftrightarrow$	$\mathcal{A} \models \varphi[e(x/a)]$ pro nějaké $a \in A$

Pozorování Nechť term t je **substituovatelný** za proměnnou x do formule φ a formule ψ je **varianta** φ . Pak pro každou strukturu $\mathcal{A}$ a ohodnocení e platí

- $\mathcal{A} \models \varphi(x/t)[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro $a = t^{\mathcal{A}}[e]$,
- $\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$.

Platnost ve struktuře

Nechť φ je formule jazyka L a $\mathcal{A}$ je struktura pro L .

- φ je **pravdivá (platí) ve struktuře $\mathcal{A}$** , značeno $\mathcal{A} \models \varphi$, pokud $\mathcal{A} \models \varphi[e]$ pro každé ohodnocení $e: \text{Var} \rightarrow A$. V opačném případě píšeme $\mathcal{A} \not\models \varphi$.
- φ je **lživá v $\mathcal{A}$** , pokud $\mathcal{A} \models \neg\varphi$, tj. $\mathcal{A} \not\models \varphi[e]$ pro každé $e: \text{Var} \rightarrow A$.
- Pro každé formule φ, ψ , proměnnou x a strukturu $\mathcal{A}$ platí

$$(1) \quad \mathcal{A} \models \varphi \quad \Rightarrow \quad \mathcal{A} \not\models \neg\varphi$$

$$(2) \quad \mathcal{A} \models \varphi \wedge \psi \quad \Leftrightarrow \quad \mathcal{A} \models \varphi \text{ a } \mathcal{A} \models \psi$$

$$(3) \quad \mathcal{A} \models \varphi \vee \psi \quad \Leftarrow \quad \mathcal{A} \models \varphi \text{ nebo } \mathcal{A} \models \psi$$

$$(4) \quad \mathcal{A} \models \varphi \quad \Leftrightarrow \quad \mathcal{A} \models (\forall x)\varphi$$

- Je-li φ **sentence**, je φ pravdivá v $\mathcal{A}$ či lživá v $\mathcal{A}$ a tedy implikace (1) platí i obráceně. Je-li φ nebo ψ sentence, implikace (3) platí i obráceně.
- Z (4) plyne, že $\mathcal{A} \models \varphi$ právě když $\mathcal{A} \models \psi$, kde ψ je **generální uzávěr** φ , tj. formule $(\forall x_1) \cdots (\forall x_n)\varphi$, v níž $x_1, \dots, x_n$ jsou všechny volné proměnné φ .

Platnost v teorii a logická platnost

- **Teorie** jazyka L je libovolná množina T formulí jazyka L (tzv. **axiomů**).
- **Model teorie** T je L -struktura $\mathcal{A}$ taková, že $\mathcal{A} \models \varphi$ pro každé $\varphi \in T$, značíme $\mathcal{A} \models T$.
- **Třída modelů** teorie T je $M(T) = \{\mathcal{A} \in M(L) \mid \mathcal{A} \models T\}$.
- Formule φ je **pravdivá v T** (**platí v T**), značíme $T \models \varphi$, pokud $\mathcal{A} \models \varphi$ pro každý model $\mathcal{A}$ teorie T . V opačném případě píšeme $T \not\models \varphi$.
- Formule φ je **lživá v T** , pokud $T \models \neg\varphi$, tj. je lživá v každém modelu T .
- Formule φ je **nezávislá v T** , pokud není pravdivá v T ani lživá v T .
- Je-li $T = \emptyset$, je $M(T) = M(L)$ a teorii T vynecháváme, případně říkáme “v logice”. Pak $\models \varphi$ značí, že φ je **pravdivá** ((**logicky**) **platí**, **tautologie**).
- **Důsledek** T je množina $\theta^L(T)$ všech **sentencí** jazyka L pravdivých v T , tj.

$$\theta^L(T) = \{\varphi \in \text{Fm}_L \mid T \models \varphi \text{ a } \varphi \text{ je sentence}\}.$$

Příklad teorie

Teorie uspořádání T jazyka $L = \langle \leq \rangle$ s rovností má axiomy

$$x \leq x \quad (\text{reflexivita})$$

$$x \leq y \wedge y \leq x \rightarrow x = y \quad (\text{antisymetrie})$$

$$x \leq y \wedge y \leq z \rightarrow x \leq z \quad (\text{tranzitivita})$$

Modely T jsou L -struktury $\langle S, \leq_S \rangle$, tzv. **uspořádané množiny**, ve kterých platí axiomy T , např. $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$ nebo $\mathcal{B} = \langle \mathcal{P}(X), \subseteq \rangle$ pro $X = \{0, 1, 2\}$.

- Formule φ ve tvaru $x \leq y \vee y \leq x$ platí v $\mathcal{A}$, ale neplatí v $\mathcal{B}$, neboť např. $\mathcal{B} \not\models \varphi[e]$ při ohodnocení $e(x) = \{0\}$, $e(y) = \{1\}$, je tedy nezávislá v T .
- Sentence ψ ve tvaru $(\exists x)(\forall y)(y \leq x)$ je pravdivá v $\mathcal{B}$ a lživá v $\mathcal{A}$, je tedy rovněž nezávislá v T . Píšeme $\mathcal{B} \models \psi$, $\mathcal{A} \models \neg\psi$.
- Formule χ ve tvaru $(x \leq y \wedge y \leq z \wedge z \leq x) \rightarrow (x = y \wedge y = z)$ je pravdivá v T , píšeme $T \models \chi$, totéž platí pro její **generální uzávěr**.

Výroková a predikátová logika - VII

Petr Gregor

KTIML MFF UK

ZS 2021/22

Platnost v teorii a logická platnost

- **Teorie** jazyka L je libovolná množina T formulí jazyka L (tzv. **axiomů**).
- **Model teorie** T je L -struktura $\mathcal{A}$ taková, že $\mathcal{A} \models \varphi$ pro každé $\varphi \in T$, značíme $\mathcal{A} \models T$.
- **Třída modelů** teorie T je $M(T) = \{\mathcal{A} \in M(L) \mid \mathcal{A} \models T\}$.
- Formule φ je **pravdivá v T** (**platí v T**), značíme $T \models \varphi$, pokud $\mathcal{A} \models \varphi$ pro každý model $\mathcal{A}$ teorie T . V opačném případě píšeme $T \not\models \varphi$.
- Formule φ je **lživá v T** , pokud $T \models \neg\varphi$, tj. je lživá v každém modelu T .
- Formule φ je **nezávislá v T** , pokud není pravdivá v T ani lživá v T .
- Je-li $T = \emptyset$, je $M(T) = M(L)$ a teorii T vynecháváme, případně říkáme “v logice”. Pak $\models \varphi$ značí, že φ je **pravdivá** ((**logicky**) **platí**, **tautologie**).
- **Důsledek** T je množina $\theta^L(T)$ všech **sentencí** jazyka L pravdivých v T , tj.

$$\theta^L(T) = \{\varphi \in \text{Fm}_L \mid T \models \varphi \text{ a } \varphi \text{ je sentence}\}.$$

Příklad teorie

Teorie uspořádání T jazyka $L = \langle \leq \rangle$ s rovností má axiomy

$$x \leq x \quad (\text{reflexivita})$$

$$x \leq y \wedge y \leq x \rightarrow x = y \quad (\text{antisymetrie})$$

$$x \leq y \wedge y \leq z \rightarrow x \leq z \quad (\text{tranzitivita})$$

Modely T jsou L -struktury $\langle S, \leq_S \rangle$, tzv. **uspořádané množiny**, ve kterých platí axiomy T , např. $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$ nebo $\mathcal{B} = \langle \mathcal{P}(X), \subseteq \rangle$ pro $X = \{0, 1, 2\}$.

- Formule φ ve tvaru $x \leq y \vee y \leq x$ platí v $\mathcal{A}$, ale neplatí v $\mathcal{B}$, neboť např. $\mathcal{B} \not\models \varphi[e]$ při ohodnocení $e(x) = \{0\}$, $e(y) = \{1\}$, je tedy nezávislá v T .
- Sentence ψ ve tvaru $(\exists x)(\forall y)(y \leq x)$ je pravdivá v $\mathcal{B}$ a lživá v $\mathcal{A}$, je tedy rovněž nezávislá v T . Píšeme $\mathcal{B} \models \psi$, $\mathcal{A} \models \neg\psi$.
- Formule χ ve tvaru $(x \leq y \wedge y \leq z \wedge z \leq x) \rightarrow (x = y \wedge y = z)$ je pravdivá v T , píšeme $T \models \chi$, totéž platí pro její **generální uzávěr**.

Nesplnitelnost a pravdivost

Problém pravdivosti v teorii lze převést na problém existence modelu.

Tvrzení Pro každou teorii T a *sentenci* φ (stejného jazyka)

$$T, \neg\varphi \text{ nemá model} \Leftrightarrow T \models \varphi.$$

Důkaz Z definic plynou ekvivalence následujících tvrzení.

- (1) $T, \neg\varphi$ nemá model,
- (2) $\neg\varphi$ neplatí v žádném modelu teorie T ,
- (3) φ platí v každém modelu teorie T ,
- (4) $T \models \varphi$. $\square$

Poznámka Předpoklad, že φ je sentence, je nutný pro (2) $\Leftrightarrow$ (3).

Např. teorie $\{P(c), \neg P(x)\}$ nemá model, ale $P(c) \not\models P(x)$, kde P je unární relační symbol a c je konstantní symbol.

Základní algebraické teorie - příklady

- **Teorie grup** nad jazykem $L = \langle +, -, 0 \rangle$ s rovností má axiomy

$$x + (y + z) = (x + y) + z \quad (\text{asociativita } +)$$

$$0 + x = x = x + 0 \quad (\text{neutralita } 0 \text{ k } +)$$

$$x + (-x) = 0 = (-x) + x \quad (-x \text{ je inverzní prvek k } x)$$

- **Teorie komutativních grup** má navíc ax. $x + y = y + x$ (komutativita +)

- **Teorie okruhů** je jazyka $L = \langle +, -, \cdot, 0, 1 \rangle$ s rovností, má navíc axiomy

$$1 \cdot x = x = x \cdot 1 \quad (\text{neutralita } 1 \text{ k } \cdot)$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad (\text{asociativita } \cdot)$$

$$x \cdot (y + z) = x \cdot y + x \cdot z, (x + y) \cdot z = x \cdot z + y \cdot z \quad (\text{distributivita } \cdot \text{ k } +)$$

- **Teorie komutativních okruhů** má navíc ax. $x \cdot y = y \cdot x$ (komutativita $\cdot$)

- **Teorie těles** stejného jazyka má navíc axiomy

$$x \neq 0 \rightarrow (\exists y)(x \cdot y = 1) \quad (\text{existence inverzního prvku k } \cdot)$$

$$0 \neq 1 \quad (\text{netrivialita})$$

Vlastnosti teorií

Teorie T jazyka L je (*sémanticky*)

- *sporná*, jestliže v ní platí $\perp$ (spor), jinak je *bezesporná* (*splnitelná*),
- *kompletní*, jestliže není sporná a každá *sentence* je v ní pravdivá či lživá,
- *extenze* teorie T' jazyka L' , jestliže $L' \subseteq L$ a $\theta^{L'}(T') \subseteq \theta^L(T)$,
o extenzi T teorie T' řekneme, že je *jednoduchá*, pokud $L = L'$, a
konzervativní, pokud $\theta^{L'}(T') = \theta^L(T) \cap \text{Fm}_{L'}$,
- *ekvivalentní* s teorií T' , jestliže T je extenzí T' a T' je extenzí T ,

Struktury $\mathcal{A}, \mathcal{B}$ pro jazyk L jsou *elementárně ekvivalentní*, značeno $\mathcal{A} \equiv \mathcal{B}$, platí-li v nich stejné formule.

Pozorování Necht' T a T' jsou teorie jazyka L . Teorie T je (*sémanticky*)

- (1) *bezesporná*, právě když má model,
- (2) *kompletní*, právě když má až na *elementární ekvivalenci* jediný model,
- (3) *extenze* T' , právě když $M(T) \subseteq M(T')$,
- (4) *ekvivalentní* s T' , právě když $M(T) = M(T')$.

Podstruktura

Nechť $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ a $\mathcal{B} = \langle B, \mathcal{R}^B, \mathcal{F}^B \rangle$ jsou struktury pro jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$.

Řekneme, že $\mathcal{B}$ je (indukovaná) **podstruktura** $\mathcal{A}$, značeno $\mathcal{B} \subseteq \mathcal{A}$, pokud

- (i) $B \subseteq A$,
- (ii) $R^B = R^A \cap B^{\text{ar}(R)}$ pro každé $R \in \mathcal{R}$,
- (iii) $f^B = f^A \cap (B^{\text{ar}(f)} \times B)$, tj. $f^B = f^A \upharpoonright B^{\text{ar}(f)}$, pro každé $f \in \mathcal{F}$.

Pozorování Množina $C \subseteq A$ je doménou nějaké podstruktury struktury $\mathcal{A}$, právě když C je **uzavřená** na všechny funkce struktury $\mathcal{A}$ (včetně konstant).

- Pak příslušnou podstrukturu značíme $\mathcal{A} \upharpoonright C$ a říkáme, že je to **restrikce** (**parcializace**) struktury $\mathcal{A}$ na C .
- Množina $C \subseteq A$ je **uzavřená** na funkci $f: A^n \rightarrow A$, pokud $f(x_1, \dots, x_n) \in C$ pro každé $x_1, \dots, x_n \in C$.

Např. $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$ je podstrukturou $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$ a lze psát $\underline{\mathbb{Z}} = \underline{\mathbb{Q}} \upharpoonright \mathbb{Z}$.

Dále $\underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$ je jejich podstrukturou a $\underline{\mathbb{N}} = \underline{\mathbb{Q}} \upharpoonright \mathbb{N} = \underline{\mathbb{Z}} \upharpoonright \mathbb{N}$.

Platnost v podstruktuře

Nechť $\mathcal{B}$ je podstruktura struktury $\mathcal{A}$ pro (pevný) jazyk L .

Tvrzení Pro každou *otevřenou* formuli φ a ohodnocení $e: \text{Var} \rightarrow B$ platí

$$\mathcal{B} \models \varphi[e] \quad \text{právě když} \quad \mathcal{A} \models \varphi[e].$$

Důkaz Je-li φ atomická, plyne tvrzení z definice platnosti při ohodnocení. Dále snadno indukcí dle struktury formule. $\square$

Důsledek *Otevřená* formule platí ve struktuře $\mathcal{A}$, právě když platí v každé podstruktuře $\mathcal{B} \subseteq \mathcal{A}$.

- Teorie T je *otevřená*, jsou-li všechny její axiomy otevřené formule.

Důsledek Každá podstruktura modelu *otevřené* teorie T je modelem T .

Např. každá podstruktura grafu, tj. modelu teorie grafů, je rovněž grafem, zveme ho *podgraf*. Obdobně např. podgrupa nebo Booleova podalgebra.

Generovaná podstruktura, expanze, redukt

Nechť $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ je struktura a $X \subseteq A$. Označme B **nejmenší** podmnožinu množiny A obsahující X , která je **uzavřená** na všechny funkce struktury $\mathcal{A}$ (včetně konstant). Pak strukturu $\mathcal{A} \upharpoonright B$ značíme rovněž $\mathcal{A}\langle X \rangle$ a podstruktura říkáme, že je to $\mathcal{A}$ **generovaná** množinou X .

Např. pro $\mathbb{Q} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$, $\mathbb{Z} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$ a $\mathbb{N} = \langle \mathbb{N}, +, \cdot, 0 \rangle$ je $\mathbb{Q}\langle \{1\} \rangle = \mathbb{N}$, $\mathbb{Q}\langle \{-1\} \rangle = \mathbb{Z}$ a $\mathbb{Q}\langle \{2\} \rangle$ je podstruktura na všech sudých přirozených číslech.

Nechť $\mathcal{A}'$ je struktura pro jazyk L' a $L \subseteq L'$ je jazyk. Odebráním realizací symbolů, jež nejsou v L , získáme z $\mathcal{A}'$ strukturu $\mathcal{A}$, kterou nazýváme **redukt** struktury $\mathcal{A}'$ na jazyk L . Obráceně, $\mathcal{A}'$ je **expanze** struktury $\mathcal{A}$ do jazyka L' .

*Např. $\langle \mathbb{N}, + \rangle$ je redukt $\langle \mathbb{N}, +, \cdot, 0 \rangle$. Naopak, struktura $\langle \mathbb{N}, +, c_i \rangle_{i \in \mathbb{N}}$ taková, že $c_i = i$ pro všechna $i \in \mathbb{N}$, je expanze $\langle \mathbb{N}, + \rangle$ o **jména prvků** z $\mathbb{N}$.*

Věta o konstantách

Věta *Nechť φ je formule jazyka L s volnými proměnnými $x_1, \dots, x_n$ a T je teorie jazyka L . Označme L' rozšíření L o nové konstantní symboly $c_1, \dots, c_n$ a T' teorii T nad jazykem L' . Pak*

$$T \models \varphi \quad \text{právě když} \quad T' \models \varphi(x_1/c_1, \dots, x_n/c_n).$$

Důkaz ($\Rightarrow$) Je-li $\mathcal{A}'$ model teorie T' , nechť $\mathcal{A}$ je **redukt** $\mathcal{A}'$ na L . Jelikož $\mathcal{A} \models \varphi[e]$ pro každé ohodnocení e , platí i

$$\mathcal{A} \models \varphi[e(x_1/c_1^{A'}, \dots, x_n/c_n^{A'})], \quad \text{tj.} \quad \mathcal{A}' \models \varphi(x_1/c_1, \dots, x_n/c_n).$$

($\Leftarrow$) Je-li $\mathcal{A}$ model teorie T a e ohodnocení, nechť $\mathcal{A}'$ je **expanze** $\mathcal{A}$ na L' o konstanty $c_i^{A'} = e(x_i)$ pro všechna i . Jelikož $\mathcal{A}' \models \varphi(x_1/c_1, \dots, x_n/c_n)[e']$ pro libovolné ohodnocení e' , platí i

$$\mathcal{A}' \models \varphi[e(x_1/c_1^{A'}, \dots, x_n/c_n^{A'})], \quad \text{tj.} \quad \mathcal{A} \models \varphi[e]. \quad \square$$

Definovatelné množiny

Zajímá nás, které množiny lze v dané struktuře zadefinovat.

- **Množina definovaná formulí** $\varphi(x_1, \dots, x_n)$ **ve struktuře** $\mathcal{A}$ je množina

$$\varphi^{\mathcal{A}}(x_1, \dots, x_n) = \{(a_1, \dots, a_n) \in A^n \mid \mathcal{A} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]\}.$$

Zkráceným zápisem, $\varphi^{\mathcal{A}}(\bar{x}) = \{\bar{a} \in A^{|\bar{x}|} \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a})]\}$, kde $|\bar{x}| = n$.

- **Množina definovaná formulí** $\varphi(\bar{x}, \bar{y})$ **s parametry** $\bar{b} \in A^{|\bar{y}|}$ **ve struktuře** $\mathcal{A}$ je

$$\varphi^{\mathcal{A}, \bar{b}}(\bar{x}, \bar{y}) = \{\bar{a} \in A^{|\bar{x}|} \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a}, \bar{y}/\bar{b})]\}.$$

Např. pro $\varphi = E(x, y)$ je $\varphi^{\mathcal{G}, b}(x, y)$ množina sousedů vrcholu b v grafu $\mathcal{G}$.

- Pro strukturu $\mathcal{A}$, množinu $B \subseteq A$ a $n \in \mathbb{N}$ označme $\text{Df}^n(\mathcal{A}, B)$ třídu všech množin $D \subseteq A^n$ definovatelných ve struktuře $\mathcal{A}$ s parametry z B .

Pozorování $\text{Df}^n(\mathcal{A}, B)$ je uzavřená na doplněk, sjednocení, průnik a obsahuje $\emptyset, A^n$. Tedy tvoří podalgebru potenční algebry $\mathcal{P}(A^n)$.

Příklad - databázové dotazy

<i>Filmy</i>	<i>název</i>	<i>režisér</i>	<i>herec</i>	<i>Program</i>	<i>kino</i>	<i>název</i>	<i>čas</i>
	Lidé z Maringotek	M. Frič	J. Tříška		Světovozor	Po strništi bos	13:15
	Po strništi bos	J. Svěrák	Z. Svěrák		Mat	Po strništi bos	16:15
	Po strništi bos	J. Svěrák	J. Tříška		Mat	Lidé z Maringotek	18:30
	...	...	...		...	...	...

Kde a kdy mohu dnes vidět film s Janem Třískou?

select *Program.kino, Program.čas* **from** *Filmy, Program*
where *Filmy.název = Program.název* **and** *herec = 'J. Tříška'*;

Totéž dostaneme jako množinu $\varphi^D(x, y)$ definovanou formulí $\varphi(x, y)$

$$(\exists n)(\exists r)(P(x, n, y) \wedge F(n, r, \text{'J. Tříška'}))$$

ve struktuře $\mathcal{D} = \langle D, \textit{Filmy}, \textit{Program}, c^D \rangle_{c \in D}$ jazyka $L = \langle F, P, c \rangle_{c \in D}$, kde $D = \{\text{'Po strništi bos'}, \text{'J. Tříška'}, \text{'Mat'}, \text{'13:15'}, \dots\}$ a $c^D = c$ pro každé $c \in D$.

Booleovy algebry

Teorie *Booleových algeber* jazyka $L = \langle -, \wedge, \vee, 0, 1 \rangle$ s rovností má axiomy

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \quad (\text{asociativita } \wedge)$$

$$x \vee (y \vee z) = (x \vee y) \vee z \quad (\text{asociativita } \vee)$$

$$x \wedge y = y \wedge x \quad (\text{komutativita } \wedge)$$

$$x \vee y = y \vee x \quad (\text{komutativita } \vee)$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad (\text{distributivita } \wedge \text{ k } \vee)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad (\text{distributivita } \vee \text{ k } \wedge)$$

$$x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x \quad (\text{absorbce})$$

$$x \vee (-x) = 1, \quad x \wedge (-x) = 0 \quad (\text{komplementace})$$

$$0 \neq 1 \quad (\text{netrivialita})$$

Nejmenší model je $\underline{2} = \langle 2, -, \wedge_1, \vee_1, 0, 1 \rangle$. Konečné Booleovy algebry jsou (až na izomorfismus) právě $\underline{n} = \langle n, -, \wedge_n, \vee_n, 0_n, 1_n \rangle$ pro $n \in \mathbb{N}^+$, kde jednotlivé operace (na binárních n -ticích) jsou operace z $\underline{2}$ “po složkách”.

Vztah výrokové a predikátové logiky

- Výrokové formule s (*univerzálními*) spojky $\neg, \wedge, \vee$ (případně s $\top, \perp$) lze považovat za **Booleovské termy**. Hodnota výroku φ při daném ohodnocení je pak hodnotou termu v Booleově algebře $\underline{2}$.
- **Algebra výroků** nad $\mathbb{P}$ je Booleova algebra (i pro $\mathbb{P}$ nekonečné).
- Reprezentujeme-li atomické formule v **otevřené** formuli φ (bez rovnosti) pomocí prvovýroků, získáme výrokovou formuli, která je pravdivá, právě když φ je pravdivá.
- Výrokovou logiku lze zavést jako **fragment** predikátové logiky pomocí **nulárních** relačních symbolů (*syntax*) a nulárních relací (*sémantika*), přičemž $A^0 = \{\emptyset\} = 1$ a tedy $R^A \subseteq A^0$ je $R^A = \emptyset = 0$ anebo $R^A = \{\emptyset\} = 1$.

Tablo metoda v PL - rozdíly

- Formule v položkách budou **sentence** (**uzavřené** formule), tj. formule bez volných proměnných.
- Přidáme **nová atomická tabla** pro kvantifikátory.
- Za kvantifikované proměnné se budou substituovat **konstantní termy** dle jistých pravidel.
- Jazyk rozšíříme o **nové (pomocné) konstantní symboly** (spočetně mnoho) pro reprezentaci “svědků” položek $T(\exists x)\varphi(x)$ a $F(\forall x)\varphi(x)$.
- V **dokončené** bezesporné větvi s položkou $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$ budou **instance** $T\varphi(x/t)$ resp. $F\varphi(x/t)$ pro každý konstantní term t (rozšířeného jazyka).

Tablo v PL - příklady

$$F((\exists x)\neg P(x) \rightarrow \neg(\forall x)P(x))$$

$$\begin{array}{c}
 | \\
 T(\exists x)\neg P(x) \\
 | \\
 F(\neg(\forall x)P(x)) \\
 | \\
 T(\forall x)P(x) \\
 | \\
 T(\neg P(c)) \quad c \text{ nové} \\
 | \\
 \textcolor{red}{FP(c)} \\
 | \\
 T(\forall x)P(x) \\
 | \\
 \textcolor{red}{TP(c)} \\
 | \\
 \otimes
 \end{array}$$

$$F(\neg(\forall x)P(x) \rightarrow (\exists x)\neg P(x))$$

$$\begin{array}{c}
 | \\
 T(\neg(\forall x)P(x)) \\
 | \\
 F(\exists x)\neg P(x) \\
 | \\
 F(\forall x)P(x) \\
 | \\
 \textcolor{red}{FP(d)} \quad d \text{ nové} \\
 | \\
 F(\exists x)\neg P(x) \\
 | \\
 F(\neg P(d)) \\
 | \\
 \textcolor{red}{TP(d)} \\
 | \\
 \otimes
 \end{array}$$

Výroková a predikátová logika - VIII

Petr Gregor

KTIML MFF UK

ZS 2021/22

Tablo metoda ve VL - opakování

- **Tablo** je binární strom reprezentující vyhledávání *protipříkladu*.
- Vrcholy jsou označeny **položkami**, tj. formulami s **příznakem** T / F , který reprezentuje předpoklad, že formule v nějakém modelu platí / neplatí.
- Je-li tento předpoklad správný, je správný i v nějaké větvi pod ní.
- Větev je **sporná** (selže), pokud obsahuje $T\psi$, $F\psi$ pro nějaké ψ .
- **Důkaz** formule φ je **sporné** tablo s kořenem $F\varphi$, tj. tablo v němž každá větev je sporná (nebyl nalezen protipříklad), pak φ je pravdivá.
- Pokud protipříklad existuje, v **dokončeném** tablu bude větev, která ho **poskytuje**, tato větev může být nekonečná.
- Lze zkonstruovat **systematické tablo**, jež je vždy dokončené.
- Pokud je φ pravdivá, systematické tablo pro φ je sporné, tj. důkazem φ , v tom případě je i **konečné**.

Tablo metoda v PL - rozdíly

- Formule v položkách budou **sentence** (**uzavřené** formule), tj. formule bez volných proměnných.
- Přidáme **nová atomická tabla** pro kvantifikátory.
- Za kvantifikované proměnné se budou substituovat **konstantní termy** dle jistých pravidel.
- Jazyk rozšíříme o **nové (pomocné) konstantní symboly** (spočetně mnoho) pro reprezentaci “svědků” položek $T(\exists x)\varphi(x)$ a $F(\forall x)\varphi(x)$.
- V **dokončené** bezesporné větvi s položkou $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$ budou **instance** $T\varphi(x/t)$ resp. $F\varphi(x/t)$ pro každý konstantní term t (rozšířeného jazyka).

Tablo v PL - příklady

$$F((\exists x)\neg P(x) \rightarrow \neg(\forall x)P(x))$$

$$\begin{array}{c}
 | \\
 T(\exists x)\neg P(x) \\
 | \\
 F(\neg(\forall x)P(x)) \\
 | \\
 T(\forall x)P(x) \\
 | \\
 T(\neg P(c)) \quad c \text{ nové} \\
 | \\
 \textcolor{red}{FP(c)} \\
 | \\
 T(\forall x)P(x) \\
 | \\
 \textcolor{red}{TP(c)} \\
 | \\
 \otimes
 \end{array}$$

$$F(\neg(\forall x)P(x) \rightarrow (\exists x)\neg P(x))$$

$$\begin{array}{c}
 | \\
 T(\neg(\forall x)P(x)) \\
 | \\
 F(\exists x)\neg P(x) \\
 | \\
 F(\forall x)P(x) \\
 | \\
 \textcolor{red}{FP(d)} \quad d \text{ nové} \\
 | \\
 F(\exists x)\neg P(x) \\
 | \\
 F(\neg P(d)) \\
 | \\
 \textcolor{red}{TP(d)} \\
 | \\
 \otimes
 \end{array}$$

Předpoklady

- 1) *Dokazovaná formule φ je **sentence**.* Není-li φ sentence, můžeme ji nahradit za její **generální uzávěr** φ' , neboť pro každou teorii T ,

$$T \models \varphi \quad \text{právě když} \quad T \models \varphi'.$$

- 2) *Dokazujeme z teorie v **uzavřeném tvaru**, tj. každý axiom je sentence.* Nahrazením každého axiomu ψ za jeho generální uzávěr ψ' získáme **ekvivalentní** teorii, neboť pro každou strukturu $\mathcal{A}$ (daného jazyka L),

$$\mathcal{A} \models \psi \quad \text{právě když} \quad \mathcal{A} \models \psi'.$$

- 3) *Jazyk L je **spočetný**.* Pak každá teorie nad L je spočetná. Označme L_C rozšíření jazyka L o nové konstantní symboly $c_0, c_1, \dots$ (spočetně nekonečně mnoho). Platí, že konstantních termů jazyka L_C je spočetně. Necht' t_i označuje i -tý konstantní term (v pevně zvoleném **očíslování**).

- 4) *Zatím budeme předpokládat, že jazyk je **bez rovnosti**.*

Atomická tabla - původní

Atomická tabla jsou všechny následující (položkami značkové) stromy, kde α je libovolná atomická sentence a φ, ψ jsou libovolné sentence, vše v L_C .

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

Atomická tabla - nová

Atomická tabla jsou i následující (položkami značkové) stromy, kde φ je libovolná formule jazyka L_C ve volné proměnné x , t je libovolný konstantní term jazyka L_C a c je **nový** konstantní symbol z $L_C \setminus L$.

#	*	*	#
$T(\forall x)\varphi(x)$	$F(\forall x)\varphi(x)$	$T(\exists x)\varphi(x)$	$F(\exists x)\varphi(x)$
$T\varphi(x/t)$	$F\varphi(x/c)$	$T\varphi(x/c)$	$F\varphi(x/t)$
pro libovolný konst. term t	pro <i>novou</i> konstantu c	pro <i>novou</i> konstantu c	pro libovolný konst. term t

Poznámka Konstantní symbol c reprezentuje “svědka” položky $T(\exists x)\varphi(x)$ či $F(\forall x)\varphi(x)$. Jelikož nechceme, aby na c byly kladeny další požadavky, je v definici tabla omezeno, jaký konstantní symbol c lze použít.

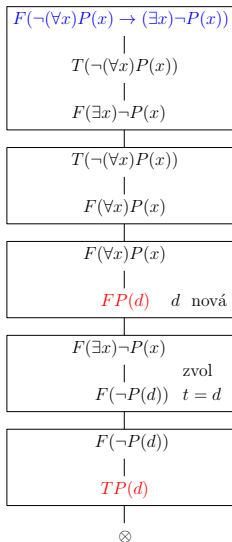
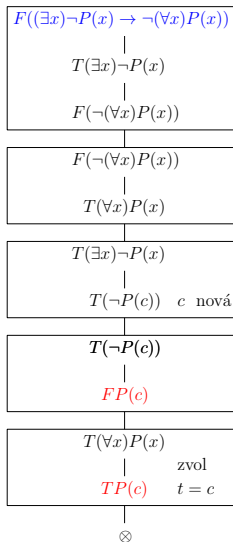
Tablo

Konečné tablo z teorie T je binární, položkami značkový strom s předpisem

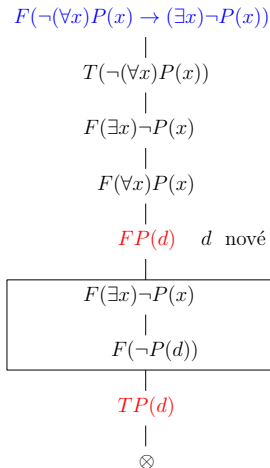
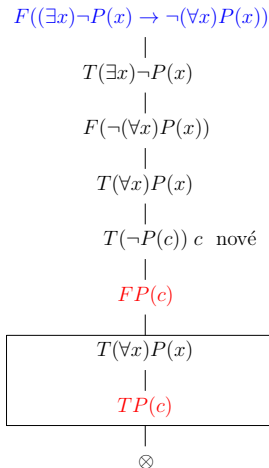
- (i) každé atomické tablo je konečné tablo z T , přičemž v případě $(*)$ lze použít libovolný konstantní symbol $c \in L_C \setminus L$,
- (ii) je-li P položka na větvi V konečného tabla z T , pak připojením atomického tabla pro P na **konec větve** V vznikne konečné tablo z T , přičemž v případě $(*)$ lze použít pouze konstantní symbol $c \in L_C \setminus L$, který se dosud **nevyskytuje** na V ,
- (iii) je-li V větev konečného tabla z T a $\varphi \in T$, pak připojením **$T\varphi$** na konec větve V vznikne rovněž konečné tablo z T .
- (iv) každé konečné tablo z T vznikne **konečným** užitím pravidel (i), (ii), (iii).

Tablo z teorie T je posloupnost $\tau_0, \tau_1, \dots, \tau_n, \dots$ konečných tabel z T takových, že τ_{n+1} vznikne z τ_n pomocí (ii) či (iii), formálně $\tau = \cup \tau_n$.

Konstrukce tabla



Konvence



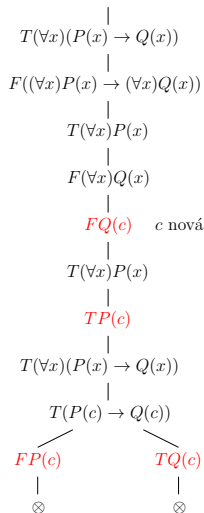
Položku, dle které tablo prodlužujeme, nebudeme na větev znovu zapisovat kromě případů, kdy položka je tvaru $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$.

Tablo důkaz

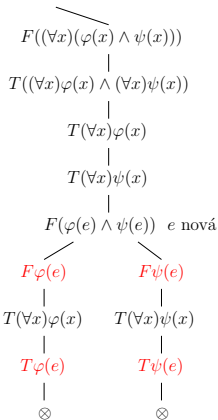
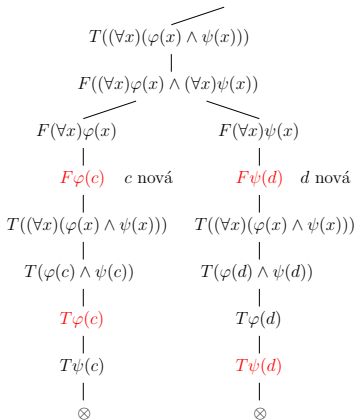
- Větev V tabla τ je *sporná*, obsahuje-li položky $T\varphi$ a $F\varphi$ pro nějakou sentenci φ , jinak je *bezesporná*.
- Tablo τ je *sporné*, pokud je každá jeho větev sporná.
- *Tablo důkaz* (*důkaz tablem*) sentence φ z teorie T je *sporné tablo* z T s položkou $F\varphi$ v kořeni.
- φ je (*tablo*) *dokazatelná* z teorie T , píšeme $T \vdash \varphi$, má-li tablo důkaz z T .
- *Zamítnutí* sentence φ *tablem* z teorie T je *sporné tablo* z T s položkou $T\varphi$ v kořeni.
- Sentence φ je (*tablo*) *zamítnutelná* z teorie T , má-li zamítnutí tablem z T , tj. $T \vdash \neg\varphi$.

Příklady

$$F((\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)P(x) \rightarrow (\forall x)Q(x)))$$



$$F((\forall x)(\varphi(x) \wedge \psi(x)) \leftrightarrow ((\forall x)\varphi(x) \wedge (\forall x)\psi(x)))$$



Dokončené tablo

Chceme, aby dokončená bezesporná větev poskytovala *protipříklad*.

Výskyt položky P ve vrcholu v tabla τ je *i-tý*, pokud v má v τ právě $i - 1$ předků označených P a je *redukovaný* na větvi V skrze v , pokud

- a) P není tvaru $T(\forall x)\varphi(x)$ ani $F(\exists x)\varphi(x)$ a P se vyskytuje na V jako kořen atomického tabla, tj. při konstrukci τ již došlo k rozvoji P na V , nebo
- b) P je tvaru $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$, má $(i + 1)$ -ní výskyt na V a zároveň se na V vyskytuje $T\varphi(x/t_i)$ resp. $F\varphi(x/t_i)$, kde t_i je i -tý konstantní term (jazyka L_C).

Nechť V je větev tabla τ z teorie T . Řekneme, že

- větev V je *dokončená*, je-li sporná, nebo každý výskyt položky na V je redukovaný na V a navíc V obsahuje $T\varphi$ pro každé $\varphi \in T$,
- tablo τ je *dokončené*, pokud je každá jeho větev dokončená.

Systematické tablo - konstrukce

Nechť R je položka a $T = \{\varphi_0, \varphi_1, \dots\}$ je (konečná či nekonečná) teorie.

- (1) Za τ_0 vezmi atomické tablo pro R . V případě $(*)$ vezmi lib. $c \in L_C \setminus L$, v případě $(\#)$ za t vezmi term t_1 . Dokud to lze, aplikuj následující kroky.
- (2) Nechť v je **nejlevější** vrchol v co **nejmenší** úrovni již daného tabla τ_n obsahující výskyt položky P , který není redukovaný na nějaké bezesporné větvi **skrže** v . (Neexistuje-li v , vezmi $\tau'_n = \tau_n$ a jdi na (4).)
- (3a) Není-li P tvaru $T(\forall x)\varphi(x)$ ani $F(\exists x)\varphi(x)$, za τ'_n vezmi tablo vzniklé z τ_n přidáním atomického tabla pro P na každou bezespornou větev skrže v . V případě $(*)$ za c vezmi c_i pro nejmenší možné i .
- (3b) Je-li P tvaru $T(\forall x)\varphi(x)$ či $F(\exists x)\varphi(x)$ a ve v má i -tý výskyt, za τ'_n vezmi tablo vzniklé z τ_n připojením atomického tabla pro P na každou bezespornou větev skrže v , přičemž za t vezmi term t_i .
- (4) Za τ_{n+1} vezmi tablo vzniklé z τ'_n přidáním $T\varphi_n$ na každou bezespornou větev neobsahující $T\varphi_n$. (Neexistuje-li φ_n , vezmi $\tau_{n+1} = \tau'_n$.)

Systematické tablo z T pro R je výsledkem uvedené konstrukce, tj. $\tau = \bigcup \tau_n$.

Systematické tablo - příklad

$$T((\exists y)(\neg R(y, y) \vee P(y, y)) \wedge (\forall x)R(x, x))$$

$$T(\exists y)(\neg R(y, y) \vee P(y, y))$$

$$T(\forall x)R(x, x)$$

$$T(\neg R(c_0, c_0) \vee P(c_0, c_0)) \quad c_0 \text{ nová}$$

$$T(\forall x)R(x, x)$$

$$TR(c_0, c_0)$$

(za předpokladu $t_1 = c_0$)

$$T(\neg R(c_0, c_0))$$

$$TP(c_0, c_0)$$

$$T(\forall x)R(x, x)$$

$$T(\forall x)R(x, x)$$

$$TR(t_2, t_2)$$

$$TR(t_2, t_2)$$

$$FR(c_0, c_0)$$

$$T(\forall x)R(x, x)$$

$$\otimes$$

$$TR(t_3, t_3)$$

⋮

Systematické tablo - dokončenost

Tvrzení Pro každou teorii T a položku R je systematické tablo τ **dokončené**.

Důkaz Nechť $\tau = \cup \tau_n$ je systematické tablo z $T = \{\varphi_0, \varphi_1, \dots\}$ s R v kořeni a nechť P je položka ve vrcholu v tabla τ .

- Do úrovně v (včetně) je v τ jen konečně mnoho výskytů všech položek.
- Kdyby výskyt P ve v byl neredukovaný na nějaké bezesporné větvi v τ , byl by vybrán v nějakém kroku (2) a zredukován v (3a) či (3b).
- Každá $\varphi_n \in T$ bude dle (4) nejpozději v τ_{n+1} na každé bezesporné větvi.
- Tedy systematické tablo τ obsahuje pouze dokončené větve. $\square$

Tvrzení Je-li systematické tablo τ důkazem (z teorie T), je τ konečné.

Důkaz Kdyby bylo τ nekonečné, dle **Königova lemmatu** by obsahovalo nekonečnou větev. Tato větev by byla bezesporná, neboť při konstrukci τ se sporné větve neprodlužují. Pak by ale τ nebylo sporné. $\square$

Tablo metoda v jazyce s rovností

Axiomy rovnosti pro jazyk L s rovností jsou

(i) $x = x$

(ii) $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n)$
pro každý n -ární funkční symbol f jazyka L .

(iii) $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow (R(x_1, \dots, x_n) \rightarrow R(y_1, \dots, y_n))$
pro každý n -ární relační symbol R jazyka L včetně $=$.

Tablo důkaz z teorie T jazyka L *s rovností* je tablo důkaz z teorie T^* , kde T^* je rozšíření teorie T o axiomy rovnosti pro L (resp. jejich generální uzávěry).

Poznámka V kontextu logického programování má rovnost často jiný význam než v matematice (identita). Např. v Prologu $t_1 = t_2$ znamená, že t_1 a t_2 jsou unifikovatelné.

Kongruence a faktorstruktura

Nechť $\sim$ je ekvivalence na A , $f : A^n \rightarrow A$ a $R \subseteq A^n$, kde $n \in \mathbb{N}$. Pak $\sim$ je

- **kongruence pro funkci** f , pokud pro každé $x_1, \dots, x_n, y_1, \dots, y_n \in A$ platí

$$x_1 \sim y_1 \wedge \dots \wedge x_n \sim y_n \Rightarrow f(x_1, \dots, x_n) \sim f(y_1, \dots, y_n),$$
- **kongruence pro relaci** R , pokud pro každé $x_1, \dots, x_n, y_1, \dots, y_n \in A$ platí

$$x_1 \sim y_1 \wedge \dots \wedge x_n \sim y_n \Rightarrow (R(x_1, \dots, x_n) \Leftrightarrow R(y_1, \dots, y_n)).$$

Nechť ekvivalence $\sim$ na A je kongruence pro každou funkci i relaci struktury

$\mathcal{A} = \langle A, \mathcal{F}^A, \mathcal{R}^A \rangle$ pro jazyk $L = \langle \mathcal{F}, \mathcal{R} \rangle$. **Faktorstruktura** (**podílová struktura**)

struktury $\mathcal{A}$ dle $\sim$ je struktura $\mathcal{A}/\sim = \langle A/\sim, \mathcal{F}^{A/\sim}, \mathcal{R}^{A/\sim} \rangle$, kde

$$f^{A/\sim}([x_1]_{\sim}, \dots, [x_n]_{\sim}) = [f^A(x_1, \dots, x_n)]_{\sim}$$

$$R^{A/\sim}([x_1]_{\sim}, \dots, [x_n]_{\sim}) \Leftrightarrow R^A(x_1, \dots, x_n)$$

pro každé $f \in \mathcal{F}$, $R \in \mathcal{R}$ a $x_1, \dots, x_n \in A$, tj. funkce a relace jsou definované z $\mathcal{A}$ pomocí **reprezentantů**.

Např. $\mathbb{Z}_p$ je faktorstruktura $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$ dle kongruence modulo p .

Význam axiomů rovnosti

Nechť $\mathcal{A}$ je struktura pro jazyk L , ve které je rovnost interpretovaná jako relace $=^A$ splňující axiomy rovnosti, tj. ne nutně identita.

- 1) Z axiomů (i) a (iii) plyne, že relace $=^A$ je **ekvivalence** na A .
- 2) Axiomy (ii) a (iii) vyjadřují, že relace $=^A$ je **kongruence** pro každou funkci a relaci v $\mathcal{A}$.
- 3) Je-li $\mathcal{A} \models T^*$, je i $(\mathcal{A}/=^A) \models T^*$, kde $\mathcal{A}/=^A$ je **faktorstruktura** struktury $\mathcal{A}$ dle $=^A$, přičemž rovnost je v $\mathcal{A}/=^A$ interpretovaná jako identita.

Na druhou stranu, v každém modelu, v kterém je rovnost interpretovaná jako identita, všechny axiomy rovnosti evidentně platí.

Korektnost

Řekneme, že struktura $\mathcal{A}$ se **shoduje s položkou** P , pokud P je $T\varphi$ a $\mathcal{A} \models \varphi$, nebo pokud P je $F\varphi$ a $\mathcal{A} \models \neg\varphi$, tj. $\mathcal{A} \not\models \varphi$. Navíc, $\mathcal{A}$ se **shoduje s větví** V , shoduje-li se s každou položkou na V .

Lemma *Nechť $\mathcal{A}$ je model teorie T jazyka L , který se shoduje s položkou R v kořeni tabla $\tau = \cup \tau_n$ z T . Pak $\mathcal{A}$ lze **expandovat** do jazyka L_C tak, že se shoduje s **nějakou** větví V v tablu τ .*

Poznámka Postačí nám expanze modelu $\mathcal{A}$ o konstanty c^A pro $c \in L_C \setminus L$ vyskytující se na větví V , ostatní konstanty lze dodefinovat libovolně.

Důkaz Indukcí dle n nalezneme větev V_n v tablu τ_n a expanzi $\mathcal{A}_n$ modelu $\mathcal{A}$ o konstanty c^A pro $c \in L_C \setminus L$ na V_n tak, že $\mathcal{A}_n$ se shoduje s V_n a $V_{n-1} \subseteq V_n$.

Předpokládejme, že máme větev V_n v τ_n a expanzi $\mathcal{A}_n$ shodující se s V_n .

- Vznikne-li τ_{n+1} z τ_n bez prodloužení V_n , položme $V_{n+1} = V_n$, $\mathcal{A}_{n+1} = \mathcal{A}_n$.
- Vznikne-li τ_{n+1} z τ_n připojením $T\varphi$ k V_n pro nějaké $\varphi \in T$, nechť V_{n+1} je tato větev a $\mathcal{A}_{n+1} = \mathcal{A}_n$. Jelikož $\mathcal{A} \models \varphi$, shoduje se $\mathcal{A}_{n+1}$ s V_{n+1} .

Korektnost - důkaz (pokr.)

- Jinak τ_{n+1} vznikne z τ_n prodloužením V_n o atomické tablo nějaké položky P na V_n . Z indukčního předpokladu víme, že $\mathcal{A}_n$ se shoduje s P .
- (i) V případě atomického tabla pro **spojku** položíme $\mathcal{A}_{n+1} = \mathcal{A}_n$ a snadno ověříme, že V_n lze prodloužit na větev V_{n+1} shodující se s $\mathcal{A}_{n+1}$.
- (ii) Je-li P tvaru $T(\forall x)\varphi(x)$, necht' V_{n+1} je (jednoznačné) prodloužení V_n na větev v τ_{n+1} , tj. o položku $T\varphi(x/t)$. Necht' $\mathcal{A}_{n+1}$ je **libovolná** expanze $\mathcal{A}_n$ o nové konstanty z termu t . Jelikož $\mathcal{A}_n \models (\forall x)\varphi(x)$, platí $\mathcal{A}_{n+1} \models \varphi(x/t)$. Obdobně pro P tvaru $F(\exists x)\varphi(x)$.
- (iii) Je-li P tvaru $T(\exists x)\varphi(x)$, necht' V_{n+1} je (jednoznačné) prodloužení V_n na větev v τ_{n+1} , tj. o položku $T\varphi(x/c)$. Jelikož $\mathcal{A}_n \models (\exists x)\varphi(x)$, pro nějaké $a \in A$ platí $\mathcal{A}_n \models \varphi(x)[e(x/a)]$ pro každé ohodnocení e . Necht' $\mathcal{A}_{n+1}$ je expanze $\mathcal{A}_n$ o novou konstantu $c^A = a$. Pak $\mathcal{A}_{n+1} \models \varphi(x/c)$. Obdobně pro P tvaru $F(\forall x)\varphi(x)$.

Základní krok pro $n = 0$ plyne z obdobné analýzy atomických tabel pro položku R v kořeni s využitím předpokladu, že model $\mathcal{A}$ se shoduje s R . □

Věta o korektnosti

Ukážeme, že tablo metoda v predikátové logice je *korektní*.

Věta Pro každou teorii T a sentenci φ , je-li φ tablo dokazatelná z T , je φ pravdivá v T , tj. $T \vdash \varphi \Rightarrow T \models \varphi$.

Důkaz

- Necht' φ je tablo dokazatelná z teorie T , tj. existuje sporné tablo τ z T s položkou $F\varphi$ v kořeni.
- Pro spor předpokládejme, že φ není pravdivá v T , tj. existuje model $\mathcal{A}$ teorie T , ve kterém φ neplatí (*protipříklad*).
- Jelikož se $\mathcal{A}$ shoduje s položkou $F\varphi$, dle předchozího lemmatu lze $\mathcal{A}$ expandovat do jazyka L_C tak, že se shoduje s nějakou větví v tablu τ .
- To ale není možné, neboť každá větev tabla τ je sporná, tj. obsahuje dvojici $T\psi, F\psi$ pro nějakou sentenci ψ . $\square$

Kanonický model

Z bezesporné větve V dokončeného tabla vyrobíme model, který se shoduje s V . Vyjdeme z dostupných syntaktických objektů - *konstantních termů*.

Nechť V je bezesporná větev dokončeného tabla z teorie T jazyka

$L = \langle \mathcal{F}, \mathcal{R} \rangle$. *Kanonický model* z větve V je L_C -struktura $\mathcal{A} = \langle A, \mathcal{F}^A, \mathcal{R}^A \rangle$, kde

(1) A je množina všech konstantních termů jazyka L_C ,

(2) $f^A(s_1, \dots, s_n) = f(s_1, \dots, s_n)$

pro každý n -ární funkční symbol $f \in \mathcal{F} \cup (L_C \setminus L)$ a $s_1, \dots, s_n \in A$.

(3) $R^A(s_1, \dots, s_n) \Leftrightarrow TR(s_1, \dots, s_n)$ je položka na V

pro každý n -ární relační symbol $R \in \mathcal{R}$ či *rovnost* a $s_1, \dots, s_n \in A$.

Poznámka Výraz $f(s_1, \dots, s_n)$ na pravé straně v (2) je konstantní term jazyka L_C , tedy prvek z A . Neformálně, pro zdůraznění, že jde o syntaktický objekt

$$f^A(s_1, \dots, s_n) = "f(s_1, \dots, s_n)"$$

Kanonický model - příklad

Nechť teorie $T = \{(\forall x)R(f(x))\}$ je jazyka $L = \langle R, f, d \rangle$. Systematické tablo pro $F \neg R(d)$ z T obsahuje jedinou větev V a ta je bezesporná.

Kanonický model $\mathcal{A} = \langle A, R^A, f^A, d^A, c_i^A \rangle_{i \in \mathbb{N}}$ z V je pro jazyk L_C a platí

$$\begin{aligned} A &= \{d, f(d), f(f(d)), \dots, c_0, f(c_0), f(f(c_0)), \dots, c_1, f(c_1), f(f(c_1)), \dots\}, \\ d^A &= d, \quad c_i^A = c_i \text{ pro } i \in \mathbb{N}, \\ f^A(d) &= "f(d)", \quad f^A(f(d)) = "f(f(d))", \quad f^A(f(f(d))) = "f(f(f(d)))", \dots \\ R^A &= \{d, f(d), f(f(d)), \dots, f(c_0), f(f(c_0)), \dots, f(c_1), f(f(c_1)), \dots\}. \end{aligned}$$

Redukt $\mathcal{A}$ na jazyk L je $\mathcal{A}' = \langle A, R^A, f^A, d^A \rangle$.

Kanonický model s rovností

Je-li jazyk L s rovností, T^* označuje rozšíření T o axiomy rovnosti pro L .

Požadujeme-li, aby rovnost byla interpretovaná jako identita, kanonický model $\mathcal{A}$ z bezesporné větve V dokončeného tabla z T^ musíme **faktorizovat** dle $=^A$.*

Dle definice (3), v modelu $\mathcal{A}$ z V pro relaci $=^A$ platí, že pro každé $s_1, s_2 \in A$,

$$s_1 =^A s_2 \Leftrightarrow T(s_1 = s_2) \text{ je položka na } V.$$

Jelikož V je dokončená a obsahuje axiomy rovnosti, relace $=^A$ je ekvivalence na A a navíc **kongruence** pro všechny funkce a relace v $\mathcal{A}$.

Kanonický model s rovností z větve V je faktorstruktura $\mathcal{A}/=^A$.

Pozorování Pro každou formuli φ ,

$$\mathcal{A} \models \varphi \Leftrightarrow (\mathcal{A}/=^A) \models \varphi,$$

přičemž v $\mathcal{A}$ je $=$ interpretovaná relací $=^A$, zatímco v $\mathcal{A}/=^A$ jako identita.

Poznámka $\mathcal{A}$ je (spočetně) nekonečný model, ale $\mathcal{A}/=^A$ může být konečný.

Kanonický model s rovností - příklad

Nechť $T = \{(\forall x)R(f(x)), (\forall x)(x = f(f(x)))\}$ je nad $L = \langle R, f, d \rangle$ s rovností. Systematické tablo pro $F \neg R(d)$ z T^* obsahuje bezespornou větev V .

V kanonickém modelu $\mathcal{A} = \langle A, R^A, =^A, f^A, d^A, c_i^A \rangle_{i \in \mathbb{N}}$ z V pro relaci $=^A$ platí

$$s_1 =^A s_2 \iff s_1 = f(\cdots (f(s_2)) \cdots) \text{ nebo } s_2 = f(\cdots (f(s_1)) \cdots),$$

kde f je aplikováno $2i$ -krát pro nějaké $i \in \mathbb{N}$.

Kanonický model s rovností z V je $\mathcal{B} = (\mathcal{A}/=^A) = \langle A/=^A, R^B, f^B, d^B, c_i^B \rangle_{i \in \mathbb{N}}$

$$(A/=^A) = \{[d]_{=^A}, [f(d)]_{=^A}, [c_0]_{=^A}, [f(c_0)]_{=^A}, [c_1]_{=^A}, [f(c_1)]_{=^A}, \dots\},$$

$$d^B = [d]_{=^A}, \quad c_i^B = [c_i]_{=^A} \text{ pro } i \in \mathbb{N},$$

$$f^B([d]_{=^A}) = [f(d)]_{=^A}, \quad f^B([f(d)]_{=^A}) = [f(f(d))]_{=^A} = [d]_{=^A}, \quad \dots$$

$$R^B = (A/=^A).$$

Redukt $\mathcal{B}$ na jazyk L je $\mathcal{B}' = \langle A/=^A, R^B, f^B, d^B \rangle$.

Výroková a predikátová logika - IX

Petr Gregor

KTIML MFF UK

ZS 2021/22

Úplnost

Lemma Kanonický model $\mathcal{A}$ z bezesporné dok. větve V se *shoduje* s V .

Důkaz Indukcí dle struktury sentence vyskytující se v položce na V .

- Pro φ *atomickou*, je-li $T\varphi$ na V , je $\mathcal{A} \models \varphi$ dle (3). Je-li $F\varphi$ na V , není $T\varphi$ na V , neboť V je bezesporná, a tedy $\mathcal{A} \models \neg\varphi$ dle (3).
- Je-li $T(\varphi \wedge \psi)$ na V , je $T\varphi$ a $T\psi$ na V , neboť V je dokončená. Dle indukčního předpokladu je $\mathcal{A} \models \varphi$ a $\mathcal{A} \models \psi$, tedy $\mathcal{A} \models \varphi \wedge \psi$.
- Je-li $F(\varphi \wedge \psi)$ na V , je $F\varphi$ nebo $F\psi$ na V , neboť V je dokončená. Dle indukčního předpokladu je $\mathcal{A} \models \neg\varphi$ nebo $\mathcal{A} \models \neg\psi$, tedy $\mathcal{A} \models \neg(\varphi \wedge \psi)$.
- Pro ostatní spojky obdobně jako v předchozích dvou případech.
- Je-li $T(\forall x)\varphi(x)$ na V , je $T\varphi(x/t)$ na V pro každé $t \in A$, neboť V je dokončená. Dle indukčního předpokladu je $\mathcal{A} \models \varphi(x/t)$ pro každé $t \in A$, tedy $\mathcal{A} \models (\forall x)\varphi(x)$. Obdobně pro $F(\exists x)\varphi(x)$ na V .
- Je-li $T(\exists x)\varphi(x)$ na V , je $T\varphi(x/c)$ na V pro nějaké $c \in A$, neboť V je dokončená. Dle indukčního předpokladu je $\mathcal{A} \models \varphi(x/c)$, tedy $\mathcal{A} \models (\exists x)\varphi(x)$. Obdobně pro $F(\forall x)\varphi(x)$ na V . $\square$

Věta o úplnosti

Ukážeme, že tablo metoda ve predikátové logice je *úplná*.

Věta Pro každou teorii T a sentenci φ , je-li φ pravdivá v T , je φ tablo dokazatelná z T , tj. $T \models \varphi \Rightarrow T \vdash \varphi$.

Důkaz Nechť φ je pravdivá v T . Ukážeme, že libovolné *dokončené* tablo (např. *systematické*) τ z teorie T s položkou $F\varphi$ v kořeni je *sporné*.

- Kdyby ne, v tablu τ je nějaká bezesporná větev V .
- Dle předchozího lemmatu existuje struktura $\mathcal{A}$ pro jazyk L_C shodující se s větví V , speciálně s položkou $F\varphi$ v kořeni, tj. $\mathcal{A} \models \neg\varphi$.
- Nechť $\mathcal{A}'$ je redukt struktury $\mathcal{A}$ na původní jazyk L . Platí $\mathcal{A}' \models \neg\varphi$.
- Jelikož větev V je dokončená, obsahuje $T\psi$ pro každé $\psi \in T$.
- Tedy $\mathcal{A}'$ je modelem T (neboť $\mathcal{A}'$ se shoduje s $T\psi$ pro každé $\psi \in T$).
- To je ale ve sporu s tím, že φ platí v každém modelu teorie T .

Tedy tablo τ je důkazem φ z T . $\square$

Vlastnosti teorií

Zavedeme syntaktické varianty již definovaných sémantických pojmů.

Nechť T je teorie jazyka L . Je-li sentence φ dokazatelná z T , řekneme, že φ je **věta (teorém)** teorie T . Množinu vět teorie T označme

$$\text{Thm}^L(T) = \{\varphi \in \text{Fm}_L \mid T \vdash \varphi\}.$$

Řekneme, že teorie T je

- **sporná**, jestliže je v T dokazatelný $\perp$ (spor), jinak je **bezesporná**,
- **kompletní**, jestliže není sporná a každá sentence je v ní dokazatelná či zamítnutelná, tj. $T \vdash \varphi$ či $T \vdash \neg\varphi$.
- **extenze** teorie T' jazyka L' , jestliže $L' \subseteq L$ a $\text{Thm}^{L'}(T') \subseteq \text{Thm}^L(T)$, o extenzi T teorie T' řekneme, že je **jednoduchá**, pokud $L = L'$, a **konzervativní**, pokud $\text{Thm}^{L'}(T') = \text{Thm}^L(T) \cap \text{Fm}_{L'}$,
- **ekvivalentní** s teorií T' , jestliže T je extenzí T' a T' je extenzí T .

Důsledky

Z korektnosti a úplnosti tablo metody vyplývá, že předchozí pojmy se shodují se svými sémantickými variantami.

Důsledek Pro každou teorii T a sentence φ, ψ jazyka L ,

- $T \vdash \varphi$ právě když $T \models \varphi$,
- $\text{Thm}^L(T) = \theta^L(T)$,
- T je sporná, právě když je sémanticky sporná, tj. nemá model,
- T je kompletní, právě když je sémanticky kompletní, tj. má až na *elementární ekvivalenci* jediný model,
- $T, \varphi \vdash \psi$ právě když $T \vdash \varphi \rightarrow \psi$ (*Věta o dedukci*).

Poznámka Větu o dedukci lze dokázat přímo, transformací příslušných tabel.

Löwenheim-Skolemova věta a kompaktnost

Věta Každá bezesporná teorie T spočetného jazyka L bez rovnosti má spočetně nekonečný model.

Důkaz Necht' τ je systematické tablo z T s $F\perp$ v kořeni. Jelikož je dokončené a obsahuje bezespornou větev V , neboť $\perp$ není dokazatelný z T , existuje kanonický model $\mathcal{A}$ z V . Jelikož se $\mathcal{A}$ shoduje s V , jeho redukt na jazyk L je hledaným spočetně nekonečným modelem T . $\square$

Poznámka Jde o slabou verzi tzv. Löwenheim-Skolemovy věty. Ve spočetném jazyce s rovností je kanonický model s rovností spočetný.

Věta Teorie má model, právě když každá její konečná část má model.

Důkaz Implikace zleva doprava je zřejmá. Pokud teorie T nemá model, je sporná, tj. je z ní dokazatelný $\perp$ systematickým tablem τ . Jelikož je τ konečné, je $\perp$ dokazatelný z nějaké konečné $T' \subseteq T$, tj. T' nemá model. $\square$

Nestandardní model přirozených čísel

Nechť $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je standardní model přirozených čísel.

Označme $\text{Th}(\underline{\mathbb{N}})$ množinu všech pravdivých **sentencí** v $\underline{\mathbb{N}}$. Pro $n \in \mathbb{N}$ označme $\underline{n}$ term $S(S(\dots(S(0)\dots)))$, tzv. ***n-tý numerál***, kde S je aplikováno n -krát.

Uvažme následující teorii T , kde c je nový konstantní symbol.

$$T = \text{Th}(\underline{\mathbb{N}}) \cup \{ \underline{n} < c \mid n \in \mathbb{N} \}$$

Pozorování Každá konečná část teorie T má model.

Tedy dle věty o kompaktnosti má T model $\mathcal{A}$, jde o **nestandardní model přirozených čísel**. Každá sentence z $\text{Th}(\underline{\mathbb{N}})$ v něm platí, ale zároveň obsahuje prvek $c^{\mathcal{A}}$ větší než každé $n \in \mathbb{N}$ (tj. hodnota termu $\underline{n}$ v $\mathcal{A}$).

Rozšiřování teorií

Ukážeme, že zavádění nových pojmů má “pomocný charakter”.

Tvrzení *Nechť T je teorie jazyka L , T' je teorie jazyka L' a $L \subseteq L'$.*

- (i) T' je extenze T , právě když **redukt** $\mathcal{A}$ každého modelu $\mathcal{A}'$ teorie T' na jazyk L je modelem teorie T ,*
- (ii) T' je **konzervativní** extenze T , je-li T' extenze T a každý model $\mathcal{A}$ teorie T lze **expandovat** do jazyka L' na model $\mathcal{A}'$ teorie T' .*

Důkaz

- (i)a) Je-li T' extenze T a φ libovolný axiom T , pak $T' \models \varphi$. Tedy $\mathcal{A}' \models \varphi$ a rovněž $\mathcal{A} \models \varphi$, z čehož plyne, že $\mathcal{A}$ je modelem T .*
- (i)b) Je-li $\mathcal{A}$ modelem T a $T \models \varphi$, kde φ je jazyka L , pak $\mathcal{A} \models \varphi$ a rovněž $\mathcal{A}' \models \varphi$. Z toho plyne, že $T' \models \varphi$ a tedy T' je extenze T .*
- (ii) Je-li $T' \models \varphi$, kde φ je nad L , a $\mathcal{A}$ je model T , pak v nějaké jeho expanzi $\mathcal{A}' \models \varphi$ a tedy $\mathcal{A} \models \varphi$. Z čehož $T \models \varphi$, tj. T' je konzervativní. $\square$*

Extenze o definovaný relační symbol

Nechť T je teorie jazyka L , $\psi(x_1, \dots, x_n)$ je formule jazyka L ve volných proměnných $x_1, \dots, x_n$ a L' je rozšíření L o nový n -ární relační symbol R .

Extenze teorie T **o definici R** formulí ψ je teorie T' vzniklá přidáním axiomu

$$R(x_1, \dots, x_n) \leftrightarrow \psi(x_1, \dots, x_n)$$

Pozorování Každý model teorie T lze **jednoznačně** expandovat na model T' .

Důsledek T' je **konzervativní** extenze T .

Tvrzení Pro každou formuli φ' nad L' existuje φ nad L , t.ž. $T' \models \varphi' \leftrightarrow \varphi$.

Důkaz Každou podformuli $R(t_1, \dots, t_n)$ nahradíme za $\psi'(x_1/t_1, \dots, x_n/t_n)$, kde ψ' je vhodná varianta ψ zaručující substituovatelnost všech termů. $\square$

Např. symbol $\leq$ lze zavést v jazyce aritmetiky pomocí axiomu

$$x_1 \leq x_2 \leftrightarrow (\exists y)(x_1 + y = x_2)$$

Extenze o definovaný funkční symbol

Nechť T je teorie jazyka L a pro formuli $\psi(x_1, \dots, x_n, y)$ jazyka L ve volných proměnných $x_1, \dots, x_n, y$ platí

$$T \models (\exists y)\psi(x_1, \dots, x_n, y) \quad (\text{existence})$$

$$T \models \psi(x_1, \dots, x_n, y) \wedge \psi(x_1, \dots, x_n, z) \rightarrow y = z \quad (\text{jednoznačnost})$$

Označme L' rozšíření L o nový n -ární funkční symbol f .

Extenze teorie T **o definici f** formulí ψ je teorie T' vzniklá přidáním axiomu

$$f(x_1, \dots, x_n) = y \leftrightarrow \psi(x_1, \dots, x_n, y)$$

Poznámka Je-li ψ tvaru $t(x_1, \dots, x_n) = y$, kde $x_1, \dots, x_n$ jsou proměnné termu t , podmínky existence a jednoznačnosti platí.

Např. binární funkční symbol – lze zavést pomocí + a unárního – axiomem

$$x_1 - x_2 = y \leftrightarrow x_1 + (-x_2) = y$$

Extenze o definovaný funkční symbol (pokr.)

Pozorování Každý model teorie T lze *jednoznačně* expandovat na model T' .

Důsledek T' je *konzervativní* extenze T .

Tvrzení Pro každou formuli φ' nad L' existuje φ nad L , t.ž. $T' \models \varphi' \leftrightarrow \varphi$.

Důkaz Stačí uvážit φ' s jediným výskytem f . Má-li φ' více výskytů f , lze postup aplikovat induktivně (v případě vnořených výskytů jdeme od vnitřních k vnějším). Označme φ^* formuli vzniklou z φ' nahrazením termu $f(t_1, \dots, t_n)$ za *novou* proměnnou z . Za φ vezmeme formuli

$$(\exists z)(\varphi^* \wedge \psi'(x_1/t_1, \dots, x_n/t_n, y/z)),$$

kde ψ' je vhodná varianta ψ zaručující substituovatelnost všech termů.

Nechť $\mathcal{A}$ je model T' , e je ohodnocení, $a = f^A(t_1, \dots, t_n)[e]$. Díky oběma podmínkám platí $\mathcal{A} \models \psi'(x_1/t_1, \dots, x_n/t_n, y/z)[e]$ právě když $e(z) = a$. Tedy

$$\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{A} \models \varphi^*[e(z/a)] \Leftrightarrow \mathcal{A} \models \varphi'[e]$$

pro každé ohodnocení e , tj. $\mathcal{A} \models \varphi' \leftrightarrow \varphi$ a tedy $T' \models \varphi' \leftrightarrow \varphi$. $\square$

Extenze o definice

Teorie T' jazyka L' je **extenze** teorie T jazyka L **o definice**, pokud vznikla z T postupnou extenzí o definici relačního či funkčního symbolu.

Důsledek *Necht' T' je extenze teorie T o definice. Pak*

- *každý model teorie T lze jednoznačně expandovat na model T' ,*
- *T' je konzervativní extenze T ,*
- *pro každou formuli φ' nad L' existuje φ nad L taková, že $T' \models \varphi' \leftrightarrow \varphi$.*

Např. v teorii $T = \{(\exists y)(x + y = 0), (x + y = 0) \wedge (x + z = 0) \rightarrow y = z\}$ nad $L = \langle +, 0, \leq \rangle$ s rovností lze zavést $<$ a unární funkční symbol – axiomy

$$-x = y \leftrightarrow x + y = 0$$

$$x < y \leftrightarrow x \leq y \wedge \neg(x = y)$$

Pak formule $-x < y$ je v této extenzi o definice ekvivalentní formuli

$$(\exists z)((z \leq y \wedge \neg(z = y)) \wedge x + z = 0).$$

Ekvisplnitelnost

*Ukážeme, že problém splnitelnosti lze **redukovat** na otevřeně teorie.*

- Teorie T , T' jsou **ekvisplnitelné**, jestliže T má model $\Leftrightarrow T'$ má model.
- Formule φ je v **prenexním (normálním) tvaru (PNF)**, má-li tvar

$$(Q_1x_1) \dots (Q_nx_n)\varphi',$$

kde Q_i značí $\forall$ nebo $\exists$, proměnné $x_1, \dots, x_n$ jsou navzájem různé a φ' je otevřená formule, zvaná **otevřené jádro**. $(Q_1x_1) \dots (Q_nx_n)$ je tzv. **prefix**.

- Speciálně, jsou-li všechny kvantifikátory $\forall$, je φ **univerzální** formule.

K teorii T nalezneme ekvisplnitelnou otevřenou teorii následujícím postupem.

- (1) Axiomy teorie T nahradíme za ekvivalentní formule v **prenexním** tvaru.
- (2) Pomocí nových funkčních symbolů je převedeme na univerzální formule, tzv. **Skolemovy varianty**, čímž dostaneme ekvisplnitelnou teorii.
- (3) Jejich **otevřená jádra** budou tvořit hledanou teorii.

Vytýkání kvantifikátorů

Nechť Q značí kvantifikátor $\forall$ nebo $\exists$ a $\overline{Q}$ značí opačný kvantifikátor.

Pro každé formule φ, ψ takové, že x **není volná** ve formuli ψ ,

$$\models \neg(Qx)\varphi \leftrightarrow (\overline{Q}x)\neg\varphi$$

$$\models ((Qx)\varphi \wedge \psi) \leftrightarrow (Qx)(\varphi \wedge \psi)$$

$$\models ((Qx)\varphi \vee \psi) \leftrightarrow (Qx)(\varphi \vee \psi)$$

$$\models ((Qx)\varphi \rightarrow \psi) \leftrightarrow (\overline{Q}x)(\varphi \rightarrow \psi)$$

$$\models (\psi \rightarrow (Qx)\varphi) \leftrightarrow (Qx)(\psi \rightarrow \varphi)$$

Uvedené ekvivalence lze ověřit sémanticky nebo dokázat tablo metodou (přes generální uzávěr, *není-li to sentence*).

Poznámka Předpoklad, že x *není volná* ve formuli ψ je v každé ekvivalenci (kromě té první) nutný pro nějaký kvantifikátor Q . Např.

$$\not\models ((\exists x)P(x) \wedge P(x)) \leftrightarrow (\exists x)(P(x) \wedge P(x))$$

Převod na prenexní tvar

Tvrzení Necht' φ' je formule vzniklá z formule φ nahrazením některých výskytů podformule ψ za formuli ψ' . Jestliže $T \models \psi \leftrightarrow \psi'$, pak $T \models \varphi \leftrightarrow \varphi'$.

Důkaz Snadno indukcí dle struktury formule φ . $\square$

Tvrzení Ke každé formuli φ existuje ekvivalentní formule φ' v *prenexním normálním tvaru*, tj. $\models \varphi \leftrightarrow \varphi'$.

Důkaz Indukcí dle struktury φ pomocí *vytýkání kvantifikátorů*, náhradou podformulí za jejich *varianty* a využitím předchozího tvrzení o ekvivalenci. $\square$

Např.

$$\begin{aligned}
 ((\forall z)P(x, z) \wedge P(y, z)) &\rightarrow \neg(\exists x)P(x, y) \\
 ((\forall u)P(x, u) \wedge P(y, z)) &\rightarrow (\forall x)\neg P(x, y) \\
 (\forall u)(P(x, u) \wedge P(y, z)) &\rightarrow (\forall v)\neg P(v, y) \\
 (\exists u)((P(x, u) \wedge P(y, z)) &\rightarrow (\forall v)\neg P(v, y)) \\
 (\exists u)(\forall v)((P(x, u) \wedge P(y, z)) &\rightarrow \neg P(v, y))
 \end{aligned}$$

Výroková a predikátová logika - X

Petr Gregor

KTIML MFF UK

ZS 2021/22

Skolemova varianta

Nechť φ je **sentence** jazyka L v **prenexním normálním tvaru**, $y_1, \dots, y_n$ jsou **existenčně** kvantifikované proměnné ve φ (v tomto pořadí) a pro každé $i \leq n$ nechť $x_1, \dots, x_{n_i}$ jsou **univerzálně** kvantifikované proměnné před y_i . Označme L' rozšíření L o nové n_i -ární funkční symboly f_i pro každé $i \leq n$.

Nechť φ_S je formule jazyka L' , jež vznikne z formule φ odstraněním $(\exists y_i)$ z jejího prefixu a nahrazením každého výskytu proměnné y_i za term $f_i(x_1, \dots, x_{n_i})$. Pak formule φ_S se nazývá **Skolemova varianta** formule φ .

Např. pro formuli φ

$$(\exists y_1)(\forall x_1)(\forall x_2)(\exists y_2)(\forall x_3)R(y_1, x_1, x_2, y_2, x_3)$$

je následující formule φ_S její Skolemovou variantou

$$(\forall x_1)(\forall x_2)(\forall x_3)R(f_1, x_1, x_2, f_2(x_1, x_2), x_3),$$

kde f_1 je nový konstantní symbol a f_2 je nový binární funkční symbol.

Vlastnosti Skolemovy varianty

Lemma *Nechť φ je sentence $(\forall x_1) \dots (\forall x_n)(\exists y)\psi$ jazyka L a φ' je sentence $(\forall x_1) \dots (\forall x_n)\psi(y/f(x_1, \dots, x_n))$, kde f je nový funkční symbol. Pak*

- (1) *redukt $\mathcal{A}$ každého modelu $\mathcal{A}'$ formule φ' na jazyk L je modelem φ ,*
- (2) *každý model $\mathcal{A}$ formule φ lze expandovat na model $\mathcal{A}'$ formule φ' .*

Poznámka *Na rozdíl od extenze o definici funkčního symbolu, expanze v tvrzení (2) tentokrát nemusí být jednoznačná.*

Důkaz (1) Nechť $\mathcal{A}' \models \varphi'$ a $\mathcal{A}$ je redukt $\mathcal{A}'$ na jazyk L . Jelikož pro každé ohodnocení e je $\mathcal{A} \models \psi[e(y/a)]$, kde $a = (f(x_1, \dots, x_n))^{\mathcal{A}'}[e]$, platí $\mathcal{A} \models \varphi$.
 (2) Nechť $\mathcal{A} \models \varphi$. Pak existuje funkce $f^{\mathcal{A}}: A^n \rightarrow A$ taková, že pro každé ohodnocení e platí $\mathcal{A} \models \psi[e(y/a)]$, kde $a = f^{\mathcal{A}}(e(x_1), \dots, e(x_n))$, a tedy expanze $\mathcal{A}'$ struktury $\mathcal{A}$ o funkci $f^{\mathcal{A}}$ je modelem φ' . $\square$

Důsledek *Je-li φ' Skolemova varianta formule φ , obě tvrzení (1) a (2) pro φ, φ' rovněž platí. Tedy φ, φ' jsou ekvisplnitelné.*

Skolemova věta

Věta Každá teorie T má *otevřenou konzervativní* extenzi T^* .

Důkaz Lze předpokládat, že T je v uzavřeném tvaru. Nechť L je její jazyk.

- Nahrazením každého axiomu teorie T za ekvivalentní formuli v *prenexním tvaru* získáme ekvivalentní teorii T° .
- Nahrazením každého axiomu teorie T° za jeho *Skolemovu variantu* získáme teorii T' rozšířeného jazyka L' .
- Jelikož je redukt každého modelu teorie T' na jazyk L modelem teorie T , je T' *extenze* T .
- Jelikož i každý model teorie T lze expandovat na model teorie T' , je to extenze *konzervativní*.
- Jelikož každý axiom teorie T' je univerzální sentence, jejich nahrazením za *otevřená jádra* získáme otevřenou teorii T^* ekvivalentní s T' . $\square$

Důsledek Ke každé teorii existuje ekvivalentní otevřená teorie.

Redukce nesplnitelnosti na úroveň VL

Je-li otevřená teorie nesplnitelná, lze to “doložit na konkrétních prvcích”.

Např. teorie

$$T = \{P(x, y) \vee R(x, y), \neg P(c, y), \neg R(x, f(x))\}$$

jazyka $L = \langle P, R, f, c \rangle$ nemá model, což lze doložit nesplnitelnou konjunkcí konečně mnoha **instancí** (některých) axiomů teorie T v **konstantních termech**

$$(P(c, f(c)) \vee R(c, f(c))) \wedge \neg P(c, f(c)) \wedge \neg R(c, f(c)),$$

což je lživá formule ve tvaru výroku

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

Instance $\varphi(x_1/t_1, \dots, x_n/t_n)$ otevřené formule φ ve volných proměnných $x_1, \dots, x_n$ je **základní (ground) instance**, jsou-li všechny termy $t_1, \dots, t_n$ konstantní. Konstantní termy nazýváme také **základní (ground) termy**.

Herbrandův model

Nechť $L = \langle \mathcal{R}, \mathcal{F} \rangle$ je jazyk s alespoň jedním konstantním symbolem.

(Je-li třeba, do L přidáme nový konstantní symbol.)

- **Herbrandovo univerzum** pro L je množina všech konstantních termů z L .
Např. pro $L = \langle P, f, c \rangle$, kde P je relační, f je binární funkční, c konstantní

$$A = \{c, f(c, c), f(f(c, c), c), f(c, f(c, c)), f(f(c, c), f(c, c)), \dots\}$$
- Struktura $\mathcal{A}$ pro L je **Herbrandova struktura**, je-li doména A Herbrandovo univerzum pro L a pro každý n -ární funkční symbol $f \in \mathcal{F}$ a $t_1, \dots, t_n \in A$,

$$f^A(t_1, \dots, t_n) = f(t_1, \dots, t_n)$$

(včetně $n = 0$, tj. $c^A = c$ pro každý konstantní symbol c).

Poznámka Na rozdíl od **kanonické struktury** nejsou předepsané relace.

Např. $\mathcal{A} = \langle A, P^A, f^A, c^A \rangle$, kde $P^A = \emptyset$, $c^A = c$ a $f^A(c, c) = f(c, c), \dots$

- **Herbrandův model** teorie T je Herbrandova struktura, jež je modelem T .

Herbrandova věta

Věta *Nechť T je otevřená teorie jazyka L bez rovnosti a s alespoň jedním konstantním symbolem. Pak*

- (a) *T má Herbrandův model, anebo*
- (b) *existuje konečně mnoho základních instancí axiomů z T , jejichž konjunkce je nespílitelná, a tedy T nemá model.*

Důkaz Nechť T' je množina všech základních instancí axiomů z T . Uvažme dokončené (např. systematické) tablo τ z T' v jazyce L (bez přidávání nových konstant) s položkou $F \perp$ v kořeni.

- Obsahuje-li tablo τ bezespornou větev V , kanonický model z větve V je Herbrandovým modelem teorie T .
- Jinak je τ sporné, tj. $T' \vdash \perp$. Navíc je konečné, tedy $\perp$ je dokazatelný jen z konečně mnoha formulí T' , tj. jejich konjunkce je nespílitelná. $\square$

Poznámka V případě jazyka L s rovností teorií T rozšíříme na T^* o *axiomy rovnosti* pro L a pokud T^* má Herbrandův model $\mathcal{A}$, *zfaktorizujeme* ho dle $=^A$.

Důsledky Herbrandovy věty

Nechť L je jazyk obsahující alespoň jeden konstantní symbol.

Důsledek Pro každou otevřenou $\varphi(x_1, \dots, x_n)$ jazyka L je $(\exists x_1) \dots (\exists x_n)\varphi$ pravdivá, právě když existují konstantní termy t_{ij} jazyka L takové, že

$$\varphi(x_1/t_{11}, \dots, x_n/t_{1n}) \vee \dots \vee \varphi(x_1/t_{m1}, \dots, x_n/t_{mn})$$

je (výroková) tautologie.

Důkaz $(\exists x_1) \dots (\exists x_n)\varphi$ je pravdivá $\Leftrightarrow (\forall x_1) \dots (\forall x_n)\neg\varphi$ je nespílitelná $\Leftrightarrow \neg\varphi$ je nespílitelná. Ostatní vyplývá z Herbrandovy věty pro $\neg\varphi$. $\square$

Důsledek Otevřená teorie T jazyka L má model, právě když teorie T' všech základních instancí axiomů z T má model.

Důkaz Má-li T model $\mathcal{A}$, platí v něm každá instance každého axiomu z T , tedy $\mathcal{A}$ je modelem T' . Nemá-li T model, dle H. věty existuje (konečně) formulí z T' , jejichž konjunkce je nespílitelná, tedy T' nemá model. $\square$

Rezoluční metoda v PL - úvod

- **Zamítací** procedura - cílem je ukázat, že daná formule (či teorie) je nespílitelná.
- Předpokládá **otevřené** formule v **CNF** (v množinové reprezentaci).

Literál je (tentokrát) atomická formule nebo její negace.

Klauzule je konečná množina literálů, $\square$ značí **prázdnou klauzuli**.

Formule (v množinové reprezentaci) je množina (i nekonečná) klauzulí.

Poznámka Každou formuli (teorii) umíme převést na ekvivalentní otevřenou formuli (teorii) v CNF, tj. na formuli v množinové reprezentaci.

- **Rezoluční pravidlo** je obecnější - umožňuje rezolvovat přes literály, které jsou **unifikovatelné**.
- Rezoluce v PL je založená na **rezoluci ve VL** a **unifikaci**.

Lokální význam proměnných

Proměnné v rámci *klauzule* můžeme přejmenovat.

Nechť φ je (vstupní) otevřená formule v CNF.

- Formule φ je splnitelná, právě když její generální uzávěr φ' je splnitelný.
- Pro každé formule ψ , χ a proměnnou x

$$\models (\forall x)(\psi \wedge \chi) \leftrightarrow (\forall x)\psi \wedge (\forall x)\chi$$

(i když x je volná v ψ a χ zároveň).

- Každou klauzuli ve φ lze tedy nahradit jejím generálním uzávěrem.
- Uzávěry klauzulí lze *variovat* (přejmenovat proměnné).

Např. variovaním druhé klauzule v (1) získáme ekvisplnitelnou formuli (2).

$$(1) \{ \{P(x), Q(x, y)\}, \{\neg P(x), \neg Q(y, x)\} \}$$

$$(2) \{ \{P(x), Q(x, y)\}, \{\neg P(v), \neg Q(u, v)\} \}$$

Přímá redukce do VL

Herbrandova věta umožňuje následující postup. Je ale značně neefektivní.

- Necht' S je (vstupní) formule v množinové reprezentaci.
- Lze předpokládat, že jazyk obsahuje alespoň jeden konstantní symbol.
- Necht' S' je množina všech **základních instancí** klauzulí z S .
- Zavedením prvovýroků pro každou **atomickou sentenci** lze S' převést na (případně nekonečnou) výrokovou formuli v množinové reprezentaci.
- Rezolucí na úrovni VL ověříme její nesplnitelnost.

Např. pro $S = \{\{P(x, y), R(x, y)\}, \{\neg P(c, y)\}, \{\neg R(x, f(x))\}\}$ je

$$S' = \{\{P(c, c), R(c, c)\}, \{P(c, f(c)), R(c, f(c))\}, \{P(f(c), f(c)), R(f(c), f(c))\}, \dots, \\ \{\neg P(c, c)\}, \{\neg P(c, f(c))\}, \dots, \{\neg R(c, f(c))\}, \{\neg R(f(c), f(f(c)))\}, \dots\}$$

nesplnitelná, neboť na úrovni VL je

$$S' \supseteq \{\{P(c, f(c)), R(c, f(c))\}, \{\neg P(c, f(c))\}, \{\neg R(c, f(c))\}\} \vdash_R \square.$$

Substituce - příklady

Efektivnější je využívat vhodných substitucí. Např. pro

- a) $\{P(x), Q(x, a)\}, \{\neg P(y), \neg Q(b, y)\}$ substitucí $x/b, y/a$ dostaneme $\{P(b), Q(b, a)\}, \{\neg P(a), \neg Q(b, a)\}$ a z nich rezolucí $\{P(b), \neg P(a)\}$.

Nebo substitucí x/y a rezolucí dle $P(y)$ dostaneme $\{Q(y, a), \neg Q(b, y)\}$.

- b) $\{P(x), Q(x, a), Q(b, y)\}, \{\neg P(v), \neg Q(u, v)\}$ substituce $x/b, y/a, u/b, v/a$ dává $\{P(b), Q(b, a)\}, \{\neg P(a), \neg Q(b, a)\}$ a z nich rezolucí $\{P(b), \neg P(a)\}$.

- c) $\{P(x), Q(x, z)\}, \{\neg P(y), \neg Q(f(y), y)\}$ substitucí $x/f(z), y/z$ dostaneme $\{P(f(z)), Q(f(z), z)\}, \{\neg P(z), \neg Q(f(z), z)\}$ a z nich $\{P(f(z)), \neg P(z)\}$.

Při substituci $x/f(a), y/a, z/a$ dostaneme $\{P(f(a)), Q(f(a), a)\}, \{\neg P(a), \neg Q(f(a), a)\}$ a z nich rezolucí $\{P(f(a)), \neg P(a)\}$. Předchozí substituce je ale **obecnější**.

Substitute

- **Substitute** je (konečná) množina $\sigma = \{x_1/t_1, \dots, x_n/t_n\}$, kde x_i jsou navzájem různé proměnné a t_i jsou termy, přičemž t_i není x_i .
- Jsou-li všechny termy t_i konstantní, je σ **základní substitute**.
- Jsou-li t_i navzájem různé proměnné, je σ **přejmenování proměnných**.
- **Výraz** je literál nebo term. (*Substituci lze aplikovat na výrazy.*)
- **Instance** výrazu E **při substituci** $\sigma = \{x_1/t_1, \dots, x_n/t_n\}$ je výraz $E\sigma$ vzniklý z E **současným** nahrazením **všech** výskytů proměnných x_i za t_i .
- Pro množinu výrazů S označme $S\sigma$ množinu instancí $E\sigma$ výrazů E z S .

Poznámka Jelikož substitute je současná pro všechny proměnné zároveň, případný výskyt proměnné x_i v termu t_j nevede k zřetězení substitucí.

Např. pro $S = \{P(x), R(y, z)\}$ a substituci $\sigma = \{x/f(y, z), y/x, z/c\}$ je

$$S\sigma = \{P(f(y, z)), R(x, c)\}.$$

Skládání substitucí

Zdefinujeme $\sigma\tau$ tak, aby $E(\sigma\tau) = (E\sigma)\tau$ pro každý výraz E .

Např. pro $E = P(x, w, u)$, $\sigma = \{x/f(y), w/v\}$, $\tau = \{x/a, y/g(x), v/w, u/c\}$ je

$$E\sigma = P(f(y), v, u), \quad (E\sigma)\tau = P(f(g(x)), w, c).$$

Pak by mělo být $\sigma\tau = \{x/f(g(x)), y/g(x), v/w, u/c\}$.

Pro substitute $\sigma = \{x_1/t_1, \dots, x_n/t_n\}$ a $\tau = \{y_1/s_1, \dots, y_m/s_m\}$ definujeme

$$\sigma\tau = \{x_i/t_{i\tau} \mid x_i \in X, x_i \text{ není } t_{i\tau}\} \cup \{y_j/s_j \mid y_j \in Y \setminus X\}$$

složenou substitucí σ a τ , kde $X = \{x_1, \dots, x_n\}$ a $Y = \{y_1, \dots, y_m\}$.

Poznámka Skládání substitucí není komutativní, např. pro uvedené σ a τ je

$$\tau\sigma = \{x/a, y/g(f(y)), u/c, w/v\} \neq \sigma\tau.$$

Skládání substitucí - vlastnosti

Ukážeme, že definice vyhovuje našemu požadavku a skládání je asociativní.

Tvrzení Pro každý výraz E a substituce σ, τ, ϱ platí

$$(i) (E\sigma)\tau = E(\sigma\tau),$$

$$(ii) (\sigma\tau)\varrho = \sigma(\tau\varrho).$$

Důkaz Nechť $\sigma = \{x_1/t_1, \dots, x_n/t_n\}$ a $\tau = \{y_1/s_1, \dots, y_m/s_m\}$. Stačí uvážit případ, kdy E je proměnná, řekněme v .

(i) Je-li v proměnná x_i pro nějaké i , je $v\sigma = t_i$ a $(v\sigma)\tau = t_i\tau$, což je $v(\sigma\tau)$ dle definice $\sigma\tau$. Jinak $v\sigma = v$ a $(v\sigma)\tau = v\tau$.

Je-li v proměnná y_j pro nějaké j , je dále $(v\sigma)\tau = v\tau = s_j$, což je $v(\sigma\tau)$ dle definice $\sigma\tau$. Jinak $(v\sigma)\tau = v\tau = v$ a zároveň $v(\sigma\tau) = v$.

(ii) Opakovaným užitím (i) dostaneme pro každý výraz E ,

$$E((\sigma\tau)\varrho) = (E(\sigma\tau))\varrho = ((E\sigma)\tau)\varrho = (E\sigma)(\tau\varrho) = E(\sigma(\tau\varrho)). \quad \square$$

Unifikace

Nechť $S = \{E_1, \dots, E_n\}$ je (konečná) množina výrazů.

- **Unifikace** pro S je substituce σ taková, že $E_1\sigma = E_2\sigma = \dots = E_n\sigma$, tj. $S\sigma$ je singleton.
- S je **unifikovatelná**, pokud má unifikaci.
- Unifikace σ pro S je **nejobecnější unifikace (mgu)**, pokud pro každou unifikaci τ pro S existuje substituce λ taková, že $\tau = \sigma\lambda$.

Např. $S = \{P(f(x), y), P(f(a), w)\}$ je unifikovatelná pomocí nejobecnější unifikace $\sigma = \{x/a, y/w\}$. Unifikaci $\tau = \{x/a, y/b, w/b\}$ dostaneme jako $\sigma\lambda$ pro $\lambda = \{w/b\}$. τ není mgu, nelze z ní získat unifikaci $\varrho = \{x/a, y/c, w/c\}$.

Pozorování Jsou-li σ, τ různé nejobecnější unifikace pro S , liší se pouze přejmenováním proměnných.

Unifikační algoritmus

Nechť S je (konečná) neprázdná množina výrazů a p je **nejlevější** pozice, na které se nějaké dva výrazy z S liší. Pak **neshoda** v S je množina $D(S)$ podvýrazů začínajících na pozici p ze **všech** výrazů v S .

Např. pro $S = \{P(x, y), P(f(x), z), P(z, f(x))\}$ je $D(S) = \{x, f(x), z\}$.

Vstup Neprázdná (konečná) množina výrazů S .

Výstup Nejobecnější unifikace σ pro S nebo “ S není unifikovatelná”.

- (0) Nechť $S_0 := S$, $\sigma_0 := \emptyset$, $k := 0$. (inicializace)
- (1) Je-li S_k singleton, vydej substituci $\sigma = \sigma_0 \sigma_1 \cdots \sigma_k$. (mgu pro S)
- (2) Zjisti, zda v $D(S_k)$ existuje proměnná x a term t **neobsahující** x .
- (3) Pokud ne, vydej “ S není unifikovatelná”.
- (4) Jinak $\sigma_{k+1} := \{x/t\}$, $S_{k+1} := S_k \sigma_{k+1}$, $k := k + 1$ a jdi na (1).

Poznámka Test výskytu proměnné x v termu t v kroku (2) může být “drahý”.

Unifikační algoritmus - příklad

$$S = \{P(f(y, g(z)), h(b)), P(f(h(w), g(a)), t), P(f(h(b), g(z)), y)\}$$

- 1) $S_0 = S$ není singleton a $D(S_0) = \{y, h(w), h(b)\}$ obsahuje term $h(w)$ a proměnnou y nevyskytující se v $h(w)$. Pak $\sigma_1 = \{y/h(w)\}$, $S_1 = S_0\sigma_1$, tj.

$$S_1 = \{P(f(h(w), g(z)), h(b)), P(f(h(w), g(a)), t), P(f(h(b), g(z)), h(w))\}.$$
- 2) $D(S_1) = \{w, b\}$, $\sigma_2 = \{w/b\}$, $S_2 = S_1\sigma_2$, tj.

$$S_2 = \{P(f(h(b), g(z)), h(b)), P(f(h(b), g(a)), t)\}.$$
- 3) $D(S_2) = \{z, a\}$, $\sigma_3 = \{z/a\}$, $S_3 = S_2\sigma_3$, tj.

$$S_3 = \{P(f(h(b), g(a)), h(b)), P(f(h(b), g(a)), t)\}.$$
- 4) $D(S_3) = \{h(b), t\}$, $\sigma_4 = \{t/h(b)\}$, $S_4 = S_3\sigma_4$, tj.

$$S_4 = \{P(f(h(b), g(a)), h(b))\}.$$
- 5) S_4 je singleton a nejobecnější unifikace pro S je

$$\sigma = \{y/h(w)\}\{w/b\}\{z/a\}\{t/h(b)\} = \{y/h(b), w/b, z/a, t/h(b)\}.$$

Unifikační algoritmus - korektnost

Tvrzení Pro každé S unifikační algoritmus vydá po konečně mnoha krocích korektní výsledek, tj. nejobecnější unifikaci σ pro S nebo pozná, že S není unifikovatelná. (*) Navíc, pro každou unifikaci τ pro S platí, že $\tau = \sigma\tau$.

Důkaz V každém kroku eliminuje jednu proměnnou, někdy tedy skončí.

- Skončí-li neúspěchem po k krocích, nelze unifikovat $D(S_k)$, tedy ani S .
- Vydá-li $\sigma = \sigma_0\sigma_1 \cdots \sigma_k$, je σ evidentně **unifikace** pro S .
- Dokážeme-li, že σ má vlastnost (*), je σ **nejobecnější** unifikace pro S .

- (1) Necht' τ je unifikace pro S . Ukážeme, že $\tau = \sigma_0\sigma_1 \cdots \sigma_i\tau$ pro každé $i \leq k$.
- (2) Pro $i = 0$ platí (1). Necht' $\sigma_{i+1} = \{x/t\}$, předpokládejme $\tau = \sigma_0\sigma_1 \cdots \sigma_i\tau$.
- (3) Stačí dokázat, že $v\sigma_{i+1}\tau = v\tau$ pro každou proměnnou v .
- (4) Pro $v \neq x$ je $v\sigma_{i+1} = v$, tedy platí (3). Nyní $v = x$ a $v\sigma_{i+1} = x\sigma_{i+1} = t$.
- (5) Jelikož τ unifikuje $S_i = S\sigma_0\sigma_1 \cdots \sigma_i$ a proměnná x i term t jsou v $D(S_i)$, musí τ unifikovat x a t , tj. $t\tau = x\tau$, jak bylo požadováno pro (3). □

Výroková a predikátová logika - XI

Petr Gregor

KTIML MFF UK

ZS 2021/22

Obečné rezoluční pravidlo

Nechť klauzule C_1 , C_2 neobsahují stejnou proměnnou a jsou ve tvaru

$$C_1 = C'_1 \sqcup \{A_1, \dots, A_n\}, \quad C_2 = C'_2 \sqcup \{\neg B_1, \dots, \neg B_m\},$$

kde $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ lze unifikovat a $n, m \geq 1$. Pak klauzule

$$C = C'_1\sigma \cup C'_2\sigma,$$

kde σ je **nejobecnější unifikace** pro S , je **rezolventa** klauzulí C_1 a C_2 .

Např. v klauzulích $\{P(x), Q(x, z)\}$ a $\{\neg P(y), \neg Q(f(y), y)\}$ lze unifikovat $S = \{Q(x, z), Q(f(y), y)\}$ pomocí nejobecnější unifikace $\sigma = \{x/f(y), z/y\}$ a získat z nich rezolventu $\{P(f(y)), \neg P(y)\}$.

***Poznámka** Podmínce o různých proměnných lze vyhovět přejmenováním proměnných v rámci klauzule. Je to nutné, např. z $\{\{P(x)\}, \{\neg P(f(x))\}\}$ lze po přejmenování získat $\square$, ale $\{P(x), P(f(x))\}$ nelze unifikovat.*

Rezoluční důkaz

Pojmy zavedeme jako ve VL, jen navíc dovolíme přejmenování proměnných.

- **Rezoluční důkaz (odvození)** klauzule C z formule S je **konečná** posloupnost $C_0, \dots, C_n = C$ taková, že pro každé $i \leq n$ je $C_i = C'_i \sigma$, kde $C'_i \in S$ a σ je přejmenování proměnných, nebo je C_i rezolventou nějakých dvou předchozích klauzulí (i stejných).
- Klauzule C je (rezolucí) **dokazatelná** z S , psáno $S \vdash_R C$, pokud má rezoluční důkaz z S .
- **Zamítnutí** formule S je rezoluční důkaz $\square$ z S .
- S je (rezolucí) **zamítnutelná**, pokud $S \vdash_R \square$.

Poznámka Eliminace více literálů najednou je někdy nezbytná, např.

$S = \{\{P(x), P(y)\}, \{\neg P(x), \neg P(y)\}\}$ je rezolucí zamítnutelná, ale nemá zamítnutí, při kterém by se v každém kroku eliminoval pouze jeden literál.

Příklad rezoluce

Mějme teorii $T = \{\neg P(x, x), P(x, y) \rightarrow P(y, x), P(x, y) \wedge P(y, z) \rightarrow P(x, z)\}$.

Je $T \models (\exists x)\neg P(x, f(x))$? Tedy, je následující formule T' nesplnitelná?

$T' = \{\{\neg P(x, x)\}, \{\neg P(x, y), P(y, x)\}, \{\neg P(x, y), \neg P(y, z), P(x, z)\}, \{P(x, f(x))\}\}$

$T' \vdash_R \square$



x'/x

$\{P(x, x)\}$

$\{\neg P(x', x')\}$

$z/x, x'/x$

$\{\neg P(f(x), z), P(x, z)\}$

$\{P(f(x'), x')\}$

$y/f(x), x'/x$

$x/x', y/f(x')$

$\{\neg P(x, y), \neg P(y, z), P(x, z)\}$

$\{P(x', f(x'))\}$

$\{\neg P(x, y), P(y, x)\}$

$\{P(x', f(x'))\}$

Korektnost rezoluce

Nejprve ukážeme, že obecné rezoluční pravidlo je korektní.

Tvrzení Nechť C je rezolventa klauzulí C_1, C_2 . Pro každou L -strukturu $\mathcal{A}$,

$$\mathcal{A} \models C_1 \text{ a } \mathcal{A} \models C_2 \Rightarrow \mathcal{A} \models C.$$

Důkaz Nechť $C_1 = C'_1 \sqcup \{A_1, \dots, A_n\}$, $C_2 = C'_2 \sqcup \{\neg B_1, \dots, \neg B_m\}$, σ je nejobecnější unifikace pro $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ a $C = C'_1\sigma \cup C'_2\sigma$.

- Jelikož C_1, C_2 jsou otevřené, platí i $\mathcal{A} \models C_1\sigma$ a $\mathcal{A} \models C_2\sigma$.
- Máme $C_1\sigma = C'_1\sigma \cup \{S\sigma\}$ a $C_2\sigma = C'_2\sigma \cup \{\neg(S\sigma)\}$.
- Ukážeme, že $\mathcal{A} \models C[e]$ pro každé e . Je-li $\mathcal{A} \models S\sigma[e]$, pak $\mathcal{A} \models C'_1\sigma[e]$ a tedy $\mathcal{A} \models C[e]$. Jinak $\mathcal{A} \not\models S\sigma[e]$, pak $\mathcal{A} \models C'_1\sigma[e]$ a tedy $\mathcal{A} \models C[e]$. $\square$

Věta (korektnost) *Je-li formule S rezolucí zamítnutelná, je S nesplnitelná.*

Důkaz Nechť $S \vdash_R \square$. Kdyby $\mathcal{A} \models S$ pro nějakou strukturu $\mathcal{A}$, z korektnosti rezolučního pravidla by platilo i $\mathcal{A} \models \square$, což není možné. $\blacksquare$

Lifting lemma

Rezoluční důkaz na úrovni VL lze “zdvihnout” na úroveň PL.

Lemma Necht' $C_1^* = C_1\tau_1$, $C_2^* = C_2\tau_2$ jsou **základní instance** klauzulí C_1 , C_2 **neobsahující stejnou proměnnou** a C^* je rezolventa C_1^* a C_2^* . Pak existuje rezolventa C klauzulí C_1 a C_2 taková, že $C^* = C\tau_1\tau_2$ je základní instance C .

Důkaz Předpokládejme, že C^* je rezolventa C_1^* , C_2^* přes **literál** $P(t_1, \dots, t_k)$.

- Pak lze psát $C_1 = C'_1 \sqcup \{A_1, \dots, A_n\}$ a $C_2 = C'_2 \sqcup \{\neg B_1, \dots, \neg B_m\}$, kde $\{A_1, \dots, A_n\}\tau_1 = \{P(t_1, \dots, t_k)\}$ a $\{\neg B_1, \dots, \neg B_m\}\tau_2 = \{\neg P(t_1, \dots, t_k)\}$.
- Tedy $(\tau_1\tau_2)$ unifikuje $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ a je-li σ **mgu** pro S z unifikačního algoritmu, pak $C = C'_1\sigma \cup C'_2\sigma$ je rezolventa C_1 a C_2 .
- Navíc $(\tau_1\tau_2) = \sigma(\tau_1\tau_2)$ z vlastnosti $(*)$ pro σ a tedy

$$\begin{aligned} C\tau_1\tau_2 &= (C'_1\sigma \cup C'_2\sigma)\tau_1\tau_2 = C'_1\sigma\tau_1\tau_2 \cup C'_2\sigma\tau_1\tau_2 = C'_1\tau_1 \cup C'_2\tau_2 \\ &= (C_1 \setminus \{A_1, \dots, A_n\})\tau_1 \cup (C_2 \setminus \{\neg B_1, \dots, \neg B_m\})\tau_2 \\ &= (C_1^* \setminus \{P(t_1, \dots, t_k)\}) \cup (C_2^* \setminus \{\neg P(t_1, \dots, t_k)\}) = C^*. \quad \square \end{aligned}$$

Úplnost

Důsledek *Nechť S' je množina všech základních instancí klauzulí formule S . Je-li $S' \vdash_R C'$ (na úrovni VL), kde C' je základní klauzule, pak existuje klauzule C a základní substituce σ t.ž. $C' = C\sigma$ a $S \vdash_R C$ (na úrovni PL).*

Důkaz Indukcí dle délky rezolučního odvození pomocí lifting lemmatu. $\square$

Věta (úplnost) *Je-li formule S nespílitelná, je $S \vdash_R \square$.*

Důkaz Je-li S nespílitelná, dle (důsledku) Herbrandovy věty je nespílitelná i množina S' všech základních instancí klauzulí z S .

- Dle úplnosti rezoluční metody ve VL je $S' \vdash_R \square$ (na úrovni VL).
- Dle předchozího důsledku existuje klauzule C a substituce σ taková, že $\square = C\sigma$ a $S \vdash_R C$ (na úrovni PL).
- Jediná klauzule, jejíž instance je $\square$, je klauzule $C = \square$. $\blacksquare$

Lineární rezoluce

Stejně jako ve VL, rezoluční metodu lze značně omezit (bez ztráty úplnosti).

- **Lineární důkaz** klauzule C z formule S je konečná posloupnost dvojic $(C_0, B_0), \dots, (C_n, B_n)$ t.ž. C_0 je **varianta** klauzule v S a pro každé $i \leq n$
 - B_i je varianta klauzule v S nebo $B_i = C_j$ pro nějaké $j < i$, a
 - C_{i+1} je rezolventa C_i a B_i , kde $C_{n+1} = C$.
- C je **lineárně dokazatelná** z S , psáno $S \vdash_L C$, má-li lineární důkaz z S .
- **Lineární zamítnutí** S je lineární důkaz $\square$ z S .
- S je **lineárně zamítnutelná**, pokud $S \vdash_L \square$.

Věta S je lineárně zamítnutelná, právě když S je nesplnitelná.

Důkaz ($\Rightarrow$) Každý lineární důkaz lze transformovat na rezoluční důkaz.

($\Leftarrow$) Plyne z úplnosti lineární rezoluce ve VL (nedokazováno), neboť lifting lemma zachovává **linearitu** odvození. $\square$

LI-rezoluce

Stejně jako ve VL, pro Hornovy formule můžeme lineární rezoluci dál omezit.

- **LI-rezoluce** (“linear input”) z formule S je lineární rezoluce z S , ve které je každá boční klauzule B_i variantou klauzule ze (vstupní) formule S .
- Je-li klauzule C dokazatelná LI-rezolucí z S , píšeme $S \vdash_{LI} C$.
- **Hornova formule** je množina (i nekonečná) Hornových klauzulí.
- **Hornova klauzule** je klauzule obsahující nejvýše jeden pozitivní literál.
- **Fakt** je (Hornova) klauzule $\{p\}$, kde p je pozitivní literál.
- **Pravidlo** je (Hornova) klauzule s právě jedním pozitivním a aspoň jedním negativním literálem. Pravidla a fakta jsou **programové klauzule**.
- **Cíl** je neprázdná (Hornova) klauzule bez pozitivního literálu.

Věta Je-li Hornova T splnitelná a $T \cup \{G\}$ nespílitelná pro cíl G , lze $\square$ odvodit LI-rezolucí z $T \cup \{G\}$ začínající G .

Důkaz Plyne z Herbrandovy věty, stejné věty ve VL a lifting lemmatu. $\square$

Program v Prologu

Program (v Prologu) je Hornova formule obsahující pouze **programové klauzule**, tj. **fakta** nebo **pravidla**.

$\text{syn}(X, Y) :- \text{otec}(Y, X), \text{muz}(X).$

$\{\text{syn}(X, Y), \neg \text{otec}(Y, X), \neg \text{muz}(X)\}$

$\text{syn}(X, Y) :- \text{matka}(Y, X), \text{muz}(X).$

$\{\text{syn}(X, Y), \neg \text{matka}(Y, X), \neg \text{muz}(X)\}$

$\text{muz}(\text{jan}).$

$\{\text{muz}(\text{jan})\}$

$\text{otec}(\text{jiri}, \text{jan}).$

$\{\text{otec}(\text{jiri}, \text{jan})\}$

$\text{matka}(\text{julie}, \text{jan}).$

$\{\text{matka}(\text{julie}, \text{jan})\}$

$?- \text{syn}(\text{jan}, X) \quad P \models (\exists X) \text{syn}(\text{jan}, X) ? \quad \{\neg \text{syn}(\text{jan}, X)\}$

Zajímá nás, zda daný **existenční dotaz** vyplývá z daného programu.

Důsledek Pro program P a cíl $G = \{\neg A_1, \dots, \neg A_n\}$ v proměnných $X_1, \dots, X_m$

(1) $P \models (\exists X_1) \dots (\exists X_m) (A_1 \wedge \dots \wedge A_n)$, právě když

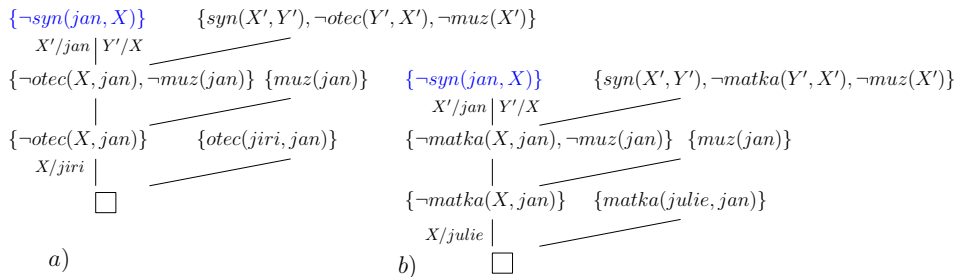
(2) $\square$ lze odvodit LI-rezolucí z $P \cup \{G\}$ začínající (variantou) cíle G .

LI-rezoluce nad programem

Je-li odpověď na dotaz kladná, chceme navíc znát výstupní substituci.

Výstupní substitute σ LI-rezoluce $\square$ z $P \cup \{G\}$ začínající $G = \{\neg A_1, \dots, \neg A_n\}$ je složení mgu v jednotlivých krocích (jen na proměnné v G). Platí,

$$P \models (A_1 \wedge \dots \wedge A_n)\sigma.$$



Výstupní substituce a) $X = \text{jiri}$, b) $X = \text{julie}$.

Hilbertovský kalkul

- základní logické spojky a kvantifikátory: $\neg$, $\rightarrow$, $(\forall x)$ (ostatní odvozené)
- dokazují se libovolné formule (nejen sentence)
- logické axiomy** (schémata logických axiomů)

$$(i) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(ii) \quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$$

$$(iii) \quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

$$(iv) \quad (\forall x)\varphi \rightarrow \varphi(x/t) \quad \text{je-li } t \text{ substituovatelný za } x \text{ do } \varphi$$

$$(v) \quad (\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi) \quad \text{není-li } x \text{ volná proměnná ve } \varphi$$

kde φ, ψ, χ jsou libovolné formule (daného jazyka), t je libovolný term a x je libovolná proměnná.

- je-li jazyk s rovností, mezi logické axiomy patří navíc **axiomy rovnosti**
- odvozovací (deduktivní) pravidla**

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi} \quad (\text{modus ponens}), \quad \frac{\varphi}{(\forall x)\varphi} \quad (\text{generalizace})$$

Pojem důkazu

Důkaz (Hilbertova stylu) formule φ z teorie T je **konečná** posloupnost $\varphi_0, \dots, \varphi_n = \varphi$ formulí taková, že pro každé $i \leq n$

- φ_i je logický axiom nebo $\varphi_i \in T$ (axiom teorie), nebo
- φ_i lze odvodit z předchozích formulí pomocí odvozovacích pravidel.

Formule φ je **dokazatelná** v T , má-li důkaz z T , značíme $T \vdash_H \varphi$.

Věta Pro každou teorii T a formuli φ , $T \vdash_H \varphi \Rightarrow T \models \varphi$.

Důkaz

- Je-li $\varphi \in T$ nebo logický axiom, je $T \models \varphi$ (logické axiomy jsou tautologie),
- jestliže $T \models \varphi$ a $T \models \varphi \rightarrow \psi$, pak $T \models \psi$, tj. *modus ponens* je korektní,
- jestliže $T \models \varphi$, pak $T \models (\forall x)\varphi$, tj. *pravidlo generalizace* je korektní,
- tedy každá formule vyskytující se v důkazu z T platí v T . $\square$

Poznámka Platí i **úplnost**, tj. $T \models \varphi \Rightarrow T \vdash_H \varphi$ pro každou teorii T a formuli φ .

Teorie struktury

Mnohdy nás zajímá, co platí v jedné konkrétní struktuře.

Teorie struktury $\mathcal{A}$ je množina $\text{Th}(\mathcal{A})$ **sentencí** (stejného jazyka) platných v $\mathcal{A}$.

Pozorování Pro každou strukturu $\mathcal{A}$ a teorii T jazyka L ,

- (i) $\text{Th}(\mathcal{A})$ je **kompletní** teorie,
- (ii) je-li $\mathcal{A} \models T$, je $\text{Th}(\mathcal{A})$ jednoduchá (kompletní) **extenze** teorie T ,
- (iii) je-li $\mathcal{A} \models T$ a T je kompletní, je $\text{Th}(\mathcal{A})$ **ekvivalentní** s T ,
tj. $\theta^L(T) = \text{Th}(\mathcal{A})$.

Např. pro $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je $\text{Th}(\underline{\mathbb{N}})$ **aritmetika přirozených čísel**.

Poznámka Později uvidíme, že ačkoliv je $\text{Th}(\underline{\mathbb{N}})$ kompletní teorie, je (algoritmicky) **nerozhodnutelná**.

Elementární ekvivalence

- Struktury $\mathcal{A}$ a $\mathcal{B}$ jazyka L jsou *elementárně ekvivalentní*, psáno $\mathcal{A} \equiv \mathcal{B}$, pokud v nich platí stejné formule (jazyka L), tj. $\text{Th}(\mathcal{A}) = \text{Th}(\mathcal{B})$.

Např. $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$, ale $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$, neboť v $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, zatímco v $\langle \mathbb{Q}, \leq \rangle$ ne.

- T je kompletní, právě když má až na el. ekvivalenci právě jeden model.

Např. teorie DeLO hustých lineárních uspořádání bez konců je kompletní.

Zajímá nás, jak vypadají modely dané teorie (až na elementární ekvivalenci).

Pozorování Pro modely $\mathcal{A}, \mathcal{B}$ teorie T platí $\mathcal{A} \equiv \mathcal{B}$, právě když $\text{Th}(\mathcal{A}), \text{Th}(\mathcal{B})$ jsou *ekvivalentní* (jednoduché kompletní extenze teorie T).

Poznámka Lze-li *efektivně* (algoritmicky) popsat pro efektivně danou teorii T , jak vypadají všechny její kompletní extenze, je T (algoritmicky) *rozhodnutelná*.

Jednoduché kompletní extenze - příklad

Teorie *DeLO** hustého lineárního uspořádání jazyka $L = \langle \leq \rangle$ s rovností je

$$x \leq x \quad (\text{reflexivita})$$

$$x \leq y \wedge y \leq x \rightarrow x = y \quad (\text{antisymetrie})$$

$$x \leq y \wedge y \leq z \rightarrow x \leq z \quad (\text{tranzitivita})$$

$$x \leq y \vee y \leq x \quad (\text{dichotomie})$$

$$x < y \rightarrow (\exists z)(x < z \wedge z < y) \quad (\text{hustota})$$

$$(\exists x)(\exists y)(x \neq y) \quad (\text{netrivialita})$$

kde ' $x < y$ ' je zkratka za ' $x \leq y \wedge x \neq y$ '.

Označme φ, ψ sentence $(\exists x)(\forall y)(x \leq y)$, resp. $(\exists x)(\forall y)(y \leq x)$. Uvidíme, že

$$DeLO = DeLO^* \cup \{\neg\varphi, \neg\psi\}, \quad DeLO^\pm = DeLO^* \cup \{\varphi, \psi\},$$

$$DeLO^+ = DeLO^* \cup \{\neg\varphi, \psi\}, \quad DeLO^- = DeLO^* \cup \{\varphi, \neg\psi\}$$

jsou všechny (neekvivalentní) jednoduché kompletní extenze teorie *DeLO**.

Důsledek Löwenheim-Skolemovy věty

Pomocí kanonického modelu (s rovností) jsme dříve dokázali následující větu.

Věta *Nechť T je bezesporná teorie spočetného jazyka L . Je-li L bez rovnosti, má T model, který je **spočetně nekonečný**. Je-li L s rovností, má T model, který je **spočetný**.*

Důsledek *Ke každé struktuře $\mathcal{A}$ spočetného jazyka **bez rovnosti** existuje **spočetně nekonečná** elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Teorie $\text{Th}(\mathcal{A})$ je bezesporná, neboť má model $\mathcal{A}$. Dle předchozí věty má spočetně nek. model $\mathcal{B}$. Jelikož je teorie $\text{Th}(\mathcal{A})$ kompletní, je $\mathcal{A} \equiv \mathcal{B}$. $\square$

Důsledek *Ke každé **nekonečné** struktuře $\mathcal{A}$ spočetného jazyka **s rovností** existuje **spočetně nekonečná** elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Obdobně jako výše. Jelikož v $\mathcal{A}$ neplatí sentence “existuje právě n prvků” pro žádné $n \in \mathbb{N}$ a $\mathcal{A} \equiv \mathcal{B}$, není $\mathcal{B}$ konečná, tedy je nekonečná. $\square$

Spočetné algebraicky uzavřené těleso

Řekneme, že těleso $\mathcal{A}$ je *algebraicky uzavřené*, pokud v něm každý polynom (nenulového stupně) má kořen, tj. pro každé $n \geq 1$ platí

$$\mathcal{A} \models (\forall x_{n-1}) \dots (\forall x_0) (\exists y) (y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0)$$

kde y^k je zkratka za term $y \cdot y \cdot \dots \cdot y$ ($\cdot$ aplikováno $(k - 1)$ -krát).

Např. těleso $\mathbb{C} = \langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ je algebraicky uzavřené, zatímco tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou (neboť polynom $x^2 + 1$ v nich nemá kořen).

Důsledek Existuje *spočetné algebraicky uzavřené těleso*.

Důkaz Dle předchozího důsledku existuje spočetná struktura (nekonečná), která je elementárně ekvivalentní s tělesem $\mathbb{C}$, tedy je to rovněž algebraicky uzavřené těleso. $\square$

Výroková a predikátová logika - XII

Petr Gregor

KTIML MFF UK

ZS 2021/22

Izomorfismus struktur

Nechť $\mathcal{A}, \mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$.

- **Bijekce** $h: A \rightarrow B$ je **izomorfismus** struktur $\mathcal{A}$ a $\mathcal{B}$, pokud platí zároveň

$$(i) \quad h(f^A(a_1, \dots, a_n)) = f^B(h(a_1), \dots, h(a_n))$$

pro každý n -ární funkční symbol $f \in \mathcal{F}$ a každé $a_1, \dots, a_n \in A$,

$$(ii) \quad R^A(a_1, \dots, a_n) \Leftrightarrow R^B(h(a_1), \dots, h(a_n))$$

pro každý n -ární relační symbol $R \in \mathcal{R}$ a každé $a_1, \dots, a_n \in A$.

- $\mathcal{A}$ a $\mathcal{B}$ jsou **izomorfní** (via h), psáno $\mathcal{A} \simeq \mathcal{B}$ ($\mathcal{A} \simeq_h \mathcal{B}$), pokud existuje izomorfismus h struktur $\mathcal{A}$ a $\mathcal{B}$. Říkáme rovněž, že $\mathcal{A}$ je **izomorfní s** $\mathcal{B}$.
- **Automorfismus** struktury $\mathcal{A}$ je izomorfismus $\mathcal{A}$ s $\mathcal{A}$.

Např. potenční algebra $\mathcal{P}(X) = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ s $X = n$ je izomorfní s Booleovou algebrou $\underline{n}2 = \langle {}^n2, -_n, \wedge_n, \vee_n, 0_n, 1_n \rangle$ via $h: A \mapsto \chi_A$, kde χ_A je charakteristická funkce množiny $A \subseteq X$.

Izomorfismus a sémantika

Uvidíme, že izomorfismus zachovává sémantiku.

Tvrzení Necht' $\mathcal{A}, \mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$. Bijekce $h: A \rightarrow B$ je **izomorfismus** $\mathcal{A}$ a $\mathcal{B}$, právě když platí zároveň

- (i) $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[e \circ h]$ pro každý term t a $e: \text{Var} \rightarrow A$,
- (ii) $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[e \circ h]$ pro každou formuli φ a $e: \text{Var} \rightarrow A$.

Důkaz ($\Rightarrow$) Indukcí dle struktury termu t , respektive formule φ .

($\Leftarrow$) Dosazením termu $f(x_1, \dots, x_n)$ do (i) či atomické formule $R(x_1, \dots, x_n)$ do (ii) pro ohodnocení $e(x_i) = a_i$ máme, že h vyhovuje def. izomorfismu. $\square$

Důsledek Pro každé struktury $\mathcal{A}, \mathcal{B}$ stejného jazyka,

$$\mathcal{A} \simeq \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}.$$

Poznámka Obrácená implikace **obecně** neplatí, např. $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, ale $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{R}, \leq \rangle$, neboť $|\mathbb{Q}| = \omega$ a $|\mathbb{R}| = 2^\omega$.

Konečné modely s rovností

Tvrzení Pro každé *konečné* struktury $\mathcal{A}, \mathcal{B}$ stejného jazyka s *rovností*,

$$\mathcal{A} \equiv \mathcal{B} \Rightarrow \mathcal{A} \simeq \mathcal{B}.$$

Důkaz Je $|A| = |B|$, neboť lze vyjádřit “existuje právě n prvků”.

- Nechť $\mathcal{A}'$ je expanze $\mathcal{A}$ do jazyka $L' = L \cup \{c_a\}_{a \in A}$ o *jména prvků* z A .
- Ukážeme, že $\mathcal{B}$ lze expandovat na $\mathcal{B}'$ do jazyka L' tak, že $\mathcal{A}' \equiv \mathcal{B}'$. Pak zřejmě $h: a \mapsto c_a^{B'}$ je izomorfismus $\mathcal{A}'$ s $\mathcal{B}'$ a tedy i izomorfismus $\mathcal{A}$ s $\mathcal{B}$.
- Stačí ukázat, že pro každé $c_a^{A'} = a \in A$ existuje $b \in B$ t.ž. $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.
- Označme Ω množinu formulí $\varphi(x)$ t.ž. $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, tj. $\mathcal{A} \models \varphi[e(x/a)]$.
- Jelikož je A konečné, existuje konečně formulí $\varphi_0(x), \dots, \varphi_m(x)$ tak, že pro každé $\varphi \in \Omega$ je $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$ pro nějaké i .
- Jelikož $\mathcal{B} \equiv \mathcal{A} \models (\exists x) \bigwedge_{i \leq m} \varphi_i$, existuje $b \in B$ t.ž. $\mathcal{B} \models \bigwedge_{i \leq m} \varphi_i[e(x/b)]$.
- Tedy pro každou $\varphi \in \Omega$ je $\mathcal{B} \models \varphi[e(x/b)]$, tj. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$. $\square$

Důsledek Má-li *kompletní* teorie jazyka s *rovností* konečný model, jsou všechny její modely *izomorfní*.

Kategoričnost

- *Izomorfní spektrum* teorie T je počet $I(\kappa, T)$ navzájem neizomorfních modelů teorie T pro každou **kardinalitu** κ .
- Teorie T je **κ -kategoričná**, pokud má až na izomorfismus právě jeden model kardinality κ , tj. $I(\kappa, T) = 1$.

Tvrzení Teorie DeLO (tj. “bez konců”) je ω -kategoričná.

Důkaz Nechť $\mathcal{A}, \mathcal{B} \models \text{DeLO}$ s $A = \{a_i\}_{i \in \mathbb{N}}$, $B = \{b_i\}_{i \in \mathbb{N}}$. Indukcí dle n lze nalézt prosté **parciální** funkce $h_n \subseteq h_{n+1} \subset A \times B$ **zachovávající uspořádání** tak, že $\{a_i\}_{i < n} \subseteq \text{dom}(h_n)$ a $\{b_i\}_{i < n} \subseteq \text{rng}(h_n)$. Pak $\mathcal{A} \simeq \mathcal{B}$ via $h = \cup h_n$. $\square$

Obdobně dostaneme, že např. $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$, $\mathcal{A} \upharpoonright (0, 1]$, $\mathcal{A} \upharpoonright [0, 1)$, $\mathcal{A} \upharpoonright [0, 1]$ jsou až na izomorfismus všechny spočetné modely teorie DeLO. Pak*

$$I(\kappa, \text{DeLO}^*) = \begin{cases} 0 & \text{pro } \kappa \in \mathbb{N}, \\ 4 & \text{pro } \kappa = \omega. \end{cases}$$

ω -kategorické kritérium kompletnosti

Věta *Nechť jazyk L je spočetný.*

- (i) Je-li teorie T jazyka L bez rovnosti ω -kategorická, je kompletní.*
- (ii) Je-li teorie T jazyka L s rovností ω -kategorická a bez konečného modelu, je kompletní.*

Důkaz Každý model teorie T je elementárně ekvivalentní s nějakým spočetně nekonečným modelem T , ale ten je až na izomorfismus jediný. Tedy všechny modely T jsou elementárně ekvivalentní, tj. T je kompletní. $\square$

Např. teorie $DeLO$, $DeLO^+$, $DeLO^-$, $DeLO^\pm$ jsou kompletní a jsou to všechny (navzájem neekvivalentní) jednoduché kompletní extenze teorie $DeLO^$.*

Poznámka *Obdobné kritérium platí i pro vyšší kardinality než ω .*

Definovatelné množiny

Zajímá nás, které množiny lze v dané struktuře zadefinovat.

- **Množina definovaná formulí** $\varphi(x_1, \dots, x_n)$ **ve struktuře** $\mathcal{A}$ je množina

$$\varphi^{\mathcal{A}}(x_1, \dots, x_n) = \{(a_1, \dots, a_n) \in A^n \mid \mathcal{A} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]\}.$$

Zkráceným zápisem, $\varphi^{\mathcal{A}}(\bar{x}) = \{\bar{a} \in A^{|\bar{x}|} \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a})]\}$, kde $|\bar{x}| = n$.

- **Množina definovaná formulí** $\varphi(\bar{x}, \bar{y})$ **s parametry** $\bar{b} \in A^{|\bar{y}|}$ **ve struktuře** $\mathcal{A}$ je

$$\varphi^{\mathcal{A}, \bar{b}}(\bar{x}, \bar{y}) = \{\bar{a} \in A^{|\bar{x}|} \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a}, \bar{y}/\bar{b})]\}.$$

Např. pro $\varphi = E(x, y)$ je $\varphi^{\mathcal{G}, b}(x, y)$ množina sousedů vrcholu b v grafu $\mathcal{G}$.

- Pro strukturu $\mathcal{A}$, množinu $B \subseteq A$ a $n \in \mathbb{N}$ označme $\text{Df}^n(\mathcal{A}, B)$ třídu všech množin $D \subseteq A^n$ definovatelných ve struktuře $\mathcal{A}$ s parametry z B .

Pozorování $\text{Df}^n(\mathcal{A}, B)$ je uzavřená na doplněk, sjednocení, průnik a obsahuje $\emptyset, A^n$. Tedy tvoří podalgebru potenční algebry $\mathcal{P}(A^n)$.

Definovatelnost a automorfismy

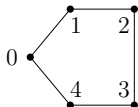
Ukážeme, že definovatelné množiny jsou invariantní na automorfismy.

Tvrzení *Nechť $D \subseteq A^n$ je množina definovatelná ve struktuře $\mathcal{A}$ z parametrů $\bar{b}$ a h je **automorfismus** $\mathcal{A}$, který je **identický** na $\bar{b}$. Pak $h[D] = D$.*

Důkaz *Nechť $D = \varphi^{\mathcal{A}, \bar{b}}(\bar{x}, \bar{y})$. Pak pro každé $\bar{a} \in A^{|\bar{x}|}$*

$$\begin{aligned} \bar{a} \in D &\Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \Leftrightarrow \mathcal{A} \models \varphi[(e \circ h)(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \\ &\Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/h(\bar{a}), \bar{y}/h(\bar{b}))] \Leftrightarrow \mathcal{A} \models \varphi[e(\bar{x}/h(\bar{a}), \bar{y}/\bar{b})] \Leftrightarrow h(\bar{a}) \in D. \end{aligned}$$

Např. graf $\mathcal{G}$ má právě jeden netrivi. automorfismus h zachovávající vrchol 0.



$$h(0) = 0, \quad h(1) = 4, \quad h(2) = 3, \quad h(3) = 2, \quad h(4) = 1$$

$$\{0\} = (x = y)^{\mathcal{G}, 0}, \quad \{1, 4\} = (E(x, y))^{\mathcal{G}, 0}, \quad \{2, 3\} = (x \neq y \wedge \neg E(x, y))^{\mathcal{G}, 0}$$

Navíc množiny $\{0\}$, $\{1, 4\}$, $\{2, 3\}$ jsou definovatelné z parametru 0. Tedy

$$\text{Df}^1(\mathcal{G}, \{0\}) = \{\emptyset, \{0\}, \{1, 4\}, \{2, 3\}, \{0, 1, 4\}, \{0, 2, 3\}, \{1, 4, 2, 3\}, \{0, 1, 2, 3, 4\}\}.$$

Axiomatizovatelnost

Zajímá nás, zda se daná část světa dá “dobře” popsat.

Nechť $K \subseteq M(L)$ je třída struktur jazyka L . Řekneme, že K je

- **axiomatizovatelná**, pokud existuje teorie T jazyka L s $M(T) = K$,
- **konečně axiomatizovatelná**, pokud je axiomatizovatelná **konečnou** teorií,
- **otevřeně axiomatizovatelná**, pokud je axiomatizovatelná **otevřenou** teorií,
- teorie T je **konečně (otevřeně) axiomatizovatelná**, pokud $M(T)$ je konečně (respektive otevřeně) axiomatizovatelná.

Pozorování *Je-li K axiomatizovatelná, je uzavřená na elem. ekvivalenci.*

Například

- lineární uspořádání jsou konečně i otevřeně axiomatizovatelná,*
- tělesa jsou konečně axiomatizovatelná, ale ne otevřeně,*
- nekonečné grupy jsou axiomatizovatelné, ale ne konečně.*

Důsledek kompaktnosti

Věta Má-li teorie T pro každé $n \in \mathbb{N}$ alespoň n -prvkový model, má i nekonečný model.

Důkaz V jazyce bez rovnosti je to zřejmé, uvažme jazyk s rovností.

- Označme $T' = T \cup \{c_i \neq c_j \mid \text{pro } i \neq j\}$ extenzi teorie T v rozšířeném jazyce o spočetně nekonečně mnoho nových konstantních symbolů c_i .
- Dle předpokladu má každá konečná část teorie T' model.
- Tedy dle věty o **kompaktnosti** má T' model, ten je nutně nekonečný.
- Jeho redukt na původní jazyk je hledaný nekonečný model teorie T . □

Důsledek Má-li teorie T pro každé $n \in \mathbb{N}$ alespoň n -prvkový model, není třída všech jejích konečných modelů axiomatizovatelná.

Např. nelze axiomatizovat konečné grupy, konečná tělesa, atd. Avšak třída nekonečných modelů teorie T jazyka s rovností je axiomatizovatelná.

Konečná axiomatizovatelnost

Věta Necht' $K \subseteq M(L)$ a $\overline{K} = M(L) \setminus K$, kde L je jazyk. Pak K je *konečně axiomatizovatelná*, právě když K i $\overline{K}$ jsou axiomatizovatelné.

Důkaz ($\Rightarrow$) Je-li T konečná axiomatizace K v *uzavřeném* tvaru, pak teorie s jediným axiomem $\bigvee_{\varphi \in T} \neg \varphi$ axiomatizuje $\overline{K}$. Nyní dokažme ($\Leftarrow$).

- Necht' T, S jsou teorie jazyka L takové, že $M(T) = K$, $M(S) = \overline{K}$.
- Pak $M(T \cup S) = M(T) \cap M(S) = \emptyset$ a dle věty o *kompaktnosti* existují konečné $T' \subseteq T$ a $S' \subseteq S$ takové, že $\emptyset = M(T' \cup S') = M(T') \cap M(S')$.
- Jelikož

$$M(T) \subseteq M(T') \subseteq \overline{M(S')} \subseteq \overline{M(S)} = M(T),$$

je $M(T) = M(T')$, tj. konečná T' axiomatizuje K . $\square$

Konečná axiomatizovatelnost - příklad

Nechť T je teorie těles. Řekneme, že těleso $\mathcal{A} = \langle A, +, -, \cdot, 0, 1 \rangle$ je

- **charakteristiky 0**, neexistuje-li žádné $p \in \mathbb{N}^+$ takové, že $\mathcal{A} \models p1 = 0$, kde $p1$ značí term $1 + 1 + \dots + 1$ ($+$ aplikováno $(p - 1)$ -krát).
- **charakteristiky p** , kde p je prvočíslo, je-li p je nejmenší t.ž. $\mathcal{A} \models p1 = 0$.
- Třída těles charakteristiky p pro p prvočíslo je **konečně** axiomatizována teorií $T \cup \{p1 = 0\}$.
- Třída těles charakteristiky 0 je axiomatizována (**nekonečnou**) teorií $T' = T \cup \{p1 \neq 0 \mid p \in \mathbb{N}^+\}$.

Tvrzení Třída K těles charakteristiky 0 není **konečně** axiomatizovatelná.

Důkaz Stačí dokázat, že $\overline{K}$ není axiomatizovatelná. Kdyby $M(S) = \overline{K}$, tak $S' = S \cup T'$ má model $\mathcal{B}$, neboť každá konečná $S^* \subseteq S'$ má model (těleso prvočíselné charakteristiky větší než jakékoliv p vyskytující se v axiomech S^*). Pak ale $\mathcal{B} \in M(S) = \overline{K}$ a zároveň $\mathcal{B} \in M(T') = K$, což není možné. $\square$

Výroková a predikátová logika - XIII

Petr Gregor

KTIML MFF UK

ZS 2021/22

Otevřená axiomatizovatelnost

Věta *Je-li teorie T otevřeně axiomatizovatelná, pak každá podstruktura modelu T je rovněž modelem T .*

Důkaz Nechť T' je otevřená axiomatika $M(T)$, $\mathcal{A} \models T'$ a $\mathcal{B} \subseteq \mathcal{A}$. Víme, že pro každé $\varphi \in T'$ je $\mathcal{B} \models \varphi$, neboť φ je otevřená. Tedy $\mathcal{B}$ je modelem T' . $\square$

Poznámka *Platí i obrácená implikace, tj. je-li každá podstruktura modelu teorie T rovněž modelem T , pak T je otevřeně axiomatizovatelná.*

Např. teorie DeLO není otevřeně axiomatizovatelná, neboť např. konečná podstruktura modelu DeLO není modelem DeLO.

Např. nejvýše n -prvkové grupy pro pevné $n > 1$ jsou otevřeně axiomatizovány

$$T \cup \left\{ \bigvee_{\substack{i,j \leq n \\ i \neq j}} x_i = x_j \right\},$$

kde T je (otevřená) teorie grup.

Rekurzivní axiomatizace a rozhodnutelnost

- Intuitivní pojem “*algorithmus*” lze přesně formalizovat (např. pomocí TS).
- Teorie T je *rekurzivně axiomatizovaná*, pokud existuje algoritmus, který pro každou vstupní formuli φ *skončí* a oznámí, zda $\varphi \in T$.
- Teorie T je *rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ *skončí* a oznámí, zda $\varphi \in Thm(T)$.
- Teorie T je *částečně rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ *skončí*, právě když $\varphi \in Thm(T)$.

Tvrzení Pro každou rekurzivně axiomatizovanou teorii T ,

- (i) T je *částečně rozhodnutelná*,
- (ii) je-li navíc T *kompletní*, je T *rozhodnutelná*.

Důkaz Konstrukce systematického tabla z T s $F\varphi$ v kořeni poskytuje algoritmus, který rozpoznává $T \vdash \varphi$. Je-li navíc T *kompletní*, *paralelní* konstrukce pro $F\varphi$ resp. $T\varphi$ v kořeni rozhoduje, zda $T \vdash \varphi$ či $T \vdash \neg\varphi$. □

Rekurzivně spočetná kompletace

Co když efektivně popíšeme všechny jednoduché kompletní extenze?

Řekneme, že množina všech (až na ekvivalenci) **jednoduchých kompletních extenzí** teorie T je **rekurzivně spočetná**, existuje-li algoritmus $\alpha(i, j)$, který generuje i -tý axiom j -té extenze (při nějakém očíslování), případně oznámí, že (takový axiom či extenze) neexistuje.

Tvrzení *Je-li teorie T rekurzivně axiomatizovaná a množina všech (až na ekvivalenci) jejích jednoduchých kompletních extenzí je rekurzivně spočetná, je T rozhodnutelná.*

Důkaz Díky rek. axiomatizaci poskytuje konstrukce systematického tabla z T s $F\varphi$ v kořeni algoritmus pro rozpoznání $T \vdash \varphi$. Pokud ale $T \not\vdash \varphi$, pak $T' \vdash \neg\varphi$ v nějaké jednoduché kompletní extenzi T' teorie T . To lze rozpoznat **paralelní postupnou** konstrukcí systematických tabel pro $T\varphi$ z jednotlivých extenzí.

V i -tém stupni se sestojí tabla do i kroků pro prvních i extenzí. $\square$

Příklady rozhodnutelných teorií

Následující teorie jsou rozhodnutelné, ačkoliv jsou nekompletní.

- teorie **čisté rovnosti**; bez axiomů v jazyce $L = \langle \rangle$ s rovností,
- teorie **unárního predikátu**; bez axiomů v jazyce $L = \langle U \rangle$ s rovností, kde U je unární relační symbol,
- teorie **hustých lineárních uspořádání** $DeLO^*$,
- teorie **algebraicky uzavřených těles** v jazyce $L = \langle +, -, \cdot, 0, 1 \rangle$ s rovností, s axiomy teorie těles a navíc axiomy pro každé $n \geq 1$,

$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0),$$

kde y^k je zkratka za term $y \cdot y \cdot \dots \cdot y$ ($\cdot$ aplikováno $(k - 1)$ -krát).

- teorie **komutativních grup**,
- teorie **Booleových algeber**.

Rekurzivní axiomatizovatelnost

Dají se matematické struktury “efektivně” popsat?

- Třída $K \subseteq M(L)$ je **rekurzivně axiomatizovatelná**, pokud existuje rekurzivně axiomatizovaná teorie T jazyka L s $M(T) = K$.
- Teorie T je **rekurzivně axiomatizovatelná**, pokud $M(T)$ je rekurzivně axiomatizovatelná.

Tvrzení Pro každou **konečnou** strukturu $\mathcal{A}$ v konečném jazyce s rovností je $\text{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná. Tedy, $\text{Th}(\mathcal{A})$ je **rozhodnutelná**.

Důkaz Nechť $A = \{a_1, \dots, a_n\}$. Teorii $\text{Th}(\mathcal{A})$ axiomatizujeme jednou sentencí (tedy rekurzivně) kompletně popisující $\mathcal{A}$. Bude tvaru “existuje právě n prvků $a_1, \dots, a_n$ splňujících právě ty **základní vztahy** o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$.” $\square$

Příklady rekurzivní axiomatizovatelnosti

Následující struktury $\mathcal{A}$ mají **rekurzivně** axiomatizovatelnou teorii $\text{Th}(\mathcal{A})$.

- $\langle \mathbb{Z}, \leq \rangle$, teorií **diskrétních lineárních uspořádání**,
- $\langle \mathbb{Q}, \leq \rangle$, teorií **hustých lineárních uspořádání bez konců** (*DeLO*),
- $\langle \mathbb{N}, S, 0 \rangle$, teorií **následníka s nulou**,
- $\langle \mathbb{N}, S, +, 0 \rangle$, tzv. **Presburgerovou aritmetikou**,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorií **reálně uzavřených těles**,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorií **algebraicky uzavřených těles charakteristiky 0**.

Důsledek Pro uvedené struktury je $\text{Th}(\mathcal{A})$ **rozhodnutelná**.

Poznámka Uvidíme, že ale $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ rekurzivně axiomatizovat **nelze**. (Vyplývá to z první Gödelovy věty o neúplnosti).

Robinsonova aritmetika

Jak *efektivně* a přitom co nejúplněji axiomatizovat $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$?

Jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností.

Robinsonova aritmetika Q má axiomy (konečně mnoho)

$$S(x) \neq 0$$

$$x \cdot 0 = 0$$

$$S(x) = S(y) \rightarrow x = y$$

$$x \cdot S(y) = x \cdot y + x$$

$$x + 0 = x$$

$$x \neq 0 \rightarrow (\exists y)(x = S(y))$$

$$x + S(y) = S(x + y)$$

$$x \leq y \leftrightarrow (\exists z)(z + x = y)$$

Poznámka Q je velmi slabá, např. nedokazuje komutativitu či asociativitu operací $+$, $\cdot$ ani tranzitivitu $\leq$. Nicméně postačuje například k důkazu *existenčních* tvrzení o numerálech, která jsou pravdivá v $\underline{\mathbb{N}}$.

Např. pro $\varphi(x, y)$ tvaru $(\exists z)(x + z = y)$ je

$$Q \vdash \varphi(\underline{1}, \underline{2}), \quad \text{kde } \underline{1} = S(0) \text{ a } \underline{2} = S(S(0)).$$

Peanova aritmetika

Peanova aritmetika PA má axiomy

(a) Robinsonovy aritmetiky Q,

(b) schéma indukce, tj. pro každou formuli $\varphi(x, \bar{y})$ jazyka L axiom

$$(\varphi(0, \bar{y}) \wedge (\forall x)(\varphi(x, \bar{y}) \rightarrow \varphi(S(x), \bar{y}))) \rightarrow (\forall x)\varphi(x, \bar{y}).$$

Poznámka PA je poměrně dobrou aproximací $\text{Th}(\mathbb{N})$, dokazuje všechny základní vlastnosti platné v $\mathbb{N}$ (např. komutativitu +). Na druhou stranu existují sentence pravdivé v $\mathbb{N}$ ale nezávislé v PA.

Poznámka V jazyce 2. řádu lze axiomatizovat $\mathbb{N}$ (až na izomorfismus), vezmeme-li místo schéma indukce přímo axiom indukce (2. řádu)

$$(\forall X) ((X(0) \wedge (\forall x)(X(x) \rightarrow X(S(x)))) \rightarrow (\forall x) X(x)).$$

Hilbertův 10. problém

- Necht' $p(x_1, \dots, x_n)$ je polynom s celočíselnými koeficienty.
Má **Diofantická rovnice** $p(x_1, \dots, x_n) = 0$ **celočíselné** řešení?
- Hilbert (1900) “Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má **celočíselné** řešení.”

Poznámka Ekvivalentně lze požadovat algoritmus rozhodující, zda existuje řešení v **přirozených** číslech.

Věta (DPRM, 1970) Problém existence celočíselného řešení dané Diofantické rovnice s celočíselnými koeficienty je alg. **nerozhodnutelný**.

Důsledek Neexistuje algoritmus rozhodující pro dané polynomy $p(x_1, \dots, x_n)$, $q(x_1, \dots, x_n)$ s **přirozenými** koeficienty, zda

$$\mathbb{N} \models (\exists x_1) \dots (\exists x_n) (p(x_1, \dots, x_n) = q(x_1, \dots, x_n)).$$

Nerozhodutelnost predikátové logiky

*Existuje algoritmus, rozhodující o dané sentenci, zda je **logicky** pravdivá?*

- Víme, že **Robinsonova aritmetika** Q má konečně axiomů, má za model $\mathbb{N}$ a stačí k důkazu **existenčních** tvrzení o numerálech, která platí v $\mathbb{N}$.

- Přesněji, pro každou existenční formuli $\varphi(x_1, \dots, x_n)$ jazyka aritmetiky

$$Q \vdash \varphi(\underline{a_1}, \dots, \underline{a_n}) \Leftrightarrow \mathbb{N} \models \varphi[e(x_1/\underline{a_1}, \dots, x_n/\underline{a_n})]$$

pro každé $a_1, \dots, a_n \in \mathbb{N}$, kde $\underline{a_i}$ značí a_i -tý numerál.

- Speciálně, pro φ tvaru $(\exists x_1) \dots (\exists x_n)(p(x_1, \dots, x_n) = q(x_1, \dots, x_n))$, kde p, q jsou polynomy s přirozenými koeficienty (numerály), platí

$$\mathbb{N} \models \varphi \Leftrightarrow Q \vdash \varphi \Leftrightarrow \vdash \psi \rightarrow \varphi \Leftrightarrow \models \psi \rightarrow \varphi,$$

kde ψ je konjunkce (uzávěrů) všech axiomů Q .

- Tedy, pokud by existoval algoritmus rozhodující **logickou pravdivost**, existoval by i algoritmus rozhodující, zda $\mathbb{N} \models \varphi$, což není možné.

Gödelova 1. věta o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence **pravdivá** v $\mathbb{N}$ a **nedokazatelná** v T .*

Poznámky

- “Rekurzivně axiomatizovaná” znamená, že je “efektivně zadaná”.
- “Extenze R . aritmetiky” znamená, že je “základní aritmetické síly”.
- Je-li navíc $\mathbb{N} \models T$, je teorie T **nekompletní**.
- V důkazu sestavená sentence vyjadřuje “**nejsem dokazatelná v T** ”.
- Důkaz je založen na dvou principech:
 - (a) **aritmetizaci syntaxe**,
 - (b) **self-referenci**.

Aritmetizace - predikát dokazatelnosti

- **Konečné objekty** syntaxe (symboly jazyka, termy, formule, konečná tabla, tablo důkazy) lze vhodně **zakódovat** přirozenými čísly.
- Nechť $\lceil \varphi \rceil$ značí kód formule φ a nechť $\underline{\varphi}$ značí **numerál** (term jazyka aritmetiky) reprezentující $\lceil \varphi \rceil$.
- Je-li T rekurzivně axiomatizovaná, je relace $\text{Prf}_T \subseteq \mathbb{N}^2$ **rekurzivní**.

$$\text{Prf}_T(x, y) \Leftrightarrow (\text{tablo}) \text{ } y \text{ je důkazem (sentence) } x \text{ v } T.$$

- Je-li T navíc extenze Robinsonovy aritmetiky Q , dá se dokázat, že Prf_T je **reprezentovatelná** nějakou formulí $\text{Prf}_T(x, y)$ tak, že pro každé $x, y \in \mathbb{N}$

$$Q \vdash \text{Prf}_T(\underline{x}, \underline{y}), \quad \text{je-li} \quad \text{Prf}_T(x, y),$$

$$Q \vdash \neg \text{Prf}_T(\underline{x}, \underline{y}), \quad \text{jinak.}$$

- $\text{Prf}_T(x, y)$ vyjadřuje “ y je důkaz x v T ”.
- $(\exists y)\text{Prf}_T(x, y)$ vyjadřuje “ x je dokazatelná v T ”.
- Je-li $T \vdash \varphi$, pak $\mathbb{N} \models (\exists y)\text{Prf}_T(\underline{\varphi}, y)$ a navíc $T \vdash (\exists y)\text{Prf}_T(\underline{\varphi}, y)$.

Princip self-reference

- *Tato věta má 16 písmen.*

Self-reference ve formálních systémech většinou není přímo k dispozici.

- *Následující věta má 24 písmen "Následující věta má 24 písmen".*

Přímá reference obvykle je k dispozici, stačí, když umíme "mluvit" o posloupnostech symbolů. Uvedená věta ale není self-referenční.

- *Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen".*

Pomocí přímé reference lze dosáhnout self-reference. Namísto "má x písmen" může být jiná vlastnost.

- `main(){char *c="main(){char *c=%c%s%c; printf(c,34,c,34);}"; printf(c,34,c,34);}`

Věta o pevném bodě

Věta Necht' T je bezesporné rozšíření Robinsonovy aritmetiky. Pro každou formuli $\varphi(x)$ jazyka teorie T existuje sentence ψ taková, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.

Poznámka Sentence ψ je self-referenční, říká “splňuji podmínku φ ”.

Důkaz (idea) Uvažme **zdvojující** funkci d takovou, že pro každou formuli $\chi(x)$

$$d(\lceil \chi(x) \rceil) = \lceil \chi(\underline{\chi(x)}) \rceil$$

- Platí, že d je **reprezentovatelná** v T . Předpokládejme (pro jednoduchost), že nějakým termem, který si označme d , stejně jako funkci d .

- Pak pro každou formuli $\chi(x)$ jazyka teorie T platí

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \quad (1)$$

- Za ψ vezmeme sentenci $\varphi(d(\underline{\varphi(d(x))}))$. Stačí ověřit $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.

- To plyne z (1) pro $\chi(x)$ tvaru $\varphi(d(x))$, neboť v tom případě

$$T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))} \quad \square$$

Nedefinovatelnost pravdy

Řekneme, že formule $\tau(x)$ **definuje pravdu** v aritmetické teorii T , pokud pro každou sentenci φ platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Věta V žádném bezesporném rozšíření Robinsonovy aritmetiky neexistuje definice pravdy.

Důkaz Dle věty o pevném bodě pro $\neg\tau(x)$ existuje sentence φ taková, že

$$T \vdash \varphi \leftrightarrow \neg\tau(\underline{\varphi}).$$

Kdyby formule $\tau(x)$ definovala pravdu v T , bylo by

$$T \vdash \varphi \leftrightarrow \neg\varphi,$$

což v bezesporné teorii není možné. $\square$

Poznámka Důkaz je založen na paradoxu lháře, sentence φ by vyjadřovala “nejsem pravdivá v T ”.

Důkaz 1. věty o neúplnosti

Věta (Gödel) Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence **pravdivá** v $\mathbb{N}$ a **nedokazatelná** v T .

Důkaz Nechť $\varphi(x)$ je $\neg(\exists y)Prf_T(x, y)$, vyjadřuje “ x není dokazatelná v T ”.

- Dle věty o pevném bodě pro $\varphi(x)$ existuje sentence ψ_T taková, že

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \quad (2)$$

ψ_T říká “**nejsem dokazatelná v T** ”. Přesněji, ψ_T je ekvivalentní sentenci vyjadřující, že ψ_T není dokazatelná v T . (Ekvivalence platí v $\mathbb{N}$ i v T).

- Nejprve ukážeme, že ψ_T *není dokazatelná* v T . Kdyby $T \vdash \psi_T$, tj. ψ_T je lživá v $\mathbb{N}$, pak $\mathbb{N} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy z (2) plyne $T \vdash \neg\psi_T$, což ale není možné, neboť T je bezesporná.
- Zbývá dokázat, že ψ_T je pravdivá v $\mathbb{N}$. Kdyby ne, tj. $\mathbb{N} \models \neg\psi_T$, pak $\mathbb{N} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy $T \vdash \psi_T$, což jsme již dokázali, že neplatí. $\square$

Důsledky a zesílení 1. věty

Důsledek *Je-li navíc $\mathbb{N} \models T$, je teorie T nekompletní.*

Důkaz Kdyby byla T kompletní, pak $T \vdash \neg\psi_T$ a tedy $\mathbb{N} \models \neg\psi_T$, což je ve sporu s $\mathbb{N} \models \psi_T$. $\square$

Důsledek $\text{Th}(\mathbb{N})$ *není rekurzivně axiomatizovatelná.*

Důkaz $\text{Th}(\mathbb{N})$ je bezesporná extenze Robinsonovy aritmetiky a má model $\mathbb{N}$. Kdyby byla rekurzivně axiomatizovatelná, dle předchozího důsledku by byla nekompletní, ale $\text{Th}(\mathbb{N})$ je kompletní. $\square$

Gödelovu 1. větu o neúplnosti lze následovně zesílit.

Věta (Rosser) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje **nezávislá** sentence. Tedy T je nekompletní.*

Poznámka *Tedy předpoklad, že $\mathbb{N} \models T$, je v prvním důsledku nadbytečný.*

Gödelova 2. věta o neúplnosti

Označme Con_T sentenci $\neg(\exists y)Prf_T(\underline{0} = \underline{1}, y)$. Platí $\mathbb{N} \models Con_T \Leftrightarrow T \not\vdash \underline{0} = \underline{1}$. Tedy Con_T vyjadřuje, že “ T je bezesporná”.

Věta (Gödel) Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že Con_T není dokazatelná v T .

Důkaz (náznak) Nechť ψ_T je Gödelova sentence “nejsm dokazatelná v T ”.

- V první části důkazu 1. věty o neúplnosti jsme ukázali, že

“Je-li T bezesporná, pak ψ_T není dokazatelná v T .” (3)

Jinak vyjádřeno, platí $Con_T \rightarrow \psi_T$.

- Je-li T extenze Peanovy aritmetiky, důkaz tvrzení (3) lze formalizovat v rámci T . Tedy $T \vdash Con_T \rightarrow \psi_T$.
- Jelikož T je bezesporná dle předpokladu věty, podle (3) je $T \not\vdash \psi_T$.
- Z předchozích dvou bodů vyplývá, že $T \not\vdash Con_T$. $\square$

Poznámka Taková teorie T tedy neumí dokázat vlastní bezespornost.

Důsledky 2. věty

Důsledek Existuje model $\mathcal{A}$ Peanovy aritmetiky t.ž. $\mathcal{A} \models (\exists y) \text{Prf}_{PA}(\underline{0} = \underline{1}, y)$.

Poznámka $\mathcal{A}$ musí být nestandardní model PA , svědkem musí být nestandardní prvek (jiný než hodnoty numerálů).

Důsledek Existuje bezesporná rekurzivně axiomatizovaná extenze T Peanovy aritmetiky taková, že $T \vdash \neg \text{Con}_T$.

Důkaz Nechť $T = PA \cup \{\neg \text{Con}_{PA}\}$. Pak T je bezesporná, neboť $PA \not\vdash \text{Con}_{PA}$. Navíc $T \vdash \neg \text{Con}_{PA}$, tj. T dokazuje spornost $PA \subseteq T$, tedy i $T \vdash \neg \text{Con}_T$. $\square$

Poznámka $\mathbb{N}$ nemůže být modelem teorie T .

Důsledek Je-li teorie množin ZFC bezesporná, není Con_{ZFC} dokazatelná v ZFC.

Co bude u zkoušky?

Písemná část: 90 min, pro postup do ústní části aspoň 1/2 bodů.

Ústní část: cca 20 min, obvykle v pořadí odevzdávání písemné části.

Co nebude v písemné části.

- Hilbertovský kalkul (ani v ústní části).
- LD a SLD rezoluce, SLD stromy (ani v ústní části).
- Programy v Prologu (ani v ústní části).
- (Ne)rozhodnutelnost a neúplnost.

Co bude v ústní části?

(a) Definice, algoritmy či konstrukce, znění vět.

(b) Důkaz zadané věty či tvrzení.

Poznámka Část *(a)* bude včetně nerozhodnutelnosti a neúplnosti.

Na stránce z minulého roku jsou zadání písemek jako vzor.

Které důkazy se zkouší?

- Algoritmy pro 2-SAT a Horn-SAT (důkaz korektnosti).
- Tablo metoda ve VL: syst. tablo (dokončenost, kon. důkazu), korektnost, úplnost.
- Věta o kompaktnosti VL a její důsledky.
- Rezoluce ve VL: korektnost, úplnost. LI-rezoluce (úplnost pro Horn. formule).
- Sémantika PL: věta o konstantách, vlastnosti otevřených teorií, věta o dedukci.
- Tablo metoda v PL: syst. tablo (dokon., kon. důkazu), význam axiomů rovnosti.
- Tablo metoda v PL: korektnost, kanonický model (s rovnostmi), úplnost.
- Löwenheim-Skolemova věta. Věta o kompaktnosti PL a její důsledky.
- Extenze o definice, Skolemova věta, Herbrandova věta.
- Rezoluce v PL: korektnost, úplnost, lifting lemma, LI-rezoluce.
- Elementární ekvivalence, důsledky L.-S. věty. Izomorfismus a sémantika.
- Invariance definovatelných množin na automorfismy.
- ω -kategoričnost, podmínky pro konečnou a otevřenou axiomatizovatelnost.