Všechny prezentace z přednášek

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2025

Jak se učit?

Velmi doporučuji tento online minikurz o efektivním učení:

https://www.samford.edu/departments/academic-success-center/how-to-study

Investujte 35 minut nyní, ušetřete mnoho hodin později!

Cesta k jistému úspěchu u zkoušky

- Před přednáškou alespoň zběžně projděte skripta, snažte se pochopit motivaci a smysl definic a hlavních tvrzení.
- Po přednášce skripta podrobně přečtěte, nejasnosti ujasněte.
- Ujistěte se, že umíte pracovat i s formalizmem.
- Věnujte pozornost i cvičení, pomůže vám vše pochopit.
- Studujte průběžně, a průběžně testujte své znalosti.

První přednáška

Program

- úvod do logiky
- neformální představení výrokové a predikátové logiky („upoutávka")
- syntaxe výrokové logiky
- sémantika výrokové logiky (začátek)

Materiály

Zápisky z přednášky, Kapitola 1 a Sekce 2.1-2.2.4 z Kapitoly 2

Kapitola 1: Úvod do logiky

Co je logika?

Dvě definice:

1. soubor principů, které jsou základem uspořádání prvků nějakého systému (např. programu, zařízení, protokolu)
2. věda o uvažování prováděném podle striktních pravidel zachovávajících platnost

V informatice obojí: daný systém nejprve *formálně popíšeme*, a poté o něm *formálně uvažujeme* (automaticky!), tj. odvozujeme platné inference za použití nějakého dokazovacího systému

Filozofie → Matematika → Teoretická informatika →

Aplikovaná informatika

- logic programming
- discrete optimization (SAT solving, scheduling, planning)
- database theory
- verification (software, hardware, protocol)
- automated reasoning and proving
- knowledge-based representation
- artificial intelligence

1.1 Výroková logika

Příklad ze života: Hledání pokladu

Při hledání pokladu jsme narazili na rozcestí dvou chodeb. Víme, že na konci každé chodby je buď poklad, nebo drak, ale ne obojí.

Trpaslík nám řekl, že:

- *"Alespoň jedna z těch dvou chodeb vede k pokladu"*, a že
- *"První chodba vede k drakovi."*

Je známo, že trpaslíci buď vždy mluví pravdu, nebo vždy lžou. Kterou cestou se máme vydat?

Výroky neformálně

Výrok je tvrzení, kterému lze přiřadit pravdivostní hodnotu:

pravdivý (*True*, 1), nebo lživý (*False*, 0)

Prvovýroky (atomické výroky, výrokové proměnné) zkombinované pomocí logických spojek a závorek do složených výroků:

“(Trpaslík lže,) *právě když* (druhá chodba vede k drakovi.)”

- $\neg$ “neplatí X”, *negace*
- $\bigwedge$ “X a Y”, *konjunkce*
- $\bigvee$ “X nebo Y”, *disjunkce* (není exkluzivní)
- $\rightarrow$ “pokud X, potom Y”, *implikace* (čistě logická)
- $\leftrightarrow$ “X, právě když Y”, *ekvivalence*

Formalizace ve výrokové logice

Volba množiny prvovýroků: bity informace popisující daný systém

$p_1 =$ "*Poklad je v první chodbě.*"

$p_2 =$ "*Poklad je ve druhé chodbě.*"

(Co nejmenší, např. hodnota $t =$ "*Trpaslík mluví pravdu.*" je jednoznačně určená hodnotami $\mathbb{P} = \{p_1, p_2\}$.)

- *Poklad nebo drak, ale ne obojí*: zakódované do volby $\mathbb{P}$ (přítomnost draka je absence pokladu)
- "*První chodba vede k drakovi.*" $\Leftrightarrow$ $\neg p_1$
- "*Alespoň jedna z chodeb vede k pokladu.*" $\Leftrightarrow$ $p_1 \vee p_2$
- *Trpaslík buď mluví pravdu, nebo lže*:

$$\varphi = (\neg p_1 \wedge (p_1 \vee p_2)) \vee (\neg(\neg p_1) \wedge \neg(p_1 \vee p_2))$$

Teorie $T = \{\varphi\}$ v jazyce $\mathbb{P} = \{p_1, p_2\}$, φ je axiom T.

Modely a důsledky

Lze určit, kde je poklad? Je p_1 nebo p_2 důsledkem φ resp. T?

"Svět", ve kterém je např. v první chodbě poklad a ve druhé drak, popíšeme pomocí pravdivostního ohodnocení $p_1 = 1, p_2 = 0$, neboli modelu $v = (1, 0)$ jazyka $\mathbb{P}$. Celkem máme 4 "světy" a modely:

$$\mathrm{M}_{\mathbb{P}} = \{(0,0),(0,1),(1,0),(1,1)\}.$$

Je "svět" popsaný modelem $v = (1, 0)$ *konzistentní* s tím, co víme, tj. platí v modelu v výrok φ resp. teorie T? Vyhodnotíme podle stromové struktury φ:

$$v(p_1) = 1,\ v(p_2) = 0,\ v(\neg p_1) = 0,\ v(p_1 \vee p_2) = 1,\ \ldots,\ v(\varphi) = 0$$

Množina modelů výroku φ (resp. *modelů teorie* T):

$$\mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}(T) = \{(0,1)\}.$$

V každém modelu teorie T platí výrok p_2, neboli p_2 je důsledek T.

Dokazovací systémy

Ověřovat všechny modely je nepraktické, pro $|\mathbb{P}| = n$ máme 2^n modelů, a $\mathbb{P}$ může být i nekonečná.

Dokazovací systém

- důkaz výroku ψ z teorie T je formálně definovaný syntaktický objekt, snadno (mechanicky) ověřitelný
- lze hledat algoritmicky čistě na základě struktury ψ a axiomů T ("*syntaxe*"), nemusíme se zabývat modely ("*sémantikou*").

Klíčové vlastnosti:

- korektnost: pokud existuje důkaz ψ z T, potom ψ platí v T
- úplnost, pokud ψ platí v T, potom existuje důkaz ψ z T

Ukážeme si metodu analytického tabla a rezoluční metodu. Obě dokazují *sporem*: předpokládají platnost T a $\neg\psi$, hledají spor.

Metoda analytického tabla

- důkaz je strom olabelovaný předpoklady o platnosti výroků
- v kořeni: neplatí dokazovaný výrok ψ (důkaz sporem)
- připojíme platnost axiomů z T
- při konstrukci zjednodušujeme výroky ve vrcholech, invariant:

  Každý model teorie T, ve kterém neplatí ψ, se musí shodovat s některou z větví tabla.

  např.:

  True $(\varphi_1 \to \varphi_2)$ zredukujeme rozvětvením na False φ_1 a True φ_2,
  False $(\varphi_1 \to \varphi_2)$ zredukujeme připojením True φ_1 a False φ_2.

- sporná větev = předpokládá True i False stejného výroku
- důkaz = všechny větve sporné (tj. nemůže existovat model T, ve kterém neplatí ψ)

Příklad tablo důkazu

- False p_2
  - True $(\neg p_1 \wedge (p_1 \vee p_2)) \vee (\neg(\neg p_1) \wedge \neg(p_1 \vee p_2))$
    - True $\neg p_1 \wedge (p_1 \vee p_2)$
      - True $\neg p_1$
        - True $p_1 \vee p_2$
          - False p_1
            - True p_1
              - fail
            - True p_2
              - fail
    - True $\neg(\neg p_1) \wedge \neg(p_1 \vee p_2)$
      - True $\neg(\neg p_1)$
        - True $\neg(p_1 \vee p_2)$
          - False $(\neg p_1)$
            - True p_1
              - False $p_1 \vee p_2$
                - False p_1
                  - False p_2
                    - fail

Konjunktivní normální forma (CNF)

literál p, $\neg p$ klauzule disjunkce literálů CNF konjunkce klauzulí

každý výrok má ekvivalentní CNF ($\psi \sim \psi'$, stejné modely)

např. pro výrok $(\neg p_1 \wedge (p_1 \vee p_2)) \vee (\neg(\neg p_1) \wedge \neg(p_1 \vee p_2))$

nahradíme $\neg(\neg p_1) \sim p_1$ a $\neg(p_1 \vee p_2) \sim (\neg p_1 \wedge \neg p_2)$ (*De Morgan*)

$$(\neg p_1 \wedge (p_1 \vee p_2)) \vee (p_1 \wedge \neg p_1 \wedge \neg p_2)$$

a dále opakovaně použijeme distributivitu $\vee$ vůči $\wedge$:

$$(\neg p_1 \vee p_1) \wedge (\neg p_1 \vee \neg p_1) \wedge (\neg p_1 \vee \neg p_2) \wedge (p_1 \vee p_2 \vee p_1) \wedge$$
$$(p_1 \vee p_2 \vee \neg p_1) \wedge (p_1 \vee p_2 \vee \neg p_2)$$

už je CNF, ještě zjednodušíme: odstraníme duplicitní literály, a klauzule obsahující p_i a zároveň $\neg p_i$ (to jsou tautologie)

$$\neg p_1 \wedge (\neg p_1 \vee \neg p_2) \wedge (p_1 \vee p_2)$$

Rezoluční důkaz

Dk sporem, převeď negaci dokazovaného do CNF a přidej k T

p_2 platí v T, právě když je následující CNF výrok nesplnitelný:

$$\neg p_1 \wedge (\neg p_1 \vee \neg p_2) \wedge (p_1 \vee p_2) \wedge \neg p_2$$

množinový zápis: $S = \{\{\neg p_1\}, \{\neg p_1, \neg p_2\}, \{p_1, p_2\}, \{\neg p_2\}\}$

rezoluční pravidlo: je-li $p \in C_1$ a $\neg p \in C_2$, potom *rezolventa*

$$C = (C_1 \setminus \{p\}) \cup (C_2 \setminus \{\neg p\})$$

platí v každém modelu, ve kterém platí C_1 i C_2

rezoluční zamítnutí S: posloupnost klauzulí, kde každá je buď z S nebo rezolventa předchozích, poslední je prázdná klauzule $\square$

myšlenka: protože $\square$ nemá žádný model, je i S nesplnitelná

Příklad rezolučního důkazu

rezoluční zamítnutí (3. klauzule je rezolventou 1.&2., 5. je z 3.&4.)

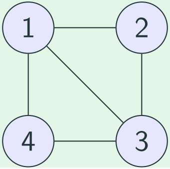
$$\{\neg p_1\}, \{p_1, p_2\}, \{p_2\}, \{\neg p_2\}, \square$$

rezoluční strom (listy klauzule z S, vnitřní vrcholy rezolventy synů)

$$\begin{array}{ccccc}
\{\neg p_1\} & & \{p_1, p_2\} & & \\
& \diagdown \quad \diagup & & & \\
& \{p_2\} & & \{\neg p_2\} & \\
& & \diagdown \quad \diagup & & \\
& & \square & &
\end{array}$$

Příklad: Barvení grafů

Najděte vrcholové obarvení následujícího grafu třemi barvami.



graf: množina vrcholů a množina (libovolně) orientovaných hran

$$\mathcal{G} = \langle V; E \rangle = \langle \{1, 2, 3, 4\}; \{(1, 2), (1, 3), (1, 4), (2, 3), (3, 4)\} \rangle$$

jak formalizovat? pro $v \in V$ a $c \in C = \{R, G, B\}$:

$$p_v^c = \text{“}\textit{vrchol } v \textit{ má barvu } c\text{”}$$

$\mathbb{P} = \{p_v^c \mid c \in C, v \in V\} = \{p_1^R, p_1^G, p_1^B, p_2^R, p_2^G, p_2^B, p_3^R, p_3^G, p_3^B, p_4^R, p_4^G, p_4^B\}$

máme celkem $|\,\mathrm{M}_{\mathbb{P}}\,| = 2^{12} = 4096$ modelů jazyka (12-dim. vektorů)

Formalizace hranového obarvení

- každý vrchol má nejvýše jednu barvu: $4^4 = 2^8 = 256$ modelů

$$T_1 = \{(\neg p_v^R \vee \neg p_v^G) \wedge (\neg p_v^R \vee \neg p_v^B) \wedge (\neg p_v^G \vee \neg p_v^B) \mid v \in V\}$$

- a každý vrchol má alespoň jednu barvu: $3^4 = 81$ modelů

$$T_2 = T_1 \cup \{p_v^R \vee p_v^G \vee p_v^B \mid v \in V\} = T_1 \cup \{\bigvee_{c \in C} p_v^c \mid v \in V\}$$

T_2 je extenze teorie T_1 neboť každý důsledek T_1 platí i v T_2, zde dokonce $\mathrm{M}_{\mathbb{P}}(T_2) \subseteq \mathrm{M}_{\mathbb{P}}(T_1)$

- nakonec přidáme hranovou podmínku:

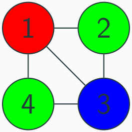
$$T_3 = T_2 \cup \{\bigwedge_{c \in C} (\neg p_u^c \vee \neg p_v^c) \mid (u, v) \in E\}$$

Výsledná teorie T_3 je splnitelná (má model), právě když je graf $\mathcal{G}$ 3-obarvitelný.

Co s ní?

Všechna obarvení?

T_3 má 6 modelů: $v = (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$ a další získané permutací barev



Obarvení, ve kterých je vrchol 1 modrý a vrchol 2 zelený?

Odpovídají modelům teorie $T_3 \cup \{p_1^B, p_2^G\}$

Důkaz, že vrcholy 2 a 4 musí mít stejnou barvu?

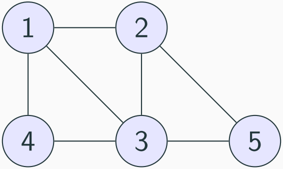
Tablo s kořenem False $(p_2^R \wedge p_4^R) \vee (p_2^G \wedge p_4^G) \vee (p_2^B \wedge p_4^B)$

Nebo rezolucí: přidáme negaci $(p_2^R \wedge p_4^R) \vee (p_2^G \wedge p_4^G) \vee (p_2^B \wedge p_4^B)$, vše převedeme do CNF a zamítneme

1.2 Predikátová logika

Nevýhody formalizace ve výrokové logice

Teorie T_3 je poměrně velká, a 'natvrdo' kóduje graf $\mathcal{G}$.



Obohatit jazyk $\mathbb{P}' = \mathbb{P} \cup \{p_5^R, p_5^G, p_5^B\}$ a vytvořit ještě větší teorii T_3' přidáním axiomů o vrcholu 5 a hranách $(2,5),(3,5)$?

A co vlastnosti obecně platné o všech nebo mnoha grafech?

V predikátové logice můžeme mluvit o vrcholech grafu pomocí proměnných a přirozeně vyjádřit vlastnosti jako:

- *"z vrcholu u vede hrana do vrcholu v"*
- *"vrchol u je zelený"*

Predikátová logika: struktury a jazyk

Modely už nejsou 0–1 vektory, ale struktury, např. naše (orientované) grafy:

$\mathcal{G} = \langle V^{\mathcal{G}}; E^{\mathcal{G}} \rangle = \langle \{1,2,3,4\}; \{(1,2),(1,3),(1,4),(2,3),(3,4)\} \rangle$

$\mathcal{G}' = \langle V^{\mathcal{G}'}; E^{\mathcal{G}'} \rangle = \langle \{1,2,3,4,5\}; \{(1,2),(1,3),(1,4),(2,3),(3,4),(2,5),(3,5)\} \rangle$

- množina vrcholů, a binární relace na této množině
- jazyk specifikuje kolik relací jakých arit má struktura mít, a symboly pro ně
- např. jazyk grafů $\mathcal{L} = \langle E \rangle$ (kde E je binární relační symbol)
- $\mathcal{G}$ a $\mathcal{G}'$ jsou struktury v jazyce $\mathcal{L}$ ($\mathcal{L}$-struktury)
- můžeme mít také funkce a konstanty, a symbol $=$ pro rovnost

Predikátová logika: syntaxe a sémantika

Syntaxe: místo prvovýroků atomické formule, např. $E(x, y)$, kde x, y jsou proměnné reprezentující vrcholy; stejné logické spojky, ale navíc kvantifikátory:

$(\forall x)$ *"pro všechny vrcholy x"*

$(\exists y)$ *"existuje vrchol y"*

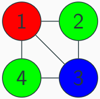
(hrají roli "konjunkce" a "disjunkce" přes všechny prvky)

- "V grafu nejsou smyčky": $(\forall x)(\neg E(x, x))$
- "Existuje vrchol výstupního stupně 1": $(\exists x)(\exists y)(E(x, y) \wedge (\forall z)(E(x, z) \rightarrow y = z))$

Sémantika: V daném grafu $\mathcal{G}$ a při dosazení vrcholu u za proměnnou x a vrcholu v za proměnnou y vyhodnotíme $E(x, y)$ jako True, právě když $(u, v) \in E^{\mathcal{G}}$.

Barvení grafů v predikátové logice

Jazyk $\mathcal{L}' = \langle E, R, G, B \rangle$, kde E je binární a R, G, B jsou unární relační symboly ($R(x)$ znamená *"vrchol x je červený"*)



$\mathcal{L}'$-struktura: graf s trojicí množin vrcholů

$$\begin{aligned}\mathcal{G}_C &= \langle V^{\mathcal{G}_C}; E^{\mathcal{G}_C}, R^{\mathcal{G}_C}, G^{\mathcal{G}_C}, B^{\mathcal{G}_C} \rangle \\ &= \langle \{1,2,3,4\}; \{(1,2),(1,3),(1,4),(2,3),(3,4)\}, \{1\}, \{2,4\}, \{3\} \rangle\end{aligned}$$

$\mathcal{G}_C$ je expanze $\mathcal{L}$-struktury $\mathcal{G}$ do jazyka $\mathcal{L}'$

Nejvýše jedna barva, alespoň jedna barva, hranová podmínka:

- $(\forall x)((\neg R(x) \vee \neg G(x)) \wedge (\neg R(x) \vee \neg B(x)) \wedge (\neg G(x) \vee \neg B(x)))$
- $(\forall x)(R(x) \vee G(x) \vee B(x))$
- $(\forall x)(\forall y)(E(x,y) \rightarrow ((\neg R(x) \vee \neg R(y)) \wedge (\neg G(x) \vee \neg G(y)) \wedge (\neg B(x) \vee \neg B(y))))$

1.3 Další druhy logických systémů

Predikátové logiky vyšších řádů

- Predikátová logika, kde proměnné reprezentují jednotlivé vrcholy, je logika prvního řádu (first-order, FO)
- Logika druhého řádu (second-order, SO): proměnné i pro množiny vrcholů a n-tic vrcholů (tj. relace, funkce)

$$(\exists S)(\forall x)(\forall y)(E(x,y) \rightarrow (S(x) \leftrightarrow \neg S(y)))$$

"Graf je bipartitní."

- A v logice *třetího řádu* máme i množiny množin (např. v topologii).

Logiky zobecňující pojem pravdy

Kromě toho lze zobecnit pojem platnosti (pravdy):

- temporální logiky (platnost ‘vždy’, ‘někdy v budoucnosti’, ‘dokud’ apod.) – např. v paralelním programování
- modální logiky (‘je možné’, ‘je nutné’) – v umělé inteligenci, uvažování autonomních agentů o svém okolí
- fuzzy logiky (‘je 0.35 pravdivé’) – v automatických pračkách
- intuicionistická logika (povoluje jen konstruktivní důkazy, nemá *zákon vyloučeného třetího*)

1.4 O přednášce

Obsah předmětu

I. Výroková logika
   - Syntaxe a sémantika
   - Problém SAT
   - Tablo metoda
   - Rezoluční metoda
II. Predikátová logika
   - Syntaxe a sémantika
   - Tablo metoda v predikátové logice
   - Rezoluční metoda v predikátové logice
   - Aplikace: databáze, Prolog
III. Pokročilé partie
   - Teorie modelů
   - Nerozhodnutelnost a neúplnost

ČÁST I – VÝROKOVÁ LOGIKA

Kapitola 2: Syntaxe a sémantika výrokové logiky

Syntaxe a sémantika

syntaxe dává pravidla pro tvoření korektních formálních výrazů sestávajících ze symbolů, a pro operace s nimi (*výrok*, *důkaz*, …)

sémantika popisuje význam syntaktických objektů "v reálném světě" (*model*, …)

Klíčem k logice je vztah mezi syntaxí a sémantikou:

- sémantické objekty studujeme pomocí syntaxe ('jaké výroky platí v modelu?')
- syntaktické pomocí sémantiky, např. ekvivalence výroků: $\psi \sim \psi'$ právě když $\mathrm{M}_{\mathbb{P}}(\psi) = \mathrm{M}_{\mathbb{P}}(\psi')$

2.1 Syntaxe výrokové logiky

Jazyk

- určený množinou prvovýroků (výrokových proměnných, atomických výroků) – neprázdná, konečná nebo i *nekonečná*

$$\mathbb{P}_1 = \{p, q, r\}$$
$$\mathbb{P}_2 = \{p_0, p_1, p_2, p_3, \ldots\} = \{p_i \mid i \in \mathbb{N}\}$$

  (obvykle *spočetná*, *uspořádaná*)

- dále do jazyka patří logické symboly:
  - logické spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
  - závorky $($, $)$

Výrok

Výrok (výroková formule) v jazyce $\mathbb{P}$ je prvek množiny $\mathrm{VF}_{\mathbb{P}}$ definované *induktivně*: $\mathrm{VF}_{\mathbb{P}}$ je nejmenší množina splňující

- pro každý prvovýrok $p \in \mathbb{P}$ platí $p \in \mathrm{VF}_{\mathbb{P}}$,
- pro každý výrok $\varphi \in \mathrm{VF}_{\mathbb{P}}$ je $(\neg\varphi)$ také prvek $\mathrm{VF}_{\mathbb{P}}$
- pro každé $\varphi, \psi \in \mathrm{VF}_{\mathbb{P}}$ jsou $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, a $(\varphi \leftrightarrow \psi)$ také prvky $\mathrm{VF}_{\mathbb{P}}$.

Výroky jsou nutně *konečné* řetězce!

$\mathrm{Var}(\varphi)$: množina všech prvovýroků ve φ (vždy konečná)

podvýrok: podřetězec, který je sám výrok

$\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$, $\mathrm{Var}(\varphi) = \{p, q, r\}$
podvýroky: $p, q, (\neg q), (p \vee (\neg q)), r, (p \wedge q), (r \rightarrow (p \wedge q)), \varphi$

pravda: $\top = (p \vee (\neg p))$, spor: $\bot = (p \wedge (\neg p))$ ($p \in \mathbb{P}$ je pevně daný)

Konvence zápisu

při *zápisu* výroků můžeme vynechat některé závorky:

$\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$ lze zapsat jako $p \vee \neg q \leftrightarrow (r \rightarrow p \wedge q)$

- priorita operátorů: $\neg$ nejvyšší, dále $\wedge$ a $\vee$, nakonec $\rightarrow$ a $\leftrightarrow$
- asociativita $\wedge$ a $\vee$: nápis $p \wedge q \wedge r$ znamená výrok $(p \wedge (q \wedge r))$
- vnější závorky nemusíme psát

Poznámka: v definici jsme mohli místo *infixového* zápisu zvolit *prefixový* ("polskou notaci"): *"každý prvovýrok je výrok, jsou-li φ, ψ výroky, jsou výroky také $\neg\varphi$, $\wedge\varphi\psi$, $\vee\varphi\psi$, $\rightarrow\varphi\psi$, a $\leftrightarrow\varphi\psi$"*
nebo i *postfixový*

$\varphi = \leftrightarrow\vee p\neg q\rightarrow r\wedge pq$

$\varphi = pq\neg\vee rpq\wedge\rightarrow\leftrightarrow$

Důležitá je jen stromová struktura výroků!

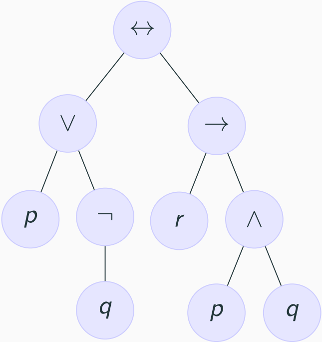
Strom výroku

Tree(φ) je zakořeněný uspořádaný strom, definovaný induktivně:

- $\varphi = p \in \mathbb{P}$: jediný vrchol, s labelem p
- $\varphi = (\neg\varphi')$: kořen s labelem $\neg$, jediný syn je kořen Tree(φ').
- $\varphi = (\varphi' \,\square\, \varphi'')$ pro $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$: kořen s labelem $\square$ a dvěma syny: levý syn je kořen Tree(φ'), pravý Tree(φ'').

$\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$
rekonstrukce φ průchodem stromu,
podvýroky odpovídají podstromům

Tree(φ) je jednoznačně určený!



Teorie

Teorie v jazyce $\mathbb{P}$ je libovolná množina výroků $T \subseteq \mathrm{VF}_{\mathbb{P}}$. Výrokům $\varphi \in T$ říkáme také axiomy.

$T = \emptyset$ a $T = \mathrm{VF}_{\mathbb{P}}$ nad libovolným jazykem,
$T = \{p \wedge q, q \to (p \vee r)\}$ v jazyce $\mathbb{P} = \{p, q, r\}$
$T = \{p_0\} \cup \{p_i \to p_{i+1} \mid i \in \mathbb{N}\}$ nad *nekonečným* $\mathbb{P} = \{p_i \mid i \in \mathbb{N}\}$

Poznámka: *Konečnou* teorii by bylo možné (byť ne praktické!) nahradit jediným výrokem: konjunkcí všech axiomů.

Připouštíme ale i *nekonečné teorie*; hodí se např. pro popis systému v (diskrétním) čase $t = 0, 1, 2, \ldots$.

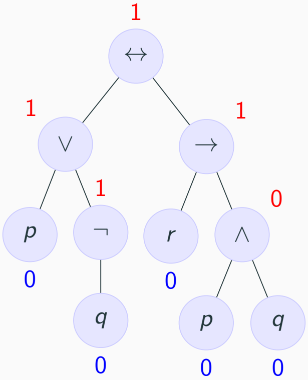
2.2 Sémantika výrokové logiky

Pravdivostní hodnota: příklad

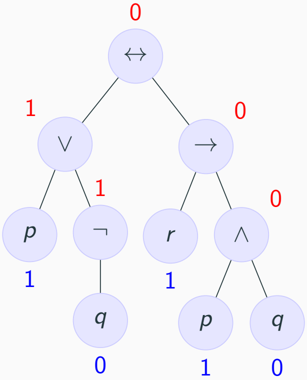
pravdivostní ohodnocení výrokových proměnných jednoznačně určuje pravdivostní hodnotu výroku (vyhodnoť od listů ke kořeni)

$$\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$$

(a) φ platí při ohodnocení $p = 0,\ q = 0,\ r = 0$



(b) φ neplatí při ohodnocení $p = 1,\ q = 0,\ r = 1$



Sémantika logických spojek

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

$$\begin{array}{cc} 0 & 1 \\ \hline 1 & 0 \end{array} \qquad f_{\neg}(x) = 1 - x$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad f_{\wedge}(x, y) = \min(x, y)$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad f_{\vee}(x, y) = \max(x, y)$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \qquad f_{\rightarrow}(x, y)$$

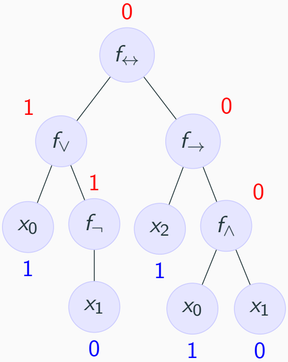
$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array} \qquad f_{\leftrightarrow}(x, y)$$

Výroky a booleovské funkce

sémantika logických spojek je daná booleovskými funkcemi, každý výrok určuje *složenou* booleovskou funkci, tzv. pravdivostní funkci

např. $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$ v jazyce $\mathbb{P}' = \{p, q, r, s\}$

$$f_{\varphi,\mathbb{P}'}(x_0, x_1, x_2, x_3) = f_{\leftrightarrow}(f_{\vee}(x_0, f_{\neg}(x_1)), f_{\rightarrow}(x_2, f_{\wedge}(x_0, x_1)))$$



pravdivostní hodnota φ při ohodnocení $p = 1,\ q = 0,\ r = 1,\ s = 1$:

$$\begin{aligned} f_{\varphi,\mathbb{P}'}(1,0,1,1) &= f_{\leftrightarrow}(f_{\vee}(1, f_{\neg}(0)), f_{\rightarrow}(1, f_{\wedge}(1,0))) \\ &= f_{\leftrightarrow}(f_{\vee}(1,1), f_{\rightarrow}(1,0)) \\ &= f_{\leftrightarrow}(1,0) \\ &= 0 \end{aligned}$$

Pravdivostní funkce formálně

Pravdivostní funkce výroku φ v *konečném* jazyce $\mathbb{P}$ je funkce $f_{\varphi,\mathbb{P}}\colon \{0,1\}^{|\mathbb{P}|} \to \{0,1\}$ definovaná induktivně:

- je-li φ *i*-tý prvovýrok z $\mathbb{P}$: $f_{\varphi,\mathbb{P}}(x_0, \ldots, x_{n-1}) = x_i$
- je-li $\varphi = (\neg\varphi')$: $f_{\varphi,\mathbb{P}}(x_0, \ldots, x_{n-1}) = f_\neg(f_{\varphi',\mathbb{P}}(x_0, \ldots, x_{n-1}))$
- je-li $\varphi = (\varphi' \mathbin{\square} \varphi'')$ kde $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$:
  $f_{\varphi,\mathbb{P}}(x_0, \ldots, x_{n-1}) =$
  $f_\square(f_{\varphi',\mathbb{P}}(x_0, \ldots, x_{n-1}), f_{\varphi'',\mathbb{P}}(x_0, \ldots, x_{n-1}))$

Poznámka: Pravdivostní funkce $f_{\varphi,\mathbb{P}}$ závisí pouze na proměnných odpovídajících prvovýrokům z $\mathrm{Var}(\varphi) \subseteq \mathbb{P}$.

Je-li výrok v *nekonečném* jazyce $\mathbb{P}$, můžeme se omezit na jazyk $\mathrm{Var}(\varphi)$ (který je konečný) a uvažovat pravdivostní funkci nad ním.

Modely

Pravdivostní ohodnocení reprezentuje ‘reálný svět’ (systém) v námi zvoleném ‘formálním světě’, proto mu také říkáme model

Model jazyka $\mathbb{P}$: libovolné pravdivostní ohodnocení $v\colon \mathbb{P} \to \{0,1\}$
Množina všech modelů: $\mathrm{M}_{\mathbb{P}} = \{v \mid v\colon \mathbb{P} \to \{0,1\}\} = \{0,1\}^{\mathbb{P}}$

$\mathbb{P} = \{p, q, r\}$, ohodnocení p je pravda, q nepravda, a r pravda:
formálně $v = \{(p,1),(q,0),(r,1)\}$ ale píšeme[1] jen $v = (1,0,1)$

$$\begin{aligned}\mathrm{M}_{\mathbb{P}} = \{&(0,0,0),(0,0,1),(0,1,0),(0,1,1),\\ &(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}\end{aligned}$$

[1] Formálně ztotožňujeme $\{0,1\}^{\mathbb{P}}$ s $\{0,1\}^{|\mathbb{P}|}$, množina $\mathbb{P}$ je uspořádaná.

Platnost

výrok platí v modelu, pokud je jeho pravdivostní hodnota rovna 1

Výrok φ v jazyce $\mathbb{P}$, model $v \in \mathrm{M}_{\mathbb{P}}$. Pokud $f_{\varphi,\mathbb{P}}(v) = 1$, potom říkáme, že φ platí v modelu v, v je modelem φ, a píšeme $v \models \varphi$.

Množina všech modelů resp. *nemodelů* φ:

$$\mathrm{M}_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[1]$$

$$\overline{\mathrm{M}_{\mathbb{P}}(\varphi)} = M_{\mathbb{P}} \setminus M_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \not\models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[0]$$

Je-li jazyk zřejmý z kontextu, můžeme vynechat, ale jinak ne!

$$\mathrm{M}_{\{p,q\}}(p \to q) = \{(0,0),(0,1),(1,1)\}$$

$$\mathrm{M}_{\{p,q,r\}}(p \to q) = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,1,0),(1,1,1)\}$$

Platnost teorie, model teorie

Teorie T platí v modelu v, pokud každý axiom $\varphi \in T$ platí ve v.
Podobně jako pro výrok: v je modelem T, $v \models T$, $v \in \mathrm{M}_{\mathbb{P}}(T)$.

Někdy píšeme $\mathrm{M}_{\mathbb{P}}(T, \varphi)$ místo $\mathrm{M}_{\mathbb{P}}(T \cup \{\varphi\})$, $\mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2, \dots, \varphi_n)$ místo $\mathrm{M}_{\mathbb{P}}(\{\varphi_1, \varphi_2, \dots, \varphi_n\})$.

- $\mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T) \cap \mathrm{M}_{\mathbb{P}}(\varphi)$
- $\mathrm{M}_{\mathbb{P}}(T) = \bigcap_{\varphi \in T} \mathrm{M}_{\mathbb{P}}(\varphi)$
- $\mathrm{M}_{\mathbb{P}}(\varphi_1) \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2) \supseteq \cdots \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2, \dots, \varphi_n)$

Najděme modely $T = \{p \vee q \vee r, q \to r, \neg r\}$ (v jazyce $\mathbb{P} = \{p, q, r\}$):

$$\mathrm{M}_{\mathbb{P}}(\neg r) = \{(0,0,0), (0,1,0), (1,0,0), (1,1,0)\}$$

$$\mathrm{M}_{\mathbb{P}}(\neg r, q \to r) = \{(0,0,0), (1,0,0)\}$$

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

Druhá přednáška

Program

- sémantika výrokové logiky (pokračování)
- normální formy
- vlastnosti a důsledky teorií
- extenze teorií
- algebra výroků

Materiály

Zápisky z přednášky, Sekce 2.2.5-2.5 z Kapitoly 2

Další sémantické pojmy

- výrok φ (nad $\mathbb{P}$) je pravdivý, tautologie, platí (v logice), $\models \varphi$, pokud platí v každém modelu, $\mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}$
- lživý, sporný, pokud nemá žádný model, $\mathrm{M}_{\mathbb{P}}(\varphi) = \emptyset$
  (Být lživý není totéž, co nebýt pravdivý!)
- nezávislý, pokud platí v nějakém modelu a neplatí v nějakém jiném modelu, tj. není pravdivý ani lživý, $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(\varphi) \subsetneq \mathrm{M}_{\mathbb{P}}$
- splnitelný, pokud má nějaký model, tj. není lživý, $\mathrm{M}_{\mathbb{P}}(\varphi) \neq \emptyset$

výroky φ, ψ (ve stejném jazyce) jsou (logicky) ekvivalentní, $\varphi \sim \psi$, pokud mají stejné modely, tj. $\varphi \sim \psi \;\Leftrightarrow\; \mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}(\psi)$

- pravdivé: $\top$, $p \vee q \leftrightarrow q \vee p$
- lživé: $\bot$, $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$
- nezávislé, splnitelné: p, $p \wedge q$
- ekvivalentní: $p \to q \sim \neg p \vee q$, $\neg p \to (p \to q) \sim \top$

Sémantické pojmy vzhledem k teorii

relativně k dané teorii T (omezíme se na její modely):

- pravdivý/platí v T, důsledek T, $T \models \varphi$ je-li $\mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)$
- lživý/sporný v T pokud $\mathrm{M}_{\mathbb{P}}(\varphi) \cap \mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T, \varphi) = \emptyset$.
- nezávislý v T pokud $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(T, \varphi) \subsetneq \mathrm{M}_{\mathbb{P}}(T)$,
- splnitelný v T, konzistentní s T pokud $\mathrm{M}_{\mathbb{P}}(T, \varphi) \neq \emptyset$
- φ a ψ jsou ekvivalentní v T, T-ekvivalentní, $\varphi \sim_T \psi$ platí-li v týchž modelech T, tj. $\varphi \sim_T \psi \;\Leftrightarrow\; \mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T, \psi)$

např. $T = \{p \vee q, \neg r\}$:

- $\neg p \vee \neg q \vee \neg r$ je v T pravdivý
- $(\neg p \wedge \neg q) \vee r$ je v T lživý
- $p \leftrightarrow q, p \wedge q$ jsou v T nezávislé, splnitelné
- platí $p \sim_T p \vee r$ (ale $p \not\sim p \vee r$)

Univerzálnost logických spojek

množina logických spojek je univerzální, pokud:

- každá booleovská funkce je pravdivostní funkcí nějakého výroku vybudovaného z těchto spojek
- ekvivalentně: každá množina modelů nad konečným jazykem je množinou modelů nějakého výroku

Tvrzení: $\{\neg, \wedge, \vee\}$ a $\{\neg, \rightarrow\}$ jsou univerzální.

[Důkaz na příštím slidu.]

Další zajímavé logické spojky:

- Shefferova spojka (NAND, $\uparrow$) $\quad p \uparrow q \sim \neg(p \wedge q)$,
- Pierceova spojka (NOR, $\downarrow$) $\quad p \downarrow q \sim \neg(p \vee q)$,
- Exclusive-OR (XOR, $\oplus$) $\quad p \oplus q \sim (p \vee q) \wedge \neg(p \wedge q)$

např. $\{\uparrow\}$ je univerzální, $\{\wedge, \vee\}$ není

Důkaz, že $\{\neg, \wedge, \vee\}$ a $\{\neg, \rightarrow\}$ jsou univerzální

Mějme $f\colon \{0,1\}^n \to \{0,1\}$, resp. $M = f^{-1}[1] \subseteq \{0,1\}^n$

Pro jediný model: $\varphi_v =$ 'musím být model v'

- příklad: $v = (1,0,1,0) \rightsquigarrow \varphi_v = p_1 \wedge \neg p_2 \wedge p_3 \wedge \neg p_4$
- obecně: $v = (v_1, \ldots, v_n)$, použijeme značení $p^1 = p$, $p^0 = \neg p$

$$\varphi_v = p_1^{v_1} \wedge p_2^{v_2} \wedge \cdots \wedge p_n^{v_n} = \bigwedge_{i=1}^{n} p_i^{v(p_i)} = \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

Pro více modelů: 'musím být alespoň jeden z modelů z M'

$$\varphi_M = \bigvee_{v \in M} \varphi_v = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

Zřejmě $\mathrm{M}(\varphi_M) = M$ neboli $f_{\varphi_M,\mathbb{P}} = f$, a φ_M používá jen $\{\neg, \wedge, \vee\}$. Protože $p \wedge q \sim \neg(p \to \neg q)$ a $p \vee q \sim \neg p \to q$, mohli bychom φ_M ekvivalentně vyjádřit i pomocí $\{\neg, \rightarrow\}$. $\square$

2.3 Normální formy

CNF a DNF

- literál je prvovýrok nebo jeho negace, $\overline{\ell}$ je opačný literál k ℓ (pro *pozitivní* $\ell = p$ je $\overline{\ell} = \neg p$, pro *negativní* $\ell = \neg p$ je $\overline{\ell} = p$)
- klauzule je disjunkce literálů $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_n$ (*jednotková klauzule* je samotný literál, *prázdná klauzule* je $\bot$)
- výrok je v konjunktivní normální formě (CNF) je-li konjunkcí klauzulí (prázdný CNF výrok je $\top$)
- elementární konjunkce je konjunkce literálů $E = \ell_1 \wedge \cdots \wedge \ell_n$ (*jednotková* el. konjunkce je samotný literál, *prázdná* je $\top$)
- výrok je v disjunktivní normální formě (DNF) je-li disjunkcí elementárních konjunkcí (prázdný DNF výrok je $\bot$)

- $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$ je v CNF
- $\neg p \vee (p \wedge q)$ je v DNF
- φ_v je v CNF i DNF, φ_M je v DNF

O dualitě

zaměníme-li $0 \leftrightsquigarrow 1$, negace zůstává stejná, z $\wedge$ se stává $\vee$ a naopak

- φ nad $\{\neg, \wedge, \vee\}$, zaměníme-li $\wedge, \vee$ a znegujeme-li prvovýroky: duální $\psi \sim \neg\varphi$, modely φ jsou nemodely ψ, $f_\psi(\neg x) = \neg f_\varphi(x)$
- CNF a DNF jsou duální pojmy
- pravdivost je duální k nesplnitelnosti

Pozorování: Výrok v CNF je pravdivý, právě když každá klauzule má dvojici opačných literálů.

Duálně: Výrok v DNF je nesplnitelný, právě když každá elementární konjunkce má dvojici opačných literálů.

Převod do normální formy: sémanticky (příklad)

mějme výrok $\varphi = p \leftrightarrow (q \vee \neg r)$

jeho modely jsou $M = \{(0,0,1),(1,0,0),(1,1,0),(1,1,1)\}$

najdeme DNF a CNF výroky se stejnými modely, tj. ekvivalentní φ

konstrukce DNF: každý model popsaný jednou elem. konjunkcí

$\varphi_{\mathrm{DNF}} = (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$

konstrukce CNF: potřebujeme nemodely

$$\overline{M} = \{(0,0,0),(0,1,0),(0,1,1),(1,0,1)\}$$

každá klauzule zakáže jeden nemodel:

$\varphi_{\mathrm{CNF}} = (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r)$

Převod do normální formy: sémanticky

Tvrzení: Buď $\mathbb{P}$ konečný, $M \subseteq \mathrm{M}_{\mathbb{P}}$ libovolná. Potom existují DNF a CNF výroky $\varphi_{\mathrm{DNF}}, \varphi_{\mathrm{CNF}}$, že $M = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{DNF}}) = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{CNF}})$.

$$\varphi_{\mathrm{DNF}} = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

$$\varphi_{\mathrm{CNF}} = \bigwedge_{v \in \overline{M}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}} = \bigwedge_{v \notin M} \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$$

Důkaz: $\varphi_{\mathrm{DNF}} = \varphi_M$ říká 'jsem jeden z modelů z M'

φ_{CNF} říká 'nejsem žádný z nemodelů z M', je duální k $\varphi'_{\mathrm{DNF}} = \varphi_{\overline{M}}$ pro doplněk M, nebo přímo: modely klauzule $C_v = \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$ jsou $\mathrm{M}_C = \mathrm{M}_{\mathbb{P}} \setminus \{v\}$, tedy každá klauzule zakáže jeden nemodel $\square$

Důsledek: Každý výrok (v libovolném, i nekonečném jazyce $\mathbb{P}$) je ekvivalentní nějakému výroku v CNF a nějakému výroku v DNF.

Důkaz: použijeme konečný jazyk $\mathbb{P}' = \mathrm{Var}(\varphi)$, $M = \mathrm{M}_{\mathbb{P}'}(\varphi)$ $\square$

Převod do normální formy: syntakticky

Hledat všechny modely je neefektivní, lze i syntakticky pomocí ekvivalentních úprav.

Pozorování: Nahradíme-li podvýrok ψ výroku φ ekvivalentním ψ', výsledný výrok φ' je také ekvivalentní φ.

Postup úprav:

1. přepiš ekvivalenci a implikaci pomocí $\neg, \wedge, \vee$
2. přesuň negace dolů (k listům) ve stromu výroku pomocí de Morganových pravidel, odstraň dvojité negace
3. přesuň dolů disjunkce (pro CNF) resp. konjunkce (pro DNF) pomocí distributivity $\wedge$ a $\vee$
4. případně zjednoduš (odstranění duplicit, tautologií apod.)

Důkaz, že funguje: indukcí dle struktury výroku

Převod do normální formy: syntakticky (příklad)

$$\varphi = p \leftrightarrow (q \vee \neg r)$$

- přepsat ekvivalence a implikace

$$\begin{aligned} p \leftrightarrow (q \vee \neg r) &\sim (p \rightarrow (q \vee \neg r)) \wedge ((q \vee \neg r) \rightarrow p) \\ &\sim (\neg p \vee q \vee \neg r) \wedge (\neg(q \vee \neg r) \vee p) \end{aligned}$$

- negace dolů

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

- do CNF (+ seřadíme prvovýroky v klauzulích)

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

- do DNF (+ zjednodušení)

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

Ekvivalentní úpravy

- Implikace a ekvivalence:

$$\varphi \to \psi \sim \neg\varphi \vee \psi$$
$$\varphi \leftrightarrow \psi \sim (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$$

- Negace:

$$\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$$
$$\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$$
$$\neg\neg\varphi \sim \varphi$$

- Konjunkce (převod do DNF):

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

- Disjunkce (převod do CNF):

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

2.4 Vlastnosti a důsledky teorií

Vlastnosti teorií

- sporná: $T \models \bot$, ekvivalentně: nemá model, platí v ní vše
- bezesporná (splnitelná): není sporná, tj. má model
- kompletní: bezesporná + každý výrok je v ní pravdivý nebo lživý (nemá nezávislé výroky), ekvivalentně: právě jeden model
- ekvivalence teorií: $T \sim T'$ právě když $\mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T')$ (různé *axiomatizace* týchž vlastností)

- $T_1 = \{p, p \to q, \neg q\}$ je sporná
- $T_2 = \{p \vee q, r\}$ je bezesporná, ale není kompletní, např. $p \wedge q$ je v ní nezávislý: platí v modelu $(1,1,1)$, neplatí v $(1,0,1)$
- $T_2 \cup \{\neg p\}$ je kompletní, jediným modelem je $(0,1,1)$.
- ekvivalentní teorie: $\{p \to q, r\} \sim \{(\neg p \vee q) \wedge r\}$

Důsledky teorií

Buď T teorie v jazyce $\mathbb{P}$. Množina všech důsledků T v jazyce $\mathbb{P}'$:

$$\mathrm{Csq}_{\mathbb{P}'}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}'} \mid T \models \varphi\}$$

pokud $\mathbb{P}' = \mathbb{P}$: $\mathrm{Csq}_{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid \mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)\}$

Tvrzení: Jsou-li T, T' teorie a $\varphi, \varphi_1, \ldots, \varphi_n$ výroky v jazyce $\mathbb{P}$:

(i) $T \subseteq \mathrm{Csq}_{\mathbb{P}}(T)$

(ii) $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(\mathrm{Csq}_{\mathbb{P}}(T))$

(iii) pokud $T \subseteq T'$, potom $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}}(T')$

(iv) $\varphi \in \mathrm{Csq}_{\mathbb{P}}(\{\varphi_1, \ldots, \varphi_n\})$ právě když $\models (\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \varphi$

Důkaz: snadný, použijte následující:

- $\mathrm{M}(\mathrm{Csq}(T)) = \mathrm{M}(T)$
- je-li $T \subseteq T'$ potom $\mathrm{M}(T) \supseteq \mathrm{M}(T')$
- $\models \psi \rightarrow \varphi$ právě když $\mathrm{M}(\psi) \subseteq \mathrm{M}(\varphi)$ $\square$

Extenze teorií: neformálně

Extenze teorie T je jakákoliv teorie, která splňuje vše, co platí v T

- dodatečné požadavky o systému: jednoduchá extenze
- přidání nových částí k systému (a v původním platí totéž, co předtím): konzervativní extenze

Úvodní příklad o barvení grafů:

- T_3 (úplná obarvení s hranovou podmínkou) je jednoduchou extenzí teorie T_1 (částečná obarvení bez ohledu na hrany)
- T_3' (přidání nového vrcholu) je konzervativní, ale ne jednoduchou extenzí T_3
- T_3' je extenze T_1, která není ani jednoduchá, ani konzervativní

Extenze teorií: formálně

Buď T v jazyce $\mathbb{P}$. Extenze teorie T je libovolná teorie T' v jazyce $\mathbb{P}' \supseteq \mathbb{P}$ splňující $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}'}(T')$,

- jednoduchá: $\mathbb{P}' = \mathbb{P}$
- konzervativní: $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(T') = \mathrm{Csq}_{\mathbb{P}'}(T') \cap \mathrm{VF}_{\mathbb{P}}$

"nové důsledky musí obsahovat nové prvovýroky"

Pozorování:

1. T' je jednoduchá extenze T, právě když $\mathbb{P}' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') \subseteq \mathrm{M}_{\mathbb{P}}(T)$
2. T' je extenze T, právě když $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$. Tj. restrikce modelů T' na $\mathbb{P}$ musí být modely T: $\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$
3. T' je konzervativní extenze T, je-li to extenze a navíc každý model T lze expandovat na model T' (tj. *každý* model T získáme restrikcí *nějakého* modelu T' na jazyk $\mathbb{P}$): $\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} = \mathrm{M}_{\mathbb{P}}(T)$
4. T' je extenze T a zároveň T je extenze T', právě když $T \sim T'$
5. Kompletní jednoduché extenze T odpovídají modelům T (až na $\sim$)

Extenze teorií: příklad

- mějme $T = \{p \to q\}$ v jazyce $\mathbb{P} = \{p, q\}$, teorie $T_1 = \{p \wedge q\}$ v jazyce $\mathbb{P}$ je jednoduchá extenze T: $\mathrm{M}_{\mathbb{P}}(T_1) \subseteq \mathrm{M}_{\mathbb{P}}(T)$
- T_1 je kompletní, až na ekvivalenci všechny jednoduché kompletní extenze T jsou: T_1, $T_2 = \{\neg p, q\}$, a $T_3 = \{\neg p, \neg q\}$
- teorie $T' = \{p \leftrightarrow (q \wedge r)\}$ v $\mathbb{P}' = \{p, q, r\}$ je extenzí teorie T: $\mathbb{P} \subseteq \mathbb{P}'$ a $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$, restrikce modelů T' na $\mathbb{P}$ jsou $\{(0,0), (0,1), (1,1)\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$
- protože dokonce $\{(0,0), (0,1), (1,1)\} = \mathrm{M}_{\mathbb{P}}(T)$, každý model T lze rozšířit na model T', T' je konzervativní extenze T
- každý výrok v jazyce $\mathbb{P}$ platí v T, právě když platí v T', ale výrok $p \to r$ je novým důsledkem: platí v T' ale ne v T
- teorie $T'' = \{\neg p \vee q, \neg q \vee r, \neg r \vee p\}$ v jazyce $\mathbb{P}'$ je extenze T, ale není konzervativní, neboť v ní platí $p \leftrightarrow q$, což neplatí v T (nebo proto, že model $(0,1)$ teorie T nelze rozšířit na model teorie T'')

2.5 Algebra výroků

Výroky až na ekvivalenci

Kolik existuje výroků nad $\mathbb{P} = \{p, q, r\}$? Nekonečně mnoho. Až na ekvivalenci? Tolik, kolik je možných množin modelů: $2^{2^3} = 256$.

Výroky až na ekvivalenci studujeme pomocí jejich množin modelů.

Ekvivalenční třídy: ${}^{\mathrm{VF}_{\mathbb{P}}}/_{\sim}$, např. $[p \to q]_\sim = \{p \to q, \neg p \vee q, \dots\}$

Přiřazení modelů: $h : {}^{\mathrm{VF}_{\mathbb{P}}}/_{\sim} \to \mathcal{P}(\mathrm{M}_{\mathbb{P}})$ definované $h([\varphi]_\sim) = \mathrm{M}(\varphi)$ (je dobře definované, prosté, pro konečný jazyk bijekce)

Na ${}^{\mathrm{VF}_{\mathbb{P}}}/_{\sim}$ zavedeme operace $\neg, \wedge, \vee$ pomocí reprezentantů:

$$\neg[\varphi]_\sim = [\neg\varphi]_\sim$$
$$[\varphi]_\sim \wedge [\psi]_\sim = [\varphi \wedge \psi]_\sim$$
$$[\varphi]_\sim \vee [\psi]_\sim = [\varphi \vee \psi]_\sim$$

přidáme konstanty $\bot = [\bot]_\sim, \top = [\top]_\sim$, máme *Booleovu algebru*: algebru výroků jazyka $\mathbb{P}$; totéž relativně k teorii T (použijeme $\sim_T$)

Algebra výroků

Algebra výroků jazyka $\mathbb{P}$ resp. teorie T:

$$\mathbf{AV}_{\mathbb{P}} = \langle {}^{\mathrm{VF}_{\mathbb{P}}}/_{\sim}; \neg, \wedge, \vee, \bot, \top \rangle$$

$$\mathbf{AV}_{\mathbb{P}}(T) = \langle {}^{\mathrm{VF}_{\mathbb{P}}}/_{\sim_T}; \neg_T, \wedge_T, \vee_T, \bot_T, \top_T \rangle$$

přiřazení modelů h je prosté zobrazení algebry výroků jazyka do potenční algebry $\mathcal{P}(\mathrm{M}_{\mathbb{P}}) = \langle \mathcal{P}(\mathrm{M}_{\mathbb{P}}); \overline{}, \cap, \cup, \emptyset, \mathrm{M}_{\mathbb{P}} \rangle$ zachovávající operace a konstanty: $h(\bot) = \emptyset$, $h(\top) = \mathrm{M}_{\mathbb{P}}$, a

$$h(\neg[\varphi]_{\sim}) = \overline{h([\varphi]_{\sim})} = \overline{\mathrm{M}(\varphi)} = \mathrm{M}_{\mathbb{P}} \setminus \mathrm{M}(\varphi)$$

$$h([\varphi]_{\sim} \wedge [\psi]_{\sim}) = h([\varphi]_{\sim}) \cap h([\psi]_{\sim}) = \mathrm{M}(\varphi) \cap \mathrm{M}(\psi)$$

$$h([\varphi]_{\sim} \vee [\psi]_{\sim}) = h([\varphi]_{\sim}) \cup h([\psi]_{\sim}) = \mathrm{M}(\varphi) \cup \mathrm{M}(\psi)$$

tj. je to homomorfismus Booleových algeber, a nad konečným jazykem bijekce, tzv. izomorfismus; stejně pro algebru výroků teorie

Důsledek: Pro bezespornou teorii T nad *konečným jazykem* $\mathbb{P}$ je algebra výroků $\mathbf{AV}_{\mathbb{P}}(T)$ izomorfní potenční algebře $\mathcal{P}(\mathrm{M}_{\mathbb{P}}(\mathbf{T}))$ prostřednictvím zobrazení $h([\varphi]_{\sim_T}) = M(T, \varphi)$.

Počítání až na ekvivalenci

Tvrzení: Mějme n-prvkový jazyk $\mathbb{P}$ a bezespornou teorii T mající právě k modelů. Potom v jazyce $\mathbb{P}$ existuje až na ekvivalenci:

- 2^{2^n} výroků (resp. teorií),
- 2^{2^n-k} výroků pravdivých (resp. lživých) v T,
- $2^{2^n} - 2 \cdot 2^{2^n-k}$ výroků nezávislých v T,
- 2^k jednoduchých extenzí teorie T (z toho 1 sporná),
- k kompletních jednoduchých extenzí T.

Dále až na T-ekvivalenci existuje:

- 2^k výroků,
- 1 výrok pravdivý v T, 1 lživý v T,
- $2^k - 2$ výroků nezávislých v T.

Důkaz: stačí spočítat možné množiny modelů $\square$

Třetí přednáška

Program

- problém splnitelnosti, SAT solvery
- 2-SAT a implikační graf
- Horn-SAT a jednotková propagace
- algoritmus DPLL
- úvod do tablo metody

Materiály

Zápisky z přednášky, Kapitola 3, Sekce 4.1-4.2 z Kapitoly 4

Kapitola 3: Problém splnitelnosti

Problém splnitelnosti Booleovských formulí

Problém SAT:

- vstup: výrok φ v CNF
- otázka: je φ splnitelný?

univerzální problém: každou teorii nad konečným jazykem lze převést do CNF

Cook-Levinova věta: SAT je NP-úplný (důkaz: formalizuj výpočet nedeterministického Turingova stroje ve výrokové logice)

ale některé *fragmenty* jsou v P, efektivně řešitelné, např. 2-SAT a Horn-SAT (viz Sekce 3.2 a 3.3)

praktický problém: moderní *SAT solvery* (viz Sekce 3.1) se používají v řadě odvětví aplikované informatiky, poradí si s obrovskými instancemi

3.1 SAT solvery

SAT solvery

- existují od 60. let 20. století, v 21. století dramatický rozvoj dnes až 10^8 proměnných, viz www.satcompetition.org.
- nejčastěji založeny na jednoduchém algoritmu DPLL (viz Sekce 3.4), umí i najít řešení (model)
- různá rozšíření, zejména Conflict-driven clause learning (CDCL)
- řada technologií pro efektivnější řešení instancí pocházejících z různých aplikačních domén, heuristiky pro řízení prohledávání (za použití ML, NN) — desítky tisíc řádků kódu

Praktická ukázka: boardomino

Lze pokrýt šachovnici s chybějícími dvěma protilehlými rohy perfektně pokrýt kostkami domina?

těžká instance SATu (proč?), jak zakódovat?

řešič Glucose, formát vstupu: DIMACS CNF

3.2 2-SAT a implikační graf

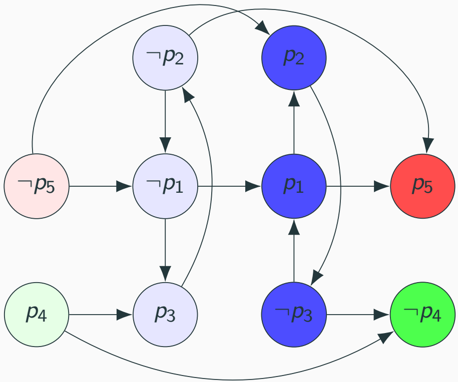
2-SAT vs. 3-SAT

- k-CNF: CNF a každá klauzule nejvýše k literálů
- k-SAT: je daný k-CNF výrok splnitelný?
- k-SAT je NP-úplný pro $k \geq 3$ (ke každému výroku lze sestrojit ekvisplnitelný 3-CNF výrok)
- ale 2-SAT je v P, dokonce řešitelný v lineárním čase
- algoritmus využívá tzv. implikační graf:
  - 2-klauzule $p \vee q$ je ekvivalentní $\neg p \rightarrow q$ a také $\neg q \rightarrow p$
  - $p \sim p \vee p$ je ekvivalentní $\neg p \rightarrow p$
  - vrcholy jsou literály
  - hrany dané implikacemi
  - **myšlenka**: ohodnotíme-li vrchol 1, všude kam se dostaneme po hranách (komponenta silné souvislosti) musí být také 1

Implikační graf

$$V(\mathcal{G}_\varphi) = \{p, \neg p \mid p \in \mathrm{Var}(\varphi)\},$$
$$E(\mathcal{G}_\varphi) = \{(\overline{\ell_1}, \ell_2), (\overline{\ell_2}, \ell_1) \mid \ell_1 \vee \ell_2 \text{ je klauzule } \varphi\} \cup$$
$$\{(\bar{\ell}, \ell) \mid \ell \text{ je jednotková klauzule } \varphi\}$$

$(\neg p_1 \vee p_2) \wedge (\neg p_2 \vee \neg p_3) \wedge (p_1 \vee p_3) \wedge (p_3 \vee \neg p_4) \wedge (\neg p_1 \vee p_5) \wedge (p_2 \vee p_5) \wedge p_1 \wedge \neg p_4$

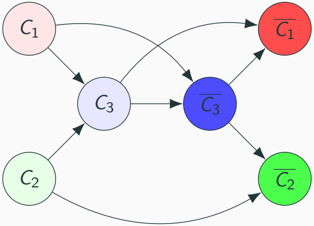


- najdeme komponenty silné souvislosti
- literály v komponentě musí být ohodnoceny stejně (jinak "$1 \to 0$")
- pokud má nějaká komponenta opačné literály, je φ nesplnitelný
- jinak sestrojíme model

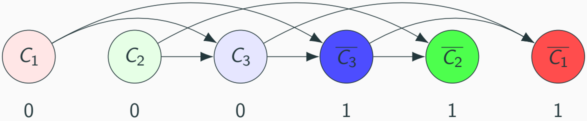
Konstrukce modelu

Všimněte si: stačí, aby z žádné komponenty ohodnocené 1 nevedla hrana do komponenty ohodnocené 0

provedeme kontrakci komponent, výsledný graf $\mathcal{G}_\varphi^*$ je acyklický



najdeme nějaké topologické uspořádání; v něm najdeme nejlevější dosud neohodnocenou komponentu, ohodnotíme ji 0, opačnou komponentu ohodnotíme 1, a opakujeme



Shrnutí

Tvrzení: φ je splnitelný, právě když žádná silně souvislá komponenta v $\mathcal{G}_\varphi$ neobsahuje dvojici opačných literálů.

Důkaz: $\Rightarrow$ literály v komponentě musí být ohodnoceny stejně

$\Leftarrow$ ohodnocení zkonstruované výše je model φ:

- jednotková klauzule ℓ platí kvůli hraně $\overline{\ell} \to \ell$, komponenta s $\overline{\ell}$ byla ohodnocena dříve, a to 0, takže $v(\ell) = 1$
- podobně pro 2-klauzuli $\ell_1 \vee \ell_2$, máme hrany $\overline{\ell_1} \to \ell_2$, $\overline{\ell_2} \to \ell_1$ pokud jsme ℓ_1 ohodnotili dříve než ℓ_2, museli jsme jako první narazit na komponentu s $\overline{\ell_1}$ a ohodnotit ji 0, tedy ℓ_1 platí; v opačném případě symetricky platí ℓ_2 $\square$

Důsledek: 2-SAT je řešitelný v lineárním čase, včetně konstrukce modelu (pokud existuje).

Důkaz: Komponenty silné souvislosti i topologické uspořádání najdeme v čase $\mathcal{O}(|V| + |E|)$, stačí je projít jednou $\square$

3.3 Horn-SAT a jednotková propagace

Horn-SAT

- hornovská klauzule: *nejvýše jeden *pozitivní* literál*

$$\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n \vee q \;\sim\; (p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

  základ logického programování (Prolog `q:-p1,p2,...,pn.`)

- Horn-SAT, tj. splnitelnost hornovského výroku (konjunkce hornovských klauzulí) je opět v P, v lineárním čase
- algoritmus využívá tzv. jednotkovou propagaci:
  - jednotková klauzule vynucuje hodnotu výrokové proměnné
  - tím můžeme výrok zjednodušit, např. pro $\neg p$ ($p = 0$):
    odstraníme klauzule s literálem $\neg p$, už jsou splněné
    odstraníme literál p (nemůže být splněný)
  - žádná jednotková klauzule $\Rightarrow$ každá klauzule má aspoň jeden negativní literál $\Rightarrow$ vše nastavíme na 0

Jednotková propagace

$\varphi = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3) \wedge (\neg p_5 \vee \neg p_4) \wedge p_4$

- nastav $v(p_4) = 1$, odstraň klauzule obsahující literál p_4, z ostatních klauzulí odstraň $\neg p_4$

$$\varphi^{p_4} = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3) \wedge \neg p_5$$

- nastav $v(p_5) = 0$, proveď jednotkovou propagaci $\neg p_5$

$$(\varphi^{p_4})^{\neg p_5} = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3)$$

- už žádná jednotková klauzule, v každé klauzuli alespoň dva literály ale nejvýše jeden pozitivní, tj. alespoň jeden negativní: $v(p_1) = v(p_2) = v(p_3) = 0$, model $v = (0, 0, 0, 1, 0)$

$$\varphi^{\ell} = \{C \setminus \{\overline{\ell}\} \mid C \in \varphi, \ell \notin C\} \qquad \text{(množinový zápis)}$$

Pozorování: φ^{ℓ} neobsahuje ℓ ani $\overline{\ell}$, modely = modely φ splňující ℓ

$\psi = p \wedge (\neg p \vee q) \wedge (\neg q \vee r) \wedge \neg r$ je nesplnitelný, co se stane?

Algoritmus pro Horn-SAT

vstup: výrok φ v Hornově tvaru,

výstup: model φ nebo informace, že φ není splnitelný

1. Pokud φ obsahuje dvojici opačných jednotkových klauzulí $\ell, \overline{\ell}$, není splnitelný.
2. Pokud φ neobsahuje žádnou jednotkovou klauzuli, je splnitelný, ohodnoť všechny zbývající proměnné 0.
3. Pokud φ obsahuje jednotkovou klauzuli ℓ, ohodnoť literál ℓ hodnotou 1, proveď jednotkovou propagaci, nahraď φ výrokem φ^{ℓ}, a vrať se na začátek.

Tvrzení: Algoritmus je korektní.

Důsledek: Horn-SAT lze řešit v lineárním čase.

Důkaz: Korektnost plyne z pozorování a z diskuze. V každém kroku stačí projít, výrok zkrátíme (kvadratický horní odhad, ale při vhodné implementaci lineární) $\square$

3.4 Algoritmus DPLL

Algoritmus DPLL (Davis-Putnam-Logemann-Loveland, 1961)

myšlenka: čistý výskyt p buď jen v pozitivních nebo jen v negativních literálech $\Rightarrow$ lze mu nastavit příslušnou hodnotu!

DPLL = jednotková propagace + čistý výskyt + větvení (rekurze)

vstup: výrok φ v CNF,

výstup: model φ nebo informace, že φ není splnitelný

1. Dokud φ obsahuje jednotkovou klauzuli ℓ, ohodnoť literál ℓ hodnotou 1, proveď jednotkovou propagaci, nahraď φ výrokem φ^ℓ.
2. Dokud existuje literál ℓ, který má ve φ čistý výskyt, ohodnoť ℓ hodnotou 1, a odstraň klauzule obsahující ℓ.
3. Pokud φ neobsahuje žádnou klauzuli, je splnitelný.
4. Pokud φ obsahuje prázdnou klauzuli, není splnitelný.
5. Jinak zvol dosud neohodnocenou výrokovou proměnnou p, a zavolej algoritmus rekurzivně na $\varphi \wedge p$ a na $\varphi \wedge \neg p$.

Ukázkový běh

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

žádná jednotková klauzule, $\neg r$ má čistý výskyt: nastav $v(r) = 0$ a odstraň klauzule obsahující $\neg r$:

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

už žádný čistý výskyt, rekurzivně zavolej na:

1. $(\neg p \vee \neg q \vee \neg s) \wedge (p \vee s) \wedge (p \vee \neg s) \wedge (q \vee s) \wedge p$
2. $(\neg p \vee \neg q \vee \neg s) \wedge (p \vee s) \wedge (p \vee \neg s) \wedge (q \vee s) \wedge \neg p$

a pokračuj dále v obou větvích výpočtu

$$\vdots$$

1. větev dává $(1, 0, 0, 1)$ a $(1, 1, 0, 0)$, 2. je sporná. Modelem je také $(1, 1, 1, 0)$, ten ztratíme nastavením $v(r) = 0$. Odstranění čistého výskytu zachová splnitelnost, ne všechny modely.

Kapitola 4: Metoda analytického tabla

4.1 Formální dokazovací systémy

Formální dokazovací systém

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

důkaz je konečný syntaktický objekt vycházející z φ a axiomů T

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

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

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

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

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

4.2 Úvod do tablo metody

Tablo metoda neformálně

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

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

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

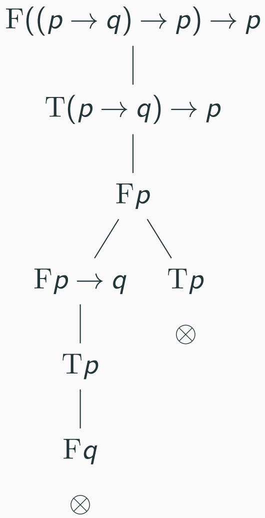
kořen $\mathrm{F}\varphi$, dále rozvíjíme redukcí položek (podle struktury výroků v nich), aby platil invariant:

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

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

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

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



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

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

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

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

$$\mathrm{F}p$$

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

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

$$\checkmark$$

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

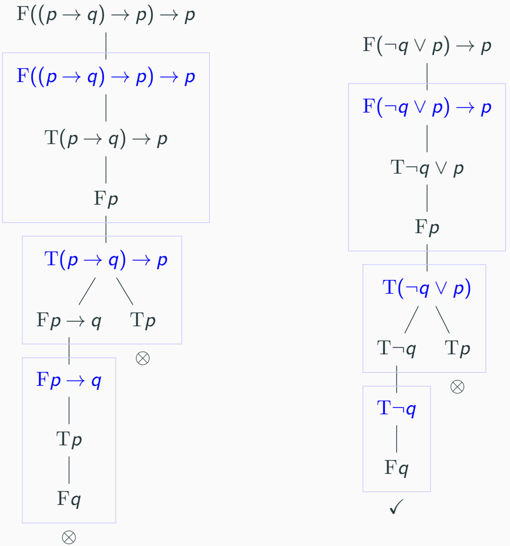
Poznámky

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

Atomická tabla

	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
True	$\begin{array}{c} \mathrm{T}\neg\varphi \\ \mathrm{F}\varphi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi \wedge \psi \\ \mathrm{T}\varphi \\ \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi \vee \psi \\ \mathrm{T}\varphi \qquad \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi \rightarrow \psi \\ \mathrm{F}\varphi \qquad \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi \leftrightarrow \psi \\ \mathrm{T}\varphi \qquad \mathrm{F}\varphi \\ \mathrm{T}\psi \qquad \mathrm{F}\psi \end{array}$
False	$\begin{array}{c} \mathrm{F}\neg\varphi \\ \mathrm{T}\varphi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \wedge \psi \\ \mathrm{F}\varphi \qquad \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \vee \psi \\ \mathrm{F}\varphi \\ \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \rightarrow \psi \\ \mathrm{T}\varphi \\ \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi \leftrightarrow \psi \\ \mathrm{T}\varphi \qquad \mathrm{F}\varphi \\ \mathrm{F}\psi \qquad \mathrm{T}\psi \end{array}$

Konstrukce tabel z příkladů



konvence: kořeny atomických tabel (modře) nezakreslujeme

O stromech

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

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

Čtvrtá přednáška

Program

- tablo důkaz
- korektnost a úplnost
- věta o kompaktnosti

Materiály

Zápisky z přednášky, Sekce 4.3-4.7 z Kapitoly 4 (Sekci 4.8 zatím přeskočíme)

4.3 Tablo důkaz

Formální definice tabla

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

Dokončené a sporné tablo

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

Tablo důkaz a tablo zamítnutí

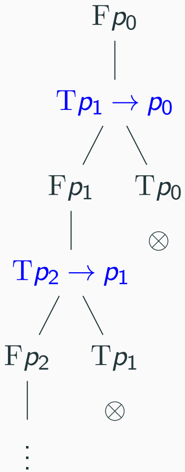
- tablo důkaz výroku φ z teorie T je sporné tablo z teorie T s položkou $\mathrm{F}\varphi$ v kořeni
- pokud existuje, je φ (tablo) dokazatelný z T, píšeme $T \vdash \varphi$
- podobně, tablo zamítnutí je sporné tablo s $\mathrm{T}\varphi$ v kořeni
- existuje-li, je φ (tablo) zamítnutelný z T, tj. platí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

Příklad: tablo důkaz

$$\begin{tikzcd}[column sep=small]
& \mathrm{F}\psi \arrow[d, no head] & \\
& \color{blue}{\mathrm{T}\varphi \to \psi} \arrow[dl, no head] \arrow[dr, no head] & \\
\mathrm{F}\varphi \arrow[d, no head] & & \mathrm{T}\psi \\
\color{blue}{\mathrm{T}\varphi} & & \otimes \\
\otimes & &
\end{tikzcd}$$

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

Příklad: dokončené tablo, které není sporné



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

4.4 Konečnost a systematičnost důkazů

Konečnost a systematičnost důkazů

Dokážeme:

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

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

  (pokud tablo důkaz neexistuje, algoritmus se nemusí zastavit)

Dokončení tabla: v čem je problém?

Pro konečnou T je snadné zkonstruovat dokončené tablo:

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

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

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

Myšlenka systematického tabla: na všechny se dostane, střídáme:

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

Definice systematického tabla

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

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

Dokončenost systematického tabla

Lemma: Systematické tablo je dokončené.

Důkaz: Jsou všechny větve dokončené?

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

Konečnost sporu

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

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

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

Důsledky konečnosti sporu

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

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

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

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

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

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

4.5 Korektnost a úplnost

Korektnost a úplnost

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

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

Rozdělíme na dvě implikace:

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

Korektnost: pomocné lemma

Model v se shoduje

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

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

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

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

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

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

Pokračování důkazu pomocného lemmatu

Indukční krok:

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

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

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

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

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

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

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

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

Úplnost: pomocné lemma

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

Kanonický model pro bezespornou, dokončenou větev V je model

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

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

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

Důkaz pomocného lemmatu

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

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

Indukční krok: rozebereme dva případy, ostatní jsou obdobné

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

Věta o úplnosti (+ důkaz systematičnosti)

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

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

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

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

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

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

4.6 Důsledky korektnosti a úplnosti

$\vdash = \models$

Syntaktickou analogií důsledků jsou teorémy:

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

Z korektnosti a úplnosti okamžitě dostáváme:

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

Všude můžeme nahradit 'platnost' pojmem 'dokazatelnost'. Např:

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

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

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

4.7 Věta o kompaktnosti

Věta (O kompaktnosti): Teorie má model, právě když každá její konečná část má model.

Důkaz: $\Rightarrow$ Snadné: Model T je zjevně modelem každé její části.

$\Leftarrow$ Nepřímo: buď T sporná, najdeme spornou konečnou $T' \subseteq T$.

Z úplnosti víme, že $T \vdash \bot$, tedy existuje i konečný tablo důkaz τ výroku $\bot$ z T. Konstrukce τ má konečně mnoho kroků, použili jsme tedy jen konečně mnoho axiomů z T. Definujme:

$$T' = \{\alpha \in T \mid \mathrm{T}\alpha \text{ je položka v tablu } \tau\}$$

Tedy τ je tablo jen z teorie T', máme tablo důkaz $T' \vdash \bot$, dle korektnosti je T' sporná. $\square$

Aplikace kompaktnosti

vlastnost nekonečného objektu $\mathcal{O}$

$$\Updownarrow$$

vlastnost všech konečných podobjektů $\mathcal{O}'$

- vlastnost popíšeme pomocí (nekonečné) teorie T
- ke každé konečné $T' \subseteq T$ sestrojíme konečný podobjekt $\mathcal{O}'$
- $\mathcal{O}'$ splňuje danou vlastnost
- to nám dává model T'
- dle Věty o kompaktnosti má i T model
- což ukazuje, že i nekonečný objekt $\mathcal{O}$ splňuje vlastnost

Věta o kompaktnosti má mnoho aplikací (několik z nich uvidíme později), následující příklad chápejte jako 'šablonu'.

Aplikace kompaktnosti: příklad

Důsledek: Spočetně nekonečný graf je bipartitní, právě když je každý jeho konečný podgraf bipartitní.

Důkaz: $\Rightarrow$ Každý podgraf bipartitního grafu je bipartitní.

$\Leftarrow$ G je bipartitní, právě když je obarvitelný 2 barvami. Mějme jazyk $\mathbb{P} = \{p_v \mid v \in V(G)\}$ (kde p_v je barva v) a uvažme teorii

$$T = \{p_u \leftrightarrow \neg p_v \mid \{u, v\} \in E(G)\}$$

Zřejmě G je bipartitní, právě když T má model. Dle Věty o kompaktnosti stačí ukázat, že každá konečná $T' \subseteq T$ má model.

Buď G' podgraf G indukovaný na vrcholech, o kterých T' mluví:

$$V(G') = \{v \in V(G) \mid p_v \in \mathrm{Var}(T')\}$$

Protože je T' konečná, je G' také konečný, tedy je dle předpokladu 2-obarvitelný. Libovolné 2-obarvení $V(G')$ ale určuje model T'. $\square$

Pátá přednáška

Program

- rezoluční metoda
- korektnost a úplnost rezoluce
- úvod do predikátové logiky
- syntaxe predikátové logiky

Materiály

Zápisky z přednášky, Sekce 5.1-5.3 z Kapitoly 5 (Sekci 5.4 zatím přeskočíme), Sekce 6.1-6.3 z Kapitoly 6

Kapitola 5: Rezoluční metoda

Rezoluční metoda

- jiný důkazový systém než tablo metoda
- mnohem efektivnější implementace
- logické programování, automatické dokazování, SAT solvery (důkaz jako certifikát nesplnitelnosti)
- pracuje s CNF (každý výrok/teorii lze převést do CNF)
- jediné inferenční pravidlo: rezoluční pravidlo

$$\frac{\{p\} \dot\sqcup C_1, \{\neg p\} \dot\sqcup C_2}{C_1 \cup C_2}$$

- platí obecnější pravidlo řezu:

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

5.1 Množinová reprezentace

Množinová reprezentace

- literál ℓ je p nebo $\neg p$ (pro $p \in \mathbb{P}$), $\bar{\ell}$ je opačný literál k ℓ
- klauzule C je konečná množina literálů
- prázdná klauzule $\square$ je nesplnitelná
- CNF formule S je množina klauzulí(může být i nekonečná!)
- prázdná formule $\emptyset$ je vždy splněna

Modely reprezentujeme jako množiny literálů:

- (částečné) ohodnocení je libovolná konzistentní množina literálů (tj. nesmí obsahovat dvojici opačných literálů)
- úplné ohodnocení obsahuje p nebo $\neg p$ pro každý prvovýrok
- ohodnocení $\mathcal{V}$ splňuje formuli S, píšeme $\mathcal{V} \models S$, pokud $\mathcal{V}$ obsahuje nějaký literál z každé klauzule v S:

$$\mathcal{V} \cap C \neq \emptyset \text{ pro každou } C \in S$$

Množinová reprezentace: příklad

$$\varphi = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_3 \vee \neg p_4) \wedge (\neg p_4 \vee \neg p_5) \wedge p_4$$

- v množinové reprezentaci:
  $S = \{\{\neg p_1, p_2\}, \{\neg p_1, \neg p_2, p_3\}, \{\neg p_3, \neg p_4\}, \{\neg p_4, \neg p_5\}, \{p_4\}\}$
- ohodnocení $\mathcal{V} = \{\neg p_1, \neg p_3, p_4, \neg p_5\}$ splňuje S, $\mathcal{V} \models S$
- není úplné, můžeme rozšířit libovolným literálem pro p_2:
  - $\mathcal{V} \cup \{p_2\} \models S$
  - $\mathcal{V} \cup \{\neg p_2\} \models S$
- tato dvě úplná ohodnocení odpovídají modelům
  - $(0, 1, 0, 1, 0)$
  - $(0, 0, 0, 1, 0)$

5.2 Rezoluční důkaz

Rezoluční pravidlo

Mějme klauzule C_1 a C_2 a literál ℓ takový, že $\ell \in C_1$ a $\bar{\ell} \in C_2$. Potom rezolventa klauzulí C_1 a C_2 přes literál ℓ je klauzule:

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

tedy z první klauzule odstraníme ℓ a z druhé $\bar{\ell}$ (musely tam být!) a zbylé literály sjednotíme, mohli bychom také psát:

$$C_1' \cup C_2' \text{ je rezolventou klauzulí } C_1' \mathbin{\dot\sqcup} \{\ell\} \text{ a } C_2' \mathbin{\dot\sqcup} \{\bar{\ell}\}$$

- z klauzulí $C_1 = \{\neg q, r\}$ a $C_2 = \{\neg p, \neg q, \neg r\}$ odvodíme klauzuli $\{\neg p, \neg q\}$ přes literál r
- z $\{p, q\}$ a $\{\neg p, \neg q\}$ odvodíme $\{p, \neg p\}$ přes literál q, nebo $\{q, \neg q\}$ přes literál p (obojí jsou ale tautologie)
- nelze z nich ale odvodit $\square$ *"rezolucí přes p a q najednou"*! ($S = \{\{p, q\}, \{\neg p, \neg q\}\}$ je splnitelná, např. $(1, 0)$ je model)

Rezoluční důkaz

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

Pokud $\mathcal{V} \models C_1$ a $\mathcal{V} \models C_2$, potom $\mathcal{V} \models C$.

V rezolučním důkazu můžeme vždy napsat buď axiom, nebo rezolventu již napsaných klauzulí; tím zaručíme korektnost důkazů:

Rezoluční důkaz (odvození) klauzule C z formule S je konečná posloupnost klauzulí $C_0, C_1, \ldots, C_n = C$ taková, že pro každé i:

- $C_i \in S$, nebo
- C_i je rezolventou nějakých C_j, C_k kde $j, k < i$

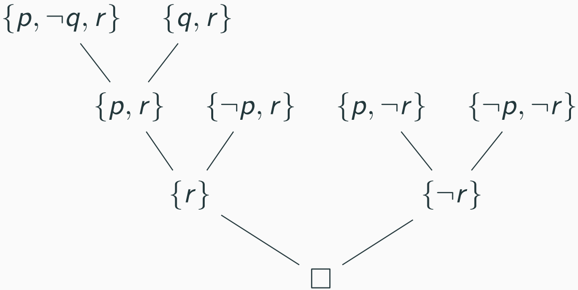
- existuje-li rez. důkaz, je C rezolucí dokazatelná z S, $S \vdash_R C$
- rezoluční zamítnutí formule S je rezoluční důkaz $\square$ z S
- v tom případě je S rezolucí zamítnutelná

Příklad

Formule $S = \{\{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{\neg p, \neg r\}, \{q, r\}\}$ je rezolucí zamítnutelná, jedno z možných zamítnutí je:

$$\{p, \neg q, r\}, \{q, r\}, \{p, r\}, \{\neg p, r\}, \{r\}, \{p, \neg r\}, \{\neg p, \neg r\}, \{\neg r\}, \square$$

Rezoluční důkaz má přirozeně stromovou strukturu, tzv. rezoluční strom: na listech jsou axiomy, vnitřní vrcholy jsou rezoluční kroky.



Rezoluční strom

Rezoluční strom klauzule C z formule S je konečný binární strom s vrcholy označenými klauzulemi, kde

- v kořeni je C,
- v listech jsou klauzule z S,
- v každém vnitřním vrcholu je rezolventa klauzulí ze synů tohoto vrcholu.

Pozorování: C má rezoluční. strom z S, právě když $S \vdash_R C$. (Důkaz snadno indukcí dle hloubky stromu a délky důkazu.)

- rezolučnímu důkazu odpovídá jednoznačný rezoluční strom
- z rezolučního stromu můžeme získat více důkazů (jsou dané libovolnou procházkou po vrcholech, která navštíví vnitřní vrchol až poté, co navštívila oba jeho syny)

Rezoluční uzávěr

jaké všechny klauzule se můžeme rezolucí 'naučit' z dané formule? (není praktické je všechny najít, jde o užitečný teoretický pohled)

Rezoluční uzávěr $\mathcal{R}(S)$ formule S je definován induktivně jako nejmenší množina klauzulí splňující:

- $C \in \mathcal{R}(S)$ pro všechna $C \in S$,
- jsou-li $C_1, C_2 \in \mathcal{R}(S)$ a C jejich rezolventa, potom i $C \in \mathcal{R}(S)$

Pro $S = \{\{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{\neg p, \neg r\}, \{q, r\}\}$ máme:

$$\begin{aligned}\mathcal{R}(S) = \{&\{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{p, s\}, \{q, r\},\\ &\{p, \neg q\}, \{\neg q, r\}, \{r, \neg r\}, \{p, \neg p\}, \{r, s\},\\ &\{p, r\}, \{p, q\}, \{r\}, \{p\}\}\end{aligned}$$

5.3 Korektnost a úplnost rezoluční metody

Korektnost rezoluce

Korektnost dokážeme snadno indukcí podle délky důkazu (nebo alternativně indukcí dle hloubky rezolučního stromu).

Věta (O korektnosti rezoluce): Je-li CNF formule S rezolucí zamítnutelná, potom je S nesplnitelná.

Důkaz: Nechť $S \vdash_R \square$, a vezměme nějaký rezoluční důkaz $C_0, C_1, \ldots, C_n = \square$. Sporem: nechť existuje ohodnocení $\mathcal{V} \models S$. Indukcí podle i dokážeme, že $\mathcal{V} \models C_i$. Potom i $\mathcal{V} \models \square$, což je spor.

Pro $i = 0$ to platí, neboť $C_0 \in S$. Pro $i > 0$ máme dva případy:

- $C_i \in S$: v tom případě $\mathcal{V} \models C_i$ plyne z předpokladu, že $\mathcal{V} \models S$,
- C_i je rezolventou C_j, C_k, kde $j, k < i$: z indukčního předpokladu víme $\mathcal{V} \models C_j$ a $\mathcal{V} \models C_k$, $\mathcal{V} \models C_i$ plyne z korektnosti rezolučního pravidla $\square$

Dosazení

Je-li S CNF formule a ℓ literál, potom dosazení ℓ do S je formule

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

- S^ℓ je výsledkem jednotkové propagace aplikované na $S \cup \{\{\ell\}\}$.
- S^ℓ neobsahuje v žádné klauzuli literál ℓ ani $\bar{\ell}$ (vůbec tedy neobsahuje prvovýrok z ℓ)
- Pokud S neobsahovala literál ℓ ani $\bar{\ell}$, potom $S^\ell = S$.
- Pokud S obsahovala jednotkovou klauzuli $\{\bar{\ell}\}$, potom $\square \in S^\ell$, tedy S^ℓ je sporná.

Větvení

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

Důkaz: $\Rightarrow$ Ohodnocení $\mathcal{V} \models S$ nemůže obsahovat ℓ i $\bar{\ell}$; BÚNO $\bar{\ell} \notin \mathcal{V}$. Ukážeme, že potom $\mathcal{V} \models S^\ell$.

Vezměme libovolnou klauzuli v S^ℓ. Ta je tvaru $C \setminus \{\bar{\ell}\}$ pro klauzuli $C \in S$ (neobsahující literál ℓ). Víme, že $\mathcal{V} \models C$, protože ale $\mathcal{V}$ neobsahuje $\bar{\ell}$, muselo ohodnocení $\mathcal{V}$ splnit nějaký jiný literál v C, takže platí i $\mathcal{V} \models C \setminus \{\bar{\ell}\}$.

$\Leftarrow$ BÚNO mějme ohodnocení $\mathcal{V} \models S^\ell$. Protože se $\bar{\ell}$ (ani ℓ) nevyskytuje v S^ℓ, platí také $\mathcal{V} \setminus \{\bar{\ell}\} \models S^\ell$. Ohodnocení $\mathcal{V}' = (\mathcal{V} \setminus \{\bar{\ell}\}) \cup \{\ell\}$ potom splňuje všechny $C \in S$, tedy $\mathcal{V}' \models S$:

- pokud $\ell \in C$, potom $\ell \in C \cap \mathcal{V}'$ a $C \cap \mathcal{V}' \neq \emptyset$
- jinak $C \cap \mathcal{V}' = C \cap (\mathcal{V} \setminus \{\bar{\ell}\}) = (C \setminus \{\bar{\ell}\}) \cap (\mathcal{V} \setminus \{\bar{\ell}\}) \neq \emptyset$ neboť $\mathcal{V} \setminus \{\bar{\ell}\} \models C \setminus \{\bar{\ell}\} \in S^\ell$ $\square$

Strom dosazení

Zda je *konečná* formule S splnitelná můžeme zjišťovat rekurzivně, dosazením obou literálů pro některý prvovýrok p, a rozvětvením na $S^p, S^{\bar{p}}$ (jako v DPLL). Výslednému stromu říkáme strom dosazení.

Např. pro $S = \{\{p\},\{\neg q\},\{\neg p, \neg q\}\}$:

$$S$$

$$S^p = \{\{\neg q\}\} \qquad S^{\bar{p}} = \{\square, \{\neg q\}\}$$

$$\otimes$$

$$S^{pq} = \{\square\} \qquad S^{p\bar{q}} = \emptyset$$

$$\otimes \qquad \mathcal{V} = \{p, \bar{q}\}$$

- jakmile větev obsahuje $\square$, je nesplnitelná a nepokračujeme v ní
- listy jsou buď nesplnitelné, nebo prázdné teorie: v tom případě z posloupnosti dosazení získáme splňující ohodnocení.

Důsledek: CNF formule S (ve spočetném jazyce, může být i nekonečná) je nesplnitelná, právě když každá větev stromu dosazení obsahuje $\square$.

Důkaz: Pro konečnou S snadno dokážeme indukcí dle $|\mathrm{Var}(S)|$:

- Je-li $|\mathrm{Var}(S)| = 0$, máme $S = \emptyset$ nebo $S = \{\square\}$, v obou případech je strom dosazení jednoprvkový a tvrzení platí.
- V indukčním kroku vybereme libovolný literál $\ell \in \mathrm{Var}(S)$ a aplikujeme Lemma.

Je-li S nekonečná a splnitelná, má splňující ohodnocení, to se ‘shoduje’ s odpovídající (nekonečnou) větví ve stromu dosazení.

Je-li nekonečná a nesplnitelná, dle Věty o kompaktnosti existuje konečná $S' \subseteq S$, která je také nesplnitelná. Po dosazení pro všechny proměnné z $\mathrm{Var}(S')$ bude v každé větvi $\square$, to nastane po konečně mnoha krocích. $\square$

Úplnost rezoluce

Věta (O úplnosti rezoluce): Je-li CNF formule S nesplnitelná, je rezolucí zamítnutelná (tj. $S \vdash_R \square$).

Důkaz: Je-li S nekonečná, má z kompaktnosti konečnou nesplnitelnou část, její rezoluční zamítnutí je také zamítnutí S.

Je-li S konečná, ukážeme indukcí dle počtu proměnných: Je-li $|\mathrm{Var}(S)| = 0$, jediná možná nesplnitelná formule bez proměnných je $S = \{\square\}$, a máme jednokrokový důkaz $S \vdash_R \square$.

Jinak vyberme $p \in \mathrm{Var}(S)$. Podle Lemmatu jsou S^p i $S^{\bar{p}}$ nesplnitelné. Mají o proměnnou méně, tedy dle ind. předpokladu existují rezoluční stromy T pro $S^p \vdash_R \square$ a T' pro $S^{\bar{p}} \vdash_R \square$.

Ukážeme, jak z T vyrobit rezoluční strom $\widehat{T}$ pro $S \vdash_R \neg p$. Analogicky $\widehat{T'}$ pro $S \vdash_R p$ a potom už snadno vyrobíme rezoluční strom pro $S \vdash_R \square$: ke kořeni $\square$ připojíme kořeny stromů $\widehat{T}$ a $\widehat{T'}$ jako levého a pravého syna (tj. získáme $\square$ rezolucí z $\{\neg p\}$ a $\{p\}$).

Dokončení důkazu

Rezoluční strom T pro $S^p \vdash_R \square \rightsquigarrow \widehat{T}$ pro $S \vdash_R \neg p$:

Vrcholy i uspořádání jsou stejné, jen do některých klauzulí ve vrcholech přidáme literál $\neg p$.

Na každém listu stromu T je nějaká klauzule $C \in S^p$, a

- buď $C \in S$,
- nebo $C \notin S$, ale $C \cup \{\neg p\} \in S$

V prvním případě necháme label stejný. Ve druhém případě přidáme do C a do všech klauzulí nad tímto listem literál $\neg p$.

Listy jsou nyní klauzule z S, a každý vnitřní vrchol je nadále rezolventou svých synů. V kořeni jsme $\square$ změnili na $\neg p$ (ledaže každý list T už byl klauzule z S, to ale už T dává $S \vdash_R \square$). $\square$

ČÁST II – PREDIKÁTOVÁ LOGIKA

Kapitola 6: Syntaxe a sémantika predikátové logiky

6.1 Úvod

Predikátová logika neformálně

Výroková logika: popis světa pomocí výroků složených z prvovýroků (výrokových proměnných) – bitů informace

Predikátová logika [prvního řádu]:

- základní stavební kámen jsou proměnné reprezentující individua – nedělitelné objekty z nějaké množiny (např. přirozená čísla, vrcholy grafu, stavy mikroprocesoru)
- tato individua mají určité vlastnosti a vzájemné vztahy (relace), kterým říkáme predikáty
  - $\mathrm{Leaf}(x)$ nebo $\mathrm{Edge}(x, y)$ mluvíme-li o grafu
  - $x \leq y$ v přirozených číslech
- a mohou vstupovat do funkcí
  - $\mathrm{lowest\_common\_ancestor}(x, y)$ v zakořeněném stromu
  - $\mathrm{succ}(x)$ nebo $x + y$ v přirozených číslech
- a mohou být konstantami se speciálním významem, např. root v zakořeněném stromu, 0 v tělese.

Syntaxe neformálně

- atomické formule: predikát (včetně rovnosti $=$) o proměnných nebo o termech ('výrazy' složené z funkcí popř. konstant)
- formule jsou složené z atomických formulí pomocí logických spojek, a dvou kvantifikátorů:

$\forall x$ "pro všechna individua (reprezentovaná proměnnou x)"
$\exists x$ "existuje individuum (reprezentované proměnnou x)"

Např. *"Každý, kdo má dítě, je rodič."* lze formalizovat takto:

$$(\forall x)((\exists y)\text{child\_of}(y, x) \rightarrow \text{is\_parent}(x))$$

- $\text{child\_of}(y, x)$ je binární predikát vyjadřující, že individuum reprezentované proměnnou y je dítětem individua reprezentovaného proměnnou x
- $\text{is\_parent}(x)$ je unární predikát vyjadřující, že individuum reprezentované x je rodič

Sémantika neformálně

$$(\forall x)((\exists y)\mathrm{child\_of}(y, x) \rightarrow \mathrm{is\_parent}(x))$$

Platnost? Záleží na modelu světa/systému, který nás zajímá:

Model je. . .

- (neprázdná) množina individuí, spolu
- s binární relací interpretující binární relační symbol $\mathrm{child\_of}$, a
- s unární relací (tj. podmnožinou) interpretující unární relační symbol $\mathrm{is\_parent}$

Obecně mohou být relace jakékoliv, snadno sestrojíme model, ve kterém formule neplatí, např.

$$\mathcal{A} = \langle \{0, 1\}, \{(0, 0), (0, 1), (1, 0), (1, 1)\}, \emptyset \rangle$$

Příklad s funkcemi a konstantami

"Je-li $x_1 \leq y_1$ a $x_2 \leq y_2$, potom platí $(y_1 \cdot y_2) - (x_1 \cdot x_2) \geq 0$."

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- dva binární relační symboly $(\leq, \geq)$, binární funkční symbol $+$, unární funkční symbol $-$, a konstantní symbol 0
- model, ve kterém φ platí: $\mathbb{N}$ s binárními relacemi $\leq^{\mathbb{N}}, \geq^{\mathbb{N}}$, bin. funkcemi $+^{\mathbb{N}}, \cdot^{\mathbb{N}}$, unární funkcí $-^{\mathbb{N}}$, a konstantou $0^{\mathbb{N}} = 0$
- vezmeme-li ale podobně množinu $\mathbb{Z}$, φ už platit nebude

Poznámky:

- mohli bychom chápat '$-$' jako binární, obvykle ale bývá unární
- pro konstantní symbol 0 používáme (jak je zvykem) stejný symbol, jako pro přirozené číslo 0. Ale pozor, v našem modelu může být symbol 0 interpretován jako jiné číslo, nebo náš model vůbec nemusí sestávat z čísel!

Ještě o syntaxi

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- φ nemá žádné kvantifikátory, tj. je otevřená
- x_1, x_2, y_1, y_2 jsou volné proměnné této formule (nejsou vázané žádným kvantifikátorem), píšeme $\varphi(x_1, x_2, y_1, y_2)$
- sémantiku φ chápeme stejně jako $(\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)\varphi$
- používáme konvence (infixový zápis, vynechání závorek), jinak:

$$\varphi = ((\leq (x_1, y_1) \wedge \leq (x_2, y_2)) \rightarrow \leq (+(\cdot(y_1, y_2), -(\cdot(x_1, x_2))), 0))$$

- cvičení: definujte strom formule, nakreslete ho pro φ

Termy vs. atomické formule

$$\varphi = (x_1 \leq y_1) \land (x_2 \leq y_2) \to ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- výraz $(y_1 \cdot y_2) + (-(x_1 \cdot x_2))$ je term
- výrazy $(x_1 \leq y_1)$, $(x_2 \leq y_2)$ a $((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$ jsou (všechny) atomické (pod)formule φ

V čem je rozdíl? Máme-li konkrétní model, a konkrétní ohodnocení proměnných individui (prvky) tohoto modelu:

- výsledkem termu (při daném ohodnocení proměnných) je konkrétní individuum z modelu, zatímco
- atomickým formulí lze přiřadit pravdivostní hodnotu (a tedy kombinovat je logickými spojkami)

6.2 Struktury

Signatura

- specifikuje jakého typu bude daná struktura, tj. jaké má relace, funkce (jakých arit) a konstanty, a symboly pro ně
- konstanty lze chápat jako funkce arity 0, tj. funkce bez vstupů

Signatura je dvojice $\langle \mathcal{R}, \mathcal{F} \rangle$, kde $\mathcal{R}, \mathcal{F}$ jsou disjunktní množiny symbolů (relační a funkční, ty zahrnují konstantní) spolu s danými aritami (tj. danými funkcí $\mathrm{ar}\colon \mathcal{R} \cup \mathcal{F} \to \mathbb{N}$) a neobsahující symbol '$=$'(ten je rezervovaný pro rovnost).

- často zapíšeme jen výčtem symbolů, jsou-li arity a zda jsou relační nebo funkční zřejmé
- kromě běžně používaných symbolů typicky používáme:
  - pro relační symboly $P, Q, R, \ldots$
  - pro funkční (nekonstantní) symboly $f, g, h, \ldots$
  - pro konstantní symboly $c, d, a, b, \ldots$

Příklady signatur

- $\langle E \rangle$ signatura grafů: E je binární relační symbol (struktury jsou uspořádané grafy)
- $\langle \leq \rangle$ signatura částečných uspořádání: stejná jako signatura grafů, jen jiný symbol (ne každá struktura v této signatuře je částečné uspořádání! k tomu musí splňovat příslušné axiomy)
- $\langle +, -, 0 \rangle$ signatura grup: $+$ je binární funkční, $-$ unární funkční, 0 konstantní symbol
- $\langle +, -, 0, \cdot, 1 \rangle$ signatura těles: $\cdot$ je binární funkční, 1 konstantní symbol
- $\langle +, -, 0, \cdot, 1, \leq \rangle$ signatura uspořádaných těles: $\leq$ je binární relační symbol
- $\langle -, \wedge, \vee, \bot, \top \rangle$ signatura Booleových algeber: $\wedge, \vee$ jsou binární funkční, $\bot, \top$ jsou konstantní symboly
- $\langle S, +, \cdot, 0, \leq \rangle$ signatura aritmetiky: S je unární funkční symbol

Struktury

Strukturu dané signatury získáme tak, že:

- zvolíme neprázdnou doménu, a na ní
- zvolíme realizace (také říkáme interpretace) všech relačních a funkčních symbolů (včetně konstantních)
- to znamená konkrétní relace resp. funkce příslušných arit
- realizací konstantního symbolu je zvolený prvek z domény
- na tom, jaké konkrétní symboly jsou v signatuře nezáleží (např. $+$ neznamená, že realizace musí souviset se sčítáním)

Příklady struktur 1/3

- Struktura v prázdné signatuře $\langle\ \rangle$ je libovolná neprázdná množina. (Nemusí být konečná, ani spočetná! Formálně to bude trojice $\langle A, \emptyset, \emptyset \rangle$, ale rozdíl zanedbáme.)
- Struktura v signatuře grafů je $\mathcal{G} = \langle V, E \rangle$, kde $V \neq \emptyset$ a $E \subseteq V^2$, říkáme jí orientovaný graf.
  - je-li E ireflexivní a symetrická, je to jednoduchý graf
  - je-li E reflexivní, tranzitivní, a antisymetrická, jde o částečné uspořádání
  - je-li E reflexivní, tranzitivní, a symetrická, je to ekvivalence
- Struktury v signatuře částečných uspořádání jsou tytéž, jako v signatuře grafů, signatury se liší jen symbolem. (Ne každá struktura v signatuře částečných uspořádání je č. uspořádání!)

Příklady struktur 2/3

Struktury v signatuře grup jsou například následující grupy:

- $\underline{\mathbb{Z}_n} = \langle \mathbb{Z}_n, +, -, 0 \rangle$, aditivní grupa celých čísel modulo n (operace jsou modulo n).

  Poznámka: $\underline{\mathbb{Z}_n}$ znamená strukturu, zatímco $\mathbb{Z}_n$ jen její doménu. Často se to ale nerozlišuje a $\mathbb{Z}_n$ se používá i pro strukturu. Podobně $+, -, 0$ jsou jak symboly, tak interpretace.
- $\mathcal{S}_n = \langle \mathrm{Sym}_n, \circ, {}^{-1}, \mathrm{id} \rangle$ je symetrická grupa (grupa všech permutací) na n prvcích.
- $\underline{\mathbb{Q}}^* = \langle \mathbb{Q} \setminus \{0\}, \cdot, {}^{-1}, 1 \rangle$ je multiplikativní grupa (nenulových) racionálních čísel. (Interpretací symbolu 0 je číslo 1!)

Všechny tyto struktury splňují axiomy teorie grup, snadno ale najdeme jiné, které axiomy nesplňují, nejsou tedy grupami.

Příklady struktur 3/3

- Struktury $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, -, 0, \cdot, 1, \leq \rangle$ a $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, -, 0, \cdot, 1, \leq \rangle$ (se standardními operacemi a uspořádáním) jsou v signatuře uspořádaných těles (ale jen první z nich je uspořádané těleso).
- $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), \bar{}, \cap, \cup, \emptyset, X \rangle$, tzv. potenční algebra nad množinou X, je struktura v signatuře Booleových algeber. (Booleova algebra je to pokud $X \neq \emptyset$.)
- $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$, kde $S(x) = x + 1$, a ostatní symboly jsou realizovány standardně, je standardní model aritmetiky.

Definice struktury

Struktura v signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$ je trojice $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$, kde

- A je neprázdná množina, říkáme jí doména (také univerzum),
- $\mathcal{R}^{\mathcal{A}} = \{R^{\mathcal{A}} \mid R \in \mathcal{R}\}$ kde $R^{\mathcal{A}} \subseteq A^{\mathrm{ar}(R)}$ je interpretace relačního symbolu R,
- $\mathcal{F}^{\mathcal{A}} = \{f^{\mathcal{A}} \mid f \in \mathcal{F}\}$ kde $f^{\mathcal{A}} \colon A^{\mathrm{ar}(f)} \to A$ je interpretace funkčního symbolu f (speciálně pro konstantní symbol $c \in \mathcal{F}$ máme $c^{\mathcal{A}} \in A$).

Příklad: rozmyslete si, jak vypadají struktury v signatuře n konstant $\langle c_1, c_2, \ldots, c_n \rangle$? Popište všechny 5-prvkové v signatuře 3 konstant.

6.3 Syntaxe

Jazyk

Jazyk je daný signaturou a informací, zda je s rovností nebo ne.

Tj. specifikujeme ‘typ’ modelů a zda můžeme používat symbol ‘$=$’ interpretovaný jako identita prvků z domény; většinou to dovolíme. (Je-li jazyk bez rovnosti, musí mít signatura relační symbol. Proč?)

Do jazyka patří:

- spočetně mnoho proměnných $x_0, x_1, x_2, \dots$ (píšeme také $x, y, z, \dots$; množinu všech proměnných označíme Var)
- relační, funkční a konstantní symboly ze signatury, symbol $=$ jde-li o jazyk s rovností (to jsou ‘mimologické’ symboly)
- univerzální a existenční kvantifikátory $(\forall x), (\exists x)$ pro každou proměnnou $x \in \mathrm{Var}$ (kvantifikátor ‘$(\forall x)$’ chápeme jako jediný symbol, tj. neobsahuje proměnnou x)
- symboly pro log. spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$, závorky $($, $)$, a čárka ‘,’

Jazyk: příklady

- Jazyk $L = \langle\rangle$ s rovností je jazyk čisté rovnosti
- jazyk $L = \langle c_0, c_1, c_2, \ldots\rangle$ s rovností je jazyk spočetně mnoha konstant
- jazyk uspořádání je $\langle\leq\rangle$ s rovností
- jazyk teorie grafů je $\langle E\rangle$ s rovností
- jazyky teorie grup, teorie těles, teorie uspořádaných těles, Booleových algeber, aritmetiky jsou jazyky s rovností odpovídající daným signaturám

Termy

čistě syntaktické 'výrazy' z proměnných, konstantních symbolů, funkčních symbolů, závorek a čárek

Termy jazyka L jsou konečné nápisy definované induktivně:

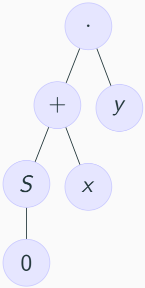
- každá proměnná a každý konstantní symbol z L je term,
- je-li f funkční symbol z L arity n a jsou-li $t_1, \ldots, t_n$ termy, potom nápis $f(t_1, t_2, \ldots, t_n)$ je také term.

Množinu všech termů jazyka L označíme Term_L.

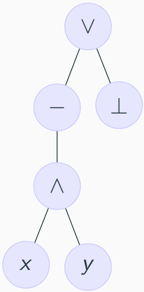
- podterm je podřetězec, který je sám termem
- term bez proměnných je konstantní (ground), např. $((S(0) + S(0)) \cdot S(S(0)))$ v jazyce aritmetiky
- termy nesmí obsahovat prvky struktury, jen symboly z jazyka
- $(1 + 1) \cdot 2$ není term, ledaže rozšíříme jazyk o symboly 1 a 2
- jako lidé můžeme použít infixový zápis, např. $(t_1 + t_2)$ místo $+(t_1, t_2)$, vynechat závorky je-li struktura termu zřejmá

Strom termu

Strom termu t, Tree(t): v listech proměnné nebo konst. symboly, ve vnitřních vrcholech funkční symboly (arita je rovna počtu synů)



(a) $(S(0) + x) \cdot y$ v jazyce aritmetiky



(b) $-(x \wedge y) \vee \perp$ v jazyce Booleových algeber

- symboly $\wedge, \vee$ nejsou logické, ale mimologické ze signatury
- sémantika: proměnné ohodnotíme prvky, konst. a funkční symboly nahradíme interpretacemi, výsledek je prvek z domény

Atomické formule

Termům nelze přiřadit pravdivostní hodnotu, potřebujeme predikát (relační symbol nebo $=$), který mluví o 'vztahu' termů: v dané struktuře při ohodnocení proměnných prvky je buď splněn, nebo ne.

Formule ('tvrzení o strukturách') skládáme z atomických formulí pomocí logických spojek a kvantifikátorů:

Atomická formule jazyka L je nápis $R(t_1, \dots, t_n)$, kde R je n-ární relační symbol z L (včetně $=$ jde-li o jazyk s rovností) a $t_i \in \mathrm{Term}_L$.

- $R(f(f(x)), c, f(d))$ kde R je ternární relační, f unární funkční, c, d konstantní symboly
- infixový zápis $\leq (x, y)$, $= (t_1, t_2)$ píšeme jako $x \leq y$, $t_1 = t_2$
- $(x \cdot x) + (y \cdot y) \leq (x + y) \cdot (x + y)$ v jazyce uspořád. těles
- $x \cdot y \leq (S(0) + x) \cdot y$ v jazyce aritmetiky
- $-(x \wedge y) \vee \bot = \bot$ v jazyce Booleových algeber

Formule

Formule jazyka L jsou konečné nápisy definované induktivně:

- každá atomická formule jazyka L je formule,
- je-li φ formule, potom $(\neg\varphi)$ je také formule
- jsou-li φ, ψ formule, potom $(\varphi \,\square\, \psi)$ pro $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ jsou také formule
- je-li φ formule a x proměnná, potom $((Qx)\varphi)$ pro $Q \in \{\forall, \exists\}$ jsou také formule

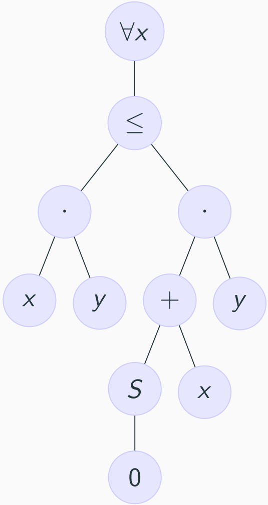
- podformule je podřetězec, který je sám formulí
- při zápisu formulí jako lidé používáme obvyklé konvence
- kvantifikátory mají stejnou prioritu jako $\neg$, vyšší než ostatní logické spojky! místo $((\forall x)\varphi)$ píšeme $(\forall x)\varphi$
- pozor, $(\forall x)\varphi \wedge \psi$ neznamená totéž, co $(\forall x)(\varphi \wedge \psi)$!
- někde uvidíte $\forall x\varphi$ nebo $\forall_x\varphi$, my ale budeme psát jen $(\forall x)\varphi$

Strom formule

Příklad: $(\forall x)(x \cdot y \leq (S(0) + x) \cdot y)$

Strom formule, $\mathrm{Tree}(\varphi)$:

- strom atomické formule $R(t_1, \ldots, t_n)$: v kořeni R, připojíme stromy $\mathrm{Tree}(t_i)$
- pro složené formule podobně jako ve výrokové logice
- kvantifikátory mají jediného syna



Volné a vázané proměnné

Význam formule (pravdivostní hodnota) může/nemusí záviset na proměnných v ní: $x \leq 0$ vs. $(\exists x)(x \leq 0)$ vs. $x \leq 0 \vee (\exists x)(x \leq 0)$

- výskyt x ve φ: list Tree(φ) označený x [v (Qx) nemá výskyt!]
- vázaný: součástí podformule začínající (Qx), jinak volný
- x je volná ve φ má-li volný výskyt, vázaná má-li vázaný výskyt
- zápis $\varphi(x_1, \ldots, x_n)$ znamená, že mezi $x_1, \ldots, x_n$ jsou všechny volné proměnné ve formuli φ

Proměnná může být volná i vázaná, např.:

$$\varphi = (\forall x)(\exists y)(x \leq y) \vee x \leq z$$

- první výskyt x je vázaný a druhý volný (nakreslete si strom!)
- y je vázaná a z je volná, můžeme tedy psát $\varphi(x, z)$

Otevřené a uzavřené formule

otevřená formule: nemá žádný kvantifikátor

uzavřená formule (sentence): nemá žádnou volnou proměnnou

- $x + y \leq 0$ je otevřená formule
- $(\forall x)(\forall y)(x + y \leq 0)$ je uzavřená formule neboli sentence
- $(\forall x)(x + y \leq 0)$ není ani otevřená, ani uzavřená
- $(0 + 1 = 1) \wedge (1 + 1 = 0)$ je otevřená i uzavřená
- atomické formule je otevřená, otevřené formule jsou kombinace atomických pomocí logických spojek
- je-li formule otevřená i uzavřená potom nemá žádné proměnné (všechny termy v ní jsou konstantní)
- formule bez vázané proměnné není nutně otevřená! $(\forall x)0 = 1$

Uvidíme, že pravdivostní hodnota závisí jen na ohodnocení volných proměnných; sentence mají ve struktuře pravdiv. hodnotu 0 nebo 1

Instance a varianty: neformálně

- proměnná může hrát různé 'role' ('lokální' vs. 'globální')
- instance: 'dosazení' do 'globální' proměnné (lépe 'nahrazení' proměnné nějakým termem, který ji počítá, čistě syntaktické!)
- varianta: 'přejmenování' 'lokální' proměnné

$$P(x) \wedge (\forall x)(Q(x) \wedge (\exists x)R(x))$$

- první výskyt x je volný, 2. je vázaný $(\forall x)$, 3. je vázaný $(\exists x)$
- pokud substituujeme za proměnnou x term $t = 1 + 1$, dostáváme instanci formule φ, kterou označíme $\varphi(x/t)$:
$$P(1 + 1) \wedge (\forall x)(Q(x) \wedge (\exists x)R(x))$$
- přejmenujeme-li kvantifikátory, získáme variantu formule φ:
$$P(x) \wedge (\forall y)(Q(y) \wedge (\exists z)R(z))$$

Kdy a jak to lze, aby instance byla důsledek a varianta ekvivalentní?

Instance

Substituujeme-li do φ za x term t, chceme aby výsledná formule 'říkala o t totéž, co φ o x'. Např. $\varphi(x) = (\exists y)(x + y = 1)$

- říká o x, že 'existuje $1 - x$'
- term $t = 1$ lze: $\varphi(x/t) = (\exists y)(1 + y = 1)$ říká 'existuje $1 - 1$'
- term $t = y$ nelze: $(\exists y)(y + y = 1)$ říká '1 je dělitelné 2'
  problém: obsahuje y, po nahrazení bude nově vázané $(\exists y)$

Term t je substituovatelný za proměnnou x ve formuli φ, pokud po simultánním nahrazení všech volných výskytů x za t nevznikne žádný vázaný výskyt proměnné z t. Potom je vzniklá formule instance φ vzniklá substitucí t za x, $\varphi(x/t)$.

- t není substituovatelný za x do φ, právě když x má volný výskyt v nějaké podformuli φ tvaru $(Qy)\psi$ a y se vyskytuje v t
- speciálně: konstantní termy jsou vždy substituovatelné

Varianta

Substituovat t můžeme vždy do varianty φ, ve které přejmenujeme všechny kvantifikované proměnné na nové (které nejsou v t ani φ)

Má-li formule φ podformuli tvaru $(Qx)\psi$ a je-li y proměnná, že

(i) y je substituovatelná za x do ψ, a

(ii) y nemá volný výskyt v ψ.

Varianta φ vznikne nahrazením $(Qx)\psi$ formulí $(Qy)\psi(x/y)$, říkáme tak i výsledku postupné variace ve více podformulích.

Mějme $\varphi = (\exists x)(\forall y)(x \leq y)$:

- $(\exists u)(\forall v)(u \leq v)$ je varianta φ
- $(\exists y)(\forall y)(y \leq y)$ není varianta kvůli (i): y není substituovatelná za x do $\psi = (\forall y)(y \leq y)$
- $(\exists x)(\forall x)(x \leq x)$ není varianta kvůli (ii): x má volný výskyt v $\psi = (x \leq y)$

Šestá přednáška

Program

- sémantika predikátové logiky
- vlastnosti teorií
- podstruktura, expanze, redukt

Materiály

Zápisky z přednášky, Sekce 6.4–6.6 z Kapitoly 6

6.4 Sémantika

Sémantika neformálně

- modely jsou struktury dané signatury,
- formule platí ve struktuře, pokud platí při každém ohodnocení volných proměnných prvky z domény,
- hodnoty termů (jsou to prvky z domény) se vyhodnocují podle jejich stromů, kde symboly nahradíme jejich interpretacemi (funkcemi, a konstantami z domény),
- z hodnot termů získáme pravdivostní hodnoty atomických formulí: je výsledná n-tice v relaci (interpretující daný relační symbol)?
- hodnoty složených formulí vyhodnocujeme také podle jejich stromu, přičemž $(\forall x)$ hraje roli 'konjunkce přes všechny prvky' a $(\exists y)$ hraje roli 'disjunkce přes všechny prvky' z domény struktury

Modely jazyka

Model jazyka L, nebo také L-struktura, je libovolná struktura v signatuře jazyka L. Třídu všech modelů jazyka označíme M_L.

- zda je jazyk s rovností nebo bez nehraje roli
- proč třída a ne množina všech modelů M_L? doména je libovolná neprázdná množina, 'množina všech množin' neexistuje; třída je 'soubor' všech množin splňujících danou vlastnost (popsatelnou v jazyce teorie množin)

Mezi modely jazyka uspořádání $L = \langle \leq \rangle$ patří:

- částečně uspořádané množiny $\langle \mathbb{N}, \leq \rangle$, $\langle \mathbb{Q}, > \rangle$, $\langle \mathcal{P}(X), \subseteq \rangle$
- libovolný orientovaný graf $G = \langle V, E \rangle$, typicky není částečné uspořádání, tj. nesplňuje axiomy teorie uspořádání
- $\langle \mathbb{C}, R^{\mathbb{C}} \rangle$ kde $(z_1, z_2) \in R^{\mathbb{C}}$ právě když $|z_1| = |z_2|$ (není č. usp.)

Hodnota termu

Mějme term t jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a L-strukturu $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, F^{\mathcal{A}} \rangle$.
Ohodnocení proměnných v množině A je lib. funkce $e : \mathrm{Var} \to A$.

Hodnota termu t ve struktuře $\mathcal{A}$ při ohodnocení e, značíme $t^{\mathcal{A}}[e]$, je definovaná induktivně:

- $x^{\mathcal{A}}[e] = e(x)$ pro proměnnou $x \in \mathrm{Var}$,
- $c^{\mathcal{A}}[e] = c^{\mathcal{A}}$ pro konstantní symbol $c \in \mathcal{F}$, a
- je-li $t = f(t_1, \ldots, t_n)$ složený term, kde $f \in \mathcal{F}$, potom:

$$t^{\mathcal{A}}[e] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[e], \ldots, t_n^{\mathcal{A}}[e])$$

- závisí pouze na ohodnocení proměnných vyskytujících se v t
- obecně, term t reprezentuje termovou funkci $f_t^{\mathcal{A}} \colon A^k \to A$, kde k je počet proměnných v t
- speciálně, hodnota konstantního termu na ohodnocení nezávisí, konstantní termy reprezentují konstantní funkce

Hodnota termu: příklady

1. Hodnota termu $t = -(x \vee \bot) \wedge y$ v Booleově algebře $\mathcal{A} = \underline{\mathcal{P}(\{0,1,2\})}$ při ohodnocení e ve kterém:

- $e(x) = \{0,1\}$
- $e(y) = \{1,2\}$

$$t^{\mathcal{A}}[e] = \{2\}$$

2. Hodnota termu $x + 1$ ve struktuře $\mathcal{N} = \langle \mathbb{N}, \cdot, 3 \rangle$ jazyka $L = \langle +, 1 \rangle$ při ohodnocení e ve kterém $e(x) = 2$

$$(x+1)^{\mathcal{N}}[e] = 6$$

Pravdivostní hodnota formule

Buď φ v jazyce L, $\mathcal{A} \in \mathrm{M}_L$, $e : \mathrm{Var} \to A$ ohodnocení proměnných.
Pravdivostní hodnota φ v $\mathcal{A}$ při ohodnocení e, $\mathrm{PH}^{\mathcal{A}}(\varphi)[e]$:

- pro atomickou formuli $R(t_1, \ldots, t_n)$:

$$\mathrm{PH}^{\mathcal{A}}(R(t_1, \ldots, t_n))[e] = \begin{cases} 1 & \text{pokud } (t_1^{\mathcal{A}}[e], \ldots, t_n^{\mathcal{A}}[e]) \in R^{\mathcal{A}} \\ 0 & \text{jinak} \end{cases}$$

- pro formuli tvaru $(\neg\varphi)$:

$$\mathrm{PH}^{\mathcal{A}}(\neg\varphi)[e] = f_{\neg}(\mathrm{PH}^{\mathcal{A}}(\varphi)[e]) = 1 - \mathrm{PH}^{\mathcal{A}}(\varphi)[e]$$

- pro formuli tvaru $(\varphi \,\square\, \psi)$ kde $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$:

$$\mathrm{PH}^{\mathcal{A}}(\varphi \,\square\, \psi)[e] = f_{\square}(\mathrm{PH}^{\mathcal{A}}(\varphi)[e], \mathrm{PH}^{\mathcal{A}}(\psi)[e])$$

Pravdivostní hodnota formule: zbytek definice a poznámky

- pro formuli tvaru $(Qx)\varphi$ kde $Q \in \{\forall, \exists\}$:

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

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

kde $e(x/a)$ je ohodnocení získané z e změnou $e(x)$ na a

Pozorování: Závisí pouze na ohodnocení volných proměnných. Speciálně, pro sentenci nezávisí na ohodnocení.

- tedy v ohodnocení e nastavíme hodnotu proměnné x postupně na všechny prvky $a \in A$ a požadujeme, aby PH byla jedna vždy (v případě $\forall$) nebo alespoň jednou (v případě $\exists$)
- speciálně, $\mathrm{PH}^{\mathcal{A}}(t_1 = t_2)[e] = 1 \Leftrightarrow (t_1^{\mathcal{A}}[e], t_2^{\mathcal{A}}[e]) \in =^{\mathcal{A}}$ (identita na A), tj. $t_1^{\mathcal{A}}[e] = t_2^{\mathcal{A}}[e]$ (je to stejný prvek A)

Příklady

Vezměme si uspořádané těleso $\underline{\mathbb{Q}}$. Potom:

- $\mathrm{PH}^{\underline{\mathbb{Q}}}(x \leq 1 \wedge \neg(x \leq 0))[e] = 1$ právě když $e(x) \in (0, 1]$
- $\mathrm{PH}^{\underline{\mathbb{Q}}}((\forall x)(x \cdot y = y))[e] = 1$ právě když $e(y) = 0$
- $\mathrm{PH}^{\underline{\mathbb{Q}}}((\exists x)(x \leq 0 \wedge \neg x = 0))[e] = 1$ pro každé ohodnocení e (je to sentence)

Ale pro strukturu $\mathcal{A} = \langle \mathbb{N}, +, -, 0, \cdot, 1, \leq \rangle$ máme:

- $\mathrm{PH}^{\mathcal{A}}((\exists x)(x \leq 0 \wedge \neg x = 0))[e] = 0$

Platnost ve struktuře

Mějme formuli φ, strukturu $\mathcal{A}$ (ve stejném jazyce), a ohodnocení e.

- je-li $\mathrm{PH}^{\mathcal{A}}(\varphi)[e] = 1$, φ platí v $\mathcal{A}$ při ohodnocení e, $\mathcal{A} \models \varphi[e]$
- je-li $\mathrm{PH}^{\mathcal{A}}(\varphi)[e] = 0$, φ neplatí v $\mathcal{A}$ při ohodnoc. e, $\mathcal{A} \not\models \varphi[e]$
- φ je pravdivá (platí) v $\mathcal{A}$, $\mathcal{A} \models \varphi$, pokud platí při každém ohodnocení $e : \mathrm{Var} \to A$
- φ je lživá v $\mathcal{A}$, pokud neplatí při žádném ohodnocení (v tom případě $\mathcal{A} \models \neg\varphi$)
- pozor, lživá není totéž, co není pravdivá (neplatí)!
  (je to pravda jen pro sentence)
- platnost je klíčový pojem sémantiky a celé logiky

Zřejmé vlastnosti platnosti ve struktuře při ohodnocení

- $\mathcal{A} \models \neg\varphi[e]$ právě když $\mathcal{A} \not\models \varphi[e]$
- $\mathcal{A} \models (\varphi \wedge \psi)[e]$ právě když $\mathcal{A} \models \varphi[e]$ a $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \vee \psi)[e]$ právě když $\mathcal{A} \models \varphi[e]$ nebo $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \rightarrow \psi)[e]$ právě když platí: jestliže $\mathcal{A} \models \varphi[e]$ potom $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \leftrightarrow \psi)[e]$ právě když platí: $\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\forall x)\varphi[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro každé $a \in A$
- $\mathcal{A} \models (\exists x)\varphi[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro nějaké $a \in A$
- je-li term t substituovatelný za proměnnou x do φ, potom:
  $\mathcal{A} \models \varphi(x/t)[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro $a = t^{\mathcal{A}}[e]$
- je-li ψ varianta φ, potom $\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$

(dokažte si snadno z definic, najděte protipříklady)

Zřejmé vlastnosti platnosti ve struktuře

- pokud $\mathcal{A} \models \varphi$, potom $\mathcal{A} \not\models \neg\varphi$; je-li φ sentence, platí i opačná implikace
- $\mathcal{A} \models \varphi \wedge \psi$ právě když $\mathcal{A} \models \varphi$ a $\mathcal{A} \models \psi$
- pokud $\mathcal{A} \models \varphi$ nebo $\mathcal{A} \models \psi$, potom $\mathcal{A} \models \varphi \vee \psi$; je-li φ sentence, platí i opačná implikace.
- $\mathcal{A} \models \varphi$ právě když $\mathcal{A} \models (\forall x)\varphi$
- speciálně, $\varphi(x_1, \ldots, x_n)$ platí ve struktuře $\mathcal{A}$, právě když v $\mathcal{A}$ platí její generální uzávěr, tj. sentence $(\forall x_1) \cdots (\forall x_n)\varphi$

(dokažte si snadno z definic, najděte protipříklady)

6.5 Vlastnosti teorií

Platnost v teorii

- teorie jazyka L je množina L-formulí, její prvky jsou axiomy
- model teorie T je L-struktura, ve které platí všechny axiomy T, tj. $\mathcal{A} \models \varphi$ pro všechna $\varphi \in T$, značíme $\mathcal{A} \models T$
- třída modelů teorie T je:

$$\mathrm{M}_L(T) = \{\mathcal{A} \in \mathrm{M}_L \mid \mathcal{A} \models T\}$$

Je-li T teorie v jazyce L a φ L-formule, potom φ je:

- pravdivá (platí) v T, značíme $T \models \varphi$, pokud $\mathcal{A} \models \varphi$ pro všechna $\mathcal{A} \in \mathrm{M}(T)$ (neboli: $\mathrm{M}(T) \subseteq \mathrm{M}(\varphi)$)
- lživá v T, pokud $T \models \neg\varphi$, tj. pokud je lživá v každém modelu T (neboli: $\mathrm{M}(T) \cap \mathrm{M}(\varphi) = \emptyset$)
- nezávislá v T, pokud není pravdivá v T ani lživá v T
- je-li $T = \emptyset$ (tj. $\mathrm{M}(T) = \mathrm{M}_L$), píšeme jen $\models \varphi$, a říkáme, že φ je pravdivá (v logice), (logicky) platí, je tautologie, apod.

Další sémantické pojmy o teorii

- T je sporná, pokud v ní platí spor $\perp$ (definujeme jako $R(x_1, \ldots, x_n) \wedge \neg R(x_1, \ldots, x_n)$, kde R je lib. relační symbol)
- T je sporná, právě když v ní platí každá formule (ekvivalentně, nemá žádný model), jinak je bezesporná (neplatí-li v ní spor, má-li alespoň jeden model)
- důsledky T jsou sentence pravdivé v T, množina všech důsledků T v jazyce L je

$$\mathrm{Csq}_L(T) = \{\varphi \mid \varphi \text{ je sentence a } T \models \varphi\}$$

Kompletnost v predikátové logice

- T je kompletní, je-li bezesporná a každá sentence je v ní buď pravdivá, nebo lživá. Pozor: neplatí, že má jediný model!
- máme-li jeden model, máme i nekonečně mnoho izomorfních modelů (liší se jen pojmenováním prvků, definujeme později)
- uvažovat jediný model až na izomorfismus ale také nestačí!

Struktury $\mathcal{A}, \mathcal{B}$ (v témž jazyce) jsou elementárně ekvivalentní, píšeme $\mathcal{A} \equiv \mathcal{B}$, pokud v nich platí tytéž sentence.

Pozorování: Teorie je kompletní, právě když má právě jeden model až na elementární ekvivalenci.

Příklad: uspořádané množiny $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$ a $\mathcal{B} = \langle \mathbb{R}, \leq \rangle$.

- nejsou izomorfní, $\mathbb{Q}$ je spočetná a $\mathbb{R}$ nespočetná množina, neexistuje dokonce žádná bijekce mezi doménami
- ale $\mathcal{A} \equiv \mathcal{B}$: indukcí dle struktury sentence φ lze ukázat $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$; netriviální případ je $\exists$, klíčová je hustota

Platnost pomocí nesplnitelnosti

Otázku platnosti v teorii lze převést na problém existence modelu:

Tvrzení (O nesplnitelnosti a pravdivosti): Je-li T teorie a φ sentence (v témž jazyce), potom: $T \models \varphi \Leftrightarrow T \cup \{\neg\varphi\}$ nemá model.

Důkaz: Platí následující ekvivalence:

- $T \cup \{\neg\varphi\}$ nemá model,
- právě když $\neg\varphi$ neplatí v žádném modelu T,
- právě když φ platí v každém modelu T (φ je sentence!). $\square$

NB: Předpoklad, že φ je sentence, je nutný: pro $T = \{P(c)\}$ a formuli $\varphi = P(x)$ je $P(c) \not\models P(x)$ ale $\{P(c), \neg P(x)\}$ nemá model.

Příklady teorií: Teorie grafů

Teorie grafů: $L = \langle E \rangle$ s rovností, axiomy ireflexivity a symetrie

$$T_{\text{graph}} = \{\neg E(x,x), E(x,y) \to E(y,x)\}$$

Modely: $\mathcal{G} = \langle G, E^{\mathcal{G}} \rangle$, kde $E^{\mathcal{G}}$ je symetrická ireflexivní relace, tj. jednoduché grafy, hranu $\{x,y\}$ reprezentuje dvojice $(x,y), (y,x)$

- Formule $\neg x = y \to E(x,y)$ platí v grafu, právě když je úplný. Je tedy nezávislá v T_{graph}.
- Formule $(\exists y_1)(\exists y_2)(\neg y_1 = y_2 \wedge E(x,y_1) \wedge E(x,y_2) \wedge (\forall z)(E(x,z) \to z = y_1 \vee z = y_2)$ vyjadřuje, že každý vrchol má stupeň právě 2. Platí tedy právě v grafech, které jsou disjunktní sjednocení kružnic, a je nezávislá v teorii T_{graph}.

Příklady teorií: Teorie uspořádání

Teorie uspořádání: v jazyce uspořádání $L = \langle \leq \rangle$ s rovností, axiomy reflexivity, antisymetrie, a tranzitivity

$$T = \{x \leq x,\ x \leq y \wedge y \leq x \rightarrow x = y,\ x \leq y \wedge y \leq z \rightarrow x \leq z\}$$

Modely: $\langle S, \leq^S \rangle$, kde $\leq^S$ je částečné uspořádání.

Příklad: $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$, $\mathcal{B} = \langle \mathcal{P}(X), \subseteq \rangle$ pro $X = \{0, 1, 2\}$.

- Formule $x \leq y \vee y \leq x$ (linearita) platí v $\mathcal{A}$, ale neplatí v $\mathcal{B}$: neplatí např. při ohodnocení kde $e(x) = \{0\}$, $e(y) = \{1\}$ (píšeme $\mathcal{B} \not\models \varphi[e]$). Je tedy nezávislá v T.
- Sentence $(\exists x)(\forall y)(y \leq x)$ (označme ψ) je pravdivá v $\mathcal{B}$ a lživá v $\mathcal{A}$, píšeme $\mathcal{B} \models \psi$, $\mathcal{A} \models \neg\psi$. Je také nezávislá v T.
- Formule $(x \leq y \wedge y \leq z \wedge z \leq x) \rightarrow (x = y \wedge y = z)$ (označme χ) je pravdivá v T, píšeme $T \models \chi$. Totéž platí pro její generální uzávěr $(\forall x)(\forall y)(\forall z)\chi$.

Příklady teorií: Algebraické teorie 1/2

Teorie grup: $L = \langle +, -, 0 \rangle$ s rovností, axiomy asociativita $+$, neutralita 0 vůči $+$, a $-x$ je inverzní prvek k x (vůči $+$ a 0)

$$\begin{aligned} T_1 = \{ & x + (y + z) = (x + y) + z, \\ & 0 + x = x,\ x + 0 = x, \\ & x + (-x) = 0,\ (-x) + x = 0 \} \end{aligned}$$

Teorie komutativních grup: navíc komutativita $+$

$$T_2 = T_1 \cup \{x + y = y + x\}$$

Teorie okruhů: $L = \langle +, -, 0, \cdot, 1 \rangle$ s rovností, navíc neutralita 1 vůči $\cdot$, asociativita $\cdot$, a (levá i pravá) distributivita $\cdot$ vůči $+$

$$\begin{aligned} T_3 = T_2 \cup \{ & 1 \cdot x = x \cdot 1, \\ & x \cdot (y \cdot z) = (x \cdot y) \cdot z, \\ & x \cdot (y + z) = x \cdot y + x \cdot z, \\ & (x + y) \cdot z = x \cdot z + y \cdot z \} \end{aligned}$$

Příklady teorií: Algebraické teorie 2/2

Teorie komutativních okruhů: navíc axiom komutativity $\cdot$:

$$T_4 = T_3 \cup \{x \cdot y = y \cdot x\}$$

Teorie těles je ve stejném jazyce, ale má navíc axiomy existence inverzního prvku k $\cdot$ a netriviality:

$$T_5 = T_4 \cup \{\neg\, x = 0 \rightarrow (\exists y)(x \cdot y = 1),\ \neg\, 0 = 1\}$$

Teorie uspořádaných těles je v jazyce $\langle +, -, 0, \cdot, 1, \leq \rangle$ s rovností, sestává z axiomů teorie těles, teorie uspořádání spolu s axiomem linearity, a z následujících axiomů kompatibility uspořádání:

- $x \leq y \rightarrow (x + z \leq y + z)$
- $(0 \leq x \wedge 0 \leq y) \rightarrow 0 \leq x \cdot y$

Modely jsou tělesa s lineárním (totálním) uspořádáním, které je kompatibilní s tělesovými operacemi.

6.6 Podstruktura, expanze, redukt

Podstruktura

- podstruktura zobecňuje podgrupu, podprostor vektorového prostoru, (indukovaný) podgraf: na podmnožině B univerza vytvoříme strukturu, která "zdědí" relace, funkce a konstanty
- B musí být uzavřená na všechny funkce (vč. konstant)

Struktura $\mathcal{B} = \langle B, \mathcal{R}^{\mathcal{B}}, \mathcal{F}^{\mathcal{B}} \rangle$ je (indukovaná) podstruktura struktury $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ (v též signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$), značíme $\mathcal{B} \subseteq \mathcal{A}$, jestliže:

- $\emptyset \neq B \subseteq A$
- $R^{\mathcal{B}} = R^{\mathcal{A}} \cap B^{\mathrm{ar(R)}}$ pro každý relační symbol $R \in \mathcal{R}$
- $f^{\mathcal{B}} = f^{\mathcal{A}} \cap (B^{\mathrm{ar(f)}} \times B)$ pro každý funkční symbol $f \in \mathcal{F}$, tj. $f^{\mathcal{B}}$ je restrikce $f^{\mathcal{A}}$ na množinu B, a výstupy jsou všechny z B

speciálně, pro konstantní symbol $c \in \mathcal{F}$ máme $c^{\mathcal{B}} = c^{\mathcal{A}} \in B$

Restrikce na podmnožinu, příklady

Množina $C \subseteq A$ je uzavřená na funkci $f : A^n \to A$, pokud $f(x_1, \ldots, x_n) \in C$ pro všechna $x_i \in C$.

Pozorování: Množina $\emptyset \neq C \subseteq A$ je univerzem podstruktury, právě když je uzavřená na všechny funkce struktury $\mathcal{A}$ (včetně konstant). V tom případě je to restrikce $\mathcal{A}$ na množinu C, značíme $\mathcal{A} \restriction C$.

- $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$ je podstrukturou $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$, můžeme psát: $\underline{\mathbb{Z}} = \underline{\mathbb{Q}} \restriction \mathbb{Z}$
- $\underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$ je podstrukturou obou těchto struktur, platí: $\underline{\mathbb{N}} = \underline{\mathbb{Q}} \restriction \mathbb{N} = \underline{\mathbb{Z}} \restriction \mathbb{N}$
- Množina $\{k \in \mathbb{Z} \mid k \leq 0\}$ není univerzem podstruktury $\underline{\mathbb{Z}}$ ani $\underline{\mathbb{Q}}$, není uzavřená na násobení.

Platnost v podstruktuře (pro otevřené formule je zachována)

Pozorování: Je-li $\mathcal{B} \subseteq \mathcal{A}$, φ otevřená formule, a $e \colon \mathrm{Var} \to B$, potom platí: $\mathcal{B} \models \varphi[e]$ právě když $\mathcal{A} \models \varphi[e]$.

Důkaz: Snadno indukcí dle struktury φ, pro atomickou zřejmé. $\square$

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: Modely otevřené teorie jsou uzavřené na podstruktury, tj. každá podstruktura modelu této teorie je také její model.

- Teorie grafů je otevřená. Podstruktura grafu je také graf: (indukovaný) podgraf. Stejně podgrupy, Booleovy podalgebry.
- Teorie těles není otevřená. Později ukážeme, že ani otevřeně axiomatizovatelná (kvantifikátoru v axiomu o existenci inverzního prvku se nezbavíme). Podstruktura tělesa $\mathbb{Q}$ na množině $\mathbb{Z}$, $\mathbb{Q} \restriction \mathbb{Z}$, není těleso. (Je to tzv. okruh.)

Generovaná podstruktura (zobecníme lineární obal vektorů)

Co když podmnožina univerza není uzavřená? Vezmeme její uzávěr.

Mějme $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ a $\emptyset \neq X \subseteq A$. Buď $B \subseteq A$ nejmenší podmnožina, která obsahuje X a je uzavřená na všechny funkce $\mathcal{A}$ (tj. obsahuje i všechny konstanty). Potom podstruktura $\mathcal{A} \restriction B$ je generovaná X, značíme ji $\mathcal{A}\langle X \rangle$.

Např. pro $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$, $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, \cdot, 0 \rangle$, $\underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$:

- $\underline{\mathbb{Q}}\langle \{1\} \rangle = \underline{\mathbb{N}}$
- $\underline{\mathbb{Q}}\langle \{-1\} \rangle = \underline{\mathbb{Z}}$
- $\underline{\mathbb{Q}}\langle \{2\} \rangle$ je podstruktura $\underline{\mathbb{N}}$ na množině všech sudých čísel

Pokud $\mathcal{A}$ nemá žádné funkce (ani konstanty), např. graf či uspořádání, potom není čím generovat, a $\mathcal{A}\langle X \rangle = \mathcal{A} \restriction X$.

Expanze a redukt

Mějme $L \subseteq L'$, L-strukturu $\mathcal{A}$ a L'-strukturu $\mathcal{A}'$ na stejné doméně. Je-li interpretace každého symbolu z L stejná v $\mathcal{A}$ i v $\mathcal{A}'$, potom:

- $\mathcal{A}'$ je expanze $\mathcal{A}$ do L' (L'-expanze struktury $\mathcal{A}$)
- $\mathcal{A}$ je redukt $\mathcal{A}'$ na L (L-redukt struktury $\mathcal{A}'$)

Například:

- Mějme grupu celých čísel $\langle \mathbb{Z}, +, -, 0 \rangle$. Potom:
  - struktura $\langle \mathbb{Z}, + \rangle$ je její redukt
  - struktura $\langle \mathbb{Z}, +, -, 0, \cdot, 1 \rangle$ (okruh celých čísel) je její expanze
- Mějme graf $\mathcal{G} = \langle G, E^{\mathcal{G}} \rangle$. Potom expanze $\mathcal{G}$ o jména prvků (z množiny G) je struktura $\langle G, E^{G}, c_v^{\mathcal{G}} \rangle_{v \in G}$ v jazyce $\langle E, c_v \rangle_{v \in G}$, kde $c_v^{\mathcal{G}} = v$ pro všechny vrcholy $v \in G$.

Věta o konstantách

- splnit formuli s volnou proměnnou x je totéž, co splnit formuli, ve které je x nahrazena novým konstantním symbolem c
- proč: nový symbol lze v modelu interpretovat každým prvkem
- podobný trik využijeme v tablo metodě

Věta (O konstantách): Mějme L-formuli φ s volnými proměnnými $x_1, \ldots, x_n$. Označme jako L' rozšíření L o nové konstantní symboly $c_1, \ldots, c_n$ a buď T' stejná teorie jako T, ale v jazyce L'. Potom:

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

Důkaz: stačí ukázat pro jednu volnou proměnnou, rozšířit indukcí

$\Rightarrow$ **Víme:** φ platí v každém modelu T. **Chceme:** $\varphi(x/c)$ platí v každém modelu T'. Mějme model $\mathcal{A}' \models T'$ a ohodnocení $e\colon \mathrm{Var} \to A'$ a ukažme, že $\mathcal{A}' \models \varphi(x/c)[e]$.

Pokračování důkazu

Buď $\mathcal{A}$ redukt $\mathcal{A}'$ na L ('zapomeneme' konstantu $c^{\mathcal{A}'}$). Všimněte si, že $\mathcal{A}$ je model T (axiomy $T = T'$ neobsahují nový symbol c). Dle předpokladu $\mathcal{A} \models \varphi$, tj. $\mathcal{A} \models \varphi[e']$ pro libovolné ohodnocení e', speciálně pro $e(x/c^{\mathcal{A}'})$ kde x ohodnotíme interpretací c v $\mathcal{A}'$.

Máme $\mathcal{A} \models \varphi[e(x/c^{\mathcal{A}'})]$, což ale znamená $\mathcal{A}' \models \varphi(x/c)[e]$.

$\Leftarrow$ **Víme:** $\varphi(x/c)$ platí v každém modelu T'. **Chceme:** φ platí v každém modelu T. Zvolme $\mathcal{A} \models T$ a ohodnocení $e\colon \mathrm{Var} \to A$ a ukažme, že $\mathcal{A} \models \varphi[e]$.

Buď $\mathcal{A}'$ expanze $\mathcal{A}$ do L', kde c interpretujeme jako $c^{\mathcal{A}'} = e(x)$. Dle předpokladu platí $\mathcal{A}' \models \varphi(x/c)[e']$ pro všechna ohodnocení e'. Tedy $\mathcal{A}' \models \varphi(x/c)[e]$, což znamená $\mathcal{A}' \models \varphi[e]$ ($e = e(x/c^{\mathcal{A}'})$), z toho plyne $\mathcal{A}' \models \varphi(x/c)[e] \Leftrightarrow \mathcal{A}' \models \varphi[e(x/c^{\mathcal{A}'})] \Leftrightarrow \mathcal{A}' \models \varphi[e]$).

Formule φ neobsahuje c (je nový), máme tedy i $\mathcal{A} \models \varphi[e]$. $\square$

Sedmá přednáška

Program

- extenze teorií, extenze o definice
- definovatelnost a databázové dotazy
- vztah výrokové a predikátové logiky
- tablo metoda v predikátové logice, jazyky s rovností

Materiály

Zápisky z přednášky, Sekce 6.7-6.9 z Kapitoly 6, Sekce 7.1-7.3 z Kapitoly 7

6.7 Extenze teorií

Extenze teorie

Stejně jako ve výrokové logice, je-li T teorie v jazyce L:

- extenze: T' v jazyce $L' \supseteq L$ splňující $\mathrm{Csq}_L(T) \subseteq \mathrm{Csq}_{L'}(T')$
- jednoduchá: $L' = L$
- konzervativní: $\mathrm{Csq}_L(T) = \mathrm{Csq}_L(T') = \mathrm{Csq}_{L'}(T') \cap \mathrm{Fm}_L$
- ekvivalentní: T' extenzí T a T extenzí T' (obě v témž jazyce)

Jsou-li T, T' ve stejném jazyce L:

- T' je extenze T, právě když $\mathrm{M}_L(T') \subseteq \mathrm{M}_L(T)$
- T' je ekvivalentní s T, právě když $\mathrm{M}_L(T') = \mathrm{M}_L(T)$

Zvětšíme-li jazyk:

- ve výrokové logice: přidáváme/zapomínáme hodnoty pro nové prvovýroky
- v predikátové logice: expandujeme/redukujeme modely (přidáváme/zapomínáme nové relace, funkce, konstanty)

Extenze teorie: sémantický popis

Mějme jazyky $L \subseteq L'$, L-teorii T a L'-teorii T':

(i) T' je extenzí T $\Leftrightarrow$ L-redukt každého modelu T' je model T

(ii) T' je konzervativní extenzí T $\Leftrightarrow$ T' je extenzí T, a každý model T lze expandovat do L' na nějaký model T'

Poznámka: Důkaz (ii) $\Longrightarrow$ vynecháme (technický problém: model, který nelze expandovat $\rightsquigarrow$ L-sentence platná v T ale ne v T')

Důkaz:(i) $\Longrightarrow$ Buď $\mathcal{A}'$ model T', $\mathcal{A}$ jeho L-redukt. Protože T' je extenzí, platí v ní, tedy i v $\mathcal{A}'$, každý axiom $\varphi \in T$. Ten ale obsahuje jen symboly z L, tedy platí i v $\mathcal{A}$.

(i) $\Longleftarrow$ **Mějme:** L-sentenci φ, $T \models \varphi$. **Chceme:** $T' \models \varphi$. Pro lib. model $\mathcal{A}' \in \mathrm{M}_{L'}(T')$ víme, že jeho L-redukt $\mathcal{A}$ je modelem T, tedy $\mathcal{A} \models \varphi$. Z toho plyne i $\mathcal{A}' \models \varphi$ (opět φ je v L).

(ii) $\Longleftarrow$ **Mějme:** L-sentenci φ, $T' \models \varphi$. **Chceme:** $T \models \varphi$. Každý $\mathcal{A} \in \mathrm{M}_L(T)$ lze expandovat na nějaký $\mathcal{A}' \in \mathrm{M}_{L'}(T')$. Víme, že $\mathcal{A}' \models \varphi$, takže i $\mathcal{A} \models \varphi$. Tím jsme dokázali $T \models \varphi$. $\square$

Extenze o definice (neformálně)

- přidáme nový symbol, jehož význam je jednoznačně daný definující formulí (jako procedura/funkce v programování)
- pro relační symboly jednoduché, pro funkční symboly musíme navíc zaručit existenci a jednoznačnost funkční hodnoty

Ukážeme:

- je to konzervativní extenze, dokonce každý model původní teorie lze jednoznačně expandovat na model nové teorie
- každou formuli používající nové symboly lze přepsat na formuli v původním jazyce (tak, že jsou v extenzi ekvivalentní)

Definice relačního symbolu

nový n-ární relační symbol R lze definovat lib. formulí $\psi(x_1, \ldots, x_n)$

- teorii v jazyce s rovností lze rozšířit o symbol $\neq$ definovaný formulí $\neg x_1 = x_2$; tj. požadujeme, aby: $x_1 \neq x_2 \leftrightarrow \neg x_1 = x_2$
- teorii uspořádání lze rozšířit o $<$ definovaný formulí $x_1 \leq x_2 \wedge \neg x_1 = x_2$; tj. platí: $x_1 < x_2 \leftrightarrow x_1 \leq x_2 \wedge \neg x_1 = x_2$
- v aritmetice lze zavést $\leq$ takto: $x_1 \leq x_2 \leftrightarrow (\exists y)(x_1 + y = x_2)$
- v uspořádaném stromu lze zavést unární predikát $\mathrm{Leaf}(x)$: $\mathrm{Leaf}(x) \leftrightarrow \neg(\exists y)(x <_T y)$

Mějme teorii T a formuli $\psi(x_1, \ldots, x_n)$ v jazyce L. Označme jako L' rozšíření jazyka L o nový n-ární relační symbol R. Extenze teorie T o definici R formulí ψ je L'-teorie:

$$T' = T \cup \{R(x_1, \ldots, x_n) \ \leftrightarrow \ \psi(x_1, \ldots, x_n)\}$$

Definice relačního symbolu: vlastnosti

Tvrzení:

(i) T' je konzervativní extenze T.

(ii) Pro každou L'-formuli φ' existuje L-formule φ taková, že $T' \models \varphi' \leftrightarrow \varphi$.

Důkaz: (i) ihned ze sémantického popisu extenzí, neboť zřejmě každý model T lze jednoznačně expandovat na model T'

(ii) atomickou podformuli s novým symbolem R, tj. tvaru $R(t_1, \ldots, t_n)$, nahradíme formulí

$$\psi'(x_1/t_1, \ldots, x_n/t_n)$$

kde ψ' je varianta ψ zaručující substituovatelnost všech termů (např. přejmenujeme všechny vázané proměnné ψ na zcela nové) $\square$

Definice funkčního symbolu: příklady

vztah $f(x_1, \ldots, x_n) = y$ definujeme formulí $\psi(x_1, \ldots, x_n, y)$; pro každý vstup $(x_1, \ldots, x_n)$ musí existovat jednoznačný výstup y

1. Teorie grup: binární funkční symbol $-_b$ pomocí $+$ a unárního $-$

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

- zřejmě pro každá x, y existuje jednoznačné z splňující definici

2. Teorie lineárních uspořádání: binární funkční symbol min

$$\min(x_1, x_2) = y \leftrightarrow y \leq x_1 \wedge y \leq x_2 \wedge (\forall z)(z \leq x_1 \wedge z \leq x_2 \rightarrow z \leq y)$$

- existence a jednoznačnost platí díky linearitě $(x \leq y \vee y \leq x)$
- pouze v teorii uspořádání by nešlo o dobrou definici: $\min^{\mathcal{A}}(a_1, a_2)$ nemusí existovat

Definice funkčního symbolu: definice

Mějme teorii T a formuli $\psi(x_1, \ldots, x_n, y)$ v jazyce L. Označme L' rozšíření L o nový n-ární funkční symbol f. Nechť platí:

- $T \models (\exists y)\psi(x_1, \ldots, x_n, y)$ (existence)
- $T \models \psi(x_1, \ldots, x_n, y) \wedge \psi(x_1, \ldots, x_n, z) \rightarrow y = z$ (jednoznačnost)

Potom extenze teorie T o definici f formulí ψ je L'-teorie:

$$T' = T \cup \{f(x_1, \ldots, x_n) = y \ \leftrightarrow \ \psi(x_1, \ldots, x_n, y)\}$$

- ψ definuje v modelu $(n+1)$-ární relaci, ta musí být funkcí
- je-li ψ tvaru $t(x_1, \ldots, x_n) = y$ pro term t, vždy to platí

Tvrzení:

(i) T' je konzervativní extenze T.

(ii) Pro každou L'-formuli φ' existuje L-formule φ taková, že $T' \models \varphi' \leftrightarrow \varphi$.

Důkaz: (i) modely T lze jednoznačně expandovat na modely T'

Pokračování důkazu

(ii) stačí pro jediný výskyt symbolu f, jinak induktivně (je-li více vnořených výskytů $f(\dots f(\dots)\dots)$, potom od vnitřních k vnějším)

1. nahradíme term $f(t_1, \dots, t_n)$ novou proměnnou z: výsledek φ^*
2. φ zkonstruujeme takto: $(\exists z)(\varphi^* \wedge \psi'(x_1/t_1, \dots, x_n/t_n, y/z))$
   (kde ψ' je varianta ψ zaručující substituovatelnost)

Ukážeme, že pro libovolný model $\mathcal{A} \models T'$ a ohodnocení e platí:

$$\mathcal{A} \models \varphi'[e] \text{ právě když } \mathcal{A} \models \varphi[e]$$

Označme $a = (f(t_1, \dots, t_n))^{\mathcal{A}}[e]$. Díky existenci a jednoznačnosti:

$$\mathcal{A} \models \psi'(x_1/t_1, \dots, x_n/t_n, y/z)[e] \text{ právě když } e(z) = a$$

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

Definice konstantního symbolu

- speciální případ: funkční symbol arity 0
- extenze o definici konstantního symbolu c formulí $\psi(y)$:

$$T' = T \cup \{c = y \leftrightarrow \psi(y)\}$$

- musí platit $T \models (\exists y)\psi(y)$ a $T \models \psi(y) \wedge \psi(z) \rightarrow y = z$
- platí stejná tvrzení

1. teorie v jazyce aritmetiky, rozšíříme o definici symbolu 1 formulí $\psi(y)$ tvaru $y = S(0)$, přidáme tedy axiom $1 = y \ \leftrightarrow \ y = S(0)$

2. teorie těles, nový symbol $\frac{1}{2}$, definice formulí $y \cdot (1+1) = 1$, tj. přidáním $\frac{1}{2} = y \ \leftrightarrow \ y \cdot (1+1) = 1$?

- není extenze o definici! neplatí existence: v tělese charakteristiky 2, např. $\mathbb{Z}_2$, nemá rovnice $y \cdot (1+1) = 1$ řešení
- ale v teorii těles charakteristiky různé od 2, tj. přidáme-li axiom $\neg(1+1=0)$, už ano; např. v $\mathbb{Z}_3$ máme $\frac{1}{2}^{\mathbb{Z}_3} = 2$

Extenze o definice

L'-teorie T' je extenzí L-teorie T o definice, pokud vznikla postupnou extenzí o definice relačních a funkčních (vč. konstantních) symbolů.

Tvrzení: (snadno indukcí)

- Každý model T lze jednoznačně expandovat na model T'.
- T' je konzervativní extenze T.
- Pro L'-formuli φ' existuje L-formule φ, že $T' \models \varphi' \leftrightarrow \varphi$.

Příklad: $T = \{(\exists y)(x + y = 0), (x + y = 0) \wedge (x + z = 0) \rightarrow y = z\}$

$L = \langle +, 0, \leq \rangle$ s rovností, zavedeme $<$ a unární $-$ přidáním axiomů:

$$\begin{aligned} T' = T \cup \{-x = y \ &\leftrightarrow \ x + y = 0, \\ x < y \ &\leftrightarrow \ x \leq y \wedge \neg(x = y)\} \end{aligned}$$

Formule $-x < y$ v jazyce $L' = \langle +, -, 0, \leq, < \rangle$ s rovností je v T' ekvivalentní formuli: $(\exists z)((z \leq y \wedge \neg(z = y)) \wedge x + z = 0)$

6.8 Definovatelnost ve struktuře

Definovatelné množiny

- formule φ s jednou volnou proměnnou x ... "vlastnost" prvků
- ve struktuře definuje množinu prvků, které vlastnost splňují (tj. prvků a takových, že φ platí při ohodnocení kde $e(x) = a$)
- $\varphi(x, y)$ definuje binární relaci, atp.

Množina definovaná $\varphi(x_1, \ldots, x_n)$ ve struktuře $\mathcal{A}$ (v témž jazyce):

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

Zkráceně píšeme: $\varphi^{\mathcal{A}}(\bar{x}) = \{\bar{a} \in A^n \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a})]\}$

- formule $\neg(\exists y)E(x, y)$ definuje v daném grafu množinu všech izolovaných vrcholů
- $(\exists y)(y \cdot y = x) \wedge \neg(x = 0)$ definuje v tělese $\mathbb{R}$ množinu všech kladných reálných čísel
- $x \leq y \wedge \neg(x = y)$ definuje v uspořádané množině $\langle S, \leq^S \rangle$ relaci ostrého uspořádání $<^S$

Definovatelnost s parametry

- vlastnosti prvků relativně k jiným prvkům? nelze čistě syntakticky, ale můžeme dosadit prvky jako parametry
- zápis $\varphi(\bar{x},\bar{y})$: volné proměnné $x_1,\dots,x_n,y_1,\dots,y_k$

Mějme $\varphi(\bar{x},\bar{y})$ (kde $|\bar{x}|=n$, $|\bar{y}|=k$), strukturu $\mathcal{A}$ (v témž jazyce), $\bar{b}\in A^k$. Množina definovaná $\varphi(\bar{x},\bar{y})$ s parametry $\bar{b}$ ve struktuře $\mathcal{A}$:

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

Pro $B\subseteq A$ označíme $\mathrm{Df}^n(\mathcal{A},B)$ množinu všech množin definovatelných v $\mathcal{A}$ s parametry pocházejícími z B.

Pozorování: $\mathrm{Df}^n(\mathcal{A},B)$ je uzavřená na doplněk, průnik, sjednocení, a obsahuje $\emptyset$ a A^n: je to podalgebra potenční algebry $\mathcal{P}(A^n)$.

Např. pro $\varphi(x,y)=E(x,y)$ a vrchol $v\in V(\mathcal{G})$ je $\varphi^{\mathcal{G},v}(x,y)$ množina všech sousedů vrcholu v.

Aplikace: databázové dotazy

- relační databáze: jedna nebo více tabulek, také relace
- řádky tabulky jsou záznamy (records), také tice (tuples)
- struktura v čistě relačním jazyce

Movies

title	director	actor
Forrest Gump	R. Zemeckis	T. Hanks
Philadelphia	J. Demme	T. Hanks
Batman Returns	T. Burton	M. Keaton
⋮	⋮	⋮

Program

cinema	title	time
Atlas	Forrest Gump	20:00
Lucerna	Forrest Gump	21:00
Lucerna	Philadelphia	18:30
⋮	⋮	⋮

Příklad SQL dotazu

- SQL dotaz v nejjednodušší formě je formule (pomineme např. agregační funkce)
- výsledek je množina definovaná touto formulí (s parametry)

"Kdy a kde můžeme vidět film s Tomem Hanksem?"

```
select Program.cinema, Program.time from Program, Movies where
Program.title = Movies.title and Movies.actor = 'T. Hanks'
```

- výsledek je množina $\varphi^{\text{Database},\text{'T. Hanks'}}(x_{\text{cinema}}, x_{\text{time}}, y_{\text{actor}})$
- definovaná ve struktuře $\text{Database} = \langle D, \text{Program}, \text{Movies}\rangle$
- jejíž doména je $D = \{\texttt{'Atlas'}, \texttt{'Lucerna'}, \ldots, \texttt{'M. Keaton'}\}$
- s parametrem `'T. Hanks'`,
- definující formule $\varphi(x_{\text{cinema}}, x_{\text{time}}, y_{\text{actor}})$:

$$(\exists z_{\text{title}})(\exists z_{\text{director}})(\text{Program}(x_{\text{cinema}}, z_{\text{title}}, x_{\text{time}}) \wedge \text{Movies}(z_{\text{title}}, z_{\text{director}}, y_{\text{actor}}))$$

6.9 Vztah výrokové a predikátové logiky

Teorie Booleových algeber $L = \langle -, \wedge, \vee, \perp, \top \rangle$ s rovností

- asociativita $\wedge$ a $\vee$:
$$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$
$$x \vee (y \vee z) = (x \vee y) \vee z$$
- komutativita $\wedge$ a $\vee$:
$$x \wedge y = y \wedge x$$
$$x \vee y = y \vee x$$
- distributivita $\wedge$ vůči $\vee$, $\vee$ vůči $\wedge$:
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$
- absorpce:
$$x \wedge (x \vee y) = x$$
$$x \vee (x \wedge y) = x$$
- komplementace:
$$x \wedge (-x) = \perp$$
$$x \vee (-x) = \top$$
- netrivialita:
$$-(\perp = \top)$$

- dualita: záměnou $\wedge$ s $\vee$ a $\perp$ s $\top$ získáme tytéž axiomy
- nejmenší model: 2-prvková B. algebra $\langle \{0,1\}, f_\neg, f_\wedge, f_\vee, 0, 1 \rangle$
- konečné modely, až na izomorfismus (f^n je f po složkách):
$$\langle \{0,1\}^n, f_\neg^n, f_\wedge^n, f_\vee^n, (0,\ldots,0), (1,\ldots,1) \rangle$$
- jsou izomorfní potenčním algebrám $\mathcal{P}(\{1,\ldots,n\})$ pomocí bijekce mezi podmnožinami a charakteristickými vektory

Vztah výrokové a predikátové logiky

- výrokovou logiku lze ‘simulovat’ v predikátové logice v teorii Booleových algeber
- výroky jsou Booleovské termy, konstanty $\perp, \top$ představují pravdu a lež
- pravdivostní hodnota výroku (při daném pravdivostním ohodnocení) je hodnota termu v 2-prvkové Booleově algebře
- kromě toho, algebra výroků daného výrokového jazyka nebo teorie je Booleovou algebrou (i pro nekonečné jazyky)

Na druhou stranu...

- máme-li otevřenou formuli φ (bez rovnosti), můžeme reprezentovat atomické formule pomocí prvovýroků, a získat tak výrok, který platí, právě když platí φ
- viz Kapitola 8: Rezoluce v predikátové logice, kde se nejprve zbavíme kvantifikátorů pomocí tzv. Skolemizace
- výrokovou logiku lze také zavést jako fragment logiky predikátové, pokud povolíme nulární relace
- $A^0 = \{\emptyset\}$, tedy na libovolné množině jsou právě dvě nulární relace $R^A \subseteq A^0$: $R^A = \emptyset = 0$ a $R^A = \{\emptyset\} = \{0\} = 1$

Kapitola 7: Tablo metoda v predikátové logice

7.1 Neformální úvod

Úvodní příklady: dva tablo důkazy

$$
\begin{array}{c}
\mathrm{F}(\exists x)\neg P(x) \to \neg(\forall x)P(x) \\
| \\
\mathrm{T}(\exists x)\neg P(x) \\
| \\
\mathrm{F}\neg(\forall x)P(x) \\
| \\
\mathrm{T}(\forall x)P(x) \\
| \\
\mathrm{T}\neg P(c_0) \\
| \\
\mathrm{F}P(c_0) \\
| \\
\mathrm{T}(\forall x)P(x) \\
| \\
\mathrm{T}P(c_0) \\
\otimes
\end{array}
\qquad
\begin{array}{c}
\mathrm{F}\neg(\forall x)P(x) \to (\exists x)\neg P(x) \\
| \\
\mathrm{T}\neg(\forall x)P(x) \\
| \\
\mathrm{F}(\exists x)\neg P(x) \\
| \\
\mathrm{F}(\forall x)P(x) \\
| \\
\mathrm{F}P(c_0) \\
| \\
\mathrm{F}(\exists x)\neg P(x) \\
| \\
\mathrm{F}\neg P(c_0) \\
| \\
\mathrm{T}P(c_0) \\
\otimes
\end{array}
$$

Tablo metoda v predikátové logice

- opět vždy předpokládáme, že jazyk L je spočetný (nejprve bez rovnosti, později metodu rozšíříme pro rovnost)
- v položkách musí být sentence: pravdivostní hodnota nesmí záviset na ohodnocení (ale můžeme vzít generální uzávěry)
- redukce položek: stejná atomická tabla pro logické spojky (kde φ, ψ jsou sentence), ale čtyři nové případy pro kvantifikátory:
  - typ "svědek": položky tvaru $\mathrm{T}(\exists x)\varphi(x)$ a $\mathrm{F}(\forall x)\varphi(x)$
  - typ "všichni": položky tvaru $\mathrm{T}(\forall x)\varphi(x)$ a $\mathrm{F}(\exists x)\varphi(x)$
- kvantifikátor nelze odstranit, $\varphi(x)$ by typicky nebyla sentence
- místo toho za x substituujeme konstantní term t: $\varphi(x/t)$
- jaký? podle typu položky ("svědek" vs. "všichni")

Redukce položek s kvantifikátorem

- jazyk L rozšíříme o spočetně mnoho nových (pomocných) konstantních symbolů $C = \{c_0, c_1, c_2, \dots\}$, označíme L_C
- vždy máme k dispozici nový, dosud nepoužitý symbol $c \in C$
- **typ "svědek":** dosadíme nový $c \in C$ (dosud na větvi není)
  - pro $\mathrm{T}(\exists x)\varphi(x)$ tedy máme $\mathrm{T}\varphi(x/c)$
  - c hraje roli prvku, který položku 'splňuje'
- **typ "všichni":** substituujeme libovolný konstantní L_C-term
  - pro $\mathrm{T}(\forall x)\varphi(x)$ tedy máme $\mathrm{T}\varphi(x/t)$
  - bezesporná větev je dokončená jen pokud dosadíme všechny t ('použijeme vše, co víme')
- **konvence:** kořeny atomických tabel nekreslíme kromě položek typu "všichni" (po jednom dosazení ještě nejsme hotovi!)
- **typický postup:** nejprve zredukujeme položky typu "svědek", poté zjistíme, co 'o svědcích říkají' položky typu "všichni"

7.2 Formální definice

Jazyk, položky, atomická tabla

- buď L spočetný jazyk bez rovnosti.
- označme L_C rozšíření L o spočetně mnoho nových pomocných konstantních symbolů $C = \{c_i \mid i \in \mathbb{N}\}$
- zvolme očíslování konstantních L_C-termů: $\{t_i \mid i \in \mathbb{N}\}$
- mějme nějakou L-teorii T a L-sentenci φ
- položka je nápis $\mathrm{T}\varphi$ nebo $\mathrm{F}\varphi$, kde φ je L_C-sentence
- položky tvaru $\mathrm{T}(\exists x)\varphi(x)$ a $\mathrm{F}(\forall x)\varphi(x)$ jsou typu "svědek"
- položky tvaru $\mathrm{T}(\forall x)\varphi(x)$ a $\mathrm{F}(\exists x)\varphi(x)$ jsou typu "všichni"
- atomická tabla jsou násl. položkami označkované stromy:

Atomická tabla pro kvantifikátory

φ je libovolná L_C-sentence, x proměnná, t_i konstantní L_C-term, $c_i \in C$ je nový pomocný konstantní symbol (při konstrukci tabla nesměl dosud být na dané větvi)

	$\forall$	$\exists$
True	$\mathrm{T}(\forall x)\varphi(x)$ $\vert$ $\mathrm{T}\varphi(x/t_i)$	$\mathrm{T}(\exists x)\varphi(x)$ $\vert$ $\mathrm{T}\varphi(x/c_i)$
False	$\mathrm{F}(\forall x)\varphi(x)$ $\vert$ $\mathrm{F}\varphi(x/c_i)$	$\mathrm{F}(\exists x)\varphi(x)$ $\vert$ $\mathrm{F}\varphi(x/t_i)$

Atomická tabla pro logické spojky

φ a ψ jsou libovolné L_C-sentence

	$\neg$	$\wedge$	$\vee$	$\to$	$\leftrightarrow$
True	$\begin{array}{c} \mathrm{T}\neg\varphi \\ \mid \\ \mathrm{F}\varphi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi\wedge\psi \\ \mid \\ \mathrm{T}\varphi \\ \mid \\ \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi\vee\psi \\ / \quad \backslash \\ \mathrm{T}\varphi \quad \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi\to\psi \\ / \quad \backslash \\ \mathrm{F}\varphi \quad \mathrm{T}\psi \end{array}$	$\begin{array}{c} \mathrm{T}\varphi\leftrightarrow\psi \\ / \quad \backslash \\ \mathrm{T}\varphi \quad \mathrm{F}\varphi \\ \mid \quad\quad \mid \\ \mathrm{T}\psi \quad \mathrm{F}\psi \end{array}$
False	$\begin{array}{c} \mathrm{F}\neg\varphi \\ \mid \\ \mathrm{T}\varphi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi\wedge\psi \\ / \quad \backslash \\ \mathrm{F}\varphi \quad \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi\vee\psi \\ \mid \\ \mathrm{F}\varphi \\ \mid \\ \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi\to\psi \\ \mid \\ \mathrm{T}\varphi \\ \mid \\ \mathrm{F}\psi \end{array}$	$\begin{array}{c} \mathrm{F}\varphi\leftrightarrow\psi \\ / \quad \backslash \\ \mathrm{T}\varphi \quad \mathrm{F}\varphi \\ \mid \quad\quad \mid \\ \mathrm{F}\psi \quad \mathrm{T}\psi \end{array}$

Formální definice tabla

- konečné tablo z teorie T je uspoř., položkami označ. strom zkonstruovaný aplikací konečně mnoha následujících pravidel:
  - jednoprvkový strom s libovolnou položkou je tablo z teorie T
  - pro libovolnou položku P na libovolné větvi V můžeme na konec větve V připojit atomické tablo pro položku P
    je-li P typu "svědek", můžeme použít jen $c_i \in C$, který dosud na V není (pro typ "všichni" lze použít lib. konst. L_C-term t_i)
  - na konec libovolné větve můžeme připojit položku $\mathrm{T}\alpha$ pro libovolný axiom $\alpha \in T$
- tablo z teorie T je buď konečné, nebo i nekonečné: v tom případě je spočetné a definujeme ho jako $\tau = \bigcup_{i \geq 0} \tau_i$, kde:
  - τ_i jsou konečná tabla z T
  - τ_0 je jednoprvkové tablo
  - τ_{i+1} vzniklo z τ_i v jednom kroku
- tablo pro položku P je tablo, které má položku P v kořeni

konvence: kořen atom. tabla nezapisujeme není-li P typu "všichni"

Dokončené a sporné tablo

- Tablo je sporné, pokud je každá jeho větev sporná.
- Větev je sporná, pokud obsahuje položky $\mathrm{T}\psi$ a $\mathrm{F}\psi$ pro nějakou sentenci ψ, jinak je bezesporná.
- Tablo je dokončené, pokud je každá jeho větev dokončená.
- Větev je dokončená, pokud je sporná, nebo
  - každá její položka je na této větvi redukovaná,
  - a zároveň obsahuje položku $\mathrm{T}\alpha$ pro každý axiom $\alpha \in T$.
- Položka P je redukovaná na větvi V procházející P, pokud
  - je tvaru $\mathrm{T}\psi$ resp. $\mathrm{F}\psi$ pro atomickou sentenci, nebo
  - není typu "všichni" a vyskytuje se na V jako kořen atomického tabla (tj., typicky, již došlo k jejímu rozvoji na V), nebo
  - je typu "všichni" a všechny její výskyty na větvi V jsou na V redukované.

Kdy je výskyt položky typu "všichni" redukovaný?

Výskyt položky P typu "všichni" na V je i-tý, má-li právě $i-1$ předků označených P, a i-tý výskyt je redukovaný na V, pokud

- P má $(i+1)$-ní výskyt na V, a zároveň
- na V je položka $\mathrm{T}\varphi(x/t_i)$ (je-li $P = \mathrm{T}(\forall x)\varphi(x)$) resp. $\mathrm{F}\varphi(x/t_i)$ (je-li $P = \mathrm{F}(\exists x)\varphi(x)$), kde t_i je i-tý konstantní L_C-term (tj., typicky, už jsme za x substituovali t_i)

NB: je-li položka typu "všichni" na V redukovaná, má na V nekonečně výskytů, a dosadili jsme všechny konstantní L_C-termy

Tablo důkaz a tablo zamítnutí

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

Příklad: tablo důkaz (v logice)

$$\mathrm{F}(\forall x)(P(x) \to Q(x)) \to ((\forall x)P(x) \to (\forall x)Q(x))$$

$$\mathrm{T}(\forall x)(P(x) \to Q(x))$$

$$\mathrm{F}(\forall x)P(x) \to (\forall x)Q(x)$$

$$\mathrm{T}(\forall x)P(x)$$

$$\mathrm{F}(\forall x)Q(x)$$

$$\mathrm{F}Q(c_0)$$

$$\mathrm{T}(\forall x)P(x)$$

$$\mathrm{T}P(c_0)$$

$$\mathrm{T}(\forall x)(P(x) \to Q(x))$$

$$\mathrm{T}P(c_0) \to Q(c_0)$$

$$\begin{array}{cc} \diagup & \diagdown \\ \mathrm{F}P(c_0) & \mathrm{T}Q(c_0) \\ \otimes & \otimes \end{array}$$

Ještě příklad (φ, ψ jsou formule s jedinou volnou proměnnou x)

- $\mathrm{F}(\forall x)(\varphi(x) \wedge \psi(x)) \leftrightarrow ((\forall x)\varphi(x) \wedge (\forall x)\psi(x))$
  - $\mathrm{T}(\forall x)(\varphi(x) \wedge \psi(x))$
    - $\mathrm{F}(\forall x)\varphi(x) \wedge (\forall x)\psi(x)$
      - $\mathrm{F}(\forall x)\varphi(x)$
        - $\mathrm{F}\varphi(c_0)$
        - $\mathrm{T}(\forall x)(\varphi(x) \wedge \psi(x))$
        - $\mathrm{T}\varphi(c_0) \wedge \psi(c_0)$
        - $\mathrm{T}\varphi(c_0)$
        - $\mathrm{T}\psi(c_0)$
        - $\otimes$
      - $\mathrm{F}(\forall x)\psi(x)$
        - $\mathrm{F}\psi(c_0)$
        - $\mathrm{T}(\forall x)(\varphi(x) \wedge \psi(x))$
        - $\mathrm{T}\varphi(c_0) \wedge \psi(c_0)$
        - $\mathrm{T}\varphi(c_0)$
        - $\mathrm{T}\psi(c_0)$
        - $\otimes$
  - $\mathrm{F}(\forall x)(\varphi(x) \wedge \psi(x))$
    - $\mathrm{T}(\forall x)\varphi(x) \wedge (\forall x)\psi(x)$
    - $\mathrm{T}(\forall x)\varphi(x)$
    - $\mathrm{T}(\forall x)\psi(x)$
    - $\mathrm{F}(\varphi(c_0) \wedge \psi(c_0))$
      - $\mathrm{F}\varphi(c_0)$
        - $\mathrm{T}(\forall x)\varphi(x)$
        - $\mathrm{T}\varphi(c_0)$
        - $\otimes$
      - $\mathrm{F}\psi(c_0)$
        - $\mathrm{T}(\forall x)\psi(x)$
        - $\mathrm{T}\psi(c_0)$
        - $\otimes$

(c_0 lze použít jako nový ve všech případech: na dané větvi se dosud nevyskytuje)

Systematické tablo

musí někdy zredukovat každou položku, použít každý axiom, a nově ve všech položkách typu "všichni" dosadit každý L_C term t_i

Systematické tablo z $T = \{\alpha_0, \alpha_1, \alpha_2, \dots\}$ pro položku R je $\tau = \bigcup_{i \geq 0} \tau_i$, kde τ_0 je jednoprvkové s položkou R, a pro $i \geq 0$:

- buď P nejlevější položka v co nejmenší úrovni, která není redukovaná na nějaké bezesporné větvi procházející P (resp. je-li typu "všichni", její výskyt není redukovaný)
- nejprve definujeme τ_i' vzniklé z τ_i připojením atomického tabla pro P na každou bezespornou větev procházející P, kde je-li P typu "všichni" a má-li ve vrcholu k-tý výskyt, dosadíme k-tý L_C-term t_k, je-li typu "svědek", substituujeme $c_i \in C$ s nejmenším i, které na větvi zatím není
- pokud taková položka P neexistuje, potom $\tau_i' = \tau_i$
- τ_{i+1} vznikne z τ_i' připojením $\mathrm{T}\alpha_{i+1}$ na vš. bezesporné větve (pokud už jsme použili všechny axiomy, definujeme $\tau_{i+1} = \tau_i'$)

Konečnost a systematičnost důkazů

Lemma: Systematické tablo je dokončené.

Důkaz: k-tý výskyt položky typu "všichni" redukujeme když na něj narazíme: připojíme $(k+1)$-ní výskyt a dosadíme k-tý L_C-term t_k. Zbytek důkazu jako ve výrokové logice. □

Neprodlužujeme-li sporné větve (což nemusíme), je sporné tablo vždy konečné. Důkaz stejný jako ve výrokové logice:

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

Stejně jako ve výrokové logice z důkazu plyne:

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

7.3 Jazyky s rovností

Rovnost

$1 + 0 = 0 + 1$? identita celých čísel, výrazů, množin, unifikovatelnost termů (v Prologu), ...

Tablo je čistě syntaktický objekt, ale $=^{\mathcal{A}}$ má být identita na A. Jak toho docílit?

Mějme dokončenou bezespornou větev tabla s položkou $\mathrm{T}c_1 = c_2$. V kanonickém modelu musí platit nejen $(c_1^{\mathcal{A}}, c_2^{\mathcal{A}}) \in =^{\mathcal{A}}$, ale také:

- $c_2^{\mathcal{A}} =^{\mathcal{A}} c_1^{\mathcal{A}}$
- $f^{\mathcal{A}}(c_1^{\mathcal{A}}) =^{\mathcal{A}} f^{\mathcal{A}}(c_2^{\mathcal{A}})$
- $c_1^{\mathcal{A}} \in P^{\mathcal{A}}$ právě když $c_2^{\mathcal{A}} \in P^{\mathcal{A}}$

To vynutíme přidáním axiomů rovnosti, $=^{\mathcal{A}}$ bude kongruence $\mathcal{A}$ (ekvivalence, která se chová dobře k funkcím a relacím).

Poté vezmeme faktorstrukturu $\mathcal{B} = \mathcal{A}/_{=^{\mathcal{A}}}$, v ní už je $=^{\mathcal{B}}$ identita.

Kongruence a faktorstruktura

Buď $\sim$ ekvivalence na A, $f\colon A^n \to A$, $R \subseteq A^n$. Říkáme, že $\sim$ je:

- kongruence pro f, pokud pro všechna $a_i, b_i \in A$ taková, že $a_i \sim b_i$ $(1 \leq i \leq n)$, platí $f(a_1, \ldots, a_n) \sim f(b_1, \ldots, b_n)$
- kongruence pro R, pokud pro všechna $a_i, b_i \in A$ taková, že $a_i \sim b_i$ $(1 \leq i \leq n)$, platí $R(a_1, \ldots, a_n) \Leftrightarrow R(b_1, \ldots, b_n)$

Kongruence struktury $\mathcal{A}$ je ekvivalence na A, která je kongruencí pro všechny funkce a relace $\mathcal{A}$.

Faktorstruktura (podílová struktura) $\mathcal{A}$ podle $\sim$ je struktura $\mathcal{A}/_\sim$ v témž jazyce, doména $A/_\sim$ je množina všech rozkladových tříd A podle $\sim$, funkce a relace definujeme pomocí reprezentantů:

- $f^{\mathcal{A}/\sim}([a_1]_\sim, \ldots, [a_n]_\sim) = [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\sim$
- $R^{\mathcal{A}/\sim}([a_1]_\sim, \ldots, [a_n]_\sim) \Leftrightarrow R^{\mathcal{A}}(a_1, \ldots, a_n)$

Axiomy rovnosti

Axiomy rovnosti pro jazyk L s rovností:

(i) $x = x$

(ii) pro každý n-ární funkční symbol f jazyka L:

$$x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

(iii) pro každý n-ární relační symbol R jazyka L včetně rovnosti:

$$x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow (R(x_1, \ldots, x_n) \rightarrow R(y_1, \ldots, y_n))$$

- symetrie a tranzitivita plynou z (iii) pro $=$ (dokažte si)
- z axiomů (i) a (iii) tedy plyne, že relace $=^{\mathcal{A}}$ je ekvivalence
- axiomy (ii) a (iii) vyjadřují, že $=^{\mathcal{A}}$ je kongruence

V tablo metodě pro jazyk s rovností implicitně přidáme axiomy rovnosti (přesněji jejich generální uzávěry, potřebujeme sentence).

Tablo důkaz s rovností

Je-li T teorie v jazyce L s rovností, označme jako T^* rozšíření T o generální uzávěry axiomů rovnosti pro L.

- tablo důkaz z teorie T je tablo důkaz z T^*
- podobně pro tablo zamítnutí, a obecně jakékoliv tablo z T

Pozorování:

- Je-li $\mathcal{A} \models T^*$, potom i $\mathcal{A}/_{=^\mathcal{A}} \models T^*$, a ve struktuře $\mathcal{A}/_{=^\mathcal{A}}$ je symbol rovnosti interpretován jako identita.
- Na druhou stranu, v každém modelu, ve kterém je symbol rovnosti interpretován jako identita, platí axiomy rovnosti.

(Použijeme při konstrukci kanonického modelu v důkazu úplnosti.)

Osmá přednáška

Program

- korektnost a úplnost, kanonický model
- věta o kompaktnosti, Löwenheim-Skolemova věta
- hilbertovský kalkulus

Materiály

Zápisky z přednášky, Sekce 7.4-7.6 z Kapitoly 7 (+ Sekce 4.8)

7.4 Korektnost a úplnost

Korektnost a úplnost

Stejně jako ve výrokové logice:

dokazatelnost je totéž, co platnost

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

(Důkazy mají stejnou strukturu, liší se jen v implementačních detailech pomocných lemmat.)

Korektnost: pomocné lemma

Model $\mathcal{A}$ se shoduje s položkou P, pokud $P = \mathrm{T}\varphi$ a $\mathcal{A} \models \varphi$, nebo $P = \mathrm{F}\varphi$ a $\mathcal{A} \not\models \varphi$, a s větví V, shoduje-li s každou položkou na V.

Lemma: Shoduje-li se model $\mathcal{A}$ teorie T (v jazyce L) s položkou v kořeni tabla z T, potom lze $\mathcal{A}$ expandovat do jazyka L_C (interpretovat symboly $c_i \in C$) tak, že se shoduje s některou větví v tablu.

NB: Stačí interpret. symboly c_i vyskytující se na větvi, ostatní libovolně.

Důkaz: Indukcí podle konstrukce $\tau = \bigcup_{i \geq 0} \tau_i$ najdeme posloupnost větví $V_0 \subseteq V_1 \subseteq \dots$ a expanzí $\mathcal{A}_i$ o konstanty na V_i tak, že:

- V_i je větev v tablu τ_i shodující se s modelem $\mathcal{A}_i$
- V_{i+1} je prodloužením V_i a $\mathcal{A}_{i+1}$ je expanzí $\mathcal{A}_i$

Hledaná větev v τ je $V = \bigcup_{i \geq 0} V_i$, L_C-expanze $\mathcal{A}$ je 'limita' $\mathcal{A}_i$: vyskytuje-li se $c \in C$ na V_i, interpretuj jako v $\mathcal{A}_i$, jinak libovolně.

Báze: $\mathcal{A}_0 = \mathcal{A}$ se shoduje s kořenem, tj. s (jednoprvkovou) V_0 v τ_0.

Pokračování důkazu pomocného lemmatu

Indukční krok: Pokud jsme neprodloužili V_i: $V_{i+1} = V_i$, $\mathcal{A}_{i+1} = \mathcal{A}_i$.

Pokud jsme připojili $\mathrm{T}\alpha$ (pro $\alpha \in T$) na konec V_i, definujeme V_{i+1} jako tuto prodlouženou větev, $\mathcal{A}_{i+1} = \mathcal{A}_i$ (nepřidali jsme nový symbol). Protože $\mathcal{A} \models T$, máme i $\mathcal{A}_{i+1} \models \alpha$, tedy se shoduje.

Nechť τ_{i+1} vzniklo připojením atomického tabla pro P na konec V_i.

- **logická spojka:** $\mathcal{A}_{i+1} = \mathcal{A}_i$ se shoduje s kořenem atomického tabla, tedy i s některou větví, o tu prodloužíme V_i na V_{i+1}
- **typ "svědek":** SÚNO $P = \mathrm{T}(\exists x)\varphi(x)$: $\mathcal{A}_i \models (\exists x)\varphi(x)$, tedy existuje $a \in A$, že $\mathcal{A}_i \models \varphi(x)[e(x/a)]$. V_{i+1} je prodloužení V_i o nově přidanou $\mathrm{T}\varphi(x/c)$, $\mathcal{A}_{i+1}$ je expanze $\mathcal{A}_i$ o $c^{\mathcal{A}_{i+1}} = a$.
- **typ "všichni":** V_{i+1} je prodloužení V_i o atomické tablo. SÚNO nová položka $\mathrm{T}\varphi(x/t)$ pro nějaký L_C-term t. Model $\mathcal{A}_{i+1}$ je libovolná expanze $\mathcal{A}_i$ o nové symboly z t. $\mathcal{A}_i \models (\forall x)\varphi(x) \Rightarrow \mathcal{A}_{i+1} \models (\forall x)\varphi(x) \Rightarrow \mathcal{A}_{i+1} \models \varphi(x/t)$, tedy se shoduje. $\square$

Věta o korektnosti [tablo metody ve predikátové logice]

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

Myšlenka důkazu: Protipříklad by se [po vhodné interpretaci pomocných symbolů] shodoval s některou větví, ty jsou ale sporné.

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

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

Model $\mathcal{A}$ se shoduje s kořenem $\mathrm{F}\varphi$, tedy podle Lemmatu lze interpretovat symboly $c \in C$ tak, že se výsledná L_C-expanze $\mathcal{A}'$ shoduje s nějakou větví V. Všechny větve jsou ale sporné, musela by se shodovat s $\mathrm{T}\psi$ a zároveň $\mathrm{F}\psi$ pro nějakou L_C-sentenci ψ. $\square$

Kanonický model: jazyk bez rovnosti

opět z bezesporné dokončené větve V (tabla z T) vyrobíme model

jeho doména? trik: ze syntaktických objektů uděláme sémantické

Je-li $L = \langle \mathcal{F}, \mathcal{R} \rangle$ bez rovnosti, kanonický model pro bezespornou dokončenou V je L_C-struktura $\mathcal{A} = \langle A, \mathcal{F}^{\mathcal{A}} \cup C^{\mathcal{A}}, \mathcal{R}^{\mathcal{A}} \rangle$, kde:

- doména A je množina všech konstantních L_C-termů
- pro n-ární relační symbol $R \in \mathcal{R}$ a "s_1", ..., "s_n" z A:

$$(\text{“}s_1\text{”}, \ldots, \text{“}s_n\text{”}) \in R^{\mathcal{A}} \;\Leftrightarrow\; \text{na } V \text{ je položka } \mathrm{T}R(s_1, \ldots, s_n)$$

- pro n-ární funkční symbol $f \in \mathcal{F}$ a "s_1", ..., "s_n" z A:

$$f^{\mathcal{A}}(\text{“}s_1\text{”}, \ldots, \text{“}s_n\text{”}) = \text{“}f(s_1, \ldots, s_n)\text{”}$$

- speciálně, pro konstantní symbol c máme $c^{\mathcal{A}} = \text{“}c\text{”}$

(funkce $f^{\mathcal{A}}$ je "vytvoření" termu ze symbolu f a vstupních termů)

Příklad

$T = \{(\forall x)R(f(x))\}$ v jazyce $L = \langle R, f, d\rangle$ bez rovnosti (R unární relační, f unární funkční, d konstantní). Protipříklad: $T \not\models \neg R(d)$

- dokončené tablo z T s položkou $\mathrm{F}\neg R(d)$ v kořeni má jedinou, bezespornou větev V
- kanon. model: L_C-struktura $\mathcal{A} = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}, c_0^{\mathcal{A}}, c_1^{\mathcal{A}}, \dots\rangle$
- doména je $A = \{\text{“}d\text{”}, \text{“}f(d)\text{”}, \text{“}f(f(d))\text{”}, \dots, \text{“}c_0\text{”}, \text{“}f(c_0)\text{”}, \text{“}f(f(c_0))\text{”}, \dots, \text{“}c_1\text{”}, \text{“}f(c_1)\text{”}, \text{“}f(f(c_1))\text{”}, \dots\}$
- interpretace symbolů jsou:
  - $d^{\mathcal{A}} = \text{“}d\text{”}$
  - $c_i^{\mathcal{A}} = \text{“}c_i\text{”}$ pro všechna $i \in \mathbb{N}$
  - $f^{\mathcal{A}}(\text{“}d\text{”}) = \text{“}f(d)\text{”}$, $f^{\mathcal{A}}(\text{“}f(d)\text{”}) = \text{“}f(f(d))\text{”}$, …
  - $R^{\mathcal{A}} = A \setminus C = \{\text{“}d\text{”}, \text{“}f(d)\text{”}, \text{“}f(f(d))\text{”}, \dots, \text{“}f(c_0)\text{”}, \text{“}f(f(c_0))\text{”}, \dots, \text{“}f(c_1)\text{”}, \text{“}f(f(c_1))\text{”}, \dots\}$.
- redukt na původní jazyk L: $\mathcal{A}' = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}\rangle$

Kanonický model: jazyk s rovností

Je-li L s rovností:

- vezmeme kanonický model $\mathcal{B}$ pro V jako by byl L bez rovnosti
- definujeme relaci $=^B$ stejně jako pro ostatní relační symboly:

$$\text{“}s_1\text{”} =^B \text{“}s_2\text{”} \;\Leftrightarrow\; \text{na } V \text{ je položka } \mathrm{T}s_1 = s_2$$

- kanonický model pro V je faktorstruktura $\mathcal{A} = \mathcal{B}/_{=^B}$

- tablo je nyní z teorie T^* (rozšíření o axiomy rovnosti)
- $=^B$ je opravdu kongruence struktury $\mathcal{B}$ a $=^{\mathcal{A}}$ je identita na A
- **Pozorování:** pro lib. formuli φ platí $\mathcal{B} \models \varphi$ právě když $\mathcal{A} \models \varphi$ (symbol $=$ interpretujeme jako $=^B$ v $\mathcal{B}$ a jako identitu v $\mathcal{A}$)

Všimněte si:

- v jazyce bez rovnosti je kanonický model spočetně nekonečný
- v jazyce s rovností může být i konečný

Příklad

$T = \{(\forall x)R(f(x)), (\forall x)(x = f(f(x)))\}$ $L = \langle R, f, d\rangle$ s rovností
opět chceme protipříklad ukazující, že $T \not\models \neg R(d)$

- dokončené tablo z T^* pro $\mathrm{F}\neg R(d)$ má jedinou, bezespornou V
- sestrojíme kanonický model jako by byl jazyk bez rovnosti:

$$\mathcal{B} = \langle B, R^{\mathcal{B}}, f^{\mathcal{B}}, d^{\mathcal{B}}, c_0^{\mathcal{B}}, c_1^{\mathcal{B}}, c_2^{\mathcal{B}}, \dots\rangle$$

- '$=$' jako obyčejný symbol: $s_1 =^B s_2 \Leftrightarrow s_1 = f(\cdots(f(s_2))\cdots)$ nebo $s_2 = f(\cdots(f(s_1))\cdots)$ pro sudý počet f

$$B/_{=^B} = \{[\text{“}d\text{”}]_{=^B}, [\text{“}f(d)\text{”}]_{=^B}, [\text{“}c_0\text{”}]_{=^B}, [\text{“}f(c_0)\text{”}]_{=^B}, [\text{“}c_1\text{”}]_{=^B}, [\text{“}f(c_1)\text{”}]_{=^B}, \dots\}$$

- kanonický model: $\mathcal{A} = \mathcal{B}/_{=^B} = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}, c_0^{\mathcal{A}}, c_1^{\mathcal{A}}, c_2^{\mathcal{A}}, \dots\rangle$
  - $A = B/_{=^B}$, $d^{\mathcal{A}} = [\text{“}d\text{”}]_{=^B}$, $c_i^{\mathcal{A}} = [\text{“}c_i\text{”}]_{=^B}$ pro všechna $i \in \mathbb{N}$,
  - $f^{\mathcal{A}}([\text{“}d\text{”}]_{=^B}) = [\text{“}f(d)\text{”}]_{=^B}$,
    $f^{\mathcal{A}}([\text{“}f(d)\text{”}]_{=^B}) = [\text{“}f(f(d))\text{”}]_{=^B} = [\text{“}d\text{”}]_{=^B}$, ...
  - $R^{\mathcal{A}} = A = B/_{=^B}$.
- redukt na původní jazyk L: $\mathcal{A}' = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}\rangle$

Úplnost: pomocné lemma

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

Důkaz: Jazyk bez rovnosti: indukcí podle struktury sentence v P

- **atomická sentence:** stejně jako ve VL (báze indukce)
- **logická spojka:** stejně jako ve VL
- **typ "svědek":** $P = \mathrm{T}(\exists x)\varphi(x)$, potom je na V i $T\varphi(x/c)$ pro nějaké "c" $\in A$; z indukčního předpokladu $\mathcal{A} \models \varphi(x/c)$, tj. $\mathcal{A} \models \varphi(x)[e(x/\text{“}c\text{”})]$ tedy i $\mathcal{A} \models (\exists x)\varphi(x)$
- **typ "všichni":** $P = \mathrm{T}(\forall x)\varphi(x)$, na V jsou i položky $T\varphi(x/t)$ pro každý konstantní L_C-term, tj. pro každý prvek "t" $\in A$; z ind. předpokladu je $\mathcal{A} \models \varphi(x/t)$, tj. $\mathcal{A} \models \varphi(x)[e(x/\text{“}t\text{”})]$ pro každé "t" $\in A$, tedy $\mathcal{A} \models (\forall x)\varphi(x)$

Jazyk s rovností: $\mathcal{A} = \mathcal{B}/_{=^B}$, pro $\mathcal{B}$ máme, zbytek z Pozorování $\square$

Věta o úplnosti

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

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

Sporem: Není-li sporné, má bezespornou (dokončenou) větev V, a dle Lemmatu se kanonický model $\mathcal{A}$ s větví V shoduje.

Buď $\mathcal{A}'$ redukt $\mathcal{A}$ na jazyk teorie T (zapomeň pomocné symboly).

Protože je V dokončená, obsahuje $\mathrm{T}\alpha$ pro všechny axiomy T. Model $\mathcal{A}$, tedy i $\mathcal{A}'$, splňuje všechny axiomy a máme $\mathcal{A}' \models T$.

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

7.5 Důsledky korektnosti a úplnosti

$\vdash\ =\ \models$

Syntaktickou analogií důsledků jsou teorémy:

$$\mathrm{Thm}_L(T) = \{\varphi \mid \varphi \text{ je } L\text{-sentence a } T \vdash \varphi\}$$

Z korektnosti a úplnosti okamžitě dostáváme:

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

Všude můžeme nahradit 'platnost' pojmem 'dokazatelnost'. Např:

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

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

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

Löwenheim-Skolemova věta & Věta o kompaktnosti

Věta (Löwenheim-Skolemova): Je-li L spočetný bez rovnosti, potom každá bezesporná L-teorie má spočetně nekonečný model.

(Později ukážeme i verzi s rovností, kan. model může být konečný.)

Důkaz: V T není dokazatelný spor. Dokončené tablo z T s $\mathrm{F}\bot$ v kořeni tedy musí obsahovat bezespornou větev. Hledaný model je L-redukt kanonického modelu pro tuto větev. $\square$

Věta o kompaktnosti, vč. důkazu, je stejná jako ve výrokové logice:

Věta (O kompaktnosti): Teorie má model, právě když každá její konečná část má model.

Důkaz: Model teorie je modelem každé části. Naopak, pokud T nemá model, je sporná, tedy $T \vdash \bot$. Vezměme nějaký konečný tablo důkaz $\bot$ z T. K jeho konstrukci stačí konečně mnoho axiomů T, ty tvoří konečnou podteorii $T' \subseteq T$, která nemá model. $\square$

Nestandardní model přirozených čísel

- $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je standardní model přirozených čísel
- teorie struktury $\mathrm{Th}(\underline{\mathbb{N}})$: všechny sentence pravdivé v $\underline{\mathbb{N}}$
- n-tý numerál: term $\underline{n} = S(S(\cdots(S(0)\cdots)))$, kde S je n-krát

Přidáme nový konstantní symbol c a vyjádříme, že je ostře větší než každý n-tý numerál:

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

- každá konečná část T má model
- dle věty o kompaktnosti: i T má model
- říkáme mu nestandardní model (označme $\mathcal{A}$)
- platí v něm tytéž sentence, které platí ve standardním modelu
- ale zároveň obsahuje prvek $c^{\mathcal{A}}$, který je větší než každé $n \in \mathbb{N}$ (tzn. větší než hodnota termu $\underline{n}$ v nestandardním modelu $\mathcal{A}$)

Hilbertovský kalkulus

Hilbertovský deduktivní systém

- jiný, původní dokazovací systém
- používá jen logické spojky $\neg$, $\to$
- schémata logických axiomů (φ, ψ, χ jsou lib. výroky/formule)

(i) $\varphi \to (\psi \to \varphi)$

(ii) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

(iii) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$

v predikátové logice navíc:

(iv) $(\forall x)\varphi \to \varphi(x/t)$ je-li t substituovatelný za x do φ

(v) $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$ není-li x volná ve φ

(vi) **axiomy rovnosti**, je-li jazyk s rovností

- odvozovací pravidla:

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

v predikátové logice navíc:

$$\frac{\varphi}{(\forall x)\varphi} \text{ (generalizace)}$$

Hilbertovský důkaz

- hilbertovský důkaz výroku φ z teorie T je konečná posloupnost $\varphi_0, \dots, \varphi_n = \varphi$, ve které pro každé $i \leq n$:
  - φ_i je logický axiom, nebo
  - φ_i je axiom teorie ($\varphi_i \in T$), nebo
  - φ_i lze odvodit z předchozích pomocí odvozovacího pravidla
- existuje-li hilbertovský důkaz, píšeme: $T \vdash_H \varphi$

Příklad (jen ve výrokové logice)

Ukažme, že pro teorii $T = \{\neg\varphi\}$ a pro libovolný výrok ψ platí:

$$T \vdash_H \varphi \to \psi$$

Hilbertovský důkaz:

1. $\neg\varphi$ — *axiom teorie*
2. $\neg\varphi \to (\neg\psi \to \neg\varphi)$ — *logický axiom (i)*
3. $\neg\psi \to \neg\varphi$ — *modus ponens na 1. a 2.*
4. $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$ — *logický axiom (iii)*
5. $\varphi \to \psi$ — *modus ponens na 3. a 4.*

Korektnost a úplnost

Věta (o korektnosti hilbertovského kalkulu): $T \vdash_H \varphi \Rightarrow T \models \varphi$

Důkaz: Indukcí dle délky důkazu: každá φ_i (vč. $\varphi_n = \varphi$) platí v T

- logické axiomy (vč. axiomů rovnosti) jsou tautologie, platí v T
- axiomy z T jistě v T také platí
- modus ponens i generalizace jsou korektní inferenční pravidla:
  - je-li $T \models \varphi$ a $T \models \varphi \rightarrow \psi$, potom $T \models \psi$
  - je-li $T \models \varphi$, potom $T \models (\forall x)\varphi$ $\square$

Věta (o úplnosti hilbertovského kalkulu): $T \models \varphi \;\Rightarrow\; T \vdash_H \varphi$

Důkaz vynecháme.

Devátá přednáška

Program

- úvod do rezoluce v predikátové logice
- skolemizace
- grounding, Herbrandova věta

Materiály

Zápisky z přednášky, Sekce 8.1-8.3 z Kapitoly 8

Kapitola 8: Rezoluce v predikátové logice

8.1 Úvod

Rezoluce v predikátové logice

$T \models \varphi? \rightsquigarrow T \cup \{\neg\varphi\} \rightsquigarrow$ CNF formule $S \rightsquigarrow$ rezoluční zamítnutí

(pozor: φ musí být sentence!)

- literál je atomická formule $R(t_1, \ldots, t_n)$ nebo její negace
- klauzule je konečná množina literálů, formule množina klauzulí
- otevřenou formuli snadno převedeme do CNF, i univerzální kvantifikátor na začátku: $(\forall x)(P(x) \vee \neg Q(x)) \sim \{P(x), \neg Q(x)\}$
- co s existenčními kvantifikátory? nové symboly pro 'svědky' $(\exists x)(P(x) \vee \neg Q(x)) \rightsquigarrow \{P(c), \neg Q(c)\}$ "skolemizace"
- není ekvivalentní, ale zachovává [ne]splnitelnost, to nám stačí
- rezoluční krok? literály nemusí být stejné, stačí unifikovatelné z klauzulí $\{P(x), \neg Q(x)\}$ a $\{Q(f(c))\}$ odvodíme $\{P(f(c))\}$
- unifikace je substituce $\{x/f(c)\}$

Příklady

1. $T = \{(\forall x)P(x), (\forall x)(P(x) \to Q(x))\}$, $\varphi = (\exists x)Q(x)$

$$\neg\varphi = \neg(\exists x)Q(x) \sim (\forall x)\neg Q(x) \sim \neg Q(x)$$

$T \cup \{\neg\varphi\}$ je ekvivalentní $S = \{\{P(x)\}, \{\neg P(x), Q(x)\}, \{\neg Q(x)\}\}$
rezoluční zamítnutí: představte si p místo $P(x)$, q místo $Q(x)$

2. $T = \{(\forall x)(\exists y)R(x, y), R(x, y) \to Q(x)\}$, $\varphi = (\exists x)Q(x)$

$$T \cup \{\neg\varphi\} \sim \{(\forall x)(\exists y)R(x, y), \neg R(x, y) \vee Q(x), \neg Q(x)\}$$

formuli $(\forall x)(\exists y)R(x, y)$ nahradíme $R(x, f(x))$, kde f je nový unární funkční symbol (reprezentuje výběr svědka):

$$S = \{\{R(x, f(x))\}, \{\neg R(x, y), Q(x)\}, \{\neg Q(x)\}\}$$

není ekvivalentní, ale ekvisplnitelná (zde obě nesplnitelné), vidíme po substituci $y/f(x)$, která unifikuje $R(x, f(x))$ a $R(x, y)$

Unifikace

$$S = \{\{R(x, f(x))\}, \{\neg R(x, y), Q(x)\}, \{\neg Q(x)\}\}$$

- na úrovni výrokové logiky (ground level):

  $$\{\{r\}, \{\neg p, q\}, \{\neg q, p\}, \{\neg q\}\}$$

  není nesplnitelné! musíme využít, že $R(x, f(x))$ a $R(x, y)$ mají ‘podobnou strukturu’ (jsou unifikovatelné)
- klauzule $\{\neg R(x, y), Q(x)\}$ platí i po provedení libovolné substituce: $\{\neg R(x/t), Q(x/t)\}$ je důsledek S pro lib. term t
- představme si ‘přidání’ všech takto získaných klauzulí do S: potom už je na ground level nesplnitelné (ale nekonečné)
- unifikační algoritmus nám dá správnou substituci $y/f(x)$
- zahrneme už do rezolučního pravidla, tedy rezolventou klauzulí $\{P(c)\}$ a $\{\neg P(x), Q(x)\}$ bude klauzule $\{Q(c)\}$.

Rezoluční pravidlo

- zahrnuje aplikaci unifikace
- lze vybrat více literálů najednou, ale musí být unifikovatelné:

  např. z $\{R(x, f(x)), R(g(y), z)\}, \{\neg R(g(c), u), P(u)\}$ odvodíme rezolventu $\{P(f(g(c)))\}$ za použití unifikace

  $$\{x/g(c), y/c, z/f(g(c)), u/f(g(c))\}$$

- budeme vyžadovat disjunktní množiny proměnných v klauzulích; lze přejmenovat, proměnné mají lokální význam:

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

8.2 Skolemizace

Ekvisplnitelná otevřená teorie

- teorie T v jazyce L a T' v (ne nutně stejném) jazyce L' jsou ekvisplnitelné, pokud platí: T má model $\Leftrightarrow$ T' má model
- zajímá nás jen [ne]splnitelnost (dokazujeme sporem)
- pro převod do CNF a rezoluci potřebujeme otevřené formule

Cíl: Ke každé teorii T sestrojíme ekvisplnitelnou, otevřenou T'.

1. převod do prenexní normální formy (vytkneme kvantifikátory)
2. nahradíme generálními uzávěry (potřebujeme sentence!)
3. nahradíme sentence Skolemovými variantami (odstranění $\exists$)
4. odstraníme zbývající $\forall$, máme otevřené formule

Prenexní normální forma

Formule φ je v prenexní normální formě (PNF), je-li následujícího tvaru, kde $Q_i \in \{\forall, \exists\}$ a formule φ' je otevřená:

$$(Q_1 x_1) \dots (Q_n x_n) \varphi'$$

- $(Q_1 x_1) \dots (Q_n x_n)$ je kvantifikátorový prefix, φ' otevřené jádro
- univerzální formule: v PNF a všechny kvantifikátory jsou $\forall$

Tvrzení: Ke každé formuli φ existuje ekvivalentní formule v PNF.

Důkaz: nahrazujeme podformule ekvivalentními s cílem posunout kvantifikátory blíž kořeni Tree(φ), dle pravidel z násl. Lemmatu. $\square$

Důsledek: Existuje i ekvivalentní PNF sentence (generální uzávěr).

Pravidla vytýkání kvantifikátorů

Lemma: Označme $\overline{Q}$ opačný kvantifikátor ke Q. Jsou-li φ a ψ formule, kde x není volná v ψ, potom:

$$\begin{aligned} \neg(Qx)\varphi &\sim (\overline{Q}x)\neg\varphi \\ (Qx)\varphi \wedge \psi &\sim (Qx)(\varphi \wedge \psi) \\ (Qx)\varphi \vee \psi &\sim (Qx)(\varphi \vee \psi) \\ (Qx)\varphi \rightarrow \psi &\sim (\overline{Q}x)(\varphi \rightarrow \psi) \\ \psi \rightarrow (Qx)\varphi &\sim (Qx)(\psi \rightarrow \varphi) \end{aligned}$$

Důkaz: snadno ověříme sémanticky, nebo tablo metodou (potom ale nejsou-li sentence, musíme nahradit generálními uzávěry) $\square$

Pozorování: Nahradíme-li ve φ podformuli ψ ekvivalentní ψ', je i výsledná formule φ' ekvivalentní φ. (Připomeňme: $\varphi \sim \varphi'$ právě když mají stejné modely, tj. $\models \varphi \leftrightarrow \varphi'$)

Převod do PNF: příklad

$$(\forall z)P(x,z) \wedge P(y,z) \;\rightarrow\; \neg(\exists x)P(x,y)$$

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

- v prvním kroku přejmenujeme z na u, nesmí být volná v $P(y,z)$
- podobně ve druhém kroku x na v
- která pravidla používáme? sledujte postup na stromu formule
- chceme-li sentenci:

$$(\forall x)(\forall y)(\forall z)(\exists u)(\forall v)(P(x,u) \wedge P(y,z) \rightarrow \neg P(v,y))$$

Poznámky

1. proč se při vytýkání z antecedentu mění kvantifikátor?

$$\begin{aligned}(Qx)\varphi \rightarrow \psi &\sim \neg(Qx)\varphi \vee \psi \\ &\sim (\overline{Q}x)(\neg\varphi) \vee \psi \\ &\sim (\overline{Q}x)(\neg\varphi \vee \psi) \sim (\overline{Q}x)(\varphi \rightarrow \psi)\end{aligned}$$

2. proč nesmí být x volná v ψ? neplatilo by, např:

   $$(\exists x)P(x) \wedge Q(x) \;\not\sim\; (\exists x)(P(x) \wedge Q(x))$$

   musíme přejmenovat vázanou proměnnou x na novou:

   $$(\exists x)P(x) \wedge Q(x) \;\sim\; (\exists y)P(y) \wedge Q(x) \sim (\exists y)(P(y) \wedge Q(x))$$

3. PNF není jednoznačná, lze vytýkat v různém pořadí; lepší je nejprve vytknout ty, ze kterých se nakonec stanou existenční:

   $$(\exists y)(\forall x)\varphi(x,y) \text{ je lepší než } (\forall x)(\exists y)\varphi(x,y)$$

   (protože "y nezávisí na x")

Skolemova varianta

Je-li PNF sentence univerzální, tvaru $(\forall x_1)\dots(\forall x_n)\psi(x_1,\dots,x_n)$, nahradíme otevřeným jádrem ψ. Jinak musíme provést skolemizaci:

Buď φ L-sentence v PNF, všechny vázané proměnné různé. Nechť

- existenční kvantifikátory jsou $(\exists y_1),\dots,(\exists y_n)$ (v tom pořadí)
- pro každé i jsou $(\forall x_1),\dots,(\forall x_{n_i})$ právě všechny univerzální kvantifikátory předcházející $(\exists y_i)$ v prefixu φ

Buď L' rozšíření L o nové funkční symboly $f_1,\dots,f_n$, kde f_i je n_i-ární. Skolemova varianta φ je L'-sentence φ_S vzniklá odstraněním $(\exists y_i)$ a substitucí termu $f_i(x_1,\dots,x_{n_i})$ za y_i, postupně pro $i=1,\dots,n$.

$$\varphi = (\exists y_1)(\forall x_1)(\forall x_2)(\exists y_2)(\forall x_3)\ R(y_1,x_1,x_2,y_2,x_3)$$
$$\varphi_S = (\forall x_1)(\forall x_2)(\forall x_3)\ R(f_1,x_1,x_2,f_2(x_1,x_2),x_3)$$

- musí být sentence! pro $(\exists y)E(x,y)$ ne $\cancel{E(x,c)}$ ale $E(x,f(x))$
- nové symboly! (jedinou rolí je reprezentovat 'svědky' ve φ)

Je to konzervativní extenze

Lemma: Buď φ L-sentence $(\forall x_1)\dots(\forall x_n)(\exists y)\psi$, f nový funkční symbol, a φ' sentence $(\forall x_1)\dots(\forall x_n)\psi(y/f(x_1,\dots,x_n))$. Potom:

(i) L-redukt každého modelu φ' je modelem φ, a

(ii) každý model φ lze expandovat na model φ'.

Důkaz: (i) Buď $\mathcal{A}'$ model φ', $\mathcal{A}$ jeho L-redukt, $e : \mathrm{Var} \to \mathcal{A}$. $\mathcal{A} \models \varphi[e]$ platí neboť $\mathcal{A} \models \psi[e(y/a)]$ pro $a = (f(x_1,\dots,x_n))^{\mathcal{A}'}[e]$.

(ii) Protože $\mathcal{A} \models \varphi$, existuje funkce $f^A : A^n \to A$, že pro každé ohodnocení e platí $\mathcal{A} \models \psi[e(y/a)]$ pro $a = f^A(e(x_1),\dots,e(x_n))$. To znamená, že expanze o funkci f^A splňuje φ'. $\square$

- říká, že $\{\varphi'\}$ je konzervativní extenze $\{\varphi\}$, opakovaná aplikace dává Skolemovu větu (výsledek skolemizace je otevřená konzervativní extenze, speciálně je ekvisplnitelná)
- expanze v (ii) není jednoznačná (na rozdíl od extenze o definici nového funkčního symbolu)

Skolemova věta (shrnutí postupu)

Věta: Každá teorie má otevřenou konzervativní extenzi.

Důkaz Mějme L-teorii T. Axiomy nahradíme generálními uzávěry a převedeme do PNF, máme ekvivalentní L-teorii T'. V ní každý axiom nahradíme jeho Skolemovou variantou.

Tím získáme teorii T'' v rozšířeném jazyce L'. Lemma říká:

- L-redukt každého modelu T'' je model T'
- každý model T' lze expandovat do L' na model T''

Neboli T'' je konzervativní extenzí T', tedy i T. Je axiomatizovaná univerzálními sentencemi, odstraníme kvantifikátorové prefixy (vezmeme jádra) a máme ekvivalentní otevřenou teorii T'''. $\square$

Důsledek: Ke každé teorii můžeme pomocí skolemizace najít ekvisplnitelnou otevřenou teorii. (A tu už snadno převedeme do CNF.)

8.3 Grounding

Grounding

- základní (ground) instance otevřené φ ve volných proměnných $x_1, \ldots, x_n$ je $\varphi(x_1/t_1, \ldots, x_n/t_n)$, kde vš. t_i jsou konstantní

  Herbrandova věta říká, že je-li otevřená teorie nesplnitelná, lze to doložit "na konkrétních prvcích": existuje konečně mnoho základních instancí axiomů, jejichž konjunkce je nesplnitelná

- např. pro $T = \{P(x,y) \vee R(x,y), \neg P(c,y), \neg R(x, f(x))\}$ substituujeme konstantní termy $\{x/c, y/f(c)\}$:

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

- základní atomické sentence chápeme jako prvovýroky:

  $$(p_1 \vee p_2) \wedge \neg p_1 \wedge \neg p_2$$

- to už snadno zamítneme výrokovou rezolucí
- p_1 znamená "platí $P(c, f(c))$", p_2 znamená "platí $R(c, f(c))$"

Přímá redukce do výrokové logiky

Herbrandova věta + korektnost a úplnost výrokové rezoluce dává následující, neefektivní postup (S' je moc velká, i nekonečná):

1. $S \rightsquigarrow S' =$ množina všech základních instancí klauzulí z S
2. atomické sentence v S' chápeme jako prvovýroky
3. S nesplnitelná $\Leftrightarrow$ S' zamítnutelná 'na úrovni výrokové logiky'

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

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

S' je nesplnitelná obsahuje konečnou nesplnitelnou podmnožinu:

$$\{\{P(c,f(c)), R(c,f(c))\}, \{\neg P(c,f(c))\}, \{\neg R(c,f(c))\}\} \vdash_R \square$$

Efektivnější je hledat vhodné základní instance unifikací [za chvíli]

Herbrandův model

Mějme jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$ s alespoň jedním konstantním symbolem. L-struktura $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ je Herbrandův model, jestliže:

- A je množina všech konst. L-termů (Herbrandovo univerzum)
- pro každý n-ární $f \in \mathcal{F}$ a (konstantní) "t_1", ..., "t_n" $\in A$:
$$f^{\mathcal{A}}(\text{"}t_1\text{"}, \ldots, \text{"}t_n\text{"}) = \text{"}f(t_1, \ldots, t_n)\text{"}$$
- speciálně, pro konstantní symbol $c \in \mathcal{F}$ je $c^{\mathcal{A}} = \text{"}c\text{"}$
- na relační symboly neklademe podmínky

Např. $L = \langle P, f, c \rangle$ (P unární rel., f binární funkční, c konstantní)
Herbrandův model je každá struktura $\mathcal{A} = \langle A, P^{\mathcal{A}}, f^{\mathcal{A}}, c^{\mathcal{A}} \rangle$, kde

- $A = \{\text{"}c\text{"}, \text{"}f(c,c)\text{"}, \text{"}f(c,f(c,c))\text{"}, \text{"}f(f(c,c),c)\text{"} \ldots\}$
- $c^{\mathcal{A}} = \text{"}c\text{"}$
- $f^{\mathcal{A}}(\text{"}c\text{"}, \text{"}c\text{"}) = \text{"}f(c,c)\text{"}$, $f^{\mathcal{A}}(\text{"}c\text{"}, \text{"}f(c,c)\text{"}) = \text{"}f(c,f(c,c))\text{"}$, $f^{\mathcal{A}}(\text{"}f(c,c)\text{"}, \text{"}c\text{"}) = \text{"}f(f(c,c),c)\text{"}$, atd.
- $P^{\mathcal{A}} \subseteq A$ může být libovolná

Věta (Herbrandova): Je-li T otevřená, v jazyce bez rovnosti a s alespoň jedním konstantním symbolem, potom:

- buď má T Herbrandův model, nebo
- existuje konečně mnoho základních instancí axiomů T, jejichž konjunkce je nesplnitelná.

Důkaz: $T_{\text{ground}} =$ množina všech základních instancí axiomů T

Zkonstruujeme "systematické tablo" τ z T_{ground} s $\mathrm{F}\bot$ v kořeni, ale z jazyka L, bez rozšíření o pomocné konstantní symboly na L_C. (Nepotřebujeme je, protože v T_{ground} nejsou kvantifikátory.)

Pokud má τ bezespornou větev, je "kanonický model" (opět bez pomocných symbolů) Herbrandovým modelem T.

Jinak je τ důkaz sporu, T_{ground} (a tedy i T) je nesplnitelná. Tablo τ je konečné, používá jen konečně mnoho $\alpha_{\text{ground}} \in T_{\text{ground}}$, jejich konjunkce už je nesplnitelná. $\square$

Poznámky

- konstatní symbol potřebujeme, aby existovaly vůbec nějaké konstantní termy (ale není-li v L žádný, můžeme ho přidat)
- Herbrandův model je podobný kanonickému, ale nepřidáváme pomocné symboly, a neříkáme nic o relacích
- je-li jazyk s rovností, najdeme Herbrandův model pro T^* (přidané axiomy rovnosti) a faktorizujeme podle $=^A$

Důsledky Herbrandovy věty

Důsledek: Je-li T otevřená v jazyce s konstantním symbolem, potom T má model, právě když má model teorie T_{ground}.

Důkaz: $\Rightarrow$ V modelu T platí i všechny základní instance axiomů. Je tedy i modelem T_{ground}.

$\Leftarrow$ Pokud T nemá model, podle Herbrandovy věty je nějaká konečná podmnožina teorie T_{ground} nesplnitelná. □

Důsledek: Mějme otevřenou $\varphi(x_1, \ldots, x_n)$ v L s konst. symbolem. Potom existuje $m \in \mathbb{N}$ a konstantní L-termy t_{ij} ($i \in [m], j \in [n]$), že sentence $(\exists x_1) \ldots (\exists x_n)\varphi(x_1, \ldots, x_n)$ je pravdivá, právě když je následující formule (výroková) tautologie:

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

Důkaz: Je pravdivá, právě když $(\forall x_1) \ldots (\forall x_n)\neg\varphi$ neboli $\neg\varphi$ je nesplnitelná. Stačí aplikovat Herbrandovu větu na $T = \{\neg\varphi\}$. □

Desátá přednáška

Program

- unifikace, unifikační algoritmus
- rezoluční pravidlo, rezoluční důkaz
- korektnost rezoluce
- lifting lemma a úplnost rezoluce

Materiály

Zápisky z přednášky, Sekce 8.4-8.6 z Kapitoly 8

8.4 Unifikace

Příklady substitucí

Místo všech základních použijeme 'vhodné' substituce (unifikace):

1. $\{P(x), Q(x,a)\}$ a $\{\neg P(y), \neg Q(b,y)\}$
   - substitucí $\{x/b, y/a\}$ získáme $\{P(b), Q(b,a)\}$ a $\{\neg P(a), \neg Q(b,a)\}$, z nich rezolucí $\{P(b), \neg P(a)\}$
   - nebo $\{x/y\}$ a rezolucí přes $P(y)$ máme $\{Q(y,a), \neg Q(b,y)\}$
   - šlo by např. $\{x/a\}$, získat $\{Q(a,a), \neg Q(b,a)\}$, ale to je horší

2. $\{P(x), Q(x,z)\}$ a $\{\neg P(y), \neg Q(f(y),y)\}$
   - lze použít $\{x/f(a), y/a, z/a\}$, získat $\{P(f(a)), Q(f(a),a)\}$ a $\{\neg P(a), \neg Q(f(a),a)\}$, rezolucí $\{P(f(a)), \neg P(a)\}$
   - lepší je $\{x/f(z), y/z\}$, dává $\{P(f(z)), Q(f(z),z)\}$ a $\{\neg P(z), \neg Q(f(z),z)\}$, rezolventu $\{P(f(z)), \neg P(z)\}$
   - proč lepší? obecnější, rezolventa 'říká více': $\{P(f(a)), \neg P(a)\}$ je důsledkem $\{P(f(z)), \neg P(z)\}$, ale nejsou ekvivalentní
   - $\{x/f(a), y/a, z/a\}$ získáme složením $\{x/f(z), y/z\}$ a $\{z/a\}$

Substituce formálně

- substituce je konečná množina $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$, kde x_i jsou navzájem různé proměnné, t_i jsou termy, t_i není x_i
  - základní: všechny termy t_i jsou konstantní
  - přejmenování proměnných: vš. t_i navzájem různé proměnné
- výraz je term nebo literál (atomická formule nebo její negace)
- instance výrazu E při substituci $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$, $E\sigma$: simultánně nahradíme všechny výskyty x_i za termy t_i
- pro množinu výrazů S je $S\sigma = \{E\sigma \mid E \in S\}$

- simultánně proto, aby výskyt x_i v termu t_j nevedl ke zřetězení
- např. $S = \{P(x), R(y,z)\}$, $\sigma = \{x/f(y,z), y/x, z/c\}$

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

Skládání substitucí

- substituce lze skládat, $\sigma\tau$ znamená nejprve σ a potom τ
- chceme, aby platilo $E(\sigma\tau) = (E\sigma)\tau$, pro libovolný výraz E
- např. pro výraz $E = P(x, w, u)$ a substituce

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

máme $E\sigma = P(f(y), v, u)$ a $(E\sigma)\tau = P(f(g(x)), w, c)$, takže:

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

- skládání není komutativní, $\sigma\tau$ je (typicky) jiná než $\tau\sigma$, zde

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

- ale je asociativní (takže nemusíme psát závorky v $\sigma_1\sigma_2 \cdots \sigma_n$)

Buď $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$ a $\tau = \{y_1/s_1, \ldots, y_m/s_m\}$, označme $X = \{x_1, \ldots, x_n\}$ a $Y = \{y_1, \ldots, y_m\}$. Složení σ a τ je substituce

$$\sigma\tau = \{x_i/t_i\tau \mid x_i \in X, x_i \neq t_i\tau\} \cup \{y_j/s_j \mid y_j \in Y \setminus X\}$$

Vlastnosti skládání

Tvrzení: Pro libovolné substituce σ, τ, ϱ a výraz E platí:

$$\text{(i) } (E\sigma)\tau = E(\sigma\tau) \qquad \text{(ii) } (\sigma\tau)\varrho = \sigma(\tau\varrho)$$

Důkaz: (i) Buď $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$ a $\tau = \{y_1/s_1, \ldots, y_m/s_m\}$. Stačí pro E proměnnou (substituce nemění ostatní symboly):

- pro $E = x_i$ je $E\sigma = t_i$ a $(E\sigma)\tau = t_i\tau = E(\sigma\tau)$
- pro $E = y_j \notin X$ je $E\sigma = E$ a $(E\sigma)\tau = E\tau = s_j = E(\sigma\tau)$
- je-li E jiná proměnná, potom $(E\sigma)\tau = E = E(\sigma\tau)$.

(i) opakovaným užitím (i) máme pro lib. výraz, tedy i proměnnou:

$$E((\sigma\tau)\varrho) = (E(\sigma\tau))\varrho = ((E\sigma)\tau)\varrho = (E\sigma)(\tau\varrho) = E(\sigma(\tau\varrho))$$

Z toho plyne, že $(\sigma\tau)\varrho$ a $\sigma(\tau\varrho)$ jsou touž substitucí.

(Podrobněji, zřejmě platí: $\pi = \{z_1/v_1, \ldots, z_k/v_k\}$ právě když $z_i\pi = v_i$ a $E\pi = E$ je-li E proměnná různá od všech z_i.) $\square$

Unifikace

- unifikace pro $S = \{E_1, \ldots, E_n\}$ je substituce σ taková, že $E_1\sigma = E_2\sigma = \cdots = E_n\sigma$, tj. $S\sigma$ obsahuje jediný výraz
- pokud má S unifikaci, je unifikovatelná
- unifikace pro S je nejobecnější, pokud pro každou unifikaci τ pro S existuje substituce λ taková, že $\tau = \sigma\lambda$

NB: různé nejobecnějších unifikace pro S se liší jen přejmenováním proměnných

Např. pro $S = \{P(f(x), y), P(f(a), w)\}$

- $\sigma = \{x/a, y/w\}$ je nejobecnější unifikace
- $\tau = \{x/a, y/b, w/b\}$ je unifikace, ale není nejobecnější, nelze z ní získat např. unifikaci $\varrho = \{x/a, y/c, w/c\}$
- z nejobecnější unifikace σ získáme $\tau = \sigma\lambda$ pro $\lambda = \{w/b\}$

Unifikační algoritmus

- postupně od začátku výrazů aplikuje substituce
- buď p nejlevější pozice, na které se nějaké dva výrazy z S liší
- $D(S)$ je množina všech podvýrazů začínajících na pozici p
- $S = \{P(x, y), P(f(x), z), P(z, f(x))\}, p = 3, D(S) = \{x, f(x), z\}$

vstup: konečná množina výrazů $S \neq \emptyset$

výstup: nejobecnější unifikace σ nebo info, že není unifikovatelná

(0) nastav $S_0 := S$, $\sigma_0 := \emptyset$, $k := 0$

(1) pokud $|S_k| = 1$, vrať $\sigma = \sigma_0\sigma_1 \cdots \sigma_k$

(2) zjisti, zda je v $D(S_k)$ proměnná x a term t neobsahující x

(3) pokud ano, nastav $\sigma_{k+1} := \{x/t\}$, $S_{k+1} := S_k\sigma_{k+1}$, $k := k + 1$, a jdi na (1)

(4) pokud ne, odpověz, že S není unifikovatelná

NB: hledání x a t v kroku (2) je relativně výpočetně náročné

Ukázkový běh

$S = S_0 = \{P(f(y, g(z)), h(b)),\ P(f(h(w), g(a)), t),\ P(f(h(b), g(z)), y)\}$

$(k = 0)$ $|S_0| > 1$, $D(S_0) = \{y, h(w), h(b)\}$, proměnná y není v $h(w)$, nastavíme $\sigma_1 := \{y/h(w)\}$ a $S_1 = S_0\sigma_1$

$S_1 = \{P(f(h(w), g(z)), h(b)),\ P(f(h(w), g(a)), t),\ P(f(h(b), g(z)), h(w))\}$

$(k = 1)$ $D(S_1) = \{w, b\}$, $\sigma_2 = \{w/b\}$, $S_2 = S_1\sigma_2$

$S_2 = \{P(f(h(b), g(z)), h(b)),\ P(f(h(b), g(a)), t)\}$

$(k = 2)$ $D(S_2) = \{z, a\}$, $\sigma_3 = \{z/a\}$, $S_3 = S_2\sigma_3$

$S_3 = \{P(f(h(b), g(a)), h(b)),\ P(f(h(b), g(a)), t)\}$

$(k = 3)$ $D(S_3) = \{h(b), t\}$, $\sigma_4 = \{t/h(b)\}$, $S_4 = S_3\sigma_4$

$S_4 = \{P(f(h(b), g(a)), h(b))\}$

$(k = 4)$ $|S_4| = 1$, nejobecnější unifikace pro S je $\sigma = \sigma_1\sigma_2\sigma_3\sigma_4 = \{y/h(w)\}\{w/b\}\{z/a\}\{t/h(b)\} = \{y/h(b), w/b, z/a, t/h(b)\}$

Důkaz korektnosti

Tvrzení: Unifikační algoritmus je korektní. Pro sestrojenou σ navíc platí, že je-li τ libovolná unifikace, potom $\tau = \sigma\tau$.

Důkaz: Algoritmus vždy skončí, neboť v každém kroku eliminuje proměnnou. Skončí-li neúspěchem, nelze unifikovat S_k, tedy ani S.

Odpoví-li $\sigma = \sigma_0\sigma_1 \cdots \sigma_k$, zjevně jde o unifikaci. Zbývá dokázat, že je nejobecnější, k tomu stačí dokázat vlastnost 'navíc': Buď τ lib. unifikace pro S. Indukcí pro $0 \leq i \leq k$ ukážeme $\tau = \sigma_0\sigma_1 \cdots \sigma_i\tau$

(báze indukce) Pro $i = 0$ je $\sigma_0 = \emptyset$, $\tau = \sigma_0\tau$ tedy platí triviálně.

(indukční krok) Buď $\sigma_{i+1} = \{x/t\}$. Ukažme, že pro lib. proměnnou platí: $u\sigma_{i+1}\tau = u\tau$ Z toho okamžitě plyne i $\tau = \sigma_0\sigma_1 \cdots \sigma_i\sigma_{i+1}\tau$.

Pro $u \neq x$ je $u\sigma_{i+1} = u$, tedy i $u\sigma_{i+1}\tau = u\tau$. Je-li $u = x$, máme $u\sigma_{i+1} = x\sigma_{i+1} = t$. Protože τ unifikuje $S_i = S\sigma_0\sigma_1 \cdots \sigma_i$ a $x, t \in D(S_i)$, τ unifikuje i x a t, tzn. $t\tau = x\tau$, tj. $u\sigma_{i+1}\tau = u\tau$. $\square$

8.5 Rezoluční metoda

Příklad rezolučního kroku

Chceme-li ukázat $T \models \varphi$, skolemizací najdeme CNF formuli S ekvisplnitelnou s $T \cup \{\neg\varphi\}$. Stačí najít rezoluční zamítnutí S.

Jediným podstatným rozdílem bude rezoluční pravidlo.

Rezolventou dvojice klauzulí bude klauzule, kterou lze odvodit aplikací (nejobecnější) unifikace. Nejprve příklad:

$C_1 = \{P(x), Q(x, y), Q(x, f(z))\}, C_2 = \{\neg P(u), \neg Q(f(u), u)\}$

Vyberme z C_1 oba pozitivní literály začínající Q, z C_2 negativní.

$S = \{Q(x, y), Q(x, f(z)), Q(f(u), u)\}$ lze unifikovat pomocí nejobecnější unifikace $\sigma = \{x/f(f(z)), y/f(z), u/f(z)\}$

- $C_1\sigma = \{P(f(f(z))), Q(f(f(z)), f(z))\}$
- $C_2\sigma = \{\neg P(f(z)), \neg Q(f(f(z)), f(z))\}$

z nich odvodíme rezolventu $C = \{P(f(f(z))), \neg P(f(z))\}$

Rezoluční pravidlo

Mějme klauzule C_1 a C_2 s disjunktními množinami proměnných 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 $n, m \geq 1$ a $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ lze unifikovat. Buď σ nejobecnější unifikace S. Rezolventa C_1 a C_2 je potom klauzule

$$C = C_1'\sigma \cup C_2'\sigma$$

- Disjunktní množ. proměnných získáme přejmenováním. Proč? Z $\{\{P(x)\}, \{\neg P(f(x))\}\}$ odvodíme $\square$, nahradíme-li $\{P(x)\}$ klauzulí $\{P(y)\}$. Ale $S = \{P(x), P(f(x))\}$ není unifikovatelná.
- Proč potřebujeme z klauzule odstranit více literálů najednou? $S = \{\{P(x), P(y)\}, \{\neg P(x), \neg P(y)\}\}$ je zamítnutelná, ale nemá zamítnutí, které by v každém kroku odstranilo jen jeden.

Rezoluční důkaz

Rezoluční důkaz (odvození) klauzule C z formule S je konečná posloupnost klauzulí $C_0, C_1, \dots, C_n = C$ taková, že pro každé i je buď

- $C_i = C_i'\sigma$ pro nějakou $C_i' \in S$ a přejmenování proměnných σ
- nebo C_i je rezolventou nějakých C_j, C_k kde $j < i$ a $k < i$.

Existuje-li, je C rezolucí dokazatelná z S, $S \vdash_R C$. (Rezoluční) zamítnutí S je rez. důkaz $\square$ z S, potom je S (rezolucí) zamítnutelná.

Příklad

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

rezoluční zamítnutí:

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

rezoluční strom:

$$\begin{tikzcd}[column sep=tiny]
\{\neg P(x,y), \neg P(y,z), P(x,z)\} \arrow[dr, dash] & & \{P(x',f(x'))\} \arrow[dl, dash] & & \{\neg P(x,y), P(y,x)\} \arrow[dr, dash] & & \{P(x',f(x'))\} \arrow[dl, dash] \\
 & y/f(x'), x'/x \quad \{\neg P(f(x),z), P(x,z)\} \arrow[drr, dash] & & & & \{P(f(x'),x')\} \quad x/x', y/f(x') \arrow[dll, dash] & \\
 & & & z/x, x'/x \quad \{P(x,x)\} \arrow[dr, dash] & & \{\neg P(x',x')\} \arrow[dl, dash] & \\
 & & & & x'/x \quad \square & &
\end{tikzcd}$$

8.6 Korektnost a úplnost

Korektnost rezolučního kroku

Tvrzení: Mějme klauzule C_1, C_2 a jejich rezolventu C. Platí-li v nějaké struktuře $\mathcal{A}$ klauzule C_1 a C_2, potom v ní platí i C.

Důkaz: Buď $C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}$, $C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$, a $C = C_1'\sigma \cup C_2'\sigma$, kde $S\sigma = \{A_1\sigma\}$ (a σ je nejobecnější). Klauzule jsou otevřené formule, proto platí i jejich instance:

$$\mathcal{A} \models C_1\sigma \ \text{ a } \ \mathcal{A} \models C_2\sigma$$

Po aplikaci unifikace máme:

$$C_1\sigma = C_1'\sigma \cup \{A_1\sigma\}$$
$$C_2\sigma = C_2'\sigma \cup \{\neg A_1\sigma\}$$

Chceme ukázat, že $\mathcal{A} \models C[e]$ pro lib. ohodnocení e.

- Je-li $\mathcal{A} \models A_1\sigma[e]$, potom $\mathcal{A} \not\models \neg A_1\sigma[e]$ a musí $\mathcal{A} \models C_2'\sigma[e]$. Tedy i $\mathcal{A} \models C[e]$.
- Je-li $\mathcal{A} \not\models A_1\sigma[e]$, musí být $\mathcal{A} \models C_1'\sigma[e]$ a opět $\mathcal{A} \models C[e]$. $\square$

Korektnost rezoluce

Věta (O korektnosti rezoluce): Pokud je CNF formule S rezolucí zamítnutelná, potom je nesplnitelná.

Důkaz: Víme, že $S \vdash_R \square$, vezměme tedy nějaký rezoluční důkaz $\square$ z S. Kdyby existoval model $\mathcal{A} \models S$, díky korektnosti rezolučního pravidla bychom dokázali (indukcí podle délky důkazu) i $\mathcal{A} \models \square$, což ale není možné. $\square$

Lifting lemma

úplnost rezoluce dokážeme převedením na případ výrokové logiky: rezoluční důkaz 'na úrovni VL' je možné 'zvednout' na úroveň PL

Lifting lemma: Buďte C_1 a C_2 klauzule s disj. množ. proměnných, C_1^* a C_2^* jejich základní instance, C^* rezolventa C_1^* a C_2^*. Potom C_1 a C_2 mají rezolventu C takovou, že C^* je základní instance C.

(důkaz na příštím slidu)

Důsledek: Buď S CNF formule a označme S^* množinu všech jejích základních instancí. Pokud $S^* \vdash_R C^*$ pro nějakou základní klauzuli C^* ('na úrovni VL'), potom existuje klauzule C a základní substituce σ taková, že $C^* = C\sigma$ a $S \vdash_R C$ ('na úrovni PL').

Důkaz: Snadno z Lifting lemmatu indukcí dle délky důkazu. $\square$

Důkaz Lifting lemmatu

Nechť $C_1^* = C_1\tau_1$ a $C_2^* = C_2\tau_2$, τ_1 a τ_2 zákl. substituce nesdílející žádnou proměnnou. Najdeme rezolventu C, že $C^* = C\tau_1\tau_2$.

Buď C^* rezolventa C_1^* a C_2^* přes literál $P(t_1, \dots, t_k)$. Víme, že:

$C_1 = C_1' \sqcup \{A_1, \dots, A_n\}$, kde $\{A_1, \dots, A_n\}\tau_1 = \{P(t_1, \dots, t_k)\}$

$C_2 = C_2' \sqcup \{\neg B_1, \dots, \neg B_m\}, \{\neg B_1, \dots, \neg B_m\}\tau_2 = \{\neg P(t_1, \dots, t_k)\}$

Tedy $(\tau_1\tau_2)$ unifikuje $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$. Buď σ nejob. unifikace pro S z Unifikačního algoritmu. Zvolme $C = C_1'\sigma \cup C_2'\sigma$.

$C\tau_1\tau_2 = (C_1'\sigma \cup C_2'\sigma)\tau_1\tau_2 = C_1'\sigma\tau_1\tau_2 \cup C_2'\sigma\tau_1\tau_2 = C_1'\tau_1\tau_2 \cup C_2'\tau_1\tau_2$

$= C_1'\tau_1 \cup C_2'\tau_2 = (C_1 \setminus \{A_1, \dots, A_n\})\tau_1 \cup (C_2 \setminus \{\neg B_1, \dots, \neg B_m\})\tau_2$

$= (C_1^* \setminus \{P(t_1, \dots, t_k)\}) \cup (C_2^* \setminus \{\neg P(t_1, \dots, t_k)\}) = C^*$

Zde $=$ plyne z vlastnosti 'navíc' Unif. algoritmu $(\tau_1\tau_2) = \sigma(\tau_1\tau_2)$, a $=$ z toho, že jde o základní substituce nesdílející proměnnou. $\square$

Úplnost rezoluce

Věta (O úplnosti rezoluce): Je-li CNF formule S nesplnitelná, potom je zamítnutelná rezolucí.

Důkaz: Množina S^* všech základních instancí klauzulí z S je také nesplnitelná (důsledek Herbrandovy věty). Úplnost výrokové rezoluce dává $S^* \vdash_R \square$ ('na úrovni VL').

Z důsledku Lifting lemmatu dostáváme klauzuli C a základní substituci σ takové, že $C\sigma = \square$ a $S \vdash_R C$ ('na úrovni PL').

Ale protože prázdná klauzule $\square$ je instancí C, musí být $C = \square$. Tím jsme našli rezoluční zamítnutí $S \vdash_R \square$. $\square$

Jedenáctá přednáška

Program

- LI-rezoluce a Prolog
- elementární ekvivalence
- izomorfismus a konečné modely
- definovatelnost a automorfismy
- ω-kategoricita a úplnost

Materiály

Zápisky z přednášky, Sekce 8.7 z Kapitoly 8, Sekce 9.1-9.3 z Kapitoly 9

8.7 LI-rezoluce (více podrobností ve skriptech, VL v Sekci 5.4)

Lineární důkaz a LI-důkaz

- Lineární důkaz klauzule C z formule S je konečná posloupnost

$$\begin{bmatrix} C_0 \\ B_0 \end{bmatrix}, \begin{bmatrix} C_1 \\ B_1 \end{bmatrix}, \ldots, \begin{bmatrix} C_n \\ B_n \end{bmatrix}, C_{n+1}$$

  kde: B_0 a C_0 jsou varianty klauzulí z S, $C_{n+1} = C$,
  - C_{i+1} je rezolventa C_i a B_i
  - B_i varianta klauzule z S nebo $B_i = C_j$ pro nějaké $j < i$.
- Lineární zamítnutí S je lineární důkaz $\square$ z S
- LI-důkaz je lin. důkaz, kde vš. B_i jsou varianty klauzulí z S
- C LI-dokazatelná z S, $S \vdash_{LI} C$, pokud existuje LI-důkaz
- S je LI-zamítnutelná, pokud $S \vdash_{LI} \square$
- korektnost (lineární i LI-rezoluce) je zřejmá

Úplnost LI-rezoluce pro Hornovy formule

Věta (O úplnosti lineární rezoluce): C má lineární důkaz z S, právě když má rezoluční důkaz z S (tj. $S \vdash_R C$).

Důkaz: převodem na VL (Lifting lemma zachovává linearitu) $\square$

Věta (O úplnosti LI-rezoluce pro Hornovy formule): Je-li Hornova formule T splnitelná, a $T \cup \{G\}$ je nesplnitelná pro cíl G, potom $T \cup \{G\} \vdash_{LI} \square$, a to LI-zamítnutím, které začíná cílem G.

Důkaz: úplnost ve VL + Herbrandova věta + Lifting lemma $\square$

- Hornova formule: množina Hornových klauzulí
- Hornova klauzule: nejvýše jeden pozitivní literál
- Pravidlo: klauzule s 1 pozitivním a alespoň 1 negativním literálem
- Fakt: pozitivní jednotková klauzule
- Cíl: neprázdná klauzule bez pozitivního literálu
- Programové klauzule: pravidla a fakta
- Program: Hornova formule obsahující jen programové klauzule

Program v Prologu

```
son(X,Y):-father(Y,X),man(X).
son(X,Y):-mother(Y,X),man(X).
man(charlie).
father(bob,charlie).
mother(alice,charlie).

?-son(charlie,X).
```

$\{son(X,Y), \neg father(Y,X), \neg man(X)\}$

$\{son(X,Y), \neg mother(Y,X), \neg man(X)\}$

$\{man(charlie)\}$

$\{father(bob, charlie)\}$

$\{mother(alice, charlie)\}$

$\{\neg son(charlie, X)\}$

LI-rezoluce v Prologu

Platí v programu daný existenční dotaz, $P \models (\exists X) son(charlie, X)$?

Důsledek: Pro program P a cíl $G = \{\neg A_1, \dots, \neg A_k\}$ v proměnných $X_1, \dots, X_n$ jsou následující ekvivalentní:

- $P \models (\exists X_1) \dots (\exists X_n)(A_1 \wedge \dots \wedge A_k)$
- $P \cup \{G\}$ má LI-zamítnutí začínající G

Důkaz: Plyne z Důkazu sporem a Úplnosti LI-rezoluce pro Hornovy formule (Program je vždy splnitelný). $\square$

Je-li odpověď na dotaz kladná, chceme znát i výstupní substituci σ, tj. složení unifikací z rez. kroků, zúžené na proměnné v G. Platí:

$$P \models (A_1 \wedge \dots \wedge A_k)\sigma$$

Příklady

`?-son(charlie,X).`

$\{\neg son(c,X)\}$ — $\{\neg father(X,c), \neg man(c)\}$ – $\{\neg father(X,c)\}$ – $\square$

$\{son(X',Y'), \neg father(Y',X'), \neg man(X')\}$ $\quad$ $\{man(c)\}$ $\quad$ $\{father(b,c)\}$

$\{X'/c, Y'/X\}$ $\quad$ $\emptyset$ $\quad$ $\{X/b\}$

`X=bob` výstupní substituce $\sigma = \{X/b\}$

$\{\neg son(c,X)\}$ — $\{\neg mother(X,c), \neg man(c)\}$ – $\{\neg mother(X,c)\}$ – $\square$

$\{son(X',Y'), \neg mother(Y',X'), \neg man(X')\}$ $\quad$ $\{man(c)\}$ $\quad$ $\{mother(a,c)\}$

$\{X'/c, Y'/X\}$ $\quad$ $\emptyset$ $\quad$ $\{X/a\}$

`X=alice` výstupní substituce $\sigma = \{X/a\}$

ČÁST III – POKROČILÉ PARTIE

Kapitola 9: Teorie modelů

Teorie modelů

- vztah mezi vlastnostmi teorií a tříd jejich modelů
- bližší matematice než informatice a aplikacím
- jen několik vybraných dostupných výsledků

\+ co je třeba pro Gödelovy věty (Kapitola 10)

\+ co se nevešlo jinam

9.1 Elementární ekvivalence

Teorie struktury

Teorie struktury $\mathcal{A}$ (v jazyce L):

$$\mathrm{Th}(\mathcal{A}) = \{\varphi \mid \varphi \text{ je } L\text{-sentence a } \mathcal{A} \models \varphi\}$$

Např. pro standardní model aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ říkáme $\mathrm{Th}(\underline{\mathbb{N}})$ aritmetika přirozených čísel, je nerozhodnutelná (neexistuje algoritmus, který pro každou φ doběhne a odpoví, zda $T \models \varphi$)

Pozorování: Nechť $\mathcal{A}$ je L-struktura a T je L-teorie.

- $\mathrm{Th}(\mathcal{A})$ je kompletní teorie
- $\mathcal{A} \in \mathrm{M}_L(T) \Rightarrow \mathrm{Th}(\mathcal{A})$ je (kompletní) jednoduchá extenze T
- $\mathcal{A} \in \mathrm{M}_L(T)$, T kompletní $\Rightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Csq}_L(T) \sim T$

Elementární ekvivalence

L-struktury $\mathcal{A}$ a $\mathcal{B}$ jsou elementárně ekvivalentní ($\mathcal{A} \equiv \mathcal{B}$), pokud v nich platí tytéž L-sentence, neboli: $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$

Například pro $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{Z}, \leq \rangle$

- $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$: snadno pomocí hustoty
- $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$: v $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, v $\langle \mathbb{Q}, \leq \rangle$ ne, tedy $\varphi \in \mathrm{Th}(\langle \mathbb{Z}, \leq \rangle) \setminus \mathrm{Th}(\langle \mathbb{Q}, \leq \rangle)$ pro následující sentenci:

$$\varphi = (\forall x)(\exists y)(x \leq y \wedge \neg x = y \wedge (\forall z)(x \leq z \rightarrow z = x \vee y \leq z))$$

Kompletní jednoduché extenze

Pro teorii T nás hlavně zajímá, jak vypadají modely.

- T je kompletní, právě když má jediný model až na elementární ekvivalenci (všechny modely jsou elementárně ekvivalentní)
- Modely T až na elementární ekvivalenci jednoznačně odpovídají kompletním jednoduchým extenzím T, ty jsou tvaru $\mathrm{Th}(\mathcal{A})$ pro $\mathcal{A} \in \mathrm{M}(T)$, kde $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$

Místo hledání modelů stačí najít kompletní jednoduché extenze!

Motivace: ukážeme, že lze-li efektivně popsat všechny kompletní jednoduché extenze efektivně dané teorie, potom je rozhodnutelná.

- algoritmus, který pro vstup (i, j) vypíše j-tý axiom i-té kompletní jednoduché extenze (v nějakém očíslování)
- algoritmus, který postupně vygeneruje všechny axiomy teorie

Schopnost efektivně popsat kompletní jedn. extenze je vzácná, vyžaduje silné předpoklady, ale u mnoha důležitých teorií to lze.

Příklad: DeLO*

Teorie hustého lin. uspořádání (DeLO*) je extenze teorie uspořádání o linearitu (dichotomii), hustotu, a někdy se přidává netrivialita:

- $x \leq y \vee y \leq x$
- $x \leq y \wedge \neg\, x = y \rightarrow (\exists z)(x \leq z \wedge z \leq y \wedge \neg\, z = x \wedge \neg\, z = y)$
- $(\exists x)(\exists y)(\neg\, x = y)$

Tvrzení: Buď $\varphi = (\exists x)(\forall y)(x \leq y)$ a $\psi = (\exists x)(\forall y)(y \leq x)$. Následující jsou právě všechny kompletní jednoduché extenze DeLO* (až na ekvivalenci):

- $\mathrm{DeLO} = \mathrm{DeLO}^* \cup \{\neg\varphi, \neg\psi\}$
- $\mathrm{DeLO}^- = \mathrm{DeLO}^* \cup \{\varphi, \neg\psi\}$
- $\mathrm{DeLO}^+ = \mathrm{DeLO}^* \cup \{\neg\varphi, \psi\}$
- $\mathrm{DeLO}^\pm = \mathrm{DeLO}^* \cup \{\varphi, \psi\}$

Stačí ukázat, že jsou kompletní. Potom už je zřejmé, že žádná další kompletní jednoduchá extenze DeLO* nemůže existovat.

Jak ukážeme, kompletnost plyne z faktu, že jsou ω-kategorické, tj. mají jediný spočetný model až na izomorfismus.

Důsledky Löwenheim-Skolemovy věty bez rovnosti

Připomeňme:

Věta (L.-S. bez rovnosti): Ve spočetném jazyce bez rovnosti má každá bezesporná teorie spočetně nekonečný model.

Jednoduchý důsledek:

Důsledek: Je-li L spočetný bez rovnosti, potom ke každé L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz: $\mathrm{Th}(\mathcal{A})$ je bezesporná (má model $\mathcal{A}$), tedy dle L.-S. věty má spočetně nekonečný model $\mathcal{B} \models \mathrm{Th}(\mathcal{A})$, to znamená $\mathcal{B} \equiv \mathcal{A}$. $\square$

Bez rovnosti tedy nelze vyjádřit např. ‘model má právě 42 prvků’.

Důsledky Löwenheim-Skolemovy věty s rovností

V důkazu L.-S. věty máme kanonický model pro bezespornou větev tabla z T pro $\mathrm{F}\bot$; pro jazyk s rovností stačí faktorizovat dle $=^A$:

Věta (L.-S. s rovností): Ve spočetném jazyce s rovností má každá bezesporná teorie spočetný model (konečný, nebo nekonečný).

I tato verze má snadný důsledek pro konkrétní struktury:

Důsledek: Je-li L spočetný s rovností, ke každé nekonečné L-struktuře existuje elem. ekvivalentní spočetně nekonečná struktura.

Důkaz: Mějme nekonečnou L-strukturu $\mathcal{A}$. Podobně jako v důkazu Důsledku bez rovnosti najdeme spočetnou $\mathcal{B} \equiv \mathcal{A}$.

Protože v $\mathcal{A}$ platí pro kažné $n \in \mathbb{N}$ sentence vyjadřující 'existuje alespoň n prvků' (což lze pomocí rovnosti snadno zapsat), platí i v $\mathcal{B}$, tedy $\mathcal{B}$ musí být nekonečná. $\square$

Spočetné algebraicky uzavřené těleso

- algebraicky uzavřené těleso: každý polynom nenulového stupně v něm má kořen
- $\mathbb{Q}$ není, $x^2 - 2$ nemá v $\mathbb{Q}$ kořen
- $\mathbb{R}$ není, $x^2 + 1$ nemá v $\mathbb{R}$ kořen
- $\mathbb{C}$ je algebraicky uzavřené, ale je nespočetné

Algebraickou uzavřenost vyjádříme sentencemi ψ_n, pro $n > 0$:

$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \cdots + x_1 \cdot y + x_0) = 0$$

kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$

Důsledek: Existuje spočetné algebraicky uzavřené těleso.

Důkaz: Dle Důsledku L.S. věty (s rovností) existuje spočetně nekonečná $\mathcal{A} \equiv \mathbb{C}$. Protože $\mathbb{C}$ je těleso a splňuje ψ_n pro všechna $n > 0$, je i $\mathcal{A}$ algebraicky uzavřené těleso. $\square$

9.2 Izomorfismus struktur

Definice izomorfismu

Izomorfismus $\mathcal{A}$ a $\mathcal{B}$ (v $L = \langle \mathcal{R}, \mathcal{F} \rangle$) je bijekce $h \colon A \to B$ splňující:

- pro každý (n-ární) $f \in \mathcal{F}$ a pro všechna $a_i \in A$:

$$h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$

- speciálně, je-li $c \in \mathcal{F}$ konstantní: $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$
- pro každý (n-ární) $R \in \mathcal{R}$ a pro všechna $a_i \in A$:

$$R^{\mathcal{A}}(a_1, \dots, a_n) \ \text{ právě když } \ R^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$

Existuje-li, jsou izomorfní ('via h'), $\mathcal{A} \simeq \mathcal{B}$ (nebo $\mathcal{A} \simeq_h \mathcal{B}$).

Automorfismus $\mathcal{A}$ je izomorfismus $\mathcal{A}$ a $\mathcal{A}$.

- tj. liší se jen 'pojmenováním prvků'
- relace 'být izomorfní' je ekvivalence
- např. potenční algebra $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$, $|X| = n$, je izomorfní s $\underline{2^n} = \langle \{0,1\}^n, -_n, \wedge_n, \vee_n, (0, \dots, 0), (1, \dots, 1) \rangle$ (operace po složkách) via $h(A) = \chi_A$ (charakt. vektor $A \subseteq X$)

Izomorfismus zachovává sémantiku & vztah $\simeq$ a $\equiv$

Tvrzení: Bijekce $h\colon A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$, právě když:

(i) pro každý term t a $e : \mathrm{Var} \to A$: $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[e \circ h]$

(ii) pro každou φ a $e : \mathrm{Var} \to A$: $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[e \circ h]$

Důkaz: $\Rightarrow$ snadno indukcí podle struktury termu resp. formule

$\Leftarrow$ je-li h bijekce splňující (i)&(ii), dosazení $t = f(x_1, \ldots, x_n)$ resp. $\varphi = R(x_1, \ldots, x_n)$ dává vlastnosti z definice izomorfismu $\square$

Důsledek: $\mathcal{A} \simeq \mathcal{B} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{B}$.

Důkaz: pro každou sentenci φ máme z (ii) $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$ $\square$

Naopak obecně ne, $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle \not\simeq \langle \mathbb{R}, \leq \rangle$ Platí ale:

Tvrzení: Jsou-li $\mathcal{A}, \mathcal{B}$ konečné v jazyce s rovností, potom

$$\mathcal{A} \simeq \mathcal{B} \;\Leftrightarrow\; \mathcal{A} \equiv \mathcal{B}$$

Důsledek Pokud má kompletní teorie v jazyce s rovností konečný model, potom jsou všechny její modely izomorfní.

Důkaz $\equiv \Rightarrow \simeq$ pro konečné struktury s rovností

Díky $=$ vyjádříme "existuje právě n prvků", z toho plyne $|A| = |B|$.
Buď $\mathcal{A}'$ expanze $\mathcal{A}$ o jména prvků, v jazyce $L' = L \cup \{c_a \mid a \in A\}$.
Ukážeme: $\mathcal{B}$ lze expandovat na L'-strukturu $\mathcal{B}'$ že $\mathcal{A}' \equiv \mathcal{B}'$.Potom je $h(a) = c_a^{\mathcal{B}'}$ izomorfismus $\mathcal{A}'$ a $\mathcal{B}'$, i pro L-redukty $\mathcal{A} \simeq \mathcal{B}$.

Stačí ukázat, že pro $c_a^{\mathcal{A}'} = a \in A$ existuje $b \in B$ tak, že expanze o interpretaci konstantního symbolu c_a splňují $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.

Buď Ω množina 'vlastností prvku a', tj. formulí $\varphi(x)$ splňujících $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, neboli $\mathcal{A} \models \varphi[e(x/a)]$. Protože je A konečná, existuje konečně mnoho $\varphi_1(x), \ldots, \varphi_m(x)$ tak, že pro každou $\varphi \in \Omega$ existuje i takové, že $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$. Potom i $\mathcal{B} \models \varphi \leftrightarrow \varphi_i$.

Protože v $\mathcal{A}$ platí sentence $(\exists x) \bigwedge_{i=1}^{m} \varphi_i$ (je splněna díky $a \in A$) a $\mathcal{B} \equiv \mathcal{A}$, máme i $\mathcal{B} \models (\exists x) \bigwedge_{i=1}^{m} \varphi_i$. Neboli existuje $b \in B$ takové, že $\mathcal{B} \models \bigwedge_{i=1}^{m} \varphi_i[e(x/b)]$. Tedy pro každou $\varphi \in \Omega$ platí $\mathcal{B} \models \varphi[e(x/b)]$, tj. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$, z toho $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$. $\square$

Definovatelnost a automorfismy

definovatelné množiny jsou invariantní na automorfismy (např. automorfismus grafu musí zobrazit trojúhelník na trojúhelník):

Tvrzení: Je-li $D \subseteq A^n$ definovatelná v $\mathcal{A}$, potom pro každý automorfismus $h \in \mathrm{Aut}(\mathcal{A})$ platí $h[D] = D$ (kde $h[D]$ značí $\{(h(\overline{a}) \mid \overline{a} \in D\})$. Je-li definovatelná s parametry $\overline{b}$, platí to pro automorfismy identické na $\overline{b}$ (tj. $h(\overline{b}) = \overline{b}$ neboli $h(b_i) = b_i$ pro všechna i).

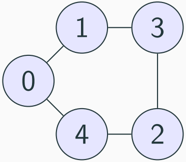
Důkaz: Ukážeme jen verzi s parametry. Nechť $D = \varphi^{\mathcal{A},\overline{b}}(\overline{x}, \overline{y})$. Potom pro každé $\overline{a} \in A^n$ platí následující ekvivalence:

$$\begin{aligned}
\overline{a} \in D \;&\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/\overline{a}, \overline{y}/\overline{b})] \\
&\Leftrightarrow\; \mathcal{A} \models \varphi[(e \circ h)(\overline{x}/\overline{a}, \overline{y}/\overline{b})] \\
&\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/h(\overline{a}), \overline{y}/h(\overline{b}))] \\
&\Leftrightarrow\; \mathcal{A} \models \varphi[e(\overline{x}/h(\overline{a}), \overline{y}/\overline{b})] \\
&\Leftrightarrow\; h(\overline{a}) \in D.
\end{aligned}$$

$\square$

Příklad

Množiny definovatelné s parametrem 0, $\mathrm{Df}^1(\mathcal{G}, \{0\})$?



Jediný netriviální automorfismus zachovávající 0:

$h(i) = (5 - i) \bmod 5$, orbity $\{0\}$, $\{1, 4\}$, a $\{2, 3\}$.

Tyto množiny jsou definovatelné:

- $\{0\}$ formulí $x = y$, tj. $(x = y)^{\mathcal{G}, \{0\}} = \{0\}$
- $\{1, 4\}$ lze definovat pomocí $E(x, y)$
- $\{2, 3\}$ formulí $\neg E(x, y) \wedge \neg x = y$

$\mathrm{Df}^1(\mathcal{G}, \{0\})$ je podalgebra $\underline{\mathcal{P}(V(\mathcal{G}))}$, tedy uzavřená na doplněk, sjednocení, průnik, obsahuje $\emptyset$ a $V(\mathcal{G})$. Podalgebra generovaná $\{\{0\}, \{1, 4\}, \{2, 3\}\}$ už ale obsahuje všechny podmnožiny zachovávající automorfismus h. Dostáváme:

$$\mathrm{Df}^1(\mathcal{G}, \{0\}) = \{\emptyset, \{0\}, \{1, 4\}, \{2, 3\}, \{0, 1, 4\}, \{0, 2, 3\},$$
$$\{1, 4, 2, 3\}, \{0, 1, 2, 3, 4\}\}$$

9.3 ω-kategorické teorie

ω-kategorické teorie

Izomorfní spektrum T je počet modelů T kardinality κ až na $\simeq$.
T je κ-kategorická pokud $I(\kappa, T) = 1$, ω-kategorická má-li jediný spočetně nekonečný model až na izomorfismus.

Tvrzení: Teorie DeLO je ω-kategorická.

Důkaz: Buďte $\mathcal{A}, \mathcal{B}$ spočetně nekonečné modely, $A = \{a_i \mid i \in \mathbb{N}\}$, $B = \{b_i \mid i \in \mathbb{N}\}$. Z hustoty najdeme indukcí $h_0 \subseteq h_1 \subseteq h_2 \subseteq \dots$ prosté parciální fce z A do B zach. usp., $\{a_0, \dots, a_{n-1}\} \subseteq \operatorname{dom} h_n$, $\{b_0, \dots, b_{n-1}\} \subseteq \operatorname{rng} h_n$. Potom $\mathcal{A} \simeq \mathcal{B}$ via $h = \bigcup_{n \in \mathbb{N}} h_n$. $\square$

Důsledek: Izomorfní spektrum teorie DeLO*:

- $I(\kappa, DeLO^*) = 0$ pro $\kappa \in \mathbb{N}$
- $I(\omega, DeLO^*) = 4$

Spočetné modely až na izomorfismus jsou například:

$$\mathbb{Q} = \langle \mathbb{Q}, \leq \rangle \simeq \mathbb{Q} \restriction (0,1),\ \mathbb{Q} \restriction (0,1],\ \mathbb{Q} \restriction [0,1),\ \mathbb{Q} \restriction [0,1]$$

Důkaz: Husté uspořádání nemůže být konečné. Izomorfismus zobrazí minimum na minimum a maximum na maximum. $\square$

ω-kategorické kritérium kompletnosti

Věta: Buď T ω-kategorická ve spočetném jazyce L. Je-li

(i) L bez rovnosti, nebo

(ii) L s rovností a T nemá konečné modely,

potom je T kompletní.

Důkaz:(i) Důsledek L.-S. věty bez rovnosti říká, že každý model je elementárně ekvivalentní nějakému spočetně nekonečnému, ten je ale až na izomorfismus jediný.

(ii) Důsledek L.-S. věty s rovností podobně říká, že všechny nekonečné modely jsou elementárně ekvivalentní. Mohla by mít elementárně neekvivalentní konečné modely, to jsme ale zakázali. □

Důsledek: DeLO, DeLO$^+$, DeLO$^-$, a DeLO$^\pm$ jsou kompletní, jsou to všechny (navzájem neekvivalentní) kompletní jedn. extenze $DeLO^*$.

Analogické kritérium platí i pro kardinality κ větší než ω.

Dvanáctá přednáška

Program

- axiomatizovatelnost
- rekurzivní axiomatizace a rozhodnutelnost
- aritmetické teorie
- nerozhodnutelnost predikátové logiky
- Gödelovy věty o neúplnosti

Materiály

Zápisky z přednášky, Sekce 9.4 z Kapitoly 9, Kapitola 10

9.4 Axiomatizovatelnost

Axiomatizovatelnost

Třída struktur $K \subseteq \mathrm{M}_L$ je:

- axiomatizovatelná, existuje-li teorie T taková, že $\mathrm{M}_L(T) = K$
- konečně/otevřeně axiomatiz., je-li ax. konečnou/otevřenou T
- teorie T' je konečně/otevřeně axiomatizovatelná, platí-li to o třídě jejích modelů $K = \mathrm{M}_L(T')$

Pozorování: Je-li K axiomatizovatelná, musí být uzavřená na $\equiv$.

Například, jak ukážeme:

- grafy a částečná uspořádání jsou konečně i otevřeně ax.
- tělesa jsou konečně, ale ne otevřeně axiomatizovatelná
- nekonečné grupy jsou axiomatizovatelné, ale ne konečně
- konečné grafy nejsou axiomatizovatelné

Neaxiomatizovatelnost konečných modelů

Věta: Má-li T libovolně velké konečné modely, má i nekonečný model. Potom není třída jejích konečných modelů axiomatizovatelná.

Důkaz: Je-li jazyk bez rovnosti, vezmeme kanonický model pro bezespornou větev v tablu z T pro $\mathrm{F}\bot$ (T je bezesporná).

Je-li jazyk s rovností, přidáme spočetně mnoho nových konst. symbolů c_i a vezmeme extenzi: $T' = T \cup \{\neg c_i = c_j \mid i \neq j \in \mathbb{N}\}$

Každá konečná část T' má model: buď k největší, že c_k je v této konečné části: lib. $\geq (k+1)$-prvkový model,21 interpretuj $c_0, \ldots, c_k$ jako různé prvky.

Věta o kompaktnosti dává model T', ten je nekonečný, redukt na původní jazyk (zapomenutí $c_i^{\mathcal{A}}$) je nekonečný model T. $\square$

- např. konečné grafy nejsou axiomatizovatelné
- nekonečné modely teorie jsou vždy axiomatizovatelné, máme-li rovnost: stačí přidat 'existuje alespoň n prvků' pro vš. $n \in \mathbb{N}$

Konečná axiomatizovatelnost

Věta (O konečné axiomatizovatelnosti): $K \subseteq \mathrm{M}_L$ je konečně axiomatizovatelná, právě když K i $\overline{K} = \mathrm{M}_L \setminus K$ jsou axiomatizovatelné.

Důkaz: $\Rightarrow$ Je-li K axiomatizovatelná sentencemi $\varphi_1, \dots, \varphi_n$ (vezmi gen. uzávěry), potom $\neg(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n)$ axiomatizuje $\overline{K}$.

$\Leftarrow$ Buď $K = \mathrm{M}(T)$ a $\overline{K} = \mathrm{M}(S)$. Potom $T \cup S$ je sporná, neboť:

$$\mathrm{M}(T \cup S) = \mathrm{M}(T) \cap \mathrm{M}(S) = K \cap \overline{K} = \emptyset$$

Věta o kompaktnosti dává konečné $T' \subseteq T$ a $S' \subseteq S$ takové, že:

$$\emptyset = \mathrm{M}(T' \cup S') = \mathrm{M}(T') \cap \mathrm{M}(S')$$

Nyní si všimněme, že platí:

$$\mathrm{M}(T) \subseteq \mathrm{M}(T') \subseteq \overline{\mathrm{M}(S')} \subseteq \overline{\mathrm{M}(S)} = \mathrm{M}(T)$$

Tím jsme dokázali, že $M(T) = M(T')$, neboli T' je konečná axiomatizace K. $\square$

Tělesa charakteristiky 0 nejsou konečně axiomatizovatelná

Buď T teorie těles. Těleso $\mathcal{A} = \langle A, +, -, 0, \cdot, 1\rangle$ je

- charakteristiky p, je-li p nejmenší prvočíslo takové, že $\mathcal{A} \models p1 = 0$, kde $p1$ je term $1 + 1 + \cdots + 1$ (s p jedničkami),
- charakteristiky 0, pokud není charakteristiky p pro žádné p.
- Tělesa charakteristiky p jsou konečně axiomatizovatelná:
$$T_p = T \cup \{p1 = 0\}$$
- Tělesa char. 0 jsou axiomatizovatelná, ale ne konečně:
$$T_0 = T \cup \{\neg\, p1 = 0 \mid p \text{ prvočíslo}\}$$

Tvrzení: Třída K těles char. 0 není konečně axiomatizovatelná.

Důkaz: Stačí ukázat, že $\overline{K}$ (tělesa nenulové char. a netělesa) není axiomatizovatelná. Sporem: $\overline{K} = \mathrm{M}(S)$. Potom $S' = S \cup T_0$ má model, neboť každá konečná část má model: těleso charakteristiky větší než jakékoliv p z axiomu T_0 tvaru $\neg\, p1 = 0$. Je-li $\mathcal{A}$ je model S', potom $\mathcal{A} \in \mathrm{M}(S) = \overline{K}$. Zároveň ale $\mathcal{A} \in \mathrm{M}(T_0) = K$, spor. $\square$

Otevřená axiomatizovatelnost

Tvrzení: Je-li T otevřeně axiomatizovatelná, potom je každá podstruktura modelu T také modelem T.

Důkaz: Buď T' otevřená axiomatizace T, $\mathcal{A}$ model T', $\mathcal{B} \subseteq \mathcal{A}$. Pro každou $\varphi \in T'$ platí $\mathcal{B} \models \varphi$ (φ je otevřená), tedy i $\mathcal{B} \models T'$. □

Poznámka: Platí i obráceně, je-li každá podstruktura modelu také model, potom je otevřeně axiomatizovatelná. (Důkaz neuvedeme.)

- DeLO není otevřeně axiomatizovatelná, např. žádná konečná podstruktura modelu DeLO není hustá
- teorie těles není otevřeně axiomatizovatelná, podstruktura $\mathbb{Z} \subseteq \mathbb{Q}$ není těleso, nemá inverzní prvek k 2 vůči násobení
- pro dané $n \in \mathbb{N}$ jsou nejvýše n-prvkové grupy otevřeně axiomatizovatelné (i jejich podgrupy jsou nejvýše n-prvkové); k (otevřené) teorii grup stačí přidat: $\bigvee_{1 \leq i < j \leq n+1} x_i = x_j$

Kapitola 10: Nerozhodnutelnost a neúplnost

Nerozhodnutelnost a neúplnost

Jak lze s teoriemi pracovat algoritmicky?

+ zlatý hřeb přednášky: Gödelovy věty o neúplnosti (1931)

- ukazují limity formálního přístupu
- zastavily program formalizace matematiky
- pojem algoritmu budeme chápat jen intuitivně
- technické podrobnosti důkazů vynecháme

Typicky potřebujeme spočetný jazyk.

10.1 Rekurzivní axiomatizace a rozhodnutelnost

Rekurzivní axiomatizace

- v dokazování povolujeme nekonečné teorie, jak jsou zadané?
- pro ověření že daný důkaz (např. tablo, rezoluční zamítnutí) je korektní potřebujeme algoritmický přístup ke všem axiomům
- mohli bychom požadovat enumerátor pro T, tj. algoritmus, který vypisuje axiomy z T, a každý axiom někdy vypíše
- ale kdyby byl v důkazu chybný axiom, nikdy bychom se to nedozvěděli: stále bychom čekali, zda ho enumerátor vypíše
- proto požadujeme silnější vlastnost:

T je rekurzivně axiomatizovaná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $\varphi \in T$.

(ekvivalentní enumerátoru vypisujícímu axiomy v lexikograf. pořadí)

Rozhodnutelnost

Můžeme v dané teorii 'algoritmicky rozhodovat pravdu'?

- T je rozhodnutelná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $T \models \varphi$,
- T je částečně rozhodnutelná, existuje-li algoritmus, který:
  - pokud $T \models \varphi$, doběhne a odpoví "ano"
  - pokud $T \not\models \varphi$, buď nedoběhne, nebo doběhne a odpoví "ne"

Tvrzení: Je-li T je rekurzivně axiomatizovaná, potom:
(i) T je část. rozhod. (ii) je-li navíc kompletní, je rozhodnutelná

Důkaz: (i) Algoritmus konstruuje systematické tablo z T pro $\mathrm{F}\varphi$; stačí enumerátor pro T, nebo postupně generovat vš. sentence a testovat, jsou-li v T. Je-li $T \models \varphi$, konstrukce skončí, ověříme, že je tablo sporné. (Jinak skončit nemusí.)

(ii) Víme, že buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$. Paralelně konstruujeme tablo pro $\mathrm{F}\varphi$ a pro $\mathrm{T}\varphi$ (důkaz a zamítnutí φ z T). Jedna z konstrukcí po konečně mnoha krocích skončí. $\square$

Rekurzivně spočetná kompletace

T má rekurzivně spočetnou kompletaci, je-li (nějaká) množina až na $\sim$ všech kompletních jednoduchých extenzí T spočetná, a rekurzivně spočetná, tj. existuje algoritmus, který pro vstup (i, j) vypíše i-tý axiom j-té extenze (v nějakém uspořádání), nebo odpoví, že už neexistuje.

Tvrzení: Je-li T rekurzivně axiomatizovaná a má rekurzivně spočetnou kompletaci, potom je rozhodnutelná.

Důkaz: Buď $T \vdash \varphi$, nebo existuje protipříklad $\mathcal{A} \not\models \varphi$, tj. kompl. jedn. extenze T_i, že $T_i \not\vdash \varphi$. Kompletnost T_i dává $T_i \vdash \neg\varphi$.

Algoritmus paralelně konstruuje tablo důkaz φ z T a (postupně) tablo důkazy $\neg\varphi$ ze všech kompletních jedn. extenzí $T_1, T_2, \ldots$. (Je-li jich nekonečně mnoho, uděláme dovetailing: 1. krok 1. tabla, potom 2. krok 1., 1. krok 2., 3. krok 1., 2. krok 2., 1. krok 3., atd.)

Alespoň jedno z tabel je sporné, můžeme předpokládat konečné, algoritmus ho po konečně mnoha krocích zkonstruuje. $\square$

Příklady

Následující teorie jsou rekurzivně axiomatizované a mají rekurzivně spočetnou kompletaci, tedy jsou rozhodnutelné:

(a) Teorie čisté rovnosti
(b) Teorie unárního predikátu ($T = \emptyset$, $L = \langle U \rangle$ s rovností)
(c) Teorie hustých lineárních uspořádání DeLO*
(d) Teorie Booleových algeber (Alfred Tarski 1940),
(e) Teorie algebraicky uzavřených těles (Tarski 1949),
(f) Teorie komutativních grup (Wanda Szmielew 1955).

Rekurzivní axiomatizovatelnost

Kdy lze třídu struktur 'efektivně (algoritmicky) popsat'?

$K \subseteq \mathrm{M}_L$ je rek. axiomatizovatelná, pokud existuje rek. axiomatizovaná T, že $K = M_L(T)$. T' je rek. axiomatizovatelná, platí-li to pro třídu jejích modelů (tj. je-li ekvivalentní rek. axiomatizované teorii).

(podobně lze definovat rek. spočetnou axiomatizovatelnost)

Tvrzení: Je-li $\mathcal{A}$ konečná struktura v konečném jazyce s rovností, potom je teorie $\mathrm{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná.

(z toho plyne i rozhodnutelnost $\mathrm{Th}(\mathcal{A})$, ale $\mathcal{A} \models \varphi$ lze ověřit přímo)

Důkaz: Buď $A = \{a_1, \ldots, a_n\}$. $\mathrm{Th}(\mathcal{A})$ axiomatizujeme sentencí "existuje právě n prvků $a_1, \ldots, a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí v $\mathcal{A}$".

Např. je-li $f^{\mathcal{A}}(a_4, a_2) = a_{17}$, přidej atom. formuli $f(x_{a_4}, x_{a_2}) = x_{a_{17}}$, je-li $(a_3, a_3, a_1) \notin R^{\mathcal{A}}$ přidej $\neg R(x_{a_3}, x_{a_3}, x_{a_1})$. $\square$

Příklady

Pro následující struktury je $\mathrm{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná:

- $\langle \mathbb{Z}, \leq \rangle$, jde o tzv. teorii diskrétních lineárních uspořádání
- $\langle \mathbb{Q}, \leq \rangle$, jde o teorii DeLO
- $\langle \mathbb{N}, S, 0 \rangle$, teorie následníka s nulou
- $\langle \mathbb{N}, S, +, 0 \rangle$, Presburgerova aritmetika
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorie reálně uzavřených těles, znamená že lze algoritmicky rozhodovat Euklid. geometrii (Tarski, 1949)
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorie algebraicky uzavřených těles char. 0

Důsledek: Pro struktury výše platí, že $\mathrm{Th}(\mathcal{A})$ je rozhodnutelná.

Důkaz: $\mathrm{Th}(\mathcal{A})$ je vždy kompletní.

Teorie standardního modelu aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ ale není rekurzivně axiomatizovatelná (viz První Gödelova věta o neúplnosti).

10.2 Aritmetika

Aritmetika

- přirozená čísla hrají důležitou roli v matematice i v aplikacích
- jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností
- standardní model aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ nemá rekurzivně axiomatizovatelnou teorii (První věta o neúplnosti)
- proto používáme rekurzivně axiomatizované teorie, které vlastnosti $\underline{\mathbb{N}}$ popisují částečně; říkáme jim aritmetiky
- představíme dvě: Robinsonovu Q a Peanovu PA

Robinsonova aritmetika Q

$$\begin{array}{ll} \neg S(x) = 0 & x \cdot 0 = 0 \\ S(x) = S(y) \rightarrow x = y & x \cdot S(y) = x \cdot y + x \\ x + 0 = x & \neg x = 0 \rightarrow (\exists y)(x = S(y)) \\ x + S(y) = S(x + y) & x \leq y \leftrightarrow (\exists z)(z + x = y) \end{array}$$

- velmi slabá, nelze v ní dokázat např. komutativitu ani asociativitu $+$ či $\cdot$, nebo tranzitivitu $\leq$
- ale lze dokázat všechna existenční tvrzení o numerálech pravdivá v $\underline{\mathbb{N}}$, tj. formule v PNF, jen $\exists$, za volné proměnné substituujeme numerály $\underline{n} = S(\dots S(0)\dots)$
- např. pro $\varphi(x, y) = (\exists z)(x + z = y)$ je $Q \vdash \varphi(\underline{1}, \underline{2})$

Tvrzení: Je-li $\varphi(x_1, \dots, x_n)$ existenční formule, $a_1, \dots, a_n \in \mathbb{N}$, pak $Q \vdash \varphi(x_1/\underline{a_1}, \dots, x_n/\underline{a_n})$ právě když $\underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \dots, x_n/a_n)]$

(Důkaz vynecháme.)

Extenze Q o schéma indukce, tj. pro každou L-formuli $\varphi(x, \overline{y})$:

$$(\varphi(0, \overline{y}) \wedge (\forall x)(\varphi(x, \overline{y}) \rightarrow \varphi(S(x), \overline{y}))) \rightarrow (\forall x)\varphi(x, \overline{y})$$

- mnohem lepší aproximace $\mathrm{Th}(\underline{\mathbb{N}})$
- dokáže ‘základní’ vlastnosti (např. komut. a asociativitu $+$)
- stále ale existují sentence platné v $\underline{\mathbb{N}}$ ale nezávislé v PA (opět dokážeme v První větě o neúplnosti)

Poznámka: strukturu $\underline{\mathbb{N}}$ lze axiomatizovat (až na $\simeq$) v predikátové logice 2. řádu, extenzí PA o tzv. axiom indukce:

$$(\forall X)((X(0) \wedge (\forall x)(X(x) \rightarrow X(S(x)))) \rightarrow (\forall x)X(x))$$

- X reprezentuje (libovolnou) podmnožinu modelu
- použijeme na množinu všech následníků 0
- každý prvek je následník 0 $\Rightarrow$ izomorfismus s $\underline{\mathbb{N}}$

10.3 Nerozhodnutelnost predikátové logiky

Nerozhodnutelnost predikátové logiky

Věta (O nerozhodnutelnosti predikátové logiky): Neexistuje algoritmus, který pro vstupní formuli φ rozhodne, zda je logicky platná.

- tj. zda je formule φ [v lib. jazyce 1. řádu] tautologie ($\models \varphi$)
- neboli $T = \emptyset$ není rozhodnutelná

Nemáme formalismus pro algoritmy (Turingovy stroje), dokážeme redukcí na jiný nerozhodnutelný problém: Hilbertův 10. problém

> *"Najděte algoritmus, který po konečně mnoha krocích určí, zda daná diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."*

diofantická rovnice: $p(x_1, \ldots, x_n) = 0$, kde p je celočíselný polynom

ukážeme, že existuje redukce 'těžkého' Hilbertova 10. problému na náš problém, tedy i náš problém je 'těžký'

Nerozhodnutelnost Hilbertova desátého problému

Věta (Matiyasevich 1970): Problém existence celočíselného řešení dané diofantické rovnice s celočís. koeficienty je nerozhodnutelný.

(Důkaz neuvedeme.)

Důsledek: Neexistuje algoritmus rozhodující, mají-li dané polynomy $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ s přiroz. koeficienty přirozené řešení, tj.

$$\underline{\mathbb{N}} \models (\exists x_1) \ldots (\exists x_n)\ p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$$

Důkaz: Lagrangeova věta o čtyřech čtvercích říká, že každé přirozené číslo lze vyjádřit jako součet čtyř čtverců (celých čísel). Naopak, každé celé číslo je rozdíl dvou přirozených. Diofantickou rovnici lze tedy transformovat na rovnici z důsledku, a naopak. $\square$

Důkaz nerozhodnutelnosti predikátové logiky

Uvažme φ tvaru $(\exists x_1)\ldots(\exists x_n)\ p(x_1,\ldots,x_n) = q(x_1,\ldots,x_n)$ kde p a q jsou přirozené polynomy. Dle Tvrzení o Robinsonově aritmetice:

$$\underline{\mathbb{N}} \models \varphi \ \Leftrightarrow\ Q \vdash \varphi$$

Buď ψ_Q konjunkce (gen. uzávěrů) axiomů Q (je konečná). Zřejmě:

$$Q \vdash \varphi \ \Leftrightarrow\ \psi_Q \vdash \varphi \ \Leftrightarrow\ \vdash \psi_Q \to \varphi$$

Díky úplnosti a korektnosti je to ale ekvivalentní $\models \psi_Q \to \varphi$. Dostáváme:

$$\underline{\mathbb{N}} \models \varphi \ \Leftrightarrow\ \models \psi_Q \to \varphi$$

Sporem: Pokud bychom měli algoritmus rozhodující logickou platnost, mohli bychom rozhodovat i existenci přirozeného řešení rovnice $p(x_1,\ldots,x_n) = q(x_1,\ldots,x_n)$, tj. Hilbertův 10. problém. $\square$

10.4 Gödelovy věty

První věta o neúplnosti + důsledek o nekompletnosti

Věta (Gödel 1931): Je-li T bezesporná rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky, potom existuje sentence, která je pravdivá v $\underline{\mathbb{N}}$, ale není dokazatelná v T.

- vlastnosti aritmetiky přir. čísel nelze 'rozumně', efektivně popsat (v logice 1. řádu), takový popis je nutně 'neúplný'
- pravdivost je ve standardním modelu $\underline{\mathbb{N}}$ zatímco dokazatelnost v T (samozřejmě pravdivá v T je v T i dokazatelná)
- bezespornost nutná (sporná teorie dokáže vše)
- bez rekurzivní axiomatizovatelnosti by teorie nebyla 'užitečná'
- extenze Q znamená 'základní aritmetická síla' (různé varianty předpokladu; nelze-li zakódovat přir. čísla s $+, \cdot$ je moc 'slabá'

Důsledek: Splňuje-li teorie T předpoklady První věty o neúplnosti a je-li navíc $\underline{\mathbb{N}}$ modelem T, potom T není kompletní.

Důkaz: Vezměme Gödelovu sentenci φ ($\underline{\mathbb{N}} \models \varphi$, $T \nvdash \varphi$). Je-li T kompletní, víme $T \vdash \neg\varphi$, z korektnosti $T \models \neg\varphi$, tedy $\underline{\mathbb{N}} \models \neg\varphi$. $\square$

O důkazu

- Gödelova sentence formalizuje "Nejsem dokazatelná v T"
- převratná důkazová technika, dva hlavní principy:
- aritmetizace syntaxe, zakódování sentencí a jejich dokazatelnosti do přirozených čísel
- self-reference, sentence 'mluví sama o sobě' (o svém kódu)
- všechny technické detaily vynecháme, viz např. V. Švejdar: *Logika – neúplnost, složitost a nutnost*, Academia 2002

Aritmetizace syntaxe a dokazatelnosti

- Gödelovo číslování 'rozumně' kóduje konečné syntaktické objekty (termy, formule, tablo důkazy) do $\mathbb{N}$: lze algoritmicky [de-]kódovat, simulovat 'manipulaci' s objekty na jejich kódech
- pro φ bude $\ulcorner\varphi\urcorner$ příslušný kód, $\underline{\varphi}$ odpovídající $\ulcorner\varphi\urcorner$-tý numerál
- pro danou T máme binární relaci $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ definovanou $(n, m) \in \mathrm{Proof}_T \Leftrightarrow n = \ulcorner\varphi\urcorner$, $m = \ulcorner\tau\urcorner$, τ je tablo důkaz φ z T
- je-li T rek. axiomatizovaná, je relace $\mathrm{Proof}_T \subseteq \mathbb{N}^2$ rekurzivní (lze algoritmicky ověřit korektnost tabla, tj. $(n, m) \in \mathrm{Proof}_T$)
- klíčovou technickou částí důkazu První věty je fakt, že relaci Proof_T lze reprezentovat predikátem v Robinsonově aritmetice

Predikát dokazatelnosti

Tvrzení: Je-li T rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky, potom existuje formule $Prf_T(x, y)$ v jazyce aritmetiky, která reprezentuje relaci Proof_T, tj. pro každá $n, m \in \mathbb{N}$:

- je-li $(n, m) \in \mathrm{Proof}_T$, potom $Q \vdash Prf_T(\underline{n}, \underline{m})$
- jinak $Q \vdash \neg Prf_T(\underline{n}, \underline{m})$

(Důkaz vynecháme!)

- formule $Prf_T(x, y)$ vyjadřuje "y je důkaz x v T"
- formule $(\exists y)Prf_T(x, y)$ znamená "x je dokazatelná v T"
- svědek poskytuje kód tablo důkazu, a $\underline{\mathbb{N}}$ splňuje Q, proto:

Pozorování: $T \vdash \varphi$ právě když $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi}, y)$.

Budeme potřebovat následující důsledek (také bez důkazu):

Důsledek: Je-li $T \vdash \varphi$, potom $T \vdash (\exists y)Prf_T(\underline{\varphi}, y)$.

Self-reference

vyjádřili jsme φ je dokazatelná ale chceme já nejsem dokazatelná

přirozené jazyky mají self-referenci: `Tato věta má 22 znaků.`; formální systémy obvykle ne, umožňují ale přímou referenci (mluvit o posloupnostech symbolů):

```
Následující věta má 29 znaků. "Následující věta má 29 znaků."
```

zde není žádná self-reference, pomůžeme si proto trikem zdvojení:

```
Následující věta zapsaná jednou a ještě jednou v uvozovkách má 149 znaků. "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 149 znaků."
```

přímou referencí a zdvojením tedy získáme self-referenci; podobně program v C, který vypíše svůj kód (34 je ASCII kód uvozovek):

```
main(){char *c="main(){char *c=%c%s%c; printf(c,34,c,34);}";
printf(c,34,c,34);}
```

Věta o pevném bodě

Věta: Je-li T extenzí Robinsonovy aritmetiky, potom pro každou formuli $\varphi(x)$ (v jazyce teorie T) existuje sentence ψ taková, že:

$$T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$$

- také "diagonalizační lemma" nebo "self-referenční" lemma
- ψ je self-referenční, říká o sobě: "já splňuji vlastnost φ"
- v důkazu První věty bude $\varphi(x)$ formule $\neg(\exists y)Prf_T(x, y)$
- všimněte si, jak se v důkazu použije přímá reference a zdvojení

Důkaz (myšlenka): Zdvojující funkce $d\colon \mathbb{N} \to \mathbb{N}$ dekóduje vstup n jako $\varphi(x)$, dosadí numerál $\underline{n}$, znovu zakóduje: pro vš. $\chi(x)$ platí:

$$d(\ulcorner \chi(x) \urcorner) = \ulcorner \chi(\underline{\chi(x)}) \urcorner$$

S využitím T extenze Q se dokáže, že d je v T reprezentovatelná. Pro jednoduchost ať ji reprezentuje term, označíme ho také d (ale ve skutečnosti je to složitá formule).

Pokračování důkazu

Tedy Q, proto i T, dokazuje o numerálech, že d opravdu 'zdvojuje':

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})}$$

Hledaná self-referenční sentence ψ je sentence:

$$\varphi(d(\underline{\varphi(d(x))}))$$

Chceme dokázat, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$, neboli:

$$T \vdash \varphi(d(\underline{\varphi(d(x))})) \leftrightarrow \varphi(\underline{\varphi(d(\underline{\varphi(d(x))}))})$$

K tomu stačí $T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))}$ což máme z reprezentovatelnosti d, kde $\chi(x)$ je $\varphi(d(x))$. $\square$

ψ tedy říká: »Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost φ. "Následující věta zapsaná jednou a ještě jednou v uvozovkách má vlastnost φ."« kde v uvozovkách znamená numerál kódu (přímá reference)

Nedefinovatelnost pravdy

Věta: V žádném bezesporném rozšíření Robinsonovy aritmetiky nemůže existovat definice pravdy.

- definice pravdy v aritmetické teorii T je formule $\tau(x)$ taková, že pro každou sentenci ψ platí: $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$
- kdyby existovala, místo dokazování by stačilo spočíst kód $\ulcorner\psi\urcorner$, dosadit numerál $\underline{\psi}$ do τ, a vyhodnotit
- rozcvička pro důkaz Gödelovy První věty o neúplnosti
- důkaz užívá Paradox lháře, vyjádříme "Nejsem pravdivá v T"
- důkaz První věty užívá stejný trik s "Nejsem dokazatelná v T"

Důkaz: Sporem, ať existuje definice pravdy $\tau(x)$. Z Věty o pevném bodě kde $\varphi(x)$ je $\neg\tau(x)$ dostáváme sentenci ψ takovou, že:

$$T \vdash \psi \leftrightarrow \neg\tau(\underline{\psi})$$

Protože $\tau(x)$ je definice pravdy, platí ale i $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$, tedy i $T \vdash \tau(\underline{\psi}) \leftrightarrow \neg\tau(\underline{\psi})$. To by ale znamenalo, že T je sporná. $\square$

Důkaz První věty o neúplnosti

T bezesp. rek. ax. ext. Q. Gödelovu sentenci ($\underline{\mathbb{N}} \models \psi_T$, $T \not\vdash \psi_T$) získáme z Věty o pevném bodě kde $\varphi(x)$ je $\neg(\exists y) Prf_T(x, y)$:

$$T \vdash \psi_T \leftrightarrow \neg(\exists y) Prf_T(\underline{\psi_T}, y)$$

Tedy ψ_T je v T ekvivalentní "ψ_T není dokazatelná v T". Ekvivalence platí i v $\underline{\mathbb{N}}$ (z konstrukce, protože $\underline{\mathbb{N}}$ splňuje Q), a spolu s ekvivalencí z Pozorování o predikátu dokazatelnosti:

$$\underline{\mathbb{N}} \models \psi_T \;\Leftrightarrow\; \underline{\mathbb{N}} \models \neg(\exists y) Prf_T(\underline{\psi_T}, y) \;\Leftrightarrow\; T \not\vdash \psi_T$$

Stačí tedy ukázat nedokazatelnost ψ_T v T. Sporem: ať $T \vdash \psi_T$.

- Self-reference: $T \vdash \neg(\exists y) Prf_T(\underline{\psi_T}, y)$
- Důsledek o predikátu dokazatelnosti: $T \vdash (\exists y) Prf_T(\underline{\psi_T}, y)$

To by ale znamenalo, že T je sporná. $\square$

Důsledky a zesílení

Důsledek (už byl): Je-li T rekurzivně axiomatizovaná extenze Robinsonovy aritmetiky a je-li $\underline{\mathbb{N}}$ model T, potom T není kompletní.

Důkaz: T není sporná, tedy splňuje předpoklady První věty. Víme, že G. sentence splňuje $\underline{\mathbb{N}} \models \psi_T$ a $T \not\vdash \psi_T$. Je-li T kompletní, máme $T \vdash \neg\psi_T$, z korektnosti $T \models \neg\psi_T$, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, spor. $\square$

Důsledek: Teorie Th($\underline{\mathbb{N}}$) není rekurzivně axiomatizovatelná.

Důkaz: Th($\underline{\mathbb{N}}$) je extenze Q, platí v $\underline{\mathbb{N}}$. Kdyby byla rekurzivně axiomatizovatelná, podle Důsledku by [její rekurzivní axiomatizace] nebyla kompletní, ale je. $\square$

Zesílení První věty: předpoklad $\underline{\mathbb{N}} \models T$ v Důsledku je nadbytečný.

Věta (Rosserův trik, 1936): V bezesporné rekurzivně axiomatizované extenzi Robinsonovy aritmetiky existuje nezávislá sentence.

(Bez důkazu.)

Gödelova Druhá věta o neúplnosti

Efektivně daná, dostatečně bohatá T nedokáže svou bezespornost.

- bezespornost vyjádří sentence Con_T: $\neg(\exists y)Prf_T(\underline{0 = S(0)}, y)$
- všimněte si: $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \not\vdash 0 = S(0)$
- tj. Con_T opravdu vyjadřuje, že "T je bezesporná"

Věta (Gödel, 1931): Je-li T bezesporná rekurzivně axiomatizovaná extenze PA, potom Con_T není dokazatelná v T.

- všimněte si: Con_T je pravdivá v $\underline{\mathbb{N}}$ (neboť T je bezesporná)
- není třeba plná síla PA, stačí slabší předpoklad
- ukážeme si hlavní myšlenku důkazu

Myšlenka důkazu

Gödelova sentence ψ_T vyjadřuje: "Nejsem dokazatelná v T."

V důkazu První věty o neúplnosti jsme ukázali:

"Pokud je T bezesporná, potom ψ_T není dokazatelná v T."

Z toho jednak plyne, že $T \not\vdash \psi_T$, neboť T bezesporná je.

Na druhou stranu to lze formulovat jako: "Platí $Con_T \rightarrow \psi_T$."

Je-li T extenze Peanovy aritmetiky, lze důkaz tohoto tvrzení zformalizovat v rámci teorie T, tedy ukázat, že:

$$T \vdash Con_T \rightarrow \psi_T$$

Kdyby platilo $T \vdash Con_T$, dostali bychom i $T \vdash \psi_T$, což je spor. $\square$

Důsledky

Důsledek: PA má model, ve kterém platí $(\exists y)Prf_{PA}(\underline{0 = S(0)}, y)$.

Důkaz: Sentence Con_{PA} není dokazatelná, tedy ani pravdivá v PA. Platí ale v $\underline{\mathbb{N}}$ (neboť PA je bezesporná), což znamená, že je Con_{PA} nezávislá v PA. V nějakém modelu tedy musí platit její negace, která je ekvivalentní $(\exists y)Prf_{PA}(\underline{0 = S(0)}, y)$. $\square$

Poznámka: Musí to být nestandardní model PA, svědek nestandardní prvek (není hodnotou žádného numerálu).

Důsledek: PA má bezespornou rekurzivně axiomatizovanou extenzi, která "dokazuje svou spornost", tj. $T \vdash \neg Con_T$.

Důkaz: $T = PA \cup \{\neg Con_{PA}\}$ je bezesporná, neboť $PA \nvdash Con_{PA}$. Také triviálně $T \vdash \neg Con_{PA}$, tj. T 'dokazuje spornost' PA. Protože $PA \subseteq T$, platí i $T \vdash \neg Con_T$. $\square$

Poznámka: $\underline{\mathbb{N}}$ nemůže být modelem T.

Bezespornost ZFC

Formalizace matematiky je založena na Zermelově–Fraenkelově teorii množin s axiomem výběru (ZFC). Formálně vzato to není extenze PA, ale můžeme v ní Peanovu aritmetiku ‘interpretovat’.

Důsledek: Je-li ZFC bezesporná, není Con_{ZFC} v ZFC dokazatelná.

Pokud by tedy někdo v rámci ZFC dokázal, že je ZFC bezesporná, znamenalo by to, že je ZFC sporná.