

Logika

Studijní materiál ke státnicím (M6)

Jakub Klesa

Pokryté předměty: NAIL062 (Výroková a predikátová logika)

Obsah

Úvod	2
1 Syntaxe a normální formy (CNF, DNF, PNF)	2
1.1 Jazyk a formule výrokové logiky	2
1.2 Jazyk a formule predikátové logiky	3
1.3 Normální formy výrokové logiky: CNF a DNF	4
1.4 Prenexní normální forma (PNF)	6
2 Sémantika: model, splnitelnost, tautologie, důsledek	7
2.1 Sémantika výrokové logiky	7
2.2 Sémantika predikátové logiky	8
3 Extenze teorií: síla, konzervativnost, skolemizace	10
3.1 Extenze a porovnání síly teorií	10
3.2 Extenze o definice	11
3.3 Skolemizace	11
4 Dokazatelnost: tablo metoda, rezoluce, Hilbert	12
4.1 Tablo metoda ve výrokové logice	12
4.2 Tablo metoda v predikátové logice	14
4.3 Rezoluční metoda ve výrokové logice	14
4.4 Rezoluce v predikátové logice	16
4.5 Hilbertovský kalkulus	17
4.6 Souhrnná úloha: model teorie	17
5 Věty o kompaktnosti a úplnosti	18
5.1 Korektnost a úplnost	18
5.2 Věta o kompaktnosti	19
5.3 Löwenheim-Skolemova věta	19
6 Rozhodnutelnost	20
6.1 Kompletní teorie a kritéria kompletnosti	20
6.2 Rozhodnutelnost a její vztah ke kompletnosti	20
6.3 Příklady rozhodnutelných a nerozhodnutelných teorií	21
Shrnutí	21
Zdroje	23

Úvod

Tento materiál pokrývá okruh **M6 – Logika** (předmět NAIL062 *Výroková a predikátová logika*). Výklad stojí na **skriptech přednášejícího dr. Jakuba Bulína** (NAIL062 *Výroková a predikátová logika: zápisky z přednášky*, zimní semestr 2025), jejichž struktura i obsah jsou převzaty z dřívějších přednášek P. Gregora a z učebnic A. Nerode, R. Shore *Logic for Applications* a M. Ben-Ari *Mathematical Logic for Computer Science*. Značení a hloubka odpovídají kurzu pro informatiky.

Logika má dvě patra: **výrokovou logiku** (atomy jsou nedělitelné „prvovýroky“ bez vnitřní struktury) a **predikátovou logiku prvního řádu** (atomy mluví o individuích pomocí relací, funkcí a kvantifikátorů). Obě patra procházíme paralelně ve čtyřech vrstvách: *syntaxe* (jak vypadají formule), *sémantika* (co znamenají, kdy platí), *dokazatelnost* (jak platnost ověřit syntaktickým výpočtem) a *metavěty* (korektnost, úplnost, kompaktnost, rozhodnutelnost), které obě vrstvy spojují.

Role důkazů. Požadavky okruhu výslovně žádají **schopnost vést formální důkaz** v některém dokazovacím systému (tablo metoda, rezoluce, Hilbertovský kalkul), kdežto u vět o kompaktnosti a úplnosti jen *znění, porozumění významu a použití*. Tablo a rezoluční postupy proto rozepisujeme do detailu (krok po kroku, celé stromy), zatímco metavěty komentujeme intuicí, náčrtem myšlenky a aplikacemi. Do výkladu je zařazena řešená reálná otázka SZZ k okruhu (léto 2024: model teorie); je i v samostatném dokumentu *Příklady otázek*. Použité zdroje jsou uvedeny na konci.

Značení. Prvovýroky (výrokové proměnné) značíme p, q, r , výrokové formule řeckými písmeny φ, ψ, χ ; binární spojku zastupuje $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$. Teorie je množina formulí T , její prvky jsou *axiomy*. V predikátové logice je *signatura* $\langle \mathcal{R}, \mathcal{F} \rangle$ (relační a funkční symboly s aritami; konstanty jsou nulární funkce), *struktura* $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ s neprázdnou doménou A . Sémantické vyplývání (platnost) píšeme $\models$, syntaktickou dokazatelnost $\vdash$. Třidu modelů teorie T značíme $M(T)$, množinu důsledků $Csq(T)$, teorii struktury $Th(\mathcal{A})$. Prázdná klauzule je $\square$. Sjednocujeme značení s okruhy M2 (algebraické struktury), M3 (relace, ekvivalence) a M4 (grafy jako struktury), na něž místy odkazujeme.

1 Syntaxe a normální formy (CNF, DNF, PNF)

Syntaxe popisuje, *jak formule vypadají* – jako konečné nápisy vzniklé podle gramatických pravidel, bez ohledu na význam. Klíčová je induktivní definice a stromová struktura, díky níž je každá formule jednoznačně čitelná.

1.1 Jazyk a formule výrokové logiky

Definice – Jazyk a výrok

Jazyk výrokové logiky je neprázdná množina $\mathbb{P}$ *prvovýroků* (výrokových proměnných), obvykle spočetná. *Výrok* (výroková formule) v jazyce $\mathbb{P}$ je prvek nejmenší množiny $VF_{\mathbb{P}}$ takové, že

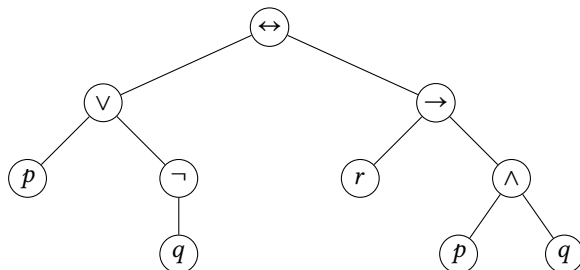
- (1) každý prvovýrok $p \in \mathbb{P}$ je výrok;
- (2) je-li φ výrok, je výrokem i $(\neg\varphi)$;
- (3) jsou-li φ, ψ výroky, je výrokem i $(\varphi \square \psi)$ pro $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

Podvýrok je podřetězec, který je sám výrokem. *Teorie* je libovolná množina výroků $T \subseteq VF_{\mathbb{P}}$.

 **Intuice.** Definice je *induktivní*: výroky jsou přesně ty konečné nápisy, které vzniknou konečně mnoha aplikacemi pravidel z prvovýroků. Vnější závorky a méně závorek píšeme dle priority $\neg$ (nejvyšší) $> \wedge, \vee > \rightarrow, \leftrightarrow$ (nejnižší); $\wedge, \vee$ asociují doprava. Tatáž data lze zapsat prefixově (polsky) i postfixově – podstatná je stromová struktura, ne řetězec znaků.

Definice – Strom výroku

Strom výroku $\text{Tree}(\varphi)$ je zakořeněný uspořádaný strom: prvovýrok p má jediný vrchol s návěštím p ; výrok $(\neg\varphi')$ má kořen $\neg$ s jediným synem $\text{Tree}(\varphi')$; výrok $(\varphi' \sqcap \psi')$ má kořen $\sqcap$ s levým synem $\text{Tree}(\varphi')$ a pravým $\text{Tree}(\psi')$. Podstromy odpovídají podvýrokům.



Strom výroku $\varphi = ((p \vee \neg q) \leftrightarrow (r \rightarrow (p \wedge q)))$. Kořen je hlavní spojka $\leftrightarrow$, listy jsou prvovýroky; $\text{Var}(\varphi) = \{p, q, r\}$. Každý podvýrok je podstrom.

1.2 Jazyk a formule predikátové logiky

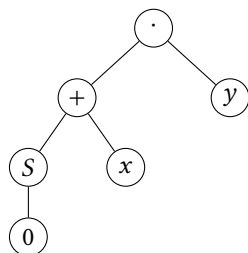
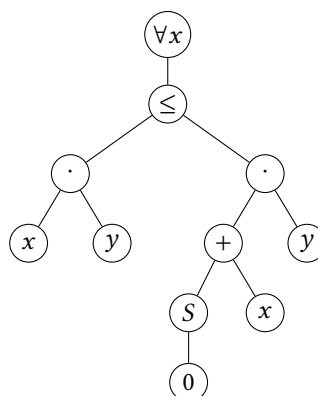
Výroková logika nevidí dovnitř atomů. Predikátová logika *prvního řádu* mluví o *individuích* (prvcích nějaké domény): vyjadřuje jejich vlastnosti a vztahy (relace), skládá je funkcemi a kvantifikuje přes „všechna“ ($\forall$) a „nějaké“ ($\exists$) individuum.

Definice – Jazyk, termy, formule

Jazyk predikátové logiky je dán *signaturou* $\langle \mathcal{R}, \mathcal{F} \rangle$ (disjunktní množiny relačních a funkčních symbolů s aritami; konstantní symbol je funkční symbol arity 0) a údajem, zda jde o *jazyk s rovností* (smí se užívat predikát $=$). K dispozici jsou navíc spočetně mnoho *proměnných* $x, y, z, \dots$, spojky, závorky a kvantifikátory ($\forall x$), ($\exists x$).

- *Termy*: každá proměnná a každý konstantní symbol je term; je-li $f \in \mathcal{F}$ arity n a $t_1, \dots, t_n$ termy, je termem i $f(t_1, \dots, t_n)$.
- *Atomická formule*: $R(t_1, \dots, t_n)$ pro n -ární $R \in \mathcal{R}$ (či $=$), t_i termy.
- *Formule*: každá atomická formule je formule; jsou-li φ, ψ formule, jsou jimi i $(\neg\varphi)$, $(\varphi \sqcap \psi)$; je-li φ formule a x proměnná, jsou formulemi i $((\forall x)\varphi)$ a $((\exists x)\varphi)$.

Intuice. Termy jsou „jména prvků“ (vyhodnotí se na prvek domény), formule mají pravdivostní hodnotu. Term i formuli zachycuje *strom* (vnitřní vrcholy = funkční/relační symboly a spojky, kvantifikátor má jako $\neg$ jediného syna). Pozor: termy jsou čistě syntaktické – $1 + 1$ je term v jazyce aritmetiky, ale jeho „hodnota“ 2 termem není.

(a) strom termu $(S(0) + x) \cdot y$ (b) strom formule $(\forall x)(x \cdot y \leq (S(0) + x) \cdot y)$ 

Stromy termu a formule v jazyce aritmetiky $\langle S, +, \cdot, 0, \leq \rangle$. V (b) je $\forall x$ kořen s jediným synem; listem jsou proměnné a konstanta 0.

Definice – Volné a vázané proměnné, otevřená a uzavřená formule

Výskyt proměnné x ve φ (list stromu s návěštím x) je *vázaný*, je-li uvnitř podformule tvaru $(\forall x)\psi$ či $(\exists x)\psi$; jinak je *volný*. Proměnná je *volná* ve φ , má-li volný výskyt. Zápisem $\varphi(x_1, \dots, x_n)$ míníme, že $x_1, \dots, x_n$ jsou *všechny* volné proměnné. Formule je *otevřená*, neobsahuje-li kvantifikátor, a *uzavřená* (*sentence*), nemá-li volnou proměnnou.

Intuice. Pravdivostní hodnota formule závisí jen na ohodnocení *volných* proměnných; *sentence* má proto v dané struktuře hodnotu nezávisle na ohodnocení – proto v logice hrají hlavní roli. Pojmy „otevřená“ a „uzavřená“ jsou nezávislé: $x+y \leq 0$ je otevřená neuzavřená, $(\forall x)(\forall y)(x+y \leq 0)$ uzavřená neotevřená, $(\forall x)(x+y \leq 0)$ ani jedno, $(0+1=1)$ obojí. Pozor: „nemá vázanou proměnnou“ $\neq$ „otevřená“ (protipříklad $(\forall x) 0=1$).

Definice – Instance a varianta

Term t je *substituovatelný* za x do φ , pokud po nahrazení všech volných výskytů x termem t nevznikne nový vázaný výskyt žádné proměnné z ; výsledek je *instance* $\varphi(x/t)$. *Varianta* vznikne přejmenováním vázané proměnné: podformuli $(Qx)\psi$ nahradíme $(Qy)\psi(x/y)$, je-li y substituovatelná za x do ψ a nemá v ψ volný výskyt.

Intuice. Substituovatelnost brání „zachycení“ proměnné. Do $\varphi(x) = (\exists y)(x+y=1)$ („existuje $1-x$ “) nelze dosadit $t = y$: $(\exists y)(y+y=1)$ už říká „1 je sudé“. Řešení: nejdřív přejmenovat vázané proměnné na zcela nové (varianta), pak dosadit. *Příklad varianty*: $(\forall y)(x \leq y)$ má variantu $(\forall w)(x \leq w)$ (přejmenování $y \rightarrow w$), ale *ne* $(\forall x)(x \leq x)$ – to by zachytilo volné x . Konstantní termy jsou substituovatelné vždy.

1.3 Normální formy výrokové logiky: CNF a DNF

Definice – Literál, klauzule, CNF, DNF

Literál je prvovýrok p nebo jeho negace $\neg p$. *Klauzule* je disjunkce literálů, *elementární konjunkce* je konjunkce literálů. Výrok je v *konjunktivní normální formě* (CNF), je-li konjunkcí klauzulí, a v *disjunktivní normální formě* (DNF), je-li disjunkcí elementárních konjunkcí.

Poznámka. Prázdná klauzule (disjunkce ničeho) je nespílitelná, značíme ji $\square$; prázdná elementární konjunkce je pravdivá. Rozhodování zdarma: výrok v CNF je **tautologie** právě tehdy, když

každá klauzule obsahuje dvojici opačných literálů; výrok v **DNF je splnitelný** právě tehdy, když ne každá elementární konjunkce obsahuje opačnou dvojici.

★ Věta — Existence normálních forem

Ke každému výroku existuje ekvivalentní výrok v CNF i ekvivalentní výrok v DNF.

Intuice. Dvě cesty k normální formě. **(1) Sémanticky (z pravdivostní tabulky):** pro výrok φ nad konečným P s množinou modelů $M(\varphi)$ je

$$\varphi_{\text{DNF}} = \bigvee_{v \in M(\varphi)} \bigwedge_{p \in P} p^{v(p)}, \quad \varphi_{\text{CNF}} = \bigwedge_{v \notin M(\varphi)} \bigvee_{p \in P} p^{1-v(p)},$$

kde $p^1 = p$, $p^0 = \neg p$: DNF má po jedné elementární konjunkci na každý *model*, CNF po jedné klauzuli zakazující každý *nemodel*. **(2) Úpravami:** odstraň $\leftrightarrow, \rightarrow$ ($\varphi \rightarrow \psi \sim \neg\varphi \vee \psi$), zatlač $\neg$ k listům (de Morgan), pak distribuuj.

✎ Příklad — Převod do CNF a DNF dvěma způsoby

Zadání.

Převedte $\varphi = p \leftrightarrow (q \vee \neg r)$ do CNF i DNF (a) sémanticky, (b) ekvivalentními úpravami.

Řešení.

(a) Sémanticky. Z pravdivostní tabulky odečteme modely a nemodely:

p	q	r	$q \vee \neg r$	φ	
0	0	0	1	0	nemodel
0	0	1	0	1	model
0	1	0	1	0	nemodel
0	1	1	1	0	nemodel
1	0	0	1	1	model
1	0	1	0	0	nemodel
1	1	0	1	1	model
1	1	1	1	1	model

Čtyři modely (každý dá jednu elementární konjunkci do DNF), čtyři nemodely (každý jednu klauzuli do CNF).

Modely jsou tedy $M(\varphi) = \{(0, 0, 1), (1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ (zápis (p, q, r)), nemodely zbylé čtyři trojice. Odtud

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

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

(b) Úpravami.

$$\begin{aligned} p \leftrightarrow (q \vee \neg r) &\sim (p \rightarrow (q \vee \neg r)) \wedge ((q \vee \neg r) \rightarrow p) \\ &\sim (\neg p \vee q \vee \neg r) \wedge (\neg(q \vee \neg r) \vee p) \\ &\sim (\neg p \vee q \vee \neg r) \wedge ((\neg q \wedge r) \vee p) \quad (\text{de Morgan, dvojité negace}). \end{aligned}$$

Pro **CNF** distribuujeme poslední závorku: $(\neg q \wedge r) \vee p \sim (\neg q \vee p) \wedge (r \vee p)$, tedy

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

Pro **DNF** roznásobíme druhou závorku $((\neg q \wedge r) \vee p)$ první a vynecháme sporné členy:

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

i Poznámka. Obě CNF z (a) a (b) jsou ekvivalentní, ale různě dlouhé: sémantická metoda dává „úplné“ klauzule (každá obsahuje všechny proměnné), úpravy dají kratší. V praxi je CNF důležitější než DNF (přirozeně popisuje systém mnoha jednoduchých podmínek a je společným vstupem algoritmů níže).

i Poznámka. Použití – problém SAT. CNF je vstupem pro *problém splnitelnosti SAT*: rozhodnout, zda má daný výrok v CNF model. SAT je první dokázaný **NP-úplný** problém (Cook-Levin; viz okruh I2). Rozhoduje se buď *rezolucí* (výrok je nesplnitelný právě tehdy, když z jeho klauzulí lze odvodit prázdnou klauzuli □, sekce 4), nebo prohledáváním s návratem – *algoritmem DPLL* (jednotková propagace + větvení), na němž stojí praktické SAT solvery. Některé tvary jsou snadné: **2-SAT** (klauzule s nejvýše dvěma literály) i **Horn-SAT** (nejvýše jeden pozitivní literál v klauzuli) se rozhodnou v lineárním čase. Detailně tyto algoritmy probírá okruh S1.

1.4 Prenexní normální forma (PNF)

V predikátové logice je „normálním tvarem“ prenexní forma: všechny kvantifikátory vepředu, zbytek otevřený. Slouží jako mezikrok ke skolemizaci (sekce 3) a k rezoluci.

Definice – Prenexní normální forma

Formule je v *prenexní normální formě (PNF)*, je-li tvaru

$$(Q_1 x_1)(Q_2 x_2) \cdots (Q_n x_n) \varphi',$$

kde každý $Q_i \in \{\forall, \exists\}$ a φ' je *otevřená (otevřené jádro)*. Předponu kvantifikátorů zveme *kvantifikátorem prefix*. Jsou-li všechny $Q_i = \forall$, je formule *univerzální*.

★ Věta – Převod do PNF

Ke každé formuli existuje ekvivalentní formule v PNF.

💡 Intuice. Kvantifikátory „vytýkáme“ ven podle pravidel (níže x není volná v ψ , $\bar{Q}$ je opačný kvantifikátor):

$$\neg(Qx)\varphi \sim (\bar{Q}x)\neg\varphi, \quad (Qx)\varphi \wedge \psi \sim (Qx)(\varphi \wedge \psi), \quad (Qx)\varphi \vee \psi \sim (Qx)(\varphi \vee \psi),$$

$$((Qx)\varphi) \rightarrow \psi \sim (\bar{Q}x)(\varphi \rightarrow \psi), \quad \psi \rightarrow ((Qx)\varphi) \sim (Qx)(\psi \rightarrow \varphi).$$

Klíčová past: v *antecedentu* implikace se kvantifikátor **překlopí** (protože $(Qx)\varphi \rightarrow \psi \sim \neg(Qx)\varphi \vee \psi \sim (\bar{Q}x)\neg\varphi \vee \psi$). Podmínku „ x není volná v ψ “ si vynutíme *přejmenováním* vázané proměnné (variantou).

Příklad – Převod do PNF

Zadání.

Převedte do PNF formuli $((\forall z)P(x, z) \wedge P(y, z)) \rightarrow \neg(\exists x)P(x, y)$.

Řešení. Postupujeme zleva, u kolize přejmenujeme vázanou proměnnou:

$$\begin{aligned} & ((\forall z)P(x, z) \wedge P(y, z)) \rightarrow \neg(\exists x)P(x, y) \\ & \sim ((\forall u)P(x, u) \wedge P(y, z)) \rightarrow (\forall x)\neg P(x, y) && (z \rightarrow u \text{ uvnitř kvant.}; \neg(\exists x) \sim (\forall x)\neg) \\ & \sim (\forall u)(P(x, u) \wedge P(y, z)) \rightarrow (\forall v)\neg P(v, y) && (\text{vytknutí } \forall u \text{ z } \wedge; x \rightarrow v) \\ & \sim (\exists u)((P(x, u) \wedge P(y, z)) \rightarrow (\forall v)\neg P(v, y)) && (\forall u \text{ z antecedentu} \Rightarrow \text{překlopí na } \exists u) \\ & \sim (\exists u)(\forall v)(P(x, u) \wedge P(y, z) \rightarrow \neg P(v, y)) && (\text{vytknutí } \forall v \text{ z konsekventu}). \end{aligned}$$

Výsledek je v PNF s prefixem $(\exists u)(\forall v)$. Proměnné x, y, z jsou ve vstupní formulí *volné* (nejsou nikde kvantifikované), proto zůstávají ve výsledku volné; vytýkáme jen vázané u, v . Generální uzávěr (sentence) je $(\forall x)(\forall y)(\forall z)(\exists u)(\forall v)(P(x, u) \wedge P(y, z) \rightarrow \neg P(v, y))$, kde se volné x, y, z teprve uzavrou $\forall$.

i Poznámka. PNF *není* jednoznačná (pravidla lze aplikovat v různém pořadí). Vyplatí se vytýkat přednostně kvantifikátory, ze kterých se stanou *existenční*: čím méně $\forall$ jim při skolemizaci předchází, tím nižší aritu má Skolemova funkce (žádný $\Rightarrow$ *konstanta*). Pořadí ovšem volíme jen mezi *nezávislými* kvantifikátory z různých podformulí (jako $\exists u$ a $\forall v$ výše); $(\forall x)(\exists y)\varphi$ a $(\exists y)(\forall x)\varphi$ nad *toutéž* maticí ekvivalentní nejsou, přehazovat je tedy nelze.

2 Sémantika: model, splnitelnost, tautologie, důsledek

Sémantika dává formulím *význam*: přiřadí jim pravdivostní hodnotu a tím definuje, kdy formule *platí*, kdy je *splnitelná* a co z teorie *vyplývá*. Ve výrokové logice je význam dán ohodnocením prvovýroků, v predikátové strukturou.

2.1 Sémantika výrokové logiky

☰ Definice – Model výroku a teorie

(Pravdivostní) ohodnocení, neboli *model jazyka* $\mathbb{P}$, je funkce $v : \mathbb{P} \rightarrow \{0, 1\}$. Pravdivostní hodnotu složeného výroku spočteme po stromu od listů (pomocí tabulek spojek). Výrok φ *platí* v v (v je *model* φ), píšeme $v \models \varphi$, je-li jeho hodnota 1; množinu modelů značíme $M(\varphi)$. Ohodnocení je *model teorie* T , píšeme $v \models T$, platí-li v něm *každý* axiom; $M(T) = \bigcap_{\varphi \in T} M(\varphi)$.

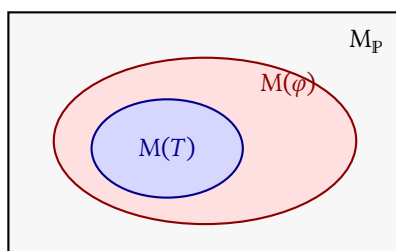
☰ Definice – Sémantické pojmy

Výrok φ (nad jazykem $\mathbb{P}$, s třídou všech modelů $M_{\mathbb{P}}$) je

- *tautologie* (pravdivý), $\models \varphi$, platí-li ve všech modelech: $M(\varphi) = M_{\mathbb{P}}$;
- *sporný* (lživý), nemá-li model: $M(\varphi) = \emptyset$;
- *nezávislý*, je-li $\emptyset \subsetneq M(\varphi) \subsetneq M_{\mathbb{P}}$;
- *splnitelný*, má-li model: $M(\varphi) \neq \emptyset$.

Vzhledem k teorii T je φ *pravdivý* (*důsledek* T), $T \models \varphi$, platí-li ve všech modelech T ($M(T) \subseteq M(\varphi)$); *lživý* v T , je-li $M(T) \cap M(\varphi) = \emptyset$; *nezávislý* v T , není-li ani pravdivý, ani lživý v T ; *splnitelný* v T (*konzistentní* s T), je-li $M(T) \cap M(\varphi) \neq \emptyset$.

💡 Intuice. Vše je o *množinách modelů*. „ φ je důsledek T “ znamená, že modely T jsou podmnožinou modelů φ – žádný model T nesmí φ porušit. Pro $T = \emptyset$ je $M(T) = M_{\mathbb{P}}$ a důsledek splývá s tautologií. Pojmy ilustruje obrázek: pravdivost = $M(\varphi)$ vyplní celé pole, spornost = je prázdná, nezávislost = je vlastní neprázdná část, důsledek = $M(T)$ leží uvnitř $M(\varphi)$.



Modely jako podmnožiny pole všech ohodnocení $M_{\mathbb{P}}$. Zde $M(T) \subseteq M(\varphi)$, tj. $T \models \varphi$ (φ je důsledek T). Kdyby $M(\varphi) = M_{\mathbb{P}}$, je φ tautologie; kdyby $M(\varphi) = \emptyset$, je sporný; jinak je nezávislý.

Definice – Důsledky a vlastnosti teorie

Důsledky teorie jsou $\text{Csq}(T) = \{\varphi : T \models \varphi\}$. Teorie T je *sporná*, nemá-li model (pak v ní platí vše); *bezesporná* (splnitelná), má-li model; *kompletní*, je-li bezesporná a každý výrok je v ní pravdivý, nebo lživý (žádný nezávislý) – to ve výrokové logice nastane *právě tehdy, když má jediný model*. (V predikátové logice se „jediný model“ zjemní na „jediný model až na elementární ekvivalenci“, viz sekci 6.)

Poznámka. Věta o dedukci (konečná verze): pro konečnou teorii je $\varphi \in \text{Csq}(\{\varphi_1, \dots, \varphi_n\})$ právě tehdy, když je $(\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \varphi$ tautologie. Plyne přímo z $M(\varphi_1, \dots, \varphi_n) \subseteq M(\varphi) \iff \models (\bigwedge \varphi_i) \rightarrow \varphi$. Z existence DNF/CNF (sekce 1) navíc plyne *funkční úplnost* systému $\{\neg, \wedge, \vee\}$: nad konečným P vyjádří každou booleovskou funkci, a tedy každou množinu modelů, nějaký výrok.

Příklad – Analýza teorie nad konečně mnoha prvovýroky

Zadání.

Nad $P = \{p, q, r\}$ uvažme $T = \{p \vee q \vee r, q \rightarrow r, \neg r\}$. (1) Najděte všechny modely T . (2) Rozhodněte, zda je p pravdivý, lživý, či nezávislý v T .

Řešení. Postupujeme od nejselektivnějšího axiomu (zúžíme množinu kandidátů):

(1) $\neg r$ vynutí $r = 0$; zbývají $(p, q, r) \in \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\}$.

$q \rightarrow r$ při $r = 0$ vyžaduje $q = 0$; zbývají $(0, 0, 0), (1, 0, 0)$.

$p \vee q \vee r$ vyloučí $(0, 0, 0)$. Tedy $M(T) = \{(1, 0, 0)\}$ – jediný model.

(2) V jediném modelu je $p = 1$, takže $M(T) \subseteq M(p)$: p je **pravdivý v T** (a T je dokonce kompletní, má jediný model).

Příklad – Počítání nad konečným jazykem

Zadání. Nad P s $|P| = n = 3$ má bezesporná teorie T právě $k = 2$ modely. Kolik je (až na ekvivalenci) výroků nezávislých v T ?

Řešení. Výrok až na ekvivalenci určuje jeho množina modelů $M = M(\varphi) \subseteq M_P$, kde $|M_P| = 2^n = 8$. Nezávislost v T znamená $\emptyset \neq M \cap M(T) \neq M(T)$: na dvou modelech teorie máme $2^k - 2 = 2$ „ netriviální “ volby průniku, na zbylých $2^n - k = 6$ ohodnoceních volíme libovolně (2^6). Celkem $(2^k - 2) \cdot 2^{2^n - k} = 2 \cdot 2^6 = 128$ výroků nezávislých v T .

2.2 Sémantika predikátové logiky

V predikátové logice nese význam *struktura*: zvolí doménu a realizuje (interpretuje) všechny symboly jazyka.

Definice – Struktura, model jazyka

Struktura (model jazyka L) je $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$: neprázdná *doména* A ; pro každý n -ární relační symbol R realizace $R^{\mathcal{A}} \subseteq A^n$; pro každý n -ární funkční symbol f realizace $f^{\mathcal{A}} : A^n \rightarrow A$ (pro konstantu c je $c^{\mathcal{A}} \in A$).

Definice – Hodnota termu, pravdivostní hodnota formule

Ohodnocení proměnných je $e : \text{Var} \rightarrow A$; $e(x/a)$ změni hodnotu x na a . *Hodnota termu* $t^{\mathcal{A}}[e] : x^{\mathcal{A}}[e] = e(x)$, $c^{\mathcal{A}}[e] = c^{\mathcal{A}}$, $f(t_1, \dots, t_n)^{\mathcal{A}}[e] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e])$. *Pravdivostní hodnota* $H^{\mathcal{A}}(\varphi)[e]$ je dána indukcí:

$$H^{\mathcal{A}}(R(t_1, \dots, t_n))[e] = 1 \iff (t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e]) \in R^{\mathcal{A}},$$

spojky přes pravdivostní tabulky a pro kvantifikátory

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

💡 Intuice. Tarského definice: hodnotu formule počítáme „zevnitř ven“. Kvantifikátor $\forall$ je „konjunkce přes všechny prvky domény“ (proto min), $\exists$ je „disjunkce přes prvky“ (proto max). Pozor na záměnu symbolu a jeho realizace: ve struktuře $\langle \mathbb{N}, \cdot, 3 \rangle$ jazyka $\langle +, 1 \rangle$ je $(x + 1)$ vyhodnoceno jako $e(x) \cdot 3$.

📖 Definice – Platnost, model teorie

φ platí v $\mathcal{A}$ při e , $\mathcal{A} \models \varphi[e]$, je-li $H^{\mathcal{A}}(\varphi)[e] = 1$. φ je pravdivá v $\mathcal{A}$, $\mathcal{A} \models \varphi$, platí-li při každém e (pro sentenci na e nezáleží); je lživá v $\mathcal{A}$, je-li $\mathcal{A} \models \neg\varphi$. Model teorie T je struktura, v níž platí všechny axiomy ($\mathcal{A} \models T$); třída modelů je $M_L(T)$. Sentence φ je pravdivá / lživá / nezávislá v T přesně jako ve výrokovém případě (přes $M_L(T)$ a $M_L(\varphi)$); pravdivým sentencím říkáme *důsledky*, $Csq_L(T)$.

📌 Poznámka. Lživá $\neq$ „není pravdivá“: u formule s volnou proměnnou může $\mathcal{A} \not\models \varphi$ i $\mathcal{A} \models \neg\varphi$ (např. $\varphi = P(x)$, kde $P^{\mathcal{A}}$ je vlastní neprázdná podmnožina). Konkrétně pro $A = \{0, 1\}$ a $P^{\mathcal{A}} = \{0\}$: při $e(x) = 0$ formule platí, při $e(x) = 1$ neplatí, takže $P(x)$ není pravdivá (neplatí při každém e) ani lživá (neplatí $\neg P(x)$ při každém e). Pro sentence už „lživá“ a „není pravdivá“ splývají. *Formule platí ve struktuře právě tehdy, když v ní platí její generální (univerzální) uzávěr.*

📌 Poznámka. Jazyk s rovností a axiomy rovnosti. Je-li $=$ v jazyce, žádáme, aby se ve všech uvažovaných strukturách interpretoval jako *skutečná identita* na doméně (relace „být též prvek“). V dokazovacích systémech, kde je $=$ jen další relační symbol (tablo, rezoluce), tuto interpretaci vynutíme přidáním *axiomů rovnosti*:

- *reflexivita*: $x = x$;
- *slučitelnost s funkcemi*: pro každý n -ární funkční symbol f

$$x_1 = y_1 \wedge \dots \wedge x_n = y_n \rightarrow f(x_1, \dots, x_n) = f(y_1, \dots, y_n);$$

- *slučitelnost s relacemi*: pro každý n -ární relační symbol R (včetně samotného $=$)

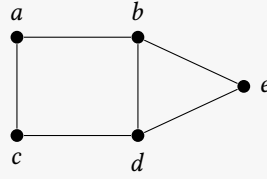
$$x_1 = y_1 \wedge \dots \wedge x_n = y_n \rightarrow (R(x_1, \dots, x_n) \rightarrow R(y_1, \dots, y_n)).$$

Symetrii ($x = y \rightarrow y = x$) ani tranzitivitu ($x = y \wedge y = z \rightarrow x = z$) přidávat netřeba – plynou z reflexivity a slučitelnosti aplikované na R rovné $=$. Tyto axiomy zaručí, že $=^{\mathcal{A}}$ je *kongruence*; faktorizací podle ní vznikne model, kde je $=$ skutečná identita.

🔍 Příklad – Struktura jako model teorie

Zadání. V jazyce $\langle E \rangle$ s rovností je *teorie grafů* $T_{\text{graf}} = \{\neg E(x, x), E(x, y) \rightarrow E(y, x)\}$ (ireflexivita, symetrie). Rozhodněte, zda je struktura $\mathcal{G}$ na obrázku jejím modelem, a zda je v ní sentence $\psi = (\forall x)(\exists y)E(x, y)$ („každý vrchol má souseda“) pravdivá.

Řešení. Modely T_{graf} jsou přesně *jednoduché grafy* ($E^{\mathcal{A}}$ je ireflexivní a symetrická relace). Na obrázku je $E^{\mathcal{G}}$ symetrická (hrany kreslíme neorientovaně) a bez smyček, takže $\mathcal{G} \models T_{\text{graf}}$. Sentence ψ je pravdivá, právě když žádný vrchol není izolovaný; zde má každý vrchol aspoň jednu hranu, tedy $\mathcal{G} \models \psi$. (Naopak ve struktuře s izolovaným vrcholem by ψ neplatila – ψ je v T_{graf} **nezávislá**.)



Struktura $\mathcal{G} = \langle \{a, b, c, d, e\}, E^{\mathcal{G}} \rangle$ jako model teorie grafů: $E^{\mathcal{G}}$ je symetrická (neorientované hrany) a ireflexivní (bez smyček), tj. $\mathcal{G} \models \{\neg E(x, x), E(x, y) \rightarrow E(y, x)\}$. Žádný vrchol není izolovaný, proto $\mathcal{G} \models (\forall x)(\exists y)E(x, y)$.

★ Věta – Platnost převedená na nespelnitelnost

Je-li T teorie a φ sentence (téhož jazyka), pak

$$T \models \varphi \iff T \cup \{\neg\varphi\} \text{ nemá model.}$$

Důkaz (nepovinný – řetězec ekvivalencí). $T \cup \{\neg\varphi\}$ nemá model $\iff \neg\varphi$ neplatí v žádném modelu T $\iff$ (protože φ je sentence) φ platí v každém modelu T $\iff T \models \varphi$. $\square$

Intuice. Tato drobná věta je *motor* dokazovacích metod: tablo i rezoluce „dokazují“ φ tak, že *vyvrátí* (ukážou nespelnitelnost) $T \cup \{\neg\varphi\}$ – důkaz sporem. Předpoklad „ φ je sentence“ je nutný (pro $\varphi = P(x)$, $T = \{P(c)\}$ věta selže).

3 Extenze teorií: síla, konzervativnost, skolemizace

Často chceme jednu teorii *rozšířit* – přidat axiomy, nebo dokonce nové symboly – a ptát se, jak se změní její síla. Klíčové je, kdy rozšíření „nic nového neřekne“ o původním jazyce (konzervativnost) a jak teorii zjednodušit na otevřenou (skolemizace), což je vstupní krok rezoluce.

3.1 Extenze a porovnání síly teorií

📖 Definice – Extenze teorie

Nechť T je teorie v jazyce L a T' teorie v jazyce $L' \supseteq L$.

- T' je *extenze* T , pokud $\text{Cs}_{\mathcal{L}}(T) \subseteq \text{Cs}_{\mathcal{L}'}(T')$ (každý důsledek T platí i v T').
- Extenze je *jednoduchá*, je-li $L' = L$ (beze změny jazyka).
- Extenze je *konzervativní*, platí-li navíc $\text{Cs}_{\mathcal{L}}(T) = \text{Cs}_{\mathcal{L}'}(T') \cap \{L\text{-sentence}\}$ (v původním jazyce T' nedokáže nic nového).
- Teorie jsou *ekvivalentní*, jsou-li navzájem svými extenzemi.

Intuice. „Více axiomů = méně modelů = silnější teorie.“ Pro jednoduché extenze ($L' = L$) je T' extenze T právě tehdy, když $M_L(T') \subseteq M_L(T)$. *Konzervativní* extenze smí používat nové symboly, ale o starém jazyce říká přesně totéž co T – typicky jen zavádí pohodlnou „zkratku“. To je přesně situace *extenze o definice*.

★ Věta – Sémantické kritérium extenze

Nechť $L \subseteq L'$, $T \vdash L$, $T' \vdash L'$. Pak:

- T' je extenze T právě tehdy, když L -redukt každého modelu T' je modelem T ;
- je-li T' extenze T a lze-li *každý* model T expandovat (dointerpretováním nových symbolů) na model T' , je T' *konzervativní* extenze T .

i Poznámka. Věta o konstantách (podpůrná): rozšíříme-li L o nové konstanty $c_1, \dots, c_n$ a T ponecháme, pak pro formuli $\varphi(x_1, \dots, x_n)$ platí $T \models \varphi$ právě tehdy, když $T \models \varphi(x_1/c_1, \dots, x_n/c_n)$ v rozšířeném jazyce. „Volná proměnná“ a „nová konstanta nesvázaná axiomy“ jsou tedy zaměnitelné; tohoto triku využijí „svědci“ v tablo metodě (sekce 4).

3.2 Extenze o definice

Nejdůležitější konzervativní extenze zavádí *definovaný symbol* pohodlnou zkratkou.

Definice – Extenze o definici relačního a funkčního symbolu

Nechť T je teorie v L .

- *Definice relačního symbolu*: pro formuli $\psi(x_1, \dots, x_n)$ a nový n -ární relační symbol R je $T' = T \cup \{R(x_1, \dots, x_n) \leftrightarrow \psi(x_1, \dots, x_n)\}$.
- *Definice funkčního symbolu*: pro $\psi(x_1, \dots, x_n, y)$ a nový n -ární funkční symbol f , *pokud* v T platí axiom existence $(\exists y)\psi$ a jednoznačnosti $\psi(\bar{x}, y) \wedge \psi(\bar{x}, z) \rightarrow y = z$, je $T' = T \cup \{f(x_1, \dots, x_n) = y \leftrightarrow \psi(x_1, \dots, x_n, y)\}$.

★ Důsledek – Konzervativnost

Extenze o definice je *konzervativní* (každý model T se rozšíří na model T' , navíc *jednoznačně*). Pro každou L' -formuli φ' existuje L -formule φ s $T' \models \varphi' \leftrightarrow \varphi$ – definovaný symbol lze vždy „rozvést“ zpět.

💡 Intuice. Ekvivalence $R(\bar{x}) \leftrightarrow \psi(\bar{x})$ *jednoznačně* dourčí interpretaci nového R z modelu T , takže nepřibudou ani neubudou modely (až na nový symbol). U funkce je navíc třeba, aby ψ definovala *totální a jednoznačnou* relaci – proto axiomy existence a jednoznačnosti (např. min lze definovat až nad *lineárním* uspořádáním; $\frac{1}{2}$ až nad tělesem charakteristiky $\neq 2$).

Příklad – Rozvedení definovaného symbolu

Zadání. Nad teorií uspořádaných grup T jazyka $\langle +, 0, \leq \rangle$ (s rovností) zavedme *inverzní prvek* – definicí $-x = y \leftrightarrow x + y = 0$ a ostré uspořádání $<$ pomocí $\leq$ definicí $x < y \leftrightarrow (x \leq y \wedge \neg x = y)$. Rozvedte formuli $-x < y$ na formuli původního jazyka.

Řešení. Definovaný term $-x$ nahradíme novou proměnnou z vázanou existenčním kvantifikátorem (a dodáme definující podmínku $x + z = 0$); definovaný predikát $<$ rozepíšeme:

$$-x < y \equiv_{T'} (\exists z) \left(\underbrace{(z \leq y \wedge \neg z = y)}_{z < y} \wedge \underbrace{x + z = 0}_{z = -x} \right).$$

Výsledná formule je v jazyce $\langle +, 0, \leq \rangle$ a je T' -ekvivalentní s $-x < y$.

3.3 Skolemizace

Skolemizace odstraní existenční kvantifikátory zavedením nových funkčních symbolů („svědků jako funkcí“) a převede teorii na *otevřenou* – za cenu, že nová teorie je s původní *ekvisplnitelná*, ne nutně ekvivalentní. To stačí pro důkaz sporem (rezoluci).

Definice – Ekvisplnitelnost

Teorie T a T' (i v různých jazycích) jsou *ekvisplnitelné*, pokud platí: T má model právě tehdy, když T' má model.

Definice – Skolemova varianta

Nechť $\varphi = (\forall x_1) \cdots (\forall x_m)(\exists y)\psi$ je sentence v PNF, kde před $(\exists y)$ stojí právě univerzální kvantifikátory $(\forall x_1), \dots, (\forall x_m)$. Zavedeme nový m -ární funkční symbol f a nahradíme φ za $(\forall x_1) \cdots (\forall x_m)\psi(y/f(x_1, \dots, x_m))$. Opakováním přes všechny existenční kvantifikátory (vždy zleva) vznikne *Skolemova varianta* φ^S ; postupu říkáme *skolemizace*. Aritu každého f je počet univerzálních kvantifikátorů nalevo od rušeného $\exists$ – nestojí-li nalevo žádný, je f *konstanta*.

★ Věta – Skolemova věta

Každá teorie má *otevřenou konzervativní extenzi*. Speciálně každá sentence φ je se svou Skolemovou variantou φ^S *ekvisplnitelná*.

 **Intuice.** „Existuje y “ pro každou volbu $x_1, \dots, x_m$ znamená, že y je *funkcí* těchto x_i ; tu funkci pojmenujeme novým f a y jí nahradíme (volba svědka = axiom výběru). Skolemova varianta φ^S *není* ekvivalentní φ (mluví o bohatším jazyce), ale je s ní ekvisplnitelná, což pro hledání sporu stačí. Postup: $PNF \rightarrow$ *generální uzávěr (sentence!)* $\rightarrow$ *skolemizace* $\rightarrow$ *vypuštění $\forall$* $\rightarrow$ *CNF*. Pozor: skolemizovat se musí ze *sentence* – pro $(\exists y)E(x, y)$ není $E(x, c)$ Skolemova varianta (napřed generální uzávěr $(\forall x)(\exists y)E(x, y)$, pak $E(x, f(x))$).

Příklad – Skolemizace

Zadání. Skolemizujte sentence (a) $(\forall x)(\exists y)(\forall z)(\exists w)P(x, y, z, w)$ a (b) $(\exists y)(\forall x)Q(x, y)$.

Řešení.

- (a) Před $(\exists y)$ stojí $(\forall x) \Rightarrow y \mapsto f(x)$ (unární f); před $(\exists w)$ stojí $(\forall x), (\forall z) \Rightarrow w \mapsto g(x, z)$ (binární g). Po vypuštění $\forall$:

$$\boxed{P(x, f(x), z, g(x, z))} \quad (\text{otevřené jádro Skolemovy varianty}).$$

- (b) Před $(\exists y)$ nestojí žádný $\forall \Rightarrow y \mapsto c$ (konstanta). Výsledek: $\boxed{Q(x, c)}$.

Obě otevřené formule jsou s původními sentencemi ekvisplnitelné a lze je rovnou převést do CNF (množiny klauzulí) pro rezoluci.

4 Dokazatelnost: tablo metoda, rezoluce, Hilbert

Dokazovací systém formalizuje „dokazování“ jako syntaktickou proceduru: *důkaz* je konečný objekt, který lze algoritmicky ověřit. Píšeme $T \vdash \varphi$ („ φ je dokazatelná z T “). Žádáme *korektnost* ($T \vdash \varphi \Rightarrow T \models \varphi$ – co dokážeme, platí) a ideálně *úplnost* ($T \models \varphi \Rightarrow T \vdash \varphi$ – co platí, dokážeme). Tablo i rezoluce dokazují *sporem*: vyvrátí $T \cup \{\neg\varphi\}$.

4.1 Tablo metoda ve výrokové logice

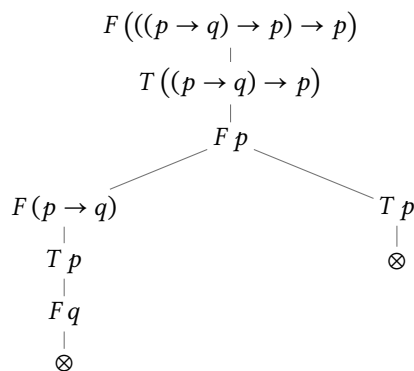
Definice – Tablo, položka, tablo důkaz

Položka je $T\psi$ nebo $F\psi$ („ ψ v hledaném modelu platí / neplatí“). *Tablo* z teorie T je strom označovaný položkami, který vzniká z kořene *redukcemi* (připojením *atomického tabla* pro položku na větev dle tabulky níže) a připojením $T\alpha$ pro libovolný axiom $\alpha \in T$. Větev je *sporná* (značka $\otimes$), obsahuje-li $T\psi$ i $F\psi$; *dokončená*, je-li sporná nebo má všechny položky zredukované a obsahuje všechny axiomy. *Tablo důkaz* φ z T je *sporné* tablo s $F\varphi$ v kořeni (tehdy $T \vdash \varphi$); *zamítnutí* je sporné tablo s $T\varphi$ v kořeni.

položka	rozvoj	položka	rozvoj
$T \neg \varphi$	$F \varphi$	$F \neg \varphi$	$T \varphi$
$T(\varphi \wedge \psi)$	$T \varphi, T \psi$	$F(\varphi \wedge \psi)$	$F \varphi \mid F \psi$
$T(\varphi \vee \psi)$	$T \varphi \mid T \psi$	$F(\varphi \vee \psi)$	$F \varphi, F \psi$
$T(\varphi \rightarrow \psi)$	$F \varphi \mid T \psi$	$F(\varphi \rightarrow \psi)$	$T \varphi, F \psi$
$T(\varphi \leftrightarrow \psi)$	$T \varphi, T \psi \mid F \varphi, F \psi$	$F(\varphi \leftrightarrow \psi)$	$T \varphi, F \psi \mid F \varphi, T \psi$

Atomická tabla. Čárka „|“ = položky pod sebou na téže větvi; svislité „|“ = rozvětvení. (Pravidla čtou „jak může položka nastat“: $F(\varphi \rightarrow \psi)$ jen tak, že platí φ a neplatí ψ .)

Intuice. Tablo hledá protipříklad: do kořene dáme $F\varphi$ („kéž φ neplatí“) a rozvíjíme důsledky. *Sporná* větev ($\otimes$) znamená, že protipříklad na ní neexistuje; *každá* větev sporná $\Rightarrow$ protipříklad neexistuje vůbec $\Rightarrow \varphi$ platí. Naopak *dokončená bezesporná* větev dává *protipříklad*: „kanonický model“ $v(p) = 1$ právě když je na větvi Tp .



Tablo důkaz Peirceova zákona $((p \rightarrow q) \rightarrow p) \rightarrow p$. Kořen $F\varphi$; po redukci $F \rightarrow$ máme $T((p \rightarrow q) \rightarrow p)$ a Fp , redukce $T \rightarrow$ větví na $F(p \rightarrow q) \mid Tp$. Pravá větev: Tp proti $Fp \otimes$. Levá: $F(p \rightarrow q)$ dá Tp, Fq , opět Tp proti $Fp \otimes$. Obě větve sporné $\Rightarrow \vdash \varphi$ (tautologie).

Příklad — Tablo: důkaz vs. protipříklad

Zadání.

(1) Dokažte tablo metodou, že $\{\neg q, p \vee q\} \models p$. (2) Tablo metodou rozhodněte, zda je $(\neg q \vee p) \rightarrow p$ tautologie.

Řešení.

- Kořen Fp ; připojíme axiomy $T\neg q$ a $T(p \vee q)$. Redukce $T\neg q \rightsquigarrow Fq$. Redukce $T(p \vee q)$ větví na $Tp \mid Tq$: levá Tp proti $Fp \otimes$, pravá Tq proti $Fq \otimes$. Obě sporné $\Rightarrow \{\neg q, p \vee q\} \vdash p$, tedy (korektnost) i $\models p$.
- Kořen $F((\neg q \vee p) \rightarrow p)$; redukce $F \rightarrow$ dá $T(\neg q \vee p)$ a Fp . Redukce $T(\neg q \vee p)$ větví na $T\neg q \mid Tp$: pravá Tp proti $Fp \otimes$; levá $T\neg q \rightsquigarrow Fq$ je **dokončená a bezesporná** (Fp, Fq). Kanonický model $v = (p=0, q=0)$: $(\neg q \vee p) = 1$, ale $p = 0$, takže $1 \rightarrow 0 = 0$ – **protipříklad**. Formule *není* tautologie.

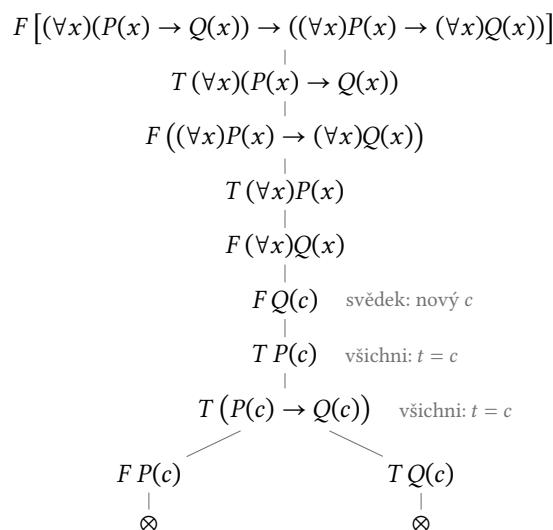
(1) sporné tablo = důkaz $ \begin{array}{c} Fp \\ \vdots \\ T\neg q \\ \vdots \\ T(p \vee q) \\ \vdots \\ Fq \\ \swarrow \quad \searrow \\ Tp \quad Tq \\ \otimes \quad \otimes \end{array} $ Obě větve sporné: $\{\neg q, p \vee q\} \vdash p$.	(2) otevřená větev = protimodel $ \begin{array}{c} F((\neg q \vee p) \rightarrow p) \\ \vdots \\ T(\neg q \vee p) \\ \vdots \\ Fp \\ \swarrow \quad \searrow \\ T\neg q \quad Tp \\ \vdots \quad \otimes \\ Fq \quad \checkmark \end{array} $ Větev $\{Fp, Fq\}$ bezsporná $\Rightarrow$ protimodel $(0, 0)$.
--	--

4.2 Tablo metoda v predikátové logice

V PL pracují položky se *sentencemi* (formuli i axiomy nahradíme generálními uzávěry). Spojkové rozvoje jsou stejné, přibývají *kvantifikátorová* pravidla dvojího druhu:

typ „všichni“ (libovolný term t)	typ „svědek“ (nový konstantní symbol c)
$T(\forall x)\varphi(x) \rightsquigarrow T\varphi(x/t)$	$T(\exists x)\varphi(x) \rightsquigarrow T\varphi(x/c)$
$F(\exists x)\varphi(x) \rightsquigarrow F\varphi(x/t)$	$F(\forall x)\varphi(x) \rightsquigarrow F\varphi(x/c)$

Intuice. „Svědek“ ($T\exists, F\forall$): existenci dosvědčí *nový* konstantní symbol c – pojmenuje onen prvek (formálně věta o konstantách). „Všichni“ ($T\forall, F\exists$): smíme dosadit *libovolný* term, a aby byla větev dokončená, musíme postupně dosadit *všechny* termy (proto tato položka zůstává „nehotová“ a může generovat nekonečnou větev). V jazyce s rovností přidáme *axiomy rovnosti* (reflexivita a slučitelnost = s funkcemi i relacemi), které vynutí, že $=$ se chová jako identita.



Tablo důkaz $(\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)P(x) \rightarrow (\forall x)Q(x))$. Z $F\forall$ vznikne svědek $FQ(c)$; položky „všichni“ $T(\forall x)P$ a $T(\forall x)(P \rightarrow Q)$ dosadíme též c . Redukce $T(P(c) \rightarrow Q(c))$ větví: $FP(c)$ proti $TP(c) \otimes$, $TQ(c)$ proti $FQ(c) \otimes$. Obě větve sporné $\Rightarrow$ formule je dokazatelná.

4.3 Rezoluční metoda ve výrokové logice

Rezoluce pracuje s CNF v *množinové reprezentaci*: *klauzule* je množina literálů, *formule* je množina klauzulí, prázdná klauzule $\square$ je nesplnitelná. Má jediné pravidlo a dokazuje sporem (zamítnutím).

4.4 Rezoluce v predikátové logice

Po skolemizaci (sekce 3) je teorie množinou klauzulí s termy a proměnnými. Rezoluce přibírá *unifikaci*: před řezem ztotožníme literály substitucí.

Definice – Unifikace, rezoluční pravidlo s unifikací

Substituce σ je nejobecnější *unifikace* (mgu) množiny výrazů $\{E_1, \dots, E_k\}$, je-li $E_1\sigma = \dots = E_k\sigma$ a každá jiná unifikace přes ni „vznikne“. *Rezoluční pravidlo*: klauzule C_1, C_2 s disjunktími proměnnými, $C_1 = C'_1 \cup \{A_1, \dots, A_n\}$, $C_2 = C'_2 \cup \{\neg B_1, \dots, \neg B_m\}$; je-li σ mgu množiny $\{A_1, \dots, A_n, B_1, \dots, B_m\}$, je rezolventou $C = C'_1\sigma \cup C'_2\sigma$.

 **Intuice.** *Unifikátor* množiny výrazů je substituce, která je syntakticky *ztotožní* ($E_1\sigma = \dots = E_k\sigma$). *Nejobecnější* z nich (mgu) je „nejméně zavazující“: sváže jen nezbytné a každý jiný unifikátor θ z něj vznikne dodatečným dosazením, $\theta = \sigma\lambda$. Např. $P(x)$ a $P(y)$ má mgu $\sigma = \{x/y\}$ (výsledek $P(y)$); také $\theta = \{x/a, y/a\}$ je unifikuje, ale *konkrétněji* ($\theta = \sigma\lambda$ s $\lambda = \{y/a\}$) – zbytečně se upnul na a . V rezoluci proto bereme *vždy* mgu: s konkrétnější unifikací bychom ztratili obecnost rezolventy a rezoluce by nebyla úplná (mgu je jednoznačný až na přejmenování proměnných).

Klauzule mají *lokální* proměnné (implicitně univerzálně kvantované), proto je před řezem přejmenujeme na disjunktí a pak *unifikujeme* řezané literály nejobecnějším způsobem (mgu). Mgu hledáme *zleva*: porovnáváme termy a vynucujeme potřebné rovnosti. Např. $P(f(x), y)$ a $P(f(a), w)$ unifikuje $\sigma = \{x/a, y/w\}$; naopak x a $f(x)$ unifikovat *nelze*, protože x se vyskytuje uvnitř $f(x)$ (tzv. *occurs-check*). Na rozdíl od výrokové logiky je dovoleno řezat přes *více* literálů naráz: po unifikaci se totiž dva literály téže klauzule mohou ztotožnit („faktorizace“), např. $\{P(x), P(y)\}$ se přes $\{x/y\}$ slije na $\{P(y)\}$. Korektnost a úplnost zůstávají (úplnost se „zvedne“ z výrokové přes Herbrandovu větu).

Příklad – Rezoluce v PL: holičův paradox

Zadání.

„Každý holič holí právě ty, kdo neholí sami sebe.“ Dokažte rezolucí, že *žádný holič neexistuje*. Jazyk $\langle B, S \rangle$ ($B(x)$ – „ x je holič“, $S(x, y)$ – „ x holí y “).

Řešení.

Formalizace.

„Holič holí právě ty, kdo neholí sami sebe“ dává ekvivalenci $S(x, y) \leftrightarrow \neg S(y, y)$ platnou pro každého y , jakmile je x holič:

$$T = \{(\forall x)(B(x) \rightarrow (\forall y)(S(x, y) \leftrightarrow \neg S(y, y)))\}.$$

Dokazované tvrzení je $\psi = \neg(\exists x)B(x)$ („neexistuje holič“); podle „platnost = nesplnitelnost“ zamítáme $T \cup \{\neg\psi\}$, kde $\neg\psi = (\exists x)B(x)$.

Skolemizace a CNF.

Jediný existenční kvantifikátor je v negovaném cíli.

- *Negovaný cíl* $(\exists x)B(x)$: před $\exists x$ nestojí žádný $\forall$, svědek je tedy *konstanta* c – vznikne $B(c)$ (klauzule C_3).
- *Premisa*: po rozepsání $\leftrightarrow$ a zatažení $B(x)$ pod $\forall y$ je *čistě univerzální*

$$(\forall x)(\forall y)(B(x) \rightarrow [(S(x, y) \rightarrow \neg S(y, y)) \wedge (\neg S(y, y) \rightarrow S(x, y))]),$$

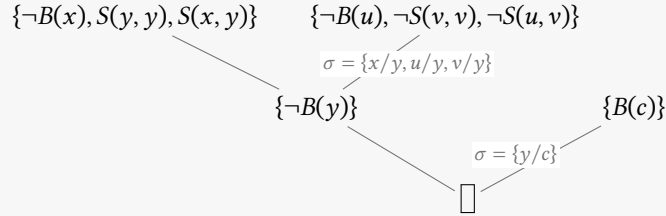
takže *neobsahuje žádný* $\exists$ a skolemizovat není co (žádné Skolemovy funkce).

Vypuštěním $\forall$ a převodem jádra premisy do CNF ($\neg B(x)$ se distribuuje přes obě implikace) vzniknou dvě klauzule; po přejmenování proměnných na disjunktí (x, y v první, u, v ve druhé) dostáváme

$$S = \{ \underbrace{\{\neg B(x), S(y, y), S(x, y)\}}_{C_1}, \underbrace{\{\neg B(u), \neg S(v, v), \neg S(u, v)\}}_{C_2}, \underbrace{\{B(c)\}}_{C_3} \}.$$

Rezoluce.

Řez C_1, C_2 proběhne přes *všechny* jejich S -literály naráz. Mgu najdeme krok po kroku: ztotožníme $S(x, y)$ s $S(y, y)$ (vynutí x/y), pak $S(u, v)$ s $S(y, y)$ (vynutí $u/y, v/y$); tím se i $S(v, v)$ stane $S(y, y)$. Společné mgu je $\sigma = \{x/y, u/y, v/y\}$ a všechny čtyři S -literály splynou na $S(y, y)$, takže rezolventa je $\{\neg B(y)\}$. Řez s C_3 (unifikace $\{y/c\}$) dá $\square$. Žádný holič tedy nemůže existovat.



Rezoluční zamítnutí holičova paradoxu. Řez C_1, C_2 přes dva literály (unifikace σ je sjednotí na $S(y, y)$) dá $\{\neg B(y)\}$; po řezu s $\{B(c)\}$ vzniká $\square$. U hran jsou použité unifikace.

4.5 Hilbertovský kalkulus

Poznámka. Hilbertovský kalkulus je třetí systém: pevná **schémata axiomů** (logických tautologií, např. $\varphi \rightarrow (\psi \rightarrow \varphi)$; v PL navíc $(\forall x)\varphi \rightarrow \varphi(x/t)$) a jediné odvozovací pravidlo *modus ponens* (z φ a $\varphi \rightarrow \psi$ odvod ψ); v PL ještě pravidlo generalizace. *Důkaz* je posloupnost formulí, každá axiom nebo odvozená z předchozích. Je korektní a úplný, ale důkazy se hledají pracně – hodí se spíš teoreticky. Platí **věta o dedukci**: pro sentenci φ je $T, \varphi \vdash \psi \iff T \vdash \varphi \rightarrow \psi$ (pro formuli s volnou proměnnou by generalizace větu pokazila).

4.6 Souhrnná úloha: model teorie

Následující reálná otázka SZZ propojuje syntaxi (formalizace), sémantiku (model teorie) i dokazatelnost (hledání modelu vs. zamítnutí).

Příklad – SZZ léto 2024 č. 4: Model teorie

(Reálná otázka SZZ: léto 2024, č. 4 – Model teorie)

Zadání.

- (1) Definujte pojmy *struktura jazyka* $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a *model teorie* T .
- (2) V jazyce $L = \langle Z, S, P \rangle$ (unární predikáty: „složit zkoušku“, „mít štěstí“, „být připraven“) vyjádřete: (a) *Ne každý, kdo složí zkoušku, má štěstí, ale kdo má štěstí, zkoušku složí.* (b) *Štěstí přeje připraveným. (Kdo je připraven, má štěstí.)* (c) *Nějaký student byl připraven, ale zkoušku nesložil.*
- (3) Pro $T_1 = \{\varphi_1, \varphi_2\}$ a $T_2 = \{\varphi_1, \varphi_2, \varphi_3\}$ najděte model, nebo formálně dokažte, že žádný nemá.

Řešení.

- (1) *Struktura* $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ je neprázdná doména A s realizacemi: $R^{\mathcal{A}} \subseteq A^{\text{ar}(R)}$ pro každý relační symbol a $f^{\mathcal{A}} : A^{\text{ar}(f)} \rightarrow A$ pro každý funkční symbol (konstanta $c^{\mathcal{A}} \in A$). *Model teorie* T je struktura, v níž platí všechny axiomy T .
- (2) Přirozená formalizace:

$$\varphi_1 : \neg(\forall x)(Z(x) \rightarrow S(x)) \wedge (\forall x)(S(x) \rightarrow Z(x)),$$

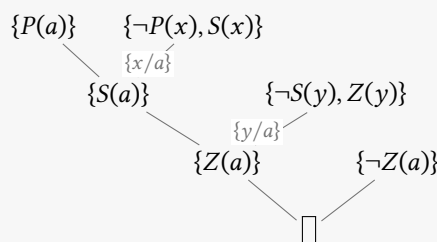
$$\varphi_2 : (\forall x)(P(x) \rightarrow S(x)), \quad \varphi_3 : (\exists x)(P(x) \wedge \neg Z(x)),$$

kde (dle zadání) Z značí „složit zkoušku“, S „mít štěstí“, P „být připraven“.

- (3) T_1 má model: jednoprvková doména $A = \{0\}$ s $S^{\mathcal{A}} = \{0\}$, $S^{\mathcal{A}} = P^{\mathcal{A}} = \emptyset$. Ověření: φ_2 platí (nikdo není připraven), φ_1 platí, protože $(\forall x)(S(x) \rightarrow Z(x))$ je vakuózně pravdivé a $\neg(\forall x)(Z(x) \rightarrow$

$S(x)$) platí, neboť $0 \in Z$, $0 \notin S$.

T_2 model nemá: z φ_3 je nějaký a připraven a nesložil ($P(a)$, $\neg Z(a)$). Z φ_2 pak $S(a)$, z druhé části φ_1 (tj. $S(a) \rightarrow Z(a)$) dostáváme $Z(a)$ – spor s $\neg Z(a)$. Formálně převedeme T_2 na klauzule (skolemizace + CNF): z $\varphi_3 = (\exists x)(P(x) \wedge \neg Z(x))$ skolemizací (existenční svědek – konstanta a) vzniknou $\{P(a)\}$ a $\{\neg Z(a)\}$; z φ_2 klauzule $\{\neg P(x), S(x)\}$ a z druhé části φ_1 , tj. $(\forall x)(S(x) \rightarrow Z(x))$, po přejmenování proměnné klauzule $\{\neg S(y), Z(y)\}$. První část φ_1 dá skolemizací (další konstanta b) klauzule $\{Z(b)\}$, $\{\neg S(b)\}$, ty ale k zamítnutí nepotřebujeme. Rezolucí (strom níže) odvodíme $\square$, takže T_2 nemá model.



Rezoluční zamítnutí T_2 (svědek a z φ_3): řezy s unifikacemi $\{x/a\}$, $\{y/a\}$ vedou k $\square$, takže T_2 nemá model.

5 Věty o kompaktnosti a úplnosti

Metavěty spojují obě patra logiky: *korektnost* a *úplnost* ztotožní dokazatelnost s platností, *kompaktnost* a *Löwenheim-Skolemova věta* jsou jejich silné důsledky. U všech stačí znát znění a význam.

5.1 Korektnost a úplnost

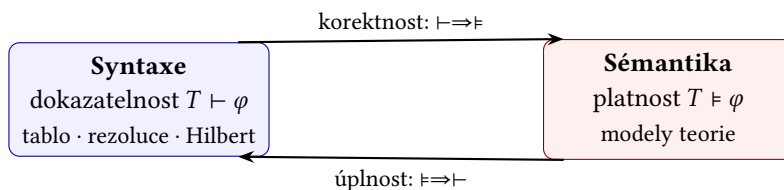
★ Věta – O korektnosti a úplnosti

Tablo metoda i rezoluce jsou *korektní* a *úplné*: pro každou (spočetnou) teorii T a sentenci φ platí

$$T \vdash \varphi \iff T \models \varphi.$$

(Pro rezoluci ve tvaru: množina klauzulí je *nesplnitelná* právě tehdy, když je *rezolucí zamítnutelná*.)

Intuice. **Korektnost** ($\vdash \Rightarrow \models$) je „bezpečnost“: co dokážeme, opravdu platí (sporné tablo nemůže mít model). **Úplnost** ($\models \Rightarrow \vdash$) je „síla“: každou platnou věc kalkulus dokáže (z dokončené bezesporné větve bychom jinak sestrojili *kanonický model* – protipříklad). Dohromady je dokazatelnost přesně platnost: syntaxe a sémantika „vidí totéž“ (viz obrázek).



z úplnosti + *konečnosti důkazů* plyne **věta o kompaktnosti**

Korektnost a úplnost ztotožňují dokazatelnost ($\vdash$) s platností ($\models$). Tablo důkaz je vždy *konečný*, použije tedy jen konečně mnoho axiomů – odtud kompaktnost.

Poznámka. „Úplnost“ a „kompletnost“ **nezaměňovat**. *Úplnost kalkulu* je vlastnost *dokazovacího systému*: $T \models \varphi \Rightarrow T \vdash \varphi$ (co platí, umíme dokázat). *Kompletní teorie* je vlastnost *teorie*: o každé sentenci rozhodne – je v ní pravdivá, nebo lživá (žádná otevřená otázka; viz sekci 6). Jsou to různé

pojmy s matoucně podobnými názvy. Pozor zvlášť na Gödela: „věta o neúplnosti“ (sekce 6) říká, že dostatečně silná teorie *není kompletní* – popírá tedy *kompletnost teorie*, nikoli úplnost kalkulu (ta platí dál).

5.2 Věta o kompaktnosti

★ Věta – O kompaktnosti (výrokové i predikátové logiky)

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

💡 Intuice. Jedna implikace je triviální (model celku je modelem každé části). Druhá je obsahem věty: *lokální* splnitelnost (po konečných kouscích) vynutí *globální*. Důvod (náčrt): nemá-li T model, je sporná, tedy $T \vdash \perp$ (úplnost); ale důkaz je *konečný* a použije jen konečně mnoho axiomů $T' \subseteq T$ – a už ta konečná T' je sporná. Kompaktnost je most mezi konečným a nekonečným.

🔗 Příklad – Použití kompaktnosti

Zadání.

Ukažte, že (spočetně) nekonečný graf G je bipartitní (2-obarvitelný), právě když je bipartitní *každý jeho konečný podgraf*.

Řešení. Pro každý vrchol v vezměme prvovýrok p_v („ v má barvu 1“) a teorii

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

(„sousedé mají různé barvy“). Modely T odpovídají dvojobarvení G , tedy G je bipartitní právě tehdy, když má T model. Podle kompaktnosti stačí, aby měla model *každá konečná* $T' \subseteq T$. Taková T' mluví o konečně mnoha hranách, tj. o konečném podgrafu G' ; ten je z předpokladu bipartitní, a jeho obarvení je modelem T' . Tedy T má model a G je bipartitní. (Stejnou šablonou se dokáže *k-obarvitelnost nebo rozšíření částečného uspořádání na lineární*.)

💡 Intuice. Druhá slavná aplikace: k $\text{Th}(\mathbb{N})$ (všem pravdivým sentencím standardní aritmetiky) přidáme konstantu c a axiomy $\underline{n} < c$ pro všechna n . Každá konečná část má model (c = dost velké číslo), takže podle kompaktnosti má model i celek – *nonstandardní model* aritmetiky s prvkem větším než všechna „obyčejná“ čísla.

5.3 Löwenheim-Skolemova věta

★ Věta – Löwenheim-Skolem

Každá bezesporná teorie ve spočetném jazyce má *spočetný* model (bez rovnosti spočetně nekonečný; s rovností konečný nebo spočetně nekonečný).

💡 Intuice. Plyne z úplnosti: dokončené bezesporné tablo dá kanonický model, jehož doménou jsou konstantní termy – a těch je jen spočetně. Důsledek je překvapivý: i teorie „velkých“ struktur (např. reálných čísel) má spočetný model. Odtud plyne existence elementárně ekvivalentních, ale neizomorfních struktur: $\text{Th}(\langle \mathbb{R}, \leq \rangle)$ má spočetný model, a ten s nespočetnou $\langle \mathbb{R}, \leq \rangle$ izomorfní být nemůže (konkrétně $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, viz DeLO v sekci 6).

6 Rozhodnutelnost

Poslední otázka je algoritmická: umíme pro danou teorii *strojově* rozhodnout, co z ní plyne? Klíčem je pojem *kompletní* teorie a jeho vztah k rozhodnutelnosti.

6.1 Kompletní teorie a kritéria kompletnosti

Definice – Kompletní teorie, elementární ekvivalence

Struktury $\mathcal{A}, \mathcal{B}$ jsou *elementárně ekvivalentní* ($\mathcal{A} \equiv \mathcal{B}$), platí-li v nich tytéž sentence. Teorie T je *kompletní*, je-li bezesporná a každá sentence je v ní pravdivá, nebo lživá (táž definice jako ve výrokové logice, sekce 2). Ekvivalentně: T je kompletní právě tehdy, když má jediný model až na elementární ekvivalenci.

 **Intuice.** Kompletní teorie „úplně popisuje“ svůj typ struktury – o žádné sentenci nenechává otázku otevřenou. Pozor: na rozdíl od výrokové logiky to *neznamená* jediný model (jeden model má vždy nekonečně mnoho izomorfních kopií), jen jedinou *teorii struktury* $\text{Th}(\mathcal{A})$.

★ Věta – Kritérium kompletnosti přes ω -kategoricitu

Je-li teorie T ve spočetném jazyce ω -kategorická (má až na izomorfismus jediný spočetně nekonečný model) a je-li jazyk bez rovnosti, nebo T nemá konečné modely, pak je T *kompletní*.

 **Intuice.** Myšlenka: podle Löwenheim-Skolemovy věty je každý model T elementárně ekvivalentní nějakému spočetně nekonečnému modelu (bez rovnosti vždy, s rovností pro nekonečné modely – proto předpoklad, že konečné modely nejsou). Ten je ale podle ω -kategoricity až na izomorfismus jediný, takže jsou *všechny* modely T navzájem elementárně ekvivalentní – a to je kompletnost. Příklad: **DeLO** (hustá lineární uspořádání bez konců, jako $\langle \mathbb{Q}, \leq \rangle$) je ω -kategorická (metoda „cik-cak“), tedy *kompletní*; teorie tak rozhodne každou sentenci o hustých lineárních uspořádáních bez konců.

6.2 Rozhodnutelnost a její vztah ke kompletnosti

Definice – Rozhodnutelná teorie

Teorie T je *rozhodnutelná*, existuje-li algoritmus, který pro každou vstupní sentenci φ doběhne a odpoví, zda $T \models \varphi$. Je *rekurzivně axiomatizovaná*, lze-li algoritmicky rozpoznat, které formule jsou její axiomy.

★ Věta – Kompletnost dává rozhodnutelnost

Bezesporná *rekurzivně axiomatizovaná* a *kompletní* teorie je *rozhodnutelná*.

 **Intuice.** Algoritmus: pro vstup φ konstruujeme *paralelně* systematické tablo důkazy pro φ (tablo s $F\varphi$) a pro $\neg\varphi$ (tablo s $T\varphi$). Z kompletnosti je dokazatelná právě jedna z nich, a díky korektnosti+úplnosti a konečnosti důkazů se příslušné tablo po konečně mnoha krocích uzavře – algoritmus tak vždy doběhne a odpoví. (Sama rekurzivní axiomatizace dává jen *částečnou* rozhodnutelnost; teprve kompletnost zaručí, že se dočkáme i záporné odpovědi.)

6.3 Příklady rozhodnutelných a nerozhodnutelných teorií

Rozhodnutelné	Nerozhodnutelné
hustá lineární uspořádání (DeLO)	predikátová logika obecně (Churchova věta)
Presburgerova aritmetika $\text{Th}(\langle \mathbb{N}, S, +, 0 \rangle)$	plná aritmetika $\text{Th}(\mathbb{N})$ ($s + i \cdot$)
algebraicky uzavřená tělesa	Robinsonova/Peanova aritmetika
reálně uzavřená tělesa (i euklidovská geometrie)	Hilbertův 10. problém (diofantické rovnice; problém, ne teorie)
teorie konečné struktury (v konečném jazyce)	teorie grup, ZFC

★ Věta – Churchova věta

Predikátová logika je *nerozhodnutelná*: neexistuje algoritmus, který by pro každou vstupní formuli (v libovolném jazyce, ten je součástí vstupu) rozhodl, zda je logicky platná ($\models \varphi$).

💡 **Intuice.** Dokazuje se *redukcí* z nerozhodnutelného problému (existence přirozeného řešení diofantické rovnice, Hilbertův 10. problém): pro sentenci $\varphi = (\exists \bar{x}) p(\bar{x}) = q(\bar{x})$ platí $\mathbb{N} \models \varphi \iff \models \psi_Q \rightarrow \varphi$, kde ψ_Q je konjunkce (konečně mnoha) axiomů Robinsonovy aritmetiky Q . Algoritmus na platnost by tedy rozhodl i Hilbertův problém. Nerozhodnutelnost je vlastnost *obecného* případu: v jazyce jen s unárními relačními symboly (bez funkčních) je platnost rozhodnutelná. Predikátová logika je ovšem *částečně* rozhodnutelná (je-li $\models \varphi$, tablo to po konečně krocích potvrdí) – jen u neplatných formulí výpočet nemusí skončit.

★ Věta – Gödelovy věty o neúplnosti

(1. věta) Každá bezesporná rekurzivně axiomatizovaná teorie obsahující „dostatek aritmetiky“ (Robinsonovu aritmetiku), jejímž modelem je standardní $\mathbb{N}$, je *neúplná*, tj. *není kompletní*: existuje sentence pravdivá v $\mathbb{N}$, kterou teorie nedokáže ani nevyvrátí. (2. věta) Je-li navíc dostatečně silná (postačí extenze Peanovy aritmetiky), nedokáže (zformalizovanou) *vlastní bezespornost*.

💡 **Intuice.** Aritmetika přirozených čísel je principiálně „příliš bohatá“ na úplné efektivní zachycení: pravdivost v $\mathbb{N}$ *nelze* ztotožnit s dokazatelností v žádné rozumné teorii. Proto $\text{Th}(\mathbb{N})$ ani není rekurzivně axiomatizovatelná, a je *nerozhodnutelná*. (Důkazy – diagonalizace, aritmetizace syntaxe – jsou nad rámec M6; stačí znát znění a smysl.)

Shrnutí

📌 **Poznámka. Klíčové vlastnosti a vzorce (přehled k SZZ).** Stručný výčet klíčových definic, vět a vzorců okruhu M6. Zkratky: VL = výroková logika, PL = predikátová logika prvního řádu, mgu = nejobecnější unifikátor.

Syntaxe VL a PL.

- VL: jazyk = neprázdná množina prvovýroků $\mathbb{P}$; formule induktivně ($p \in \mathbb{P}$; $\neg\varphi$; $\varphi \sqcap \psi$); *strom výroku* = strukturální analýza; *podvýrok* = podstrom.
- PL: jazyk dán signaturou $\langle \mathcal{R}, \mathcal{F} \rangle$ (relační a funkční symboly s aritami; konstanta = nulární funkce). *Termy* induktivně (proměnné, konstanty, $f(t_1, \dots, t_n)$). *Formule*: atomy $R(\bar{t})$ nebo $=$, pak $\neg, \sqcap, (\forall x)\varphi, (\exists x)\varphi$.
- Výskyt proměnné x je *vázaný* uvnitř $(\forall x)\psi$ nebo $(\exists x)\psi$, jinak *volný*. *Otevřená* formule = bez kvantifikátoru; *uzavřená* (sentence) = bez volné proměnné. Sentence má hodnotu nezávisle na ohodnocení.

- *Instance* $\varphi(x/t)$: nahraď volné výskyty x termem t (podmínka substituovatelnosti: t nesmí zachytit volnou proměnnou). *Varianta*: přejmenuj vázanou proměnnou (bezpečná příprava před dosazením).
- *Struktura* $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$: neprázdná doména A ; pro n -ární R : realizace $R^{\mathcal{A}} \subseteq A^n$; pro n -ární f : $f^{\mathcal{A}} : A^n \rightarrow A$ (konstanta $c^{\mathcal{A}} \in A$). *Model teorie* T = struktura, v níž platí všechny axiomy.

Normální formy (CNF, DNF, PNF) a skolemizace.

- *Literál* = p nebo $\neg p$; *klauzule* = disjunkce literálů; *elementární konjunkce* = konjunkce literálů. **CNF** = konjunkce klauzulí; **DNF** = disjunkce elem. konjunkcí; existují vždy ke každé formuli.
- Převod **sémanticky**: DNF = jedna elem. konjunkce na každý *model* ($p^{v(p)}$); CNF = jedna klauzule na každý *nemodel* ($p^{1-v(p)}$). Převod **úpravami**: eliminuj $\leftrightarrow, \rightarrow$; zatlač $\neg$ k listům (de Morgan); distribuuj.
- Prázdná klauzule $\square$ je nesplnitelná; prázdná elem. konjunkce je tautologie. CNF tautologie $\iff$ každá klauzule obsahuje opačné literály; DNF splnitelné $\iff \exists$ elem. konjunkce bez opačných literálů. CNF je vstupem **SAT** (NP-úplné; řeší se rezolucí nebo DPLL).
- **PNF** (prenexní): tvar $(Q_1 x_1) \dots (Q_n x_n) \varphi'$, kde $Q_i \in \{\forall, \exists\}$ a φ' otevřená. Postup: eliminuj $\leftrightarrow, \rightarrow$; flip $\neg Q \sim \bar{Q}\neg$; vytahuj kvantifikátory ven. **Klíčová past**: $\forall$ v antecedentu implikace se překlápí na $\exists$ ($((\forall x)\varphi) \rightarrow \psi \sim (\exists x)(\varphi \rightarrow \psi)$).
- **Skolemizace**: sentence $\rightarrow$ PNF $\rightarrow$ nahraď každé $(\exists y)$ (před nímž stojí $\forall x_1, \dots, \forall x_m$) novým m -árním funkčním symbolem $f(x_1, \dots, x_m)$ ($m=0$: konstanta) $\rightarrow$ vypusť zbylé $\forall$. Výsledek je *ekvisplnitelná* otevřená teorie (ne ekvivalentní); nutno skolemizovat ze sentence.

Sémantika: model, platnost, důsledek.

- VL: ohodnocení $v : P \rightarrow \{0, 1\}$, hodnota výroku rekurzivně po stromu; $v \models \varphi$, $M(\varphi)$, $M(T) = \bigcap M(\varphi_i)$. PL: Tarskiho rekurze – $H^{\mathcal{A}}((\forall x)\varphi)[e] = \min_{a \in A} H^{\mathcal{A}}(\varphi)[e(x/a)]$; $\exists$ je max.
- **Tautologie** $\models \varphi$: $M(\varphi) = M_P$; **sporný**: $M(\varphi) = \emptyset$; **nezávislý**: vlastní neprázdná část; **splnitelný**: $M(\varphi) \neq \emptyset$. Kategorie jsou vzájemně vylučné (vyjma splnitelnost).
- **Důsledek** $T \models \varphi$: $M(T) \subseteq M(\varphi)$ (každý model T je modelem φ). **Klíčová ekvivalence**: $T \models \varphi \iff T \cup \{\neg\varphi\}$ nemá model – základ důkazů sporem (tablo, rezoluce).
- Analýza teorie nad $|P| = n$: celkem 2^n ohodnocení; teorie s k modely má $(2^k - 2) \cdot 2^{n-k}$ nezávislých výroků (libovolná volba na $2^n - k$ ohodnoceních mimo $M(T)$, netriviální na k modelech T).
- **Kompletní teorie** = bezesporná a bez nezávislé sentence. VL: právě tehdy, když má *jediný* model; PL: *jediný* model až na *elementární ekvivalenci* ($\mathcal{A} \equiv \mathcal{B}$: tytéž sentence).

Extenze teorií.

- Extenze T' teorie T (jazyk $L \subseteq L'$): $\text{Csq}_L(T) \subseteq \text{Csq}_{L'}(T')$; pro jednoduché extenze ($L' = L$) ekvivalentní $M(T') \subseteq M(T)$ (více axiomů = méně modelů = silnější teorie).
- **Konzervativní** extenze: o původním jazyce L nedokáže nic nového. *Extenze o definice* je vždy konzervativní (každý model T se na model T' expanduje jednoznačně): relační $R(\bar{x}) \leftrightarrow \psi(\bar{x})$; funkční: nutno axiom existence a jednoznačnosti ψ v T .
- *Ekvisplnitelnost*: T a T' (různé jazyky) mají model oba, nebo žádný. Skolemizace $\Rightarrow$ ekvisplnitelná (ne ekvivalentní) extenze; stačí pro důkaz sporem.

Dokazatelnost: tablo, rezoluce, Hilbert.

- Obecné schéma: $T \vdash \varphi$ dokažeme sporem – sporujeme $T \cup \{\neg\varphi\}$ (kořen tabla $F\varphi$; vstup rezoluce $T \cup \{\neg\varphi\}$ v CNF).
- **Tablo VL**: položky $T\psi/F\psi$; atomická tabla: $T\wedge$: oba pod sebou; $F\wedge$: větví; $T\vee$: větví; $F\vee$: oba; $T\rightarrow$: větví ($F\varphi \mid T\psi$); $F\rightarrow$: $T\varphi, F\psi$; $T\neg$: $F\varphi$; $F\neg$: $T\varphi$. Sporná větev $\otimes$: $T\psi$ a $F\psi$ na téže větví. Dokončená bezesporná větev $\Rightarrow$ kanonický model $v(p) = 1 \iff Tp$ na větví.
- **Tablo PL**: tytéž spojkové rozvoje + kvantifikátorová pravidla – „svědek“ ($T(\exists x)\varphi \rightsquigarrow T\varphi(x/c)$, $F(\forall x)\varphi \rightsquigarrow F\varphi(x/c)$, kde c nový); přidáme konstantu pro existenci; „všichni“ ($T(\forall x)\varphi \rightsquigarrow T\varphi(x/t)$ pro libovolný term t , $F(\exists x)\varphi \rightsquigarrow F\varphi(x/t)$); položka zůstává „nehotová“, opakuje se. Jazyk s rovností: přidej axiomy rovnosti.
- **Rezoluce VL**: CNF v množinové repr.; rezolventa C_1, C_2 přes literál ℓ : $(C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\bar{\ell}\})$;

zamítnutí = odvození $\square$; nesplnitelná $\iff$ zamítnutelná. Řez vždy jen přes jednu dvojici opačných literálů (ne přes dvě zároveň).

- **Rezoluce PL:** skolemizace + CNF $\rightarrow$ přejmenuj proměnné klauzulí na disjunktí $\rightarrow$ najdi mgu řezaných literálů (occurs-check: x nelze unifikovat s $f(x)$) $\rightarrow$ rezolventa = zbytky po aplikaci mgu.
- **Hilbert:** schémata logických tautologií jako axiomů + modus ponens; v PL navíc generalizace. Věta o dedukci (pro sentenci φ): $T, \varphi \vdash \psi \iff T \vdash \varphi \rightarrow \psi$. Spíše teoretický nástroj.

Věty o korektnosti, úplnosti a kompaktnosti.

- **Korektnost** ($\vdash \Rightarrow \models$): co je dokazatelné, platí. **Úplnost** ($\models \Rightarrow \vdash$): co platí, je dokazatelné. Dohromady $T \vdash \varphi \iff T \models \varphi$. Pro rezoluci: S nesplnitelná $\iff S$ rezolucí zamítnutelná.
- **Pozor na záměnu:** *úplnost kalkulu* ($\models \Rightarrow \vdash$, vlastnost dokazovacího systému) $\neq$ *kompletnost teorie* (o každé sentenci rozhodne, vlastnost teorie). Gödelova věta o *neúplnosti* mluví o *nekompletnosti teorie*, ne o kalkulu.
- **Kompaktnost:** T má model $\iff$ každá konečná $T' \subseteq T$ má model. Plyne z úplnosti (důkaz je konečný $\Rightarrow$ použije jen konečně mnoho axiomů). Aplikace: nekonečný graf bipartitní $\iff$ každý konečný podgraf bipartitní; existence nestandardního modelu aritmetiky.
- **Löwenheim-Skolem:** bezesporná teorie ve spočetném jazyce má spočetný model (bez rovnosti spočetně nekonečný; s rovností konečný nebo spočetně nekonečný). Překvapivý důsledek: i teorie reálných čísel má spočetný model.

Rozhodnutelnost.

- Kritérium ω -kategoricity: teorie ve spočetném jazyce bez rovnosti (nebo bez konečných modelů) je *kompletní*, je-li ω -kategorická (jediný spočetně nekonečný model až na $\cong$). Příklad: **DeLO** (hustá lin. uspořádání bez konců, jako $\langle \mathbb{Q}, \leq \rangle$) – ω -kategorická, tedy kompletní.
- *Rekurzivně axiomatizovaná + kompletní $\Rightarrow$ rozhodnutelná:* paralelně budujeme tabla pro φ a $\neg\varphi$; kompletnost zaručí, že jedno skončí po konečně krocích.
- **Rozhodnutelné:** DeLO; Presburgerova aritmetika $\text{Th}(\langle \mathbb{N}, S, +, 0 \rangle)$; algebraicky uzavřená tělesa; reálně uzavřená tělesa; teorie konečné struktury (v konečném jazyce).
- **Nerohodnutelné:** predikátová logika (Churchova věta, jazyk je součástí vstupu – redukce z Hilbertova 10. problému; PL je ale *částečně* rozhodnutelná: $\models \varphi$ tablo potvrdí, zápornou odpověď ne); $\text{Th}(\mathbb{N})$ (plná aritmetika s $+$, $\cdot$); Robinsonova/Peanova aritmetika.
- **Gödelovy věty o neúplnosti** (znění): (1.) každá bezesporná rek. axiomatizovaná teorie s dostatkem aritmetiky (a s modelem $\mathbb{N}$) *není kompletní* (existuje sentence pravdivá v $\mathbb{N}$ bez důkazu i vyvrácení v T); (2.) taková teorie nedokáže vlastní bezespornost.

Zdroje

- J. Bulín: *NAIL062 Výroková a predikátová logika: zápisky z přednášky*, MFF UK, zimní semestr 2025 (primární zdroj výkladu: syntaxe a sémantika VL i PL, normální formy, tablo metoda, rezoluce, extenze a skolemizace, věty o úplnosti a kompaktnosti, rozhodnutelnost, Gödelovy věty). Existuje i anglická verze *Propositional and Predicate Logic: Lecture Notes*.
<https://github.com/jbulin-mff-uk/nail062>
- J. Bulín: sady příkladů ke cvičení NAIL062 se vzorovými řešeními (kalibrace hloubky řešených příkladů).
<https://github.com/jbulin-mff-uk/nail062/tree/main/tutorial/priklady>
- A. Nerode, R. A. Shore: *Logic for Applications*, 2. vyd., Springer, 1997, a M. Ben-Ari: *Mathematical Logic for Computer Science*, 3. vyd., Springer, 2012 (učebnice, na nichž stojí přednáška).
- MFF UK: požadavky ke státní závěrečné zkoušce (Informatika, Bc.) a zadání otázek z minulých termínů.
<https://www.mff.cuni.cz/cs/studenti/bakalarske-studium/statni-zaverecne-zkousky/bakalarske-statni-zkousky-studijniho-programu-informatika>