Sbírka příkladů k předmětu MA007 – Matematická logika

Petr Novotný Ľuboš Korenčiak

Fakulta informatiky Masarykovy univerzity

Autoři děkují Fondu rozvoje vysokých škol za podporu vzniku této sbírky v rámci projektu „Rozšíření studijních materiálů k předmětu matematická logika,“ projekt č. FRVS/511/2013.

Úvod

Základním cílem vědního oboru matematické logiky je konstrukce a studium tzv. *formálních systémů*. Zjednodušeně řečeno, formální systém je nějaký matematický model abstraktního myšlení. Takový model se obvykle skládá ze sady symbolů a souboru pravidel pro manipulaci s těmito symboly. Důležité je, že uvedené symboly nenesou a priori žádný význam (ten jim „zvenčí“ musí dodat někdo, kdo tyto symboly interpretuje) a manipulace s nimi je čistě mechanická. Jedná se tedy o model takového druhu myšlení, které je v principu simulovatelné našimi běžnými počítači. Zda takový model poskytuje *veškeré* lidské myšlení, to je hluboká filosofická otázka, kterou se v tomto předmětu zabývat nebudeme. I přesto je užitečné se matematickou logikou zabývat, minimálně ze dvou níže uvedených důvodů.

Z matematického hlediska je užitečné mít jasno v tom, kdy je nějaký výsledek skutečně nevyvratitelně dokázán, a za jakých předpokladů. V matematice se prakticky nikdy nepoužívají stoprocentně formální důkazy, neboť takové důkazy by byly pro člověka nečitelné. Vždy se nechává prostor pro čtenáře, aby si doplnil některé myšlenkové kroky, a důkaz se pokládá za dostatečný, pokud svého čtenáře přesvědčí. Takovýmto důkazům v našem předmětu říkáme *metadůkazy*, neboť využívají něco co leží mimo zkoumaný formální systém, například čtenářovy znalosti či intuici. Matematici si dlouho vystačili pouze s těmito metadůkazy. Časem ovšem zjistili, že matematika založená na intuitivním chápání základních pojmů v sobě obsahuje neřešitelné spory, viz například známý Russelův paradox. Začala tedy snaha o striktní formalizaci matematiky, která by ji zbavila veškerého nánosu intuice. Existovalo dokonce přesvědčení, že veškerou matematiku lze redukovat na několik základních axiomů a mechanickou manipulaci s nimi. Paradoxně to byl právě logik Kurt Gödel, který svými větami o neúplnosti ukázal, že něco takového v principu není možné. Na druhou stranu se ukazuje, že i když není možné zmechanizovat *veškerou* matematiku, je možné zmechanizovat v podstatě veškerou matematiku kterou kdy lidé používali. Existuje několik projektů, jejichž cílem je s pomocí počítačů najít mecha-

nické důkazy co největšího množství známých matematických tvrzení (viz např. projekty *Mizar* a *Metamath*). Vzhledem k tomu, že některé slavné důkazy mají desítky, ba i stovky stran, a jsou tedy těžko zkontrolovatelné i těmi nejlepšími matematiky, jde zajisté o chvályhodný počin. Mimo to, studium formálních důkazů umožnilo matematikům uvědomit si, jaké předpoklady (axiomy) potřebují k provedení daného důkazu. Některá základní tvrzení z různých oborů (např. topologie či matematické analýzy) se opírají o tzv. axiom výběru, který i dnes (byť jen ve velmi malé míře) vyvolává jistou kontroverzi – jak vzhledem ke své nekonstruktivní podstatě, tak vzhledem k některým neintuitivním výsledkům, které umožňuje dokázat.

Snad ještě důležitější je informatický pohled na matematickou logiku. Jak již bylo řečeno, matematická logika modeluje ty oblasti přemýšlení, které jsou simulovatelné počítačem. Poskytuje nám tedy přirozený jazyk, pomocí kterého lze počítači předkládat různé úlohy k řešení. Například v oblasti verifikace programů obvykle chceme formálně dokázat, že nějaký systém má nějakou vlastnost, obvykle popsatelnou vhodnou logickou formulí. To ovšem často může být nadlidský úkol, neboť zmíněné systémy bývají vysoce komplexní (a i kdyby byl důkaz proveditelný člověkem, u systémů jako jsou řídící jednotky letadel či operační systémy v jaderných elektrárnách nemusí být žádoucí spolehnout se pouze na úsudek člověka). V takové situaci je ideálním řešením předat počítači vhodnou formální specifikaci systému a požadované vlastnosti a nechat jej mechanicky najít důkaz správnosti/bezpečnosti atd. daného systému. Abychom mohli počítače naprogramovat k řešení těchto problémů, či vůbec používat výsledné programy (tj. umět specifikovat vlastnosti systémů pomocí formulí různých logik), je třeba mít alespoň základní přehled o tom, jak logické systémy fungují.

Pevně doufáme, že tato sbírka úloh, opatřená doplňujícími vysvětlujícími komentáři, napomůže čtenáři k získání tohoto přehledu.

Obsah

Kapitola 1

Syntax výrokové logiky

1.1 „Standardní“ výroková logika

V této sekci se setkáme s prvním formálním systémem: výrokovou logikou s operátory $\neg, \vee, \wedge, \rightarrow$. Existují však i systémy vyrokové logiky s jinými množinami operátorů. Budeme se jimi pro jednoduchost zabývat více až v kapitole 3. Neformálně řečeno, syntax formálního systému nám říká, o jaké symboly se v daném systému zajímáme a jak s nimi můžeme manipulovat. O manipulaci se symboly se více dozvíme v kapitole o odvozovacích systémech, zde se zaměříme pouze a jen na symboly samotné.

Připomeňme si definice z přednášky.

Definice 1.1 Abeceda výrokové logiky je soubor následujících symbolů:

- Spočetně mnoho znaků pro výrokové proměnné (např. $A, B, C, \ldots$ nebo $X_1, X_2, X_3, \ldots$).
- Symboly pro logické spojky: '$\neg$', '$\vee$', '$\wedge$' a '$\rightarrow$'.
- Symboly pro závorky: '(' a ')'.

Připomínáme, že z pohledu syntaxe nenesou tyto symboly žádný hlubší význam. Například se nikde neříká, že symbol $\wedge$, který se ve formulích výrokové logiky typicky vyskytuje, se má interpretovat jako, standardní logická spojka „AND“. Přiřazovat význam těmto symbolům budeme až v další kapitole. Ve skutečnosti nebudeme přiřazovat význam pouze symbolům samotným ale též řetězcům (slovům) z nich vytvořeným. Zároveň nás však budou zajímat pouze ty řetězce, které mají určitý speciální tvar, tzv. *formule* výrokové logiky.

Definice 1.2 Formule výrokové logiky je slovo φ nad abecedou výrokové logiky, pro které existuje tzv. vytvořující posloupnost, tj. konečná posloupnost slov $\psi_1, \ldots, \psi_k$ (kde $k \geq 1$) taková, že $\psi_k = \varphi$ a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů:

- ψ_i je výroková proměnná, nebo
- ψ_i je tvaru $\neg\psi_j$, pro nějaké $j < i$, nebo
- ψ_i je tvaru $(\psi_j \circ \psi_{j'})$ pro nějaké $j, j' < i$, kde $\circ \in \{\vee, \wedge, \rightarrow\}$.

Výše uvedená definice říká, že formule výrokové logiky jsou přesně ta slova, která lze v konečném počtu kroků vytvořit z jistých základních stavebních prvků (proměnných) pomocí různých syntaktických konstrukcí (spojek). Vzpomeňme si, že podobný postup se používá například pro definici syntaxe regulárních výrazů. Z definice je ihned vidět, že je-li $\psi_1, \ldots, \psi_k$ vytvořující posloupnost pro nějakou formuli φ, pak pro libovolné $1 \leq i < k$ je $\psi_1, \ldots, \psi_i$ vytvořující posloupnost pro ψ_i. Zejména všechna slova vyskytující se ve vytvořující posloupnosti jsou samy o sobě formulemi.

V této cvičebnici budeme standardně značit výrokové proměnné velkými znakami latinské abecedy a formule výrokové logiky malými znaky řecké abecedy.

✡☆☆ **Příklad 1.1** Určete, které z následujících slov jsou formulemi výrokové logiky.

a) $(X \wedge Y)$

b) $\neg((X \wedge Y) \rightarrow (Y \vee Z))$

c) $(X_1 \wedge \vee X_2)$

d) $\bigwedge_{i=1}^{k} X_i$ – jedná se o symbolický zápis konjunkce k proměnných, pro jenoznačnost uzávorkovaných zprava, tj. o slovo tvaru

$$(X_1 \wedge (X_2 \wedge (\cdots \wedge (X_{k-1} \wedge X_k)) \ldots))$$

e) $\bigvee_{i=1}^{\infty} X_i$

f) $((X \rightarrow Y \wedge Z))$

Řešení Probereme pouze některé případy.

Slovo z příkladu b) *je* formule, neboť pro něj máme například následující vytvořující posloupnost: $\psi_1 = X$, $\psi_2 = Y$, $\psi_3 = Z$, $\psi_4 = (\psi_2 \vee \psi_3)$, $\psi_5 = (\psi_1 \wedge \psi_2)$, $\psi_6 = (\psi_5 \to \psi_4)$, $\psi_7 = \neg\psi_6$.

Slovo z příkladu e) *není* formule, neboť formule je vždy *konečná* posloupnost znaků.

Slovo z příkladu f) rovněž není formule. Na první pohled je toto tvrzení zřejmé, ale jak jej formálně dokázat? Musíme ukázat, že *žádná* z nekonečně (dokonce nespočetně) mnoha všech možných vytvořujích posloupností nemůže být vytvořující posloupností pro slovo $((X \to Y \wedge Z))$. Způsob, jakým lze tento důkaz provést, je uveden níže. ▲

Jedním z možných způsobů jak ukázat, že dané slovo s není formulí výrokové logiky, je následující: ukážeme, že *každá* formule výrokové logiky má určitou vlastnost P, kterou zadané slovo P nemá. To, že nějakou vlastnost mají všechny formule výrokové logiky, lze nejlépe dokázat tzv. indukcí vzhledem ke struktuře formule. Tento princip je možné vyjádřit následovně:

Věta 1.3 [O strukturální indukci.] Nechť P je nějaká vlastnost taková, že:

a) Každá formule tvaru X, kde X je libovolná proměnná, má vlastnost P.

b) Mají-li formule ψ_1 a ψ_2 vlastnost P, pak i formule $\neg\psi_1$, $(\psi_1 \wedge \psi_2)$, $(\psi_1 \vee \psi_2)$ a $(\psi_1 \to \psi_2)$ mají vlastnost P.

Pak libovolná formule výrokové logiky má vlastnost P.

Použití strukturální indukce ilustrujeme na příkladu 1.1 f). Chceme ukázat, že slovo $((X \to Y \to Z))$ není formulí výrokové logiky. Ukážeme tedy, že každá formule φ výrokové logiky má následující vlastnost P:

> P: každý výskyt výrokové proměnné ve slově φ sousedí s nejvýše jedním výskytem binárního operátoru v tomto slově.

Je ihned vidět, že slovo $((X \to Y \to Z))$ tuto vlastnost nemá (jediný výskyt Y v tomto slově sousedí se dvěma výskyty operátoru $\to$) a pokud zmíněné tvrzení vskutku platí, nemůže být toto slovo formulí. Metadůkaz tvrzení povedeme strukturální indukcí. Ve skutečnosti metadokážeme silnější tvrzení, a sice že každá formule φ má následující vlastnost:

> P': každý výskyt proměnné ve slově φ sousedí s nejvýše jedním výskytem binárního operátoru *a zároveň*, pokud se nějaká proměnná vyskytuje na konci či na začátku slova φ, pak tento výskyt proměnné nesousedí s žádným výskytem binárního operátoru.

a) **Báze:** Ve formuli tvaru X, kde X je výroková proměnná, se žádné binární operátory nevyskytují. Taková formule tedy triviálně má vlastnost P'.

b) **Indukční krok:** Nechť ψ_1, ψ_2 jsou libovolné formule mající vlastnost P'. Formule $\neg\psi_1$ má rovněž tuto vlastnost, neboť připojení unárního operátoru $\neg$ na začátek slova tuto vlastnost zřejmě nijak neovlivní. Nechť nyní $\circ \in \{\vee, \wedge, \rightarrow\}$ je libovolný binární operátor. Sporem předpokládejme, že slovo $(\psi_1 \circ \psi_2)$ nemá vlastnost P'. Protože toto slovo začíná a končí závorkami (a nikoliv proměnnými), musí platit, že je v něm výskyt nějaké proměnné X sousedící se dvěma výskyty binárního operátoru. Pro určitost předpokládejme, že tento výskyt je v podslově ψ_1 (v opačném případě lze postupovat symetricky). Pak binární operátor vyskytující se vlevo od tohoto výskytu rovněž leží v podslově ψ_1, což znamená, že operátor ležící vpravo od tohoto výskytu v podslově ψ_1 neleží (to by byl spor s předpokladem, že slovo ψ_1 má vlastnost P').[1] Ale pak slovo ψ_1 končí výskytem proměnné, kterému předchází výskyt binárního operátoru – to je opět spor s předpokladem, že slovo ψ_1 má vlastnost P'.

Tím je metadůkaz hotov. Všimněte si, že v metadůkazu jsme použili standardní trik používaný v metadůkazech založených na indukci, kterým je *zesílení dokazovaného tvrzení*. Pokud bychom chtěli strukturální indukcí přímo dokazovat, že všechny formule mají původní vlastnost P, metadůkaz by se patrně ve druhém bodu „zasekl“. Neuměli bychom totiž vyloučit možnost, že slova ψ_1 a ψ_2 sice mají vlastnost P, ale formule ψ_1 končí výskytem proměnné jemuž předchází výskyt binárního operátoru.

✡✡ **Příklad 1.2** Dokažte, že mezi libovolnými dvěma binárnímy operátory ve formuli výrokové logiky je alespoň jeden výskyt (levé či pravé) závorky.

✡✡ **Příklad 1.3** Dokažte, že slovo z příkladu 1.1 c) není formulí výrokové logiky.

Délkou formule φ (značíme $|\varphi|$) se rozumí počet znaků abecedy výrokové logiky, ze kterých se formule skládá.

Příklad 1.4 Dokažte, že každá formule φ výrokové logiky, ve které se nevyskytuje operátor negace, má následující vlastnosti:

[1] Toto tedy znamená, že onen vpravo se vyskytující binární operátor je oním „$\circ$“ oddělujícím podslova ψ_1 a ψ_2. V důkazu ovšem tento fakt nepotřebujeme.

a) $|\varphi|$ je liché číslo.

b) Počet výskytů proměnných ve formuli φ je alespoň $\frac{|\varphi|}{4}$.

Řešení Metadokážeme obě dvě tvrzení zároveň. Přesněji řečeno, ukážeme, že libovolná formule φ splňuje následující metaimplikaci:

> Pokud se ve formuli nevyskytuje operátor negace, pak její délka je $4m-3$, kde m je počet výskytů proměnných v této formuli. (*)

Z toho vyplývají obě požadovaná tvrzení, neboť $4m-3$ je vždy liché číslo a $m \geq \frac{4m-3}{4} = m - \frac{3}{4}$.

Postupujeme strukturální indukcí:

Báze. Pokud $\varphi = X$, kde X je proměnná, pak máme $m = 1$ a $|\varphi| = 1 = 4m - 3$. Tvrzení tedy platí.

Indukční krok. Předpokládejme, že tvrzení platí pro nějaké formule φ_1 a φ_2. Formule tvaru $\neg\varphi_1$ evidentně obsahuje výskyt operátoru negace a triviálně tedy splňuje metaimplikaci (*). Nyní uvažme libovolnou formuli φ tvaru $(\varphi_1 \circ \varphi_2)$, kde $\circ \in \{\vee, \wedge, \rightarrow\}$. Pro $i \in \{1, 2\}$ označme m_i počet výskytů proměnných ve formuli φ_i. Zřejmě $m = m_1 + m_2$ (nepřidali jsme žádné nové výskyty proměnných). Dále dle indukčního předpokladu máme $|\varphi_i| = 4m_i - 3$, pro obě $i \in \{1, 2\}$. Konečně $|\varphi| = |\varphi_1| + |\varphi_2| + 3$ (k φ_1 a φ_2 jsme přidali dvě závorky a operátor $\circ$). Dohromady dostáváme

$$|\varphi| = |\varphi_1| + |\varphi_2| + 3 = 4m_1 - 3 + 4m_2 - 3 + 3 = 4 \cdot (m_1 + m_2) - 3 = 4m - 3.$$

Tvrzení tedy platí. Vskutku tedy platí, že pro libovolnou formuli φ máme $|\varphi| = 4m - 3$, kde m je počet výskytů proměnných v této formuli. ▲

✪✪✩ **Příklad 1.5** Dokažte, že počet výskytů závorek (levých i pravých dohromady) v libovolné formuli φ výrokové logiky je roven dvojnásobku počtu výskytů binárních operátorů ve φ.

✪✪✩ **Příklad 1.6** Pro libovolnou formuli výrokové logiky φ označme $B(\varphi)$ a $N(\varphi)$ počet výskytů binárních operátorů, resp. operátorů $\neg$, ve formuli φ. Najděte vztah mezi těmito hodnotami a délkou formule φ (tj. nalezněte vhodnou funkci f dvou celočíselných proměnných takovou, že pro libovolnou formuli φ platí $f(B(\varphi), N(\varphi)) = |\varphi|$). Příslušný vztah pak dokažte pomocí strukturální indukce.

✪✩✩ **Příklad 1.7** Rozhodněte, zda platí následující tvrzení. Své rozhodnutí zdůvodněte.

a) Ke každé formuli výrokové logiky existuje jednoznačně určená vytvořující posloupnost.

b) Ke každé formuli výrokové logiky existuje konečně mnoho vytvořujících posloupností.

c) Pokud budeme požadovat, aby se ve vytvořující posloupnosti neopakovaly formule, pak je vytvořující posloupnost každé formule určena jednoznačně až na pořadí formulí v posloupnosti.

Z definice vytvořující posloupnosti víme, že každou formuli φ lze psát v jednom z následujících tvarů: X, kde X je proměnná, nebo $\neg\psi$ či $(\psi_1 \circ \psi_2)$, kde ψ, ψ_1, ψ_2 jsou formule a $\circ$ je binární operátor. Jsou však formule ψ, ψ_1, ψ_2, na které můžeme rozložit formuli φ, určeny jednoznačně? Pokud má formule φ tvar $\neg\psi$, pak je jasně vidět, že formule ψ je určena jednoznačně. V případě formule tvaru $(\psi_1 \circ \psi_2)$ ale není okamžitě jasné, proč by takovou formuli nebylo možné psát ve tvaru $(\theta_1 \circ \theta_2)$, kde θ_1, θ_2 jsou formule různé od ψ_1, resp. ψ_2. Následující příklady nám pomohou ukázat, že tato nejednoznačnost vskutku nastat nemůže.

✩✩✩ **Příklad 1.8** Dokažte, že každá formule φ výrokové logiky je dobře uzávorkována, tj. že se v ní vyskytuje stejný počet pravých a levých závorek a zároveň se v každém prefixu ψ' slova ψ vyskytuje nejvýš tolik pravých závorek, co levých. Dále dokažte, že každý výskyt binárního operátoru v libovolné formuli je uzavřen alespoň v jedné dvojici závorek.

Definice 1.4 Řekneme, že nějaký binární operátor $\circ$ má ve formuli φ *vnější* výskyt, pokud platí $\varphi = (\psi_1 \circ \psi_2)$, kde ψ_1, ψ_2 jsou formule, ve kterých je každý výskyt binárního operátoru uzavřen v alespoň jedné dvojici závorek. Oním vnějším výskytem operátoru $\circ$ je právě výskyt oddělující podslova ψ_1 a ψ_2.

Alternativně se dá říci, že výskyt binárního operátoru ve formuli φ je vnější, pokud je uzavřen pouze v jediné dvojici závorek.

✩✩✩ **Příklad 1.9** Dokažte, že v každé formuli se vyskytuje nejvýše jeden vnější výskyt binárního operátoru. Jako důsledek pak ukažte následující: pokud máme $\varphi = (\psi_1 \circ \psi_2) = (\theta_1 \circ \theta_2)$, kde $\circ$ je binární operátor a $\psi_1, \psi_2, \theta_1, \theta_2$ jsou formule, pak $\psi_1 = \theta_1$ a $\psi_2 = \theta_2$. Během provádění důkazu si pečlivě uvědomte, která z výše uvedených tvrzení v důkazu používáte.

Každou formuli lze tedy jednoznačně rozložit na jisté kratší formule, tzv. *podformule*.

Definice 1.5 Pro formuli φ výrokové logiky definujme množinu jejích podformulí $Sub(\varphi)$ takto:

- pokud $\varphi = X$, pak $Sub(\varphi) = \{X\}$,
- pokud $\varphi = \neg\psi$, kde ψ je formule, pak $Sub(\varphi) = \{\varphi\} \cup Sub(\psi)$,
- pokud $\varphi = (\psi_1 \circ \psi_2)$, kde ψ_1, ψ_2 jsou formule, pak $Sub(\varphi) = \{\varphi\} \cup Sub(\psi_1) \cup Sub(\psi_2)$.

Všimněte si, že každá formule je svou podformulí.

✪✩✩ **Příklad 1.10** K následujícím formulím najděte množinu všech jejích podformulí:

a) $\varphi = (((\neg X_1 \to X_2) \to \neg(X_3 \wedge \neg\neg X_4)) \to (\neg X_1 \to X_2))$

b) $\psi = (X_k \to (X_{k-1} \to (X_{k-2} \dots (X_2 \to X_1) \dots)))$

Řešení

$$Sub(\varphi) = \{\varphi, ((\neg X_1 \to X_2) \to \neg(X_3 \wedge \neg\neg X_4)), (\neg X_1 \to X_2), \neg X_1, X_1, X_2, \neg(X_3 \wedge \neg\neg X_4), (X_3 \wedge \neg\neg X_4), X_3, \neg\neg X_4, \neg X_4, X_4\}.$$

$Sub(\psi) = \{X_i \mid 1 \le i \le k\} \cup \{\psi_i \mid 1 \le i \le k\}$, kde $\psi_1 = X_1$ a pro $i > 1$ je $\psi_i = (X_i \to \psi_{i-1})$. ▲

Nyní navážeme na příklad 1.7.

✪✪✩ **Příklad 1.11** Ukažte, že ke každé formuli φ existuje *právě jedna* (až na pořadí formulí v posloupnosti) vytvořující posloupnost $\psi_1, \dots, \psi_k$, v níž se vyskytují pouze formule ze $Sub(\varphi)$, z toho každá právě jednou.

✪✪✪ **Příklad 1.12** Nechť $B(\varphi)$ a $N(\varphi)$ jsou stejná čísla jako v příkladu 1.6. Dokažte, že každá formule φ má vytvořující posloupnost délky nejvýše

$$N(\varphi) + 2B(\varphi) + 1.$$

Dále dejte příklad formule ψ mající vytvořující posloupnost délky ostře menší než $N(\psi) + 2B(\psi) + 1$.

Poznámka 1.6 V okamžiku, kdy se v dalších kapitolách nebudeme zaměřovat na syntaxi výrokové logiky jako takovou, často budeme implicitně využívat různých syntaktických konvencí. Například budeme často vynechávat vnější závorky, tzn. psát např. $X \to Y$ namísto správného $(X \to Y)$. Také budeme užívat různých syntaktických zkratek, například budeme-li pracovat s výše zmíněnou „standardní“ výrokovou logikou, pak budeme zápis $X \leftrightarrow Y$ chápat jako syntaktickou zkratku pro formuli $(X \to Y) \wedge (Y \to X)$. Je důležité si uvědomit, že užíváním těchto konvencí neměníme výše uvedenou definici syntaxe standardní výrokové logiky, pouze používáme stručnější zápis pro správně utvořené formule.

1.2 Obecné systémy výrokové logiky

Obecně lze zavést výrokovou logiku i s jinými operátory. Můžeme například uvážit „omezenou“ výrokovou logiku, v níž se vyskytují pouze operátory $\neg$ a $\to$ a například zápis $X \vee Y$ je pouze syntaktickou zkratkou pro formuli $(\neg X \to Y)$. Nebo můžeme naopak obohatit standardní výrokovou logiku z předchozí kapitoly o binární operátor $\leftrightarrow$ – v takovém případě se $(X \leftrightarrow Y)$ stává formulí příslušného systému a nikoliv pouze syntaktickou zkratkou. Můžeme též používat zcela netradiční operátory, včetně operátorů arity vyšší než 2. Níže je zopakována formální definice z přednášky.

Definice 1.7 Nechť $\mathcal{F}_1, \ldots, \mathcal{F}_k$ je konečný soubor operátorů, přičemž každý operátor má přiřazenu svou *aritu*, což je nezáporné celé číslo. Definujeme formální logický systém $\mathcal{L}(\mathcal{F}_1, \ldots, \mathcal{F}_k)$, kde

- abeceda je tvořena spočetně mnoha znaky pro proměnné, znaky pro závorky a symboly pro výše uvedené operátory $\mathcal{F}_1, \ldots, \mathcal{F}_k$;
- formule φ systému $\mathcal{L}(\mathcal{F}_1, \ldots, \mathcal{F}_k)$ je slovo nad výše zmíněnou abecedou, pro nějž existuje tzv. vytvořující posloupnost, tj. konečná posloupnost slov $\psi_1, \ldots, \psi_k$ (kde $k \geq 1$) taková, že $\psi_k = \varphi$ a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů:
  - ψ_i je výroková proměnná, nebo
  - ψ_i je tvaru $\mathcal{F}_\ell(\psi_{j_1}, \ldots, \psi_{j_n})$, kde $1 \leq \ell \leq k$, n je arita $\mathcal{F}_\ell$ a $j_m < i$ pro všechna $1 \leq m \leq n$. Pokud $n = 1$, píšeme $\mathcal{F}_\ell\ \psi_1$ namísto $\mathcal{F}_\ell(\psi_1)$ (tj. vynecháváme vnější závorky u unárních operátorů), je-li $n = 2$, používáme infixový zápis (tj. píšeme $(\psi_1 \mathcal{F}_\ell \psi_2)$ namísto $\mathcal{F}_\ell(\psi_1, \psi_2)$).

V dalším textu budou příklady obsahovat přesné vymezení toho, jaký logický systém právě používáme. Pokud bude toto vymezení chybět, implicitně se má za to, že používáme standardní výrokovou logiku z předchozí podkapitoly.

Uvědomme si, že všechny syntaktické pojmy (jako například podformule) lze jednoduše rozšířit i na tyto obecné systémy výrokové logiky. Konkrétně pojem podformule bychom definovali induktivně takto: $Sub(X) = X$, kde X je proměnná, a $Sub(\mathcal{F}(\varphi_1, \ldots, \varphi_n)) = \{\mathcal{F}(\varphi_1, \ldots, \varphi_n)\} \cup \bigcup_{i=j}^{n} Sub(\varphi_i)$. Stejně jako u standardní výrokové logiky lze ukázat, že tato definice je jednoznačná.

✡✡✡ **Příklad 1.13** Uvažme formální logický systém $\mathcal{L}(\neg, \odot)$, kde $\neg$ má aritu 1 a $\odot$ má aritu 3. Rozhodněte, které z následujících slov jsou formulemi tohoto systému. Pro ta, která identifikujete jako formule, najděte vytvořující posloupnost.

a) $(X \odot Y)$

b) $\odot(\neg\neg X, Y, \neg X)$

c) $\neg \odot (X, \odot(X, Y, \neg Z), Z)$

d) $\neg(X \odot Y \odot Z)$

✡✡✡ **Příklad 1.14** Mějme stejný logický systém jako v předchozím příkladu. Pro libovolnou formuli φ tohoto systému označme $T(\varphi)$ počet výskytů operátoru $\odot$ v této formuli. Dokažte, že každá formule φ má $2T(\varphi) + 1$ výskytů proměnných.

✡✡✡ **Příklad 1.15** Mějme stejný logický systém a nechť $T(\varphi)$ je stejné číslo jako v předchozím příkladu. Nechť dále $N(\varphi)$ je počet výskutů operátoru negace ve φ. Dokažte, že pro každou fromuli φ existuje vytvořující posloupnost délky nejvýše $N(\varphi) + 3T(\varphi) + 1$.

✡✡✡ **Příklad 1.16** Dokažte, že pro libovolný logický systém $\mathcal{L}(F_1, \ldots, F_k)$ a libovolnou formuli φ tohoto systému platí, že posledním znakem ve φ je buď pravá závorka, nebo proměnná.

Řešení Nechť $\mathcal{L}(F_1, \ldots, F_k)$ je libovolný, ale nadále pevně zvolený logický systém. Důkaz vedeme strukturální indukcí.

- **Báze** $\varphi = X$ kde X je proměnná. Zřejmě φ končí na X

- **Indukční krok** φ je tvaru $\mathcal{F}_j(\varphi_1, \ldots, \varphi_n)$, kde $1 \leq j \leq k$, n je arita F_j a kde $\varphi_1, \ldots, \varphi_n$ splňují požadovanou vlastnost. Pokud $n = 1$, pak dle definice (podle které vynecháváme závorky u unárních operátorů) končí φ stejným znakem, kterým končí φ_n. Dle indukčního předpokladu je tímto znakem proměnná nebo pravá závorka. Je-li $n \geq 2$, pak formule φ nutně končí pravou závorkou.

▲

Definice 1.8 (Nahrazení podformulí) Uvažme libovolný logický systém $\mathcal{L}(F_1, \ldots, F_k)$ a libovolnou formuli φ tohoto systému. Nechť $\varphi_1, \ldots, \varphi_m$ je nějaká vytvořující posloupnost pro φ (označme tuto posloupnost Δ) a nechť $\xi_1, \theta_1, \ldots, \xi_\ell, \theta_\ell$ jsou nějaké formule uvažovaného systému, kde $\xi_i \neq \xi_j$ pro $i \neq j$. Uvažme posloupnost formulí Δ' která je definovaná takto: nejprve do Δ' postupně za sebe zařadíme vytvořující posloupnosti pro formule $\theta_1, \theta_2, \ldots, \theta_\ell$ a za takto vzniklou posloupnost připojíme posloupnost formulí $\varphi'_1, \ldots, \varphi'_m$, kde pro libovolné $1 \leq i \leq m$ platí

$$\varphi'_i = \begin{cases} \theta_j & \text{pokud } \varphi_i = \xi_j \text{ pro nějaké } j, \\ \varphi_i & \text{pokud } \varphi_i \neq \xi_j \text{ pro všechna } j \text{ a } \varphi_i \text{ je proměnná}, \\ \mathcal{F}_j(\varphi'_{j_1}, \ldots, \varphi'_{j_k}) & \text{pokud } \varphi_i \neq \xi_j \text{ pro vš. } j \text{ a } \varphi_i = \mathcal{F}_j(\varphi_{j_1}, \ldots, \varphi_{j_k}) \end{cases}$$

Zřejmě Δ' je vytvořující posloupnost pro formuli φ'_m. Tuto formuli označme $\varphi(\xi_1/\theta_1, \xi_2/\theta_2, \ldots, \xi_\ell/\theta_\ell)$.

✩✩✩ **Příklad 1.17** Dokažte, že formule $\varphi(\xi_1/\theta_1, \xi_2/\theta_2, \ldots, \xi_\ell/\theta_\ell)$ je definována korektně, tj. že nezávisí na volbě vytvořující posloupnosti Δ pro φ.

✩✩✩ **Příklad 1.18** Mějme formuli $\varphi = (X \to (Y \wedge \neg Z))$. Nalezněte formule $\theta = \varphi((X \to Y)/Z)$, $\rho = \varphi((Y \wedge \neg Z)/\neg(Y \to Z))$ a $\mu = \varphi(X/(Y \wedge Z), Y/X)$.

Řešení Máme $\theta = \varphi$, $\rho = (X \to \neg(Y \to Z))$ a $\mu = ((Y \wedge Z) \to (X \wedge \neg Z))$.

▲

Kapitola 2

Sémantika výrokové logiky

V předchozí kapitole jsme se seznámili s tím, jak vypadají formule výrokové logiky ze syntaktického hlediska. Doposud pro nás formule nebyly ničím jiným než řetězci písmenek a jiných značek. Teprve nyní těmto řetězcům přiřadíme nějaký význam, neboli *sémantiku*.

Budeme pracovat se dvěma standardními pravdivostními hodnotami: pravda (true, 1) a nepravda (false, 0). Výrokové proměnné ve formulích zastupují tzv. *atomické výroky*, které jsou buď pravdivé, nebo nepravdivé, a které již nelze dále rozložit na jednodušší výroky. Atomický výrok sám o sobě pravdivý či nepravdivý ovšem není, jeho pravdivostní hodnotu je třeba proměnným přiřadit „z vnějšku“, pomocí tzv. *valuace*.

Definice 2.1 Valuace je zobrazení, které každé ze spočetně mnoha proměnných přiřadí hodnotu 1 nebo 0.

Níže budeme zápisem Var značit (spočetný) soubor všech proměnných.

Pravdivost atomických výroků, a tedy ani formulí, které se z nich skládají, nelze vyhodnotit bez znalosti valuace. Na druhou stranu libovolnou valuaci je možné jednoznačně rozšířit z proměnných na formule a vyhodnotit tak pravdivost libovolné formule.

Definice 2.2 Nechť $v\colon Var \to \{1, 0\}$ je valuace a φ je libovolná formule. Rozšíříme v na soubor všech formulí. Hodnotu $v(\varphi)$ definujeme induktivně takto:

- pokud $\varphi = X$, pak $v(X)$ je již definováno;
- pokud $\varphi = \neg\varphi'$, pak $v(\varphi) = 1$ tehdy a jen tehdy když $v(\varphi') = 0$;

- pokud $\varphi = \varphi_1 \wedge \varphi_2$, pak $v(\varphi) = 1$ tehdy a jen tehdy když $v(\varphi_1) = v(\varphi_2) = 1$;
- pokud $\varphi = \varphi_1 \vee \varphi_2$, pak $v(\varphi) = 0$ tehdy a jen tehdy když $v(\varphi_1) = v(\varphi_2) = 0$;
- pokud $\varphi = \varphi_1 \to \varphi_2$, pak $v(\varphi) = 0$ tehdy a jen tehdy když $v(\varphi_1) = 1$ a zároveň $v(\varphi_2) = 0$.

Předchozí definice definuje valuaci pro formule standardní výrokové logiky. Sémantice obecných logik se budeme věnovat v příští kapitole.

Definice 2.3 Řekneme, že formule φ je pravdivá ve valuaci v, pokud $v(\varphi) = 1$. Formule φ je tautologie, resp. kontradikce, jestliže je pravdivá v každé, resp. není pravdivá v žádné valuaci. Řekneme, že formule je splnitelná, pokud je pravdivá v alespoň jedné valuaci. Řekneme, že formule φ a ψ jsou ekvivalentní, píšeme $\varphi \approx \psi$, pokud $v(\varphi) = v(\psi)$ pro libovolnou valuaci v.

✡☆☆ **Příklad 2.1** Rozhodněte a dokažte, zda jsou následující formule splnitelné.

a) $X \wedge \neg X$

b) $X \wedge (Y \to \neg X)$

c) $(X \vee Y) \wedge (\neg X \vee \neg Z) \wedge (\neg Y \vee Z)$

d) $((X \wedge Y) \to \neg Z) \wedge ((X \wedge \neg Z) \to \neg Y) \wedge (\neg(X \wedge Y) \to (X \wedge \neg X))$

e) $((X \wedge Y) \vee \neg(X \vee Y)) \to (\neg X \wedge X)$

Řešení Odpovědi jsou následující: a) NE, b) ANO, c) ANO , d) NE, e) ANO. Formule v b) je splněna libovolnou valuací v takovou, že $v(X) = 1$ a $v(Y) = 0$. Formule v c) je splněna například libovolnou valuací v níž $v(X) = 1$, $v(Y) = v(Z) = 0$. Formule v e) je splněna libovolnou valuací v splňující to, že *právě jedna* z proměnných X, Y se ve v zobrazí na 1. To, že formule v d) není splnitelná bychom mohli ověřit například sestrojením pravdivostní tabulky. Protože ale velikost pravdivostních tabulek roste exponenciálně s počtem proměnných, je často výhodnější argumentovat slovně. Označme

$$\varphi \quad = \quad (\underbrace{(X \wedge Y) \to \neg Z}_{\varphi_1}) \wedge \underbrace{((X \wedge \neg Z) \to \neg Y)}_{\varphi_2} \wedge \underbrace{(\neg(X \wedge Y) \to (X \wedge \neg X))}_{\varphi_3}.$$

Sporem předpokládejme, že existuje valuace v taková, že $v(\varphi) = 1$. Pak musí být $v(\varphi_1) = v(\varphi_2) = v(\varphi_3) = 1$. Protože zřejmě $v(X \wedge \neg X) = 0$, musí platit $v(\neg(X \wedge Y)) = 0$, jinak by totiž platilo $v(\varphi_3) = 0$. Musí tedy platit $v(X) = v(Y) = 1$. Protože $v(\varphi_1) = 1$, musí navíc platit i $v(\neg Z) = 1$. Protože i $v(\varphi_2) = 1$, z $v(X) = 1$ a $v(\neg Z) = 1$ plyne $v(\neg Y) = 1$, spor s tím, že $v(Y) = 1$. ▲

✪✪✩ **Příklad 2.2** Řekneme, že valuace v a v' jsou *na proměnných* $\{X, Y, Z\}$ *různé*, pokud pro některou proměnnou $A \in \{X, Y, Z\}$ platí $v(A) \neq v'(A)$.

Zadejte formuli výrokové logiky φ s proměnnými X, Y, Z, takovou že φ je pravdivá *právě* při 3 valuacích různých na $\{X, Y, Z\}$ (tedy pravdivá při 3 z 8 valuací různých na $\{X, Y, Z\}$).

Řešení Takových formulí je nekonečně mnoho, jedna z možných je

$$\varphi = X \wedge (Y \vee Z)$$

Nad rámec zadání zdůvodníme správnost našeho řešení tabulkou všech valuací různých na $\{X, Y, Z\}$.

$v(X)$	$v(Y)$	$v(Z)$	$v(\varphi)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

▲

✪✩✩ **Příklad 2.3** Rozhodněte a dokažte, zda jsou následující formule tautologiemi.

a) $X \to (Y \to X)$
b) $((X \to Y) \to Z) \to (X \to (Y \to Z))$
c) $(X \to (Y \to Z)) \to ((X \to Y) \to Z)$
d) $(X \to (Y \to Z)) \to ((X \to Y) \to (X \to Z))$
e) $(X \vee Y) \to (\neg Y \to X)$
f) $((X \wedge Y) \vee Z) \to (\neg X \to \neg(Y \vee \neg Z))$

✡✡✡ **Příklad 2.4** Najděte formule výrokové logiky φ a ψ takové, že jsou současně splněny všechny následující podmínky:

- $\varphi \to \psi$ je tautologie,
- $\varphi \leftrightarrow \psi$ není tautologie,
- $\psi \to \varphi$ je splnitelná.

✡✡✡ **Příklad 2.5** Rozhodněte, zda pro libovolné formule φ, ψ, ξ výrokové logiky platí

$$\varphi \to (\psi \to \xi) \approx (\varphi \to \psi) \to \xi$$

Své tvrzení zdůvodněte.

✡✡✡ **Příklad 2.6** Rozhodněte a zdůvodněte, zda existují takové formule φ a ψ výrokové logiky, pro které *současně* platí, že

- $\varphi \to \psi$ je splnitelná, ale není tautologie,
- a zároveň $\psi \to \varphi$ není splnitelná.

Řešení Takové formule neexistují. Abychom to ukázali, vezměme si libovolnou dvojici formulí φ a ψ splňující první podmínku, tj. to, že formule $\varphi \to \psi$ je splnitelná, a ukažme, že nemůže platit druhá podmínka, tj. že i formule $\psi \to \varphi$ musí být splnitelná. Protože formule $\varphi \to \psi$ není tautologie, musí existovat valuace v^* taková, že $v^*(\varphi \to \psi) = 0$. Z definice sémantiky pro operátor $\to$ plyne, že nutně $v^*(\psi) = 0$. Z toho ale (rovněž díky definici sémantiky pro $\to$) plyne $v^*(\psi \to \varphi) = 1$, což ukazuje, že formule $\psi \to \varphi$ je splnitelná. ▲

✡✡✡ **Příklad 2.7** Dejte příklad formulí φ a ψ takových, že

- $\varphi \to \psi$ je tautologie a zároveň
- $\psi \to \varphi$ je kontradikce.

✡✡✡ **Příklad 2.8** Nechť A je výroková proměnná. Rozhodněte a dokažte, zda existuje formule φ taková, že

a) $\varphi \to (\varphi \to A) \approx A$
b) $\varphi \to (\varphi \to A) \approx \neg A$
c) $\varphi \to (A \to \varphi) \approx A$
d) $(\varphi \to A) \to \varphi \approx \neg A$

✪✪✩ **Příklad 2.9** V jisté zemi žijí dva druhy lidí: poddaní, kteří na otázku vždy odpoví pravdivě, a politici, kteří vždy zalžou. Pocestný z ciziny, který se chce dostat do hlavního města, přijde na neoznačenou křižovatku. Naštěstí jde kolem někdo z místních – spěchá však, a odpoví tak pocestnému pouze na *jedinou* otázku. Na co se má pocestný zeptat, aby s jistotou zjistil, která cesta vede do města? (Na otázku musí jít odpověďed stylem ano/ne.)

✪✪✪ **Příklad 2.10** V ještě jiné zemi žijí tři druhy lidí: poddaní, kteří vždy říkají pravdu, politici, kteří vždy lžou, a obchodníci, kteří lžou či říkají pravdu dle své libosti. Cestovatel zrovna sedí v místní krčmě a baví se s hospodským (který je poddaným a říká tedy pravdu). Hospodský řekne cestovateli: „Vidíš tamhlety tři lidi co sedí u stejného stolu? Jeden z nich je poddaný, jeden je politik a jeden je obchodníkem. Pokud pomocí *třech* otázek zjistíš, kdo je kdo, máš u mě pivo zadarmo. Na každou otázku ti může odpověděd jen jeden z nich, ale můžeš si vždycky vybrat, který.“ Cestovatel má vskutku žízeň. Jaké otázky (a komu) má položit? (Na otázky musí opět jít odpovědět stylem ano/ne). (Hint: Nejprve pomocí dvou otázek identifikujte obchodníka.)

✪✩✩ **Příklad 2.11** Je následující soubor formulí splnitelný? Rozhodněte a zdůvodněte.

$$T = \{\, B \leftrightarrow D, A \rightarrow B, (A \vee B \vee D) \wedge (\neg A \vee C) \wedge (\neg C \vee \neg D), \\ D \rightarrow (A \leftrightarrow C))\}$$

✪✪✩ **Příklad 2.12** V systémech pro správu balíčků v linuxu (např. *dpkg* nebo *RPM*) je využita výroková logika pro řešení závislostí mezi balíčky. Jedním z problémů je zajistit, aby repozitář neobsahoval žádné *rozbité* balíčky, které není možné nainstalovat. Značně zjednodušeně máme systém jako trojici (P, d, C), kde

- P je množina balíčků,
- $d : P \rightarrow 2^P$ přiřazuje každému balíčku p množinu balíčků, na kterých p závisí, a
- $C \subseteq P \times P$ je symetrická relace dvojic balíčků, které jsou spolu v konfliktu.

Instalace je množina balíčků $Q \subseteq P$.

Řekneme, že instalace Q je *zdravá*, pokud

a) pro každý balíček $p \in Q$ platí $d(p) \subseteq Q$ a zároveň
b) pro každé dva balíčky $p, q \in Q$ platí $(p, q) \notin C$.

Dále řekneme, že balíček p je *nainstalovatelný*, pokud existuje zdravá instalace Q obsahující p.

Popište algoritmus, který pro zadaný systém (P, d, C) a balíček $p \in P$ vypíše formuli výrokové logiky φ, takovou že

$$\varphi \text{ je splnitelná} \iff \text{balíček } p \text{ je nainstalovatelný.} \tag{2.1}$$

Algoritmus by měl běžet v čase polynomiálním vzhledem k $|P|$. Dokažte, že výsledná formule splňuje metaekvivalenci (2.1).

Řešení Pro každý balíček $q \in P$ budeme používat výrokovou proměnnou X_q, jejíž valuace intuitivně odpovídá tomu, zda q patří do instalace Q. Algoritmus vrátí formuli

$$\varphi = \varphi_1 \wedge \varphi_2 \wedge \varphi_3,$$

kde (intuitivě vysvětleno)

$\varphi_1 = X_p$ vynutí $p \in Q$,

$\varphi_2 = \bigwedge_{q \in P} (X_q \to \bigwedge_{r \in d(q)} X_r)$ vynutí ke každému $q \in Q$ také jeho závislosti a

$\varphi_3 = \bigwedge_{(q,r) \in C} (\neg X_q \vee \neg X_r)$ vynutí, aby v instalaci nebyly konfliktní balíčky.

Je zřejmé, že ke konstrukci formule φ je zapotřebí počet kroků polynomiální vzhledem k $|P|$ (konkrétně můžeme použít horní odhad na počet kroků $\mathcal{O}(|P|^2)$).

Nad rámec zadání ještě dokážeme ekvivalenci (2.1).

- "$\Rightarrow$": Nechť v je valuace, při které je φ pravdivá. Ukážeme, že množina balíčků $Q = \{q \mid v(X_q) = 1\}$ je zdravá instalace obsahující p.

  Z definice dostáváme $v(\varphi_1) = v(\varphi_2) = v(\varphi_3) = 1$. Zřejmě $p \in Q$, protože $v(X_p) = 1$. Sporem dokážeme, že Q je zdravá. Předpokládejme, že Q není zdravá. Pak buď

  a) existují balíčky $q \in Q$ a $r \notin Q$ takové, že $r \in d(q)$. V tom případě dostáváme $v(X_q) = 1$ a $v(X_r) \neq 1$, a tedy $v(\varphi_2) = 0$, spor. Nebo
  b) existují balíčky $q, r \in Q$ takové, že $(q, r) \in C$. V tom případě dostáváme $v(X_q) = v(X_r) = 1$, a tedy $v(\varphi_3) = 0$, spor.

- "$\Leftarrow$": Nechť Q je zdravá instalace obsahující p. Ukážeme, že φ je pravdivá při valuaci v definované

$$v(X) = \begin{cases} 1 & \text{pokud existuje } q \in Q, \text{ takové že } X = X_q, \\ 0 & \text{jinak.} \end{cases}$$

  a) Zřejmě $v(\varphi_1) = 1$, protože Q obsahuje p.
  b) Uvažme libovolný balíček $q \in P$ a položme

$$\varphi_{2,q} = X_q \to \bigwedge_{r \in d(q)} X_r.$$

  Pokud $q \notin Q$, pak zjevně $v(\varphi_{2,q}) = 1$. Pokud $q \in Q$, pak také $d(q) \subseteq Q$, protože Q je zdravá. Tedy také $v(\varphi_{2,q}) = 1$. Celkově $v(\varphi_2) = 1$, protože $v(\varphi_{2,q}) = 1$ pro každé $q \in P$.
  c) Uvažme libovolné konfliktní balíčky $(q, r) \in C$. Pak buď $q \notin Q$ nebo $r \notin Q$, protože Q je zdravá. Tedy $v(\neg X_q \vee \neg X_r) = 1$ a celkově $v(\varphi_3) = 1$.

  Formule φ je pravdivá při valuaci v, protože $v(\varphi_1) = v(\varphi_2) = v(\varphi_3) = 1$.

▲

✪✪ **Příklad 2.13** Máme $3n$ úkolů a m lidí, z nichž každý je schopen vyřešit právě 3 konkrétní úkoly. Soubor n z těchto m lidí nazveme *dobrý*, právě když každý úkol umí vyřešit některý z vybraných n lidí.

To stejné formálněji: Jsou dána čísla $n, m \in \mathbb{N}$. Označme $N = \{1, \ldots, 3n\}$. Dále je dán soubor $S = \{N_1, \ldots, N_m\}$, kde $N_i \subseteq N$ a $|N_i| = 3$ pro každé $i \in \{1, \ldots, m\}$. Podsoubor $T \subseteq S$ nazveme *dobrý*, právě když $\bigcup T = N$ a $|T| = n$ ($\bigcup T$ značí jako obyvkle množinu právě těch prvků, které patří do aspoň jedné množiny z T).

Řešení Jak dokážeme, uvedenou vlastnost má například formule

$$\varphi = \bigwedge_{i=1}^{3n} \bigvee_{\substack{j=1 \\ i \in N_j}}^{m} A_j \quad \wedge \quad \bigwedge_{i=1}^{3n} \bigwedge_{\substack{j=1 \\ i \in N_j}}^{m} \bigwedge_{\substack{k=j+1 \\ i \in N_k}}^{m} \neg(A_j \wedge A_k).$$

Nechť n, m, $S = \{N_1, \ldots, N_m\}$ je libovolný validní vstup. Pro každou valuaci v můžeme uvažovat jí příslušný podsoubor

$$T_v = \{N_i \mid i \in \{1, \ldots, m\}, v(A_i) = 1\}.$$

Naopak pro libovolný podsoubor $T \subseteq S$ můžeme uvažovat valuaci v_T definovanou předpisem $v(A_j) = 1$ pro $j \in \{1, \ldots, m\}$ taková, že $N_j \in T$, a $v(X) = 0$ pro ostatní výrokové proměnné X.

Zřejmě

$$v\left(\bigwedge_{i=1}^{3n} \bigvee_{\substack{j=1 \\ i \in N_j}}^{m} A_j\right) = 1,$$

právě když pro všechna $i \in N$ existuje $j \in \{1, \ldots, m\}$ takové, že $i \in N_j$ a $v(A_j) = 1$, tedy právě když $\bigcup T_v = N$. Dále zřejmě

$$v\left(\bigwedge_{i=1}^{3n} \bigwedge_{\substack{j=1 \\ i \in N_j}}^{m} \bigwedge_{\substack{k=j+1 \\ i \in N_k}}^{m} \neg(A_j \wedge A_k)\right) = 1,$$

právě když pro pro všechna $i \in N$ existuje nejvýš jedno $j \in \{1, \ldots, m\}$ takové, že $i \in N_j$ a $v(A_j) = 1$, tedy právě když množiny v T_v jsou po dvou disjunktní.

Pokud $\bigcup T_v = N$ (připomeňme, že $|N| = 3n$ a každá množina N_i je trojprvková) a prvky podsouboru T jsou po dvou disjunktní, pak jich musí být právě n, a tedy T je dobrý podsoubor. Naopak je-li T dobrý, pak jsou zřejmě jeho prvky po dvou disjunktní.

Dohromady tedy dostáváme, že je-li φ splněna nějakou valuací v, pak T_v je dobrý podsoubor souboru S; naopak pokud je T nějaký dobrý podsoubor souboru S, pak $v_T(\varphi) = 1$. ▲

✿✿ **Příklad 2.14 (Sudoku)** (Pokud je na Vás následující zadání na první přečtení moc abstraktní, dosaďte si za n trojku. Zadání pak odpovídá klasickému sudoku 9×9.) Nechť $n \geq 3$ je přirozené číslo. Zadáním sudoku typu $n^2 \times n^2$ máme formálně na mysli matici Z typu $n^2 \times n^2$, kde každá buňka matice obsahuje jednu z hodnot $\{1, \ldots, n^2, \perp\}$ ($\perp$ reprezentuje nepředvyplněné políčko). Řešením takového zadání Z je libovolná matice R_Z stejného typu, jejíž buňky obsahují čísla z množiny $\{1, \ldots, n^2\}$ a která splňuje následující:

- pro libovolné (i, j) takové, že $Z(i, j) \neq \perp$, platí $Z(i, j) = R_Z(i, j)$ (tj. nelze přepsat předvyplněná čísla ze zadání);
- pro libovolné $1 \leq i, j \leq n^2$ platí, že v i-tém řádku ani v j-tém sloupci matice R_Z se žádná hodnota neopakuje.

- pro libovolné $0 \leq k, \ell < n$ platí, že množina $\{R_Z(n \cdot k + i, n \cdot \ell + j) \mid 1 \leq i, j \leq n\}$ obsahuje všechna čísla z množiny $\{1, \ldots, n^2\}$. (Jinak řečeno, rozdělíme-li matici R_Z přirozeným způsobem na podmatice typu $n \times n$, tak se v žádné podmatici nevyskytuje dvakrát totéž číslo.)

Popište algoritmus, který pro dané zadání sudoku Z zkonstruuje formuli výrokové logiky φ_Z takovou, že

$$\varphi_Z \text{ je splnitelná} \quad \Leftrightarrow \text{ existuje řešení } R_Z \text{ sudoku } Z.$$

Dále popište algoritmus který, dostane-li na vstup valuaci splňující Vámi uvedenou formuli φ_Z (například ve formě tabulky pravdivostních hodnot pro proměnné ve formuli), zkonstruuje z této valuace řešení sudoku Z. Oba dva algoritmy by měly běžet v čase polynomiálním vzhledem k n.

✡☆☆ **Příklad 2.15** Je následující formule s výrokovými proměnnými A, B, C splnitelná? Rozhodněte a dokažte.

$$(A \to \neg A) \wedge ((B \leftrightarrow C) \wedge (\neg A \to C))$$

✡☆☆ **Příklad 2.16** (SAT solver) Najděte co nejrychleji splňující valuaci.

$$(A \vee B \vee C) \wedge (\neg A \vee \neg D \vee \neg E) \wedge (B \vee C \vee \neg E) \wedge (D \vee \neg A \vee B) \wedge$$
$$(\neg A \vee B \vee E) \wedge (A \vee B \vee \neg D) \wedge (\neg A \vee \neg B \vee \neg E) \wedge (\neg B \vee C \vee \neg D) \wedge$$
$$(D \vee \neg A \vee \neg B) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg C \vee D) \wedge$$
$$(\neg D \vee \neg B \vee \neg C) \wedge (A \vee \neg C \vee E) \wedge (\neg A \vee B \vee A) \wedge (C \vee \neg B \vee D) \wedge$$
$$(A \vee \neg B \vee C) \wedge (D \vee E \vee \neg C)$$

Definice 2.4 Nechť T je soubor výrokových formulí. Řekneme, že T je splnitelný, pokud existuje valuace v taková, že pro každou formuli $\varphi \in T$ platí $v(\varphi) = 1$. O takové valuaci řekneme, že splňuje soubor T. Dále řekneme, že formule ψ je tautologickým důsledkem souboru formulí T, píšeme $T \models \psi$, jestliže pro libovolnou valuaci v splňující soubor T platí $v(\psi) = 1$.

Definice 2.5 *Neorientovaný graf* je dvojice $G = (V, E)$, kde V je množina vrcholů a $E \subseteq \{\{u, v\} \mid u, v \in V\}$ je množina hran mezi vrcholy (tedy množina nejvýše dvouprvkových neprádných množin).

Klika v neorientovaném grafu je podmnožina vrcholů $C \subseteq V$, kde každé dva vrcholy $u, v \in C$ jsou spojené hranou, tedy $\{u, v\} \in E$.

✪✪✩ **Příklad 2.17** Nechť G je neorientovaný graf. Nalezněte systém formulí $\mathcal{T}$ takový, že

$$\mathcal{T} \text{ je splnitelný} \iff G \text{ obsahuje kliku o velikosti alespoň 3}$$

✪✪✪ **Příklad 2.18** Nechť G je neorientovaný graf a $k \in \mathbb{N}$. Nalezněte systém formulí $\mathcal{T}$ takový, že

$$\mathcal{T} \text{ je splnitelný} \iff G \text{ obsahuje kliku o velikosti } k$$

a $\mathcal{T}$ lze sestrojit v polynomiálním čase vzhledem k velikosti G a k.

Definice 2.6 *Orientovaný graf* je dvojice $G = (V, E)$, kde V je množina vrcholů a $E \subseteq V^2$ je množina orientovaných hran mezi vrcholy.

Nechť $G = (V, E)$ je orientovaný graf a $|V| = n$. *Hamiltonovská kružnice* (HK) v orientovaném grafu G je posloupnost vrcholů $u_0, u_1, \ldots, u_{n-1}$ taková, že pro všechna $0 \leq i \leq n-1$ platí $(u_i, u_{i+1 \bmod n}) \in E$ a pro všechna $0 \leq i < j \leq n-1$ platí $v_i \neq v_j$.

✪✪✪ **Příklad 2.19** Nechť $G = (V, E)$ je orientovaný graf o n vrcholech. Nalezněte systém formulí $\mathcal{T}$ takový, že

$$\mathcal{T} \text{ je splnitelný} \iff G \text{ obsahuje Hamiltonovskou kružnici} \tag{2.2}$$

a $\mathcal{T}$ lze sestrojit v polynomiálním čase vzhledem k velikosti n.

Řešení Použijeme výrokové proměnné $E_{u,w}$, kde $u, w \in V$, a $X_{i,w}$, kde i je celé číslo mezi 0 a $n-1$ a $w \in V$. Proměnná $E_{u,w}$ intuitivně reprezentuje výrok „mezi vrcholy u a w vede hrana“, zatímco $X_{i,w}$ reprezentuje výrok „vrchol w je i-tým vrcholem na Hamiltonovské kružnici H“, kde H je nějaká HK grafu G. Systém $\mathcal{T}$ pak vypadá následovně:

$\mathcal{T} = \{\eta\} \cup \{\varphi_{i,w}, \psi_{i,w} \mid 0 \leq i \leq n-1, w \in V\} \cup \{\theta_i, \xi_i \mid 0 \leq i \leq n-1\}$, kde

$$\eta = \bigwedge_{(u,w)\in E} E_{u,w} \wedge \bigwedge_{\substack{u,w\in V \\ (u,w)\notin E}} \neg E_{u,w},$$

$$\varphi_{i,w} = X_{i,w} \to \Big(\bigwedge_{\substack{u\in V \\ u\neq w}} \neg X_{i,u}\Big),$$

$$\psi_{i,w} = X_{i,w} \to \Big(\bigwedge_{\substack{0\leq j\leq n-1 \\ j\neq i}} \neg X_{j,w}\Big),$$

$$\theta_i = \bigwedge_{u,w\in V} \big((X_{i,u} \wedge X_{i+1 \bmod n,w}) \to E_{u,w}\big),$$

$$\xi_i = \bigvee_{w\in V} X_{i,w}.$$

Nebudeme formálně dokazovat, že systém $\mathcal{T}$ splňuje metaekvivalenci (2.2), uvedeme pouze intuitivní zdůvodnění. Nejprve předpokládejme, že existuje valuace v splňující systém $\mathcal{T}$. Formule η vynutí, aby valuace proměnných $E_{u,w}$ kódovala vstupní graf G (tj. aby $v(E_{u,w}) = 1$ právě když mezi u a w vede hrana). Formule typu $\varphi_{i,w}$ (je jich celkem n) dohromady vynutí, že nejvýše jedna z proměnných z množiny $\{X_{i,w} \mid w \in V\}$ bude mít přiřazeno *true* (intuitivně nejvýše jeden vrchol může být i-tým vrcholem konkrétní HK), podobně n formulí tvaru $\psi_{i,w}$ dohromady vynutí, že nejvýše jedna z proměnných $\{X_{j,w} \mid 0 \leq j \leq n-1\}$ bude mít přiřazeno *true* (tj. žádný vrchol se na HK neopakuje). Konečně n formulí typu ξ_i vynutí, aby pro každé $0 \leq i \leq n-1$ existovalo alespoň jedno $w \in V$ takové, že $X_{i,w}$ bude mít přiřazeno *true*. Pokud tedy dohromady vynutí, že pro libovolnou splňující valuaci v definujeme posloupnost $u_0, \ldots u_{n-1}$ tak, že u_i je jediný vrchol w splňující $v(X_{i,w}) = 1$, pak tato posloupnost obsahuje všechny vrcholy grafu G. Navíc, formule tvaru θ_i vynutí, aby pro každé i vedla hrana mezi vrcholy u_i a $u_{i+1 \bmod n}$. Posloupnost $u_0, \ldots u_{n-1}$ je tedy Hamiltonovskou kružnicí.

Naopak se snadno ukáže, že pokud $u_0, \ldots, u_{n-1}$ je HK grafu G, pak můžeme zkonstruovat splňující valuaci v následovně: pro všechny vrcholy u, w položíme $v(E_{u,w}) = 1$ právě když mezi u a w vede hrana, a pro všechna $0 \leq i \leq n-1$ a všechna $w \in V$ položíme $v(X_{i,w}) = 1$ právě když $u_i = w$. Všem ostatním proměnným přiřadí v hodnotu 0.

▲

✩✩ **Příklad 2.20** Nechť T je *splnitelný* soubor výrokových formulí a nechť φ je *libovolná* výroková formule. Rozhodněte a dokažte, zda platí následující tvrzení:

a) jestliže $T \models \varphi$, pak $T \not\models \neg\varphi$,

b) jestliže $T \not\models \neg\varphi$, pak $T \models \varphi$.

✪✪ **Příklad 2.21** Nechť T je libovolný *neprázdný* soubor výrokových formulí a nechť φ, ψ jsou libovolné výrokové formule. Rozhodněte a dokažte, zda platí následující tvrzení:

a) Pokut $T \models \varphi \to \psi$, pak buď $T \models \psi$ nebo $T \models \neg\varphi$.

b) Je-li $T' = \{\neg\xi \mid \xi \in T\}$ (tj. T' obsahuje právě negace formulí ze souboru T), pak $T \models \varphi$ právě když $T' \models \neg\varphi$.

Řešení

a) Tvrzení **neplatí**. Jako protipříklad uveďme situaci, kdy $\varphi = A$, $\psi = B$ a $T = \{A \to B\}$. Zřejmě $\{A \to B\} \models A \to B$. Zároveň ale neplatí $\{A \to B\} \models \neg A$ ani $\{A \to B\} \models B$. Pro první zmíněný příklad stačí uvážit valuaci v takovou, že $v(A) = v(B) = 1$. Pak $v(A \to B) = 1$ a $v(\neg A) = 0$. Pro druhý případ (neplatí $\{A \to B\} \models B$) stačí uvážit valuaci v' takovou, že $v'(A) = v'(B) = 0$. Pak opět $v'(A \to B) = 1$, avšak $v'(B) = 0$.

b) Tvrzení **neplatí**. Jako protipříklad mějme situaci kdy $T = \{A \wedge B\}$ a $\varphi = A$. Zřejmě $\{A \wedge B\} \models A$, neplatí však $\{\neg(A \wedge B)\} \models \neg A$. Abychom ukázali druhé tvrzení, stačí uvážit valuaci v takovou, že $v(A) = 1$ a $v(B) = 0$. Pro tuto valuaci platí $v(\neg(A \wedge B)) = 1$, avšak $v(\neg A) = 0$.

▲

✪✪ **Příklad 2.22** Nechť $T_1, T_2, \ldots$ je posloupnost *splnitelných* souborů výrokových formulí. Rozhodněte a dokažte, zda soubory $\bigcup_{i=1}^{\infty} T_i$ a $\bigcap_{i=1}^{\infty} T_i$ jsou splnitelné.

✪✪ **Příklad 2.23** Nechť S je soubor všech *splnitelných* formulí výrokové logiky a S' je soubor všech *tautologií* výrokové logiky. Rozhodněte a dokažte, zda jsou soubory S, resp. S' splnitelné.

✪✪ **Příklad 2.24** Nechť $T_1, T_2, \ldots$ je posloupnost *nesplnitelných* souborů výrokových formulí taková, že pro libovolné i platí $T_{i+1} \subsetneq T_i$ (tj. T_{i+1} je vlastní podmnožinou T_i). Rozhodněte a dokažte, zda je soubor $\bigcap_{i=1}^{\infty} T_i$ vždy nutně nesplnitelný, či naopak vždy nutně splnitelný.

Řešení Soubor $\bigcap_{i=1}^{\infty} T_i$ může být jak splnitelný, tak nesplnitelný. Uvažme nejprve soubor výrokových formulí $T = \{X_i \wedge \neg X_i \mid i \geq 1\}$. Neformálně řečeno, soubor T obsahuje nekonečně mnoho „kopií“ formule $X \wedge \neg X$, přičemž abychom tyto kopie rozlišili, nahradíme proměnnou X v i-té kopii proměnnou X_i (tj. rozlišení provedeme pomocí indexů proměnných). Dále položme $T_i = T \setminus \{X_1 \wedge \neg X_1, \ldots, X_i \wedge \neg X_i\} = \{X_j \wedge \neg X_j \mid j \geq i+1\}$. Pak soubor T_i není splnitelný, neboť obsahuje nesplnitelnou formuli $X_i \wedge \neg X_i$. Avšak $\bigcap_{i=1}^{\infty} T_i$ je prázdný soubor (ověřte!), který je z definice splnitelný.

Na druhou stranu uvažme situaci kdy $T_i = (T \cup \{X_0 \wedge \neg X_0\}) \setminus \{X_1 \wedge \neg X_1, \ldots, X_i \wedge \neg X_i\} = \{X_j \wedge \neg X_j \mid j \geq i+1\} \cup \{X_0 \wedge \neg X_0\}$. Znovu zřejmě platí, že každý soubor T_i je nesplnitelný, ovšem tentokrát je nesplnitelný i soubor $\bigcap_{i=1}^{\infty} T_i = \{X_0 \wedge \neg X_0\}$. ▲

✡✡✡ **Příklad 2.25** Mějme libovolný neprázdný soubor výrokových formulí T a formuli φ takovou, že $T \models \varphi$. Rozhodněte a dokažte, zda existuje konečný vlastní podsoubor $T' \subsetneq T$ takový, že $T' \models \varphi$.

Věta 2.7 [o kompaktnosti] Nechť T je soubor formulí výrokové logiky. T je splnitelný právě když každá konečná část T je splnitelná.

✡✡✡ **Příklad 2.26** Mějme libovolný *nekonečný* soubor výrokových formulí T a formuli φ takovou, že $T \models \varphi$. Rozhodněte a dokažte, zda existuje konečný podsoubor $T' \subsetneq T$ takový, že $T' \models \varphi$.

Řešení Tvrzení platí. Jeden způsob, jak toto tvrzení dokázat, je s použitím věty o korektnosti a úplnosti pro Lukasiewiczův odvozovací systém pro výrokovou logiku (viz kapitola 4, kde se k tomuto příkladu ještě vrátíme). Protože jsme se však v této sbírce dosud odvozovacími systémy nezabývali, ukážeme si alternativní důkaz tohoto tvrzení pomocí věty o kompaktnosti.

Nejprve si uvědomme, že soubor $T \cup \{\neg\varphi\}$ není splnitelný. Pokud by totiž existovala valuace v splňující tento soubor, musela by tato valuace zejména splňovat soubor T. Protože dle předpokladu $T \models \varphi$, muselo by platit i $v(\varphi) = 1$ a tedy $v(\neg\varphi) = 0$, spor. Dle věty o kompaktnosti tedy existuje konečný soubor formulí $T_0 \subsetneq T \cup \{\neg\varphi\}$ který není splnitelný. Pokud $T_0 \subsetneq T$, pak za hledaný soubor T' ze zadání můžeme vzít přímo T_0, neboť libovolná formule (tedy i φ) je tautologickým důsledkem nesplnitelného souboru formulí. V opačném případě lze psát $T_0 = T_1 \cup \{\neg\varphi\}$, kde $T_1 \subseteq T$. Tvrdíme, že $T_1 \models \varphi$. Pokud je T_1 nesplnitelný, pak toto platí triviálně. V opačném případě uvažme libovolnou valuaci v splňující T_1. Pak musí platit, že $v(\neg\varphi) = 0$, jinak by T_0 byl splnitelný. Tedy $v(\varphi) = 1$. Protože v byla libovolná valuace splňující T_1, platí $T_1 \models \varphi$. ▲

✪✪✩ **Příklad 2.27** Následující příklady není těžké vyřešit bez použití věty o kompaktnosti, zkuste je ale vyřešit pomocí této věty.

a) Nechť A je spočetná množina. Dokažte, že existuje lineární uspořádání $\preceq$ na A.

b) Nechť S je nekonečný jazyk nad abecedou $\{0, 1\}$. Dokažte, že existuje nekonečné slovo $a_1 a_2 a_3 \cdots$ takové, že pro každé $i \in \mathbb{N}$ je $a_1 \cdots a_i$ prefixem nějakého prvku z S.

c) Nechť A, B jsou spočetné množiny a $R \subseteq A \times B$ je relace taková, že pro každé $a \in A$ je $B_a = \{b \mid (a, b) \in R\}$ konečný neprázdný soubor. Dokažte, že pokud pro každou *konečnou* část $A' \subseteq A$ existuje injektivní funkce $f_{A'} : A' \to B$ taková, že $f_{A'} \subseteq R$ (zde funkci $f_{A'}$ chápeme jako relaci), pak existuje také injektivní funkce $f : A \to B$ taková, že $f \subseteq R$.

✪✩✩ **Příklad 2.28** Nechť φ, ψ a ξ jsou formule výrokové logiky. Dokažte, že platí:

a) $(\varphi \to \psi) \approx (\neg\varphi \vee \psi)$
b) $\neg(\varphi \wedge \psi) \approx (\neg\varphi \vee \neg\psi)$
c) $\neg(\varphi \vee \psi) \approx (\neg\varphi \wedge \neg\psi)$
d) $(\varphi \wedge (\psi \vee \xi)) \approx ((\varphi \wedge \psi) \vee (\varphi \wedge \xi))$
e) $(\varphi \vee (\psi \wedge \xi)) \approx ((\varphi \vee \psi) \wedge (\varphi \vee \xi))$

✪✩✩ **Příklad 2.29** Převeďte formuli $(A \to B) \wedge ((C \to E) \to \neg(C \wedge \neg D))$ do DNF.

✪✩✩ **Příklad 2.30** Převeďte formuli $(A \to B) \vee ((C \to E) \to \neg(C \wedge \neg D))$ do CNF.

Kapitola 3

Nestandardní logické systémy

Jak již bylo zmíněno v první kapitole, existují systémy výrokové logiky s různými množinami operátorů. V této kapitole budeme analyzovat tyto systémy z hlediska jejich "popisné síly". Kritérium, podle kterého budeme popisnou sílu hodnotit, je schopnost vyjádřit *výrokové funkce*.

Definice 3.1 *Výroková funkce* je funkce $F : \{0,1\}^n \to \{0,1\}$, kde $n \geq 1$.

Intuitivně n-ární výroková funkce je totální funkce, která každému n-árnímu vektoru nul a jedniček přiřadí nulu, nebo jedničku. Příklad výrokové funkce můžeme vidět v tabulce 3.

✡✡✡ **Příklad 3.1** Kolik je všech n-árních výrokových funkcí?

Řešení Pro n-ární funkci máme 2^n řádků v tabulce. V posledním sloupci tabulky můžeme mít $2^{\text{počet řádků}}$ různých vektorů nul a jedniček. Každý vektor reprezentuje jednu výrokovou funkci. Tedy počet všech n-árních výrokových funkcí je 2^{2^n}. ▲

1	1	0
1	0	1
0	1	1
0	0	0

Tabulka 3.1: Příklad binární výrokové funkce zadané tabulkou - jde o klasickou funkci „XOR“.

Nyní si obecně definujeme logický systém pro libovolný konečný soubor výrokových funkcí.

Definice 3.2 Nechť $F_1, \ldots, F_k$ je konečný soubor výrokových funkcí. Definujeme formální logický systém $\mathcal{L}(F_1, \ldots, F_k)$, kde

- Abeceda je tvořena znaky pro výrokové proměnné, závorkami a znaky $\mathcal{F}_1, \ldots, \mathcal{F}_k$ pro uvedené výrokové funkce.
- Pojem formule systému $\mathcal{L}(F_1, \ldots, F_k)$ je definován v definici 1.7.
- Valuace rozšíříme z výrokových proměnných na formule předpisem $v(\mathcal{F}(\psi_1, \ldots, \psi_n)) = F(v(\psi_1), \ldots, v(\psi_n))$.

Všimněme si, že nyní už máme formálně zadefinovanou syntax i sémantiku obecného logického systému. Dosud uvažovaný logický systém je podle definice 3.2 $\mathcal{L}(\neg, \vee, \wedge, \rightarrow)$. Dříve zavedené sémantické pojmy (splnitelnost, pravdivost, atd.) se opírají pouze o pojem valuace a „fungují“ tedy v libovolném systému $\mathcal{L}(F_1, \ldots, F_k)$.

Od tohoto okamžiku budeme směřovat k definici *plnohodnotnosti* logického systému, což je schopnost popsat libovolnou výrokovou funkci. K tomu je nutné definovat pro libovolnou formuli logického systému její výrokovou funkci. Pro účely tyto definice zvolme libovolné (ale dále pevné) lineární uspořádání $\sqsubseteq$ na souboru všech výrokových proměnných.

Definice 3.3 Nechť φ je formule $\mathcal{L}(F_1, \ldots, F_k)$ a nechť $X_1, \ldots, X_n$ je vzestupně uspořádána posloupnost (vzhledem k $\sqsubseteq$) všech výrokových proměnných, které se ve φ vyskytují. Formule φ jednoznačně určuje výrokovou funkci $F_\varphi : \{0,1\}^n \rightarrow \{0,1\}$ danou předpisem $F_\varphi(\overrightarrow{u}) = v_{\overrightarrow{u}}(\varphi)$, kde $v_{\overrightarrow{u}}$ je valuace definovaná takto:

- $v_{\overrightarrow{u}}(X_i) = \overrightarrow{u}(i)$ pro každé $1 \leq i \leq n$ (kde $\overrightarrow{u}(i)$ značí i-tou složku vektoru $\overrightarrow{u}$),
- $v_{\overrightarrow{u}}(Y) = 0$ pro ostatní proměnné Y.

Z definice F_φ v definici 3.3 plyne, že $\overrightarrow{u} \in \{0,1\}^n$ je n-ární vektor nul a jedniček. Tento vektor $\overrightarrow{u}$ nám díky lineárnímu uspořádání $\sqsubseteq$ na souboru všech výrokových proměnných jednoznačně určuje valuaci $v_{\overrightarrow{u}}$ na výrokových proměnných a tím pádem i na libovolné formuli φ. Pro libovolný takový vektor a formuli φ lze tedy jednoznačně definovat hodnotu výrokové funkce $F_\varphi(\overrightarrow{u})$ na vektoru $\overrightarrow{u}$ jako valuaci $v_{\overrightarrow{u}}(\varphi)$.

Z definice funkce určené formulí přímo plyne, že pokud $\varphi \approx \varphi'$, kde formule φ obsahuje stejné proměnné jako φ', pak $F_\varphi = F_{\varphi'}$.

1	1	0
1	0	1
0	1	1
0	0	1

Tabulka 3.2: Výroková funkce pro Schefferův operátor $\varphi \curlywedge \psi \approx \neg(\varphi \wedge \psi)$

1	1	0
1	0	0
0	1	0
0	0	1

Tabulka 3.3: Výroková funkce pro Schröderův operátor $\varphi \mid \psi \approx \neg(\varphi \vee \psi)$

✪✪ **Příklad 3.2** Mějme nějaký logický systém $\mathcal{L}(F_1, \ldots, F_k)$. Nechť φ je libovolná formule tohoto systému a nechť ξ_1, $\theta_1, \ldots, \xi_\ell, \theta_\ell$ jsou formule takové, že $\xi_j \approx \theta_j$ pro všechna $1 \leq j \leq \ell$. Dokažte, že $\varphi \approx \varphi(\xi_1/\theta_1, \ldots, \xi_\ell/\theta_\ell)$ (viz definice 1.8).

✪✪ **Příklad 3.3** Mějme logický systém $\mathcal{L}(F_1, \ldots, F_k)$. Nechť φ a $\xi_1, \ldots, \xi_\ell$ jsou libovolné formule tohoto systému. Dokažte, že v libovolné valuaci v platí $v(\varphi(X_1/\xi_1, \ldots, X_\ell/\xi_\ell)) = v'(\varphi)$, kde v' je valuace definovaná následovně: pro libovolné $1 \leq j \leq \ell$ klademe $v'(X_j) = v(\xi_\ell)$, pro jakoukoliv jinou proměnnou Y klademe $v'(Y) = v(y)$.

Řešení Postupujeme indukcí vzhledem ke struktuře formule φ. Pokud $\varphi = X$, kde X je proměnná, máme dvě možnosti: buď $X = X_j$ pro nějaké $1 \leq j \leq \ell$ a pak $v(\varphi(X_1/\xi_1, \ldots, X_\ell/\xi_\ell)) = v(\xi_j) = v'(X_j) = v'(\varphi)$, nebo X není rovna ani jedné z proměnných X_j a potom $v(\varphi(X_1/\xi_1, \ldots, X_\ell/\xi_\ell)) = v(X) = v'(X)$.

Nechť nyní $\varphi = \mathcal{F}_i(\varphi_1, \ldots, \varphi_{a_i})$, kde a_i je arita funkce F_i. Pak platí, že $\varphi(X_1/\xi_1, \ldots, X_\ell/\xi_\ell) = \mathcal{F}_i(\varphi'_1, \ldots, \varphi'_{a_i})$, kde pro všechna $1 \leq r \leq a_i$ je $\varphi'_r = \varphi_r(X_1/\xi_1, \ldots, X_\ell/\xi_\ell)$. Pro libovolnou valuaci v máme

$$\begin{aligned} v(\varphi(X_1/\xi_1, \ldots, X_\ell/\xi_\ell)) &= F_i(v(\varphi'_1), \ldots, v(\varphi'_{a_i})) = F_i(v'(\varphi_1), \ldots, v'(\varphi_\ell)) \\ &= v'(\varphi), \end{aligned}$$

kde druhá rovnost plyne z indukčního předpokladu. ▲

Definice 3.4 Systém $\mathcal{L}(F_1, \ldots, F_k)$ je plnohodnotný, jestliže pro každou výrokovou funkci F existuje formule φ systému $\mathcal{L}(F_1, \ldots, F_k)$ taková, že $F = F_\varphi$.

Věta 3.5 Logický systém $\mathcal{L}(\neg, \vee, \wedge)$ je plnohodnotný.

Důkaz Použitím tabulky výrokových funkcí a disjunktivní normální formy, viz přednáška.

Termín plnohodnotnosti není samoúčelný. Například v počítačích jsou veškeré výpočty vykonávány v dvojkové soustavě a na nejnižší úrovni jsou výpočty implementovány pomocí tranzistorů nebo diod spájených do hradel, které jsou schopny vykonávat jednoduché logické operace (AND, OR, NOT, NAND, NOR, XOR). V obvodech se nemusí vyskytovat všechny typy hradel (z ekonomických důvodů), zpravidla je ale výběr hradel takový, aby bylo možné implementovat libovolnou funkci, tedy aby byl systém hradel plnohodnotný.

Další aplikace plnohodnotnosti je při dokazování vlastností logických systémů. Například doteď jsme pracovali se systémem $\mathcal{L}(\neg, \vee, \wedge, \rightarrow)$ a víme, že systém $\mathcal{L}(\neg, \vee, \wedge)$ je plnohodnotný. Tedy dokážeme $\rightarrow$ ekvivalentně vyjádřit pomocí systému $\mathcal{L}(\neg, \vee, \wedge)$ a můžeme používat $\rightarrow$ pouze jako syntaktickou zkratku. Požití systému $\mathcal{L}(\neg, \vee, \wedge)$ namísto systému $\mathcal{L}(\neg, \vee, \wedge, \rightarrow)$ může vést k zjednodušení důkazů např. budeme mít méně případů ověřování při strukturální indukci.

Abychom obecně dokázali, že je nějaký logický systém plnohodnotný, měli bychom správně ukázat, jak pro libovolnou výrokovou funkci nalézt příslušnou formuli, která tuto funkci zadává. Ve skutečnosti často využíváme faktu, že nějaký jiný logický systém je plnohodnotný. Pokud bychom např. měli formálně správně metadokázat, že systém $\mathcal{L}(\neg, \wedge)$ je plnohodnotný s pomocí toho, že systém $\mathcal{L}(\neg, \wedge, \vee)$ je plnohodnotný, měli bychom ukázat, že pro libovolnou formuli φ logického systému $\mathcal{L}(\neg, \wedge, \vee)$ existuje formule ψ logického systému $\mathcal{L}(\neg, \wedge)$ taková, že $F_\varphi = F_\psi$. Následující příklad ukazuje, že ve skutečnosti stačí ukázat, že systém $\mathcal{L}(\neg, \wedge)$ dokáže vyjádřit všechny spojky logického systému $\mathcal{L}(\neg, \wedge, \vee)$.

✩✩✩ **Příklad 3.4** Mějme formální logické systémy $\mathcal{L}_1 = \mathcal{L}(F_1, \ldots, F_k)$ a $\mathcal{L}_2 = \mathcal{L}(G_1, \ldots, G_\ell)$. Předpokládejme, že pro libovolné $1 \leq i \leq k$ existuje formule ψ_i systému $\mathcal{L}_2$ taková, že $F_{\psi_i} = F_i$. Pak pro libovolnou formuli φ systému $\mathcal{L}_1$ existuje formule ψ systému $\mathcal{L}_2$ taková, že $F_\varphi = F_\psi$.

Řešení Dle definice 3.3 lze předpokládat, že pro libovolné $1 \leq i \leq k$ se ve formuli ψ_i vyskytuje právě k_i různých proměnných $X_1, \ldots, X_{a_i}$, kde a_i je arita funkce F_i. Nechť L_1, resp. L_2, označuje soubor všech formulí systému $\mathcal{L}$, resp. $\mathcal{L}_2$. Uvažme též logický systém $\mathcal{L} = \mathcal{L}(F_1, \ldots, F_k, G_1, \ldots, G_\ell)$ a označme L soubor všech formulí tohoto systému. Zřejmě $L_1 \cup L_2 \subseteq L$. Definujeme transformaci $T\colon L_1 \to L_2$, která nahrazuje spojku $\mathcal{F}_i$ formulí ψ_i induktivně takto: pokud Y je libovolná proměnná, pak klademe $T(Y) = Y$. Pokud φ je formule tvaru $\mathcal{F}_i(\xi_1, \ldots, \xi_{a_i})$, pak klademe

$$T(\varphi) = \psi_i(X_1/T(\xi_1), X_2/T(\xi_2) \cdots, X_{a_i}/T(\xi_{a_i})).$$

Jinak řečeno, $T(\varphi)$ vznikne nahrazením proměnné X_j ve formuli ψ_i formulí $T(\xi_j)$, přičemž nahrazení provedeme současně pro všechna $1 \leq j \leq a_i$ (viz definice 1.8).

Ukážeme, že pro libovolnou formuli $\varphi \in L_1$ platí následující tvrzení: ve φ a $T(\varphi)$ se vyskytují stejné proměnné a $F_\varphi = F_(T(\varphi))$. Pak pro libovolnou formuli φ systému $\mathcal{L}_1$ je formule $T(\varphi)$ formulí systému $\mathcal{L}_2$ pro kterou platí $F_\varphi = F_{T(\varphi)}$.

Postupujeme indukcí vzhledem ke struktuře formule φ. Pokud φ je proměnná, pak $T(\varphi) = \varphi$ a triviálně platí $F_\varphi = F_{T(\varphi)}$. Pokud $\varphi \in L_1$ je tvaru $\mathcal{F}_i(\xi_1, \ldots, \xi_{a_i})$, pak formule $\xi_1, \ldots, \xi_{a_i}$ rovněž náleží L_1 a platí tedy pro ně indukční předpoklad. Zejména platí, že libovolná proměnná se vyskytuje ve φ, právě když se vyskytuje v nějakém ξ_j, $1 \leq j \leq a_i$ což dle indukčního předpokladu nastane právě tehdy, když se tato proměnná vyskytuje v nějakém $T(\xi_j)$ a tedy i v $T(\varphi)$. Ve formulích φ a $T(\varphi)$ se tedy vyskytují stejné proměnné. Dále pro libovolný vektor $u \in \{0,1\}^{a_i}$ platí

$$\begin{aligned} F_\varphi(u) &= F_i(F_{\xi_1}(u), \ldots, F_{\xi_{a_i}}(u)) = F_i(F_{T(\xi_1)}(u), \ldots, F_{T(\xi_{a_i})}(u)) \\ &= F_{\psi_i}(F_{T(\xi_1)}(u), \ldots, F_{T(\xi_{a_i})}(u)) = F_{T(\varphi)}(u), \end{aligned}$$

kde druhá rovnost plyne z indukčního předpokladu, třetí rovnost plyne z toho, že $F_{\psi_i} = F_i$ a poslední rovnost plyne z příkladu 3.3.

Tím je tvrzení dokázáno. ▲

✡☆☆ **Příklad 3.5** Rozhodněte a dokažte, zda je logický systém $\mathcal{L}(\neg, \wedge)$ plnohodnotný.

Řešení Platí $(X \vee Y) \approx \neg(\neg X \wedge \neg Y)$ (dá se ukázat např. tabulkou). Dle příkladu 3.4 tedy v systému $\mathcal{L}(\neg, \wedge)$ lze vyjádřit všechny výrokové funkce, které jsou vyjádřitelné v systému $\mathcal{L}(\neg, \vee, \wedge)$. Protože druhý zmíněný systém je plnohodnotný, je i $\mathcal{L}(\neg, \wedge)$ plnohodnotný. ▲

Toto schéma důkazu je možné využít automaticky, proto při ukázaní plnohodnotnosti systému $\mathcal{L}(F_1, \ldots, F_n)$ na základě plnohodnotnosti jiného systému $\mathcal{L}(G_1, \ldots, G_k)$ postačí, když ukážeme, že pro každou m-ární výrokovou funkci $F_i(\varphi_1, \ldots, \varphi_m)$ systému $\mathcal{L}(G_1, \ldots, G_k)$, která se nevyskytuje v $\{F_1, \ldots, F_n\}$, existuje formule φ systému $\mathcal{L}(F_1, \ldots, F_n)$, t.ž. $F_i(\varphi_1, \ldots, \varphi_m) \approx \varphi$ nebo $F_i = G_\varphi$.

✡✡ **Příklad 3.6** Rozhodněte a dokažte, zda je logický systém $\mathcal{L}(\wedge)$ plnohodnotný.

Řešení Tvrzení neplatí. Abychom to ukázali, dokážeme, že libovolná formule φ systému $\mathcal{L}(\wedge)$ má následující vlastnost P:

> P: pokud se ve φ vyskytuje pouze jedna výroková proměnná (bez újmy na obecnosti ji označíme X_1), pak $X_1 \approx \varphi$.

Uvědomme si, že z toho již plyne, že v systému $\mathcal{L}(\wedge)$ není možné vyjádřit negaci. Pro libovolnou formuli φ tohoto systému pak totiž platí platí $F_\varphi(0) = F_{X_1}(0) = 0 \neq \neg(0)$.

Fakt, že každá formule φ splňuje vlastnost P dokážeme strukturální indukcí.

- **Báze:** Pro formuli X_1 zřejmě platí $X_1 \approx X_1$.
- **Indukční krok:** Je-li φ tvaru $\varphi_1 \wedge \varphi_2$, kde φ_1 i φ_2 mají vlastnost P, pak mohou nastat dva případy. Buď φ obsahuje více než jednu proměnnou, v kterémžto případě φ triviálně splňuje P. Nebo φ obsahuje jen jednu proměnnou (označme ji X_1) a tedy i φ_1, φ_2 obsahují pouze tuto proměnnou. Protože φ_1, φ_2 mají vlastnost P, musí platit $\varphi_1 \wedge \varphi_2 \approx X_1 \wedge X_1 \approx X_1$, kde první ekvivalence plyne z příkladu 3.2 a druhá je triviální.

▲

✡✡ **Příklad 3.7** Rozhodněte a dokažte, zda jsou následující logické systémy plnohodnotné.

a) $\mathcal{L}(\neg)$
b) $\mathcal{L}(\wedge, \vee)$
c) $\mathcal{L}(\neg, \rightarrow)$
d) $\mathcal{L}(|)$

✡ **Příklad 3.8** Dejte příklad výrokové formule φ logického systému $\mathcal{L}(\rightarrow, \neg)$ takovou, že $F_\varphi : \{0,1\}^2 \rightarrow \{0,1\}$ (tedy funkce "vyjádřená"formulí φ) je dána následující tabulkou (v posledním sloupci jsou hodnoty pro vstup určený prvními dvěma sloupci):

1	1	0
1	0	1
0	1	1
0	0	0

✡✡ **Příklad 3.9** Pro výrokovou logiku mějme formální logický systém $\mathcal{L}(\bullet, m)$, kde $\bullet$ je unární výroková funkce taková, že pro libovolné $a \in \{0,1\}$ je $\bullet(a) = 1$ a m je ternární tzv. *majoritní* funkce, tj. funkce taková, že pro libovolné $a, b, c \in \{0,1\}$ máme

$$m(a,b,c) = \begin{cases} a & \text{pokud } a = b \\ c & \text{jinak.} \end{cases}$$

Rozhodněte a dokažte, zda existují formule φ, ψ systému $\mathcal{L}(\bullet, m)$ takové, že

a) $F_\varphi = F_{\neg X}$,

b) $F_\psi = F_{X \vee Y}$.

(Zde $\neg$ a $\vee$ jsou standardní operace „negace“ a „disjunkce“.)

Řešení Než popíšeme řešení, uvědomme si, že majoritní funkce vždy vrací tu z hodnot 0, 1, která se mezi jejími třemi argumenty vyskytne alespoň dvakrát.

ad a): Taková formule v systému $\mathcal{L}(\bullet, m)$ neexistuje. Abychom to dokázali, ukažme, že pro libovolnou formuli φ tohoto systému s jednou proměnnou platí $F_\varphi = id_{\{0,1\}}$ nebo $F_\varphi = F_{\bullet X}$. Postupujeme strukturální indukcí. Pokud $\varphi = X$, pak zřejmě $F_\varphi = id_{\{0,1\}}$. Pokud $\varphi = \bullet\psi$, pak $F_\varphi = F_{\bullet X}$. Předpokládejme tedy, že $\varphi = m(\psi_1, \psi_2, \psi_3)$, kde pro ψ_1, ψ_2, ψ_3 dokazované tvrzení platí. Mohou nastat dva případy. Buď pro alespoň dva indexy $j \in \{1,2,3\}$ platí $F_{\psi_j} = F_{\bullet X}$ a pak (z definice majoritní funkce) i $F_\varphi = F_{\bullet X}$. Nebo pro alespoň dva indexy $j \in \{1,2,3\}$ platí $F_{\psi_j} = id_{\{0,1\}}$, a pak i $F_\varphi = id_{\{0,1\}}$. Tím je požadované tvrzení dokázáno.

ad b): Taková formule existuje, stačí uvážit například $\psi = m(X, Y, \bullet X)$. Rovnost $F_\psi = F_{X \vee Y}$ lze ověřit sestrojením pravdivostních tabulek pro obě formule. (Ověřte!)

▲

✪✩✩ **Příklad 3.10** Pro formuli $\varphi = A \to (B \to (C \to D))$ nalezněte ekvivalentní formuli v logickém systému $\mathcal{L}(|)$, kde $|$ je Shefferův operátor (t.j. $\psi \mid \xi \approx \neg(\psi \wedge \xi)$).

✪✩✩ **Příklad 3.11** Mějme formuli výrokové logiky $\varphi \equiv (X \leftrightarrow Y)$. Najděte k ní ekvivalentní formuli v logickém systému $\mathcal{L}(\to, \neg)$, pokud taková existuje.

✪✩✩ **Příklad 3.12** K následující formuli zadejte ekvivalentní formuli v (neplnohodnotném) logickém systému $\mathcal{L}(\wedge, \to)$.

$$((B \wedge \neg C) \vee \neg A) \vee (B \wedge D)$$

✪✩✩ **Příklad 3.13** K následující formuli zadejte ekvivalentní formuli v (neplnohodnotném) logickém systému $\mathcal{L}(\vee, \to)$.

$$\neg((\neg B \vee A) \wedge (\neg C \vee A) \wedge \neg D)$$

✪✩✩ **Příklad 3.14** Mějme binární výrokovou funkci $\to$ zadávající standardní implikaci a unární výrokovou funkci $\triangle$ takovou, že

$$\triangle\,(1) = 0$$

$$\triangle\,(0) = 0$$

Rozhodněte a dokažte, zda formální logický systém $\mathcal{L}(\to, \triangle)$ je plnohodnotný.

Pro výrokové funkce $\to$ a $\triangle$ používejte ve formulích tohoto systému shodné symboly, tedy $\to$ a $\triangle$. V důkazu můžete využít plnohodnotnost jiných logických systémů z přednášky.

Definice 3.6 Výroková funkce F je Schefferovská, jestliže $\mathcal{L}(F)$ je plnohodnotný systém.

✪✪✪ **Příklad 3.15** Dokažte následující tvrzení: Výroková funkce F arity $n \geq 1$ je Shefferovská právě tehdy, když platí následující podmínky:

a) $\mathcal{F}(P, \ldots, P) \approx \neg P$ (P je výroková proměnná)

b) pro nějaká $x_1, \ldots, x_n \in \{P, Q\}$ (P, Q jsou různé výrokové proměnné) platí, že $\mathcal{F}(x_1, \ldots, x_n)$ *není* ekvivalentní ani $\neg P$ ani $\neg Q$. (Výše $\mathcal{F}$ značí n-ární výrokovou spojku příslušející funkci F.)

Řešení <=: Předpokládejme platnost podmínek 1. a 2. a nechť proměnné $x_1, \ldots, x_n \in \{P, Q\}$ jsou takové, že $\mathcal{F}(x_1, \ldots, x_n)$ *není* ekvivalentní ani $\neg P$ ani $\neg Q$.
Idea: Následující pravdivostní tabulka ukazuje, jakých pravdivostních hodnot může nabývat formule $\mathcal{F}(x_1, \ldots, x_n)$.

P	Q	$\mathcal{F}(x_1, \ldots, x_n)$	$\mathcal{F}(x_1, \ldots, x_n)$
1	1	0	0
1	0	0	1
0	1	0	1
0	0	1	1

Z tabulky je zřejmé, že máme pouze dvě možnosti. Ostatní možnosti jsou vyloučeny podmínkami 1. a 2. V prvním případě se symbol $\mathcal{F}$ chová jako spojka $\curlywedge$ (NOR) a ve druhém případě jako $|$ (NAND). Obě tyto spojky jsou Shefferovské, což nám dá požadovaný výsledek.
Formální důkaz: Pro $x, y \in \{0, 1\}$ označme $u^{xy} = (u_1^{xy}, \ldots, u_n^{xy}) \in \{0, 1\}^n$ vektor délky n definovaný takto:

$$u_i^{xy} = \begin{cases} x & \text{pokud } x_i = P \\ y & \text{pokud } x_i = Q \end{cases}$$

Pozorování:

(a) $F(u^{00}) = 1$ a $F(u^{11}) = 0$ (plyne přímo z podmínky 1.)

(b) Pokud by platilo, $F(u^{10}) = 0$ a $F(u^{01}) = 1$, pak by bylo $\mathcal{F}(x_1, \ldots, x_n) \approx \neg P$

(c) Pokud by platilo, $F(u^{10}) = 1$ a $F(u^{01}) = 0$, pak by bylo $\mathcal{F}(x_1, \ldots, x_n) \approx \neg Q$

Tudíž možnosti (b) a (c) by byly v rozporu s naším předpokladem. Z toho plyne, že nám zbývají pouze dvě možnosti, jak se může funkce F chovat na vektorech u^{xy}. Tyto možnosti jsou

i. $F(u^{10}) = F(u^{01}) = 0$

ii. $F(u^{10}) = F(u^{01}) = 1$

V případě i. platí, že $F = F_{\curlywedge}$. V případě 2 pak platí $F = F_{|}$. Dle příkladu 3.4 existuje pro každou formuli φ systému $\mathcal{L}(\curlywedge)$ (v případě i.), resp. systému $\mathcal{L}(|)$ (v případě 2) formule ψ systému $\mathcal{L}(F)$ taková, že $F_\varphi = F_\psi$. Protože

systémy $\mathcal{L}(\curlywedge)$ a $\mathcal{L}(|)$ jsou plnohodnotné (viz přednáška), musí být i systém $\mathcal{L}(F)$ plnohodnotný, tj. funkce F je Shefferovská.

=>: Důkaz provedeme obměnou. Předpokládejme nejprve, že neplatí podmínka a) ze zadání příkladu. Máme celkem tři možnosti.

(i.) $F(1,\ldots,1) = 1$ a $F(0,\ldots,0) = 0$

(ii.) $F(1,\ldots,1) = 1$ a $F(0,\ldots,0) = 1$

(iii.) $F(1,\ldots,1) = 0$ a $F(0,\ldots,0) = 0$

Následující tvrzení ukazuje, že ani v jednom z výše uvedených případů, nemůže být funkce F Shefferovská.

Tvrzení: Nechť φ je formule $\mathcal{L}(F)$ obsahující právě jednu výrokovou proměnnou P.

(i.) Jestliže $F(1,\ldots,1) = 1$ a $F(0,\ldots,0) = 0$ pak $F_\varphi(1) = 1$

(ii.) Jestliže $F(1,\ldots,1) = 1$ a $F(0,\ldots,0) = 1$ pak $F_\varphi(1) = 1$

(iii.) Jestliže $F(1,\ldots,1) = 0$ a $F(0,\ldots,0) = 0$ pak $F_\varphi(0) = 0$

Důkaz: ad (i.): Indukcí vzhledem k délce vytvořující posloupnosti pro φ.

- Jestliže φ je výroková proměnná P a ν je valuace taková, že $\nu(P) = 1$ a $\nu(Y) = 0$ pro ostatní výrokové proměnné Y, pak zřejmě $F_\varphi(1) = \nu(\varphi) = \nu(P) = 1$.
- Jestliže φ je tvaru $\mathcal{F}(\psi_1,\ldots,\psi_n)$ pro nějaké formule $\psi_1,\ldots,\psi_n$ a ν je valuace taková, že $\nu(P) = 1$ a $\nu(Y) = 0$ pro ostatní výrokové proměnné Y, pak z indukčního předpokladu plyne, že $\nu(\psi_i) = 1$ pro $1 \leq i \leq n$ a tedy

$$F_\varphi(1) = \nu(\mathcal{F}(\psi_1,\ldots,\psi_n)) = F(\nu(\psi_1),\ldots,\nu(\psi_n)) = F(1,\ldots,1) = 1$$

Body (ii.) a (iii.) se dokáží úplně stejně.

Z výše uvedeného tvrzení tedy plyne, že pokud není splněna podmínka a) ze zadání, pak funkce F není Shefferovská, neboť neexistuje formule φ systému $\mathcal{L}(F)$ taková, že $F_\varphi = F_\neg$.

Nyní předpokládejme, že podmínka a) je splněna, ale není splněna podmínka b) Dokážeme, že pro každou formuli $\varphi \in \mathcal{L}(F)$ s právě jednou výrokovou proměnnou P platí buď $\varphi \approx P$ nebo $\varphi \approx \neg P$. Důkaz povedeme indukcí vzhledem k délce vytvořující posloupnosti pro φ.

- Jestliže φ je výroková proměnná P, pak zřejmě $\varphi \approx P$.
- Jestliže φ je tvaru $\mathcal{F}(\psi_1, \ldots, \psi_n)$, pak z indukčního předpokladu plyne, že buď $\psi_i \approx P$ nebo $\psi_i \approx \neg P$ pro $1 \leq i \leq n$. Pak (viz. příklad 3.2) $\varphi \approx \mathcal{F}(\tilde{P}_1, \ldots \tilde{P}_n)$ kde

$$\tilde{P}_i = \begin{cases} P & \text{pokud } \psi_i \approx P \\ \neg P & \text{pokud } \psi_i \approx \neg P \end{cases}$$

  Uvažme nyní formuli $\varphi' = \mathcal{F}(x_1, \ldots, x_n)$, kde $x_i = P$ pokud $\tilde{P}_i = P$ a $x_i = Q$ jinak. Nechť přitom I_P (resp. I_Q) je množina všech indexů takových, že $x_i = P$ (resp. $x_i = Q$). Protože předpokládáme, že podmínka 2. *není* splněna, dostaneme, že buď $\varphi' \approx \neg P$ nebo $\varphi' \approx \neg Q$. V prvním případě to zejména znamená, že $v(\varphi') = v*(\varphi')$ pro libovolné dvě valuace takové, že $v(P) = v-(P)$. Nyní pro libovolnou valuaci v uvažme valuaci $v*$ takovou, že $v*(Q) = v(\neg P)$ a $v*(X) = v(X)$ pro proměnné $X \neq Q$. Pak pro libovolnou valuaci v platí $v(\varphi) = v*(\varphi') = v(\varphi') = v(\neg P)$, kde druhá rovnost plyne z toho, že $v(P) = v*(P)$ a třetí z toho, že $\varphi' \approx \neg P$. Tedy $\varphi \approx \neg P$. Podobně se ukáže, že pokud $\varphi' \approx \neg Q$ pak i $\varphi \approx \neg Q$.

Z výše uvedeného plyne, že neexistuje formule $\varphi \in \mathcal{L}(F)$ taková, že $F_\varphi(1) = 1$ a $F_\varphi(0) = 1$ a tudíž F není Shefferovská. ▲

✡✡ **Příklad 3.16** Rozhodněte a dokažte (bez použití Příkladu 3.15!) zda jsou následující formální logické systémy plnohodnotné.

a) $\mathcal{L}(\rightarrow)$[1]

b) $\mathcal{L}(\leftrightarrow)$

✡✡✡ **Příklad 3.17** Pokuste se na základě klasifikace z Příkladu 3.15 odvodit vzorec vyjadřující počet n-árních Shefferovských funkcí (viz. přednáška).

[1] Symbol $\rightarrow$ zde zastupuje binární funkci, která udává sémantiku (tj. pravdivostní tabulku) implikace

Kapitola 4

Dokazovací systém pro výrokovou logiku

Podstatnou motivací pro vznik matematické logiky bylo studium *platnosti úsudků*, tedy toho, zda nějaké tvrzení logicky vyplývá ze zadaných předpokladů. Řečeno jazykem výrokové logiky: zajímá nás, zda pro daný soubor formulí T a danou formuli φ platí $T \models \varphi$. Navíc bychom rádi toto ověření korektnosti zautomatizovali, aby o platnosti úsudku vskutku nebylo pochyb.

Je-li soubor T konečný, např. $T = \{\varphi_1, \ldots, \varphi_k\}$, pak lze ukázat, že $T \models \varphi$ právě když $(\varphi_1 \wedge \cdots \wedge \varphi_k) \to \varphi$ je tautologie. Přitom otázku, zda nějaká formule je tautologie, může relativně snadno zodpovědět počítač (například sestrojením tabulky pravdivostních hodnot, existují ovšem mnohem efektivnější algoritmy). Tento přístup má ovšem dvě zásadní nevýhody. Za prvé, soubor předpokladů nemusí být nutně konečný (s takovými soubory se setkáme zejména později v predikátové logice). V takovém případě není výše uvedený postup vůbec použitelný, a to ani v tom případě, kdy je soubor T nějakým způsobem konečně reprezentovatelný, tj. zpracovatelný počítačem. Za druhé, znalost toho, že $(\varphi_1 \wedge \cdots \wedge \varphi_k) \to \varphi$ je tautologie, nás sice přesvědčuje o tom, že φ je důsledkem T, nedává ale žádný vhled do toho, *proč* tomu tak je. Jinak řečeno, nedozvíme se nic o struktuře daného úsudku, o tom, jakým myšlenkovým procesem lze danou formuli z předpokladů odvodit.

Z tohoto důvodu zavádíme pojem *odvozovacího systému*, tj. souboru pravidel, pomocí nichž lze ryze syntakticky, bez jakékoliv znalosti sémantiky, vytvářet („odvozovat“) z nějakých předpokladů nové formule. Oddělení syntaxe od sémantiky je důležité, aby tuto činnost mohl vykonávat i stroj, který sémantiku „nechápe“. Cílem je získat takový odvozovací systém, pomocí

kterého lze odvodit nějakou formuli φ z nějakého souboru formulí T právě když $T \models \varphi$.

Neformálně řečeno, odvozovací systém je dán souborem axiomů (či schémat axiomů) a souborem odvozovacích pravidel. V této části se soustředíme na tzv. Lukasiewiczův odvozovací systém pro $\mathcal{L}(\rightarrow, \neg)$ (vzpomeňme si, že libovolnou logickou spojku lze vyjádřit pomocí $\neg$ a $\rightarrow$). Ten je dán následovně:

Schémata axiómů:

- A1: $\varphi \rightarrow (\psi \rightarrow \varphi)$
- A2: $(\varphi \rightarrow (\psi \rightarrow \xi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \xi))$
- A3: $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

Odvozovací pravidlo:

- MP: Z φ a $\varphi \rightarrow \psi$ odvoď ψ. (modus ponens)

Definice 4.1 Buď T soubor formulí.

- Důkaz (či odvození) formule ψ ze souboru předpokladů T je konečná posloupnost formulí $\varphi_1, \cdots, \varphi_k$, kde φ_k je ψ a pro každé φ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:
  - φ_i je prvek T;
  - φ_i je instancí jednoho ze schémat A1–A3;
  - φ_i vznikne aplikací pravidla MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.
- Formule ψ je dokazatelná z předpokladů T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ z předpokladů T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme že ψ je dokazatelná a píšeme $\vdash \psi$.

Tím, že odvození probíhá postupně, v jednotlivých krocích, lze sledovat strukturu příslušného úsudku. Navíc v každém korektní odvození se využije pouze konečně mnoho předpokladů, počítač tedy může provést důkaz i z nekonečného souboru T, je-li tento soubor nějakým způsobem reprezentovatelný v počítači.

Je-li daný odvozovací systém *korektní*, pak máme zaručeno, že všechny odvozené formule jsou důsledky původních předpokladů. Je-li systém navíc *úplný*, pak lze pomocí něj odvodit právě formule vyplývající z daných předpokladů. Pro Lukasiewiczův systém byly na přednášce dokázány následující věty:

Věta 4.2 [o dedukci] Nechť φ, ψ jsou formule a T soubor formulí. Pak pro Lukasiewiczův systém platí: $T \cup \{\psi\} \vdash \varphi$ právě když $T \vdash \psi \to \varphi$.

Věta 4.3 [o korektnosti] Nechť φ je formule a T soubor formulí. Pak pro Lukasiewiczův systém platí: jestliže $T \vdash \varphi$, pak $T \models \varphi$.

Věta 4.4 [o úplnosti] Nechť φ je formule a T soubor formulí. Pak pro Lukasiewiczův systém platí: jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Předchozí věty ukazují, že Lukasiewiczův systém je přesnou formalizací úsudků ve výrokové logice (se spojkami $\neg, \to$). Příklady odvození v Lukasiewiczově systému je možné nalézt na slidech k přednášce.

✡✡✡ **Příklad 4.1** Nechť P a Q jsou výrokové proměnné. Rozhodněte, zda jsou následující formule dokazatelné. Pokud u některé formule rozhodnete, že je dokazatelná, nalezněte její důkaz v Lukasiewiczově systému.

a) $P \to (Q \to P)$
b) $P \to P$
c) $P \to Q$

✡✡✡ **Příklad 4.2** Rozhodněte a dokažte, zda pro každou formuli φ výrokové logiky platí buď $\vdash \varphi$, nebo $\vdash \neg\varphi$.

✡✡✡ **Příklad 4.3** Mějme *konečný* soubor formulí výrokové logiky T a formuli φ takovou, že $T \models \varphi$. Dokažte (bez odvolání se na větu o úplnosti), že $T \vdash \varphi$.

Můžete mimo jiné využít toto tvrzení (a nemusíte ho dokazovat):
Pro libovolnou formuli φ výrokové logiky takovou, že $\models \varphi$, platí $\vdash \varphi$.

✡✡✡ **Příklad 4.4** Rozhodněte a dokažte, zda pro libovolný soubor T formulí výrokové logiky a pro libovolné formule φ, ψ platí $T \cup \{\varphi\} \vdash \varphi \to \psi$.

Řešení Toto obecně neplatí. Uvažme T prázdný soubor, $\varphi = A$ a $\psi = B$, kde A, B jsou výrokové proměnné. Zřejmě platí $A \not\models A \to B$. Stačí uvážit valuaci v takovou, že $v(A) = 1$ a $v(B) = 0$. Tato valuace splňuje soubor $\{A\}$, ovšem $v(A \to B) = 0$. Dle věty o korektnosti musí platit $A \nvdash A \to B$. ▲

✡✡✡ **Příklad 4.5** Rozhodněte a dokažte, zda existuje formule výrokové logiky φ, která není tautologie, a soubor formulí T takový, že platí $T \vdash \varphi$.

Věty o korektnosti a úplnosti jsou mocným nástrojem, na přednášce však byly dokázány pouze pro Lukasiewiczův systém.[1] Ve zbytku této části budeme zkoumat různé jiné odvozovací systémy, u nichž korektnost ani úplnost a priori předpokládat nemůžeme.

✪✪ **Příklad 4.6** Mějme odvozovací systém s jedním schématem axiomu A1: $\varphi \to \varphi$ a s pravidlem modus ponens. Nechť φ je formule systému $\mathcal{L}(\to, \neg)$. Rozhodněte a dokažte, zda platí následující tvrzení.

a) Pokud $\vdash \varphi$, pak $\models \varphi$.
b) Pokud $\models \varphi$, pak $\vdash \varphi$.

Příklad 4.7 Uvažme formální logický systém $\mathcal{L}(\neg, \bullet)$ se dvěmi unárními výrokovými funkcemi, kde $\neg$ je standardní negace a $\bullet$ je unární výroková funkce taková, že pro libovolnou formuli ψ platí $\bullet\psi \approx (\psi \vee \neg\psi)$.

Uvažme dále následující odvozovací systém S pro $\mathcal{L}(\neg, \bullet)$. Systém S obsahuje jedno schéma axiomů

$$\text{A1:} \qquad \bullet\neg\psi$$

a následující 3 odvozovací pravidla:

P1:	z $\bullet\psi$	odvoď $\bullet\bullet\bullet\psi$,
P2:	z $\bullet\bullet\psi$	odvoď ψ,
P3:	z $\bullet\neg\neg\neg\psi$	odvoď $\neg\bullet\psi$.

Důkaz formule φ v systému S (z prázdného souboru předpokladů) je konečná posloupnost formulí $\xi_1, \ldots, \xi_k$, kde ξ_k je φ a navíc pro každé ξ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:

- ξ_i je instancí schématu A1;
- ξ_i vznikne aplikací jednoho z pravidel P1-P3 na formuli ξ_j, pro vhodné $1 \leq j < i$.

Řekneme, že formule φ je v systému S *dokazatelná* (značíme $\vdash_S \varphi$), existuje-li její důkaz v systému S.

Rozhodněte a dokažte, zda pro libovolnou formuli φ logického systému $\mathcal{L}(\neg, \bullet)$ platí: jestliže $\vdash_S \varphi$, pak $\models \varphi$.

[1] V literatuře lze nalézt mnoho jiných korektních a úplných odvozovacích systémů pro výrokovou logiku, těmi se však v této sbírce nebudeme zabývat.

Řešení Tvrzení neplatí. Dokážeme to tak, že v tomto systému odvodíme konkrétní formuli, která není tautologií. Uvažme tedy například následující důkaz formule $\neg \bullet X$ v systému S:

1)	$\bullet \neg\neg\neg X$	instance A1 (pro $\psi = \neg\neg X$)
2)	$\neg \bullet X$	P3 na 1)

Zřejmě ale $\neg \bullet X$ není tautologie (je to dokonce kontradikce).

▲

Příklad 4.8 [2] Uvažme odvozovací systém S z předchozího příkladu. Rozhodněte a dokažte, zda je v systému S dokazatelná formule $\bullet\bullet\neg X$, kde X je výroková proměnná.

Řešení Danou formuli nelze v systému S odvodit. Abychom to mohli dokázat, (meta)dokážeme nejprve platnost následujícího tvrzení:

Tvrzení 4.5 Nechť φ je libovolná formule dokazatelná v systému S. Pak počet výskytů symbolu $\bullet$ ve φ před prvním výskytem jakéhokoliv jiného symbolu (než $\bullet$) je lichý, nebo nulový.

Z předchozího tvrzení pak ihned plyne nedokazatelnost formule $\bullet\bullet\neg X$ v systému S, neboť v této formuli je počet výskytů symbolu $\bullet$ před prvním výskytem jiného symbolu roven 2; je tedy sudý a nenulový.

(Meta)důkaz Tvrzení 4.5: Fixujme důkaz $\xi_1, \ldots, \xi_k$ formule φ (ten existuje, neboť dle předpokladu je φ dokazatelná). Pro $i \in \{1, \ldots, k\}$ označme l_i počet symbolů $\bullet$ „na začátku“[3] ξ_i. Indukcí vzhledem k i ukážeme, že pro všechna $i \in \{1, \ldots, k\}$ je l_i liché číslo, nebo nula.

Předpokládejme, že $i = 1$. Pak ξ_i musí být instancí schématu A1 a musí tedy mít tvar $\bullet\neg\psi$ pro nějakou formuli ψ. Ihned vidíme, že $l_i = 1$.

Nyní předpokládejme, že $i > 1$ a že pro všechna $j < i$ je l_i liché číslo, nebo 0. Mohou nastat následující případy:

- ξ_i je instancí schématu A1. Pak lze stejně jako výše ukázat, že $l_i = 1$.
- ξ_i vznikne aplikací P1 na ξ_j, kde $j < i$. Ihned vidíme, že $l_i = l_j + 2$. Z indukčního předpokladu víme, že l_j je buď nula, nebo liché číslo. Z definice pravidla P1 ale zároveň vidíme, že ξ_j musí mít tvar $\bullet\psi$ pro

[2] Zadání tohoto příkladu bylo inspirováno takzvaným MU-puzzle z knihy Douglase Hofstadtera *Gödel, Escher, Bach: An Eternal Golden Braid.*

[3] Kdybychom chtěli být co nejformálnější, mohli bychom definovat l_i jakožto délku nejdelšího prefixu slova ξ_i skládajícího se pouze ze symbolů $\bullet$.

nějakou formuli ψ. Zejména tedy musí být $l_j \geq 1$ a tudíž $l_j \neq 0$. Dohromady dostáváme, že l_j musí být liché číslo a tedy i $l_i = l_j + 2$ je liché číslo.

- ξ_i vznikne aplikací P2 na ξ_j, kde $j < i$. Podobně jako v předchozím případě vidíme, že $l_i = l_j - 2$. Z indukčního předpokladu víme, že l_j je buď nula, nebo liché číslo. Z definice pravidla P2 ale zároveň vidíme, že ξ_j je tvaru $\bullet\bullet\psi$ pro vhodné ψ. Zejména tedy $l_j \neq 0$. Dohromady dostáváme, že l_j musí být liché a tedy i $l_i = l_j - 2$ je liché.

- ξ_i vznikne aplikací P3 na ξ_j, kde $j < i$. Pak ξ_i musí mít tvar $\neg\bullet\psi$ pro nějakou formuli ψ a tedy $l_i = 0$.

Tím je Tvrzení 4.5 dokázáno. Všimněme si, že ačkoliv není odvozovací systém S korektní (viz předchozí příklad), nelze v něm odvodit libovolnou formuli.

▲

Příklad 4.9 Uvažme formální logický systém $\mathcal{L}(\neg, \bullet)$ se dvěmi unárními výrokovými funkcemi, kde $\neg$ je standardní negace a $\bullet$ je unární výroková funkce taková, že pro libovolnou formuli ψ platí $\bullet\psi \approx (\psi \wedge \neg\psi)$.

Uvažme dále následující odvozovací systém R pro $\mathcal{L}(\neg, \bullet)$. Systém R obsahuje jedno schéma axiomů

$$\text{A1:} \qquad \neg\bullet\psi$$

a následující 3 odvozovací pravidla:

P1:	z $\neg\bullet\psi$	odvoď $\neg\bullet\neg\bullet\psi$,
P2:	z $\neg\bullet\psi$	odvoď $\neg\bullet\neg\psi$,
P3:	z ψ	odvoď $\neg\neg\psi$.

Důkaz formule φ v systému R je definován obdobně jako v příkladu 4.7.

Řekneme, že formule φ je v systému R *dokazatelná* (značíme $\vdash_R \varphi$), existuje-li její důkaz v systému R. Rozhodněte a dokažte, zda pro libovolnou formuli φ platí: jestliže $\vdash_R \varphi$, pak $\models \varphi$.

Řešení Tvrzení platí. Chceme dokázat: pro každou formuliφ logického systému $\mathcal{L}(\neg, \bullet)$ platí

$$\vdash \varphi \Rightarrow \models \varphi.$$

Stačí ukázat, že libovolná instance schématu A1 je tautologie, a že pokud je tautologií vstup některého z pravidel P1–P3, je tautologií i jeho výstup (tj. že každé pravidlo je korektní – z tautologie vždy odvodí tautologii).

A1: ukážeme, že $\models \neg \bullet \varphi$ pro libovolnou formuli φ. Fixujme libovonou ale nadále pevnou valuaci v a formuli φ. Pak $v(\bullet\varphi) = v(\varphi \wedge \neg\varphi) = 0$, což vyplývá z definice spojek $\bullet$, $\neg$ a $\wedge$. Z toho a z definice negace vyplývá, že $v(\neg \bullet \varphi) = 1$.

Abychom snadněji dokázali korektnost pravidel P1 a P2, dokážeme si následující pomocné tvrzení.

Tvrzení 4.6 Formule φ logického systému $\mathcal{L}(\neg, \bullet)$ je tautologie, právě když obsahuje alespoň jeden výskyt symbolu $\bullet$ a počet výskytů symbolu negace před prvním výskytem symbolu $\bullet$ je lichý.

(Meta)důkaz Tvrzení 4.6: Nejprve ukážeme, že libovolná formule systému $\mathcal{L}(\neg, \bullet)$, která obsahuje lichý výskyt symbolu $\neg$ před prvním výskytem symbolu $\bullet$, je tautologie. Potom ukážeme, že žádná jiná formule systému $\mathcal{L}(\neg, \bullet)$ nemůže být tautologie.

Výše jsme ukázali, že $v(\bullet\xi) = 0$ pro libovolnou formuli ξ a valuaci v. Z definice negace dále plyne $\xi \approx \neg\neg\xi$ pro libovolnou ξ. Tedy pro formuli $\psi = \neg \ldots \neg \bullet \varphi$, která má lichý počet negací před prvým výskytem $\bullet$ platí $\psi \approx \neg \bullet \varphi$. Výše jsme ukázali, že $\neg \bullet \varphi$ je tautologie a tedy i ψ je tautologie.

Ukažme nyní, že formule nemající uvedený tvar nemůže být tautologií. Mohou nastat dva případy: buď φ neobsahuje $\bullet$, nebo obsahuje $\bullet$ a před prvním výskytem $\bullet$ má sudý počet výskytů symbolu $\neg$.

Nejprve předpokládejme, že ψ obsahuje $\bullet$ a před prvním výskytem $\bullet$ má sudý počet negací, tj. má tvar $\psi = \neg \ldots \neg \bullet \varphi$. Z $\xi \approx \neg\neg\xi$ pro libovolnou ξ plyne $\psi \approx \bullet\varphi$. Výše jsme ukázali, že $v(\bullet\xi) = 0$ pro libovolnou formuli ξ a valuaci v. Tedyψ není tautologie (je to dokonce kontradikce).

Zbývá ukázat, že formule ψ, která neobsahuje $\bullet$, není tautologie. Mohou nastat 2 případy: buď ψ obsahuje sudý počet negací, nebo lichý počet negací. Zjevně ψ obsahuje právě 1 výrokovou proměnnou, označme ji A. V případě, že ψ obsahuje sudý počet negací, uvažme valuaci v takovou, že $v(A) = 0$. Opětovným použitím $\xi \approx \neg\neg\xi$ pro libovolnou ξ dostáváme, že $v(\psi) = 0$, tedy ψ není tautologie. Podobně pro případ, kdy ψ obsahuje lichý počet negací (volíme valuaci t.ž. $v(A) = 1$).

□

Z Tvrzení 4.6 plyne, že výstupy P1 a P3 $\neg\bullet\neg\bullet\psi$ a $\neg\bullet\neg\psi$ jsou tautologie, tedy pravidla P1 a P2 jsou korektní.[4]

[4]Všimněte si, že v důkazu jsme vůbec nemuseli zkoumat tvar vstupů těchto pravidel.

Korektnost pravidla P3 vyplývá z toho, že $\xi \approx \neg\neg\xi$ pro libovolnou formuli ξ. ▲

Příklad 4.10 Uvažme odvozovací systém R z předchozího příkladu. Dokažte, že libovolná formule φ systému $\mathcal{L}(\neg, \bullet)$, která je tautologií, je v odvozovacím systému R dokazatelná.

Řešení Nechť ψ je libovolná tautologie systému $\mathcal{L}(\neg, \bullet)$. Z Tvrzení 4.6 plyne, že $\psi = \neg \ldots \neg \bullet \varphi$, kde počet výskytu symbolu $\neg$ před prvním výskytem $\bullet$ je roven $2n+1$ pro nějaké $n \in \mathbb{N}_0$. Uvažme důkaz $\xi_1, \ldots \xi_{n+1}$ formule ψ v systému R, kde $\xi_1 = \neg \bullet \varphi$ je instancí (A1), a pro libovolné $2 \leq i \leq n+1$ je $\xi_{i+1} = \neg\neg\xi_i$ formule vzniklá aplikací (P3) na ξ_i. ▲

✿✿ **Příklad 4.11** V této úloze se budeme zabývat systémem $\mathcal{L}(\rightarrow, \neg)$ výrokové logiky. Uvažujme následující schémata axiomů:

$$A_1\colon (\neg\neg\varphi \rightarrow \varphi),$$
$$A_2\colon \neg\varphi.$$

Dále pro libovolnou množinu $S \subseteq \{1, 2\}$ nechť D_S označuje odvozovací systém s pravidlem modus ponens, kde axiomy jsou právě ty formule, které jsou instancí schématu A_s pro aspoň jedno $s \in S$. (Tedy v systému $D_\emptyset$ nejsou žádné formule axiomy, v systému $D_{\{1\}}$ jsou axiomy právě instance schématu A_1 apod.) Odvozovací systém nazýváme *korektní*, právě když každá v něm dokazatelná formule je tautologie. Obráceně odvozovací systém nazveme *úplný*, právě když každá tautologie je v něm dokazatelná.

O každém ze systémů $D_\emptyset$, $D_{\{1\}}$, $D_{\{2\}}$, $D_{\{1,2\}}$ rozhodněte a dokažte, zda je korektní a zda je úplný.

Řešení V odvozovacím systému $D_\emptyset$ není žádná formule axiomem, takže žádná posloupnost (kladné délky) formulí není důkaz, a tedy žádná formule není dokazatelná. Takový odvozovací systém je tedy triviálně korektní, ale není úplný, neboť například tautologie $(A \rightarrow A)$ v něm není dokazatelná.

Podívejme se nyní na systém $D_{\{2\}}$. Jak uvidíme, v tomto odvozovacím systému jsou dokazatelné jen jeho axiomy, což (meta)dokážeme indukcí vzhledem k délce (formálního) důkazu: Dle definice důkazu může být jeho první formulí jedině axiom. Nyní předpokládejme, že máme důkaz sestávající pouze z instancí schématu A_2. Dle definice důkazu pak další formule bude opět axiomem nebo vznikne aplikací MP na formule již obsažené v důkazu. MP lze ale aplikovat jen v případě, že jedna z formulí začíná levou

závorkou, avšak všechny instance schématu A_2 začínají negací. V $D_{\{2\}}$ tak není dokazatelná například tautologie $(A \to A)$, takže $D_{\{2\}}$ není úplný. Na druhou stranu v $D_{\{2\}}$ je dokazatelná formule $\neg A$ (je totiž axiomem), která zřejmě není tautologie, takže tento odvozovací systém není ani korektní.

V systému $D_{\{1\}}$ je situace podobná — opět jsou dokazatelné jen jeho axiomy. Tentokrát ovšem bude zdůvodnění, proč nelze aplikovat MP, trochu obtížnější. Předpokládejme pro spor, že v nějakém důkazu vznikla některá formule aplikací pravidla MP na formule α, $(\alpha \to \beta)$ a uvažme první formuli, která takto vznikla (formule α, $(\alpha \to \beta)$ jsou tedy instancemi schématu A_1). Formule α je tedy tvaru $(\neg\neg\varphi \to \varphi)$, takže druhá z formulí je tvaru $((\neg\neg\varphi \to \varphi) \to \beta)$, což není možné, jelikož druhým znakem každé instance schématu A_1 je negace. Uvážíme-li navíc, že všechny axiomy tohoto odvozovacího systému jsou zřejmě tautologie, dostáváme, že je korektní. Není ovšem úplný, jelikož v něm není dokazatelná například tautologie $(A \to A)$.

Konečně v odvozovacím systému $D_{\{1,2\}}$ je každá formule ξ dokazatelná: $(\neg\neg\xi, (\neg\neg\xi \to \xi), \xi)$ je zřejmě její důkaz (instance A_2 pro $\varphi = \neg\xi$, instance A_1 pro $\varphi = \xi$, aplikace MP na předchozí dvě). Takový odvozovací systém je tedy triviálně úplný, ale není korektní, neboť například formule A je dokazatelná, ale není tautologie. ▲

Kapitola 5

Syntax predikátové logiky

Predikátová logika je rozšířením výrokové logiky. V predikátové logice proměnné nemusí nabývat pouze hodnot *pravda*/*nepravda*, ale mohou nabývat hodnot z libovolného předem určeného *univerza*. Dále predikátová logika umožňuje vyjadřovat se o vztazích mezi prvky tohoto univerza pomocí tzv. *predikátů*.

Pro definici syntaxe predikátové logiky nejprve definujeme *jazyk*.

Definice 5.1 Jazyk (stejně jako jazyk s rovností) je systém predikátových symbolů a funkčních symbolů, kde u každého symbolu je dána jeho četnost (arita), která je nezáporným celým číslem.

Predikátové symboly arity nula v jistém smyslu odpovídají konstantám True a False, funkční symboly arity nula jsou symboly pro konstanty. Predikátovým a funkčním symbolům se také říká *mimologické symboly*. Jazyk je tedy plně určen mimologickými symboly. Rozdíl mezi jazykem a jazykem s rovností se projeví v tom, že do predikátové logiky pro jazyk s rovností přidáme speciální logický symbol $=$, jehož sémantika bude definována speciálním způsobem.

Pro lepší pochopení budeme definice ilustrovat na příkladu z algebry. Víme že pologrupa je dvojice $(M, \cdot)$, kde

- M je nosná množina,
- $\cdot : M \times M \to M$ a
- $\cdot$ je asociativní (tedy pro každé k, l, m z M platí $(k \cdot l) \cdot m = k \cdot (l \cdot m)$).

Jazyk teorie pologrup tedy bude jazykem s rovností obsahující jeden funkční symbol $\cdot$ arity 2.

Definice 5.2 Abecedu predikátové logiky pro jazyk $\mathcal{L}$ tvoří následující symboly:

- Znaky pro proměnné $x, y, z, \ldots$, kterých je spočetně mnoho.
- Mimologické symboly, tj. predikátové a funkční symboly jazyka $\mathcal{L}$.
- Je-li $\mathcal{L}$ jazyk s rovností, obsahuje abeceda speciální znak $=$ pro rovnost.
- Logické spojky $\rightarrow$ a $\neg$.
- Symbol $\forall$ pro univerzální kvantifikátor.
- Závorky (a).

Definice 5.3 Termem jazyka $\mathcal{L}$ je slovo t nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $t_1, \cdots, t_k$, kde $k \geq 1$, t_k je t, a pro každé $1 \leq i \leq k$ má slovo t_i jeden z následujících tvarů:

- proměnná,
- $f(t_{i_1}, \cdots, t_{i_n})$, kde $1 \leq i_1, \cdots, i_n < k$, f je funkční symbol jazyka $\mathcal{L}$, a n je arita f.

Poznámka 5.4 U binárních funkčních symbolů (a později také predikátů) dovolíme pro větší čitelnost infixový zápis. U funkčních (a predikátových) symbolů arity nula budeme psát c místo $c()$.

Pro term $(x \cdot y) \cdot z$ jazyka pologrup $\{\cdot\}$ existuje například následující vytvořující posloupnost $x, y, z, (x \cdot y), (x \cdot y) \cdot z$. Posloupnost není určena jednoznačně a term $(x \cdot y) \cdot z$ má nekonečně mnoho jiných vytvořujících posloupností. Dále si všimneme, že term musí mít konečnou délku (vzhledem k počtu znaků), protože má konečnou vytvořující posloupnost a každým krokem ve vytvořující posloupnosti přidáme maximálně konečně mnoho znaků.

Definice 5.5 Term je uzavřený, jestliže neobsahuje proměnné.

Uzavřený term musí tedy obsahovat minimálně jeden funkční symbol arity 0.

Příklad 5.1 Mějme jazyk s rovností $\{f, g, h, i\}$, kde všechny symboly jsou funkční. Určete které z následujících termů jsou uzavřené:

- $f(g, h)$,
- $f(g, h(g, f))$,
- $f(g, f(h, i))$.

Řešení

- ano, term neobsahuje proměnné a f má aritu 2 a g, h mají aritu 0,
- ne, není to term, protože funkční symbol f by musel mít současně aritu 0 a 2,
- ano, term neobsahuje proměnné a f má aritu 2 a g, h, i mají aritu 0.

▲

Definice 5.6 Formule predikátového počtu jazyka $\mathcal{L}$ je slovo φ nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $\psi_1, \cdots, \psi_k$, kde $k \geq 1$, ψ_k je φ, a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů:

- $P(t_1, \cdots, t_n)$, kde P je predikátový symbol jazyka $\mathcal{L}$ arity n a $t_1, \cdots, t_n$ jsou termy jazyka $\mathcal{L}$.
- $t_1 = t_2$, je-li $\mathcal{L}$ jazyk s rovností a t_1, t_2 jsou termy jazyka $\mathcal{L}$.
- $\neg\psi_j$ pro nějaké $1 \leq j < i$,
- $(\psi_j \to \psi_{j'})$ pro nějaká $1 \leq j, j' < i$,
- $\forall x\, \psi_j$, kde x je proměnná a $1 \leq j < i$.

Pro formuli $\varphi = \forall x \forall y \forall z\, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ jazyka pologrup $\{\cdot\}$ existuje například následující vytvořující posloupnost $(x \cdot y) \cdot z, x \cdot (y \cdot z), (x \cdot y) \cdot z = x \cdot (y \cdot z), \forall z\, (x \cdot y) \cdot z = x \cdot (y \cdot z), \forall y \forall z\, (x \cdot y) \cdot z = x \cdot (y \cdot z), \varphi$.

Poznámka 5.7 Ve zbytku textu budeme používat následující „zkratky“:

- $\exists x\, \varphi$ značí $\neg\forall x\, \neg\varphi$
- $\varphi \vee \psi$ značí $\neg\varphi \to \psi$
- $\varphi \wedge \psi$ značí $\neg(\varphi \to \neg\psi)$.
- $\varphi \leftrightarrow \psi$ značí $(\varphi \to \psi) \wedge (\psi \to \varphi)$, kde symbol $\wedge$ dále „rozvineme“ podle předchozího bodu.

I pro predikátovou logiku lze využít techniku indukce vzhledem k délce vytvořující posloupnosti. Když budeme dokazovat složitější tvrzení tvaru „pro každou formuli predikátového počtu pro jazyka $\mathcal{L}$ platí...“, je někdy nutné využít strukturální indukci dvakrát: pro pomocné tvrzení o termech

(zde vedeme důkaz indukcí vzhledem ke struktuře termu) a pro tvrzení o formulích. Tento postup bude použit například v příkladu 7.2. Zde uvedeme jen jednoduchý příklad, nejprve ale zaveďme a procvičme další pojmy, které budeme potřebovat.

Definice 5.8 Každý výskyt proměnné ve formuli predikátového počtu je buď volný nebo vázaný podle následujícího induktivního předpisu:

- Ve formuli tvaru $P(t_1, \cdots, t_n)$ jsou všechny výskyty proměnných volné.
- Výrokové spojky nemění charakter výskytů proměnných, tj. je-li daný výskyt proměnné ve formuli ψ volný (resp. vázaný), je odpovídající výskyt ve formulích $\neg\psi$, $\varphi \to \psi$, $\psi \to \varphi$ rovněž volný (resp. vázaný).
- Ve formuli $\forall x\, \psi$ je každý výskyt proměnné x (včetně výskytu za kvantifikátorem) vázaný; byl-li výskyt proměnné různé od x volný (resp. vázaný) ve formuli ψ, je odpovídající výskyt ve formuli $\forall x\, \psi$ rovněž volný (resp. vázaný).

Definice 5.9

- Proměnná se nazývá volnou (resp. vázanou) ve formuli, má-li v ní volný (resp. vázaný) výskyt.
- Formule je otevřená, jestliže v ní žádná proměnná nemá vázaný výskyt.
- Formule je uzavřená (také sentence), jestliže v ní žádná proměnná nemá volný výskyt.
- Zápis $\varphi(x_1, \cdots, x_n)$ značí, že všechny volné proměnné ve formuli φ jsou mezi $x_1, \cdots, x_n$ (nemusí nutně platit, že každá z těchto proměnných je volná ve φ).
- Univerzální uzávěr formule φ je formule tvaru $\forall x_1 \cdots \forall x_n\, \varphi$, kde proměnné $x_1, \cdots, x_n$ jsou právě všechny volné proměnné formule φ.

Všimneme si, že proměnná může být ve formuli současne volná i vázaná, např. proměnná x ve formuli $P(x) \to \forall x P(x)$.

Příklad 5.2 Napište univerzální uzávěr pro následující formule:

- $P(x) \to \exists x\, (x = y \wedge P(z))$,
- $\forall x\, (P(x) = Q(y)) \to x \wedge \exists y\, (Q(y, z))$.

Řešení Vyřešíme první bod, druhý se vyřeší podobně. Jednoduše identifikujeme všechny proměnné, které mají v zadané formuli volný výskyt. Jsou to proměnná x v podformuli $P(x)$ a proměnné y, z v podformuli $\exists x\ (x = y \wedge P(z))$. Teď už jen stačí přidat univerzální kvantifikátory před zadanou formuli. Výsledek je tedy: $\forall x \forall y \forall z (P(x) \to \exists x\ (x = y \wedge P(z)))$. ▲

Teď už následuje slíbená aplikace strukturální indukce.

Příklad 5.3 Nechť máme jazyk s rovností $\mathcal{L} = \{P, f\}$, kde P je binární predikátový symbol a f je ternární funkční symbol. Dokažte, že pro každou otevřenou formuli jazyka $\mathcal{L}$ platí, že obsahuje sudý počet výskytů proměnných.

Řešení Nejdřív dokážeme pomocné tvrzení.

Tvrzení 5.10 Nechť máme výše definovaný jazyk $\mathcal{L}$. Každý term tohoto jazyka obsahuje lichý počet výskytů proměnných.

Důkaz Tvrzení dokážeme pro libovolný term t jazyka $\mathcal{L}$ pomocí strukturální indukce.

Báze. Pokud $t = x$, kde x je proměnná, pak t obsahuje jeden výskyt proměnné a tvrzení platí.

Indukční krok. Předpokládejme, že tvrzení platí pro nějaké termy t_1, t_2 a t_3, tedy obsahují p_1, p_2 a p_3 výskytů proměnných, kde p_1, p_2 a p_3 jsou lichá čísla. Term $f(t_1, t_2, t_3)$ obsahuje $p_1 + p_2 + p_3$ výskytů proměnných, což je zřejmě liché číslo.

Teď dokážeme tvrzení ze zadání příkladu.

Důkaz Tvrzení dokážeme pro libovolnou otevřenou formuli φ jazyka $\mathcal{L}$ pomocí strukturální indukce.

Báze. Nechť je formule φ tvaru $P(t_1, t_2)$ nebo $t_1 = t_2$, kde t_1 a t_2 mají p_1 a p_2 výskytů proměnných. Z předchozího tvrzení víme, že libovolný term obsahuje lichý počet výskytů proměnných. Zřejmě φ obsahuje $p_1 + p_2$ výskytů proměnných, což je sudé číslo.

Indukční krok. Předpokládejme, že tvrzení platí pro nějaké formule φ_1 a φ_2, tedy obsahují p_1 a p_2 výskytů proměnných a obě jsou to sudá čísla. Pokud je φ tvaru $\neg\varphi_1$ tak obsahuje p_1 výskytů proměnných, což je sudé číslo. Pokud je φ tvaru $\varphi_1 \to \varphi_2$, tak obsahuje $p_1 + p_2$ výskytů proměnných, což je sudé číslo. Formule tvaru $\forall x \varphi$ nemusíme uvažovat, protože taková formule obsahuje vázaný výskyt proměnné x přímo za kvantifikátorem, tedy není otevřená.

▲

Definice 5.11 Term t je substituovatelný za proměnnou x ve formuli φ, jestliže žádný výskyt proměnné v termu t se nestane vázaným po provedení substituce termu t za každý *volný* výskyt proměnné x ve formuli φ. Je-li t substituovatelný za x ve φ, značí zápis $\varphi(x/t)$ formuli, která vznikne nahrazením každého volného výskytu x ve φ termem t.

Příklad 5.4 Mějme jazyk $\mathcal{L} = \{P, Q\}$ s rovností, kde P i Q jsou unární predikátové symboly. Pro každou z následujících formulí rozhodněte, zda je term $f(y)$ substituovatelný za x, a pokud ano, proveďte substituci a zapište výslednou formuli.

- $\forall y \forall x x = y$,
- $\forall x(P(x) \to P(y)) \to Q(x) \wedge \exists y Q(y)$,
- $\forall y(P(x) \to \forall x P(x)) \to z = y$.

Řešení V první formuli není žádný volný výskyt proměnné x, tedy zadaný term je substituovatelný a výsledná formule je $\forall y \forall x P(x) = P(y)$. V druhé formuli bodě je term daný term opět substituovatelny, výsledná formule je $\forall x(P(x) \to P(y)) \to f(y) \wedge \exists y Q(y)$. V posledním bodě není term $Q(f(y))$ substituovatelný za x protože v podformuli $\forall y(P(x) \to \forall x P(x))$ se nachází volný výskyt x, ale y by se v této podformuli stála vázanou. ▲

Definice 5.12 Nechť φ je formule a $t_1, \cdots, t_n$ termy, které jsou v uvedeném pořadí substituovatelné za proměnné $x_1, \cdots, x_n$ ve φ (předpokládáme, že $x_1, \cdots, x_n$ jsou různé). Symbol $\varphi(x_1/t_1, \cdots, x_n/t_n)$ značí formuli, která vznikne „simultánním nahrazením“ každého volného výskytu x_i termem t_i pro každé $1 \leq i \leq n$. Přesněji, $\varphi(x_1/t_1, \cdots, x_n/t_n)$ je formule

$$\varphi(x_1/z_1) \cdots (x_n/z_n)(z_1/t_1) \cdots (z_n/t_n),$$

kde $z_1, \cdots, z_n$ jsou (různé) proměnné, které se nevyskytují v $t_1, \cdots, t_n$ ani mezi $x_1, \cdots, x_n$.

Rozdíl mezi simultánním a postupným nahrazením ilustrujeme na příkladě. Formule $P(x, y)(x/y, y/x)$ je po aplikování simultánního nahrazení $P(y, x)$, zatímco formule $P(x, y)(x/y)(y/x)$ je po aplikování prvního nahrazení $P(y, y)(y/x)$ a po aplikování druhého nahrazení $P(x, x)$. Simultánní nahrazení se používá při důkazu věty o úplnosti pro predikátovou logiku

(konkrétně ve větě o konstantách), který ale v cvičebnici neuvádíme. Definice simultánního nahrazení je zde kvůli konzistenci s přednáškou a na procvičení tohoto pojmu.

Příklad 5.5 Uvažme formuli $\varphi = \forall y((P(x) \to \exists z P(y)) \wedge P(z)) \to (P(y) \leftrightarrow P(z))$. Zapište formule $\varphi(y/x)(x/z)$ a $\varphi(y/x, x/z)$.

Kapitola 6

Sémantika predikátové logiky I

Sémantika predikátové logiky se silně opírá o pojem realizace jazyka. Abychom uměli říct, zda je nějaká formule pravdivá, musíme vědět, jakých hodnot mohou nabývat proměnné a jaký význam mají predikátové a funkční symboly.

Definice 6.1 Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je zadána

- *neprázdným* souborem M, nazývaným univerzum (případně nosič). Prvky univerza nazýváme individui.
- Přiřazením, které každému n-árnímu predikátovému symbolu P přiřadí n-ární relaci $P_{\mathcal{M}}$ na souboru M,
- přiřazením, které každému m-árnímu funkčnímu symbolu přiřadí funkci $f_{\mathcal{M}} : M^m \to M$.

Ohodnocení je zobrazení přiřazující proměnným prvky univerza M.

Realizace je vlastně svět, ve kterém se budeme pohybovat. Univerzum je to, z čeho se svět skládá. Prvky univerza mohou být úplně libovolné, napr. přirozená čísla, ovoce, auta,... Definování funkcí a relací nám zase určuje jaké zákonitosti platí mezi jednotlivými prvky univerza. To že n-ární predikátový symbol je definovaný jako n-ární relace koresponduje s tím, že predikátové symboly zadávají vlastnosti systému. Danou vlastnost splňují jenom ty n-tice univerza, které se nachází v relaci (tedy v množině n-tic). Následujícími dvěma definicemi zavedeme pojem pravdivosti formule v realizaci.

Definice 6.2 Realizace termu t při ohodnocení e v realizaci $\mathcal{M}$, psáno $t^{\mathcal{M}}[e]$ (případně jen $t[e]$, je-li $\mathcal{M}$ jasné z kontextu), definujeme induktivně takto:

- $x[e] = e(x)$
- $f(t_1, \cdots, t_m)[e] = f_{\mathcal{M}}(t_1[e], \cdots, t_m[e])$
  (pro $m = 0$ je na pravé straně uvedené definující rovnosti $f_{\mathcal{M}}(\emptyset)$).

Tedy v případě fixované realizace nám každý term představuje nějaký prvek univerza. Teď už máme v rukách vše potřebné pro zadefinování pravdivosti formule.

Definice 6.3 (A. Tarski) Buď $\mathcal{M}$ realizace $\mathcal{L}$, e ohodnocení a φ formule predikátového počtu jazyka $\mathcal{L}$. Ternární vztah $\mathcal{M} \models \varphi[e]$ definujeme indukcí ke struktuře φ takto:

- $\mathcal{M} \models P(t_1, \cdots, t_m)[e]$ právě když $(t_1[e], \cdots, t_m[e]) \in P_{\mathcal{M}}$.
- Jestliže $\mathcal{L}$ je jazyk s rovností, pak $\mathcal{M} \models (t_1 = t_2)[e]$ právě když $t_1[e]$ a $t_2[e]$ jsou stejná individua.
- $\mathcal{M} \models \neg\psi[e]$ právě když neplatí $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models (\psi \to \xi)[e]$ právě když $\mathcal{M} \models \xi[e]$ nebo neplatí $\mathcal{M} \models \psi[e]$.
- $\mathcal{M} \models \forall x\, \psi[e]$ právě když $\mathcal{M} \models \psi[e(x/a)]$ pro každý prvek a univerza M, kde ohodnocení $e(x/a)$ je takové, že proměnné x přiřadí prvek a a každé jiné proměnné y přiřadí hodnotu $e(y)$.

Jestliže $\mathcal{M} \models \varphi[e]$, říkáme, že φ je pravdivá v $\mathcal{M}$ při ohodnocení e. Jestliže $\mathcal{M} \models \varphi[e]$ pro každé e, je φ pravdivá v $\mathcal{M}$, psáno $\mathcal{M} \models \varphi$.

Jediný složitější bod v Tarského definici je definice pravdivosti formule tvaru $\forall x\, \psi[e]$. Zde musíme zaručit, že formule φ je pravdivá pro libovolný prvek univerza, který můžeme nahradit za každý výskyt proměnné x, který je vázaný uvedeným prvním výskytem kvantifikátoru $\forall$.

Teď procvičíme definice na jednoduchých příkladech.

✡ **Příklad 6.1** Mějme jazyk $\mathcal{L} = \{P\}$ bez rovnosti, kde P je unární predikátový symbol. Znegujte formuli

$$\varphi \equiv \forall x\, \exists y\, (P(x) \to \neg P(y)).$$

Tedy najděte formuli ψ *ekvivaletní* formuli $\neg\varphi$ takovou, že ψ obsahuje negaci pouze na úrovni predikátových symbolů (podobně jako formule φ). Uzavřené formule ξ, ξ' jazyka $\mathcal{L}$ nazýváme *ekvivalentní*, pokud pro každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí $\mathcal{M} \models \xi$, právě když $\mathcal{M} \models \xi'$.

Řešení $\exists x \forall y (P(x) \wedge P(y))$. ▲

✡✡✡ **Příklad 6.2** Mějme jazyk $\mathcal{L} = \{\cdot\}$ s rovností, kde $\cdot$ je binární funkční symbol. Dejte příklad *uzavřené* formule φ predikátového počtu jazyka $\mathcal{L}$ takové, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí $\mathcal{M} \models \varphi$ právě tehdy, když

a) $(M, \cdot_{\mathcal{M}})$ je pologrupa
b) $(M, \cdot_{\mathcal{M}})$ je monoid
c) $(M, \cdot_{\mathcal{M}})$ je grupa

Řešení

a) V předchozí kapitole jsme uvedli, že binární funkce musí splňovat asociativitu. Tedy formulí φ musíme vynutit, aby pro libovolné tři prvky $x, y, z \in M$ platilo, že $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Tedy výsledn8 formule zajišťující vlastnosti pologrupy je $\varphi_1 = \forall x \forall y \forall z \, (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$.
b) Podobně jako pro předchozí bod si zjistíme definici monoidu. Kromě asociativity musí ještě existovat jednotkový prvek. Formule na vynucení jednotkového prvku je $\exists x \forall y (x \cdot y = x \wedge y \cdot x = x)$. Musíme si uvědomit, že asociativita a existence jednotkového prvku musí platit současně, tedy mezi naše vytvořené formule musíme dát konjunkci. Výsledná formule je tedy $\varphi_2 = \varphi_1 \wedge \exists x \forall y (x \cdot y = x \wedge y \cdot x = x)$.
c) Okrem asociativity a existence jednotkového prvku x musíme zaručit existenci inverzního prvku pro každé $y \in M$. Pokud bychom věděli, že proměnná x se realizuje jako jednotkový prvek, mohli bychom použít formuli $\forall y \exists z (y \cdot z = k \wedge z \cdot y = k)$. To, že x se realizuje jako jednotkový prvek musíme vynutit vhodným rozšířením naší formule. Výslednou formuli pro vynucení existence inverzního prvku složíme ze dvou částí:
   - formule pro existenci jednotkového prvku,
   - formule pro existenci inverzního prvku za předpokladu, že x je jednotkový prvek.

   Proto výsledná formule pro existenci inverzního prvku je

   $$\varphi_2 = \exists x (\forall y (x \cdot y = x \wedge y \cdot x = x) \wedge \forall y \exists z (y \cdot z = x \wedge z \cdot y = x)).$$

   Všimneme si, že existenční kvantifikátor musí být před celou složenou formulí, aby se x vskutku v celé formuli realizovalo jako jednotkový prvek.
   Tedy výsledná formule zajišťující všechny vlastnosti grupy je $\varphi_1 \wedge \varphi_2$.

▲

✡✡✡ **Příklad 6.3** Mějme jazyk $\mathcal{L} = \{\sim\}$ s rovností, kde $\sim$ je binární predikátový symbol. Dejte příklad *uzavřené* formule φ predikátového počtu jazyka $\mathcal{L}$ takové, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí $\mathcal{M} \models \varphi$ právě tehdy, když

a) $\sim_{\mathcal{M}}$ je relace ekvivalence na M
b) $\sim_{\mathcal{M}}$ je relace uspořádání na M

Řešení

a) $\forall x(x \sim x) \wedge \forall x \forall y \forall z((x \sim y \wedge y \sim z \to x \sim z) \wedge \forall x \forall y(x \sim y \to y \sim x)$
b) $\forall x(x \sim x) \wedge \forall x \forall y \forall z((x \sim y \wedge y \sim z \to x \sim z) \wedge \forall x \forall y((x \sim y \wedge y \sim x) \to x = y)$

▲

✡✡✡ **Příklad 6.4** Mějme jazyk $\mathcal{L} = \{<\}$ s rovností, kde $<$ je binární predikátový symbol. Uvažme tři realizace $\mathcal{N}, \mathcal{Z}, \mathcal{Q}$ jazyka $\mathcal{L}$ s nosiči $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ (množiny přirozených, celých a racionálních čísel), které interpretují symbol $<$ jako standardní *ostré* uspořádání na příslušné množině čísel. Dejte příklad uzavřené formule φ predikátového počtu jazyka $\mathcal{L}$ takové, že

a) $\mathcal{N} \models \varphi, \mathcal{Z} \not\models \varphi, \mathcal{Q} \not\models \varphi$,

b) $\mathcal{N} \not\models \varphi, \mathcal{Z} \models \varphi, \mathcal{Q} \not\models \varphi$,

c) $\mathcal{N} \not\models \varphi, \mathcal{Z} \not\models \varphi, \mathcal{Q} \models \varphi$.

Řešení

a) $\varphi \equiv \exists x \forall y(x = y \vee x < y)$ (tedy existuje nejmenší prvek),

b) $\varphi \equiv \forall x \exists y(y < x \wedge \forall z(z < y \vee x < z \vee z = y \vee z = x))$ (neexistuje nejmenší prvek, a zároveň ke každému prvku existuje prvek bezprostředně menší- mezi tyto dva už není možné zařadit další prvek),

c) $\varphi \equiv \forall x \forall y(x < y \to \exists z(x < z \wedge z < y))$ (mezi každé dva prvky lze zařadit další). [1]

▲

✪✪✩ **Příklad 6.5** Mějme jazyk $\mathcal{L} = \{\cdot\}$ s rovností, kde $\cdot$ je binární funkční symbol. Uvažme tři realizace $\mathcal{Z}, \mathcal{Q}, \mathcal{R}$ s nosiči $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (množiny celých, racionálních a reálných čísel), které intepretují symbol $\cdot$ jako standardní násobení čísel. Dejte příklad uzavřené formule φ predikátového počtu jazyka $\mathcal{L}$ takové, že

$$\mathcal{Q} \not\models \varphi, \mathcal{R} \models \varphi.$$

✪✪✪ **Příklad 6.6** Nechť $\mathcal{L} = \{+, *\}$ je jazyk s rovností, kde $+$ a $*$ jsou binární funkční symboly. Dále nechť $\mathcal{M}$ je realizace tohoto jazyka, kde univerzum je množina přirozených čísel s nulou a $+_{\mathcal{M}}$ a $*_{\mathcal{M}}$ jsou standardní operace sčítání a násobení. Zadejte formuli $\varphi(x, y)$ se dvěma volnými proměnnými x a y takovou, že pro libovolné ohodnocení e platí

$$\mathcal{M} \models \varphi[e],$$

právě když $e(x) \cdot e(y)$ je dělitelné druhou mocninou nějakého prvočísla.

✪✪✩ **Příklad 6.7** Nechť $\mathcal{L}$ je jazyk s rovností a se dvěma binárními funkčními symboly $+$ a $*$. Dále nechť $R = (\mathbb{R}_{\geq 0}, +_{\mathbb{R}_{\geq 0}}, *_{\mathbb{R}_{\geq 0}})$ a $Q = (\mathbb{Q}_{\geq 0}, +_{\mathbb{Q}_{\geq 0}}, *_{\mathbb{Q}_{\geq 0}})$ jsou dvě realizace tohoto jazyka, které mají za nosič nezáporná reálná, resp. nezáporná racionální čísla a kde funkční symboly $+$ a $*$ jsou realizovány standardní operací sčítání a násobení na příslušných množinách. Zadejte formuli φ v jazyce $\mathcal{L}$ takovou, že $R \models \varphi$ a $Q \not\models \varphi$.

✪✪✩ **Příklad 6.8** Nechť $\mathcal{L}$ je jazyk s rovností a dvěma binárními funkčními symboly $+$ a $*$. Označme $R = (\mathbb{R}, +_R, *_R)$ realizaci tohoto jazyka s reálnými čísly jako nosičem, kde operace $+$ a $*$ jsou realizovány standardními operacemi sčítání a násobení na množině reálných čísel. Zadejte formule φ_1, φ_2 a φ_3 s volnou proměnnou x, příp. y takové, že pro libovolné ohodnocení e platí:

a) $R \models \varphi_1(x)[e]$, právě když $e(x) = 0$

b) $R \models \varphi_2(x)[e]$, právě když $0 \leq e(x)$

c) $R \models \varphi_3(x, y)[e]$, právě když $e(x) \leq e(y)$

kde $\leq$ je standardní uspořádání reálných čísel.

✪✪✩ **Příklad 6.9** Mějme jazyk $\mathcal{L} = \{f, \leq, D\}$ s rovností, kde f je unární funkční symbol, $\leq$ je binární predikátový symbol a D je binární funkční symbol.

[1] také lze použít formuli $\neg\psi_1 \wedge \neg\psi_2$ kde ψ_1 je formule z 1. a ψ_2 je formule z 2.

Mějme realizaci $\mathcal{M}$, jejímž nosičem jsou reálná čísla, $f_{\mathcal{M}}$ je libovolná funkce nad reálnými čísly, $\leq_{\mathcal{M}}$ je standardní uspořádání a $D_{\mathcal{M}}$ přiřadí dvěma reálným číslům jejich rozdíl v absolutní hodnotě, tedy $D_{\mathcal{M}}(a, b) = |a - b|$.

Zadejte formuli φ v jazyku $\mathcal{L}$ s volnou proměnnou l tak, že pro libovolné ohodnocení e platí

$$\mathcal{M} \models \varphi[e] \qquad \text{právě když} \qquad e(l) = \lim_{x \to \infty} f_{\mathcal{M}}(x)$$

Pro připomenutí: Říkáme, že $l \in \mathbb{R}$ je limita funkce f v nekonečnu, pokud pro libovolné kladné ε existuje kladné A takové, že pro všechna $x > A$ platí $|g(x) - l| < \varepsilon$.

✪✪✩ **Příklad 6.10** Mějme jazyk $\mathcal{L} = \{P\}$ s rovností, kde P je binární predikátový symbol. Dále mějme formule

$$\varphi \equiv \forall x\, \exists y\, \exists z\, (\neg(y = z) \wedge P(x, y) \wedge P(x, z))$$

$$\psi \equiv \exists x\, \forall y\, \forall z\, ((P(y, x) \wedge P(z, x)) \to y = z)$$

Zadejte realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takovou, že

- $\mathcal{M} \models \varphi$ a zároveň $\mathcal{M} \not\models \psi$,
- $\mathcal{M} \models \varphi$ a zároveň $\mathcal{M} \models \psi$.

Řešení

- $(\{a, b\}, P_{\mathcal{M}} = \{(x, y) \mid x, y \in M\})$,
- $(\{a, b, c\}, P_{\mathcal{M}} = \{(a, a), (a, b), (b, a), (b, c), (c, a), (c, b)\})$.

▲

✪✩✩ **Příklad 6.11** Mějme jazyk $\mathcal{L} = \{S, N\}$ s rovností, kde S a N jsou binární funkční symboly. Mějme realizaci $\mathcal{M}$, jejíž nosič je množina $\mathbb{N}$ (přirozená čísla bez nuly), $S_{\mathcal{M}}$ je standardní sčítání na množině $\mathbb{N}$ a $N_{\mathcal{M}}$ je standardní násobení na množině $\mathbb{N}$.

Zadejte formuli φ v jazyku $\mathcal{L}$ s volnou proměnnou x tak, že pro libovolné ohodnocení e platí

$$\mathcal{M} \models \varphi[e] \qquad \text{právě když} \qquad e(x) \text{ je prvočíslo.}$$

Pro připomenutí: Říkáme, že přirozené číslo x je prvočíslo, pokud je dělitelné právě *dvěma* čísly: x a 1.

✡✡✡ **Příklad 6.12** Mějme jazyk $\mathcal{L} = \{S, N\}$ s rovností, kde S a N jsou binární funkční symboly. Mějme realizaci $\mathcal{M}$, jejíž nosič je množina $\mathbb{N}$ (přirozená čísla bez nuly), $S_\mathcal{M}$ je standardní sčítání na množině $\mathbb{N}$ a $N_\mathcal{M}$ je standardní násobení na množině $\mathbb{N}$.

Zadejte formuli φ v jazyku $\mathcal{L}$ s volnou proměnnou x tak, že pro libovolné ohodnocení e platí

$$\mathcal{M} \models \varphi[e] \qquad \text{právě když} \qquad e(x) \text{ je násobek čísla 3.}$$

✡✡✡ **Příklad 6.13** Mějme jazyk $\mathcal{L} = \{f, \leq, D\}$ s rovností, kde f je unární funkční symbol, $\leq$ je binární predikátový symbol a D je binární funkční symbol. Mějme realizaci $\mathcal{M}$, jejíž nosič jsou reálná čísla, $f_\mathcal{M}$ je libovolná funkce nad reálnými čísly, $\leq_\mathcal{M}$ je standardní uspořádání a $D_\mathcal{M}$ přiřadí dvěma reálným číslům jejich rozdíl v absolutní hodnotě, tedy $D_\mathcal{M}(a, b) = |a - b|$.

Zadejte formuli φ v jazyce $\mathcal{L}$ takovou, že

$$\mathcal{M} \models \varphi \qquad \text{právě když} \qquad f_\mathcal{M} \text{ je spojitá funkce}$$

Pro připomenutí: Reálná funkce je *spojitá*, pokud je spojitá v každém bodě $x \in \mathbb{R}$. Reálná funkce f je *spojitá v bodě* $c \in \mathbb{R}$, pokud $\lim_{x \to c} f(x) = f(c)$, tedy pokud pro každé $\epsilon > 0$ existuje $\delta > 0$ takové, že pro libovolný bod x, který splňuje $|x - c| < \delta$, platí $|f(x) - f(c)| < \epsilon$.

✡✡✡ **Příklad 6.14** Mějme jazyk $\mathcal{L} = \{\ominus\}$ s rovností, kde $\ominus$ je binární funkční symbol. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je $2^\mathbb{N}$ (tj. množina všech podmnožin přirozených čísel) a kde $\ominus_\mathcal{M}$ je množinový rozdíl. Zadejte formuli φ v jazyce $\mathcal{L}$ s jednou volnou proměnnou x takovou, že pro libovolné ohodnocení e platí

$$\mathcal{M} \models \varphi[e] \qquad \text{právě když} \qquad e(x) \text{ je jednoprvková podmnožina množiny } \mathbb{N}.$$

Pro připomenutí uvádíme stručnou ilustraci chování operace $\ominus_\mathcal{M}$:
$\{5, 6\} \ominus_\mathcal{M} \{3, 5, 7\} = \{6\}$,
$\{1, 3\} \ominus_\mathcal{M} \{1, 2, 3\} = \emptyset$.

✡✡✡ **Příklad 6.15** Mějme jazyk $\mathcal{L} = \{+, *\}$ s rovností, kde $+$ a $*$ jsou binární funkční symboly. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je množina všech kladných celých čísel $\mathbb{Z}^{>0}$ a kde $+$ a $*$ se realizují jako standardní

sčítání, resp. násobení na této množině. Zadejte formuli φ jazyka $\mathcal{L}$ se dvěma volnými proměnnými x a y takovou, že pro libovolné ohodnocení e platí:

$$\mathcal{M} \models \varphi[e] \;\Leftrightarrow\; e(x) = \max\{k \mid k = 2^l \text{ pro nějaké } l \geq 0 \text{ a zároveň } k \leq e(y)\}.$$

(Tj. $e(x)$ musí být největší mocnina dvou menší nebo rovna $e(y)$.)

✿✿ **Příklad 6.16** Mějme jazyk $\mathcal{L} = \{+, N\}$ s rovností, kde $+$ je binární funkční symbol a N je unární predikátový symbol. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je množina $\mathbb{R}_{\geq 0}$ všech nezáporných reálných čísel, $+$ se realizuje jako standardní sčítání a $N_{\mathcal{M}}$ obsahuje právě všechna celá čísla obsažená v $\mathbb{R}_{\geq 0}$. Zadejte formuli φ jazyka $\mathcal{L}$ se dvěmi volnými proměnnými x a y takovou, že pro libovolné ohodnocení e platí:

$$\mathcal{M} \models \varphi[e] \quad \Leftrightarrow \quad e(x) = \lfloor e(y) \rfloor.$$

(Tj. $e(x)$ je celá část $e(y)$ – největší celé číslo menší nebo rovno $e(y)$.)

✿✿ **Příklad 6.17** Mějme jazyk $\mathcal{L} = \{+, *\}$ s rovností, kde $+$ a $*$ jsou binární funkční symboly. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je množina $\mathbb{N}_0$ všech přirozených čísel s nulou, $+$ se realizuje jako standardní sčítání a $*$ se realizuje jako standardní násobení. Zadejte formuli φ jazyka $\mathcal{L}$ se třemi volnými proměnnými x, y a z takovou, že pro libovolné ohodnocení e platí:

$$\mathcal{M} \models \varphi[e] \quad \Leftrightarrow e(z) \neq 0 \text{ a } e(x) \text{ je zbytek po dělení čísla } e(y) \text{ číslem } e(z)\ .$$

Neformálně popište význam formule.

✿✿ **Příklad 6.18** Mějme jazyk $\mathcal{L} = \{\leq\}$ s rovností, kde $\leq$ je binární predikátový symbol. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je množina $2^{\mathbb{N}}$ všech podmnožin přirozených čísel a kde $\leq_{\mathcal{M}}$ je standardní množinová inkluze. Zadejte formuli φ jazyka $\mathcal{L}$ se dvěma volnými proměnnými x a y takovou, že pro libovolné ohodnocení e platí:

$$\mathcal{M} \models \varphi[e] \quad \Leftrightarrow \quad \text{množiny } e(x) \text{ a } e(y) \text{ mají neprázdný průnik.}$$

Neformálně popište význam své formule.

✿✿ **Příklad 6.19** Mějme jazyk $\mathcal{L} = \{+, *\}$ s rovností, kde $+$ a $*$ jsou binární funkční symboly. Mějme dále realizaci $\mathcal{M}$ jazyka $\mathcal{L}$, jejímž nosičem je množina $\mathbb{N}_0$ všech přirozených čísel s nulou, $+$ se realizuje jako standardní sčítání

a $*$ se realizuje jako standardní násobení. Zadejte formuli φ jazyka $\mathcal{L}$ se třemi volnými proměnnými x, y a z takovou, že pro libovolné ohodnocení e platí:

$\mathcal{M} \models \varphi[e] \quad \Leftrightarrow$ $e(x) \neq 0$ a $e(x)$ je největší společný dělitel čísel $e(y)$ a $e(z)$.

Neformálně popište význam své formule.

✪✪✩ **Příklad 6.20** Nechť φ je formule predikátového počtu jazyka $\mathcal{L}$ taková, že x je jediná volná proměnná ve φ. Rozhodněte, zda pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ a libovolnou proměnnou y substituovatelnou za x ve φ platí

a) $\mathcal{M} \models \varphi \to (\varphi(x/y))$,
b) $\mathcal{M} \models \varphi \to \exists y\, (\varphi(x/y))$.

Kapitola 7

Sémantika predikátové logiky II

V této kapitole uvedeme abstraktnější a také složitější příklady týkající se sémantiky predikátové logiky.

✪✪✩ **Příklad 7.1** Rozhodněte, zda platí následující tvrzení: Mějme nějaký jazyk $\mathcal{L}$, realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ a formuli φ predikátového počtu jazyka $\mathcal{L}$. Pak

$$\mathcal{M} \models \varphi \text{ právě tehdy, když } \mathcal{M} \not\models \neg\varphi$$

Řešení Implikace "zleva doprava"platí. Dokážeme tedy následující tvrzení:

Tvrzení 7.1 Jestliže $\mathcal{M} \models \varphi$, pak $\mathcal{M} \not\models \neg\varphi$.

Důkaz Předpokládejme, že $\mathcal{M} \models \varphi$. Pak (z definice) pro každé ohodnocení e platí $\mathcal{M} \models \varphi[e]$. Nosič $\mathcal{M}$ je neprázdný (z definice realizace) a tedy *existuje* alespoň jedno ohodnocení e takové, že $\mathcal{M} \models \varphi[e]$. Pak ale $\mathcal{M} \not\models \neg\varphi[e]$ a tedy $\mathcal{M} \not\models \neg\varphi$.

Implikace "zprava doleva"neplatí. Dokážeme tedy:

Tvrzení 7.2 Existují jazyk $\mathcal{L}$, realizace $\mathcal{M}$ jazyka $\mathcal{L}$ a formule φ predikátového počtu jazyka $\mathcal{L}$ takové, že $\mathcal{M} \not\models \varphi$ a zároveň $\mathcal{M} \not\models \neg\varphi$.

Důkaz Položme $\mathcal{L} = \{P\}$ kde P je unární predikátový symbol. Realizaci $\mathcal{M}$ definujeme následovně: nosič $M = \{a, b\}$ a $P_{\mathcal{M}} = \{a\}$ ($P_{\mathcal{M}}$ je unární relace). Konečně položme $\varphi = P(x)$.

Nyní nechť e je ohodnocení takové, že $e(x) = a$. Pak $\mathcal{M} \models P(x)[e]$, protože $e(x) = a \in P_{\mathcal{M}}$ a tedy $\mathcal{M} \not\models \neg P(x)[e]$. Z toho plyne, že $\mathcal{M} \not\models \neg P(x)$.

Dále nechť e je ohodnocení takové, že $e(x) = b$. Pak $\mathcal{M} \not\models P(x)[e]$ a tedy $\mathcal{M} \not\models P(x)$.

Celkem tedy $\mathcal{M} \not\models \neg P(x)$ a zároveň $\mathcal{M} \not\models P(x)$, což bylo dokázat.

▲

✩✩✩ **Příklad 7.2** Rozhodněte, zda platí následující tvrzení: Mějme jazyk $\mathcal{L}$, realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ a *uzavřenou* formuli φ predikátového počtu jazyka $\mathcal{L}$. Pak

$$\mathcal{M} \models \varphi \text{ právě tehdy, když } \mathcal{M} \not\models \neg\varphi$$

Řešení Tvrzení platí. Nejprve ovšem dokážeme následující pomocné tvrzení.

Tvrzení 7.3 Je-li t term jazyka $\mathcal{L}$ a e_1, e_2 jsou ohodnocení taková, že $e_1(x) = e_2(x)$ platí pro každou proměnnou x vyskytující se v t, pak $t[e_1] = t[e_2]$.

Důkaz Tvrzení dokážeme metaindukcí vzhledem k délce vytvořující posloupnosti pro t (t.j. strukturální indukcí).

- Je-li $t = x$ proměnná, pak

$$t[e_1] = x[e_1] = e_1(x) = e_2(x) = x[e_2] = t[e_2]$$

- Je li $t = f(t_1, \ldots, t_n)$ kde f je n-ární funkční symbol jazyka $\mathcal{L}$ a $t_1, \ldots, t_n$ jsou termy, pak

$$t[e_1] = f(t_1, \ldots, t_n)[e_1] = f_M(t_1[e_1], \ldots, t_n[e_1]) = \\ f_M(t_1[e_2], \ldots, t_n[e_2]) = f(t_1, \ldots, t_n)[e_2] = t[e_2],$$

  kde druhá rovnost plyne z indukčního předpokladu.

Nyní si uvědomme, že tvrzení tvaru „pro všechny uzavřené formule φ platí. . . “, nelze přímo dokázat strukturální indukcí, neboť uzavřené formule vznikají z neuzavřených přidáním kvantifikátorů. Tvrzení ze zadání příkladu je tudíž příliš slabé, protože neříká nic o neuzavřených formulích. Musíme tedy dokázat následující silnější tvrzení.

Tvrzení 7.4 Je-li φ formule predikátového počtu jazyka $\mathcal{L}$ a e_1, e_2 libovolná ohodnocení taková, že $e_1(x) = e_2(x)$ pro každou proměnnou x *volnou* ve φ, pak platí: $\mathcal{M} \models \varphi[e_1]$, právě tehdy když $\mathcal{M} \models \varphi[e_2]$.

Důkaz Tvrzení dokážeme metaindukcí vzhledem k délce vytvořující posloupnosti pro φ.

- Je-li $\varphi \equiv P(t_1, \ldots, t_n)$, kde P je n-ární predikátový symbol a $t_1, \ldots, t_n$ jsou termy, pak

$$\begin{aligned} \mathcal{M} \models \varphi[e_1] &\Leftrightarrow (t_1[e_1], \ldots, t_n[e_1]) \in P_{\mathcal{M}} \\ &\Leftrightarrow (t_1[e_2], \ldots, t_n[e_2]) \in P_{\mathcal{M}} \\ &\Leftrightarrow \mathcal{M} \models \varphi[e_2], \end{aligned}$$

  kde druhá ekvivalence plyne z Tvrzení 7.3 a z toho, že ve φ jsou všechny proměnné volné, tedy e_1 a e_2 se shodují na všech proměnných majících výskyt ve φ.

- Je-li $\mathcal{L}$ jazyk s rovností a $\varphi \equiv t_1 = t_2$, kde t_1,t_2 jsou termy, pak podobně jako v předchozím bodě máme

$$\begin{aligned} \mathcal{M} \models \varphi[e_1] &\Leftrightarrow t_1[e_1] = t_2[e_1] \\ &\Leftrightarrow t_1[e_2] = t_2[e_2] \\ &\Leftrightarrow \mathcal{M} \models \varphi[e_2], \end{aligned}$$

- Je-li $\varphi \equiv \neg\psi$, pak

$$\begin{aligned} \mathcal{M} \models \varphi[e_1] &\Leftrightarrow \mathcal{M} \not\models \psi[e_1] \\ &\Leftrightarrow \mathcal{M} \not\models \psi[e_2] \\ &\Leftrightarrow \mathcal{M} \models \varphi[e_2], \end{aligned}$$

  kde druhá ekvivalence plyne z indukčního předpokladu a z toho, že libovolná proměnná je volná v ψ tehdy a jen tehdy, když je volná ve φ.

- Je-li $\varphi \equiv \psi_1 \to \psi_2$, pak

$$\begin{aligned} \mathcal{M} \models \varphi[e_1] &\Leftrightarrow \text{buď } \mathcal{M} \models \psi_2[e_1] \text{ nebo } \mathcal{M} \not\models \psi_1[e_1] \\ &\Leftrightarrow \text{buď } \mathcal{M} \models \psi_2[e_2] \text{ nebo } \mathcal{M} \not\models \psi_1[e_2] \\ &\Leftrightarrow \mathcal{M} \models \varphi[e_2], \end{aligned}$$

  kde druhá ekvivalence plyne z indukčního předpokladu a z toho, že libovolná proměnná je volná v ψ_1 nebo v ψ_2 tehdy a jen tehdy, když je volná ve φ.

- Je-li $\varphi \equiv \forall y\, \psi$, pak

$$\begin{aligned} \mathcal{M} \models \varphi[e_1] &\Leftrightarrow \text{pro každé } a \in M \text{ platí } \mathcal{M} \models \psi[e_1(y/a)] \\ &\Leftrightarrow \text{pro každé } a \in M \text{ platí } \mathcal{M} \models \psi[e_2(y/a)] \\ &\Leftrightarrow \mathcal{M} \models \varphi[e_2], \end{aligned}$$

  kde druhou ekvivalenci lze zdůvodnit takto: Z definice plyne, že pokud je libovolná proměnná x volná v ψ, pak buď x je y nebo x je volná ve φ. Z toho plyne, že pro libovolnou proměnnou x, která je volná v ψ a pro libovolné $a \in M$ platí, že $e_1(y/a)(x) = e_2(y/a)(x)$. Požadovaná ekvivalence potom plyne z indukčního předpokladu.

Nyní dokážeme tvrzení ze zadání příkladu.

$\Rightarrow$: Tento směr byl v obecnější podobě dokázán v Příkladu 7.1.

$\Leftarrow$: Předpokládejme, že $\mathcal{M} \not\models \varphi$. Potom existuje ohodnocení e takové, že $\mathcal{M} \not\models \varphi[e]$. Protože *žádná* proměnná není volná ve φ, dostaneme z předchozího tvrzení, že $\mathcal{M} \not\models \varphi[e']$ a tedy $\mathcal{M} \models \neg\varphi[e']$ pro *libovolné* ohodnocení e'. Z definice plyne, že $\mathcal{M} \models \neg\varphi$. ▲

✪✪ **Příklad 7.3** Mějme jazyk $\mathcal{L} = \{P, Q\}$ bez rovnosti, kde P a Q jsou unární predikátové symboly. Rozhodněte a dokažte, zda pro každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$$\mathcal{M} \models \forall x\, (P(x) \leftrightarrow Q(x)) \rightarrow (\forall x\, P(x) \leftrightarrow \forall x\, Q(x))$$

Řešení [Neformálně] Platí. Mějme libovolnou realizaci $\mathcal{M}$ a ohodnocení e takové, že $\mathcal{M} \models \forall x\, (P(x) \leftrightarrow Q(x))[e]$. Pro každé $a \in M$ tedy platí $\mathcal{M} \models P(x) \leftrightarrow Q(x)[e(x/a)]$. Tedy pro každé $a \in M$ platí $e[x/a](x) \in P_{\mathcal{M}}$, právě když $e[x/a](x) \in Q_{\mathcal{M}}$, a tedy platí $a \in P_{\mathcal{M}}$, právě když $a \in Q_{\mathcal{M}}$ (protože $e[x/a](x)$ je a).

Předpokládejme, že $\mathcal{M} \models \forall x\, P(x)[e]$. Obdobnou argumentací jako výše dostáváme, že pro všechna $a \in M$ platí $a \in P_{\mathcal{M}}$. Dle výše dokázaného to znamená, že pro všechna $a \in M$ platí $a \in Q_{\mathcal{M}}$. tedy $\mathcal{M} \models \forall x\, Q(x)[e]$. Symetricky se ukáže i platnost opačné implikace, tedy celkově dostáváme $\mathcal{M} \models (\forall x\, P(x) \leftrightarrow \forall x\, Q(x))[e]$. ▲

Řešení [Formálně]

Mějme libovolnou realizaci $\mathcal{M}$ a libovolné ohodnocení e. Výraz

$$\mathcal{M} \models \forall x\, (P(x) \leftrightarrow Q(x)) \rightarrow (\forall x\, P(x) \leftrightarrow \forall x\, Q(x))\ [e].$$

z definice platí pokud

$$\mathcal{M} \not\models \forall x\ (P(x) \leftrightarrow Q(x))\ [e] \quad \text{nebo}$$
$$\mathcal{M} \models \forall x\ P(x) \leftrightarrow \forall x\ Q(x)\ [e]$$

Předpokládejme, že

$$\mathcal{M} \models \forall x\ (P(x) \leftrightarrow Q(x))\ [e],$$

potřebujeme dokázat, že

$$\mathcal{M} \models \forall x\ P(x) \leftrightarrow \forall x\ Q(x)\ [e]$$

což dle definice platí, pokud

$$\mathcal{M} \models \forall x\ P(x)[e], \quad \text{právě když} \quad \mathcal{M} \models \forall x\ Q(x)\ [e].$$

Úpravou předpokladu dle definice máme

$$\mathcal{M} \models (P(x) \leftrightarrow Q(x))\ [e(x/a)] \quad \text{pro všechna } a \in M,$$

a tedy pro každé $a \in M$ platí

$$\mathcal{M} \models P(x)\ [e(x/a)], \quad \text{právě když} \quad \mathcal{M} \models Q(x)\ [e(x/a)]. \tag{7.1}$$

Nyní můžeme dokázat požadovanou ekvivalenci. Předpokládejme její levou stranu, tedy, že platí

$$\mathcal{M} \models \forall x\ P(x)\ [e],$$

to je z definice právě když pro libovolné $a \in M$ platí

$$\mathcal{M} \models P(x)\ [e(x/a)]$$

což s pomocí tvrzení (1) platí, právě když pro libovolné $a \in M$

$$\mathcal{M} \models Q(x)\ [e(x/a)]$$

což je z definice právě když

$$\mathcal{M} \models \forall x\ Q(x)\ [e].$$

Dostali jsme pravou stranu dokazované ekvivalence. Celkově tedy pro zvolené e platí

$$\mathcal{M} \models \forall x\ (P(x) \leftrightarrow Q(x)) \rightarrow (\forall x\ P(x) \leftrightarrow \forall x\ Q(x))\ [e].$$

Protože jsme zvolili e libovolně, dostáváme

$$\mathcal{M} \models \forall x\ (P(x) \leftrightarrow Q(x)) \rightarrow (\forall x\ P(x) \leftrightarrow \forall x\ Q(x)).$$

▲

✿✿ **Příklad 7.4** Nechť $\mathcal{L}$ je jazyk bez rovnosti s jedním unárním predikátovým symbolem P. Rozhodněte a dokažte, zda pro každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$$\mathcal{M} \models P(x) \rightarrow \forall x P(x)$$

✿✿ **Příklad 7.5** Nechť $\mathcal{L} = \{f, g\}$ je jazyk s rovností, kde f a g jsou unární funkční symboly. Rozhodněte a dokažte, zda pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$$\mathcal{M} \ \models\ \forall y\,(f(x) = y \rightarrow g(y) = x)\ \rightarrow\ g(f(x)) = x.$$

✿✿ **Příklad 7.6** Mějme jazyk $\mathcal{L}$ s rovností a unárním predikátovým symbolem P. Rozhodněte a dokažte, zda je následující formule pravdivá v každé realizaci jazyka $\mathcal{L}$:

$$(\forall x\ P(x) \leftrightarrow \exists x\ P(x)) \rightarrow \forall x\ \forall y\ (x = y)$$

✿✿ **Příklad 7.7** Nechť φ je formule predikátového počtu jazyka $\mathcal{L}$ taková, že x je jediná volná proměnná ve φ. Rozhodněte, zda pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ a libovolnou proměnnou y substituovatelnou za x ve φ platí $\mathcal{M} \models \varphi \rightarrow \varphi(x/y)$.

Řešení Odpověď: Tvrzení neplatí! Zdůvodnění: Nechť $\mathcal{L} = \{P\}$ kde P je unární predikátový symbol. Definujme realizaci $\mathcal{M}$ takto:

- $M = \{a, b\}$
- $P_{\mathcal{M}} = \{a\}$

Nyní uvažme ohodnocení e takové, že $e(x) = a$ a $e(y) = b$ a formuli $\varphi \equiv P(x)$. Zřejmě $\mathcal{M} \not\models (P(x) \rightarrow P(x)(x/y))[e]$, protože $e(x) = a \in P_{\mathcal{M}}$ a $e(y) = b \notin P_{\mathcal{M}}$.

Poznámka: $\mathcal{M} \models \varphi \rightarrow \exists y \varphi(x/y)$ platí pro libovolnou realizaci jazyka $\mathcal{L}$.

▲

✡✡✡ **Příklad 7.8** Rozhodněte, zda existuje jazyk $\mathcal{L}$ s rovností a jeho realizace $\mathcal{M}$ taková, že pro všechny formule φ predikátového počtu jazyka $\mathcal{L}$ platí $\mathcal{M} \not\models \varphi$. Své tvrzení zdůvodněte.

Řešení Neexistuje protože $\forall x(x = x)$ je pravdivá pro libovolnou realizaci jazyka $\mathcal{L}$. ▲

✡✡✡ **Příklad 7.9** Nechť $\mathcal{L}$ je jazyk bez rovnosti a s jedním binárním predikátovým symbolem P. Rozhodněte, zda pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ existuje ohodnocení e takové, že

$$\mathcal{M} \models (\,(\exists x P(x, y)) \to \exists z P(x, z)\,)[e]$$

Své tvrzení zdůvodněte.

Řešení Tvrzení platí, mohou nastat 2 případy:

- $P_{\mathcal{M}} = \emptyset$, pak uvedená formule je triviálně pravdivá pro libovolné ohodnocení, protože není pravdivý předpoklad implikace, tedy $\mathcal{M} \not\models \exists x P(x, y)[e]$ pro žádné e a tedy $\mathcal{M} \models (\,(\exists x P(x, y)) \to \exists z P(x, z)\,)[e]$.
- Existuje $a, b \in M$, t.ž. $(a, b) \in P_{\mathcal{M}}$. Zvolíme e tak, aby platilo $e(x) = a$. Je zřejmé, že $\mathcal{M} \models \exists z P(x, z)[e]$ a tím pádem i $\mathcal{M} \models (\,(\exists x P(x, y)) \to \exists z P(x, z)\,)[e]$.

▲

✡✡✡ **Příklad 7.10** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Rozhodněte a dokažte, zda existuje formule φ jazyka $\mathcal{L}$ taková, že pro každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ existují ohodnocení e, e' taková, že $\mathcal{M} \models \varphi[e]$ a zároveň $\mathcal{M} \not\models \varphi[e']$.

Řešení Neexistuje. Předpokládejme, že existuje taková formule φ. Vezměme realizaci $\mathcal{M}$ s *jednoprvkovým* nosičem $M = \{a\}$. V této realizaci existuje jen jedno ohodnocení e (toto ohodnocení přiřadí všem proměnným prvek a).

Z definice nemůže současně platit $\mathcal{M} \models \varphi[e]$ a $\mathcal{M} \not\models \varphi[e]$, tedy docházíme ke sporu s podmínkami, které má φ splňovat. ▲

✡✡✡

Příklad 7.11 Mějme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Uvažme následující formule predikátové logiky jazyka $\mathcal{L}$:

$$\begin{aligned}
\varphi_1 &= \exists x \left((\forall y \neg R(y,x)) \wedge \forall z(\forall y \neg R(y,z) \to z = x)\right) \\
\varphi_2 &= \forall x \forall y \forall z \left((R(y,x) \wedge R(z,x)) \to y = z\right) \\
\varphi_3 &= \forall x \forall y \left(R(x,y) \to \exists z(z \neq y \wedge R(x,z))\right) \\
\varphi_4 &= \forall x \forall y \forall z \forall u \left((R(x,y) \wedge R(x,z) \wedge R(x,u)) \to (y = z \vee y = u \vee z = u)\right)
\end{aligned}$$

Nalezněte realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ jejíž nosič má alespoň 6 prvků a pro kterou platí $\mathcal{M} \models \varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4$. Svou volbu realizace $\mathcal{M}$ zdůvodněte.[1] Dokažte, že neexistuje realizace $\mathcal{M}'$ jejíž nosič by měl 2^{2013} prvků a pro kterou by platilo $\mathcal{M}' \models \varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4$.

Řešení Nejprve si uvědomme, že každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ je možné neformálně vnímat jako (potenciálně nekonečný) graf s množinou vrcholů M a množinou hran $R_{\mathcal{M}}$. Intuitivně, formule φ_1 říká, že v tomto grafu existuje právě jeden vrchol do kterého nevede žádná hrana. Formule φ_2 říká, že do každého vrcholu vede nejvýše jedna hrana. Formule φ_3 vynucuje, že žádný vrchol nemá přesně jednoho následníka a formule φ_4 říká, že každý vrchol má nejvýše dva následníky. Konjunkci těchto formulí splňuje zejména každý binární strom, pokud tedy chceme realizaci s alespoň 6 prvky, lze uvážit realizaci $\mathcal{M}$ s nosičem $M = \{1,2,3,4,5,6,7\}$, v níž

$$R_{\mathcal{M}} = \{(1,2),(1,3),(2,4),(2,5),(3,6),(3,7)\}.$$

Pro druhou část zadání si stačí uvědomit, že každá realizace s konečným nosičem, ve které je pravdivá konjunkce uvedených formulí, má nosič liché mohutnosti. Vskutku, každá taková realizace $\mathcal{M}$ je vlastně orientovaný graf, jehož každá komponenta slabé souvislosti[2] má jeden ze dvou následujících tvarů:

a) Binární strom. Přitom $\mathcal{M}$ má právě jednu takovou slabě souvislou komponentu, neboť φ_1 vynucuje, že v grafu je právě jeden vrchol do

[1] Zdůvodnění nemusí mít formu zcela formálního důkazu, ale musí být pochopitelné a přesvědčivé. Ideální bude, pokud v přirozeném jazyce co nejlépe popíšete význam formulí φ_1-φ_4, tj. popíšete vlastnosti, které realizace musí mít, aby v ní daná formule byla pravdivá, a poté ověříte, že Vaše realizace tyto vlastnosti má.

[2] Množina vrcholů C daného orientovaného grafu je *slabě souvislá*, pokud pro libovolné dva vrcholy $u, v \in C$ platí, že pokud zapomeneme orientaci jednotlivých hran, pak u je dosažitelná z v. Komponenta slabé souvislosti je pak každá maximální (vzhledem k inkluzi) slabě souvislá množina vrcholů.

kterého nevede žádná hrana: tento vrchol je nutně binárního stromu (formule φ_2 vynucuje, že jde skutečně o strom a formule φ_3 a φ_4 vynucují binárnost).

b) Komponenta, ve které do každého vrcholu vede jedna hrana. Tvrdíme, že taková komponenta má (velmi intuitivně) tvar kružnice, na jejímž každém vrcholu je „přivěšený“ binární strom, tj. například komponenta s vrcholy $A, B, C, 1, 2, 3, 4, 5$ a hranami

$$(A, B), (B, C), (C, A), (A, 1), (B, 2), (C, 3), (3, 4), (4, 5).$$

Formalizujte toto intuitivní tvrzení!

Snadno nahlédneme, že jediná komponenta typu a) (binární strom) má lichý počet vrcholů, zatímco libovolná komponenta typu b) má sudý počet vrcholů (několik stromů s lichým počtem vrcholů a ke každému stromu příslušející vrchol na kružnici, celkem tedy sudý počet). Počet vrcholů grafu je tedy lichý a nemůže být roven číslu 2^{2013}.

▲

✡✡✡ **Příklad 7.12** Mějme jazyk $\mathcal{L} = \{\cdot\}$ s rovností, kde $\cdot$ je binární funkční symbol. Mějme formuli $\varphi \equiv \forall x\, \forall y\, (x \cdot y = y \cdot x)$. Rozhodněte a dokažte, zda

a) pro každou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí $\mathcal{M} \models \varphi$,
b) existuje realizace $\mathcal{M}$ jazyka $\mathcal{L}$ taková, že $\mathcal{M} \models \varphi$.

✡✡✡ **Příklad 7.13** Mějme jazyk $\mathcal{L} = \{P\}$ bez rovnosti, kde P je binární predikátový symbol. Rozhodněte a dokažte, zda pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí následující tvrzení:

a) $\mathcal{M} \models \forall x\, \forall z\, (P(x, z) \to \exists y\, P(x, y))$
b) $\mathcal{M} \models (\forall x\, \exists y\, P(x, y)) \to (\exists y\, \forall x\, P(x, y))$
c) $\mathcal{M} \models (\exists y\, \forall x\, P(x, y)) \to (\forall x\, \exists y\, P(x, y))$

Kapitola 8

Teorie predikátové logiky

V předchozích kapitolách jsme zavedli pojem realizace, na který nahlížíme jako na svět, o kterém se pomocí predikátových formulí vyjadřujeme. Vzhledem k tomuto světu definujeme pravdivost formulí. V této kapitole se budeme zabývat tím, jak pomocí formulí vymezit nějaký soubor *světů* (tj. realizací) pro které platí určité zákonitosti. Využijeme k tomu soubory formulí – tzv. teorie.

Definice 8.1 Buď $\mathcal{L}$ jazyk (příp. jazyk s rovností).

- Teorie (s jazykem $\mathcal{L}$) je soubor T formulí predikátového počtu jazyka $\mathcal{L}$. Prvky T se nazývají axiomy teorie T.
- Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je model teorie T, psáno $\mathcal{M} \models T$, jestliže $\mathcal{M} \models \varphi$ pro každé φ z T.

Takže teorie je jednoduše soubor formulí. Je důležité si uvědomit, že tento soubor může být nekonečný. Definici si procvičíme na dvou jednoduchých příkladech.

✡✡✡ **Příklad 8.1** Nechť $\mathcal{L} = \{P\}$ je jazyk s rovností, kde P je binární predikátový symbol a a je nulární funkční symbol. Zadejte nějaký model k následující teorii T v jazyce $\mathcal{L}$.

$$\begin{aligned} T = \{\ & \forall x\ P(x,x), \\ & \forall x\ \forall y\ ((P(x,y) \to P(y,x)), \\ & \forall x\ \forall y\ \forall z\ ((P(x,y) \wedge P(y,z)) \to P(x,z))\ \} \end{aligned}$$

Řešení První formule vynucuje, aby realizace $P_{\mathcal{M}}$ predikátového symbolu P v každém modelu $\mathcal{M}$ teorie T byla reflexivní. Tímto vlastně vyloučíme všechny realizace, které nemají reflexivní $P_{\mathcal{M}}$. Podobně druhá formule vynucuje symetrii a třetí tranzitivitu. Tím pádem pro libovolný model $\mathcal{M}$ teorie T platí, že $P_{\mathcal{M}}$ je současně reflexivní, symetrická a tranzitivní. Modelem tedy mohou být například realizace $(\{a, b, c\}, P_{\mathcal{M}} = \{(x, x) \mid x \in M\})$ anebo $(\mathbb{N}, P_{\mathcal{M}} = \{(x, y) \mid x^2 = y^2\})$. ▲

✪✪✩ **Příklad 8.2** Mějme jazyk $\mathcal{L} = \emptyset$ s rovností. Dejte příklad teorie T s jazykem $\mathcal{L}$ takové, že její modely jsou právě realizace s *nekonečným* nosičem.

Řešení Formule $\exists x \exists y \neg(x = y)$ je pravdivá pouze v realizacích s alespoň dvouprvkovým nosičem. Podobně formule

$$\exists x \exists y \exists z (\neg(x = y) \wedge \neg(y = z) \wedge \neg(x = z))$$

je pravdivá pouze v realizacích s alespoň tříprvkovým nosičem. Obecně pro $n \in \{2, 3, \ldots\}$ formule

$$\varphi_n \equiv \exists\, x_1 \cdots \exists\, x_n \bigwedge_{\substack{1 \leq i,j \leq n \\ i \neq j}} \neg(x_i = x_j)$$

je pravdivá právě v realizacích s alespoň n-prvkovým nosičem. Hledaná teorie T je tedy $\{\varphi_n \mid n \in \{2, 3, \ldots\}\}$. Vskutku, libovolná realizace $\mathcal{M}$ s nekonečným nosičem zřejmě splňuje $\mathcal{M} \models \varphi_n$ pro libovolné n (neboť zřejmě má alespoň n-prvkový nosič). Na druhou stranu žádná realizace $\mathcal{M}$, která je modelem T, nemůže mít konečný nosič, neboť kdyby měla dejme tomu n-prvkový nosič (pro nějaké $n \in \mathbb{N}$), nemohlo by platit $\mathcal{M} \models \varphi_{n+1}$. Meta-ekvivalence požadovaná v zadání je tedy splněna. ▲

Nekonečné teorie mají striktně vyšší vyjadřovací sílu jako konečné teorie. V předchozím příkladě jsme použili nekonečnou teorii. Pomocí konečné teorie příklad vyřešit nelze. Formální argument poskytneme až v kapitole 10 pomocí věty o kompaktnosti v Příkladu 10.5.

Definice 8.2 Buď $\mathcal{L}$ jazyk (příp. jazyk s rovností). Teorie je splnitelná, jestliže má model.

✪✩✩ **Příklad 8.3** Mějme jazyk $\mathcal{L} = \{S\}$ s rovností, kde S je unární funkční symbol. Dejte příklad *splnitelné konečné* teorie T s jazykem $\mathcal{L}$ takové, že všechny její modely mají *nekonečný* nosič.

Řešení Uvažme $T = \{\forall x \forall y (S(x) = S(y) \to x = y), \exists y \forall x \neg (S(x) = y)\}$.

Nejprve ukážeme, že teorie T nemá konečný model. Nechť $\mathcal{M}$ je model teorie T. Potom $S_{\mathcal{M}}$ je *injektivní* funkce definovaná na M, která není *surjektivní*. Taková funkce ovšem nemůže existovat na konečném souboru, a proto M musí být nekonečný soubor.

Nyní ukážeme, že T je splnitelná. Definujme realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takto:

- $M = \mathbb{N}_0$ (přirozená čísla s nulou)
- $S_{\mathcal{M}}(n) = n + 1$ pro $n \in \mathbb{N}_0$

Je zřejmé, že $\mathcal{M} \models T$. ▲

Všimněte si, že zadání předchozího příkladu se od příkladu 8.2 liší (kromě jiného jazyka) v tom, že jsme nepožadovali, aby modely teorie byly *právě* realizace s nekonečným nosičem. Například realizace s nosičem $\mathbb{N}$, ve které se S realizuje jako identita, není modelem teorie z řešení předchozího příkladu.

Máme-li soubor světů, kterými se zabýváme, omezený na modely nějaké teorie, můžeme se bavit o tom, zda je nějaká formule v těchto světech *pravdivá*. Například si můžeme zadefinovat teorii monoidů T tím, že do ní zahrneme formuli vynucující asociativitu a existenci jednotkového prvku, tedy

$$T = \{\forall x \forall y \forall z \, ((x \cdot y) \cdot z = x \cdot (y \cdot z)), \, \exists x \forall y \, (x \cdot y = y \wedge y \cdot x = y)\}.$$

Tím pádem se budeme pohybovat jen ve světech (tj. realizacích), které jsou monoidy. Dále nás může zajímat, zda platí, že v každém monoidu existuje nejvýše jeden jednotkový prvek. Tedy se budeme ptát, zda je formule

$$\forall x \forall y \forall z ((x \cdot z = z \wedge z \cdot x = z \wedge y \cdot z = z \wedge z \cdot y = z) \to x = y)$$

pravdivá v každém modelu teorie T.

Definice 8.3 Buď $\mathcal{L}$ jazyk (příp. jazyk s rovností). Formule φ je sémantickým důsledkem teorie T, psáno $T \models \varphi$, jestliže φ je pravdivá v každém modelu teorie T.

✡☆☆ **Příklad 8.4** Nechť $\varphi \equiv \forall x \neg (S(x) = x)$ a nechť T je teorie z řešení Příkladu 8.3. Rozhodněte, zda platí $T \models \varphi$.

Řešení Odpověď: Neplatí! Zdůvodnění: Definujme realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takto:

- $M = \mathbb{N}_0$
- $S_{\mathcal{M}}(0) = 0$ a $S_{\mathcal{M}}(i) = i + 1$ pro $i \geq 1$

Realizace $\mathcal{M}$ je zřejmě modelem T a zároveň $\mathcal{M} \not\models \varphi$. ▲

✩✩✩ **Příklad 8.5** Nechť T je konečná teorie s jazykem $\mathcal{L}$. Dokažte, že existuje konečná teorie T' s jazykem $\mathcal{L}$ taková, že $\mathcal{M} \models T'$ právě tehdy, když $\mathcal{M} \not\models T$ pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$.

Řešení Nejprve předpokládejme, že $T = \{\varphi_1, \ldots, \varphi_n\}$ kde $\varphi_1, \ldots, \varphi_n$ jsou uzavřené formule. Uvažme $T' = \{\bigvee_{i=1}^n \neg\varphi_i\}$. Pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$$\begin{aligned}
\mathcal{M} \models \textstyle\bigvee_{i=1}^n \neg\varphi_i \quad &\Leftrightarrow \quad \mathcal{M} \models \textstyle\bigvee_{i=1}^n \neg\varphi_i[e] \text{ pro každé ohodnocení } e \\
&\Leftrightarrow \quad \mathcal{M} \models \neg\varphi_i[e] \text{ pro nějaké } i \text{ a pro každé ohodnocení } e \\
&\Leftrightarrow \quad \mathcal{M} \models \neg\varphi_i \text{ pro nějaké } i \\
&\Leftrightarrow \quad \mathcal{M} \not\models \varphi_i \text{ pro nějaké } i \\
&\Leftrightarrow \quad \mathcal{M} \not\models T
\end{aligned}$$

kde druhá ekvivalence plyne z uzavřenosti formulí $\varphi_1, \ldots, \varphi_n$ a Tvrzení 7.4 z řešení Příkladu 7.2 ($\mathcal{M} \models \neg\varphi_i[e]$ pro nějaké i a nějaké e a tudíž pro všechna e, protože $\neg\varphi_i$ je uzavřená) a čtvrtá ekvivalence je přímo tvrzení dokázané v Příkladu 7.2.

V obecném případě nemusí být formule z T uzavřené. Tuto situaci řeší následující jednoduché tvrzení.

Tvrzení 8.4 Nechť φ je formule predikátového počtu jazyka $\mathcal{L}$ a nechť x je proměnná. Potom pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí $\mathcal{M} \models \forall x\varphi$ právě tehdy, když $\mathcal{M} \models \varphi$.

Důkaz

$$\begin{aligned}
\mathcal{M} \models \forall x\varphi \Leftrightarrow\ & \mathcal{M} \models \forall x\varphi[e] \text{ pro každé ohodnocení } e \\
\Leftrightarrow\ & \mathcal{M} \models \varphi[e(x/a)] \text{ pro každé ohodnocení } e \text{ a pro každé } a \in M \\
\Leftrightarrow\ & \mathcal{M} \models \varphi[e] \text{ pro každé ohodnocení } e \\
\Leftrightarrow\ & \mathcal{M} \models \varphi,
\end{aligned}$$

kde třetí metaekvivalenci je možné zdůvodnit takto: $\Rightarrow$ plyne z toho, že každé ohodnocení e je možné psát ve tvaru $e = e(x/e(x))$, zatímco $\Leftarrow$ plyne jednoduše z toho, že $e(x/a)$ je jedno konkrétní ohodnocení. ▲

✿✿✿ **Příklad 8.6** Nechť $\mathcal{L} = \{\sim, a\}$ je jazyk s rovností, kde $\sim$ je binární predikátový symbol a a je nulární funkční symbol. Zadejte nějaký model k následující teorii T v jazyce $\mathcal{L}$.

$$T = \{\ \forall x\, \exists y\, (x \sim y),\ \ \forall x\, \forall y\, ((x \sim y \wedge y \sim x) \to (x = a \wedge y = a))\ \}$$
$$\cup\{\ \varphi_n \mid n \in \mathbb{N}, n \geq 2\ \}, \text{ kde}$$

$$\varphi_n \equiv \exists\, x_1 \cdots \exists\, x_n \bigwedge_{\substack{1 \leq i,j \leq n \\ i \neq j}} \neg(x_i = x_j) \wedge \neg(x_i \sim x_j)$$

✿✿✿ **Příklad 8.7** Mějme jazyk $\mathcal{L} = \{P, \circ\}$ bez rovnosti, kde $\circ$ je binární funkční symbol a P je unární predikátový symbol. Mějme dále teorii T s jazykem $\mathcal{L}$:

$$T = \{P(x \circ y) \leftrightarrow \neg(P(x) \wedge P(y))\}.$$

Zadejte nějaký term t jazyka $\mathcal{L}$ takový, že v libovolném modelu $\mathcal{M}$ teorie T platí $\mathcal{M} \models P(t)$. Své řešení stručně zdůvodněte.

✿✿✿ **Příklad 8.8** Mějme jazyk $\mathcal{L} = \{P, a, f\}$ s rovností, kde P je binární predikátový symbol, a je nulární funkční symbol a f je unární funkční symbol. Dále mějme teorii

$$\begin{aligned} T = \{\ & \forall x\ P(x,x), \\ & \forall x\, \forall y\ ((P(x,y) \wedge P(y,x)) \to x = y), \\ & \forall x\, \forall y\, \forall z\ ((P(x,y) \wedge P(y,z)) \to P(x,z)), \\ & \forall x\ (P(x,a) \leftrightarrow \neg(P(f(x),a)))\ \} \end{aligned}$$

Zadejte realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takovou, že je modelem teorie T.

✿✿✿ **Příklad 8.9** Mějme jazyk $\mathcal{L} = \{f\}$ s rovností, kde f je binární funkční symbol. Pro libovolné přirozené číslo $n \geq 2$ uvažme následující formuli ψ_n:

$$\psi_n \quad \equiv \quad \exists x_1 \exists x_2 \ldots \exists x_{2n} \bigwedge_{1 \leq i < j \leq n} f(x_{2i-1}, x_{2i}) \neq f(x_{2j-1}, x_{2j}).$$

Uvažme dále teorii $T = \{\forall x \exists y \forall z (y = f(x,z))\} \cup \{\psi_n \mid n \geq 2\}$.

Rozhodněte, zda je teorie T splnitelná. Pokud ano, najděte nějaký její model; v opačném případě zdůvodněte, proč žádný model nemá.

✿✿✿ **Příklad 8.10** Mějme jazyk $\mathcal{L} = \{f, g\}$ s rovností, kde f a g jsou unární funkční symboly. Pro libovolné přirozené číslo $n \geq 2$ uvažme následující formuli ψ_n:

$$\psi_n \equiv \exists x_1 \exists x_2 \ldots \exists x_n \bigwedge_{1 \leq i,j \leq n, i \neq j} (f(x_i) \neq f(x_j)) \wedge (g(x_i) \neq (x_j)) \wedge (f(x_i) \neq g(x_j))).$$

Uvažme dále teorii $T = \{\forall x \exists y (f(x) = g(y))\} \cup \{\psi_n \mid n \geq 2\}$. Nalezněte nějaký model teorie T. Své řešení stručně a neformálně zdůvodněte.

✿✿✿ **Příklad 8.11** Mějme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Zadejte teorii T takovou, že realizace $\mathcal{M}$ je modelem T, právě když $(M, R_{\mathcal{M}})$ je lineárně uspořádaná množina.

✿✿✿ **Příklad 8.12** Nechť $\mathcal{L}$ je jazyk s rovností a s jedním binárním predikátovým symbolem R. Dejte příklad teorie T s jazykem $\mathcal{L}$ takové, že libovolná realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je modelem T právě když $(M, R_{\mathcal{M}})$ *není* lineárně uspořádaná množina.

✿✿✿ **Příklad 8.13** Nechť $\mathcal{L}$ je jazyk s rovností a s jedním binárním predikátovým symbolem $\leq$. Dejte příklad teorie T s jazykem $\mathcal{L}$ takové, že libovolná realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je modelem T, právě když $(M, \leq_{\mathcal{M}})$ je uspořádaná množina, v níž každý prvek je porovnatelný s nekonečně mnoha jinými prvky.

✿✿✿ **Příklad 8.14** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Zadejte teorii T takovou, že pro libovolnou realizaci $\mathcal{M}$ platí, že $\mathcal{M} \models T$, právě když nosič M realizace $\mathcal{M}$ je nekonečný nebo existuje $k \in \mathbb{N}$ takové, že $|M| = 2^k$.

✿✿✿ **Příklad 8.15** Nechť A je libovolná množina. Řekneme, že nekonečná posloupnost $X_1, X_2, X_3, \ldots$ podmnožin množiny A je *klesající*, jestliže pro libovolné $i \geq 1$ platí $X_i \supset X_{i+1}$, tj. je-li X_{i+1} vlastní podmnožinou množiny X_i. *Limitou* posloupnosti podmnožin $X_1, X_2, X_3, \ldots$ je množina $X := \bigcap_{i=1}^{\infty} X_i$.

Uvažme jazyk $\mathcal{L} = \{P^n \mid n \geq 1\} \cup \{S\}$ bez rovnosti,[1] kde $S, P^1, P^2, \ldots$ jsou unární predikátové symboly. Zadejte *splnitelnou* teorii T s jazykem $\mathcal{L}$ takovou, že v libovolném modelu $\mathcal{M}$ této teorie je $P^1_{\mathcal{M}}, P^2_{\mathcal{M}}, P^3_{\mathcal{M}}, \ldots$ klesající posloupností podmnožin množiny M s *neprázdnou* limitou.

[1] Proměnná n opět nabývá pouze hodnot z oboru přirozených čísel.

Řešení Pro libovolné $n \geq 1$ definujme formule

$$\psi_n = \underbrace{\forall x(P^{n+1}(x) \to P^n(x))}_{\text{vynucuje } P^{n+1}_{\mathcal{M}} \subseteq P^n_{\mathcal{M}}} \wedge \underbrace{\exists x(P^n(x) \wedge \neg P^{n+1}(x))}_{\text{vynucuje } P^n_{\mathcal{M}} \neq P^{n+1}_{\mathcal{M}}}$$
$$\rho_n = \underbrace{\forall x(S(x) \to P^n(x))}_{\text{vynucuje } S_{\mathcal{M}} \subseteq P^n_{\mathcal{M}}}.$$

Požadovanou teorii T pak můžeme zadat následovně:

$$T = \{\psi_n, \rho_n \mid n \geq 1\} \cup \{\exists x S(x)\}.$$

Poslední přidaná formule vynucuje neprázdnost množiny $S_{\mathcal{M}}$. Pak $S_{\mathcal{M}}$ musí být ve všech modelech teorie T neprázdná množina, která je podmnožinou všech množin $P^1_{\mathcal{M}}, P^2_{\mathcal{M}}, \ldots$ (díky formulím ρ_n). Musí tedy být i podmnožinou jejich průniku, což zaručuje neprázdnost limity.

▲

✪✪✩ **Příklad 8.16** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Rozhodněte, zda existuje teorie T s jazykem $\mathcal{L}$, která má model s jednoprvkovým nosičem a zároveň model s nekonečným nosičem a zároveň nemá žádný model s konečným nosičem mohutnosti větší než 1. Své tvrzení zdůvodněte.

✪✩✩ **Příklad 8.17** Nechť $\mathcal{L}$ je jazyk s rovností a se dvěma unárními predikátovými symboly P a Q. Zadejte teorii T takovou, že realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je modelem teorie T, právě když nosič M realizace $\mathcal{M}$ má právě čtyři prvky, z nichž dva jsou jen v $P_{\mathcal{M}}$ a další dva jen v $Q_{\mathcal{M}}$ (přesněji, právě když $|M| = 4$, $|P_{\mathcal{M}}| = |Q_{\mathcal{M}}| = 2$ a $P_{\mathcal{M}} \cap Q_{\mathcal{M}} = \emptyset$).

✪✪✩ **Příklad 8.18** Nechť $\mathcal{L}$ je jazyk s rovností a s jedním binárním predikátovým symbolem R. Zadejte teorii T takovou, že realizace $\mathcal{M} = (M, R_{\mathcal{M}})$ je modelem teorie T, právě když $R_{\mathcal{M}}$ je relace ekvivalence na M s dvouprvkovým rozkladem (tedy když množina $M/R_{\mathcal{M}}$ má právě dva prvky).

Pro připomenutí: pro množinu X a relaci ekvivalence $\sim$ definujeme pro každé $a \in X$ příslušnou třídu rozkladu $[a]_\sim = \{b \mid a \sim b\}$, dále rozklad množiny X dle $\sim$ je $X/\sim = \{[a]_\sim \mid a \in X\}$.

✪✪✩ **Příklad 8.19** Nechť $\mathcal{L} = \{R\}$ je jazyk s rovností, kde R je binární predikátový symbol. Zadejte teorii T takovou, že libovolná realizace $\mathcal{M}$ s nosičem M je modelem teorie T, právě když $R_{\mathcal{M}}$ je relace ekvivalence na množině M a každá třída rozkladu množiny M dle relace $R_{\mathcal{M}}$ má právě dva prvky.

✡✡✡ **Příklad 8.20** Nechť $\mathcal{L}$ je jazyk s rovností s jedním binárním predikátovým symbolem R. Zadejte teorii T takovou, že libovolná realizace $\mathcal{M}$ je modelem teorie T, právě když $(M, R_{\mathcal{M}})$ je uspořádaná množina s největším a nejmenším prvkem.

✡✡✡ **Příklad 8.21** Nechť $\mathcal{L}$ je jazyk s rovností s jedním *binárním predikátovým* symbolem P. Zadejte teorii T takovou, že libovolná realizace $\mathcal{M} = (M, P_{\mathcal{M}})$ je modelem teorie T, právě když $P_{\mathcal{M}}$ je *injektivní funkce* na množině M, která *má pevný bod*.

Pro připomenutí: Každá funkce je relace, zápis $f(a) = b$ je jen zkratka pro $(a, b) \in f$. Prvek a je pevným bodem funkce f, pokud $f(a) = a$.

✡✡✡ **Příklad 8.22** Nechť $\mathcal{L}$ je jazyk s rovností s jedním binárním predikátovým symbolem P a jedním unární funkčním symbolem f. Zadejte teorii T takovou, že libovolná realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je modelem teorie T, právě když $P_{\mathcal{M}}$ je uspořádání na množině M a f je izotonní funkce vzhledem k uspořádání $P_{\mathcal{M}}$.

Pro připomenutí: Funkce $f\colon X \to X$ je izotonní vzhledem k uspořádání $<$, pokud pro libovolné prvky a, b z množiny X, které splňují $a < b$, platí, že $f(a) < f(b)$.

✡✡✡ **Příklad 8.23** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Zadejte teorii T takovou, že libovolná realizace $\mathcal{M}$ je modelem teorie T, právě když nosič M realizace $\mathcal{M}$ je buď nekonečný nebo má sudý počet prvků.

Tip: Může Vám pomoct vyjádřit formuli φ_n, která vyžaduje, že "realizace má *právě* n prvků".

✡✡✡ **Příklad 8.24** Mějme jazyk $\mathcal{L} = \{N, S, +, *\}$ s rovností, kde N je nulární funkční symbol, S je unární funkční symbol a $+$ a $*$ jsou binární funkční symboly. Zadejte teorii T v jazyce $\mathcal{L}$, která splňuje (‡) pro libovolnou realizaci $\mathcal{M}$ s nosičem $\mathbb{N}_0$ (přirozená čísla s nulou), ve které je symbol N realizován jako 0, symbol $+$ jako standardní sčítání na $\mathbb{N}_0$ a symbol S jako operace následníka (tedy funkce, která číslu n přiřadí číslo $n+1$ pro libovolné $n \in \mathbb{N}_0$).

$\mathcal{M}$ je modelem teorie T, právě když je symbol $*$ realizován jako standardní násobení na $\mathbb{N}_0$. (‡)

Kapitola 9

Dokazovací systém predikátové logiky

Stejně jako u výrokové logiky (viz kapitola 4) zavádíme pojem dokazovacího systému, abychom podchytili platnost a způsob vytváření úsudků v predikátové logice. Chceme tedy mít k dispozici soubor pravidel pro přepisování formulí takový, že nějakou formuli φ lze odvodit z nějaké teorie T právě když $T \models \varphi$. Uvědomme si, že v predikátové logice je otázka, zda $T \models \varphi$, vysoce netriviální už v případě kdy T je prázdná teorie. Zatímco ve výrokové logice stačilo k ověření $\models \varphi$ projít všechny valuace různé na proměnných vyskytujících se ve φ (těch je konečně mnoho), v predikátové logice je potřeba ověřit, že φ je pravdivá v každé realizaci daného jazyka, přičemž těchto realizací je nekonečně mnoho. (A navíc některé realizace mají nekonečný nosič, čili samotné ověření, zda φ je pravdivá v dané realizaci, může být pro počítač neřešitelným úkolem.) Použití vhodného odvozovacího systému je tedy jedinou nadějí, jak automatizovat vytváření úsudků v predikátové logice.

Jak dále uvidíme, tuto naději je možné naplnit jen částečně. Gödelova věta o *úplnosti* ukazuje, že vskutku existuje odvozovací systém, v němž platí „$T \vdash \varphi$ právě když $T \models \varphi$“ (kde $\vdash$ značí relaci odvoditelnosti, či dokazatelnosti, v daném systému). To znamená, že problém, zda pro danou teorii T a formuli φ platí $T \models \varphi$ je *částečně rozhodnutelný*.[1] To znamená, že existuje algoritmus, který bude pro danou teorii T postupně vypisovat všechny formule z ní vyplývající (pokud je těchto formulí nekonečně mnoho, algoritmus nikdy neskončí) – algoritmus jednoduše bude na axiomy teorie T postupně aplikovat pravidla výše zmíněného odvozovacího systému a postupně tak

[1] Samozřejmě pouze za předpokladu, že je teorie T, pokud je nekonečná, nějakým způsobem reprezentovatelná v počítači.

bude odvozovat nové a nové formule vyplývající z T. Na druhou stranu, práce Alonza Churche a Alana Turinga z roku 1936[2] obecně ukazují, že problém, zda $T \models \varphi$, *není rozhodnutelný*, tj. neexistuje počítačový algoritmus, který by jej řešil. Nutno podotknout, že i přes toto omezení je automatické dokazování pro predikátovou logiku aktivně studováno a existují efektivní nástroje, které umí pro mnoho teorií a formulí (byť ne pro všechny) dokázat či vyvrátit, zda daná formule z dané teorie opravdu vyplývá.

V tomto předmětu studujeme následující odvozovací systém pro predikátovou logiku:

- Schémata výrokových axiómů:
  - P1: $\varphi \to (\psi \to \varphi)$
  - P2: $(\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi))$
  - P3: $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$
- Schéma axiómu specifikace:
  - P4: $\forall x\, \varphi \to \varphi(x/t)$, kde t je term substituovatelný za x ve φ.
- Schéma axiómu distribuce:
  - P5: $(\forall x\, (\varphi \to \psi)) \to (\varphi \to \forall x\, \psi)$, kde x nemá volný výskyt ve φ.
- Odvozovací pravidla:
  - MP: Z φ a $\varphi \to \psi$ odvoď ψ. (modus ponens)
  - GEN: Z φ odvoď $\forall x\, \varphi$, kde x je proměnná (generalizace)

Je-li $\mathcal{L}$ jazyk s rovností, přidáme dále následující schémata axiómů rovnosti:

- R1: $x = x$
- R2: $(x_1{=}y_1 \wedge \cdots \wedge x_n{=}y_n \wedge P(x_1, \cdots, x_n)) \to P(y_1, \cdots, y_n)$, kde P je predikátový symbol arity n.
- R3: $(x_1{=}y_1 \wedge \cdots \wedge x_m{=}y_m) \to (f(x_1, \cdots, x_m){=}f(y_1, \cdots, y_m))$, kde f je funkční symbol arity m.

[2] Oba byli ve své práci silně ovlivněni důkazem Gödelových vět o *neúplnosti*.

- Rovněž je zapotřebí následující schéma axiomů, které je možné neformálně chápat jako variantu schématu R2 pro rovnost:

$$(x = y \wedge u = v \wedge x = u) \to y = v.$$

  Toto schéma explicitně uvádíme, neboť formálně vzato $=$ není predikátový symbol a tak použitelnost tohoto schématu nevyplývá z toho, že máme k dispozici schéma R2. Přitom bez tohoto schématu není možné například dokázat symetrii rovnosti, která přitom platí v každé realizaci jazyka s rovností.

Definice 9.1 Buď T teorie jazyka $\mathcal{L}$. Důkaz (či odvození) formule ψ v teorii T je konečná posloupnost formulí $\varphi_1, \cdots, \varphi_k$, kde φ_k je ψ a pro každé φ_i, kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek:

- φ_i je prvek T;
- φ_i je instancí jednoho ze schémat P1–P5;
- $\mathcal{L}$ je jazyk s rovností a φ_i je instancí jednoho ze schémat R1–R3;
- φ_i vznikne aplikací MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.
- φ_i vznikne aplikací GEN na formuli φ_m pro vhodné $1 \leq m < i$.

Definice 9.2 Buď T teorie jazyka $\mathcal{L}$.

- Formule ψ je dokazatelná v teorii T, psáno $T \vdash \psi$, jestliže existuje důkaz ψ v T. Jestliže $T \vdash \psi$ pro prázdné T, říkáme že ψ je dokazatelná a píšeme $\vdash \psi$.
- Formule ψ je vyvratitelná v teorii T, jestliže $T \vdash \neg\psi$
- Teorie T je sporná (též inkonzistentní), jestliže každá formule predikátové logiky jazyka $\mathcal{L}$ je v T dokazatelná.
- Teorie je bezesporná (též konzistentní), jestliže není sporná.

Poznámka 9.3 (Princip dosazení do tautologie výrokového počtu) Je-li φ tautologií $\mathcal{L}(\neg, \to)$, ve které nahradíme výrokové proměnné formulemi predikátové logiky tak, že daná výroková proměnná je nahrazena vždy *touž* formulí, obdržíme formuli predikátové logiky, která je dokazatelná v odvozovacím systému predikátové logiky pouze pomocí P1–P3 a MP.

✿✿✿ **Příklad 9.1** Mějme jazyk $\mathcal{L} = \{P\}$ bez rovnosti, kde P je unární predikátový symbol. Nechť

$$T = \{\neg P(x), \exists y\, P(y)\}.$$

Ukažte, že teorie T je *sporná*.

Řešení Uvědomme si, že $\exists y\ P(y)$ je pouze syntaktickou zkratkou pro formuli $\neg\forall y\ \neg P(y)$ Ukážeme, že pro libovolnou formuli ψ jazyka $\mathcal{L}$ platí $T \vdash \psi$. Důkaz formule ψ v teorii T vypadá následovně:

1) $\neg P(x)$	axiom T
2) $\forall x \neg P(x)$	GEN na 1)
3) $\forall x \neg P(x) \to \neg P(y)$	instance P4
4) $\neg P(y)$	MP na 3) a 2)
5) $\forall y \neg P(y)$	GEN na 4)
6) $\neg\forall y\ \neg P(y)$	axiom T
7) $\neg\forall y\ \neg P(y) \to (\neg\psi \to \neg\forall y\ \neg P(y))$	instance P1
8) $\neg\psi \to \neg\forall y\ \neg P(y)$	MP na 7) a 6)
9) $(\neg\psi \to \neg\forall y\ \neg P(y)) \to (\forall y\ \neg P(y) \to \psi)$	instance P3
10) $\forall y\ \neg P(y) \to \psi$	MP na 9) a 8)
11) ψ	MP na 10) a 5).

Všimněme si, že v krocích 6)-11) jsme vůbec nevyužili konkrétní tvar formulí $\forall y \neg P(y)$ a $\neg\forall y \neg P(y)$. Využili jsme pouze faktu, že v teorii je odvoditelná nějaká formule a její negace. To ukazuje, že v každé teorii, ve které je možno dokázat nějakou formuli i její negaci, je možné dokázat libovolnou formuli. Taková teorie je tedy nutně sporná. ▲

✡✡✡ **Příklad 9.2** Mějme jazyk $\mathcal{L} = \{f, A\}$ s rovností, kde f je unární a A je nulární funkční symbol. Nalezněte důkaz formule $f(A) = A$ v teorii $\{A = f(A)\}$.

✡✡✡ **Příklad 9.3** Nechť $\mathcal{L}$ je jazyk s rovností s binárním predikátovým symbolem P. Rozhodněte a dokažte, zda platí

$$\vdash \forall x\ \forall y\ (x = y \to (P(x, y) \vee \exists z\ (\neg P(z, z)))).$$

Při práci s odvozovacím systémem pro predikátovou logiku lze využít následující pomocnou větu:

Věta 9.4 [o dedukci] Nechť T je teorie jazyka $\mathcal{L}$, ψ uzavřená formule jazyka $\mathcal{L}$ a φ (libovolná) formule jazyka $\mathcal{L}$. Pak $T \vdash \psi \to \varphi$ právě když $T \cup \{\psi\} \vdash \varphi$.

Následující věty ukazují, že pomocí výše uvedeného odvozovacího systému lze formalizovat právě všechny úsudky platné pro predikátovou logiku 1. řádu.

Věta 9.5 Nechť T je teorie a φ formule jazyka teorie T. Jestliže $T \vdash \varphi$, pak $T \models \varphi$.

Věta 9.6 Následující tvrzení jsou ekvivalentní:

a) Pro každou teorii T a pro každou formuli φ jazyka teorie T platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.

b) Každá bezesporná teorie má model.

Věta 9.7 [o úplnosti, Kurt Gödel] Každá bezesporná teorie má model. Pro každou teorii T a každou formuli jejího jazyka tedy (dle věty 9.6) platí, že jestliže $T \models \varphi$, pak $T \vdash \varphi$.

✿✿✿ **Příklad 9.4** Rozhodněte a dokažte, zda platí následující tvrzení: Pokud teorie má model, pak musí být bezesporná.

Řešení Tvrzení (možná poněkud překvapivě) neplatí. Protipříklad však existuje jen jeden a jde o velice speciální případ. Uvažme prázdný jazyk bez rovnosti a prázdnou teorii s tímto jazykem. Pak v této teorii lze triviálně dokázat libovolnou formuli daného jazyka, neboť daný jazyk žádné formule nemá. Teorie je tedy dle naší definice sporná. Na druhou stranu libovolná realizace daného jazyka (těch je dokonce nekonečně mnoho) je modelem prázdné teorie. ▲

Předchozí příklad ukazuje spíše na nedostatečnost našich definic. Pro „rozumné“ jazyky a teorie zmíněné tvrzení platí.

✿✿✿ **Příklad 9.5** Nechť $\mathcal{L}$ je libovolný jazyk, který je buď neprázdný nebo je jazykem s rovností. Dokažte, že pak pro každou splnitelnou teorii s jazykem $\mathcal{L}$ platí, že je bezesporná.

✿✿✿ **Příklad 9.6** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Mějme teorii T s jazykem $\mathcal{L}$ a její model $\mathcal{M}$. Dále nechť φ je formule v jazyce $\mathcal{L}$ taková, že platí $\mathcal{M} \models \varphi$. Platí $T \vdash \varphi$? Zdůvodněte.

✿✿✿ **Příklad 9.7** Nechť $\mathcal{L}$ je jazyk a T_1, T_2 jsou dvě bezesporné teorie v jazyce $\mathcal{L}$. Rozhodněte a dokažte, zda

a) teorie $T_1 \cup T_2$ je bezesporná;
b) teorie $T_1 \cap T_2$ je bezesporná.

Řešení

a) Tvrzení obecně neplatí. Uvažme prázdný jazyk s rovností a teorie $T_1 = \{\exists x \forall y\, x = y\}$ a $T_2 = \{\exists x \exists y\, x \neq y\}$. Zřejmě obě teorie jsou splnitelné a dle příkladu 9.5 jsou tedy bezesporné. Avšak sjednocení těchto teorií je nesplnitelná teorie a dle věty o úplnosti je tedy sporná.

b) Tvrzení platí. Uvědomme si, že v libovolném důkazu v teorii $T_1 \cap T_2$ se využívají pouze axiomy náležející jak do T_1 tak do T_2. Tedy libovolná formule dokazatelná v $T_1 \cap T_2$ je dokazatelná jak v T_1 tak v T_2. Pokud by tedy $T_1 \cap T_2$ byla sporná teorie, byly by i obě teorie T_1, T_2 sporné, (meta)spor.

▲

✩✩✩ **Příklad 9.8** Nechť $\mathcal{L}$ prázdný jazyk s rovností. Nechť $T_1, T_2, \ldots$ je posloupnost *sporných* teorií v jazyce $\mathcal{L}$ takovou, že pro každé $i \geq 1$ platí $T_{i+1} \subsetneq T_i$. Položme $S = \bigcap_{i=1}^{\infty} T_i$. Rozhodněte a dokažte, zda

a) S je sporná,
b) S je bezesporná.

✩✩ **Příklad 9.9** Dokažte, že z následujícího tvrzení (a) plyne tvrzení (b):

a) Nechť T je teorie a φ formule jejího jazyka. Pokud $T \models \varphi$, pak $T \vdash \varphi$.

b) Každá bezesporná teorie má model.

✩✩ **Příklad 9.10** Uvažme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Pro libovolné přirozené číslo $n \geq 1$ uvažme následující formule:

$$\varphi_n(x, y_1, y_2, \ldots, y_n) = \Big(\bigwedge_{1 \leq i < j \leq n} \neg(y_i = y_j) \wedge \bigwedge_{1 \leq i \leq n} R(x, y_i) \Big)$$

$$\theta_n = \forall x \forall y_1 \forall y_2 \ldots \forall y_{2n-1} (\varphi_{2n-1} \rightarrow \exists y_{2n}\ \varphi_{2n})$$

$$\xi_n = \exists x \exists y_1 \exists y_2 \ldots \exists y_{2n} \Big(\varphi_{2n} \wedge \forall z \big(R(x, z) \rightarrow \bigvee_{1 \leq i \leq 2n} (y_i = z) \big) \Big).$$

Nakonec ještě uvažme formuli

$$\rho = \forall x \exists y R(x, y).$$

Uvažme následující teorii T:

$$T = \{\theta_n \mid n \geq 1\} \cup \{\xi_n \mid n \geq 1\} \cup \{\rho\}.$$

Rozdhodněte, zda je teorie T bezesporná. Své tvrzení zdůvodněte.

Řešení Teorie T je bezesporná, neboť má model (a zároveň její jazyk je neprázdný, viz příklad 9.5). Abychom se o tom přesvědčili, uveďme nejprve intuitivní význam jednotlivých formulí. Nechť tedy $\mathcal{M}$ je libovolná realizace jazyka $\mathcal{L}$. *Následníkem* vrcholu $a \in M$ je libovolný takový vrchol $b \in M$, pro který je $(a, b) \in R_{\mathcal{M}}$.

Přejděme nyní ke slibovanému významu formulí. Nechť n je libovolné přirozené číslo a nechť $a, b_1, \ldots, b_n$ jsou takové prvky, že platí $\mathcal{M} \models \varphi_n[e]$, kde e je libovolné ohodnocení splňující $e(x) = a$ a $e(y_i) = b_i$ pro $1 \leq i \leq n$. Je zřejmé, že pak vrcholy $b_1, \ldots, b_n$ musí tvořit n po dvou různých následníků vrcholu a.

Nyní je jasné, že formule θ_n má následující význam: pro libovolný vrchol musí platit, že pokud jsme schopni najít $2n - 1$ různých následníků tohoto vrcholu, pak jsme schopni najít i $2n$ následníků tohoto vrcholu. Toto je ekvivalentní tvrzení, že žádný vrchol nemá *přesně* $2n - 1$ následníků. Z toho vyplývá, že v $\mathcal{M}$ jsou pravdivé všechny formule θ_n pro $n \geq 1$ právě tehdy, když žádný vrchol grafu $(M, R_{\mathcal{M}})$ nemá lichý počet následníků.

Formule ξ_n říká, že existuje vrchol, pro nějž umíme najít $2n$ jeho různých následníků a zároveň libovolný následník tohoto vrcholu je roven některému z těchto $2n$ následníků. Tedy jinak řečeno, že existuje vrchol který má přesně $2n$ následníků. Z toho vyplývá, že v realizaci $\mathcal{M}$ jsou pravdivé všechny formule ξ_n pro $n \geq 1$ právě tehdy, když pro každé sudé číslo k existuje v grafu $(M, R_{\mathcal{M}})$ alespoň jeden vrchol s přesně k následníky.

Konečně je zřejmé, že v $\mathcal{M}$ je pravdivá formule ρ právě tehdy, když každý vrchol grafu $(M, R_{\mathcal{M}})$ má alespoň jednoho následníka.

Rekapitulace: $\mathcal{M}$ je modelem teorie T právě tehdy, když v (potenciálně nekonečném) grafu $(M, R_{\mathcal{M}})$ platí všechny tyto tři vlastnosti:

- Neexistuje vrchol s lichým počtem následníků.
- Pro každé sudé číslo k existuje alespoň jeden vrchol s přesně k následníky.
- Každý vrchol má alespoň jednoho následníka.

Všechny tyto vlastnosti platí například v realizaci $\mathcal{M}$, kde $M = \mathbb{N}$ a

$$R_{\mathcal{M}} = \{(a, b) \mid a \text{ je liché}, b \geq a\} \cup \{(c, d) \mid c \text{ je sudé}, d \leq c\}.$$

▲

V důkazu věty o úplnosti se vyskytly dva zásadní pojmy týkající se teorií

– *henkinovskost*[3] a *úplnost*. Zatímco henkinovskost je spíše pomocným pojmem hodícím se v důkazu věty o úplnosti, pojem *úplné teorie* je významným sám o sobě.

Definice 9.8

- Teorie T je henkinovská, jestliže pro každou formuli φ jazyka teorie T s jednou volnou proměnnou x existuje v jazyce teorie T konstanta c taková, že $T \vdash \exists x\, \varphi \to \varphi(x/c)$.
- Teorie T je úplná, jestliže je bezesporná a pro každou uzavřenou formuli φ jejího jazyka platí buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.

Teorie je tedy úplná, jestliže každou formuli v ní lze buď dokázat, nebo vyvrátit. Podívejme se na pojem úplné teorie ještě optikou vět o korektnosti a úplnosti, které říkají, že $T \vdash \varphi$ právě když $T \models \varphi$. Z tohoto pohledu je teorie T úplná, jestliže každá „vlastnost“ popsatelná formulí daného jazyka je splněná buď ve všech modelech teorie T, nebo v žádném. Úplná teorie tedy popisuje své modely tak přesně, jak jen to je v jejím jazyce možné – žádné dva modely úplné teorie nelze rozlišit žádnou formulí jejího jazyka.

Pozor, nepleťme si pojem úplnosti teorie a úplnosti dokazovacího systému. Jde o dvě zcela odlišné věci. Gödelova věta o úplnosti se týká úplnosti dokazovacího systému, tedy toho, že každou formuli vyplývající z teorie lze v této teorii dokázat. Gödelovy věty o neúplnosti se naopak týkají (ne)úplnosti teorií. V podstatě říkají, že každá alespoň trochu zajímavá úplná teorie nemůže být reprezentovatelná počítačem.

✡✡✡ **Příklad 9.11** Mějme jazyk $\mathcal{L} = \{S\}$ s rovností, kde S je unární funkční symbol. Uvažme teorii

$$T = \{\forall x \forall y (S(x) = S(y) \to x = y), \exists y \forall x \neg (S(x) = y)\}$$

s tímto jazykem. Je T bezesporná? Je T úplná?

Řešení Z řešení příkladu 8.3 vidíme, že T je splnitelná. Z příkladu 9.5 plyne, že je i bezesporná.

Teorie T není úplná. Uvažme formuli $\varphi \equiv \forall x \neg (S(x) = x)$ z Příkladu 8.4. Ukázali jsme, že $T \not\models \varphi$. Na druhou stranu uvažme $\neg\varphi \equiv \exists x (S(x) = x)$. Model teorie T z Příkladu 8.3 ukazuje, že $T \not\models \neg\varphi$. Z věty o korektnosti plyne, že $T \nvdash \varphi$ a $T \nvdash \neg\varphi$ a tedy T není úplná teorie. ▲

[3] Podle Leona Henkina, amerického logika který objevil důkaz věty o úplnosti prezentovaný na přednášce – původní Gödelův důkaz je mnohem složitější.

✪✪✩ **Příklad 9.12** Je dán jazyk $\mathcal{L} = \{P, f\}$ s rovností, kde P je unární predikátový symbol a f je unární funkční symbol. Dále je dána jeho teorie $T = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, kde

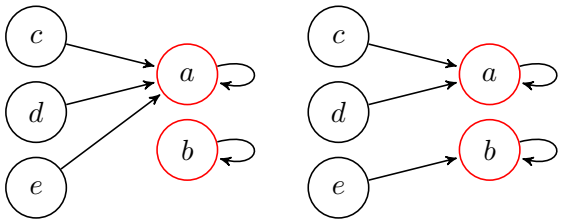
$$\begin{aligned}
\varphi_1 &= \exists x_1 \exists x_2 \exists x_3 \exists x_4 \exists x_5 \forall y \left(\bigwedge_{i=1}^{5} \bigwedge_{j=i+1}^{5} x_i \neq x_j \quad \wedge \quad \bigvee_{i=1}^{5} y = x_i \right), \\
\varphi_2 &= \exists x \exists y \forall z (x \neq y \wedge P(x) \wedge P(y) \wedge (P(z) \to (z = x \vee z = y))), \\
\varphi_3 &= \forall x (P(f(x))), \\
\varphi_4 &= \forall x (P(x) \to f(x) = x).
\end{aligned}$$

Rozhodněte a dokažte, zda je teorie T bezesporná a zda je úplná.

Řešení Nejprve si rozebereme význam jednotlivých formulí teorie T: Uvažme libovolnou realizaci $\mathcal{M} = (M, P_{\mathcal{M}}, f_{\mathcal{M}})$ jazyka $\mathcal{L}$. Pro jednodušší vyjadřování a v souladu s níže uvedenými obrázky budeme individua $x \in P_{\mathcal{M}}$ označovat jako *červená*, ostatní pak jako *černá*.

Zřejmě $\mathcal{M} \models \varphi_1$, právě když M je pětiprvková. Podobně $\mathcal{M} \models \varphi_2$, právě když právě dvě individua jsou červená. Dále $\mathcal{M} \models \varphi_3$, právě když je obraz každého individua v $f_{\mathcal{M}}$ červený. A konečně $\mathcal{M} \models \varphi_4$, právě když všechna červená individua jsou pevnými body $f_{\mathcal{M}}$.

Uvažme následující modely $\mathcal{M}$, $\mathcal{M}'$ teorie T (formálně $M = M' = \{a, b, c, d, e\}$, $P_{\mathcal{M}} = P_{\mathcal{M}'} = \{a, b\}$, $f_{\mathcal{M}} = \{(a, a), (b, b), (c, a), (d, a), (e, a)\}$, $f_{\mathcal{M}'} = \{(a, a), (b, b), (c, a), (d, a), (e, b)\}$):



model $\mathcal{M}$ model $\mathcal{M}'$

Tyto modely zřejmě nejsou izomorfní (a jsou to — až na izomorfizmus — jediné modely naší teorie; to ale k vyřešení zadání vědět nepotřebujeme), a jsou dokonce rozlišitelné v naší predikátové logice: uvažme (uzavřenou) formuli $\varphi = \forall x\,(P(x) \to \exists y\,(\neg P(y) \wedge f(y) = x))$ — intuitivně: každé červené individuum má nějaký černý vzor. Zřejmě $\mathcal{M} \not\models \varphi$ a $\mathcal{M}' \models \varphi$, takže $\mathcal{M}' \not\models \neg\varphi$. Z toho dostáváme, že $T \not\models \varphi$ ani $T \not\models \neg\varphi$.

Podle věty o korektnosti tak $T \nvdash \varphi$ ani $T \nvdash \neg\varphi$.

Teorie T je tedy bezesporná (našli jsme formuli, která v T není dokazatelná), ale není úplná (našli jsme uzavřenou formuli takovou, že v T není dokazatelná ani ona, ani její negace). ▲

✿✿✿ **Příklad 9.13** Mějme jazyk $\mathcal{L} = \{f\}$ s rovností, kde f je unární funkční symbol. Mějme teorii

$$T = \{\forall x\, \forall y\, (f(x) = f(y) \to x = y)\}.$$

Rozhodněte a dokažte, zda platí následující tvrzení.

a) $T \models \forall x\, \neg(f(x) = x)$
b) Teorie T je bezesporná.
c) Teorie T je úplná.

✿✿✿ **Příklad 9.14** Mějme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Rozhodněte a dokažte, zda existuje *úplná* teorie T s jazykem $\mathcal{L}$ taková, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí:

$$\mathcal{M} \models T \quad \text{právě když} \quad (M, R_{\mathcal{M}}) \text{ je lineárně uspořádaná množina.}$$

✿✿✿ **Příklad 9.15** Mějme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Rozhodněte a dokažte, zda existuje *úplná* teorie T s jazykem $\mathcal{L}$ taková, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí:

$$\mathcal{M} \models T \text{ právě když } (M, R_{\mathcal{M}}) \text{ je lineárně uspořádaná tříprvková množina.}$$

Intuice nám říká, že odpověď na otázku z předchozího příkladu je „ano“. Stačí uvést teorii, která vynutí, aby $R_{\mathcal{M}}$ byla lineárně uspořádaná množina a aby nosič M byl tříprvkový. Pak žádné dva modely takové teorie nelze rozlišit formulí jazyka $\mathcal{L}$, neboť všechny modely vypadají „stejně“ – nosič má tři prvky a ty jsou lineárně uspořádány nad sebou. Je otázka, jak úplnost takové teorie formálně dokázat. Jeví se být žádoucím zavést pojem *homomorfismu realizací.*

Definice 9.9 Nechť $\mathcal{L}$ je nějaký jazyk a nechť $\mathcal{M}_1$, $\mathcal{M}_2$ jsou nějaké dvě realizace tohoto jazyka. Zobrazení $\Phi\colon M_1 \to M_2$ se nazývá homomorfismus z $\mathcal{M}_1$ do $\mathcal{M}_2$, jestliže jsou splněny následující podmínky:

- Pro libovolný n-ární funkční symbol f jazyka $\mathcal{L}$ a libovolnou n-tici individuí $a_1, \ldots, a_n$ z M_1 platí:

$$\Phi(f_{\mathcal{M}_1}(a_1, \ldots, a_n)) = f_{\mathcal{M}_2}(\Phi(a_1), \ldots, \Phi(a_n)).$$

- Pro libovolný n-ární predikátový symbol jazyka $\mathcal{L}$ a libovolnou n-tici individuí $a_1, \ldots, a_n$ z M_1 platí:[4]

$$(a_1, \ldots, a_n) \in P_{\mathcal{M}_1} \Leftrightarrow (\Phi(a_1), \ldots, \Phi(a_n)) \in P_{\mathcal{M}_2}$$

Je-li navíc Φ bijekce, řekneme, že jde o izomorfismus a že realizace $\mathcal{M}_1$ a $\mathcal{M}_2$ jsou izomorfní.

✩✩✩ **Příklad 9.16** Mějme jazyk $\mathcal{L}$ a dvě izomorfní realizace $\mathcal{M}_1$, $\mathcal{M}_2$ tohoto jazyka. Dokažte, že pak pro libovolnou uzavřenou formuli φ jazyka $\mathcal{L}$ platí $\mathcal{M}_1 \models \varphi \Leftrightarrow \mathcal{M}_2 \models \varphi$.

Řešení Nechť $\Phi\colon M_1 \to M_2$ je izomorfismus z M_1 do M_2. Pro libovolné ohodnocení $e\colon Var \to M_1$ uvažme ohodnocení $\Phi(e)\colon Var \to M_2$ definované tak, že pro libovolnou proměnnou x klademe $\Phi(e)(x) = \Phi(e(x))$.

Nejprve ukážeme, že pro libovolný term t jazyka $\mathcal{L}$ a libovolné ohodnocení $e\colon Var \to M_1$ platí $\Phi(t[e]) = t[\Phi(e)]$. Postupujeme indukcí vzhledem ke struktuře termu. Pokud t je proměnná x, pak $\Phi(t[e]) = \Phi(e(x)) = \Phi(e)(x) = t[\Phi(e)]$. Předpokládejme nyní, že t je tvaru $f(t_1, \ldots, t_n)$, kde f je n-ární funkční symbol a t_i, pro $1 \leq i \leq n$, je term pro který dokazovaná rovnost platí. Pak máme

$$\begin{aligned}\Phi(t[e]) &= \Phi(f_{\mathcal{M}_1}(t_1[e], \ldots, t_n[e])) = f_{\mathcal{M}_2}(\Phi(t_1[e]), \ldots, \Phi(t_n[e])) \\ &= f_{\mathcal{M}_2}(t_1[\Phi(e)], \ldots, t_n[\Phi(e)]),\end{aligned}$$

kde druhá rovnost plyne z toho, že Φ je homomorfismus a poslední rovnost z indukčního předpokladu. Rovnost $\Phi(t[e]) = t[\Phi(e)]$ tedy platí pro libovolný term t.

Dokažme nyní tvrzení ze zadání příkladu. Přesněji, dokážeme, že pro libovolnou formuli φ jazyka $\mathcal{L}$ a libovolné ohodnocení $e\colon Var \to M_1$ platí $\mathcal{M}_1 \models \varphi[e] \Leftrightarrow \mathcal{M}_2 \models \varphi[\Phi(e)]$. Vzhledem k tomu, že Φ je bijekce, tak přiřazení, které ohodnocení e přiřadí ohodnocení $\Phi(e)$, tvoří bijekci mezi množinou všech ohodnocení typu $Var \to M_1$ a množinou všech ohodnocení typu $Var \to M_2$ (rozmyslete si, proč!). Zejména tedy bude platit, že formule φ je pravdivá v $\mathcal{M}_1$ ve všech ohodnoceních, právě když je pravdivá v $\mathcal{M}_2$ ve všech ohodnoceních. Tím bude důkaz hotov.

Postupujeme indukcí vzhledem ke struktuře φ.

[4] V literatuře se často v následující definici používá metaimplikace namísto metaekvivalence, nám však tato silnější definice ušetří trochu práce.

Báze: Musíme rozlišit dva případy. Za prvé, formule φ může být tvaru $P(t_1, \ldots, t_n)$, kde P je n-ární predikátový symbol a $t_1, \ldots, t_n$ jsou termy jazyka $\mathcal{L}$. Pak pro libovolné ohodnocení $e\colon Var \to M_1$ platí

$$\begin{aligned}\mathcal{M}_1 \models \varphi[e] &\Leftrightarrow (t_1[e], \ldots, t_n[e]) \in P_{\mathcal{M}_1} \Leftrightarrow (\Phi(t_1[e]), \ldots, \Phi(t_n[e])) \in P_{\mathcal{M}_2} \\ &\Leftrightarrow (t_1[\Phi(e)], \ldots, t_n[\Phi(e)]) \in P_{\mathcal{M}_2} \Leftrightarrow \mathcal{M}_2 \models \varphi[\Phi(e)],\end{aligned}$$

kde druhá ekvivalence plyne z toho, že Φ je homomorfismus a třetí ekvivalence plyne z výše dokázaného pomocného tvrzení o termech.
Za druhé, φ může být tvaru $t = t'$, kde t, t' jsou termy. Pak

$$\begin{aligned}\mathcal{M}_1 \models \varphi[e] &\Leftrightarrow t[e] = t'[e] \Leftrightarrow \Phi(t[e]) = \Phi(t'[e]) \Leftrightarrow t[\Phi(e)] = t'[\Phi(e)] \\ &\Leftrightarrow \mathcal{M}_2 \models \varphi[\Phi(e)],\end{aligned}$$

kde druhá ekvivalence plyne z toho, že Φ je injekce a třetí ekvivalence plyne z výše dokázaného tvrzení o termech.

Indukční krok: Nejprve předpokládejme, že φ je tvaru $\neg\psi$, kde ψ je formule pro níž dokazované tvrzení platí. Pak pro libovolné ohodnocení $e\colon Var \to M_1$ platí

$$\mathcal{M}_1 \models \varphi[e] \Leftrightarrow \mathcal{M}_1 \not\models \psi[e] \Leftrightarrow \mathcal{M}_2 \not\models \psi[\Phi(e)] \Leftrightarrow \mathcal{M}_2 \models \varphi[\Phi(e)],$$

kde druhá ekvivalence plyne z indukčního předpokladu.

Případ, kdy φ je tvaru $\psi_1 \to \psi_2$ se vyřeší obdobně. (Vyzkoušejte si to.)

Nakonec uvažme případ kdy φ je tvaru $\forall x\psi$, kde ψ je formule pro níž dokazované tvrzení platí. Pak máme, pro libovolné ohodnocení $e\colon Var \to M_1$

$$\begin{aligned}\mathcal{M}_1 \models \varphi[e] &\Leftrightarrow \mathcal{M}_1 \models \psi[e(x/a)] \text{ pro lib. } a \in M_1 \\ &\Leftrightarrow \mathcal{M}_2 \models \psi[\Phi(e(x/a))] \text{ pro lib. } a \in M_1 \\ &\Leftrightarrow \mathcal{M}_2 \models \psi[(\Phi(e))(x/b)] \text{ pro lib. } b \in M_2 \\ &\Leftrightarrow \mathcal{M}_2 \models \varphi[\Phi(e)],\end{aligned}$$

kde druhá ekvivalence plyne z toho, že Φ je homomorfismus a třetí ekvivalence z toho, že $\Phi(e(x/a)) = (\Phi(e))(x/\Phi(a))$ a z toho, že Φ je surjekce a tedy libovolné $b \in M_2$ lze psát ve tvaru $\Phi(a)$ pro vhodné $a \in M_1$.

Tím je požadované tvrzení dokázáno pro libovolnou formuli φ. ▲

✪✪✪ **Příklad 9.17** Nechť T je teorie jejíž každé dva modely jsou izomorfní. Dokažte, že pak teorie T je úplná.

Řešení Sporem předpokládejme, že existuje uzavřená formule φ jazyka teorie T taková, že $T \nvdash \varphi$ a zároveň $T \nvdash \neg\varphi$. Dle věty o úplnosti platí $T \not\models \varphi$ a $T \not\models \neg\varphi$. Zejména tedy existují modely $\mathcal{M}_1$ a $\mathcal{M}_2$ teorie T takové, že $\mathcal{M}_1 \not\models \varphi$ a $\mathcal{M}_2 \not\models \neg\varphi$. Dle příkladu 7.2 navíc platí $\mathcal{M}_2 \models \varphi$, neboť φ je uzavřená formule.

Dle předpokladu jsou realizace $\mathcal{M}_1$ a $\mathcal{M}_2$ izomorfní, dle příkladu 9.16 tedy musí platit že formule φ je pravdivá buď v obou těchto realizacích, nebo ani v jedné z nich. V předchozím odstavci jsme však ukázali, že φ je pravdivá v $\mathcal{M}_1$ a nikoliv v $\mathcal{M}_2$, spor. ▲

Poznámka 9.10 Vztah „být izomorfní“ je tranzitivní. Otázka, zda jsou libovolné dva modely teorie T izomorfní je tedy ekvivalentní otázce, zda existuje model teorie T, kterému je každý jiný model této teorie izomorfní.

Poznámka 9.11 Nyní již máme návod na to, jak vyřešit příklad 9.15. Stačí uvážit teorii

$$\begin{aligned} T = \{&\exists x_1 \exists x_2 \exists x_3 \forall y \,(\bigwedge_{1 \le i < j \le 3} (x_i \neq x_j) \wedge \bigvee_{1 \le i \le 3} y = x_i),\ \forall x\, R(x,x),\\ &\forall x \forall y \forall z\, ((R(x,y) \wedge R(y,z)) \to R(x,z)),\\ &\forall x \forall y\, ((R(x,y) \wedge R(y,x)) \to x = y),\\ &\forall x \forall y (R(x,y) \vee R(y,x))\}. \end{aligned}$$

Snadno se ukáže, že modely této teorie jsou právě realizace jazyka $\mathcal{L}$ s tříprvkovým nosičem, v nichž se R interpretuje jako relace lineárního uspořádání na nosiči. Rovněž je snadné vidět, že libovolné dvě takové realizace jsou izomorfní a tedy dle příkladu 9.17 je teorie T úplná.

✩✩✩ **Příklad 9.18** Mějme jazyk $\mathcal{L}$ *bez rovnosti* a dvě realizace $\mathcal{M}_1$, $\mathcal{M}_2$ jazyka $\mathcal{L}$. Předpokládejme, že existuje *surjektivní homomorfismus* z $\mathcal{M}_1$ do $\mathcal{M}_2$. Dokažte, že pak pro libovolnou uzavřenou formuli φ jazyka $\mathcal{L}$ platí $\mathcal{M}_1 \models \varphi$ právě když $\mathcal{M}_2 \models \varphi$.

✩✩ **Příklad 9.19** S pomocí předchozího příkladu dokažte následující: Mějme teorii T s jazykem $\mathcal{L}$ bez rovnosti. Předpokládejme, že existuje model $\mathcal{M}$ teorie T takový, že pro libovolný jiný model $\mathcal{M}'$ teorie T existuje surjektivní homomorfismus z $\mathcal{M}'$ do $\mathcal{M}$. Pak teorie T je úplná.

Dodejme, že v příkladech 9.17 a 9.19 nelze obecně nahradit implikaci ekvivalencí. Vskutku, existují úplné teorie které mají navzájem neizomorfní modely a zároveň nemají jeden konkrétní model, na nějž by šly ostatní modely zobrazit surjektivním homomorfismem.

✪✪✩ **Příklad 9.20** Uvažme jazyk $\mathcal{L} = \{A\}$ s rovností, kde A je binární funkční symbol. Uvažme následující teorii T:

$$\begin{aligned} T = \{&\exists x \exists y((x \neq y) \wedge \forall z((x = z) \vee (y = z))), \\ &\exists x \forall y A(x, y) = x, \\ &\forall x \forall y (A(x, y) = A(y, x)), \\ &\forall x A(x, x) = x\}. \end{aligned}$$

Rozhodněte, zda je teorie T úplná. Své tvrzení zdůvodněte.

Řešení Ukážeme, že zadaná teorie má až na izomorfismus právě jeden model. Dle příkladu 9.17 je tedy úplná.

Stačí ukázat, že libovolné dva modely teorie T jsou izomorfní.

Nejprve si uvědomme, že formule $\exists x \exists y((x \neq y) \wedge \forall z((x = z) \vee (y = z)))$ vynucuje, že každý model teorie T má právě dvouprvkový nosič. Ze zbývajících formulí teorie T plyne, že funkční symbol A musí být realizován jako komutativní a idempotentní operace, vůči které existuje neutrální prvek. Zejména realizace $\mathcal{M}$ v níž se A realizuje jako operace zadaná následující tabulkou, je modelem teorie T.

Uvažme nyní libovolný, ale nadále pevný model $\mathcal{M}'$ teorie T. Ukážeme, že je izomorfní modelu $\mathcal{M}$. Bez újmy na obecnosti nechť je jeho nosičem soubor $\{\alpha, \beta\}$. Z výše uvedeného vyplývá, že funkční symbol A může být v $\mathcal{M}'$ realizován dvěma způsoby:

$A_{\mathcal{M}'}$	α	β
α	α	α
β	α	β

nebo

$A_{\mathcal{M}'}$	α	β
α	α	β
β	β	β

V prvním případě volíme izomorfismus následovně: $\Phi(a) = \alpha$, $\Phi(b) = \beta$. Ve druhém případě volíme izomorfismus takto: $\Phi(a) = \beta$, $\Phi(b) = \alpha$. ▲

✪✪✩ **Příklad 9.21** Mějme jazyk $\mathcal{L} = \{f, a, b\}$ s rovností, kde f je unární funkční symbol a a a b jsou nulární funkční symboly. Mějme teorii

$$T = \{\forall x\ (x = a \vee x = b),\ \neg(f(a) = f(b)),\ \forall x\ f(f(x)) = x\}.$$

Rozhodněte a dokažte, zda je teorie T úplná.

Řešení Teorie T není úplná. Uvažme formuli $\varphi = \forall x\, f(x) = x$. Ukážeme, že $T \nvdash \varphi$ a zároveň $T \nvdash \neg\varphi$. Dle věty o korektnosti stačí ukázat, že $T \not\models \varphi$ a zároveň $T \not\models \neg\varphi$. Uvažme realizace $\mathcal{M}_1$, $\mathcal{M}_2$ jazyka $\mathcal{L}$ definované následovně:

$$\begin{array}{llllll} M_1 = \{\alpha, \beta\} & a_{\mathcal{M}_1} = \alpha & b_{\mathcal{M}_1} = \beta & f_{\mathcal{M}_1}(\alpha) = \beta & f_{\mathcal{M}_1}(\beta) = \alpha \\ M_2 = \{\alpha, \beta\} & a_{\mathcal{M}_2} = \alpha & b_{\mathcal{M}_2} = \beta & f_{\mathcal{M}_2}(\alpha) = \alpha & f_{\mathcal{M}_2}(\beta) = \beta. \end{array}$$

Obě dvě realizace jsou modelem teorie T: V obou je každý prvek nosiče realizací některé z konstant a, b; realizace funkčního symbolu f zobrazí prvky reprezentované různými konstantami na různé prvky nosiče, a term $f^(x)$ se realizuje jako identita. Zároveň $\mathcal{M}_1 \not\models \varphi$ ($f_{\mathcal{M}_1}$ není identita) a $\mathcal{M}_2 \not\models \neg\varphi$ ($f_{\mathcal{M}_2}$ je identita). Tím je důkaz hotov. ▲

✿✿ **Příklad 9.22** Mějme jazyk $\mathcal{L} = \{P, f, a, b\}$ s rovností, kde P je unární predikátový symbol, f je unární funkční symbol a a a b jsou nulární funkční symboly. Mějme teorii

$$\begin{aligned} T = \{ & P(x) \leftrightarrow (x = a \vee x = b),\ \exists x \forall y\, (\neg P(y) \rightarrow y = x), \\ & P(x) \rightarrow \big(P(f(x)) \wedge \neg(x = f(x))\big)\ \}. \end{aligned}$$

Rozhodněte a dokažte, zda je teorie T úplná.

✿✿ **Příklad 9.23** Nechť $\mathcal{L}$ je jazyk s rovností a s jedním unárním funkčním symbolem f. Rozhodněte a dokažte, zda je následující teorie úplná.

$$T \quad = \quad \{\, \forall x\, \forall y\, f(x) = f(y)\ \}.$$

✿✿ **Příklad 9.24** Mějme jazyk $\mathcal{L} = \{f\}$ s rovností, kde f je unární funkční symbol. Mějme dále následující teorii T s jazykem $\mathcal{L}$:

$$\begin{aligned} T = \Big\{ & \exists x_1 \exists x_2 \exists x_3 \exists x_4 \forall y\, \big(\big(\bigwedge_{1 \le i < j \le 4} x_i \neq x_j\big) \wedge \big(\bigvee_{1 \le k \le 4} y = x_k\big)\big), \\ & \forall x \forall y (f(x) = f(y) \rightarrow x = y),\ \forall x (x \neq f(x))\Big\}. \end{aligned}$$

Rozhodněte a dokažte, zda je teorie T úplná.

✿✿ **Příklad 9.25** Mějme jazyk $\mathcal{L} = \{M, f\}$ s rovností, kde f je unární funkční symbol. Mějme dále následující teorii T s jazykem $\mathcal{L}$:

$$T = \Big\{\exists x_1\exists x_2\exists x_3\exists x_4\forall y(\bigwedge_{1\le i<j\le 4} x_i \neq x_j) \wedge (\bigvee_{1\le k\le 4} y = x_k),$$
$$\exists x_1\exists x_2\,(x_1 \neq x_2 \wedge \forall y\,(M(y) \leftrightarrow (y = x_1 \vee y = x_2))),$$
$$\forall x\big(M(x) \to \neg M(f(x))\big), \forall x\big(\neg M(x) \to (f(x) = x)\big)\Big\}.$$

Rozhodněte a dokažte, zda je teorie T úplná.

✪✩✩ **Příklad 9.26** Nechť $\mathcal{L}$ je prázdný jazyk s rovností (tedy jazyk s rovností, který nemá žádný predikátový ani funkční symbol).

a) Zadejte příklad bezesporné teorie, která není úplná. Zdůvodněte, proč není úplná.

b) Rozhodněte a dokažte, zda existují dvě úplné teorie T_1 a T_2 takové, že $T_1 \cap T_2 = \emptyset$.

✪✪✩ **Příklad 9.27** Nechť $\mathcal{L}$ je jazyk bez rovnosti s jedním unárním predikátovým symbolem P a jedním nulárním funkčním symbolem 0. Rozhodněte a dokažte, jestli je teorie $T = \{P(0)\}$

a) bezesporná,

b) úplná.

✪✪✩ **Příklad 9.28** Mějme jazyk $\mathcal{L} = \{P\}$ bez rovnosti s unárním predikátovým symbolem P. Nechť

$$T = \{P(x),\ \exists x\ (\neg P(x))\}.$$

Rozhodněte a dokažte, zda je teorie T

a) bezesporná,

b) úplná.

✪✪✩ **Příklad 9.29** Mějme jazyk $\mathcal{L} = \{P\}$ bez rovnosti s unárním predikátovým symbolem P. Nechť

$$T = \{\exists x\ P(x),\ \exists x\ (\neg P(x))\}.$$

Rozhodněte a dokažte, zda je teorie T

a) bezesporná,

b) úplná.

Dalším důležitým syntaktickým pojmem je pojem *rozšíření teorie*.

Definice 9.12

- Teorie S je rozšíření teorie T, jestliže jazyk teorie S obsahuje jazyk teorie T a v teorii S jsou dokazatelné všechny axiómy teorie T.
- Rozšíření S teorie T se nazývá konzervativní, jestliže každá formule jazyka teorie T, která je dokazatelná v S, je dokazatelná i v T.
- Teorie S a T jsou ekvivalentní, jestliže S je rozšířením T a současně T je rozšířením S.

✡✡✡ **Příklad 9.30** Mějme teorie T a S se stejným jazykem takové, že S je rozšířením T. Dokažte, že pak každý model teorie S je modelem teorie T.

✡✡✡ **Příklad 9.31** Uvažme jazyk $\mathcal{L} = \{P\}$ s rovností, kde P je binární predikátový symbol. Uvažme následující teorie T a S:

$$T = \{\forall x \forall y (P(x,y) \leftrightarrow P(x,x))\},$$
$$S = \{\forall x \forall y (P(x,y) \leftrightarrow P(y,x))\}.$$

Rozhodněte a dokažte, zda je:

a) teorie S rozšířením teorie T,

b) teorie T rozšířením teorie S.

Řešení

a) Odpověď je ne. Musíme ukázat, že $S \nvdash \forall x \forall y (P(x,y) \leftrightarrow P(x,x))$. Dle věty o korektnosti stačí ukázat, že $S \not\models \forall x \forall y (P(x,y) \leftrightarrow P(x,x))$. Najdeme tedy model $\mathcal{M}$ teorie S, pro který platí $\mathcal{M} \not\models \forall x \forall y (P(x,y) \leftrightarrow P(x,x))$. Jako nosič realizace $\mathcal{M}$ zvolíme množinu $\{a,b\}$ a jako realizaci $P_{\mathcal{M}}$ predikátového symbolu P zvolíme binární relaci $\{(a,b),(b,a)\}$. Zjevně platí $\mathcal{M} \models S$. Dále $\mathcal{M} \models P(x,y)[e(x/a)(y/b)]$, kde e je libovolná valuace. Ale $\mathcal{M} \not\models P(x,x)[e(x/a)(y/b)]$, tedy z definice $\models$ platí $\mathcal{M} \not\models \forall x \forall y (P(x,y) \leftrightarrow P(x,x))$.

b) Odpověď je opět ne. Stejně jako výše stačí najít model $\mathcal{M}$ teorie T splňující $\mathcal{M} \not\models \forall x \forall y (P(x,y) \leftrightarrow P(y,x))$. Jako nosič realizace $\mathcal{M}$ zvolme opět množinu $\{a, b\}$ a jako realizaci $P_{\mathcal{M}}$ predikátového symbolu P zvolme binární relaci $\{(a,b),(a,a)\}$. Pak platí $\mathcal{M} \models T$, stačí si uvědomit, že $\mathcal{M} \models P(x,y)[e]$ právě když $e(x) = a$, což nastane právě když $\mathcal{M} \models P(x,x)[e]$. Ale $\mathcal{M} \not\models \forall x \forall y (P(x,y) \leftrightarrow P(y,x))$, neboť relace $P_{\mathcal{M}}$ není symetrická.

▲

✡✡✡ **Příklad 9.32** Mějme prázdný jazyk $\mathcal{L}$ s rovností a teorii v jazyce $\mathcal{L}$

$$T = \{\ \exists x\ \exists y\ \neg(x = y)\ \}.$$

Dále mějme jazyk $\mathcal{L}' = \{c, d\}$ s rovností, kde c, d jsou nulární funkční symboly, a teorii v jazyce $\mathcal{L}'$

$$T' = \{\ \neg(c = d)\ \}.$$

Rozhodněte a dokažte, zda je teorie T' konzervativním rozšířením teorie T.

Řešení Teorie T' je konzervativní rozšíření teorie T.

- T' je rozšíření T, pokud $T' \vdash \exists x\ \exists y\ \neg(x = y)$. Z věty o úplnosti stačí ukázat, že $T' \models \exists x\ \exists y\ \neg(x = y)$. Předpokládejme, že existuje model $\mathcal{M}$ teorie T' takový, že $\mathcal{M} \not\models \exists x\ \exists y\ \neg(x = y)$. Pak ovšem nosič modelu $\mathcal{M}$ má právě jeden prvek, tedy $c_M = d_M$ a nemůže platit $\mathcal{M} \models T'$, spor.
- T' je *konzervativní* rozšíření T, pokud pro každou formuli φ v jazyce $\mathcal{L}$ platí, že pokud $T' \vdash \varphi$, pak i $T \vdash \varphi$. Uvažme tedy libovolnou formuli φ v jazyce $\mathcal{L}$ takovou, že $T' \vdash \varphi$. Z věty o korektnosti je formule φ pravdivá v každém modelu teorie T'. Z věty o úplnosti nám stačí ukázat, že φ je také pravdivá v každém modelu teorie T.
  Vezměme libovolný model $\mathcal{M}$ teorie T. Nosič M modelu $\mathcal{M}$ má zjevně alespoň dva prvky, označme je a, b. Definujme rozšířenou realizaci $\mathcal{M}'$ s nosičem $M' = M$ a konstantami $c_{M'} = a$ a $d_{M'} = b$. Zjevně je $\mathcal{M}'$ modelem teorie T', tedy $\mathcal{M}' \models \varphi$. Protože formule φ je v jazyce $\mathcal{L}$, nevyskytují se v ní konstanty c a d, tudíž je φ pravdivá i v původní realizaci $\mathcal{M}$.

▲

Řešení [první část přes odvozovací systém] Mnohem pracněji je možné postupovat následovně. Budeme potřebovat následující pomocné tvrzení, které lze dokázat podobně jako větu 37 (d) ve slajdech.

Tvrzení 9.13 Nechť $\mathcal{L}$ je libovolný jazyk, T teorie v jazyce $\mathcal{L}$ a φ, ψ libovolné uzavřené formule v jazyce $\mathcal{L}$. Pak $T \vdash (\varphi \to \neg\psi) \to (\psi \to \neg\varphi)$.

$\exists x \exists y \neg(x = y)$ je zkratka pro formuli $\neg\forall x \neg\neg\forall y \neg\neg(x = y)$, již dokážeme z T':

1)	$\forall y \neg\neg(c = y) \to \neg\neg(c = d)$	P4
2)	$T' \vdash (\forall y\ \neg\neg(c = y) \to \neg\neg(c = d)) \to$ $(\neg(c = d) \to \neg\forall y\ \neg\neg(c = y))$	Tvrzení 9.13
3)	$\neg(c = d) \to \neg\forall y \neg\neg(c = y)$	MP na 1), 2)
4)	$\neg(c = d)$	
5)	$\neg\forall y \neg\neg(c = y)$	MP na 3), 4)
6)	$\forall x \neg\neg\forall y \neg\neg(x = y) \to \neg\neg\forall y \neg\neg(c = y)$	P4
7)	$T' \vdash (\forall x \neg\neg\forall y \neg\neg(x = y) \to \neg\neg\forall y \neg\neg(c = y)) \to$ $(\neg\forall y \neg\neg(c = y) \to \neg\forall x \neg\neg\forall y \neg\neg(x = y))$	Tvrzení 9.13
8)	$\neg\forall y \neg\neg(c = y) \to \neg\forall x \neg\neg\forall y \neg\neg(x = y)$	MP na 6), 7)
9)	$\neg\forall x \neg\neg\forall y \neg\neg(x = y)$	MP na 5), 8)

▲

Příklad 9.33

10 Nechť L je jazyk s rovností. O každém z následujících dvou tvrzení rozhodněte, zda je pravdivé.

a) Nechť T je teorie s jazykem L. Nechť S je *bezesporná* teorie, která je rozšířením teorie T. Pak S je *konzervativním* rozšířením T.

b) Nechť T je **úplná** teorie s jazykem L. Nechť S je *bezesporná* teorie, která je rozšířením teorie T. Pak S je *konzervativním* rozšířením T.

Svá tvrzení zdůvodněte.

✩✩ **Příklad 9.34** Mějme jazyk $\mathcal{L} = \{P\}$ s rovností, kde P je unární predikátový symbol. Dále mějme teorie $S = \{P(x) \leftrightarrow P(y)\}$ a $T = \{x = y\}$ s jazykem $\mathcal{L}$.

a) Je T rozšíření teorie S?

b) Je T *konzervativní* rozšíření teorie S?

✡✡✡ **Příklad 9.35** Nechť $\mathcal{L}$ je jazyk s rovností a s jedním unárním predikátovým symbolem P. Dále nechť T je teorie s jazykem $\mathcal{L}$. Nalezněte rozšíření T' teorie T takové, že pro každou realizaci $\mathcal{M}$ platí, že $\mathcal{M} \models T$, právě když $\mathcal{M} \models T$ a zároveň $P_M = M$. Rozhodněte a dokažte, zda je takové rozšíření konzervativní.

✡✡✡ **Příklad 9.36** Nechť $\mathcal{L} = \{f, P, c\}$ je jazyk s rovností, kde f je unární funkční symbol, P je unární predikát a c je nulární funkční symbol. Uvažme následující teorii v jazyce $\mathcal{L}$

$$T = \{\, \exists x\, \neg(f(x) = x),\ \exists x\, P(x),\ \exists x\, \neg P(x)\}.$$

Zadejte nějakou *konkrétní* [5] úplnou teorii S, která je rozšířením teorie T. Dokažte, že S je rozšířením teorie T a že S je úplná teorie.

Řešení Položme

$$S = T \cup \{\, \underbrace{\exists x\, \exists y\, \forall z\, (z = x \vee z = y)}_{\text{nanejvýš 2 prvky}},\ \underbrace{\forall x\, f(x) = c}_{f \text{ je konstantní}},\ P(c)\ \}.$$

S je rozšíření T, protože $T \subseteq S$, tedy každý axiom z T lze v S snadno dokázat. S je bezesporná, protože následující realizace $\mathcal{M}$ je zjevně modelem teorie S.

$$M = \{a, b\},\ c_M = a,\ f_M(a) = a,\ f_M(b) = a,\ P_M = \{a\}.$$

Teorie S je úplná, neboť lze snadno každý její model je izomorfní výše uvedenému modelu $\mathcal{M}$ (viz. příklad 9.17). To lze snadno ověřit: zřejmě každý model $\mathcal{M}'$ teorie S má přesně dvouprvkový nosič, označme jej $\{\alpha, \beta\}$; právě jeden z těchto prvků (ten reprezentovaný konstantou c – bez újmy na obecnosti nechť je to prvek α) náleží do $P_{\mathcal{M}'}$ (protože $P_{\mathcal{M}'} \neq M'$, což vynucuje teorie T) a funkce $f_{\mathcal{M}'}$ zobrazí všechny prvky na uvedený prvek α. V takovém případě stačí zvolit izomorfismus $\Phi(\alpha) = a$, $\Phi(\beta) = b$. ▲

✡✡✡ **Příklad 9.37** Uvažme jazyk $\mathcal{L} = \{R\}$ s rovností, kde R je binární predikátový symbol. Dále uvažme následující teorii T s jazykem $\mathcal{L}$:

$$T \quad = \quad \{\forall x \forall y\, (R(x, y) \to \forall z (R(x, z) \to z = y))\}.$$

[5] Tedy nestačí odkázat na větu 74 ze slajdů.

Nyní uvažme jazyk $\mathcal{L}' = \mathcal{L} \cup \{f\}$ s rovností, kde f je unární funkční symbol, a teorii T' s tímto jazykem zadanou následovně:

$$T' \quad = \quad \{\forall x \forall y\,(R(x,y) \to f(y) = x), \forall x \forall y\,(x \neq y \to f(x) \neq f(y))\}.$$

Rozhodněte a dokažte, zda:

a) T' je rozšířením teorie T,

b) T' je konzervativním rozšířením teorie T.

Řešení Teorie T' je rozšíření teorie T, které ovšem není konzervativní.

Nejprve ukážeme, že T' je rozšířením teorie T. Zřejmě jazyk teorie T' obsahuje jazyk teorie T, stačí tedy ukázat, že

$$T' \vdash \forall x \forall y\,(R(x,y) \to \forall z(R(x,z) \to z = y)).$$

Označme tuto formuli (jediný axiom teorie T) jako φ. Dle věty o úplnosti stačí ukázat, že $T' \models \varphi$.

Sporem předpokládejme, že existuje model $\mathcal{M}$ teorie T' takový, že $\mathcal{M} \not\models \varphi$. Z Tarského definice pravdivosti plyne, že musí existovat trojice individuí a, b, c v nosiči $\mathcal{M}$ takových, že $(a,b) \in R_{\mathcal{M}}$, $(a,c) \in R_{\mathcal{M}}$ a $b \neq c$. Protože $\mathcal{M} \models T'$, musí platit $f_{\mathcal{M}}(b) = a$ a $f_{\mathcal{M}}(c) = a$ (vynucuje to první axiom teorie T'). To ovšem není možné, neboť v každém modelu teorie T' se f realizuje jako injektivní funkce (vynucuje to druhý axiom teorie T'), spor.

Nyní ukážeme, že T' *není* konzervativním rozšířením teorie T. Dle definice musíme najít formuli ψ jazyka $\mathcal{L}$ takovou, že $T \not\vdash \psi$ a $T' \vdash \psi$. Uvažme formuli $\psi = \forall x \forall y \forall z\,((R(x,z) \wedge R(y,z)) \to x = y)$. Neformálně řečeno, formule ψ říká, že R se má realizovat jako relace, jejíž inverze je parciální funkce. Dle vět o korektnosti, resp. o úplnosti, stačí ukázat, že $T \not\models \psi$, resp. $T' \models \psi$.

Nejprve ukážeme, že $T \not\models \psi$. Uvažme realizaci $\mathcal{M}_1$ jazyka $\mathcal{L}$ danou následovně:

- jejím nosičem je soubor $M = \{0, 1\}$,
- $R_{\mathcal{M}_1} = \{(0,0), (1,0)\}$.

Pak zřejmě $\mathcal{M}_1 \models T$ (neformálně řečeno, φ říká, že R se musí realizovat jakožto parciální funkce) avšak $\mathcal{M}_1 \not\models \psi$ (neboť $R^{-1}_{\mathcal{M}_1} = \{(0,0), (0,1)\}$ není parciální funkce). Tedy $T \not\models \psi$.

Nyní ukážeme, že $T' \models \psi$. Sporem předpokládejme, že existuje model $\mathcal{M}_2$ teorie T' takový,[6] že $\mathcal{M}_2 \not\models \psi$. Z Tarského definice pravdivosti plyne, že existují prvky a, b, c v nosiči realizace $\mathcal{M}_2$ takové, že $(a, c) \in R_{\mathcal{M}_2}$, $(b, c) \in R_{\mathcal{M}_2}$ a zároveň $a \neq b$. Pak ale musí platit $f_{\mathcal{M}_2}(c) = a$ a $_{\mathcal{M}_2}(c) = b$ (vynucuje to první axiom teorie T'), což není možné, neboť $f_{\mathcal{M}_2}$ je funkce, spor. Tím je důkaz hotov. ▲

✿✿ **Příklad 9.38** Nechť $\mathcal{L}$ je jazyk s rovností a jedním unárním predikátovým symbolem P. Pro teorie $A = \{\forall x\,(P(x))\}$ a $B = \{\forall x\,\forall y\,(x = y)\}$. Rozhodněte a dokažte, zda

a) teorie B je rozšíření teorie A,

b) teorie B je *konzervativní* rozšíření teorie A.

✿✿ **Příklad 9.39** Nechť $\mathcal{L} = \{f\}$ je jazyk s rovností, kde f je unární funkční symbol.

Mějme teorie

$$S = \{\ \forall x\ \forall y\ (f(x) = f(y)\ \rightarrow\ x = y)\ \},$$
$$T = \{\ \forall x\ \exists z\ (x = f(z) \wedge \forall y\ (x = f(y)\ \rightarrow\ z = y))\ \}.$$

Rozhodněte a dokažte zda

- T je rozšířením S,
- T je konzervativním rozšířením S.

✿✿ **Příklad 9.40** Mějme teorie S, T a U takové, že teorie T je rozšířením teorie S a teorie U je rozšířením teorie T. Dokažte, že pak teorie U je rozšířením teorie S.

✿✿ **Příklad 9.41** Z přednášky víme, že ke každé bezesporné teorii

- existuje henkinovská teorie, která je jejím konzervativním rozšířením,
- existuje úplná teorie ve stejném jazyce, která je jejím rozšířením.

S využitím výše uvedeného dokažte: ke každé bezesporné teorii T existuje úplná a henkinovská teorie, která je rozšířením T.

[6] Tj. $\mathcal{M}_2$ je realizace jazyka $\mathcal{L}'$

Kapitola 10

Věta o kompaktnosti

Důležitým důsledkem Gödelovy věty o úplnosti je věta o kompaktnosti. (Ve skutečnosti jsou tyto dvě věty ekvivalentní.)

Věta 10.1 [o kompaktnosti] Teorie T má model, právě když každá její podteorie s konečně mnoha axiómy (a s minimálním jazykem, v němž jsou tyto axiómy formulovatelné) má model.

Věta o kompaktnosti má několik zásadních způsobů použití. Lze pomocí ní ukázat existenci modelů teorie splňujících určité vlastnosti. Toto lze dále využít k důkazu nevyjádřitelnosti některých vlastností pomocí teorií predikátové logiky. Podrobněji viz příklady níže.

Než se dostaneme k příkladům, připomeňme si dva důležité důsledky věty o kompaktnosti dokázané na přednášce.

Věta 10.2 Nechť T je teorie a nechť pro každé $n \in \mathbb{N}$ existuje model teorie T jehož nosič má mohutnost alespoň n. Pak T má nekonečný model.

Věta 10.3 (Löwenheimova-Skolemova) Nechť T je teorie s jazykem L, která má nekonečný model. Nechť κ je nekonečný kardinál takový, že $\kappa \geq |\mathcal{L}|$. Pak T má model mohutnosti κ.

Z Löwenheimovy-Skolemovy věty mimo jiné plyne, že každá teorie, která má nekonečný model, má nekonečně mnoho navzájem neizomorfních modelů (modely s nosičem různé kardinality nemohou být izomorfní).

Následující příklad lze vyřešit i bez věty o kompaktnosti.

✡✡ **Příklad 10.1** Nechť T je konečná teorie s jazykem $\mathcal{L}$ obsahující pouze uzavřené formule. Dokažte, že existuje konečná teorie T' s jazykem $\mathcal{L}$ taková, že $\mathcal{M} \models T'$ právě tehdy, když $\mathcal{M} \not\models T$ pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$.

✡✡✡ **Příklad 10.2** Nechť $\mathcal{L}$ je libovolný jazyk. Rozhodněte a dokažte, zda existuje teorie T s jazykem $\mathcal{L}$ taková, že realizace $\mathcal{M}$ je modelem teorie T, právě když nosič $\mathcal{M}$ má konečný sudý počet prvků.

✡✡✡ **Příklad 10.3** Nechť $\mathcal{L}$ je libovolný jazyk. Rozhodněte a dokažte, zda existuje

a) teorie T s jazykem $\mathcal{L}$ taková,
b) *konečná* teorie T s jazykem $\mathcal{L}$ taková,

že realizace $\mathcal{M}$ je modelem teorie T, právě když nosič $\mathcal{M}$ má nekonečný nebo sudý počet prvků.

✡✡✡ **Příklad 10.4** Nechť $\mathcal{L}$ je prázdný jazyk s rovností. Rozhodněte a dokažte, zda existuje *konečná* teorie T s jazykem $\mathcal{L}$ taková, že jejími modely jsou právě realizace jazyka $\mathcal{L}$ s nekonečným nosičem.

✡✡✡ **Příklad 10.5** Nechť $\mathcal{L}$ je jazyk s rovností. Rozhodněte, zda platí následující tvrzení:

a) Existuje teorie T s jazykem $\mathcal{L}$ taková, že $\mathcal{M} \models T$ právě tehdy, když nosič $\mathcal{M}$ je konečný.

b) Existuje teorie T s jazykem $\mathcal{L}$ taková, že $\mathcal{M} \models T$ právě tehdy, když nosič $\mathcal{M}$ je nekonečný.

c) Existuje *konečná* teorie T s jazykem $\mathcal{L}$ taková, že $\mathcal{M} \models T$ právě tehdy, když nosič $\mathcal{M}$ je nekonečný.

Řešení

a) Odpověď: Ne! Zdůvodnění: Z přenášky víme, že platí následující tvrzení: Pokud pro každé n existuje model teorie T mohutnosti alespoň n, pak existuje i nekonečný model teorie T.

b) Odpověď: Ano! Zdůvodnění: Uvažme

$$T = \{\varphi_i \mid \varphi_i = \forall x_1 \cdots \forall x_i \exists y (\wedge_{j=1}^{i} \neg(x_j = y)), i \geq 1\}$$

Zřejmě platí, že $\mathcal{M} \models \varphi_i$ právě tehdy, když nosič $\mathcal{M}$ obsahuje více než i prvků.

c) Odpověď: Ne! Zdůvodnění: Předpokládejme, že T je taková teorie. Pak dle Příkladu 8.5 existuje konečná teorie T' taková, že $\mathcal{M} \models T'$ právě tehdy, když $\mathcal{M} \not\models T$ pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$. Avšak, modely teorie T' jsou právě realizace jazyka $\mathcal{L}$ s konečným nosičem, což je spor s 1.

▲

✡✡✡ **Příklad 10.6** Mějme libovolnou *konečnou* teorii T s jazykem $\mathcal{L}$ takovou, že každý *neprázdný vlastní* podsoubor T je splnitelný. Rozhodněte a dokažte, zda je T splnitelný.

✡✡✡ **Příklad 10.7** Mějme jazyk $\mathcal{L} = \{\sqsubseteq\}$ s rovností, kde $\sqsubseteq$ je binární predikátový symbol.

Rozhodněte a dokažte, zda existuje teorie T taková, že realizace $\mathcal{M}$ jazyka $\mathcal{L}$ je
modelem T, právě když $(M, \sqsubseteq_{\mathcal{M}})$ je uspořádaná množina s *konečně mnoha maximálními prvky.*

Pro připomenutí: Prvek x uspořádané množiny je *maximální*, pokud neexistuje žádný ostře větší prvek než x.

Řešení Taková teorie T neexistuje. Předvedeme dva alternativní metadůkazy sporem, jeden pomocí Věty 10.1 a jeden pomocí Věty 10.2.

Zaměřme se nejprve na důkaz pomocí věty o kompaktnosti. Předpokládejme, že hledaná teorie T vskutku existuje. Pro libovolné $n \in \mathbb{N}$ uvažme formuli

$$\psi_n = \exists x_1 \ldots \exists x_n \forall y \, (\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \bigwedge_{1 \leq i \leq n} (x_i \sqsubseteq y \to x_i = y)).$$

Neformálně řečeno, formule ψ_n vynucuje existenci alespoň n navzájem různých maximálních prvků. Dále uvažme teorii

$$T' = T \cup \{\psi_n \mid n \in \mathbb{N}\}.$$

Ukážeme, že teorie T' je splnitelná. To však bude spor, neboť v každém modelu $\mathcal{M}$ teorie T' je $(M, \sqsubseteq_{\mathcal{M}})$ uspořádanou množinou (neboť $\mathcal{M}$ je zároveň modelem teorie T) s nekonečně mnoha maximálními prvky (neboť $\mathcal{M} \models \psi_n$ pro všechna $n \in \mathbb{N}$). Protože však každý model teorie T' je modelem T, ze splnitelnosti T' plyne existence modelu teorie T v němž se $\sqsubseteq$ realizuje jako relace uspořádání s nekonečně mnoha maximálními prvky, spor s předpokladem kladeným na T.

Dle věty o kompaktnosti stačí ukázat, že každá konečná podteorie F teorie T' je splnitelná. Fixujme tedy libovolnou konečnou podteorii $F \subset T'$. Lze psát $F = F_1 \cup F_2$, kde $F_1 \subseteq T$ a $F_2 \subseteq \{\psi_n \mid n \in \mathbb{N}\}$. Protože F a tedy i F_1 a F_2 jsou konečné teorie, existuje největší $m \in \mathbb{N}$ takové, že $\psi_m \in F_2$. Uvažme realizaci $\mathcal{M}_m$ jazyka $\mathcal{L}$ s nosičem $\{1, 2, \ldots, m\}$, pro niž platí $\sqsubseteq_{\mathcal{M}_m} = \{(j, j) \mid 1 \leq j \leq m\}$. Všimněme si, že $(M_m, \sqsubseteq_{\mathcal{M}_m})$ je uspořádaná množina s m navzájem neporovnatelnými (a tedy maximálními) prvky. Dle předpokladu platí $\mathcal{M}_m \models T$ (neboť $(M_m, \sqsubseteq_{\mathcal{M}_m})$ je uspořádaná množina s konečně mnoha maximálními prvky) a tedy i $\mathcal{M}_m \models F_1$. Navíc $\mathcal{M}_m \models F_2$, neboť $\varphi_i \in F_2$ implikuje $i \leq m$ a tedy F_2 vynucuje pouze existenci alespoň m maximálních prvků. Dohromady dostáváme $\mathcal{M}_m \models F$, tedy F je splnitelná, což jsme chtěli ukázat.

Nyní uvažme alternativní (avšak v jádru velmi podobný) důkaz pomocí věty 10.2. Opět sporem předpokládejme, že existuje teorie T vyhovující zadání příkladu. Uvažme teorii

$$T'' = T \cup \{\forall x \forall y \, (x \sqsubseteq y \to x = y)\}.$$

Nově přidaná formule vynucuje, aby se predikátový symbol $\sqsubseteq$ realizoval jakožto identická relace. Společně s teorií T tedy nová formule vynucuje, aby v příslušné uspořádané množině byly každé dva prvky nesrovnatelné. Uvažme nyní, pro libovolné $m \in \mathbb{N}$, realizaci $\mathcal{M}_m$ z předchozího odstavce. Výše jsme již zdůvodnili, že $\mathcal{M}_m \models T$ a rovněž zřejmě $\mathcal{M}_m \models \forall x \forall y \, (x \sqsubseteq y \to x = y)$. Tedy $\mathcal{M}_m \models T'$. Protože m bylo zvoleno libovolně, znamená to, že T' má model libovolné konečné kardinality. Dle věty 10.2 má tedy i model $\mathcal{M}_\infty$ s nekonečným nosičem. I v tomto modelu ale musí být $\sqsubseteq$ realizována jako identická relace, a tedy $(M_\infty, \sqsubseteq_{\mathcal{M}_\infty})$ obsahuje tolik maximálních prvků, kolik je prvků nosiče, tedy nekonečně mnoho. Protože $T \subset T'$, máme $\mathcal{M}_\infty \models T$, spor s předpokladem kladeným na T. ▲

✩✩✩ **Příklad 10.8** Mějme jazyk $\mathcal{L} = \{P, Q\}$ s rovností, kde P a Q jsou unární predikátové symboly. Rozhodněte a dokažte, zda existuje teorie T s jazykem $\mathcal{L}$ taková, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$\mathcal{M} \models T \Leftrightarrow P_\mathcal{M} \cup Q_\mathcal{M} \neq M$ a zároveň $P_\mathcal{M} \cap Q_\mathcal{M}$ je konečný soubor individuí.

(Výše M značí nosič realizace $\mathcal{M}$.)

✩✩✩ **Příklad 10.9** Mějme jazyk $\mathcal{L} = \{f\}$ s rovností, kde f je unární funkční symbol. Rozhodněte a dokažte, zda existuje teorie T s jazykem $\mathcal{L}$ taková, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ platí

$$\mathcal{M} \models T \quad \Leftrightarrow \quad f_\mathcal{M} \text{ má konečný obraz.}$$

✩✩✩ **Příklad 10.10** a) Nechť $T_1, T_2, T_3 \ldots$ je nekonečná posloupnost teorií se stejným jazykem. Předpokládejme, že pro každé $i \in \mathbb{N}$ *má* teorie T_i model s nekonečným nosičem a že $T_i \supseteq T_{i+1}$ pro libovolné $i \in \mathbb{N}$. Rozhodněte a dokažte, zda i teorie $\bigcap_{i=1}^{\infty} T_i$ má model s nekonečným nosičem.

b) Nechť $T_1, T_2, T_3 \ldots$ je nekonečná posloupnost teorií se stejným jazykem. Předpokládejme, že pro každé $i \in \mathbb{N}$ *má* teorie T_i model s nekonečným nosičem a že $T_i \subseteq T_{i+1}$ pro libovolné $i \in \mathbb{N}$. Rozhodněte a dokažte, zda i teorie $\bigcup_{i=1}^{\infty} T_i$ má model s nekonečným nosičem.

Řešení

a) Odpověď je ano, neboť každý model teorie T_1 je i modelem teorie $\bigcap_{i=1}^{\infty} T_i$.

b) Odpověď je opět ano, zdůvodnění je nyní poněkud složitější. Označme $T = \bigcup_{i=1}^{\infty} T_i$ a uvažme teorii

$$T' = T \cup \{\varphi_n \mid n \in \mathbb{N}\},$$

kde pro libovolné n je $\varphi_n = \exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$ formule vynucující nosič mohutnosti $\geq n$. Ukážeme, že T' je splnitelná. V takovém případě má totiž T' model, který je zjevně nekonečný (protože jsou v něm pravdivé formule φ_n pro libovolné n) a zároveň je modelem teorie T (neboť $T \subseteq T'$).

Dle věty o kompaktnosti stačí ukázat, že libovolná konečná podteorie $F \subseteq T'$ je splnitelná. Zvolme tedy libovolnou takovou konečnou podteorii. Pak lze F psát jako sjednocení $F = F_1 \cup F_2$, kde $F_1 \subseteq T$ a $F_2 \subseteq \{\varphi_n \mid n \in \mathbb{N}\}$.

Pro každou formuli $\varphi \in T$ existuje index $k_\varphi \in \mathbb{N}$ takový, že $\varphi \in T_{k_\varphi}$. Protože $F_1 \subseteq T$ je konečná teorie a protože $T_j \subseteq T_{j+1}$ pro všechna j, existuje index k takový, že $F_1 \subseteq T_k$ (stačí vzít maximální k_φ přes všechny $\varphi \in F_1$). Nechť $\mathcal{M}_\infty$ je nějaký model teorie T_k s nekonečným nosičem (dle zadání alespoň jeden takový model existuje). Pak $\mathcal{M}_\infty \models F_1$, protože $F_1 \subseteq T_k$, a zároveň $\mathcal{M}_\infty \models \{\varphi_n \mid n \in \mathbb{N}\}$ a tedy i $\mathcal{M}_\infty \models F_2$. Celkem tedy $\mathcal{M}_\infty \models F$, což jsme chtěli ukázat.

▲

Cílem následujícího příkladu je ukázat nevyjádřitelnost *tranzitivního uzávěru* v predikátové logice prvního řádu. Nejprve si připomeňme význam uvedeného pojmu.

Definice 10.4 Nechť R je binární relace na nějaké nosné množině M. Řekneme, že binární relace T na stejné množině je *tranzitivním uzávěrem* relace R, jestliže jsou splněny následující podmínky:

a) T je tranzitivní;

b) $R \subseteq T$;

c) pro libovolnou tranzitivní relaci T' takovou, že $R \subseteq T'$ platí $T \subseteq T'$.

Jinak řečeno, tranzitivní uzávěr relace R je nejmenší (vzhledem k množinové inkluzi) tranzitivní relace obsahující relaci R jako podmnožinu.

Pojem tranzitivního uzávěru je v informace nesmírně důležitý. Například relace dosažitelnosti v orientovaném grafu $G = (V, E)$ je jednoduše tranzitivním uzávěrem hranové relace $E \subseteq V^2$. Přesto nelze tento objekt definovat v predikátové logice prvního řádu.

✩✩✩ **Příklad 10.11** Nechť $\mathcal{L}$ je libovolný jazyk s rovností obsahující dva binární predikátové symboly R a T (jazyk $\mathcal{L}$ ale může obsahovat i jiné predikátové i funkční symboly). Dokažte, že neexistuje žádná teorie T s jazykem $\mathcal{L}$ taková, že pro libovolnou realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ by platilo

$$\mathcal{M} \models T \quad \Leftrightarrow \quad T_{\mathcal{M}} \text{ je tranzitivní uzávěr relace } R_{\mathcal{M}} \tag{10.1}$$

Řešení K řešení příkladu využijeme následující pomocné tvrzení, které (kvůli lepší čitelnosti důkazu) dokážeme později.

Tvrzení 10.5 Nechť ρ je binární relace na nějaké množině M. Pak uspořádaná dvojice prvků (a, b) patří do tranzitivního uzávěru relace ρ právě když existuje *konečná* posloupnost prvků $a_0, a_1, \ldots, a_m$ taková, že $a_0 = a$, $a_m = b$ a pro libovolné $0 \leq i < m$ je $(a_i, a_{i+1}) \in \rho$.

Nyní sporem předpokládejme, že existuje teorie T s jazykem $\mathcal{L}$ splňující metaekvivalenci 10.1. Uvažme teorii

$$T' = T \cup \{\forall x \forall y \forall z\, ((R(x, y) \wedge R(x, z)) \to y = z),\, \forall x \forall y\, T(x, y)\}.$$

Intuitivně, první přidaná formule vynucuje, aby realizace symbolu R byla parciální funkce, zatímco druhá formule (společně s původní teorií T) vynucuje, aby libovolná dvojice prvků ležela v tranzitivním uzávěru relace, která

je realizací symbolu R. Dokážeme, že teorie T' má model s nekonečným nosičem. Vskutku, uvažme, pro libovolné $m \in \mathbb{N}$, následující realizaci $\mathcal{M}_m$ jazyka $\mathcal{L}$:

- $\mathcal{M}_m$ má nosič $M_m = \{1, \ldots, m\}$,
- $R_{\mathcal{M}_m} = \{(j, j+1) \mid 1 \leq j < m\} \cup \{(m+1, 1)\}$,
- $T_{\mathcal{M}_m} = M_m^2$,
- jakýkoliv jiný predikátový symbol (kromě výše uvedených) je realizován jako prázdná relace a jakýkoliv funkční symbol je realizován jako konstantní funkce vracející 1 pro libovolný argument.

Zřejmě $T_{\mathcal{M}_m}$ je tranzitivním uzávěrem $R_{\mathcal{M}_m}$. Dle předpokladu $\mathcal{M}_m \models T$. Zároveň $R_{\mathcal{M}_m}$ je parciální funkce a $T_{\mathcal{M}_m}$ obsahuje všechny dvojice prvků univerza, tedy $\mathcal{M}_m \models T'$. Protože m bylo zvoleno libovolně, dostáváme, že T' má modely s nosičem libovolné konečné kardinality. Dle věty 10.2 má T' i model s nekonečným nosičem.

Nyní ukážeme, že T' nemůže mít model s nekonečným nosičem, což je spor s předchozím odstavcem. Sporem předpokládejme, že T' má model $\mathcal{M}_\infty$, jehož nosič je nekonečný. Fixujme libovolné dvě různá individua c, d z nosiče M_∞. Protože $\mathcal{M}_\infty \models \forall x \forall y\, T(x, y)$, musí platit $(c, d) \in T_{\mathcal{M}_\infty}$ a $(d, c) \in T_{\mathcal{M}_\infty}$, přičemž $T_{\mathcal{M}_\infty}$ je tranzitivním uzávěrem $R_{\mathcal{M}_\infty}$ (neboť $\mathcal{M}_\infty \models T$). Dle Tvrzení 10.5 existují dvě konečné posloupnosti individuí $a_0, \ldots, a_m$ a $b_0, \ldots, b_\ell$ takové, že $a_0 = b_\ell = c$, $a_m = b_0 = d$ a pro všechna $0 \leq i < m$ a $0 \leq j < \ell$ platí $(a_i, a_{i+1}) \in R_{\mathcal{M}_\infty}$, resp. $(b_j, b_{j+1}) \in R_{\mathcal{M}_\infty}$. Protože $\mathcal{M}_\infty$ má nekonečný nosič, existuje v tomto nosiči individuum e takové, že $e \notin \{a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_\ell\}$. Opět ale musí platit, že $(a, e) \in T_{\mathcal{M}_\infty}$, tedy existuje posloupnost individuí $e_0, \ldots, e_k$ taková, že $e_0 = a$, $e_k = e$ a $(e_i, e_{i+1}) \in R_{\mathcal{M}_\infty}$ pro všechna $0 \leq i \leq k$. Nechť q je největší index takový, že $e_q \in \{a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_\ell\}$. Ze způsobu, jakým jsme vybrali $e = e_k$, plyne $q < k$. Navíc $e_q = a_r$ nebo $e_q = b_r$ pro vhodné r. Pak ale $(e_k, e_{k+1}) \in R_{\mathcal{M}_\infty}$ a zároveň $(e_k, f) \in R_{\mathcal{M}_\infty}$, kde $f = a_{r+1}$ nebo $f = b_{r+1}$ pro vhodné r. Zřejmě $e_{k+1} \neq f$, což je spor s tím, že $\mathcal{M}_\infty \models \forall x \forall y \forall z\, ((R(x, y) \wedge R(x, z)) \to y = z)$.

Důkaz Tvrzení 10.5: Metaimplikace $\Leftarrow$ se ukáže velice snadno (zkuste si to jako jednoduché cvičení), soustředíme se tedy na důkaz metaimplikace $\Rightarrow$. Pro danou relaci ρ definujme relaci ρ' takto: $(a, b) \in \rho'$ právě když existuje konečná posloupnost prvků $a_0, \ldots, a_m$ taková, že $a_0 = a$, $a_m = b$ a pro libovolné $0 \leq i < m$ je $(a_i, a_{i+1}) \in \rho$.

Zřejmě $\rho \subseteq \rho'$. K důkazu metaimplikace $\Rightarrow$ stačí ukázat, že ρ' je tranzitivní, neboť pak tranzitivní uzávěr relace ρ je podmnožinou ρ'. Nechť tedy $(a, b) \in \rho'$ a $(b, c) \in \rho$. Existují tedy posloupnosti $a = a_0, a_1, \ldots, a_m = b$ a $b = b_0, b_1, \ldots, b_\ell = c$ takové, že dva po sobě jdoucí prvky v těchto posloupnostech jsou v relaci ρ. Pak posloupnost dosvědčující, že $(a, c) \in \rho'$ je jednoduše posloupnost $a = a_0, a_1, \ldots, a_m = b = b_0, b_1, \ldots, b_\ell = c$. ▲

Kapitola 11

Kanonická struktura

V důkazu věty o úplnosti se ukazuje, že každá bezesporná teorie má model. Jak však takový model nalézt? Jediná věc, kterou máme k dispozici a kterou můžeme při konstrukci modelu využít, je jazyk příslušné teorie. A právě z jazyka lze ryze syntaktickým způsobem vytvořit tzv. *kanonickou strukturu* teorie.

Definice 11.1 Buď T teorie, kde jazyk teorie T obsahuje alespoň jednu konstantu. Kanonická struktura teorie T je realizace $\mathcal{M}$ jazyka teorie T, kde

- univerzum M je tvořeno všemi uzavřenými termy jazyka teorie T;
- realizace funkčního symbolu f arity n je funkce $f_{\mathcal{M}}$, která uzavřeným termům $t_1, \cdots, t_n$ přiřadí uzavřený term $f(t_1, \cdots, t_n)$;
- realizace predikátového symbolu P arity m je relace $P_{\mathcal{M}}$ definovaná takto: $(t_1, \cdots, t_m) \in P_M$ platí právě když $T \vdash P(t_1, \cdots, t_m)$.

Věta 11.2 [o kanonické struktuře] Nechť T je úplná henkinovská teorie, a nechť jazyk teorie T je jazykem bez rovnosti. Pak kanonická struktura teorie T je modelem T.

Pro následující tři příklady fixujme jazyk $\mathcal{L} = \{P, 0, f\}$ kde P je unární predikátový symbol, 0 je nulární funkční symbol a f je unární funkční symbol.

✡✡✡ **Příklad 11.1** Popište kanonickou strukturu teorie $T_1 = \{P(0)\}$ s jazykem $\mathcal{L}$.

Řešení Kanonická struktura teorie T_1 je realizace $\mathcal{M}_1$ jazyka $\mathcal{L}$ taková, že

- $M_1 = \{f^i(0) \mid i \geq 0\}$ (kde $f^0(0) = 0$)
- $f_{\mathcal{M}_1}(f^i(0)) = f(f^i(0)) = f^{i+1}(0)$
- $0_{\mathcal{M}_1} = 0$
- $P_{\mathcal{M}_1} = \{0\}$

Jediná věc, která není zřejmá z definice kanonické struktury je $P_{\mathcal{M}_1} = \{0\}$. Musíme ukázat, že $T \vdash P(0)$, a že $T \nvdash P(f^i(0))$ pro $i \geq 1$.

- Zřejmě $T \vdash P(0)$.
- Nechť $i \geq 1$. Stačí ukázat, že $T \not\models P(f^i(0))$. Požadovaný výsledek pak plyne z věty o korektnosti. Nechť $\mathcal{M}$ je realizace jazyka $\mathcal{L}$ definovaná následovně:
  - $M = \{a, b\}$
  - $f_{\mathcal{M}}(a) = b$ a $f_{\mathcal{M}}(b) = b$
  - $0_{\mathcal{M}} = a$
  - $P_{\mathcal{M}} = \{a\}$

  Zřejmě $\mathcal{M} \models T$, protože $a \in P_{\mathcal{M}}$, a zřejmě také $\mathcal{M} \not\models P(f^i(0))$ pro $i > 0$, protože $f^i_{\mathcal{M}}(a) = b \notin P_{\mathcal{M}}$. Celkem tedy $T \not\models P(f^i(0))$ a dle věty o korektnosti $T \nvdash P(f^i(0))$.

▲

✿✿ **Příklad 11.2** Popište kanonickou strukturu teorie $T_2 = \{P(x)\}$ s jazykem $\mathcal{L}$.

Řešení Kanonická struktura $\mathcal{M}_2$ teorie T_2 se liší od struktury $\mathcal{M}_1$ z Příkladu 11.1 pouze v interpretaci predikátového symbolu P. Dokážeme, že $P_{\mathcal{M}_2} = \{f^i(0) \mid i \geq 0\}$.

Dle definice kanonické struktury musíme ukázat, že $T \vdash P(f^i(0))$ pro $i \geq 0$. Důkaz může vypadat takto:

T	$\vdash$	$P(x)$	$P(x) \in T$
T	$\vdash$	$\forall x P(x)$	GEN
T	$\vdash$	$\forall x P(x) \to P(x)(x/f^i(0))$	$P4$
T	$\vdash$	$P(x/f^i(0))$	MP

▲

✡✡✡ **Příklad 11.3** Popište kanonickou strukturu teorie $T_3 = \{\exists x\, P(x)\}$ s jazykem $\mathcal{L}$.

Řešení Kanonická struktura $\mathcal{M}_3$ teorie T_3 se liší od struktur $\mathcal{M}_1$ a $\mathcal{M}_2$ z předchozích příkladů pouze v interpretaci predikátového symbolu P. Dokážeme, že $P_{M_3} = \emptyset$.

Ukážeme, že $T \not\models P(f^i(0))$ pro $i \geq 0$. Požadovaný výsledek pak plyne z věty o korektnosti. Nechť $\mathcal{M}$ je realizace jazyka $\mathcal{L}$ definovaná následovně:

- $M = \{a, b\}$
- $f_{\mathcal{M}}(a) = a$ a $f_M(b) = b$
- $0_{\mathcal{M}} = b$
- $P_{\mathcal{M}} = \{a\}$

Zřejmě $\mathcal{M} \models T$, protože $P_{\mathcal{M}} \neq \emptyset$, a zřejmě také $\mathcal{M} \not\models P(f^i(0))$ pro $i \geq 0$, protože $f^i_{\mathcal{M}}(0_{\mathcal{M}}) = b \notin P_{\mathcal{M}}$. Celkem tedy $T \not\models P(f^i(0))$.

Všimněte si, že kanonická struktura $\mathcal{M}_3$ není modelem T_3. ▲

✡✡✡ **Příklad 11.4** Nechť $\mathcal{L}$ je jazyk bez rovnosti s jedním nulárním funkčním symbolem C, jedním unárním funkčním symbolem g a jedním unárním predikátovým symbolem Q. Popište realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takovou, že $\mathcal{M}$ je kanonickou strukturou teorie $T = \{Q(g(C))\}$. Zdůvodněte, že $\mathcal{M}$ je skutečně kanonická struktura teorie T.

✡✡✡ **Příklad 11.5** Nechť $\mathcal{L} = \{A, B, f, P\}$ je jazyk bez rovnosti, kde A a B jsou nulární funkční symboly, f je unární funkční symbol a P je unární predikátový symbol. Popište realizaci $\mathcal{M}$ jazyka $\mathcal{L}$ takovou, že $\mathcal{M}$ je kanonickou strukturou teorie

$$T = \{P(A),\ \neg P(B)\}.$$

Zdůvodněte, že $\mathcal{M}$ je skutečně kanonická struktura teorie T.

✡✡✡ **Příklad 11.6** Mějme jazyk $\mathcal{L} = \{A, g, P\}$ bez rovnosti, kde A je nulární funkční symbol, g je unární funkční symbol a P je unární predikátový symbol. Uvažme dále následující teorii T s jazykem $\mathcal{L}$:

$$T = \{A,\ P(x) \to P(g(g(x)))\}.$$

Popište kanonickou strukturu teorie T. Svůj výsledek zdůvodněte.

✩✩✩ **Příklad 11.7** Mějme jazyk $\mathcal{L} = \{P, f, A, B\}$ s rovností, kde P je unární predikátový symbol, f je unární funkční symbol a A, B jsou nulární funkční symboly (konstanty). Uvažme následující teorii T tohoto jazyka:

$$T = \{P(A),\, \forall x(P(x) \to P(f(x))),\, f(A) = f(f(B))\}.$$

Nechť $\mathcal{M}$ je *kanonická struktura* teorie T.

a) Popište nosič realizace $\mathcal{M}$.

b) Popište realizaci $P_{\mathcal{M}}$ predikátového symbolu P v kanonické struktuře $\mathcal{M}$. Dokažte, že Vaše řešení obsahuje $P_{\mathcal{M}}$ jako podmnožinu (tj. pro všechny prvky nosiče, které podle Vás nenáleží do $P_{\mathcal{M}}$ formálně dokažte, že do $P_{\mathcal{M}}$ vskutku patřit nemohou.)

Řešení Nosičem realizace $\mathcal{M}$ je soubor M všech uzavřených termů jazyka $\mathcal{L}$, tj. soubor $M = \{f^i(A),\, f^i(B) \mid i \geq 0\}$ (kde $f^0(A) = A$ a $f^0(B) = B$).

Tvrdíme, že $P_{\mathcal{M}} = \{f^i(A) \mid i \geq 0\} \cup \{f^j(B) \mid j \geq 2\}$. Abychom dostáli zadání, musíme ukázat, že $B \notin P_{\mathcal{M}}$ a $f(B) \notin P_{\mathcal{M}}$. Z definice kanonické struktury to znamená ukázat $T \nvdash P(B)$ a $T \nvdash P(f(B))$, přičemž podle věty o korektnosti stačí ukázat, že $T \not\models P(B)$ a $T \not\models P(f(B))$.

Uvažme realizaci $\mathcal{M}'$ jazyka $\mathcal{L}$ danou následovně:

- jejím nosičem je soubor $M' = \{a, b, c\}$,
- $A_{\mathcal{M}'} = a$, $B_{\mathcal{M}'} = b$,
- $f_{\mathcal{M}'}(a) = a$, $f_{\mathcal{M}'}(b) = c$, $f_{\mathcal{M}'}(c) = a$,
- $P_{\mathcal{M}'} = \{a\}$.

Zřejmě $\mathcal{M}'$ je modelem teorie T: $\mathcal{M}' \models P(A)$, neboť $A_{\mathcal{M}'} = a \in P_{\mathcal{M}'}$, $\mathcal{M}' \models \forall x(P(x) \to P(f(x)))$, neboť $f_{\mathcal{M}'}(a) = a \in P_{\mathcal{M}'}$ a konečně $\mathcal{M}' \models f(A) = f(f(B))$. neboť oba uvedené uzavřené termy se v $\mathcal{M}'$ realizují jako prvek a.

Zároveň ale $\mathcal{M}' \not\models P(B)$ (neboť $B_{\mathcal{M}'} = b \notin P_{\mathcal{M}'}$) a $\mathcal{M}' \not\models P(f(B))$ (neboť $f_{\mathcal{M}'}(B_{\mathcal{M}'}) = c \notin P_{\mathcal{M}'}$). Nalezli jsme tedy model teorie T ve kterém uvedené formule nejsou pravdivé, tyto formule tedy nemohou být jejím sémantickým důsledkem. ▲

✩✩✩ **Příklad 11.8** Mějme jazyk $\mathcal{L} = \{P, f, A\}$ bez rovnosti, kde P je unární predikátový symbol, f je unární funkční symbol a A je nulární funkční symbol (konstanta). Uvažme následující teorii T tohoto jazyka:

$$T = \{P(A), \forall x(P(x) \vee P(f(x)))\}.$$

Nechť $\mathcal{M}$ je *kanonická struktura* teorie T.

a) Popište nosič realizace $\mathcal{M}$.

b) Popište realizaci $P_{\mathcal{M}}$ predikátového symbolu P v kanonické struktuře $\mathcal{M}$. Dokažte, že Vaše řešení obsahuje $P_{\mathcal{M}}$ jako podmnožinu (tj. pro všechny prvky nosiče, které podle Vás nenáleží do $P_{\mathcal{M}}$ dokažte, že do $P_{\mathcal{M}}$ vskutku patřit nemohou).

✩✩✩ **Příklad 11.9** Mějme jazyk $\mathcal{L} = \{P, A, f, g\}$ s rovností, kde P je unární predikátový symbol, A je konstanta (tj. nulární funkční symbol) a f, g jsou unární funkční symboly. Mějme dále následující teorii T s jazykem $\mathcal{L}$:

$$T = \{P(A),\ A = f(A),\ P(f(x)) \to P(g(f(x))),\ P(g(x)) \to P(f(g(x)))\}.$$

Označme $\mathcal{M}$ kanonickou strukturu teorie T. Popište nosič této kanonické struktury a relaci $P_{\mathcal{M}}$. Své řešení zdůvodněte.

Řešení Nejprve popišme nosič M kanonické struktury $\mathcal{M}$, tj. soubor všech uzavřených termů daného jazyka. Chceme-li tento soubor popsat formálně zcela přesně, jakožto množinu slov nad abecedou $\{A, f, g, (,)\}$, můžeme použít například tuto formu zápisu z teorie formálních jazyků:

$$M = \bigcup_{k \geq 0} M_k, \text{ kde } M_k = \{f(, g(\}^k \cdot \{A\} \cdot \{)\}^k.$$

Popřípadě též můžeme říct, že M je jazyk generovaný gramatikou s kořenovým neterminálem S a s pravidly $\{S \to A, S \to f(S), S \to g(S)\}$. V pořádku je i klasický matematický zápis, kdy se nestaráme o závorky a zavádíme zkratky $f^0(t) = g^0(t) = t$ a $f^{i+1}(t) = f(f^i(t))$, $g^{i+1}(t) = g(g^i(t))$, pro libovolný term t. Pak lze psát například

$$M = \{z_1^{i_1}(z_2^{i_2}(\cdots z_{k-1}^{i_{k-1}}(z_k^{i_k}(A))\cdots) \mid k \geq 0, z_j \in \{f, g\} \text{ a } i_j \geq 0 \text{ pro } 1 \leq j \leq k\}.$$

Nyní popišme realizaci $P_{\mathcal{M}}$ predikátového symbolu P v kanonické struktuře $\mathcal{M}$. Využijeme opět posledně zmíněný zkratkovitý zápis, kde pro libovolný term t klademe $(f \circ g)^0(t) = t$ a $(f \circ g)^{i+1}(t) = f(g(t))$.

$$P_{\mathcal{M}} = \{g^i((f \circ g)^j(f^k(A))) \mid k \geq 0, j \geq 0, i \in \{0, 1\}\}.$$

(Neformálně: postupujeme-li od nejvnitřnější aplikace funkčního symbolu na A, pak nejprve se může objevit libovolné množství aplikací symbolu f, jakmile se však objeví první aplikace symbolu g, musí se střídat aplikace symbolů g a f, přičemž můžeme skončit jak aplikací symbolu f, tak aplikací symbolu g.)

Nyní ukažme, že pro všechny $t \in P_{\mathcal{M}}$ vskutku platí $T \vdash P(t)$. Označme $t_{i,j,k}$ term $g^i((f \circ g)^j(f^k(A)))$. Chceme tedy ukázat následující:

Věta 11.3 Pro libovolné $i \in \{0,1\}$, $j,k \geq 0$ platí $T \vdash P(t_{i,j,k})$.

Nejprve dokážeme, že Věta 11.3 platí pro libovolný term tvaru $t_{0,0,k}$, $k \geq 0$. Použijeme následující pomocné tvrzení:

Tvrzení 11.4 V libovolném modelu $\mathcal{M}'$ teorie T platí $A_{\mathcal{M}'} = f^k_{\mathcal{M}'}(A_{\mathcal{M}'})$,[1] pro libovolné $k \geq 0$.

Důkaz Nechť $\mathcal{M}'$ je libovolný model teorie T. Pro $k = 0$ je tvrzení triviální, pro $k = 1$ plyne z toho, že T obsahuje formuli $A = f(A)$. Předpokládejme, že tvrzení platí pro nějaké $k \geq 0$, tj. že $A_{\mathcal{M}'} = f^k_{\mathcal{M}'}(A_{\mathcal{M}'})$. Protože $f_{\mathcal{M}'}$ je funkce, platí též $f_{\mathcal{M}'}(A_{\mathcal{M}'}) = f^{k+1}_{\mathcal{M}'}(A_{\mathcal{M}'})$. Ale dle výše uvedeného platí $f_{\mathcal{M}'}(A_{\mathcal{M}'}) = A_{\mathcal{M}'}$, dohromady tedy $A_{\mathcal{M}'} = f^{k+1}_{\mathcal{M}'}(A_{\mathcal{M}'})$.

Z výše uvedeného tvrzení a z definice pravdivosti pro formule tvaru $P(t)$ přímo plyne, že v libovolném modelu $\mathcal{M}'$ teorie T platí $\mathcal{M}' \models P(A)$ právě když $\mathcal{M}' \models P(f^k(A))$, pro libovolné $k \geq 0$. Ovšem $\mathcal{M}' \models P(A)$, neboť tato formule je axiomem teorie T. Tedy v libovolném modelu teorie T je pro libovolné $k \geq 0$ pravdivá formule $P(f^k(A))$, tj. $T \models P(t_{0,0,k})$. Z věty o úplnosti plyne, že $T \vdash P(t_{0,0,k})$.

Nyní dokážeme platnost Věty 11.3 pro zbylé termy tvaru $t_{i,j,k}$. Všimněme si, že pro libovolné $j,k \geq 0$ je $t_{1,j,k} = g(t_{0,j,k})$ a pro libovolné $k \geq 0$, $j > 0$ je $t_{0,j,k} = f(t_{1,j-1,k})$. Stačí tedy ukázat následující:

a) Pro libovolné $k \geq 0$ platí $T \vdash P(t_{0,0,k})$.

b) Pokud $T \vdash P(t_{0,j,k})$, pak $T \vdash P(t_{1,j,k})$.

c) Pokud $T \vdash P(t_{1,j,k})$, pak $T \vdash P(t_{0,j+1,k})$.

Ad a). Bylo již dokázáno výše.

[1] Všimněte si, že symbol = je zde použit jako metasymbol, ne jako mimologický symbol pro rovnost.

Ad b). Snadno se ukáže, že $T \vdash P(t_{0,j,k}) \to P(t_{1,j,k})$:

(1) $T \vdash P(f(x)) \to P(g(f(x)))$ axiom T

(2) $T \vdash \forall x\ (P(f(x)) \to P(g(f(x))))$ GEN na (1)

(3) $T \vdash \forall x\ (P(f(x)) \to P(g(f(x)))) \to (P(t_{0,j,k}) \to P(t_{1,j,k}))$ inst. P4

(4) $T \vdash P(t_{0,j,k}) \to P(t_{1,j,k})$ MP na (2), (3).

(V kroku (3) mohou nastat dvě možnosti. Pokud $j \geq 1$, pak jde o instanci schématu specifikace, kde se za x dosadí term $t_{1,j-1,k}$. Pokud $j = 0$, pak se za x musí dosadit term $t_{0,0,k-1}$. Pokud navíc $k = 0$, pak nelze výše zmíněný důkaz použít. Stačí ale argumentovat, že formule $P(A) \to P(g(A))$ vyplývá z teorie T, neboť v každém modelu $\mathcal{M}'$ teorie T je $A_{\mathcal{M}'} = f_{\mathcal{M}'}(A_{\mathcal{M}'})$ a $g_{\mathcal{M}'}(A_{\mathcal{M}'}) = g_{\mathcal{M}'}(f_{\mathcal{M}'}(A_{\mathcal{M}'}))$. Platí tedy $\mathcal{M}' \models P(A) \to P(g(A))$ právě když platí $\mathcal{M}' \models P(f(A)) \to P(g(f(A)))$. Buď jsou tedy z T dokazatelné obě tyto formule, nebo žádná z nich, stačí tedy vyřešit případ kdy $k > 0$.)

Dále dle předpokladu máme $T \vdash P(t_{0,j,k})$. Zapišme za sebe důkazy formulí $P(t_{0,j,k})$ a $P(t_{0,j,k}) \to P(t_{1,j,k})$ a na konec této posloupnosti přidejme formuli $P(t_{1,j,k})$, kterou dostaneme aplikací MP na dvě výše zmíněné formule. Tato posloupnost je zřejmě důkazem formule $P(t_{1,j,k})$ z teorie T, tedy $T \vdash P(t_{1,j,k})$.

Ad c). Metadůkaz je symetrický k případu b). Tím je dokončen důkaz Věty 11.3.

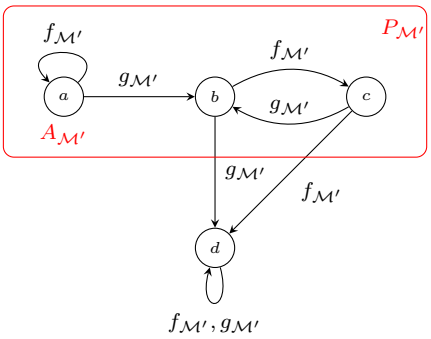
Zbývá dokázat, že termy tvaru $t_{i,j,k}$ jsou jediné uzavřené termy daného jazyka, pro které je formule $P(t)$ dokazatelná z T. Využijeme následující tvrzení:

Tvrzení 11.5 Mějme uzavřený term t mající jeden z následujících tvarů: $g(g(t_0))$ či $f(f(t_1))$, kde t_0, t_1 jsou libovolné termy takové, že t_1 obsahuje alespoň jeden výskyt symbolu g. Pak existuje model $\mathcal{M}'$ teorie T takový, že $t_{\mathcal{M}'} \notin P_{\mathcal{M}'}$ a $f_{\mathcal{M}'}(t_{\mathcal{M}'}) = g_{\mathcal{M}'}(t_{\mathcal{M}'}) = t_{\mathcal{M}'}$.

Důkaz Uvažme realizaci $\mathcal{M}'$ s nosičem $\{a, b, c, d\}$, kde $A_{\mathcal{M}'} = a$, $P_{\mathcal{M}'} = \{a, b, c\}$, a kde $f_{\mathcal{M}'}$ a $g_{\mathcal{M}'}$ jsou zadány výše uvedeným diagramem.

$\mathcal{M}'$ je modelem teorie T neboť: $A_{\mathcal{M}'} = a \in P_{\mathcal{M}'}$ a tedy $\mathcal{M}' \models P(A)$; pro libovolné individuum i, které náleží do $P_{\mathcal{M}'}$ a zároveň leží v obraze funkce $f_{\mathcal{M}'}$ (tj. $i = a$ nebo $i = c$) je též $g_{\mathcal{M}'}(i) \in P_{\mathcal{M}'}$ a tedy $\mathcal{M}' \models P(f(x)) \to P(g(f(x)))$ (symetricky se ukáže pro formuli $P(g(x)) \to P(f(g(x)))$); a konečně $a = f_{\mathcal{M}'}(a)$ a tedy $\mathcal{M}' \models A = f(A)$.

Dále vidíme, že pro libovolné individuum i je $g^2_{\mathcal{M}'}(i) = d$. Dále vidíme, že žádný term t_1 obsahující alespoň jeden výskyt symbolu g se nemůže realizovat jako prvek a. Ovšem pro každé individuum i různé od a máme $f^2_{\mathcal{M}'}(i) = d$.



Každý term t mající tvar uvedený v dokazovaném tvrzení se tedy v $\mathcal{M}'$ realizuje jako prvek $d \notin P_{\mathcal{M}'}$. Ihned vidíme, že platí $f_{\mathcal{M}'}(t_{\mathcal{M}'}) = g_{\mathcal{M}'}(t_{\mathcal{M}'}) = d = t_{\mathcal{M}'}$.

Každý uzavřený term t daného jazyka je možné jednoznačně zapsat ve tvaru $z_1(z_2(\dots z_m(A)\dots))$, kde $m \geq 0$ a pro $1 \leq l \leq m$ je $z_l \in \{f, g\}$. Pokud t *není* tvaru $t_{i,j,k}$ pro žádné i, j, k, pak nutně $m \geq 2$ a $z_l = z_{l+1}$ pro nějaké $1 \leq l < m$. Pokud navíc $z_l = f$, musí existovat $l' > l$ takové, že $z_{l'} = g$. Uvažme model $\mathcal{M}'$ teorie T z předchozího tvrzení. Z tvrzení vyplývá, že

$$z_{l\mathcal{M}'}(z_{l+1\mathcal{M}'}(\dots z_{m\mathcal{M}'}(A_{\mathcal{M}'})\dots)) \notin P_{\mathcal{M}'}$$

a že

$$t_{\mathcal{M}'} = z_{1\mathcal{M}'}(z_{2\mathcal{M}'}(\dots z_{m\mathcal{M}'}(A_{\mathcal{M}'})\dots)) = z_{l\mathcal{M}'}(z_{l+1\mathcal{M}'}(\dots z_{m\mathcal{M}'}(A_{\mathcal{M}'})\dots)).$$

Dohromady $t_{\mathcal{M}'} \notin P_{\mathcal{M}'}$.

Tedy pro term t který nemá tvar $t_{i,j,k}$ platí $\mathcal{M}' \not\models P(t)$. Protože $\mathcal{M}'$ je modelem T, máme $T \not\models P(t)$ a dle věty o korektnosti i $T \nvdash P(t)$. Tím je důkaz hotov. ▲

Příloha A

Vybrané zajímavosti

V rámci přednášky „Matematická logika“ na Fakultě informatiky MU je možné se seznámit se základními pojmy a výsledky z tohoto oboru. Matematická logika je však mnohem hlubší oblastí, než by se z této úvodní přednášky mohlo zdát. V této části naší sbírky bychom tedy chtěli dát čtenáři možnost seznámit se s některými dalšími zajímavými výsledky. Obsah následujícího textu bezprostředně navazuje na obsah zmíněného kurzu logiky a neformálním způsobem jej rozšiřuje. Naší snahou je podat tuto rozšiřující látku přístupným a spíše neformálním způsobem, od čtenáře tedy neočekáváme zvláštní znalosti mimo pochopení látky z přednášky, na kterou tento text navazuje. Doufáme, že i tyto rozšiřující kapitoly si najdou své čtenáře a budou jim sloužit jako vydatné „krmivo pro mozek.“

A.1 Löwenheimova-Skolemova věta a nestandardní modely aritmetiky

Značná část přednášky byla věnována Gödelovu důkazu neúplnosti Peanovy aritmetiky. V této kapitole si sestrojíme tzv. *nestandardní* model aritmetiky, tedy takovou realizaci jazyka $\mathcal{L} = \{0, S, +, \cdot\}$, v níž jsou pravdivé přesně ty sentence jazyka $\mathcal{L}$, které jsou pravdivé pro standardní přirozená čísla, ovšem která se od standardních přirozených čísel diametrálně liší.

Nejprve si připomeňme samotnou Peanovu aritmetiku. Fixujme jazyk $\mathcal{L} = \{0, S, +, \cdot\}$ s rovností, kde 0 je nulární funkční symbol, S je binární funkční symbol a $+$ a $\cdot$ jsou binární funkční symboly. *PA* (Peanova aritmetika) je teorie s jazykem $\mathcal{L}$ obsahující následující axiomy:

- $\forall x\, S(x) \neq 0$

- $\forall x \forall y\,(S(x) = S(y) \to x = y)$
- $\forall x\, x + 0 = x$
- $\forall x \forall y\, x + S(y) = S(x + y)$
- $\forall x\, x \cdot 0 = 0$
- $\forall x \forall y\, x \cdot S(y) = (x \cdot y) + x$
- $(\varphi(x/0) \wedge \forall x\,(\varphi \to \varphi(x/S(x)))) \to \forall x\, \varphi$, kde φ je formule s jednou volnou proměnnou x.

(Připomeňme, že tato teorie obsahuje ve skutečnosti nekonečný počet axiomů – poslední odrážka reprezentuje schéma axiomů, v němž dosazením libovolné formule s jednou volnou proměnnou x za φ dostaneme jeden konkrétní axiom Peanovy aritmetiky).

Takzvaným *standardním modelem* aritmetiky máme na mysli realizaci $\mathcal{N}$, jejímž nosičem je soubor $\mathbb{N}$ všech přirozených čísel (s nulou), a v níž se funkční symboly realizují následovně:

- $0_{\mathcal{N}}$ je číslo 0,
- $S_{\mathcal{N}}$ je operace následníka, tj. funkce $S_{\mathcal{N}}$ zobrazí libovolné přirozené číslo n na číslo o 1 větší,
- $+_{\mathcal{N}}$ a $\cdot_{\mathcal{N}}$ jsou standardní sčítání, resp. standardní násobení přirozených čísel.

Je zřejmé, že realizace $\mathcal{N}$ je vskutku modelem Peanovy aritmetiky. Budeme se nyní zabývat otázkou, zda má *PA* i jiné modely. Ačkoliv se zdá, že uvedené axiomy precizně popisují strukturu přirozených čísel, vskutku existují i modely Peanovy aritmetiky, které nejsou standardnímu modelu $\mathcal{N}$ izomorfní. Takový model nazveme nestandardním modelem. Existence nestandardního modelu plyne mimo jiné přímo z Gödelovy věty o neúplnosti, která říká, že Peanova aritmetika je neúplnou teorií, a z příkladu 9.17, ve kterém jsme ukázali, že každá teorie, která má až na isomorfismus jediný model, je úplná.

Ve skutečnosti můžeme dokázat mnohem silnější tvrzení. Uvažme teorii

$$Th\mathcal{N} = \{\varphi \mid \varphi \text{ je sentence jazyka } \mathcal{L} \text{ a } \mathcal{N} \models \varphi\}.$$

Teorie $Th\mathcal{N}$ se také nazývá *skutečná aritmetika*, neboť obsahuje právě ty sentence jazyka $\mathcal{L}$, které jsou pravdivé ve standardním modelu $\mathcal{N}$. Je

zřejmé, že teorie $Th\mathcal{N}$ je úplná teorie. Vskutku, $Th\mathcal{N}$ je splnitelná (a tedy dle příkladu 9.5 i bezesporná), neboť $\mathcal{N}$ je jejím modelem. Navíc dle příkladu 7.2 pro každou sentenci φ jazyka $\mathcal{L}$ platí buď $\mathcal{N} \models \varphi$ (a tedy $Th\mathcal{N} \vdash \varphi$, neboť v tomto případě $\varphi \in Th\mathcal{N}$), anebo $\mathcal{N} \models \neg\varphi$ (v kterémžto případě $\mathcal{N} \vdash \neg\varphi$). Jde tedy o teorii, která je rozšířením Peanovy aritmetiky (všechny Peanovy axiomy náleží do $Th\mathcal{N}$), které ovšem není konzervativní (neboť Peanova aritmetika úplná není, zatímco $Th\mathcal{N}$ úplná je).

Teorie $Th\mathcal{N}$ tedy popisuje strukturu přirozených čísel tak přesně, jak jen to je v logice prvního řádu možné. Tento popis je dokonce tak precizní, že není žádným konečným způsobem prezentovatelný: neexistuje algoritmus, který by pro danou formuli rozhodl, zda je axiomem $Th\mathcal{N}$ či nikoliv (pokud by takový algoritmus existoval, byla by $Th\mathcal{N}$ rekurzivní úplnou teorií obsahující Peanovu aritmetiku, spor s Gödelovou větou o neúplnosti). Přesto stále existují modely teorie $Th\mathcal{N}$, které nejsou standardnímu modelu $\mathcal{N}$ izomorfní. Plyne to mimo jiné z Löwenheimovy-Skolemovy věty (viz přednáška), která říká, že každá teorie se spočetným jazykem, která má nekonečný model, má model libovolné nekonečné kardinality. Zejména tedy teorie $Th\mathcal{N}$ má model s nespočetným nosičem, který zřejmě nemůže být izomorfní modelu $\mathcal{N}$.

Stále však nemáme příliš představu o tom, jak takový nestandardní model aritmetiky vlastně vypadá. Navíc jsme důkaz existence nestandardního modelu odbyli poměrně triviálním způsobem. Skutečně zajímavá otázka zní následovně: existuje nestandardní model teorie $Th\mathcal{N}$ (a tedy i Peanovy aritmetiky) *se spočetným nosičem*? Kupodivu je odpověď opět *ano*! V následujících odstavcích si existenci takového modelu dokážeme a příslušný nestandardní model si i do jisté míry popíšeme.

Nejprve si ale zformulujeme variantu Löwenheimovy-Skolemovy věty, která nám pro jisté teorie umožní ukázat existenci modelu se spočetným nosičem. Důkaz věty 82 ve slajdech ukazuje pouze to, že libovolná teorie s nějakým jazykem $\mathcal{L}'$, která má model s nekonečným nosičem, má pro libovolné kardinální číslo $\kappa \geq |\mathcal{L}'|$ model mohutnosti *alespoň* κ. My bychom chtěli ukázat, že má model mohutnosti *přesně* κ. Pro jednoduchost uvážíme konkrétní jazyk – výše fixovaný jazyk aritmetiky $\mathcal{L}$.

Věta A.1 [o existenci spočetného modelu] Nechť T je libovolná teorie jazyka aritmetiky, která má model s nekonečným nosičem. Pak T má model se spočetným nosičem.

Důkaz Uvažme teorii $T' = T \cup \{\varphi_n \mid n \in \mathbb{N}\}$, kde pro libovolné $n \in \mathbb{N}$ je φ_n formule $\exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$. Zřejmě T' je splnitelná teorie, neboť

předpokládaný model T s nekonečným nosičem je i modelem T'. Teorie T' je tedy i bezesporná (viz příklad 9.5). Uvažme model $\mathcal{M}$ teorie T' sestrojený v důkazu věty o úplnosti. Ukážeme, že tento model má spočetný nosič. Protože každý model teorie T' je i modelem T, bude tím věta dokázána.

Připomeňme si, jakým způsobem se model $\mathcal{M}$ konstruoval. Nejprve jsme dokázali existenci Henkinovské teorie S (s nějakým jazykem $\mathcal{L}^* \supseteq \mathcal{L}$), která je konzervativním rozšířením teorie T (viz věta 73 ze slajdů). Teorie S přitom vznikla sjednocením teorií $T_0, T_1, T_2, \ldots$, kde $T_0 = T$ a pro libovolné $i \geq 1$ vznikla teorie T_i z teorie T_{i-1} tak, že pro libovolnou formuli φ jazyka teorie T_{i-1} s jednou volnou proměnnou x jsme zavedli novou konstantu c_φ a přidali do teorie formuli $\exists x\varphi \to \varphi(x/c_\varphi)$. Indukcí vzhledem k i lze snadno ukázat, že jazyk každé uvedených teorií T_i je spočetný. Plyne to z toho, že soubor všech konečných slov nad nejvýše spočetnou abecedou je spočetný, zejména tedy pomocí spočetného jazyka lze utvořit nejvíce spočetně mnoho formulí. Tudíž při vytváření teorie T_i z teorie T_{i-1} přidáváme nejvýše spočetně mnoho konstant.

Protože sjednocením spočetně mnoha množin spočetné mohutnosti získáme opět spočetnou množinu, je i jazyk $\mathcal{L}^*$ teorie S spočetný.

V důkazu věty o úplnosti jsme dále ukázali, že k uvedené henkinovské teorii S existuje úplná teorie U se stejným jazykem $\mathcal{L}^*$ (U je tedy stále henkinovská), která je rozšířením teorie S. Poté jsme sestrojili model $\mathcal{M}$ teorie U, který musí být i modelem teorie T, neboť U je rozšířením T. Tvrdíme, že $\mathcal{M}$ má spočetný nosič. Vznikl totiž následovně: nejprve jsme vzali kanonickou strukturu teorie U, jejímž nosičem je soubor všech uzavřených termů jazyka $\mathcal{L}^*$. Protože $\mathcal{L}^*$ je spočetný, je soubor všech konečných slov nad tímto jazykem (a tedy i soubor uzavřených termů jazyka $\mathcal{L}^*$) nejvýše spočetný. Dále, protože $\mathcal{L}^*$ je jazyk s rovností, museli jsme tuto kanonickou strukturu dále upravit (viz věta 77 na slajdech), aby byla modelem teorie U. S nosičem jsme přitom provedli tu úpravu, že jsme namísto souboru uzavřených termů vzali rozklad tohoto souboru podle vhodné relace ekvivalence. Ovšem rozklad nějakého souboru má nejvýše takovou mohutnost, jako onen soubor, model $\mathcal{M}$ má tedy spočetný nosič.

Nyní ukážeme, že teorie $Th\mathcal{N}$ (a tedy i Peanova aritmetika) má nestandardní model se spočetným nosičem. Uvažme jazyk $\mathcal{L}' = \mathcal{L} \cup \{c\}$, kde c je nulární funkční symbol. Uvažme dále teorii $T = Th\mathcal{N} \cup \{\psi_n \mid n \in \mathbb{N}\}$, kde pro libovolné $n \in \mathbb{N}$ je ψ_n formule $\exists x\,(x \neq 0 \wedge S^n(0) + x = c)$. Pak každá konečná podteorie F teorie T je splnitelná: pro takovou teorii totiž existuje největší index n takový, že $\psi_n \in F$, a stačí tedy jako model F uvážit realizaci $\mathcal{N}'$, v níž se nosič a všechny symboly jazyka $\mathcal{L}$ realizují stejným

způsobem, jako v $\mathcal{N}$, a v níž se konstanta c realizuje jako číslo $n+1$. Dle věty o kompaktnosti je i teorie T splnitelná. Zřejmě každý model teorie T je nekonečný (neboť $Th\mathcal{N}$ obsahuje pro libovolné n výše uvedenou formuli φ_n vynucující alespoň n-prvkový nosič) a tedy dle předchozí věty má T model $\mathcal{M}$ se spočetným nosičem (který je rovněž modelem $Th\mathcal{N}$).

Označme $\omega = c_{\mathcal{M}}$. Tvrdíme, že uvedený model $\mathcal{M}$, braný jakožto realizace jazyka $\mathcal{L}$ (tj. „ignorujeme“ symbol c) nemůže být izomorfní realizaci $\mathcal{N}$. Vskutku, uvažme libovolný homomorfismus Φ z $\mathcal{N}$ do $\mathcal{M}$. Tvrdíme, Φ není surjektivní. Sporem předpokládejme, že je surjektivní. Pak existuje $n \in \mathbb{N}$ takové, že $\Phi(n) = \omega$. Zároveň ale z toho, že Φ je homomorfismus, dostáváme

$$\omega = \Phi(n) = \Phi(S^n_{\mathcal{N}}(0)) = S^n_{\mathcal{M}}(\Phi(0)) = S^n_{\mathcal{M}}(0_{\mathcal{M}}).$$

Protože $\mathcal{M} \models \psi_n$ a $c_{\mathcal{M}} = \omega$, máme $\mathcal{M} \models \exists x\,(x \neq 0 \wedge S^n(0) + x = S^n(0))$. Ovšem uvedená formule není pravdivá v $\mathcal{N}$ a tedy $\mathcal{M} \not\models Th\mathcal{N}$, spor. Nemůže tedy existovat žádný surjektivní homomorfismus z $\mathcal{N}$ do $\mathcal{M}$, zejména tedy nemůže mezi těmito realizacemi existovat izomorfismus.

Příklad A.1 Ukažte, že nemůže existovat ani žádný surjektivní homomorfismus z $\mathcal{M}$ do $\mathcal{N}$.

Neformálně řečeno, model $\mathcal{M}$ se od standardního modelu $\mathcal{N}$ liší tím, že v něm existují prvky které nejsou dosažitelné z „nuly“ konečně mnoha aplikacemi operace S. Vskutku, v logice prvního řádu nelze tuto vlastnost vynutit. Pozorný čtenář si zajisté povšiml souvislosti s nevyjádřitelností tranzitivního uzávěru v logice prvního řádu – viz kapitola 10.

Pokusme se nyní přesněji popsat nějaký takový nestandardní model $\mathcal{M}$ se spočetným nosičem. Bez újmy na obecnosti bychom mohli jakožto onen spočetný nosič vzít opět soubor všech přirozených čísel $\mathbb{N}$ a vhodným způsobem popsat operace $+_{\mathcal{M}}$ a $\cdot_{\mathcal{M}}$ (které se pochopitelně budou od standardního sčítání a násobení notně lišit). Bohužel, něco takového není možné. Plyne to z tzv. *Tennenbaumovy věty*, která říká, že v libovolném nestandardním modelu $\mathcal{M}$ Peanovy aritmetiky, jehož nosičem je soubor $\mathbb{N}$, jsou operace $+_{\mathcal{M}}$ a $\cdot_{\mathcal{M}}$ *nerekurzívní*, tj. nejsou vypočitatelné Turingovým strojem. Zejména tedy nelze doufat v to, že bychom pro tyto operace našli nějaký rozumný předpis.

Přesto však nestandardní modely nějakým způsobem popsat můžeme. Zřejmě platí

$$Th\mathcal{N} \models \forall x\, x + 0 = x \tag{A.1}$$

$$Th\mathcal{N} \models \forall x \forall y \forall z((\exists u\, x + u = y \wedge \exists u\, y + u = z) \rightarrow \exists u\, x + u = z) \tag{A.2}$$

$$Th\mathcal{N} \models \forall x \forall y((\exists z\, x + z = y \wedge \exists z\, y + z = x) \rightarrow x = y). \tag{A.3}$$

To znamená, že pro libovolný model $\mathcal{M}$ teorie $\mathcal{N}$ je binární relace $\leq_{\mathcal{M}}$ na nosiči tohoto modelu zadaná předpisem

$$a \leq_{\mathcal{M}} b \quad \Leftrightarrow \quad \text{existuje individuum } c \in M \text{ t.ž. } a +_{\mathcal{M}} c = b,$$

relací uspořádání na nosiči M. Pro standardní model $\mathcal{N}$ je $\leq_{\mathcal{N}}$ standardní uspořádání přirozených čísel. Tvrdíme, že pro nestandardní modely platí následující:

Věta A.2 Nechť $\mathcal{M}$ je libovolný nestandardní model teorie $Th\mathcal{N}$ se spočetným nosičem M. Pak uspořádaná množina $(M, \leq_{\mathcal{M}})$ je izomorfní[1] lineárně uspořádané množině $(X, \preceq)$, kde

$$X = \{(0, n) \mid n \in \mathbb{N}\} \cup \{(p, m) \mid p \in \mathbb{Q},\, p > 0,\, m \in \mathbb{Z}\}$$
$$(p, n) \preceq (q, m) \text{ pokud } p < q, \text{ nebo } p = q \text{ a } n \leq m$$

(zde $<$ a $\leq$ je standardní ostrá, resp. neostrá nerovnost v příslušném číselném oboru).

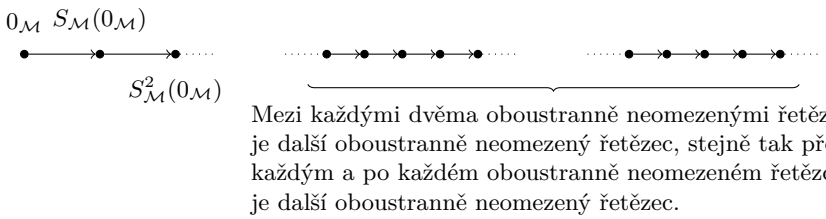
Ačkoliv tedy mohou být symboly $+$ a $\cdot$ v nestandardních spočetných modelech realizovány různými způsoby, uspořádání indukované operací $+_{\mathcal{M}}$ je vždy stejné. Uspořádanou množinu $(X, \preceq)$ si můžeme neformálně představit následovně: vezměme klasicky uspořádanou množinu všech nezáporných racionálních čísel. Odeberme z ní nulu a místo ní přidejme „kopii“ standardně uspořádaných přirozených čísel, tj. stoupající zdola ohraničený nekonečný řetězec. Dále na místo každého pozitivního racionálního čísla umisťme „kopii“ standardně uspořádaných celých čísel, tj. zdola i shora neohraničený nekonečný řetězec. Nakonec všechny prvky přidané na místo nějakého racionálního čísla q prohlašme za ostře větší než libovolný prvek přidaný na místo libovolného racionálního čísla $p < q$. Situaci ilustruje následující obrázek, v němž šipky reprezentují funkci $S_{\mathcal{M}}$.
Podáme neformální zdůvodnění věty A.2. Nejprve si povšimněme, že

$$Th\mathcal{N} \models \forall x \forall y \exists z\, (x + z = y \vee y + z = x),$$

tedy uspořádání $\leq_{\mathcal{M}}$ je lineární. Dále

$$Th\mathcal{N} \models \forall x\, 0 + x = x$$

[1] Zobrazení f mezi dvěma uspořádanými množinami $(A, \leq)$ a $(B, \sqsubseteq)$ se nazývá izomorfismus uspořádaných množin, jestliže je to bijekce a pro libovolnou dvojici prvků $a, a' \in A$ platí $a \leq a' \Leftrightarrow f(a) \sqsubseteq f(a')$.



Obrázek A.1: Náčrt uspořádané množiny $(X, \preceq)$.

a tedy $0_\mathcal{M}$ je nejmenším prvkem uspořádané množiny $(M, \leq_\mathcal{M})$. Podobnými argumenty je možné ukázat, že

$$0_\mathcal{M} \leq_\mathcal{M} S_\mathcal{M}(0_\mathcal{M}) \leq_\mathcal{M} S^2_\mathcal{M}(0_\mathcal{M}) \leq_\mathcal{M} \cdots,$$

a že pro libovolné $n \in \mathbb{N}$ již mezi individui $S^n_\mathcal{M}(0_\mathcal{M})$ a $S^{n+1}_\mathcal{M}(0_\mathcal{M})$ v uspořádání $\leq_\mathcal{M}$ žádné jiné individuum neleží. To ukazuje, že lineárně uspořádaná množina $(M, \leq_\mathcal{M})$ „začíná“ zespoda ohraničeným nekonečným[2] řetězcem izomorfním množině $(\mathbb{N}, \leq)$. Prvky tohoto iniciálního řetězce (tj. prvky tvaru $S^n_\mathcal{M}(0_\mathcal{M})$ pro nějaké n) nazýváme *standardní čísla*, neboť operace $+_\mathcal{M}$ a $\cdot_\mathcal{M}$ se na tomto iniciálním úseku chovají jako standardní sčítání a násobení přirozených čísel. Ostatní individua z M nazveme *nestandardní čísla*. Označme N soubor všech nestandardních čísel v M.

Uvažme binární relaci ekvivalence $\sim$ na souboru N definovanou následovně:

$$a \sim b \quad \text{právě když} \quad \text{existuje } n \in \mathbb{N} \text{ takové, že } S^n_\mathcal{M}(a) = b, \text{ nebo } S^n_\mathcal{M}(b) = a.$$

Nechť C je libovolná třída rozkladu $N/\!\sim$ a $a \in C$ je její libovolný prvek. Pak pro libovolné $n \in \mathbb{N}$ je $S^n_\mathcal{M}(a) \in C$. Navíc pro libovolné $n \in \mathbb{N}$ existuje individuum $a_n \in C$ takové, že $S^n_\mathcal{M}(a_n) = a$. Pokud by tomu tak nebylo, existovalo by individuum $a' \in C$ které by neleželo v obraze $S_\mathcal{M}$. Ovšem jediným takovým individuem je $0_\mathcal{M}$ (protože $\mathcal{M}$ je modelem Peanovy aritmetiky), což je standardní číslo, které nepatří do N. Protože dle definice je třída C tvořena právě těmi individui, ze kterých lze dosáhnout či které jsou dosažitelné z individua a, vidíme, že C jakožto uspořádaná podmnožina uspořádané množiny $(M, \leq_\mathcal{M})$ je oboustranně neohraničený nekonečný řetězec. Navíc lze opět ukázat, že libovolné individuum neležící v C je ostře větší či ostře menší než libovolný prvek C.[3] Vidíme tedy, že část uspořádané

[2] Nekonečným, neboť $Th\mathcal{N} \models \forall x \forall y (S(x) = S(y) \to x = y)$.

[3] Neboť $Th\mathcal{N} \models \forall x \neg\exists y \, (x \neq y \wedge S(x) \neq y \wedge \exists u \exists v \, (x + u = y \wedge y + v = S(x)))$.

množiny $(M, \leq_{\mathcal{M}})$ „nad“ iniciálním segmentem standardních čísel se skládá z (jednoho či více) oboustranně neohraničených řetězců.

Nyní ukážeme, že těchto řetězců je nekonečně mnoho. Vskutku, fixujme libovolné nestandardní číslo $a \in N$. Pro libovolné $n \in \mathbb{N}$ máme

$$Th\mathcal{N} \models \forall x \forall y \forall z\, (\exists u\, (u \neq 0 \wedge x + u = y) \rightarrow \exists u\, (u \neq 0 \wedge (x + z) + u = y + z)).$$

To znamená, že pro libovolné $n \in \mathbb{N}$ je $S^n_{\mathcal{M}}(a) = S^n_{\mathcal{M}}(0_{\mathcal{M}}) +_{\mathcal{M}} a <_{\mathcal{M}} a +_{\mathcal{M}} a$, tedy $a \not\sim a +_{\mathcal{M}} a$. Podobně lze ukázat, že žádné z individuí $a, a +_{\mathcal{M}} a, a +_{\mathcal{M}} a +_{\mathcal{M}} a, \ldots$ neleží ve stejné třídě rozkladu $N/\!\sim$. Vskutku tedy, oboustranně neohraničených řetězců nestandardních čísel nalezneme v $(M, \leq_{\mathcal{M}})$ nekonečně mnoho.

Naše dosavadní charakterizace připouští mj. to, aby $(M, \leq_{\mathcal{M}})$ byla izomorfní množině $\{0\} \times \mathbb{N} \cup \mathbb{N}^+ \times \mathbb{Z}$ s lexikografickým uspořádáním. Ukážeme však, že to není možné, neboť řetězce nestandardních čísel jsou uspořádány „hustě“, tj. mezi každými dvěma neohraničenými řetězci nestandardních čísel nalezneme další neomezený řetězec těchto čísel. Navíc ukážeme, že v uspořádané množině $(M, \leq_{\mathcal{M}})$ nemůže existovat „nejmenší“ či „největší“ řetězec nestandardních čísel. Je známo, že každá hustě a lineárně uspořádaná spočetná množina bez nejmenšího a největšího prvku je izomorfní libovolnému otevřenému intervalu racionálních čísel. Tím ukážeme, že N jakožto uspořádaná podmnožina množiny $(M, \leq_{\mathcal{M}})$ je izomorfní množině $(\mathbb{Q} \cap (0, +\infty)) \times \mathbb{Z}$ s lexikografickým uspořádáním, čímž dokončíme zdůvodnění věty A.2.

Neexistence „největšího“ řetězce je patrná z předchozího odstavce. Neexistence „nejmenšího“ řetězce plyne z toho, že

$$Th\mathcal{N} \models \forall x \exists y\, (y + y = x \vee y + y = S(x)),$$

(intuitivně, každý prvek či jeho následník je „dělitelný dvěma“). Nechť $a \in M$ je libovolné nestandardní číslo a $b \in M$ je nestandardní číslo takové, že $b +_{\mathcal{M}} b = a$ nebo $b +_{\mathcal{M}} b = S_{\mathcal{M}}(a)$. Pak zřejmě $b \leq_{\mathcal{M}} a$[4] a stejně jako výše lze ukázat, že $b \not\sim a$, tedy b leží v „nižším“ řetězci, než a.

Nakonec uvažme libovolná dvě nestandardní čísla a, b taková, že $a \not\sim b$. Bez újmy na obecnosti předpokládejme, že $a \leq_{\mathcal{M}} b$. Dle výše uvedeného existuje individuum d takové, že $d = a +_{\mathcal{M}} b$ nebo $d = S_{\mathcal{M}}(a +_{\mathcal{M}} b)$.

Příklad A.2 Ukažte (podobnými argumenty, jako výše), že $a \leq_{\mathcal{M}} d \leq_{\mathcal{M}} b$ a $a \not\sim d \not\sim b$.

[4] Neboť $Th\mathcal{N} \models \forall x \forall y\, (x + x = S(y) \rightarrow \exists u\, x + u = y$

Poznámka A.3 Formule (A.1), (A.2) a (A.3) jsou ve skutečnosti dokazatelné již z Peanovy aritmetiky. Uspořádání $\leq_{\mathcal{M}}$ lze tedy zadefinovat pro libovolný model $\mathcal{M}$ Peanovy aritmetiky. Lze ukázat, že věta A.2 platí nejen pro nestandardní modely teorie $Th\mathcal{N}$, ale též pro nestandardní modely PA (se spočetným nosičem). Důkaz této silnější věty je pak v podstatě stejný, jako důkaz nastíněný výše. Kdykoliv totiž výše používáme tvrzení tvaru $Th\mathcal{N} \models \varphi$ (které je pro formule φ uvedené v důkazu snadno ověřitelné, neboť standardní přirozená čísla dobře známe), platí ve skutečnosti $PA \vdash \varphi$ (zdůvodnění toho, že nějaká formule je v PA dokazatelná, však může být mnohem obtížnější, neboť příslušný důkaz může být poměrně dlouhý). Pokud tedy v důkazu výše nahradíme všechna tvrzení tvaru $Th\mathcal{N} \models \varphi$ tvrzením tvaru $PA \vdash \varphi$ a přidáme zdůvodnění toho, že φ je v PA vskutku dokazatelná, dostaneme opět korektní metadůkaz.

A.2 Nestandardní analýza

Když Isaac Newton a Gottfried Wilhelm Leibniz pokládali základy matematické analýzy, využívali k tomu podstatně jiný jazyk, než jaký používáme dnes. Základním pojmem tohoto jazyka bylo *infinitezimální číslo*. Tento pojem nebyl v té době přesně definován, intuitivně se tím myslelo jakési „nekonečně malé“ číslo. Tato neformálnost v samých základech analýzy se časem stala nepřijatelnou. Bernard Bolzano a Karl Weierstrass položili formální základy analýzy pomocí dodnes používaných ε-δ definic. Přesto stále přežívala myšlenka na obohacení standardních reálných čísel o nová infinitezimální čísla a konzistentní rozšíření operací $+$ a $\cdot$ na tato nová čísla (tento postup navrhoval už Leibniz), podobně jako komplexní čísla rozšiřují čísla reálná. Ukážeme si, že něco takového je vskutku možné, a to pomocí logických metod prezentovaných v předchozí kapitole.

Uvažme jazyk $\mathcal{L} = \{+, \cdot, d, <\} \cup \{a_x \mid x \in \mathbb{R}\}$ s rovností, kde $+$, $\cdot$ a d jsou binární funkční symboly, $<$ je binární predikátový symbol a pro libovolné $x \in \mathbb{R}$ je a_x nulární funkční symbol. Uvažme dále realizaci $\mathcal{R}$ jazyka $\mathcal{L}$, jejímž nosičem je soubor $\mathbb{R}$ všech reálných čísel a v níž platí, že

- $+$, $\cdot$ a $<$ se realizují jakožto standardní sčítání, násobení a ostrá nerovnost reálných čísel,
- $d_{\mathcal{R}}$ je standardní metrika na $\mathbb{R}$, tj. pro libovolné $x, y \in \mathbb{R}$ máme $d_{\mathcal{R}}(x, y) = |x - y|$,
- pro libovolné $x \in \mathbb{R}$ se a_x realizuje přímo jako číslo x.

Dále uvažme teorii $Th\mathcal{R} = \{\varphi \mid \mathcal{R} \models \varphi\}$. $Th\mathcal{R}$ je úplná teorie obsahující právě ty sentence jazyka $\mathcal{L}$ pravdivé pro standardní reálná čísla. Uvažme jazyk $\mathcal{L}' = \mathcal{L} \cup \{c\}$, kde c je nulární funkční symbol. Dále uvažme teorii $T = Th\mathcal{R} \cup \{a_x < c \mid x \in \mathbb{R}\}$. Stejně jako v předchozí kapitole se snadno ukáže, že každá konečná podteorie teorie T je splnitelná a tedy i teorie T je splnitelná.

Uvažme nějaký model $\mathcal{M}$ teorie T (který je samozřejmě i modelem $Th\mathcal{R}$). V modelu $\mathcal{M}$ jsou pravdivé ty samé sentence jazyka $\mathcal{L}$, které jsou pravdivé pro reálná čísla. Zároveň však v nosiči realizace $\mathcal{M}$ existuje individuum ∞ ostře větší než všechna „standardní“ reálná čísla (která jsou reprezentována konstantami a_x). To ale není všechno. Máme

$$Th\mathcal{R} \models \forall x\, (x \neq a_0 \to \exists y\, x \cdot y = a_1).$$

V $\mathcal{M}$ tedy existuje individuum ∞^{-1} takové, že $\infty \cdot_{\mathcal{M}} \infty^{-1} = a_{1_{\mathcal{M}}}$. Dále máme

$$Th\mathcal{R} \models \forall x \forall y \, ((a_0 < x \wedge x \cdot y = a_1) \rightarrow a_0 < y).$$

Tedy ∞^{-1} je v modelu $\mathcal{M}$ ostře větší než standardní nula. Konečně máme

$$Th\mathcal{R} \models \forall x \forall y \forall u \forall v \, ((a_0 < x \wedge x < y \wedge u \cdot x = a_1 \wedge v \cdot y = a_1) \rightarrow v < u).$$

To ale znamená, že ∞^{-1} je v modelu $\mathcal{M}$ pozitivní „číslo“ ostře menší než libovolné standardní pozitivní reálné číslo. To je ale přesně ta vlastnost, kterou očekáváme od infinitezimálních čísel. Ve světě modelu $\mathcal{M}$ tedy výrazy jako „∞“ či dx, známé z matematické analýzy, nejsou jen syntaktickými zkratkami pro nějaké ε-δ definice, ale reálně existují jako konkrétní matematické objekty, se kterými lze dále pracovat a které je možné používat ve formálních důkazech. Vskutku, vzhledem k tomu že teorie T je konzervativním rozšířením teorie $Th\mathcal{R}$, pak cokoliv, co lze o standardních reálných číslech dokázat v teorii T lze dokázat i v teorii $Th\mathcal{R}$. Důkaz s využitím infinitezimální čísel, jejichž existenci teorie T postuluje, však může být úspornější, jak ukážeme níže.

Povšimněme si, že stejně jako u nestandardních modelů aritmetiky lze i v modelu $\mathcal{M}$ nalézt nekonečně mnoho „nekonečných“ nestandardních čísel (tj. prvků ostře větších než libovolné standardní reálné číslo). To tedy znamená, že zde existuje i nekonečně mnoho různých infinitezimální čísel. Kromě toho lze v nosiči $\mathcal{M}$ nalézt nestandardní čísla která nejsou ani nekonečná ani infinitezimální: např. pro libovolné infinitezimální číslo $\alpha \in M$ je $a_{1_{\mathcal{M}}} +_{\mathcal{M}} \alpha$ nestandardní číslo které není ani infinitezimální (je větší nebo rovno standardní jedničce), ani nekonečné (je menší než libovolné standardní reálné číslo větší než 1). Nestandardní reálná čísla jsou tedy v $\mathcal{M}$ velmi nahusto rozprostřena mezi standardními reálnými čísly. Nestandardní čísla, která nejsou nekonečná, nazveme *omezená*.
Abychom si mohli udělat lepší představu, všimněme si, že

$$Th\mathcal{R} \models \forall x \forall y \forall z \, (d(x,y) + d(y,z) < d(x,z) \vee d(x,y) + d(y,z) = d(x,z)).$$

To mimo jiné znamená, že pro libovolné nestandardní číslo α existuje nejvýše jedno standardní číslo x takové, že $d_{\mathcal{M}}(\alpha, x)$ je infinitezimální. Jinak by totiž v $\mathcal{M}$ existovala dvě standardní čísla infinitezimální vzdálenosti, což zřejmě není možné ($d_{\mathcal{M}}$ se na standardních číslech chová stejně jako v $\mathcal{R}$). Poněkud obtížnější je ukázat, že ke každému omezenému nestandardnímu číslu α existuje právě jedno standardní číslo s výše uvedenou vlastností. Můžeme si tedy představit, že v modelu $\mathcal{M}$ je každé standardní reálné číslo

obklopeno „oblakem“ nestandardních čísel, které jsou k tomuto reálnému číslu nekonečně blízko a ode všech ostatních reálných čísel mají pozitivní vzdálenost.

Výše uvedený jazyk $\mathcal{L}$ umožňuje vyjadřovat se o sčítání a násobení reálných čísel, neumožňuje však vyjadřovat se o obecných reálných funkcích, jako jsou např. trigonometrické funkce, exponenciální funkce, atd. Představme si tedy, že v jazyce $\mathcal{L}$ jsme na začátku měli pro každou reálnou funkci $F\colon \mathbb{R} \to \mathbb{R}$ unární funkční symbol f, který se ve standardním modelu $\mathcal{R}$ realizuje jako funkce F. V nestandardním modelu $\mathcal{M}$ získaném výše uvedenou konstrukcí se každý takový symbol f opět realizuje jako unární funkce, která se na standardních číslech chová naprosto stejně jako v $\mathcal{R}$, je však zároveň definovaná pro nestandardní čísla. Stále platí, že libovolná sentence vyjadřující se o nějaké reálné funkci je pravdivá v $\mathcal{M}$ právě tehdy, když je pravdivá ve standardním modelu $\mathcal{R}$.

Uvažme nyní funkci $F(x) = x^2$. Ukážeme, jak lze za pomocí infinitezimálních čísel dokázat, že derivace funkce F v libovolném bodě x je rovna $2x$. Pro definici derivace funkce je klíčový pojem limity. Korespondenci mezi standardní ε-δ definicí limity a definicí limity pomocí infinitezimálních čísel ozřejmuje následující věta.

Věta A.4 Nechť $f, g \in \mathcal{L}$ jsou libovolné unární funkční symboly. Pak platí

$$\mathcal{R} \models \forall x \forall y \, (a_0 < y \to \exists z \, (a_0 < z \wedge \forall u \, ((u \neq x \wedge d(u,x) < z) \to d(f(u), g(x)) < y))) \tag{A.4}$$

právě tehdy, když platí, že

pro libovolná individua $\xi \in M$, $\alpha \in M$ taková, že $d_{\mathcal{M}}(\alpha, \xi)$ je infinitezimální číslo, je i $d_{\mathcal{M}}(f_{\mathcal{M}}(\alpha), g_{\mathcal{M}}(\xi))$ infinitezimální číslo. (A.5)

Formule v (A.4) je zřejmě pravdivá právě tehdy, když $g_{\mathcal{R}} = G\colon \mathbb{R} \to \mathbb{R}$ je funkce, která každému reálnému číslu x přiřadí limitu funkce F v bodě x.

Důkaz $\Rightarrow$: Nechť $\xi, \alpha \in M$ jsou libovolná individua taková, že $d_{\mathcal{M}}(x, \alpha)$ je infinitezimální číslo. Zvolme libovolné pozitivní $r \in \mathbb{R}$. Podle předpokladu existuje pozitivní $w \in \mathbb{R}$ takové, že

$$\mathcal{R} \models \forall x \forall u \, ((u \neq x \wedge d(u,x) < a_w) \to d(f(u), g(x)) < a_r).$$

Protože T je rozšíření úplné teorie $Th\mathcal{R}$, musí být výše uvedená formule pravdivá i v $\mathcal{M}$. Zejména tedy $d_{\mathcal{M}}(f_{\mathcal{M}}(\alpha), g_{\mathcal{M}}(\xi)) <_{\mathcal{M}} a_{r\,\mathcal{M}}$, neboť $d_{\mathcal{M}}(\alpha, \xi)$

jakožto infinitezimální číslo je v $\mathcal{M}$ ostře menší než $a_{w\mathcal{M}}$. Protože $r \in \mathbb{R}$ bylo zvoleno jako libovolné pozitivní standardní číslo, dostáváme že i číslo $d_{\mathcal{M}}(f_{\mathcal{M}}(\alpha), g_{\mathcal{M}}(\xi))$ je infinitezimální.

$\Leftarrow$: Musíme ukázat, že G je funkce přiřazující každému reálnému číslu x limitu funkce F v bodě x. Zvolme tedy libovolná $x, r \in \mathbb{R}$, $0 < r$. Fixujme $\beta \in M$ libovolné infinitezimální číslo. Dále uvažme individuum $\alpha = a_{x\mathcal{M}} +_{\mathcal{M}} \beta' \in M$, kde β' je libovolné infinitezimální číslo ostře menší než β. Zřejmě $d_{\mathcal{M}}(\alpha, a_{x\mathcal{M}}) = \beta'$. Dle předpokladu je i $d_{\mathcal{M}}(f_{\mathcal{M}}(\alpha), g_{\mathcal{M}}(a_{x\mathcal{M}}))$ infinitezimální číslo, které je dle definice ostře menší než $a_{r\mathcal{M}}$. To znamená, že

$$\mathcal{M} \models \underbrace{\exists y \forall z \left((d(a_x, z) \neq 0 \wedge d(a_x, z) < y) \rightarrow d(f(z), g(a_x) < a_r\right)}_{\varphi}$$

(stačí vzít y rovno β). Ale $\mathcal{M}$ je libovolný model teorie T, která je konzervativním rozšířením teorie $Th\mathcal{R}$. Navíc výše uvedená formule φ je formulí jazyka $\mathcal{L}$. Z toho plyne, že $\mathcal{R} \models \varphi$. To ale znamená, že existuje *reálné číslo* z takové, že pro libovolné reálné y splňující $|x-y| < z$ máme $|G(x)-F(y)| < r$. Protože r bylo zvoleno libovolně, je $G(x)$ skutečně limitou funkce F v bodě x.

Všimněme si, že na to, abychom vyjádřili vlastnost (A.5) v logice prvního řádu, potřebujeme odlišit infinitezimální čísla od neinfinitezimálních. Abychom to dovedli, rozšiřme jazyk $\mathcal{L}'$ o unární predikátový symbol I a uvažme teorii $T' = T \cup \{I(x) \rightarrow (0 < x \wedge x < a_{1/n}) \mid n \in \mathbb{N}\}$ s tímto novým jazykem.

Příklad A.3 Dokažte, že T' je konzervativní rozšíření teorie T (a tedy i konzervativní rozšíření teorie $Th\mathcal{R}$). Zdůvodněte, že v každém modelu teorie T' se I realizuje jako podsoubor souboru všech infinitezimálních čísel v daném modelu.

V jazyce $\mathcal{L}$ bychom fakt, že derivace funkce $F(x) = x^2$ v libovolném bodě x je rovna $2x$ vyjádřili následující formulí ψ:

$$\begin{aligned}\psi = &\forall x \forall \varepsilon \left(a_0 < \varepsilon \rightarrow\right.\\ &\left.\exists \delta \forall u \left((a_0 < d(x,u) \wedge d(x,u) < \delta) \rightarrow d\left(\frac{f(x+u)-f(x)}{u}, x+x\right) < \varepsilon\right)\right).\end{aligned}$$

Protože $\psi \in Th\mathcal{R}$, formule ψ je triviálně dokazatelná v jednom kroku z $Th\mathcal{R}$. To je samozřejmě poněkud podvod, neboť místo abychom tvrzení

„derivací funkce x^2 je funkce $2x$“ skutečně dokázali, odvoláváme se na to, že v reálných číslech tato vlastnost platí, tj. využíváme své metaznalosti analýzy. Správně bychom měli tento důkaz provést s využitím co možná nejmenší a zároveň co možná nejobecnější sady axiomů. Pro charakterizaci reálných čísel se se v logice většinou používá tzv. *teorie reálně uzavřených těles*. Stručně řečeno,[5] jde o teorii s jazykem $\{+, \cdot, <, d, a_0, a_1\}$, která vynucuje aby:

- $+$ a $\cdot$ se realizovaly jako operace komutativního tělesa, přičemž a_0 je neutrální prvek vůči sčítání a a_1 neutrální prvek vůči násobení.
- Symbol $<$ se realizoval jako ireflexivní relace, jejíž reflexivní uzávěr je lineární uspořádání nosiče.
- Pro každý prvek, který je ve výše zmíněném uspořádání ostře větší než a_0, existovala jeho odmocnina, tj. aby platilo

$$\forall x\,(a_0 < x \to \exists y\, y \cdot y = x).$$

- Libovolný polynom lichého stupně měl kořen.

Na vynucení prvních třech bodů přitom stačí konečně mnoho axiomů, na vynucení čtvrtého bodu musíme mít v teorii pro každé liché n axiom

$$\forall x_0 \forall x_1 \ldots \forall x_n \exists y\, x_n \cdot y^n + x_{n-1} \cdot y^{n-1} + \cdots + x_0 = a_0.$$

Zřejmě uvedená teorie je rekurzívní[6] (tj. důkazy v ní je možné provádět počítačem) a navíc je dostatečně jednoduchá na to, abychom důkazy v ní provedené mohli v jistém smyslu považovat za formálnější, než důkazy prováděné v $Th\mathcal{R}$. Důkaz výše uvedené formule ψ v teorii reálně uzavřených těles[7] ovšem není syntakticky zrovna triviální: samotná formule obsahuje

[5] Přesná podoba teorie reálně uzavřených těles se v různé literatuře liší, my zde uvedeme variantu vhodnou pro naše účely.

[6] Překvapivě lze dokázat, že tato teorie je i úplná – jsou z ní dokazatelné přesně ty formule jejího jazyka, které jsou pravdivé pro standardní reálná čísla a teorie $Th\mathcal{R}$ je jejím konzervativním rozšířením. Mohlo by se zdát, že tento výsledek odporuje Gödelově větě o neúplnosti, ale není tomu tak. Teorie reálně uzavřených těles totiž neobsahuje Peanovu aritmetiku. Zejména v jazyce této teorie nelze sestrojit formuli φ s jednou volnou proměnnou x takovou, že $\mathcal{R} \models \varphi[e]$ právě když $e(x)$ je přirozené číslo. Nelze tedy ani formulovat tvrzení tvaru „pro všechna přirozená čísla platí ψ“, bez kterých se důkaz Gödelovy věty o neúplnosti neobejde.

[7] Jazyk této teorie neobsahuje symboly pro odčítání a dělení a funkci druhé mocniny, tyto funkce však lze v tomto jazyce snadno definovat.

čtyři kvantifikátory, navíc v ní ještě dochází k alternaci univerzálního a existenčního kvantifikátoru, čímž se situace značně komplikuje. Ostatně, i kdybychom se nesnažili o přísně formální důkaz (ve smyslu definice 9.1, může se člověk snažící se o přesvědčivý metadůkaz ve změti „epsilonů a delt“ snadno ztratit.

Naproti tomu v teorii T' by pro charakterizaci derivace funkce F stačilo ukázat

$$T' \vdash \forall x \forall h \left(I(h) \to I\left(\frac{f(x+h) - f(x)}{h} - (x + x) \right) \right),$$

přičemž důkaz bychom opět měli vést s použitím co nejmenšího počtu axiomů. Snadno se ovšem ukáže $T' \vdash \frac{f(x+h)-f(x)}{h} = x + x + h$ a to pomocí ryze algebraické manipulace: máme totiž

$$\begin{aligned}
T' &\models \frac{f(x+h) - f(x)}{h} = \frac{(x+h)\cdot(x+h) - x \cdot x}{h} \\
T' &\models \frac{(x+h)\cdot(x+h) - x \cdot x}{h} = \frac{x\cdot x + x\cdot x + x\cdot h + h\cdot h - x\cdot x}{h} \\
T' &\models \frac{x\cdot x + x\cdot h + x\cdot h + h\cdot h - x\cdot x}{h} = \frac{x\cdot h + x\cdot h + h\cdot h}{h} \\
T' &\models \frac{x\cdot h + x\cdot h + h\cdot h}{h} = x + x + h,
\end{aligned}$$

přičemž jednotlivé identity (žádná z nich neobsahuje kvantifikátor!) lze odvodit pouze ze základních axiomů o sčítání, násobení a funkci F. Následně lze snadno odvodit identitu $h = \frac{f(x+h)-f(x)}{h} - (x+x)$. S pomocí této identity a schémat axiomů odvozovacího systému týkajících se symbolu $=$ odvodíme dále $I(h) \to I\left(\frac{f(x+h)-f(x)}{h} - (x+x)\right)$ a dvojnásobným použitím pravidla generalizace dostaneme požadovanou formuli.

Výše uvedený postup kopíruje způsob, kterým důkazy a výpočty provádějí výzkumníci běžně užívající matematické analýzy ve své práci – hodnoty jako $dx, dy, \ldots$, vyskytující se při výpočtech integrálů a řešení diferenciálních rovnic považují za standardní proměnné, se kterými provádějí standardní aritmetické operace, jako je např. krácení (zejména ve fyzice je podobný typ uvažování běžný). Existence nestandardního modelu analýzy s infinitezimálními čísly ukazuje, že tento postup, který může člověku obeznámenému pouze s klasickou analýzou připadat jako černá magie, je ve skutečnosti zcela formalizovatelný.