Matematicko-fyzikální fakulta UK

Predikátová logika

Petr Štěpánek

Praha 2000

Obsah

Kapitola 1

Úvod

Jedním z charakteristických rysů matematiky je práce s abstraktními objekty jako jsou čísla, funkce, relace, plochy, struktury, prostory a mnoho dalších. Podobně i (teoretická) informatika má své abstraktní objekty jazyky, automaty, funkce, procedury, programy, třídy složitosti a jiné.

Matematická logika dává zkoumání takových objektů nový rozměr tím, že studuje jazyk informatiky nebo matematiky, způsoby, jakými jsou abstraktní objekty definovány, jak se s nimi pracuje a zákonitosti, kterými se matematik nebo informatik řídí, když uvažuje o abstraktních objektech.

Matematická logika je poměrně mladá disciplina, která vznikala v 19. století v pracích G. Boolea, B. Bolzana, G. Frege a dalších. Prodělala bouřlivý vývoj v první polovině dvacátého století, který byl spojen se jmény, z nichž uveďme alespoň D. Hilberta, A. Churche, G. Peana, B. Russela, A. Tarského, A. Turinga a který pokračuje dodnes.

Bylo by nesprávné se domnívat, že teprve vznikem matematické logiky dostala matematika pevný řád a logickou výstavbu. Pojem důkazu, který rozhodujícím způsobem ovlivnil výstavbu matematiky, patří již starověké matematice. Znamenal vznik matematiky jako deduktivní vědy. Připomeňme jen známé Eukleidovy knihy, kde je geometrie budována na základě několika postulátů, ze kterých jsou postupně odvozována všechna další tvrzení, věty Eukleidovy geometrie. Každá věta musí mít důkaz, který vychází z výslovně uvedených předpokladů a musí ukázat, že tvrzení věty je odvozeno pouze rozumovou (logickou) úvahou. Ten, kdo dokazuje (mlčky) předpokládá, že rozumí tomu, co je to (neformální) důkaz a že bude schopen přesvědčit o správnosti každého kroku svého odvození. Úlohu rozhodčího ve sporných případech od starověku až do konce 19. století hrála klasická logika, jejíž konečnou podobu zachytil Aristoteles. Matematická logika se ujímá své role až v době, kdy vrcholí snaha po přesném vyjádření základů matematiky vyjasněním pojmu čísla, funkce, množiny a dalších pojmů, které se dostaly do popředí zájmu již rozvinuté matematické analýzy, algebry a geometrie. Tyto problémy již klasická logika nebyla schopna adekvátně řešit.

Nový a nečekaný impuls k rozvoji matematické logiky daly paradoxy teorie množin na přelomu století. Otázku paradoxů, z nichž jmenujme alespoň paradox Russellův, již nebylo možné řešit prostředky klasické logiky. První řešení podal Russell sám v rámci takzvané teorie typů. Dnes nejrozšířenějším řešením je axiomatická výstavba teorie množin na základě predikátové logiky prvního řádu. Matematická logika prošla od počátku století rychlým vývojem, rozvinula mnoho účinných metod, které přispěly k vyjasnění základů matematiky a našly uplatnění v různých oborech matematiky. Dokladem originálního přínosu matematické logiky je pak i skutečnost, že našla uplatnění i v moderních oborech informatiky a v některých oborech techniky, které ještě neexistovaly v době jejího vzniku.

Cílem tohoto textu je seznámit čtenáře se syntaxí a sémantikou predikátové logiky, se základy jejích formálních metod a také s omezeními, které použití formálních metod nutně s sebou nese. Další důležité části matematické logiky jako jsou teorie rekurse, zabývající se studiem metod efektivní vyčíslitelnosti, teorie modelů, která se věnuje studiu formálních teorií pomocí tříd jejích modelů, teorie důkazů, kombinatoriká logika a lambda kalkul, neklasické logiky a další discipliny matematické logiky jsou mimo zamýšlený rámec tohoto textu. K dalšímu studiu matematické logiky doporučujeme monografie ... a příručky ... .

1.1 Jazyk logiky

Matematická logika si zaslouží svůj přívlastek ze dvou důvodů, jednak proto, že zkoumá jazyk matematiky a dalších oborů například informatiky a způsob, jakým se v těchto oborech pracuje, jednak proto, že k tomuto zkoumání používá matematiky. Začneme neformální analýzou jazyků matematiky a informatiky, abych ukázali jejich podstatné součásti, které musí logika zachytit, aby mohla k těmto oborům něco platného říci.

1.1 Neformální jazyk matematiky Matematik pracuje s množstvím různých objektů, ať to jsou čísla, body, úsečky, přímky a další geometrické útvary, zobrazení nebo další složitější matematické struktury. Informatik pracuje například s jazyky v různých abecedách, které jsou vlastně množinami slov, s abstraktními automaty a stroji, které mohou takové jazyky akceptovat, transformovat nebo jinak zpracovávat. Pracuje také s třídami složitosti, které si můžeme představit jako množiny jazyků a s dalšími pojmy.

Některé objekty mají své vlastní jméno, například nula, imaginární jednotka, prázdné slovo, identické zobrazení, zřetězení slov, které označuje jeden zcela určitý objekt. K označení těchto speciálních objektů se používají ustálené symboly, například 0, i, ε, id, $*$, kterým říkáme *konstanty*.

Používají se však i obecná jména, která určují povahu objektu, například číslo, bod, čtverec, ale nijak neurčují o které číslo, bod nebo čtverec se jedná.

Taková obecná jména se používají i v běžném jazyce, kterým mluvíme. K označení takových obecných jmen se používají symboly, kterým říkáme *proměnné*. Jde zpravidla o proměnné z konce abecedy $x, y, z, \ldots$ často s různými indexy. Při práci s objekty matematik, informatik nebo technik používají *operace*, například pracujeme-li s čísly používáme operace součtu, součinu nebo rozdílu, pracujeme-li se slovy používáme zřetězení. Tyto operace mají své zvláštní označení například $+$, $\cdot$, $-$ nebo $*$. Operace například zřetězení je vlastně zobrazení, které dvěma objektům (slovům) přiřazuje další objekt, slovo, které je jejich zřetězením. V tomto případě je operace zřetězení funkcí na množině uspořádaných dvojicí slov. Jazyk logiky bude tedy obsahovat symboly pro operace, kterým budeme říkat *funkční symboly.* Každému funkčnímu symbolu je přiřazeno přirozené číslo, které vyjadřuje takzvanou četnost symbolu, to znamená počet argumentů, na které je symbol aplikován. Je-li četnost symbolu rovna přirozenému číslu n, říkáme také, že symbol je n-ární. Pro četnosti $n, n \leq 3$ se požívá vžitých názvů, symboly s četností jedna se nazývají *unární*, symboly s četností dva se nazývají *binární* a s četností tři se nazývají *ternární*. Tak funkce S následníka přirozeného čísla, $S(n) = n + 1$ je unární, a součet a součin jsou funkce binární. V obecném případě se setkáváme s n-árními funkčími symboly, které označují funkce n proměnných. Je přirozené chápat konstanty, které označují určitý objekt nezávisle na jiných objektech jako 0-ární funkce, tedy funkční symboly, které nevyžadují žádný argument.

Matematik vyjadřuje také vztahy mezi objekty, například *"číslo x je rovno dvojnásobku čísla y"* nebo *"číslo y je menší než jedna"*. Pro tyto vztahy se používá ustáleného označení $=$ a $<$, potom výrazy

$$x = 2 \cdot y \qquad\qquad y < 1 \tag{1}$$

jsou symbolickým vyjádřením vztahů mezi čísly x a y, které jsme uvedli v úvozovkách.

Povšimněme si, že každý z výrazů (1) zastupuje holou větu českého jazyka. V daném případě šlo o vztah mezi dvěma čísly x a y respektive y a 1. Jsou možné i složitější vztahy například *"číslo x leží mezi čísly y a z"*, který určuje vztah mezi třemi čísly. Jazyk logiky bude obsahovat symboly, které vyjadřují vztahy mezi objekty. Budeme jim říkat *predikátové symboly.* Ke každému predikátovému symbolu je dáno přirozené číslo, četnost symbolu, které udává počet jeho argumentů. Tedy symboly $=$ a $<$ jsou binární, vyjadřují vztah mezi dvěma čísly. Obecně se můžeme setkat s n-árními predikátovými symbolu pro $n \geq 1$. Obdobou 0-árních funkčních symbolů by mohly být "logické konstanty" označující pravdu a nepravdu, ale nebudeme jich zde používat. Povšimněme si ještě, že predikátové symboly $=$ a $<$ odpovídají slovesům českého jazyka, mají tedy schopnost tvořit formální obdobu holých vět českého jazyka.

Jazyk logiky bude obsahovat také symboly pro *logické spojky*, které jsou obdobou spojek v českém jazyce a dovolují spojovat jednodušší výrazy ve složitější.

Je to obdoba vytváření souvětí ze dvou vět. K logickým spojkám řadíme symboly & pro *konjunkci*, $\vee$ pro *disjunkci*, $\rightarrow$ pro *implikaci*, $\leftrightarrow$ pro *ekvivalenci* a symbol $\neg$ pro *negaci*.

Užijeme-li výrazy (1), můžeme roli logických spojek ilustrovat následujícím příkladem

$$\begin{array}{ll}
\neg x = 2 \cdot y & \text{čteme } \textit{"neplatí } x = 2 \cdot y\textit{"} \\
x = 2 \cdot y \;\&\; x < 1 & \text{čteme } \textit{"}x = 2 \cdot y \;\; a \;\; x < 1\textit{"} \\
x = 2 \cdot y \vee x < 1 & \text{čteme } \textit{"}x = 2 \cdot y \;\; nebo \;\; x < 1\textit{"} \\
x = 2 \cdot y \rightarrow x < 1 & \text{čteme } \textit{"}x = 2 \cdot y \;\; implikuje \;\; x < 1\textit{"} \\
 & \text{nebo } \textit{"je-li } x = 2 \cdot y \;\; potom \;\; x < 1\textit{"} \\
x = 2 \cdot y \leftrightarrow x < 1 & \text{čteme } \textit{"}x = 2 \cdot y \;\; právě\ když \;\; x < 1\textit{"} \\
 & \text{nebo } \textit{"}x = 2 \cdot y \;\; je\ ekvivalentní \;\; x < 1\textit{"}
\end{array} \tag{2}$$

Matematika používá také formulace *"pro každé x platí ..."* nebo *"existuje x takové, že ..."*. V těchto případech mluvíme o *kvantifikaci proměnných*. Jazyk logiky bude proto obsahovat i symboly $\forall$ a $\exists$, kterým říkáme *obecný* (univerzální nebo velký) *kvantifikátor* a *existenční* (nebo malý) *kvantifikátor*.

V jazyce logiky se uplatní i *pomocné symboly*, které užíváme ke zlepšení čitelnosti výrazů. Pomocné symboly jsou zpravidla různé druhy závorek (,) , [,] , { , } atd.

Je-li x proměnná, potom výrazy

$$\begin{array}{ll}
(\forall x)(x < 1) & \text{čteme } \textit{"pro každé } x \textit{ platí } x < 1\textit{"} \\
 & \\
(\exists x)(x = 2 \cdot y) & \text{čteme } \textit{"existuje } x \textit{ takové, že } x = 2 \cdot y\textit{"}
\end{array} \tag{3}$$

1.2 Symbolický jazyk Ukazuje se, že všechny důležité obraty jazyka matematiky lze zachytit vhodnou volbou odpovídajících symbolů v umělém, symbolickém jazyce. Matematická tvrzení jsou potom vyjádřena určitými výrazy tohoto symbolického jazyka. Symbolické jazyky se také nazývají formální. Pro potřeby různých matematických teorií lze sestrojit různé formální jazyky.

Předchozí analýzu shrnuje následující definice.

1.3 Jazyk 1. řádu obsahuje tyto symboly

- *proměnné* $x,\ y,\ z,\ x_1, x_2, \ldots, y_1, y_2, \ldots$ kterých je neomezeně mnoho;

- *funkční symboly* $f,\ g,\ h,\ \ldots$ ke každému symbolu je dáno přirozené číslo $n \geq 0$, které vyjadřuje jeho četnost;
- *predikátové symboly* $p,\ q,\ r,\ \ldots$ ke každému symbolu je dáno přirozené číslo $n > 0$, které udává jeho četnost. Jazyk může (ale nemusí) obsahovat binární predikátový symbol $=$ k označení rovnosti. Je-li v jazyku obsažen, mluvíme o jazyku s rovností;
- *logické spojky* $\neg,\ \&,\ \vee,\ \rightarrow,\ \leftrightarrow$ vyjadřující negaci, konjunkci, disjunkci, implikaci a ekvivalenci;
- *kvantifikátory* $\forall,\ \exists$ univerzální a existenční;
- *pomocné symboly* $(\ ,\ )\ ,\ [\ ,\ ],\ \{\ ,\ \},\ \ldots$

1.4 Speciální a logické symboly Některé symboly jsou společné všem formálním jazykům, protože odpovídají logickým konstrukcím, budeme proto nazývat *logické symboly*. Jsou to symboly pro proměnné, logické spojky, kvantifikátory, pomocné symboly a symbol rovnosti $=$, je-li v jazyku obsažen. Zbývající symboly, tedy symboly pro funkce a predikáty, označují speciální operace a vztahy v té, které matematické disciplině. Budeme je nazývat *speciální symboly*. Je zřejmé, že jazyk je určen jednoznačně výčtem svých speciálních symbolů (a tím jde-li o jazyk s rovností nebo bez rovnosti). Například jazyk teorie množin je jazyk 1. řádu s rovností, který má jediný speciální symbol ϵ - binární predikátový symbol vyjadřující náležení prvku do množiny (třídy).

1.5 Termy a formule Ze symbolů jazyka se podle jistých pravidel tvoří dva typy výrazů,

- *termy*, které popisují objekty, které vzniknou po provedení v termu naznačených operací,
- *formule*, které vyjadřují různá matematická tvrzení.

Například výraz

$$f(g(x,y),h(x),x)$$

kde $x,\ y$ jsou proměnné a $f,\ g,\ h$ jsou po řadě ternární, binární a unární funkční symboly, je term. Výrazy (1) jsou (atomické) formule.

1.6 Jazyky vyšších řádů Jazyky, které jsme popsali, se nazývají *jazyky 1. řádu*, protože mají jen jeden typ proměnných, kterým říkáme *proměnné pro individua* například čísla, prvky grupy, množiny a podobně. Jazyk neobsahuje další typy proměnných například pro přirozená čísla, množiny čísel, funkce, relace a další typy objektů. Kvantifikovat můžeme tedy jen proměnné pro individua.

Tím se jazyky 1. řádu liší od jazyků vyšších řádů, kde například jazyk takzvané slabé logiky 2. řádu má kromě proměnných pro individua další typ proměnných pro přirozená čísla (nebo obecněji pro konečné množiny individuí), které také dovoluje kvantifikovat. Jazyky 2. řádu obsahují proměnné pro množiny individuí, proměnné pro funkce a relace a dovolují kvantifikovat kromě individuí i množiny individuí a funkce a relace na universu individuí. Logika, která pracuje jen s jazyky prvního řádu, se nazývá *logika prvního řádu.*

1.7 Výrazová síla jazyků prvního řádu Je řada důvodů, pro které lze logiku prvního řádu považovat za základní jazyk matematiky. Ve srovnání s logikami vyšších řádů má jednodušší jazyk, který se neodkazuje k pojmu množiny. Protože jazyk teorie množin je prvního řádu, může logika prvního řádu sloužit jako základní teorie i pro teorii množin. Vzhledem k tomu, že jazyk teorie množin dovoluje konstruovat všechny matematické objekty uvnitř teorie množin, logika prvního řádu může prostřednictvím teorie množin posloužit jako logický základ pro matematiku.

1.8 Příklad Možnosti a omezení logiky prvního řádu budeme ilustrovat na několika příkladech z algebry a teorie množin.

a) K popisu uspořádaných množin vystačíme s jediným speciálním symbolem $<$, binárním predikátovým symbolem pro relaci uspořádání. Pracujeme s jazykem 1. řádu s rovností, který obsahuje jediný speciální symbol $<$. Částečné uspořádání je charakterizováno dvěma formulemi

$$\neg(x < x)$$
$$(x < y \,\&\, y < z) \rightarrow x < z$$

První z nich stanoví, že uspořádání není reflexivní a druhá vyjadřuje tranzitivnost uspořádání.

b) Ke studiu těles je možno použít jazyk s rovností, který obsahuje speciální symboly 0, 1, $+$ a $\cdot$. První dva z nich jsou konstanty označující nulu a jednotku, druhé dva jsou binární funkční symboly, které označují operace sčítání a násobení v tělese. V tomto jazyce lze vyjádřit obvyklé axiomy tělesa, to ponecháme čtenáři jako cvičení. Pomocí termů můžeme také vyjádřit takzvané *přirozené násobky.* Je-li x proměnná, budeme termy

$$x, (x + x), (x + (x + x)), \ldots, \underbrace{(x + (x + (x + \ldots (x + x) \ldots)))}_{n \text{ vskyt } x}$$

označovat zkratkami $1 \cdot x,\ 2 \cdot x,\ 3 \cdot x,\ \ldots, n \cdot x$ a budeme jim říkat *přirozené násobky* x. Uvědomme si, že přirozená čísla nemusí být podmnožinou zkoumaného tělesa a přirozený násobek imituje součin jako opakované přičítání. Výraz $p \cdot x$, kde p je nějaké přirozené číslo může zastupovat term značné délky. Pokud pro nějaké nenulové přirozené číslo p v určitém tělese platí formule

$$p \cdot 1 = 0 \tag{4}$$

říkáme, že těleso má konečnou charakteristiku. Nejmenší nenulové číslo p, pro které platí (4), je *charakteristika tělesa*. Pokud pro žádné nenulové p neplatí (4), říkáme, že těleso má charakteristiku nula. Přidáme-li k axiomům tělesa formule

$$p \cdot 1 \neq 0 \tag{5}_p$$

pro všechna nenulová přirozená čísla p, dostáváme axiomy tělesa charakteristiky nula. Je přirozené položit si otázku, zda lze tělesa charakteristiky nula axiomatizovat také konečným počtem axiomů v logice prvního řádu. Negativní odpověď vyplývá z následujícího tvrzení.

1.9 Věta Každá konečná množina formulí jazyka prvního řádu, které jsou splněny ve všech tělesech charakteristiky nula, je splněna i ve všech tělesech dosti velké konečné charakteristiky.

Konečná množina formulí jazyka prvního řádu tedy nemůže rozlišit mezi tělesy charakteristiky nula a tělesy některých konečných charakteristik. Tato věta je důsledkem takzvané věty o kompaktnosti logiky prvního řádu, se kterou se seznámíme později. Tělesa charakteristiky nula bychom mohli charakterizovat jedinou formulí, kdybychom překročili rámec jazyků prvního řádu, zavedli nový typ proměnných pro přirozená čísla a dovolili jej kvantifikovat. Tím by vznikl jazyk takzvané slabé logiky druhého řádu, který algebra běžně používá. Je-li p proměnná pro přirozená čísla, potom nekonečnou množinu formulí 1. řádu $(5)_p$ lze nahradit jedinou formulí

$$(\forall p)(p \neq 0 \rightarrow p \cdot 1 \neq 0)$$

slabé logiky druhého řádu. Vyjadřovací prostředky slabé logiky druhého řádu jsou silnější než vyjadřovací prostředky logiky prvního řádu. Z toho, co jsme řekli o důkazu věty 1.9 pak plyne, že věta o kompaktnosti (pro logiku prvního řádu) již nemůže platit pro slabou logiku druhého řádu. Zůstaneme-li u jazyka a logiky 1. řádu, poznamenejme, že některé vlastnosti těles, například to, že těleso je Archimedovské, nelze v tomto jazyce vyjádřit ani nekonečným počtem formulí. Zajímavým negativním důsledkem takzvané Lövenheimovy a Skolemovy věty pro logiku prvního řádu je i následující tvrzení

1.10 Věta Žádná množina formulí jazyka prvního řádu teorie těles neurčuje těleso reálných čísel jednoznačně (až na izomorfismus).

Důležitou charakteristikou tělesa reálných čísel je totiž věta o supremu, která mluví o množině reálných čísel a reálném číslu - jejím supremu. Tato věta může být vyjádřena formulí jazyka druhého řádu, který má k dispozici i proměnné pro množiny individuí, zde tedy reálných čísel. Octli bychom se tedy v logice

druhého řádu. Uvedené výsledky se stoupající gradací ukazují na omezení daná jazykem prvního řádu. Může tedy logika prvního řádu vyhovět všem požadavkům tak, aby byla spolehlivým východiskem ke studiu matematiky, informatiky a dalších oborů? Dříve než odpovíme, připomeňme již uvedené příklady. K popisu těles charakteristiky nula chyběla jazyku prvního řádu možnost pracovat vedle proměnných pro individua (prvky tělesa) ještě s proměnnými pro přirozená čísla. Tuto možnost nabízela slabá logika druhého řádu. V případě Archimedovských těles a věty o supremu šlo o to, že vedle promenných pro individua nebyla možnost pracovat s proměnnými pro množiny individuí. Tuto možnost nabízí až logika druhého řádu. V obou případech je zřejmé, že silnější logika v sobě zahrnuje nějaký fragment teorie množin. To nemusíme považovat za adekvátní řešení.

Tyto obtíže odpadnou, budujeme-li matematiku v teorii množin, tedy v teorii s jazykem prvního řádu. Takové řešení je elegantnější, místo, abychom přimíchávali potřebný fragment teorie množin k logice, kterou chceme ponechat co nejprůzračnější, vstoupíme s celou matematikou do teorie množin, která je přijímána jako nejobecneší rámec pro výstavbu matematiky a je sama teorií prvního řádu. S teorií množin může logika prvního řádu bez obtíží pracovat. Vracíme se k naší počáteční tézi, že logika prvního řádu může být adekvátním nástrojem ke studiu matematiky a informatiky. Tato téze je plně oprávněná, pokud budujeme matematiku a informatiku uvnitř teorie množin. Tento fakt ukazuje na specifickou úlohu teorie množin jak ve vztahu k matematice tak k (teoretické) informatice. Předchozí úvaha naznačuje možnost, redukce některých logických systémů vyššího řádu do logiky prvního řádu prostřednictvím teorie množin.

1.2 Formální systém logiky prvního řádu

Popsali jsme jazyk prvního řádu a naznačili jsme jaké jsou jeho vyjadřovací možnosti. Ze symbolů jazyka tvoříme podle přesných syntaktických pravidel dvě důležité třídy slov *termy* a *formule*. Zatím se spokojíme s konstatováním, že termy jsou výrazy, které označují určitá individua, která jsou výsledkem v termu naznačených operací, a formule jsou výrazy, které symbolicky zachycují matematická tvrzení. Některé formule vybíráme jako základní tvrzení - *axiomy*, abychom z nich odvozovali další důsledky. Axiomy a z nich odvozené důsledky nazýváme souhrnně *věty*. Každá věta musí mít důkaz, který je odvozen z axiomů pouze rozumovou (logickou) úvahou. Takové vymezení klade dvě přirozené otázky

- Lze pojem důkazu definovat?
- Jaká jsou logická pravidla, kterými se odvozování řídí?

Odpověď na první otázku je snadnější, protože jsme již zavedli pojem jazyka prvního řádu, který je jazykem symbolickým a formule vyjadřující matematická tvrzení jsou slova - konečné posloupnosti symbolů tohoto jazyka. Přirozený jazyk, kterým budeme mluvit o důkazech, popřípadě o zkoumané axiomatice (teorii), je odlišen a zůstává v roli takzvaného *metajazyka*. Metajazyk je tedy jazyk, kterým se mluví o symbolickém jazyku, jeho konstrukcích, důkazech a zkoumané teorii. Tímto rozlišením se vyhneme nebezpečí sémantických paradoxů, které mohou vzniknout používá-li se přirozený jazyk v obou rovinách, jako jazyk teorie a současně jako jazyk, kterým o teorii mluvíme (paradox lháře a další).

Zvolený přístup také zdůrazňuje finitní hledisko, předmětem studia jsou termy a formule, tedy konečné posloupnosti symbolů, které máme alespoň v principu plně pod kontrolou. Důkazy - jak uvidíme později - jsou posloupnosti formulí sestavené podle přesných syntaktických pravidel: každá formule důkazu je buď axiom nebo je odvozena z některých formulí, které ji předcházejí, podle některého odvozovacího pravidla. Nyní již máme pohromadě všechny součásti formálního systému logiky, které lze identifikovat ve všech logikách, nejenom v predikátové logice prvního řádu, které je věnována tato kniha.

2.1 Formální systém logiky sestává ze tří složek, kterými jsou

- *jazyk* z jehož symbolů vytváříme konečné posloupnosti, slova zejména termy a formule,
- *axiomy*, tedy jisté formule, které přijímáme jako základní tvrzení a
- *odvozovací pravidla* Jsou to syntaktická pravidla, kterými se z konečného počtu formulí mechanicky odvodí další formule, jejich důsledek.

2.2 Důkaz ve formálním systému je konečná posloupnost formulí, jejíž každý člen je buď axiom nebo formule, která je odvozena z některých předchozích formulí pomocí některého odvozovacího pravidla. Říkáme, že nějaká *formule A je větou formálního systému* nebo že *formule A je dokazatelná*, jestliže existuje důkaz, jehož posledním členem je formule A.

Uvedená definice vcelku ideálním způsobem formalizuje intuitivní pojem důkazu. Odvozování vychází z axiomů a postupuje podle přesných syntaktických pravidel, která jsou mechanicky kontrolovatelná v každém kroku. To je odpoveď na naši první otázku.

Na rozdíl od první otázky představuje druhá mnohem hlubší problém a má i filozofický rozměr. V intuitivním pojetí důkazu se jednotlivé kroky odvozují z předchozích kroků (a axiomů) jen rozumovou (logickou) úvahou. Ta je ve formálním důkazu zastoupena volbou odvozovacích pravidel a axiomů logiky. Stojíme tedy před otázkou, jaké axiomy logiky a jaká odvozovací pravidla máme zvolit. Jejich volbou ovlivňujeme třídu formulí, které lze ve vytvářeném formálním systému

dokázat. Predikátová logika řeší tuto otázku pragmaticky odkazem na sémantiku. Axiomy logiky vybírá z *univerzálně platných formulí*, to znamená z formulí, které jsou pravdivé při každé interpretaci symbolů jazyka. Logika tedy nepreferuje některé interpretace před jinými. Odvozovací pravidla jsou volena tak, aby byla korektní, to znamená, aby z pravdivých formulí odvozovala formuli, která bude opět pravdivá.

Je zřejmé, že množina všech univerzálně platných formulí je maximum toho, co by měl k ní konstruovaný formální systém dokázat. Korektnost odvozovacích pravidel a volba axiomů z množiny univerzálně platných formulí zaručuje, že množina vět formálního systému bude podmnožinou množiny všech univerzálně platných formulí. Pokud se nám podaří zvolit axiomy a odvozovací pravidla tak, že množina vět je totožná s množinou všech univerzálně platných formulí říkáme, že takový formální systém je úplný. Úplnost je důležitou charakteristikou formálního systému, protože zaručuje, že pojem dokazatelnosti se kryje s pojmem univerzální platnosti, které se také říká *logická platnost*. Není to ovšem věc samozřejmá.

Nyní můžeme přistoupit k výkladu predikátové logiky prvního řádu. Je účelné rozdělit výklad do několika etap, které odpovídají uceleným částem logiky a mají i své vžité názvy. V první etapě se budeme zabývat formálním systémem, který popisuje vlastnosti logických spojek a který se nazývá *výroková logika*. V další etapě přidáme axiomy a odvozovací pravidla pro kvantifikátory, tím vznikne *predikátová logika bez rovnosti*. Nakonec přidáme axiomy pro predikát rovnosti, který počítáme k logickým symbolům a tak vznikne nejobsažnější formální systém *predikátová logika s rovností*.

V každé etapě se nejprve seznámíme se sémantikou daného jazyka a budeme přesně definovat pojmy pravdivosti formule a korektnosti odvozovacích pravidel, na které jsme se zatím odvolávali bez bližšího vysvětlení. Pro každý formální systém dokážeme také větu o úplnosti.

Kapitola 2

Výroková logika

Výroková logika zevrubně zkoumá syntax a sémantiku formulí, které vzniknou pomocí logických spojek. Přitom odhlíží od dalších symbolů jazyka prvního řádu, zejména od predikátových symbolů a kvantifikátorů. Tím výroková logika připomíná rozbor souvětí přirozeného jazyka, při kterém se nepouštíme do rozboru jednotlivých vět souvětí. Ty chápeme jako nedělitelný celek, jako základní komponenty souvětí. Zavedeme proto jazyk výrokové logiky jako jednodušší verzi jazyka prvního řádu, která odpovídá této situaci. Formule, které ve výrokové logice nelze analyzovat, protože nejsou sestrojeny jen pomocí logických spojek budou v jazyce zastoupeny množinou takzvaných prvotních formulí, které jsou základními komponentami všech formulí výrokové logiky. Každá formule výrokové logiky vznikne z konečného počtu prvotních formulí za použití logických spojek.

2.1 Výrokové formule

V této kapitole definujeme jazyk a formule výrokové logiky, probereme sémantiku výrokové logiky, zavedeme formální systém výrokové logiky, její axiomy a odvozovací pravidlo modus ponens a dokážeme některé jednoduché věty výrokové logiky. Z hlubších výsledků dokážeme větu o kompaktnosti, věty o úplnosti výrokové logiky a věty o standardních tvarech formulí výrokové logiky.

2.1 Prvotní formule Nechť P je neprázdná množina, jejíž prvky mohou být slova nějakého formálního jazyka nebo jen písmena p, q, r, p_1, p_2, p_3, ... Prvky množiny P budeme nazývat *prvotní formule.*

2.2 Jazyk výrokové logiky *Jazyk L_P výrokové logiky nad množinou P* obsahuje prvky množiny P a dále *symboly pro logické spojky* $\neg$ *(negace),* $\&$ *(konjunkce),* $\vee$ *(disjunkce),* $\rightarrow$ *(implikace)* a $\leftrightarrow$ *(ekvivalence).* Jazyk L_P ještě obsahuje *pomocné symboly* (závorky). Říkáme, že P je *množina prvotních formulí jazyka L_P.*

2.3 Výrokové formule jazyka L_P definujeme pomocí následujících syntaktických pravidel.

(i) Každá prvotní formule $p \in P$ je výroková formule.

(ii) Jsou-li výrazy A, B výrokové formule, potom výrazy

$$\neg A, \quad (A \& B), \quad (A \vee B), \quad (A \to B), \quad (A \leftrightarrow B)$$

jsou výrokové formule.

(iii) Každá výroková formule vznikne konečným počtem užití pravidel (i) a (ii).

Definice 2.3 popisuje způsob jakým se složitější výrokové formule konstruují z formulí již sestrojených. Jde o induktivní definici opírající se o konstruktivní pravidla (i), (ii) a uzavírací klauzuli (iii), která zaručuje, že každá výroková formule je konečné slovo.

2.4 Příklad Je-li $P = \{p, q, r, s\}$ množina prvotních formulí, potom výrazy

$p,\ q,\ r$	jsou výrokové formule podle (i)
$(p \vee q)$ a $(p \& q)$	jsou výrokové formule podle (ii)

a nakonec

$((p \vee q) \to (p \& q))$	je výroková formule podle (ii)

Všechny formule, které jsme při konstrukci poslední z nich sestrojili, tedy včetně jí samé, nazýváme podformulemi formule $((p \vee q) \to (p \& q))$. Můžeme říci, že podformule nějaké formule je každé její podslovo, které je samo formulí. Říkáme, že nějaká podformule je vlastní, je-li kratší než daná formule.

Podobně bychom se přesvědčili že výraz

$$(p \to (q \to (r \to s)))$$

je výroková formule, jejíž vlastní podformule jsou

$$p,\ q,\ r,\ s$$
$$(r \to s) \text{ a } (q \to (r \to s))$$

Snadno se nahlédne, že výrazy

$$ppr, \quad (\to p) \quad \text{a} \quad (\to \to$$

nejsou výrokové formule.

2.5 Úmluva Pomocné symboly, které používíme při zápisu formulí slouží především k lepší čitelnosti těchto výrazů. Definice 2.3 stanoví psaní závorek jednoznačne. Při psaní závorek si můžeme dovolit určitou volnost pokud to nebude

na újmu srozumitelnosti. Je například obvyklé vynechávat krajní párové závorky, které jsou definicí formule předepsány, ale ve skutečnosti nic neoddělují. Píšeme například

$$(p \,\&\, q) \vee r \qquad \text{místo} \qquad ((p \,\&\, q) \vee r)$$
$$(p \,\&\, q) \to r \qquad \text{místo} \qquad ((p \,\&\, q) \to r)$$

V některých případech se také přijímá konvence doplňování chybějících závorek při kumulaci doprava. Pak píšeme

$$p_1 \to p_2 \to \ldots \to p_n \quad \text{místo} \quad (p_1 \to (p_2 \to \ldots (p_{n-1} \to p_n) \ldots))$$

Podobné úmluvy lze zavádět podle potřeby.

2.2 Sémantika výrokové logiky

Sémantika výrokové logiky zkoumá pravdivost výrokových formulí. Podle definice 2.3 jsou výrokové formule konstruovány nad množinou prvotních formulí. Přitom prvotní formule jsou ty podformule výrokových formulí, které ve výrokové logice neanalyzujeme, jejich pravdivost či nepravdivost tedy musí být dána zvnějšku zobrazením, které nazýváme pravdivostní ohodnocení. Pravdivost ostatních formulí pak může být odvozena z pravdivosti základních podformulí a ze sémantiky použitých logických spojek.

2.6 Sémantika výrokových formulí Nechť P je množina prvotních formulí jazyka L_P výrokové logiky. *Množina pravdivostních hodnot* je dvouprvková a sestává z hodnot 1 (true) a 0 (false).

(i) *Pravdivostní ohodnocení (valuace) prvotních formulí* je zobrazení $v : \to \{0, 1\}$, které každé prvotní formuli $p \in P$ přiřadí hodnotu 0 nebo 1.

(ii) Pravdivostní ohodnocení v lze jednoznačně rozšířit na všechny formule jazyka L_P. Indukcí podle složitosti formule A definujeme rozšíření $\overline{v}$ zobrazení v předpisem

$$\overline{v}(A) = v(A) \qquad \text{je-li } A \text{ prvotní formule}$$

$$\overline{v}(\neg A) = 0 \qquad \text{je-li } \overline{v}(A) = 1$$
$$= 1 \qquad \text{je-li } \overline{v}(A) = 0$$

$$\overline{v}(A \,\&\, B) = 1 \qquad \text{je-li } \overline{v}(A) = \overline{v}(B) = 1$$
$$= 0 \qquad \text{jinak}$$

$$\begin{aligned}
\overline{v}(A \vee B) &= 0 && \text{je-li } \overline{v}(A) = \overline{v}(B) = 0\\
&= 1 && \text{jinak}\\
\\
\overline{v}(A \to B) &= 0 && \text{je-li } \overline{v}(A) = 1 \text{ a } \overline{v}(B) = 0\\
&= 1 && \text{jinak}\\
\\
\overline{v}(A \leftrightarrow B) &= 1 && \text{je-li } \overline{v}(A) = \overline{v}(B)\\
&= 0 && \text{jinak}
\end{aligned}$$

Říkáme, že $\overline{v}(A)$ je *pravdivostní hodnota formule* A *při ohodnocení* v. *Formule* A *je pravdivá při ohodnocení* v, je-li $\overline{v}(A) = 1$ jinak je *nepravdivá.*

2.7 Tautologie a splnitelné formule (i) Říkáme, že formule A je *tautologie*, je-li pravdivá při každém ohodnocení prvotních formulí.

(ii) *Formule je splnitelná*, je-li pravdivá při nějakém ohodnocení prvotních formulí. Ohodnocení v, takové že $\overline{v}(A) = 1$ nazýváme *modelem formule* A.

(iii) *Množina formulí* T *je splnitelná*, jestliže existuje pravdivostní ohodnocení v, takové že každá formule A z množiny T je pravdivá při ohodnocení v. Takové ohodnocení v nazýváme *modelem množiny formulí* T.

(iv) Říkáme, že formule A je *tautologickým důsledkem množiny formulí* T a píšeme $T \models A$, je-li formule A pravdivá při každém ohodnocení, které je modelem množiny T. Je-li T prázdná množina, píšeme krátce $\models A$. V tomto případě je A pravdivá při každém ohodnocení, to znamená, že A je tautologie.

2.8 Definice 2.7 dává možnost rozhodnout o každé formuli zda je či není tautologií. Například formule

$A \vee \neg A$	(zákon vyloučeného třetího)
$\neg(A \,\&\, \neg A)$	(vyloučení kontradikce)
$\neg(A \,\&\, B) \leftrightarrow (\neg A \vee \neg B)$	(de Morganova pravidla)
$\neg(A \vee B) \leftrightarrow (\neg A \,\&\, \neg B)$	
$\neg\neg A \leftrightarrow A$	(zákon dvojité negace)

2.9 Snadno se zjistí, že pro libovolné ohodnocení v prvotních formulí a libovolné formule A, B, je-li $\overline{v}(A) = \overline{v}(A \to B) = 1$ potom také $\overline{v}(B) =$

1 . Jak uvidíme při studiu formálního systému výrokové logiky, tato vlastnost implikace zaručuje korektnost odvozovacího pravidla *modus ponens*.

Odtud také plyne, že pro libovolnou množinu formulí T, z $T \models A$ a $T \models A \to B$ plyne $T \models B$.

2.10 Věta o kompaktnosti výrokové logiky Množina formulí T je splnitelná, právě když je splnitelná libovolná konečná podmnožina $T_0 \subseteq T$.

Důkaz. a) Je-li T splnitelná, pak existuje ohodnocení v, které je modelem množiny T. Totéž ohodnocení je pak také modelem každé konečné podmnožiny T_0 množiny T.

b) důkaz obrácené implikace je možné provést matematickou indukcí, pokud se omezíme na případ, kdy je množina prvotních formulí a tedy také množina všech formulí výrokové logiky nejvýše spočetná. Provedeme důkaz, který používá větu o kompaktnosti součinu kompaktních topologických prostorů. Ten nepředpokládá žádné omezení mohutnosti množiny prvotních formulí. Věta o kompaktnosti součinu topologických prostorů, která dává i jméno dokazované větě však sama představuje určitou formu axiomu výběru. Poznamenejme, že s nespočetnou množinou prvotních formulí bychom mnoho nedokázali, kdybychom nebyli schopni její prvky dobře uspořádat.

Dvouprvková množina $\{0, 1\}$ pravdivostních hodnot je sama kompaktním prostorem s diskretní topologií. Je-li P množina všech prvotních formulí, potom kartézský součin $\prod_{p \in P}\{0, 1\}$ P exemplářů kompaktního prostoru $\{0, 1\}$ je podle věty o kompaktnosti topologického součinu také kompaktní topologický prostor. Přitom z definice kartézského součinu souboru množin vyplývá, že prvky tohoto součinu jsou právě zobrazení $v : P \to \{0, 1\}$, tedy právě všechna ohodnocení prvotních formulí.

Pro libovolnou formuli A můžeme definovat podmnožinu U_A topologického součinu předpisem

$$U_A = \{ v | \, v : P \to \{0, 1\}, \, \overline{v}(A) = 1\}$$

Protože pravdivostní hodnota $\overline{v}(A)$ závisí jen na hodnotách $v(p)$ pro konečně mnoho prvotních podformulí formule A, je U_A otevřená množina. Jejím doplňkem je množina $U_{\neg A}$, která je ze stejného důvodu také otevřená. Množina U_A je tedy také uzavřená.

Podle předpokladu je každá konečná podmnožina T_0 množiny T splnitelná. Je-li $T_0 = \{A_1, A_2, \ldots, A_n\} \subseteq T$, pak existuje ohodnocení

$$v \in U_{A_1} \cap U_{A_2} \cap \ldots \cap U_{A_n}$$

To znamená, že množiny U_A, $A \in T$ tvoří centrovaný systém obojetných množin v kompaktním prostoru $\prod_{p \in P}\{0, 1\}$. Z kompaktnosti potom plyne, že

také

$$\bigcap \{U_A \,|\, A \in T\} \neq 0$$

a to znamená, že množina T je také splnitelná.

2.11 Důsledek Je-li A formule a T je množina formulí, potom $T \models A$ platí, právě když existuje konečná podmnožina T' množiny T taková, že $T' \models A$.

Důkaz. Snadno se nahlédne, že pro libovolnou množinu formulí S platí $S \models A$, právě když množina $S' = S \cup \{\neg A\}$ není splnitelná. Tvrzení potom plyne z věty o kompaktnosti.

2.3 Formální systém výrokové logiky

Jazyk výrokové logiky je definován a spolu s ním je zaveden i pojem formule.

2.12 Volba axiomů Axiomy výrokové logiky budeme vybírat z logicky platných formulí. Přirozenými kandidáty na logicky platné formule jsou tautologie. Výrokové formule jsou sestrojeny z prvotních formulí jen pomocí logických spojek, které mají jednoznačně určenou interpretaci. To znamená, že logická platnost formule může být zaručena jen tím, že taková formule je pravdivá při každém ohodnocení prvotních formulí. Tak jsou definovány právě tautologie, které jsou pravdivé bez ohledu na pravdivost či nepravdivost svých prvotních podformulí; pravdivost tautologie je dána pouze jejím syntaktickým tvarem. Proto budeme axiomy výrokové logiky vybírat z množiny všech tautologií.

2.13 Redukce jazyka Chceme-li úsporně zvolit množinu axiomů, je výhodné redukovat počet logických spojek na několik základních a ostatní spojky chápat jako odvozené. Ukážeme, že je možné zvolit negaci a implikaci za základní logické spojky a ostatní spojky, konjunkci, disjunkci a ekvivalenci chápat jako spojky odvozené. Formule $(A \,\&\, B)$, $(A \vee B)$, $(A \leftrightarrow B)$ budeme definovat jako zkratky za formule vytvořené jen ze základních spojek, negace a implikace.

$$\begin{array}{lll} (A \,\&\, B) & \text{je zkratka za formuli} & \neg(A \to \neg B) \\ (A \vee B) & \text{je zkratka za formuli} & (\neg A \to B) \\ (A \leftrightarrow B) & \text{je zkratka za formuli} & ((A \to B) \,\&\, (B \to A)) \end{array} \qquad (1)$$

Snadno se přesvědčíme, že pro libovolné ohodnocení v prvotních formulí se sobě rovnají pravdivostní hodnoty levých i pravých stran v (1). Tak například $\overline{v}(A \,\&\, B) = \overline{v}(\neg(A \to \neg B))$, odkud plyne, že

$$(A \,\&\, B) \leftrightarrow \neg(A \to \neg B)$$

je tautologie. Podobně je tomu i se zbývajícími dvěmi zkratkami z (1). Sémanticky jsou zkratky ekvivalentní s vyjádřením pomocí základních spojek.

2.14 Volba odvozovacích pravidel Odvozovací pravidla výrokové logiky volíme tak, aby byla korektní, to znamená, aby z formulí pravdivých při nějakém ohodnocení odvozovala formuli, která je pravdivá při tomtéž ohodnocení. Inspiraci najdeme v odstavci 2.9, který ukazuje, že odvozovací pravidlo *modus ponens* je korektní.

2.15 Formální systém výrokové logiky obsahuje

- *Jazyk* L_P výrokové logiky nad množinou prvotních formulí P.
- *Axiomy* Pro libovolné formule A, B, C jazyka L_P je každá formule tvaru

$$A \to (B \to A) \tag{A1}$$

axiomem výrokové logiky. Dále je axiomem výrokové logiky každá formule

$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \tag{A2}$$

a každá formule

$$(\neg B \to \neg A) \to (A \to B) \tag{A3}$$

- *Odvozovací pravidlo (modus ponens)* Z formulí A a $A \to B$ odvoď formuli B. Místo *modus ponens* píšeme krátce MP.

Formule (A1) - (A3) dávají návod jak z daných formulí A, B, C sestrojit nový axiom výrokové logiky. Nejde tedy o jeden axiom, ale každá z formulí (A1) - (A3) zastupuje nekonečně mnoho speciálních případů. Říkáme proto, že výroková logika je axiomatizována třemi schematy axiomů (A1), (A2) a (A3).

2.16 Pojem důkazu (i) Říkáme, že konečná posloupnost formulí

$A_1, A_2, \ldots, A_n$

je důkazem formule A, jestliže A_n je formule A a pro libovolné $i, 1 \leq i \leq n$ je formule A_i buď axiom nebo je odvozena z předchozích formulí $A_j, 1 \leq j < i$ pravidlem modus ponens.

(ii) Existuje-li důkaz formule A, říkáme, že A je dokazatelná ve výrokové logice nebo že A je větou výrokové logiky, a píšeme $\vdash A$.

2.17 Jednoduché věty výrokové logiky Odvodíme několik jednoduchých vět výrokové logiky, které později použijeme k důkazu věty o úplnosti výrokové logiky.

$$A \to A \tag{v1}$$

Důkaz. Sestrojíme posloupnost formulí, která bude důkazem formule (v1).

$$\vdash A \to ((A \to A) \to A) \tag{2a}$$

$$\vdash (A \to ((A \to A) \to A)) \to [(A \to (A \to A)) \to (A \to A)] \tag{2b}$$

$$\vdash (A \to (A \to A)) \to (A \to A)] \tag{2c}$$

$$\vdash (A \to (A \to A)) \tag{2d}$$

$$\vdash A \to A \tag{2e}$$

Snadno se nahlédne, že (2a) je případem axiomu (A1), (2b) je případem axiomu (A2) a že (2c) je odvozena z (2a) a (2b) podle pravidla modus ponens. Dále (2d) je opět případem axiomu (A1) a nakonec (2e) je odvozena z (2c) a (2d) pravidlem modus ponens.

Posloupnost formulí napravo od $\vdash$ v (2a) - (2e) tedy tvoří formální důkaz věty (v1). Tato jednoduchá formule má důkaz, který obsahuje 5 kroků. Můžeme očekávat, že důkazy dalších formulí budou narůstat do délky. Bude proto užitečné mít tvrzení, který by dovolovalo přecházet od důkazu jedné formule k důkazu jiné formule, aniž bychom potřebovali celý formální důkaz konstruovat. Takové tvrzení bude hovořit o důkazech ve výrokové logice, nebude to tedy formule ani věta výrokové logiky. Z hlediska jazyka, ve kterém bude takové tvrzení vysloveno se jedná o metavětu (větu o důkazech vět výrokové logiky). Z pragmatických důvodů a při zneužití jazyka budeme toto tvrzení nazývat také větou, *větou o dedukci*. Dříve než ji vyslovíme, zavedeme obecnější pojem formálního důkazu.

2.18 Důkaz z předpokladů Nechť T je množina formulí, nechť A je formule. Říkáme, že posloupnost formulí $A_1, A_2, \ldots, A_n$ je důkaz formule A z (množiny předpokladů) T, jestliže A_n je formule A a každá formule A_i, $1 \leq i \leq n$

je buď axiom výrokové logiky, nebo formule z T, nebo je odvozena z předchozích formulí $A_1, A_2, \ldots, A_{i-1}$ pravidlem modus ponens. Jestliže existuje důkaz formule A z předpokladů T, říkáme že *formule A je dokazatelná z T* a píšeme $T \vdash A$.

2.19 Věta o dedukci Nechť T je množina formulí a nechť A, B jsou formule, potom

$$T \vdash A \to B \text{ právě když } T \cup \{A\} \vdash B$$

Tedy implikace $A \to B$ je dokazatelná z předpokladů T právě když samotná formule B je dokazatelná z množiny předpokladů T rozšířené o formuli A. To odpovídá způsobu, jakým se implikace neformálně dokazují. Přesný, ale komplikovaný, množinový zápis předpokladů na pravé straně tvrzení věty o dedukci se zpravidla zjednodušuje do tvaru $T, A \vdash B$.

Demonstrace.[1] a) Je-li $T \vdash A \to B$, pak existuje posloupnost formulí

$$A_1, A_2, \ldots, A_{n-1}, A \to B$$

která je důkazem formule $A \to B$ z předpokladů T. Snadno se nahlédne, že posloupnost

$$A,\ A_1,\ \ldots, A_{n-1},\ A \to B,\ B$$

je důkazem formule B z předpokladů T, A.

b) Nechť $A,\ A_1,\ \ldots, A_n,$ je důkaz formule B z předpokladů T, A. Indukcí pro i, $1 \leq i \leq n$ dokážeme $T \vdash A \to A_i$. Tím pro $i = n$ splníme úkol.

Předpokládejme, že pro $j < i$ jsme již důkazy formulí $A \to A_j$ sestrojili (pro $i = 1$ jde o prázdný předpoklad). Pro formuli A_i podle definice důkazu z předpokladů mohou nastat tři případy.

b1) A_i je axiom výrokové logiky nebo formule z množiny T. Potom sama formule A_i jako posloupnost o jediném členu je svým důkazem z předpokladů T. Dále formule

$$A_i \to (A \to A_i)$$

je případem axiomu (A1), je dokazatelná ve výrokové logice a tím spíše z předpokladů T. Potom posloupnost formulí

$$A_i,\ A_i \to (A \to A_i),\ A \to A_i$$

je důkazem $A \to A_i$ z předpokladů T (užij modus ponens na první dvě formule).

[1] Abychom slovo důkaz nepoužívali ve dvojím smyslu jak pro formální důkazy ve výrokové logice tak pro důkazy (meta)vět o důkazech výrokové logiky, označíme neformální důkaz věty o dedukci slovem demonstrace.

b2) Formule A_i je formule A, potom podle (v1) je formule $A \to A_i$ větou výrokové logiky a tedy je také dokazatelná z předpokladů T.

b3) Formule A_i je odvozena pravidlem modus ponens z formulí A_j, A_k pro nějaká $j, k < i$. Bez újmy na obecnosti můžeme předpokládat, že A_j je tvaru $A_k \to A_i$. Již dříve jsme ukázali, že

$$T \vdash A \to \underbrace{(A_k \to A_i)}_{A_j}$$
$$T \vdash A \to A_k$$

a z axiomu (A2) plyne

$$T \vdash (A \to (A_k \to A_i)) \to ((A \to A_k) \to (A \to A_i)) \tag{3}$$

Užijeme-li dvakrát pravidlo modus ponens dostaneme

$$T \vdash A \to A_i \tag{4}$$

Důkaz formule (4) vznikne tím, že spojíme důkazy formulí $A \to A_j$ a $A \to A_k$ do posloupnosti a na její konec přidáme formule (3), $(A \to A_k) \to (A \to A_i)$ a (4). Tímto postupem nakonec sestrojíme důkaz formule $A \to A_n$ z předpokladů T a tím dokončíme důkaz levé strany tvrzení věty o dedukci. Postup, který jsme zvolili k důkazu druhé implikace ve Větě o dedukci se nazývá *demostrace indukcí podle délky důkazu* a je založen na tom, že sestrojíme důkaz nějaké formule C tím, že přetvoříme již sestrojený důkaz nejaké jiné formule C'.

2.20 Příklad Ve složené implikaci $A \to (B \to C)$ nezáleží na pořadí předpokladů A, B. Plyne to z věty o dedukci. Přesněji, pro libovolnou množinu formulí T a formule A, B, C platí

$$T \vdash A \to (B \to C) \quad \text{právě když} \quad T, A, B \vdash C$$
$$\text{právě když} \quad T \vdash B \to (A \to C)$$

Stejným způsobem se dokáže

$$T \vdash (A \to (B \to C)) \to (B \to (A \to C))$$

a *věta o skládání implikací*

$$\vdash (A \to B) \to [(B \to C) \to (A \to C)]$$

2.21 Další věty výrokové logiky Pomocí věty o dedukci odvozujeme další jednoduché věty výrokové logiky. Nesestrojujeme již formální důkazy podle definice 2.16, ale ukazujeme, že formální důkazy vět existují. Budeme proto mluvit o demonstracích místo o (formálních) důkazech.

$$\vdash \neg A \to (A \to B) \tag{v2}$$

Demonstrace.

$\vdash \neg A \to (\neg B \to \neg A)$	případ axiomu (A1)	(a)
$\neg A \vdash \neg B \to \neg A$	VD (věta o dedukci)	(b)
$\vdash (\neg B \to \neg A) \to (A \to B)$	(A3)	(c)
$\neg A \vdash A \to B$	(b), (c) MP	(d)
$\vdash \neg A \to (A \to B)$	VD	(e)

$\vdash \neg\neg A \to A$ (v3)

Demonstrace.

$\vdash \neg\neg A \to (\neg A \to \neg\neg\neg A)$	(v2)	(a)
$\neg\neg A \vdash \neg A \to \neg\neg\neg A$	VD	(b)
$\vdash (\neg A \to \neg\neg\neg A) \to (\neg\neg A \to A)$	(A3)	(c)
$\neg\neg A \vdash \neg\neg A \to A$	(b), (c) MP	(d)
$\neg\neg A \vdash A$	VD	(e)
$\vdash \neg\neg A \to A$	VD	(f)

2.22 Lemma

$\vdash A \to \neg\neg A$ (v4)

$\vdash (A \to B) \to (\neg B \to \neg A)$ (v5)

$\vdash A \to (\neg B \to \neg(A \to B))$ (v6)

$\vdash (\neg A \to A) \to A$ (v7)

Demonstrace. (v4)

$\vdash \neg\neg\neg A \to \neg A$	(v3)	(a)
$\vdash A \to \neg\neg A$	(A3), (a) MP	(b)

(v5)

$\vdash \neg\neg A, A \to B \vdash A$	(v3) MP	(a)
$\vdash \neg\neg A, A \to B \vdash B$	(a) MP	(b)
$\vdash \neg\neg A, A \to B \vdash \neg\neg B$	(v4), (b) MP	(c)
$\vdash A \to B \vdash \neg\neg A \to \neg\neg B$	(c) VD	(d)
$\vdash A \to B \vdash \neg B \to \neg A$	(A3), (d) MP	(e)
$\vdash (A \to B) \to (\neg B \to \neg A)$	(e) VD	(f)

(v6)

$A, A \to B \vdash B$	MP	(a)
$A \vdash (A \to B) \to B$	(a) VD	(b)
$A \vdash \neg B \to \neg(A \to B)$	(v5), (A3) MP	(c)
$\vdash A \to (\neg B \to \neg(A \to B))$	(c) VD	(d)

(v7)

$\vdash \neg A \to (\neg A \to \neg(\neg A \to A))$	(v6)	(a)
$\neg A \vdash \neg(\neg A \to A)$	(a) 2 x VD	(b)
$\vdash \neg A \to \neg(\neg A \to A)$	(b) VD	(c)
$\vdash (\neg A \to A) \to A$	(A3), (c) MP	(d)

K důkazu věty o úplnosti výrokové logiky budeme kromě vět (v1) - (v7) potřebovat ještě dvě věty, které mají charakter pomocných odvozovacích pravidel. Protože jde o tvrzení o důkazech ve výrokové logice, mají stejný charakter jako věta od dedukci - jsou to metavěty.

2.23 Lemma o neutrální formuli Je-li T množina formulí, A, B jsou formule a je-li $T, A \vdash B$ a $T, \neg A \vdash B$, potom také $T \vdash B$.

Máme-li dva důkazy formule B, jeden z předpokladů T, A a druhý z předpokladů T, $\neg A$, potom existuje důkaz formule B jen z předpokladů T. Říkáme, že formule A se k důkazu formule B chová neutrálně.

Demonstrace. Užitím věty o dedukci z druhého předpokladu dostáváme

$$T \vdash \neg A \to B$$

$$T \vdash \neg B \to \neg\neg A \qquad \text{(v5) MP}$$

$$T, \neg B \vdash \neg\neg A \qquad \text{VD}$$

$$T, \neg B \vdash A \qquad \text{(v3) MP}$$

Z prvního předpokladu a věty o dedukci dostáváme

$$T \vdash A \to B$$

Tedy užitím pravidla modus ponens na dvě předchozí formule

$$T, \neg B \vdash B$$

$$T, \vdash \neg B \to B \qquad \text{VD}$$

$$\vdash (\neg A \to A) \to A \qquad \text{(v7)}$$

$$T \vdash B \qquad \text{MP}$$

Následující lemma spojuje dokazatelnost ve výrokové logice s pravdivostí formulí. Dříve než ho vyslovíme, zavedeme nové označení.

Nechť v je ohodnocení prvotních formulí, nechť B je formule, potom B^v je formule B, jestliže $\overline{v}(B) = 1$ a B^v je formule $\neg B$, jestliže $\overline{v}(B) = 0$.

2.23 Lemma Nechť v je ohodnocení prvotních formulí, nechť A je formule. Předpokládejme, že všechny prvotní podformule formule A jsou mezi formulemi $P_1, P_2, \ldots, P_n$ Potom

$$P_1^v, P_2^v, \ldots, P_n^v \vdash A^v \tag{5}$$

Demonstrace. indukcí podle složitosti formule A. a) Je-li A prvotní formule, pak je to některá z formulí P_i, $1 \leq i \leq n$ a není co dokazovat.

b) Je-li A tvaru $\neg B$ a je-li (5) pro B již dokázáno, mohou nastat dva případy:

b1) Je-li $\overline{v}(B) = 0$, potom B^v je $\neg B$, to je formule A^v a tvrzení (5) plyne z indukčního předpokladu.

b2) Je-li $\overline{v}(B) = 1$, potom B^v je B a z indukčního předpokladu dostáváme

$$P_1^v, P_2^v, \ldots, P_n^v \vdash B$$

Užijeme (v4)

$$\vdash B \to \neg\neg B$$

Podle pravidla modus ponens odvodíme

$$P_1^v, P_2^v, \ldots, P_n^v \vdash \neg\neg B$$

Nyní zbývá si uvědomit, že $\neg\neg B$ je formule A^v a (5) je dokázáno.

c) Nakonec, je-li A tvaru $C \to D$, kde pro formule C, D již bylo tvrzení (5) dokázáno, rozlišujeme čtyři případy:

c1) je-li $\overline{v}(C) = \overline{v}(D) = 1$, potom také $\overline{v}(A) = 1$. Z axiomu (A1) a věty o dedukci dostáváme $D \vdash C \to D$. Přitom D^v je D a podle indukčního předpokladu je dokazatelné z předpokladů (5). Pravidlem modus ponens odvodíme formuli $C \to D$ a to je právě formule A^v. Tím je v tomto případě (5) dokázáno.

c2) je-li $\overline{v}(C) = 1$ a $\overline{v}(D) = 0$, potom $\overline{v}(A) = 0$ Užijeme-li (v6) a větu o dedukci dostáváme

$$C, \neg D \vdash \neg(C \to D)$$

Nyní si uvědomme, že v předpokladech jsou právě formule C^v, D^v a z nich je odvozena formule A^v . Tvrzení opět plyne z indukčního předpokladu.

c3-4) Oba případy mají společnou hodnotu $\overline{v}(C) = 0$. Užijeme-li (v2) a větu o dedukci, dostáváme

$$\neg C \vdash C \to D$$

Tvrzení opět plyne z indukčního předpokladu, protože C^v je formule $\neg C$ a A^v je $C \to D$.

2.4 Věty o úplnosti

Nyní již můžeme dokázat takzvanou slabou formu věty o úplnosti výrokové logiky.

2.24 Věta (Post) Pro libovolnou formuli A výrokové logiky platí

$$\vdash A \quad \text{právě když} \quad \models A$$

Ve výrokové logice jsou dokazatelné právě tautologie.

Demonstrace. a) Nejprve dokážeme, že všechny věty výrokové logiky jsou tautologie. Provedeme to indukcí podle délky důkazu. Ukážeme, že všechny axiomy výrokové logiky jsou tautologie a z 2.9 plyne, že pravidlo modus ponens je korektní, tedy že ze dvou tautologií odvozuje opět tautologii. Při ověřování, že nějaká formule je tautologie můžeme použít obvyklou metodu, která ověřuje, že daná formule je pravdivá pro každé ohodnocení všech jejích prvotních podformulí. V řadě případů je rychlejší metoda nepřímá, která analyzuje nejhorší možný případ. Použijeme ji k ověření, že druhý axiom výrokové logiky je tautologie.

Analyzujeme podmínky, za kterých by existovalo ohodnocení v, takové, že by formule

$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \tag{A2}$$

byla nepravdivá při ohodnocení v. V takovém případě by bylo

$$\overline{v}((A \to B) \to (A \to C)) = 0$$

odkud nutně $\overline{v}((A \to B)) = 1$ a $\overline{v}((A \to C)) = 0$. Z poslední rovnosti dostáváme $\overline{v}(A) = 1$ a $\overline{v}(C) = 0$. K tomu z předposlední rovnosti ještě plyne $\overline{v}(B) = 1$. Odtud $\overline{v}(A \to (B \to C)) = 0$ a při tomto ohodnocení musí být axiom (A2) pravdivá formule. Ukázali jsme, že neexistuje ohodnocení, při kterém by axiom (A2) nebyl pravdivý. Stejný postup lze použít i pro zbývající dva typy axiomů. Tak se ukáže, že všechny věty výrokové logiky jsou tautologie.

b) Nyní ukážeme, že všechny tautologie jsou větami výrokové logiky. Nechť A je tautologie a nechť $P_1, P_2, \ldots, P_n$ jsou všechny prvotní podformule formule A. Zvolme pravdivostní ohodnocení v takové, že

$$\overline{v}(P_1) = \overline{v}(P_2) = \ldots = \overline{v}(P_n) = 1$$

Podle lemmatu 2.23 platí

$$P_1, P_2, \ldots, P_n \vdash A$$

protože A je tautologie a je tedy pravdivá při ohodnocení v stejně jako prvotní formule P_i, $1 \leq i \leq n$. Nyní pozměňme ohodnocení v na w tak, že $w(P_n) = 0$ zatímco ohodnocení ostatních prvotních formulí při v a w je stejné. Potom podle lemmatu 2.23 dostáváme

$$P_1, P_2, \ldots, P_{n-1}, P_n \vdash A$$
$$P_1, P_2, \ldots, P_{n-1}, \neg P_n \vdash A$$

a podle lemmatu o neutrální formuli dostáváme

$$P_1,\ P_2, \ldots, P_{n-1}, \vdash A$$

Opakujeme-li tento postup ještě (n-1)-krát, dokážeme že formule A je věta výrokové logiky. Tím je věta o úplnosti dokázána.

2.25 Bezespornost výrokové logiky Důsledkem věty o úplnosti je fakt, že formální systém výrokové logiky je bezesporný. Nejdříve zavedeme samotný pojem bezespornosti.

Říkáme, že *formální systém je sporný*, je-li každá jeho formule dokazatelná. V opačném případě říkáme, že formální systém je *bezesporný*.

Pojem bezespornosti lze zobecnit i na množiny formulí. Je-li T množina formulí nějakého formálního systému, říkáme, že T *je sporná*, je-li každá formule (daného formálního systému) dokazatelná z množiny T. Jinak říkáme, že T *je bezesporná*.

Je zřejmé, že formální systém je sporný, právě když je sporná prázdná množina formulí. Bezesporné formální systémy a bezesporné množiny formulí se také nazývají *konzistentní*, sporné se nazývají *inkonzistentní*.

Věta o úplnosti 2.24 ztotožnila věty výrokové logiky a tautologie. Snadno se přesvědčíme, že pro libovolnou formuli A formule $\neg(A \to A), (\neg A \& A)$ nejsou tautologie. Podle věty o úplnosti žádná z nich není dokazatelná. To znamená, že formální systém výrokové logiky je bezesporný.

Sémantickým ekvivalentem bezesporné množiny je pojem splnitelné množiny formulí.

2.26 Důsledek Množina formulí výrokové logiky je bezesporná, právě když je splnitelná.

Demonstrace. a) Je-li T splnitelná množina formulí a je-li ohodnocení v jejím modelem, potom z korektnosti pravidla modus ponens 2.9 plyne, že každá formule dokazatelná z T je pravdivá při ohodnocení v. Proto T nemůže být sporná.

b) Pokud množina T není splnitelná, podle věty o kompaktnosti existuje konečná podmnožina $\{A_1, A_2, \ldots, A_n\} \subseteq T$, která je také nesplnitelná.

To znamená, že formule

$$(\neg A_1 \vee (\neg A_2 \vee \ldots \vee (\neg A_{n-1} \vee \neg A_n) \ldots)) \tag{6}$$

je tautologie a je dokazatelná ve výrokové logice.

Na druhé straně je každá formule A_i dokazatelná z T a také

$$T \vdash (A_1 \,\&(A_2 \,\& \ldots \& \,(A_{n-1} \,\&\, A_n) \ldots)) \tag{7}$$

Označíme-li symbolem B formuli (7), potom podle de Morganových pravidel je formule (6) ekvivalentní s formulí $\neg B$. Nyní už není těžké ukázat, že T je sporná množina. Je-li C libovolná formule, potom podle (v2) platí

$$\vdash \neg B \to (B \to C) \tag{8}$$

a dvojím užitím pravidla modus ponens z $\vdash \neg B$, $T \vdash B$ a (8) odvodíme $T \vdash C$.

Dokážeme ještě silnou formu věty o úplnosti.

2.27 Věta o úplnosti výrokové logiky Nechť T je množina formulí a A je formule. Potom platí

$$T \vdash A \quad \text{právě když} \quad T \models A$$

Demonstrace. a) Stejným způsobem jako v důkazu věty 2.24 z definice důkazu z předpokladů, z faktu, že axiomy výrokové logiky jsou tautologie a z korektnosti odvozovacího pravidla modus ponens (2.9) dostáváme, že je-li $T \vdash A$, potom A je tautologickým důsledkem T.

b) Předpokládejme, že $T \models A$. Podle důsledku 2.11 věty o kompaktnosti existuje konečná podmnožina $T_0 = \{A_1, A_2, \ldots, A_n\}$ množiny T taková, že A je tautologickým důsledkem T_0. Indukcí podle n se dokáže následující fakt

$$A_1, A_2, \ldots, A_n \models A \text{ právě když } \models A_1 \to (A_2 \to \ldots \to (A_n \to A) \ldots)$$

tedy podle věty 2.24 také

$$\vdash A_1 \to (A_2 \to \ldots \to (A_n \to A) \ldots)$$

odkud plyne

$$A_1, A_2, \ldots, A_n \vdash A \text{ podle věty o dedukci.}$$

Nakonec také $T \vdash A$, protože $T_0 = \{A_1, A_2, \ldots, A_n\}$ je podmnožinou T.

2.28 Věta o úplnosti v obou formách ukazuje, že přirozený pojem logicky pravdivé formule, pojem tautologie a tautologického důsledku se podařilo plně charakterizovat ve formálním systému výrokové logiky pojmem dokazatelnosti, tedy volbou axiomů a odvozovacího pravidla. Odtud je odvozen i název těchto vět.

Již věta 2.24 dovoluje rozpoznat dokazatelnou formuli, aniž bychom byli nuceni konstruovat její důkaz. Je pouze třeba se přesvědčit, že daná formule je tautologií, to znamená vyšetřit pravdivostní hodnoty při všech ohodnoceních jejích prvotních podformulí. Má-li daná formule n prvotních podformulí, je to celkem 2^n ohodnocení. Tato úloha je tedy exponenciálně složitá.

Pokud bychom se spokojili s tímto řešením, mohli bychom na tomto místě skončit s vyšetřováním operace $\vdash$ dokazatelnosti a logického důsledku a vždy místo ní jen zkoumat operaci $\models$ tautologického důsledku. Chceme-li však hlouběji proniknout do struktury důkazů výrokové logiky, je třeba se pojmem dokazatelnosti ještě zabývat.

Dosud jsme se zabývali jen formulemi sestrojenými ze dvou základních logických spojek negace $\neg$ a implikace $\to$. Budeme se nyní zabývat všemi formulemi, tedy i takovými, které jsou sestrojeny za pomoci odvozených logických spojek konjunkce $\&$, disjunkce $\vee$ a ekvivalence $\leftrightarrow$. Ukážeme několik základních faktů.

2.29 Lemma

$$A \,\&\, B \vdash A \qquad A \,\&\, B \vdash B \tag{v8}$$

$$A, B \vdash A \,\&\, B \tag{v9}$$

Demonstrace. (v8)
Výraz $A \,\&\, B$ je zkratkou za formuli $\neg(A \to \neg B)$. Podle (v2) platí

$$\vdash \neg A \to (A \to \neg B)$$

odkud

$$\vdash \neg(A \to \neg B) \to A \qquad \text{(v3), (v5), MP}$$

Z věty o dedukci dostáváme

$$A \,\&\, B \vdash A$$

Podobně z axiomu (A1) dostáváme

$$\vdash \neg B \to (A \to \neg B)$$

odkud

$$\vdash \neg(A \to \neg B) \to B \qquad \text{(v3), (v5), MP}$$

tedy

$$A \,\&\, B \vdash B$$

(v9) Z (v4) dostáváme

$$A,\, B \vdash \neg\neg B$$

dále z (v6) pomocí věty o dedukci plyne

$$A,\, \neg\neg B \vdash \neg(A \to \neg B)$$

takže celkem

$$A,\, B \vdash A \,\&\, B$$

2.30 Důsledek Uvědomíme-li si, že výraz $A \leftrightarrow B$ je zkratkou za formuli $(A \to B) \,\&\, (B \to A)$, dostáváme

(i) $A \leftrightarrow B \vdash A \to B$

(ii) $A \leftrightarrow B \vdash B \to A$

(iii) $A \to B\ , B \to A \vdash A \leftrightarrow B$

(iv) Je-li $\vdash A \leftrightarrow B$, potom pro libovolnou množinu formulí T platí $T \vdash A$ právě když $T \vdash B$.

2.31 Důsledek

(i) $\vdash A \leftrightarrow (A \,\&\, A)$ (idempotence)

(ii) $\vdash (A \,\&\, B) \leftrightarrow (B \,\&\, A)$ (komutativnost)

(iii) $\vdash ((A \,\&\, B) \,\&\, C) \leftrightarrow (A \,\&\, (B \,\&\, C))$ (asociativnost)

(iv) $\vdash (A_1 \to (A_2 \to \ldots (A_n \to B) \ldots)) \leftrightarrow ((A_1 \,\&\, A_2 \,\&\, \ldots\ A_n) \to B)$

K formulaci pravé strany ekvivalence (iv) poznamenejme, že na uzávorkování konjunkce již nezáleží, protože podle (iii) je konjunkce asociativní.

2.32 Věta o ekvivalenci Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $A_1, A_2, \ldots, A_n$ formulemi $A'_1, A'_2, \ldots, A'_n$. Je-li

$$\vdash A_1 \leftrightarrow A'_1,\ \ldots\ , \vdash A_n \leftrightarrow A'_n \tag{9}$$

potom $\vdash A \leftrightarrow A'$.

Demonstrace. Indukcí podle složitosti formule A.

a) A je prvotní formule nebo některá z formulí $A_1, A_2, \ldots, A_n$. Potom buď A' je A, to v případě že k nahrazení nedojde, nebo A' je některá formule A'_i v případě, že A je formule A_i. Tvrzení věty plyne z předpokladů (9) a (v1).

b) A je tvaru $\neg B$ a pro formuli B již bylo tvrzení věty dokázáno. Tedy $\vdash B \leftrightarrow B'$, odkud $\vdash B \to B'$ a pomocí (v5) dostáváme $\vdash A' \to A$. Podobně se dokáže $\vdash A \to A'$.

c) A je tvaru $B \to C$ a pro formule B, C již bylo tvrzení věty dokázáno. Tedy

$$\vdash B \leftrightarrow B' \qquad \vdash C \leftrightarrow C'$$

Z důsledku 2.30 dostáváme

$$\vdash B' \to B \qquad \vdash C \to C' \tag{10}$$

Následující tvrzení je zobecněním věty o skládání implikací z příkladu 2.20.

$$\vdash (B' \to B) \to ((B \to C) \to ((C \to C') \to (B' \to C'))) \tag{11}$$

Podle téhož příkladu 2.20 můžeme zaměnit druhý a třetí předpoklad implikace (11) a dvojím užitím pravidla modus ponens z (10) dostáváme

$$\vdash (B \to C) \to (B' \to C')$$

a to je

$$\vdash A \to A'$$

Symetricky dokážeme i obrácenou implikaci a tím i tvrzení věty.

2.33 Lemma (de Morganova pravidla)

(i) $\vdash \neg(A \,\&\, B) \leftrightarrow (\neg A \vee \neg B)$

(ii) $\vdash \neg(A \vee B) \leftrightarrow (\neg A \,\&\, \neg B)$

Demonstrace. Z (v3), (v4) a důsledku 2.30 (iii) plyne $\vdash A \leftrightarrow \neg\neg A$. Užitím věty o ekvivalenci dokážeme (i), (ii) se dokazuje obdobně.

$$\vdash \neg(A \,\&\, B) \leftrightarrow \neg\neg(A \to \neg B)$$

$$\vdash \qquad \leftrightarrow (\neg\neg A \to \neg B)$$

$$\vdash \qquad \leftrightarrow (\neg A \vee \neg B)$$

2.34 Důsledek

(i) $\vdash A \to (A \vee B) \qquad \vdash B \to (A \vee B)$

(ii) $\vdash A \leftrightarrow (A \vee A)$ (idempotence)

(iii) $\vdash (A \vee B) \leftrightarrow (B \vee A)$ (komutativnost)

(iv) $\vdash ((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$ (asociativnost)

Demonstrace. (i) Podle definice disjunkce je $\vdash (A \vee B) \leftrightarrow (\neg A \to B)$, proto formule $A \to (A \vee B)$ je obdobou (v2) a $B \to (A \vee B)$ je případ axiomu (A1).

(ii) - (iv) Podle de Morganových pravidel pro libovolné formule C, D je $\vdash \neg(C \vee D) \leftrightarrow (\neg C \,\&\, \neg D)$. Tak lze důkaz (ii) - (iv) převést na důsledek 2.31.

Následující věta je zobecněním lemmatu 2.23 o neutrální formuli.

2.35 Věta o důkazu rozborem případů Nechť T je množina formulí a nechť A, B, C jsou formule. Potom platí

$$T, A \vee B \vdash C \qquad \text{právě když} \qquad T, A \vdash C \quad \text{a} \quad T, B \vdash C\,.$$

Demonstrace. a) Je-li $T, (A \vee B) \vdash C$ potom z důsledku 2.34 (ii) a z věty o dedukci také

$$T, A \vdash (A \vee B) \qquad \text{a} \qquad T, B \vdash (A \vee B)$$

odkud plyne tvrzení věty.

b) Je-li naopak $T, A \vdash C$ a $T, B \vdash C$, Podle věty o dedukci a (v5) dostáváme

$$T, \neg C \vdash \neg A, \neg B$$

odkud z (v9) plyne

$$T, \neg C \vdash \neg A \,\&\, \neg B$$

Užitím de Morganova pravidla a věty o dedukci dostáváme

$$T, \vdash \neg C \to \neg(A \vee B)$$

Odtud tvrzení plyne z axiomu (A3), pravidla modus ponens a věty o dedukci.

2.36 Důsledek (distributivnost konjunkce a disjunkce)

(i) $\quad \vdash (A \vee (B \,\&\, C)) \leftrightarrow ((A \vee B) \,\&\, (A \vee C))$

(ii) $\quad \vdash (A \,\&\, (B \vee C)) \leftrightarrow ((A \,\&\, B) \vee (A \,\&\, C))$

Demonstrace. (i) a) Nejprve dokážeme implikaci zleva doprava. Podle důsledku 2.34 (i) platí

$$A \vdash (A \vee B) \qquad A \vdash (A \vee C)$$

tedy podle (v9)

$$A \vdash (A \vee B) \,\&\, (A \vee C)$$

Podobně z (v8)

$$B \,\&\, C \vdash B \qquad B \,\&\, C \vdash C$$

odkud z důsledku 2.34 (i) použitím pravidla modus ponens dostáváme

$$B \,\&\, C \vdash A \vee B \qquad B \,\&\, C \vdash A \vee C$$

nakonec

$$B \,\&\, C \vdash (A \vee B) \,\&\, (A \vee C)$$

a tvrzení plyne z věty 2.35 o důkazu rozborem případů.

b) Implikaci zprava doleva dokážeme takto. Podle (v8) platí

$$(A \vee B) \,\&\, (A \vee C) \vdash (A \vee B),\ (A \vee C)$$

Podle definice disjunkce je formule $A \vee B$ zkratka za implikaci $\neg A \to B$. Odtud plyne

$$\neg A,\ A \vee B \vdash B \qquad \neg A,\ A \vee C \vdash C$$

Pomocí (v9) a věty o dedukci pak dostáváme

$$(A \vee B) \,\&\, (A \vee C) \vdash \neg A \to (B \,\&\, C)$$

tedy

$$\vdash ((A \vee B) \,\&\, (A \vee C)) \to (A \vee (B \,\&\, C))$$

2.5 Standardní tvary výrokových formulí

Na závěr kapitoly o výrokové logice ukážeme, že každou výrokovou formuli lze ekvivalentně vyjádřit ve dvou standardních tvarech. Při definici syntaktických tvarů standardních forem máme možnost volit spojky, které použijeme a potom ještě pořadí, v jakém budou použity. V předchozím výkladu jsme ukázali, že konjunkce a disjunkce mají řadu pěkných vlastností, jsou komutativní, asociativní a distributivní. Základní spojky negace a implikace podobné vlastnosti nemají, nicméně bez negace se při vyjádření výrokových formulí nemůžeme obejít. Standardní formy budeme vytvářet pomocí negace, disjunkce a konjunkce, přitom negaci použijeme jako první jen u prvotních formulí. Jedna standardní forma bude používat disjunkci před konjunkcí a druhá naopak. Tak vzniknou konjunktivní a disjunktivní standardní tvary formulí.

2.37 Syntax standardních tvarů výrokových formulí Nechť L_P je jazyk výrokové logiky nad množinou prvotních formulí P.

(i) Indukcí definujeme následující typy formulí

- *prvotní formule*

- *literály* jsou prvotní formule a negace prvotních formulí
- *klauzule* jsou disjunkce literálů

(ii) Říkáme, že *formule je v konjunktivním tvaru*, je li to konjunkce klauzulí.

(iii) Říkáme, že *formule je v disjunktivním tvaru*, je-li to disjunkce konjunkcí literálů.

Tedy formule v konjunktivním tvaru se vytvářejí tak, že nejprve použijeme negaci jen u prvotních formulí, potom disjunkcí z literálů tvoříme klauzule a nakonec konjunkcí z klauzulí vytvoříme konjunktivní tvar. Disjunktivní tvar formule se tvoří obdobně, jen s opačným pořadím použití konjunkce a disjunkce. Z literálů tvoříme nejprve konjunkce a z nich nakonec disjunkce.

Konjunktivní tvar formulí nachází uplatnění například ve strojovém dokazování vět, zatímco disjunktivní tvar formulí má blíže k databázovým aplikacím.

2.38 Příklad Nechť $p_1, p_2, \ldots$ jsou prvotní formule.

a) $(p_1 \vee \neg p_3 \vee p_6) \,\&\, p_1 \,\&\, (p_2 \vee p_7)$ je formule v konjunktivním tvaru.

b) $(p_2 \,\&\, \neg p_3 \,\&\, \neg p_{10} \,\&\, p_{16}) \vee (\neg p_1 \,\&\, \neg p_3) \vee (p_2 \,\&\, \neg p_7) \vee (\neg p_5 \,\&\, \neg p_9)$

je formule v disjunktivním tvaru.

2.39 Věta Ke každé formuli A výrokové logiky lze sestrojit formuli A_k v konjunktivním tvaru a formuli A_d v disjunktivním tvaru tak, že

$$\vdash A \leftrightarrow A_k \quad \text{a} \quad \vdash A \leftrightarrow A_d$$

Demonstrace. Indukcí podle složitosti formule A sestrojujeme její ekvivalentní konjunktivní a disjunktivní tvar.

a) Je-li A prvotní formule, potom A je v konjunktivním i disjunktivním tvaru a není co dokazovat.

b) Předpokládejme, že A je formule $\neg B$ a že konjunktivní tvar B_k a disjunktivní tvar B_d formule B již byly sestrojeny. Z předpokladu

$$\vdash B \leftrightarrow B_d$$

vyplývá

$$\vdash \neg B \leftrightarrow \neg B_d$$

Je-li B_d tvaru $B_1 \vee B_2 \vee \ldots \vee B_n$, kde B_i je tvaru

$$L_1^i \,\&\, L_2^i \,\&\, \ldots \,\&\, L_{m_i}^i \quad \text{pro} \quad i \leq n$$

potom podle de Morganových pravidel

$$\vdash \neg B \leftrightarrow (\neg B_1 \,\&\, \neg B_2 \,\&\, \ldots \,\&\, \neg B_n)$$

a pro každé $i \leq n$ je

$$\neg B_i \leftrightarrow (\neg L_1^i \vee \neg L_2^i \vee \ldots \vee \neg L_{m_i}^i)$$

Označíme-li A_i formuli, která vznikne z $(\neg L_1^i \vee \neg L_2^i \vee \ldots \vee \neg L_{m_i}^i)$ tím, že vynecháme dvojité negace u prvotních formulí v negovaných literálech, potom A_i je konjunkce literálů a

$$\vdash A \leftrightarrow (A_1 \,\&\, A_2 \,\&\, \ldots A_n)$$

kde na pravé straně ekvivalence je konjunktivní tvar A_k formule A.

Stejným způsobem se pomocí de Morganových pravidel z formule $\neg B_k$ sestrojí disjunktivní tvar A_d formule A.

Ukázali jsme, že k negaci formule v konjunktivním tvaru lze sestrojit ekvivalentní formuli v disjunktivním tvaru a k negaci formule v disjunktivním tvaru lze sestrojit ekvivalentní formuli v konjunktivním tvaru.

c) Předpokládejme, že formule A je tvaru $B \to C$ a že formule B_d, C_d, B_k, C_k jsou již sestrojeny. Podle definice disjunkce

$$\vdash (B \to C) \leftrightarrow (\neg B \vee C) \tag{12}$$

K sestrojení disjunktního tvaru formule A stačí sestrojit disjunktivní tvar D formule $\neg B_k$ a formule $D \vee C_d$ je disjunktivním tvarem formule A.

Konjunktivní tvar formule A sestrojíme pomocí distributivity konjunkce a disjunkce. Vyjdeme opět z ekvivalence (12), ale místo formule $\neg B_k$ v disjunkci uvažujeme formuli $\neg B_d$. K této formuli sestrojíme ekvivalentní formuli v konjunktivním tvaru $D_1 \,\&\, D_2 \,\&\, \ldots \,\&\, D_n$, kde formule D_i, $i \leq n$ jsou klauzule, tedy disjunkce literálů. Dostáváme

$$\vdash A \leftrightarrow ((D_1 \,\&\, D_2 \,\&\, \ldots \,\&\, D_n) \vee C_k)$$

odkud z distributivity plyne

$$\vdash A \leftrightarrow ((D_1 \vee C_k) \,\&\, (D_2 \vee C_k) \,\&\, \ldots \,\&\, (D_n \vee C_k)) \tag{13}$$

Dále formule C_k je v konjunktivním tvaru je tedy konjunkcí klauzulí $D_1' \,\&\, D_2' \,\&\, \ldots \,\&\, D_m'$. Z distributivity pak pro každé i, $i \leq n$ platí

$$(D_i \vee C_k) \leftrightarrow ((D_i \vee D_1') \,\&\, (D_i \vee D_2') \ldots (D_i \vee D_m'))$$

kde na pravé straně je již formule v konjunktivním tvaru. Proto i pravou stranu ekvivalence (13) lze převést do konjunktivního tvaru. Tím je věta dokázána.

2.40 Důkazy a demonstrace V této kapitole jsme poprvé pracovali s nějakým formálním systémem a proto jsme důsledně rozlišovali mezi formálním

důkazem ve smyslu uvedené definice a demonstrací, která na některých místech přechází od dokazatelnosti jedné formule k dokazatelnosti jiné formule aniž by konstruovala všechny kroky jejího důkazu. Sestrojili jsme jen jeden formální důkaz jednoho z nejjednodušších tvrzení výrokové logiky, formule (v1). Upozornili jsme na to, že formální důkazy dalších tvrzení rostou do délky, protože použití nějaké již dokázané věty znamená připojit její důkaz k důkazu, který konstruujeme. To je v principu možné, ale těžko proveditelné. V Russellově a Whiteheadově knize *Principia Mathematica* je dán odhad, že formální důkaz věty $0 \neq 1$ v jejich formálním systému aritmetiky má nejméně tři tisíce kroků. Proto jsme u prakticky všech dokazovaných vět výrokové logiky uváděli demonstrace opírající se o větu o dedukci.

Máme za to, že čtenář již umí rozlišit mezi formálním důkazem ve smyslu uvedené definice a neformální demonstrací, která zachycuje hlavní kroky důkazu. V dalším výkladu budeme slovo důkaz, jak je v literatuře obvyklé, používat i k označení demonstrací.

2.6 Cvičení A

Dokažte

Implikace

a) $(A \to (B \to C)) \to (B \to (A \to C))$ (zaměnitelnost antecedentů implikace)

b) $(A \to B) \to [(B \to C) \to (A \to C)]$ (skládání implikací)

c) $(A \to B) \to (\neg B \to \neg A)$

d) $(\neg A \to B) \to (\neg B \to A)$

e) $(A \to \neg B) \to (B \to \neg A)$

Konjunkce

a) $(A \,\&\, B) \to A$

b) $(A \,\&\, B) \to B$

c) $(A \to (B \to (A \,\&\, B)))$

d) $(A \,\&\, B) \to (B \,\&\, A)$ (komutativnost)

e) $((A \,\&\, B) \,\&\, C) \to (A \,\&\, (B \,\&\, C))$ (distributivnost)

$(A \,\&\, (B \,\&\, C)) \to ((A \,\&\, B) \,\&\, C)$ (distributivnost)

f) $(A \,\&\, A) \to A$ (idempotence)

$A \to (A \,\&\, A)$ (idempotence)

g) $(A \to B) \to [(C \to D) \to ((A \,\&\, C) \to (B \,\&\, D))]$

Ekvivalence

a) $(A \leftrightarrow B) \to (A \to B)$

b) $(A \leftrightarrow B) \to (B \to A)$

c) $(A \to B) \to [(B \to A) \to (A \leftrightarrow B)]$

d) $(A \leftrightarrow B) \leftrightarrow (B \leftrightarrow A)$

e) $(A \leftrightarrow B) \leftrightarrow (\neg A \leftrightarrow \neg B)$

f) $(\neg A \to \neg B) \leftrightarrow (B \to A)$

g) $(A \to \neg B) \leftrightarrow (B \to \neg A)$

h) $(\neg A \to B) \leftrightarrow (\neg B \to A)$

Disjunkce

a) $A \to (A \vee B)$

b) $B \to (A \vee B)$

c) $(A \to C) \to [(B \to C) \to ((A \vee B) \to C)]$

$(A \to C) \to [(B \to D) \to ((A \vee B) \to (C \vee D)]$

d) $(A \vee A) \leftrightarrow A$ (idempotence)

e) $(A \vee B) \leftrightarrow (B \vee A)$ (komutativnost)

f) $((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$ (asociativnost)

Věta o důkazu rozborem případů

Nechť T je množina formulí, nechť A, B, C jsou formule, potom platí

$T, (A \vee B) \vdash C$, právě když $T, A \vdash C$ a $T, B \vdash C$

(k důkazu použijte lemmatu o neutrálni formuli)

Distributivita

a) $(A \,\&\, (B \vee C)) \leftrightarrow [(A \,\&\, B) \vee (A \,\&\, C)]$

b) $(A \,\&\, (B_1 \vee B_2 \vee \ldots \vee B_n)) \leftrightarrow [(A \,\&\, B_1) \vee (A \,\&\, B_2) \vee \ldots \vee (A \,\&\, B_n)]$

c) $(A \vee (B \,\&\, C)) \leftrightarrow [(A \vee B) \,\&\, (A \vee C)]$

d) $(A \vee (B_1 \,\&\, B_2 \,\&\, \ldots \,\&\, B_n)) \leftrightarrow [(A \vee B_1) \,\&\, (A \vee B_2) \,\&\, \ldots$
$\&\, (A \vee B_n)]$

Normální tvary výrokových formulí

Nechť $A, B, C, D, E, ...$ jsou prvotní formule. Sestrojte konjunktivní tvary následujících formulí

a) $((A \vee B) \to (A \,\&\, B))$

b) $(((A \to B) \to B) \to A)$

c) $(\neg(A \vee \neg A) \to (A \vee \neg A))$

d) $(A \to \neg(A \to \neg A))$

e) $((A \,\&\, B) \leftrightarrow (B \,\&\, A))$

f) $((A \to B) \vee (B \to A))$

$(C \to (D \to E)) \to [(C \to E) \to (D \to E)]$

$(C \to \neg D) \leftrightarrow (D \to \neg C)$

$(\neg E \to F) \leftrightarrow (\neg F \to E)$

g) Sestrojte disjunktivní tvary formulí a) - f).

h) Rozhodněte, které z formulí a) - f) jsou dokazatelné ve výrokové logice. Dokažte je.

2.7 Cvičení B

1. (Indukce podle složitosti formule)
   Nechť Γ je množina všech formulí výrokové logiky taková, že

   (i) Γ obsahuje množinu všech prvotních formulí.

   (ii) Jsou-li A, B formule výrokové logiky, $A, B \in \Gamma$, potom i $\neg A$, $(A \,\square\, B) \in \Gamma$, kde $\square$ je symbol &, $\vee$, $\to$ nebo $\leftrightarrow$.

   Potom každá výroková formule je prvkem Γ.

2. Nechť L je nějaký jazyk, libovolnou konečnou posloupnost σ_0, $\sigma_1 \ldots \sigma_n$ symbolů jazyka L nazveme výrazem (slovem) jazyka L, $a = \sigma_0 \ldots \sigma_n$, $b = \sigma_{n+1} \ldots \sigma_{n+m}$, potom výraz $\sigma_0 \ldots \sigma_n \, \sigma_{n+1} \ldots \sigma_{n+m}$, který vznikne připojením slova b za slovo a označíme ab a nazveme ho zřetězením (konkatenace) slov a, b. Označíme-li symbolem o prázdnou posloupnost symbolů, potom pro libovolná slova a, b, c platí

$$ao = oa = a, \; (ab)c = a(bc).$$

Zřetězení je tedy asociativní operace na množině všech slov. Tato operace je komutativní, právě když jazyk L obsahuje nejvýš jeden symbol.

3. (Polský zápis formulí)
Nechť L' je jazyk výrokové logiky s množinou P prvotních formulí, ale bez pomocných symbolů (závorek). Následující syntaktická pravidla definují bezzávorkový (polský) zápis formulí výrokové logiky. Přitom slovo, které sestává z jediného symbolu σ ztotožňujeme s tímto symbolem.

   (i) Každá prvotní formule je formule.

   (ii) Jsou-li výrazy a, b formule, potom výrazy $\neg\, a$, $\vee\, ab$, $\&\, ab$, $\rightarrow\, ab$, $\leftrightarrow\, ab$ jsou také formule.

   (iii) Každá formule vznikne konečným použitím pravidel (i) a (ii).

   Platí:

   (a) Je-li a formule (podle předchozí definice), potom buď a je prvotní formule, nebo a je tvaru $\neg b$ nebo $\square\, ab$, kde b, c jsou formule a $\square$ je některý ze symbolů pro logické spojky $\&$, $\vee$, $\rightarrow$, $\leftrightarrow$.

   (b) Je-li a formule tvaru $a_0 a_1 \ldots a_n$, kde a_i, $i \leq n$ jsou formule nebo slova sestávající z jediného symbolu pro logickou spojku, potom výraz $a_0 \ldots a_i$ pro žádné $i < n$ není formule.

   (c) Je-li a formule tvaru $\neg b$ nebo $\square\, bc$ (viz bod(a)), potom symbol $\square$ a formule b, c jsou jednoznačně určeny.

   [Návod:

   (a) se dokáže indukcí podle složitosti formule,

   (b) indukcí podle počtu zřetězených slov, (c) je důsledkem (b).]

   Tento druh zápisu formulí se také nazývá prefixní, podle toho, že symbol pro logickou spojku předchází obě formule, které spojuje. Jeho výhodou je jednoznačné členění formulí bez použití závorek. *Obvyklejší zápis formulí zavedený v textu se nazývá infixní.*

4. Formulujte obdobu (a) – (c) z předchozího cvičení pro infixní zápis formulí.

5. Odvozovací pravidlo: z formulí $\neg A \vee B$, $A \vee C$ odvoďte formuli $B \vee C$ se nazývá *pravidlo řezu*. V různých variantách je typické pro Gentzenovy sytémy výrokové logiky. Pravidlo řezu se používá při takzvaném strojovém dokazování vět rezoluční metodou na samočinných počítačích.
Dokažte, že pravidlo řezu může nahradit pravidlo modus ponens a naopak.

   [Návod:

(a) ve výrokové logice pro libovolné formule A, B, C dokažte $(\neg A \vee B)$, $(A \vee C) \vdash (B \vee C)$.

(b) ve formálním systému, který vznikne z výrokové logiky vypuštěním odvozovacího pravidla modus ponens a přidáním pravidla řezu, pro libovolné formule A, B dokažte A, $A \to B \vdash B$. Požijte 6(a).]

6. Ukažte, že schema (A3) může být nahrazeno následujícím schematem

(A4) $$(\neg B \to \neg A) \to ((\neg B \to A) \to B)$$

pro libovolné formule A, B. To znamená, že každá formule (A4) je větou výrokové logiky a každá formule (A3) je větou formálního systému, který vznikne z výrokové logiky nahrazením schematu (A3) schematem (A4).

7. Konečnou posloupnost nul a jedniček budeme nazývat *Booleovská posloupnost*. Říkáme, že funkce f je *Booleovská funkce* n proměnných, jestliže f přiřazuje každé Booleovské posloupnosti délky n hodnotu 0 nebo 1.
Každé formuli A výrokové logiky, která obsahuje n prvotnívh formulí, lze jednoznačně přiřadit Booleovskou funkci f_A: Jsou-li $P_1, \ldots, P_n$ všechny prvotní formule, které se vyskytují v A a je-li $p_1, \ldots, p_n$ libovolná Booleovská posloupnost délky n, položíme

$$f_A(p_1, \ldots, p_n) = \overline{v}(A),$$

kde v je nějaká valuace prvotních formulí taková, že $v(P_i) = p_i$ platí pro $i \leq n$. (Na ohodnocení ostatních prvotních formulí nezáleží).
Přirozeným způsobem lze přiřadit Booleovské funkce i logickým spojkám. Negaci odpovídá unární funkce $f_\neg$ definovaná předpisem

$$f_\neg(0) = 1, f_\neg(1) = 0.$$

Ostatním spojkám odpovídají binární funkce definované takto:

p_1	p_2	$f_\&(p_1,p_2)$	$f_\vee(p_1,p_2)$	$f_\to(p_1,p_2)$	$f_\leftrightarrow(p_1,p_2)$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Je zřejmé, že pro libovolnou formuli A lze Booleovskou funkci f_A definovat pomocí funkcí přiřazených logickým spojkám, dokonce jen pomocí funkcí $f_\neg$ a $f_\to$.
Říkáme, že množina F Booleovských funkcí tvoří úplný systém, jestliže každou Booleovskou funkci lze definovat pomocí Booleovských funkcí množiny F.

(a) Dokažte, že dvouprvková množina $\{f_\neg, f_\to\}$ sestávající z funkcí $f_\neg$, $f_\to$ tvoří úplný systém.

(b) Dokažte, že množiny $\{f_\neg, f_\&\}$, $\{f_\neg, f_\vee\}$ tvoří úplný systém.

(c) Dokažte, že množiny $\{f_\&, f_\vee\}$, $\{f_\neg, f_\leftrightarrow\}$ úplný systém netvoří.

[Návod:

(a) pomocí věty o disjunktním tvaru výrokové formule ukažte, že každá Booleovská funkce je tvaru f_A pro jistou formuli.

(b) ukažte, že implikaci lze vyjádřit pomocí negace a konjunkce (disjunkce).

(c) ukažte, že negaci nelze vyjádřit pomocí konjunkce a disjunkce a že implikaci nelze vyjádřit pomocí negace a ekvivalence.]

8. Připomeňme, že formule A je v konjunktivním (disjunktivním) tvaru, je-li konjunkcí (disjunkcí) konečného počtu formulí $A_1, \ldots, A_n$, z nichž každá je disjunkcí (konjunkcí) prvotních formulí a negací prvotních formulí. Formulím $A_1, \ldots, A_n$ říkáme složky formule A.

   (a) Ukažte, že formule A v konjunktivním tvaru je tautologie, právě když každá její složka obsahuje dva opačné literály (to znamená jistou prvotní formuli a její negaci).

   (b) Ukažte, že formule A v disjunktivním tvaru je splnitelná, tedy pravdivá při alespoň jednom ohodnocení, právě když alespoň jedna složka formule A neobsahuje dva opačné literály.

9. Je-li T množina formulí, ukažte, že následující tvrzení jsou ekvivalentní.

   (a) T je sporná,

   (b) pro nějakou formuli A, $T \vdash A$ a $T \vdash \neg A$,

   (c) pro nějakou formuli A, $T \vdash (A \,\&\, \neg A)$.

Kapitola 3

Predikátová logika

V této kapitole se budeme zabývat predikátovou logikou prvního řádu. Budeme definovat jazyk prvního řádu a jeho sémantiku, zavedeme formální systém predikátové logiky bez rovnosti, dokážeme základní věty predikátové logiky, Větu o dedukci a Větu o uzávěru. Ukážeme, že každou formuli predikátové logiky lze převést do ekvivalentního standardního tvaru – prenexního normálního tvaru formule. Nakonec zavedeme axiomy rovnosti a dokážeme základní věty predikátové logiky s rovností.

3.1 Jazyk a jeho sémantika

Ve výrokové logice jsme detailně zkoumali vlastnosti logických spojek, nyní budeme pracovat s jazykem logiky 1. řádu, který kromě spojek obsahuje ještě proměnné, funkční symboly a predikátové symboly.

3.1 Jazyk prvního řádu obsahuje

(i) neomezeně mnoho symbolů pro *proměnné* $x,\ y,\ z,\ x_1,\ x_2, \ldots$

(ii) *symboly pro logické spojky* $\neg,\ \&,\ \vee,\ \rightarrow,\ \leftrightarrow$

(iii) *symboly pro kvantifikátory* $\forall$ (obecný), $\exists$ (existenční)

(iv) *symboly pro predikáty* $p,\ g,\ p_1, \ldots$
S každým symbolem je dáno přirozené číslo $n \geq 1$, které udává počet argumentů (četnost) predikátu. Pokud je dán i binární predikátový symbol $=$, mluvíme o jazyku s rovností.

(v) *symboly pro funkce* $f,\ g, \ldots$
U každého symbolu je dáno přirozené číslo $n \geq 0$, které udává četnost funkčního symbolu. Funkční symboly četnosti nula chápeme jako konstanty.

Má-li funkční nebo predikátový symbol četnost n, říkáme, že je to symbol n-ární. Pro četnost jedna, dvě, tři jsou vžitá označení unární, binární a ternární.

(vi) *pomocné symboly* (závorky) $(,\ ),\ [,\ ], \ldots$

Symboly pro proměnné, spojky a kvantifikátory nazýváme logické, pokud jde o jazyk s rovností, symbol predikátu rovnosti rovněž počítáme k logickým symbolům. Symboly pro ostatní predikáty a symboly pro funkce určují specifiku jazyka (a odrážejí oblast, kterou jazyk může popisovat). Proto je nazýváme speciální. Jazyk 1. řádu je dán výčtem speciálních symbolů.

3.2 Příklad a) *Jazyk teorie uspořádání* je jazyk s rovností a obsahuje jediný speciální symbol $<$, je to binární predikátový symbol.

b) *Jazyk teorie grup* je jazyk 1. řádu s rovností, který obsahuje dva speciální symboly e, konstantu pro jednotkový prvek, a binární funkční symbol '$\cdot$' pro grupovou operaci.

c) *Jazyk teorie okruhů* je jazyk s rovností, který obsahuje dva binární funkční symboly $+$ (pro sčítání) a $\cdot$ (pro násobení) a dvě konstanty $0,\ 1$ pro nulu a jednotkový prvek.

d) *Jazyk teorie množin* je jazyk s rovností a má jediný speciální symbol $\in$, binární predikátový symbol pro náležení.

e) *Jazyk elementární aritmetiky* (s rovností) obsahuje funkční symboly 0 (konstantu pro nulu), S (unární symbol pro následující přirozené číslo), $+$ a $\cdot$ (binární symboly pro sčítání a násobení.

Výrazy jazyka 1. řádu, které mají matematický význam, lze rozdělit do dvou hlavních skupin: termy a formule. Termy popisují individua (objekty), které lze sestrojit pomocí operací. Formule jsou tvrzení.

3.3 Termy Induktivně popíšeme konstrukci termů.

(i) Každá proměnná je term.

(ii) Jsou-li výrazy $t_1, \ldots, t_n$ termy a je-li f n-ární funkční symbol, potom výraz $f(t_1, \ldots, t_n)$ je term.

(iii) Každý term vznikne konečným použitím pravidel (i) a (ii).

3.4 Příklad V jazyce elementární aritmetiky jsou následující výrazy termy: $0,\ S(x),\ S(S(0)), \ldots$. U vžitých binárních symbolů $+$ a $\cdot$, případně jiných, píšeme $(x+y),\ (t_1+t_2)$ namísto $+(x,\ y),\ +(t_1,\ t_2)$ a $(x\cdot y)$ namísto $\cdot(x,\ y)$.

Proto také $((x+y)\cdot 0,\ ((S(0)+(x\cdot y))\cdot S(0))$ jsou termy. Je-li f n-ární funkční symbol, také $f((x\cdot y),\ y_1,\ y_2, \ldots,\ y_{n-1})$ je term.

3.5 Formule Konstrukci formule popíšeme induktivně.

(i) Je-li p n-ární predikátový symbol a jsou-li výrazy $t_1, \ldots, t_n$ termy, potom výraz $p(t_1, \ldots, t_n)$ je *atomická formule*.

(ii) Jsou-li výrazy $A,\ B$ formule, potom $\neg A,\ (A\,\&\,B),\ (A \vee B)$, $(A \to B)$ a $(A \leftrightarrow B)$ jsou formule.

(iii) Je-li x proměnná, A formule, potom $(\forall x)\,A$, $(\exists x)\,A$ jsou formule.

(iv) Každá formule vznikne konečným použitím pravidel (i) – (iii).

Podobně jako v případě binárních funkčních symbolů $+$, $\cdot$ atd. budeme psát $(x = y)$, $(x < y)$ namísto $=(x,\ y)$, $<(x,\ y)$ atd. V tomto případě píšeme $(x \neq y)$ namísto $\neg(x = y)$.

3.6 Příklad a) $S(0) = (0 \cdot x) + S(0)$

b) $(\exists x)\,(y = x \cdot z)$

c) $(\forall x)\,(x \neq 0 \to (\exists y)\,(x = S(y)))$

jsou formule jazyka aritmetiky. Formule a) je atomická, formule b), c) nejsou atomické.

Formule c) vznikla z atomických formulí $(x = 0)$, $(x = S(y))$ užitím pravidel

(ii) $\neg(x = 0)$

(iii) $(\exists y)\,(x = S(y))$

(ii) $\neg(x = 0) \to (\exists y)\,(x = S(y))$

(iii) $(\forall x)\,(\neg(x = 0) \to (\exists y)\,(x = S(y)))$

Právě jsme se přesvědčili, že formule c) vznikla předepsaným způsobem. Formule, které jsme během konstrukce sestrojili, se nazývají *podformule* formule c).

3.7 Symboly, slova, zřetězení Z předchozích definic je zřejmé, že termy i formule jsou jisté konečné posloupnosti symbolů daného jazyka sestavené podle pevných pravidel. Libovolnou konečnou posloupnost symbolů budeme nazývat krátce *slovo* nebo *výraz*. Je-li nějaký symbol s napsán na i-tém místě ve slově S, říkáme, že *s se vyskytuje ve slově S na i-tém místě*. V takovém případě i-tý symbol ve slově S nazýváme *výskyt symbolu s v S*. Například '(' se vyskytuje ve formuli a) z příkladu 3.6 na druhém, šestém a třináctém místě, symbol x se vyskytuje v téže formuli na devátém místě.

Spojování slov, kterému se také říká *zřetězení (konkatenace)*, je nejjednodušší operace, kterou lze se slovy provádět. Poslouží nám k přesnějšímu popisu dalších syntaktických pojmů, které budeme zavádět.

3.8 Slova a podslova Jsou-li A, B slova, potom výrazem AB označíme slovo, které vznikne ze slov A, B tak, že nejprve napíšeme slovo A a za poslední symbol slova A (bez mezery) připojíme slovo B. Říkáme, že slovo AB je *zřetězením slov A a B*.

Například slovo 112 vznikne zřetězení slov 1 12, slov 11 2 nebo také prázdného slova a slova 112. Slovo, které vznikne spojením slov $A_1, A_2, \ldots, A_n$ v uvedeném pořadí, budeme označovat $A_1 A_2 \ldots A_n$.

Říkáme, že slovo C je *podslovem* slova A, jestliže slovo A má tvar BCD pro nějaká slova B, D, z nichž jedno nebo obě mohou být prázdná.

3.9 Příklad Nechť t je term $f(x,\ g(x,\ y))$. Potom slova $g(x,\ y)$ a $g(x,\ y))$ jsou podslova t. První z nich ja samo také termem, druhé ne.

Podobně slovo $(\forall x)$ je podslovem formule c) z příkladu 3.6, ale samo není formulí.

3.10 Podtermy, podformule, volné a vázané proměnné Nechť t je term a A je formule.

(ia) Říkáme, že *term s je podtermem termu t*, je-li podslovem slova t.

(ib) Říkáme, že *formule B je podformulí formule A*, je-li B podslovem slova A.

(ii) Říkáme, že *daný výskyt proměnné x ve formuli A je vázaný*, je-li součástí nějaké podformule tvaru $(\exists x)\,B$ nebo $(\forall x)\,B$ formule A. Není-li daný výskyt proměnné x vázaný, říkáme, že je *volný*.

(iii) Říkáme, že *proměnná x je volná ve formuli A*, má-li tam volný výskyt. Říkáme, že *proměnná x je vázaná ve formuli A*, má-li tam vázaný výskyt.

(iv) Říkáme, že *formule A je otevřená*, pokud A neobsahuje žádnou vázanou proměnnou. Říkáme, že A *je uzavřená*, pokud A neobsahuje žádnou volnou proměnnou.

Je zřejmé, že otevřená formule vznikne ze svých atomárních podformulí jen pomocí logických spojek, neobsahuje tedy žádné kvantifikátory. Uzavřená formule naopak váže každou proměnnou některým kvantifikátorem.

Uvědomme si, že táž proměnná může být v dané formuli současně volná i vázaná, například ve formuli $(x = z) \to (\exists x)\,(x = z)$ má proměnná x volný i vázaný výskyt. Tato situace je umožněna volností v definici formule, v matematické praxi se většinou takové formule nezavádějí. Jak uvidíme později, vázané proměnné lze zaměnit a tak se podobné situaci můžeme vždy vyhnout. Formule, ve kterých každá proměnná je buď volná (a není vázaná) nebo jenom vázaná (a ne volná), se někdy nazývají *formule s čistými proměnnými*.

3.2 Sémantika predikátové logiky

Nyní již máme k dispozici základní fakta a pojmy o syntaxi predikátové logiky, zavedli jsme pojem termu, formule a vazby, které mohou mít proměnné ve formuli. Můžeme zkoumat otázku struktur $\mathfrak{M}$, které realizují symboly jazyka L predikátové logiky a zejména to, které formule jsou pravdivé v dané realizaci. Chceme-li dát symbolům jazyka L nějakou matematickou interpretaci, je třeba nejprve začít od proměnných. Oborem hodnot proměnných bude neprázdná množina $M \neq \emptyset$,

kterou nazveme *univerzum* $\mathfrak{M}$ a její prvky budeme nazývat *individua*. Je-li vymezeno univerzum, potom je přirozené se ptát, jak jsou realizovány operace, které jsou naznačeny v jazyce L funkčními symboly. Například se můžeme ptát, které individuum bude odpovídat součtu nebo jiné operaci z daných individuí univerza. Funkční n-ární symbol f z jazyka L bude realizován zobrazením $f_{\mathfrak{M}} : M^n \to M$ tak, že rovnost $f_{\mathfrak{M}}(i_1, \ldots, i_n) = j$ pro $i_1, \ldots, i_n \in M$ znamená, že individuum j bude výsledkem operace f provedené na individua $i_1, \ldots, i_n$. Nakonec zbývají predikátové symboly. Máme-li realizovat binární predikátový symbol $<$, který "porovnává" individua, použijeme binární relaci $<_{\mathfrak{M}} \subseteq M^2$. Podobně realizace n-árních predikátových symbolů p budou n-ární relace $p_{\mathfrak{M}} \subseteq M^n$. Zvláštní postavení zde má symbol $=$, který počítáme k symbolům logickým a který by měl být realizován tak, aby odpovídal našim představám o rovnosti. Proto jej nerealizujeme jinak než jako identitu individuí. V definici pravdivosti se to odráží zvláštní klauzulí, která definuje splňování atomických formulí s rovností. Ostatní logické symboly, jako spojky a kvantifikátory nemá smysl realizovat. Popsaná struktura $\mathfrak{M}$, která obsahuje univerzum M a realizace funkcí a relací na tomto univerzu, se nazývá *relační struktura pro jazyk* L nebo *realizace jazyka* L.

3.11 Realizace jazyka Nechť L je jazyk 1. řádu. Relační struktura $\mathfrak{M}$, která obsahuje

- neprázdnou množinu M,
- zobrazení $f_{\mathfrak{M}} : M^n \to M$ pro libovolný n-ární funkční symbol f z jazyka L,
- n-ární relaci $p_{\mathfrak{M}} \subseteq M^n$ pro každý n-ární predikátový symbol p, kromě symbolu pro rovnost,

se nazývá realizace jazyka L. Prvky *univerza* M nazýváme *individua*, zobrazení $f_{\mathfrak{M}}$ příslušné k symbolu f a relaci $p_{\mathfrak{M}}$ příslušnou k predikátovému symbolu p nazýváme *realizace funkčního symbolu* f a *realizace predikátového symbolu* p.

3.12 Příklad

a) Struktura $\langle \omega, \omega \times \omega \rangle$, kde ω je množina přirozených čísel, je realizací jazyka z příkladu 3.2 a. Není to ovšem uspořádání.

b) Struktura $\langle \{e\}, e, \cdot_e \rangle$, kde $\cdot_e$ je binární zobrazení $\{e\}^2 \to \{e\}$ definované jediným možným způsobem, je realizací jazyka teorie grup z příkladu 3.2 b. Výsledkem je jednoprvková grupa.

c) $\mathfrak{N} = \langle \omega, \emptyset, \sigma, \oplus, \odot \rangle$, kde ω je množina přirozených čísel, $\emptyset$ realizuje nulu, σ je funkce, která číslu n přiřazuje následující přirozené číslo a $\oplus$, $\odot$ jsou obvyklé operace součtu a součinu, je realizací jazyka elementární aritmetiky z příkladu 3.2 e. Pokud σ nahradíme nějakým číslem, například jednotkou, vznikne

struktura, která je realizací jazyka teorie okruhů 3.2 c (to ovšem neznamená, že je okruhem).

3.13 Realizace termů Chceme-li zkoumat pravdivost formulí v nějaké realizaci jazyka, musíme se nejprve vyrovnat s volnými proměnnými. Těm je třeba vždy přiřadit nějaké individuum jako hodnotu. Tuto úlohu budou plnit zobrazení, které každé proměnné přiřadí nějaké individuum. Zobrazení e množiny všech proměnných do univerza M struktury $\mathfrak{M}$ budeme nazývat *ohodnocení proměnných.* Je-li e ohodnocení proměnných, x proměnná a $m \in M$, potom ohodnocení proměnných, které proměnné x přiřazuje individuum m a na všech ostatních proměnných splývá s ohodnocením e budeme označovat $e(x/m)$. Zobrazení e tedy přiřazuje hodnotu všem proměnným, které jsou nejjednoduššími případy termů. Indukcí podle složitosti termu t lze ukázat, že ohodnocení e přiřazuje termu t jednoznačně hodnotu $t[e]$, kterou budeme nazývat *realizací termu t při ohodnocení e*. Definujeme $t[e]$ následujícím způsobem:

- Je-li t proměnná x, potom $t[e]$ je $e(x)$.
- Je-li t tvaru $f(t_1, \ldots, t_n)$ a hodnoty $t_1[e], \ldots, t_n[e]$ jsou již sestrojeny, potom $t[e]$ je individuum $f_{\mathfrak{M}}(t_1[e], \ldots, t_n[e])$.

Z této definice je zřejmé, že $t[e]$ závisí na realizaci $\mathfrak{M}$; měli bychom raději psát $t[e, \mathfrak{M}]$. Symbol $\mathfrak{M}$ budeme vynechávat, pokud bude zřejmé, ve které realizaci jazyka pracujeme.

3.14 Lemma Jsou-li všechny proměnné vyskytující se v termu t mezi proměnnými $x_1, \ldots, x_n$ a jsou-li e, e' dvě ohodnocení taková, že $e(x_i) = e'(x_i)$ pro $i = 1, \ldots, n$, potom $t[e] = t[e']$.

Realizace $t[e]$ tedy závisí jen na konečně mnoha hodnotách ohodnocení e.

Důkaz. Indukcí dle složitosti termu t.

3.15 Pravdivost a splňování formulí Nyní můžeme definovat, kdy je nějaká formule pravdivá v nějaké realizaci jazyka při daném ohodnocení, to znamená při pevně daném významu volných proměnných. Je-li tento pojem zaveden, můžeme již přirozeným postupem definovat splňování dané formule v relační struktuře.

Definice (Tarski) Nechť $\mathfrak{M}$ je realizace jazyka L, e ohodnocení proměnných, A formule.

(i) Indukcí podle složitosti formule A budeme definovat *pravdivost formule A v $\mathfrak{M}$ při ohodnocení e*. Označujeme $\mathfrak{M} \models A[e]$.

a1) Je-li A atomická formule tvaru $p(t_1, \ldots, t_n)$, kde p je n-ární predikátový symbol různý od $=$ a $t_1, \ldots, t_n$ jsou termy, potom $\mathfrak{M} \models A[e]$, jestliže $(t_1[e], \ldots, t_n[e]) \in p_{\mathfrak{M}}$.

a2) Je-li A atomická formule tvaru $t_1 = t_2$, potom $\mathfrak{M} \models A[e]$, jestliže $t_1[e] = t_2[e]$, to jest, když oba termy jsou realizovány týmž individuem.

b) Je-li A tvaru $\neg B$, potom $\mathfrak{M} \models A[e]$, když $\mathfrak{M} \not\models B[e]$.

c) Je-li A tvaru $(B \to C)$, potom $\mathfrak{M} \models A[e]$, jestliže $\mathfrak{M} \not\models B[e]$ nebo $\mathfrak{M} \models C[e]$.

d) Je-li A tvaru $(\forall x)\, B$, potom $\mathfrak{M} \models A[e]$, jestliže pro libovolné individuum $m \in M$, $\mathfrak{M} \models B[e(x/m)]$.

d') Je-li A tvaru $(\exists x)\, B$, potom $\mathfrak{M} \models A[e]$, jestliže pro jisté individuum $m \in M$, $\mathfrak{M} \models B[e(x/m)]$.

(ii) Říkáme, že A *je splněna v* $\mathfrak{M}$, píšeme $\mathfrak{M} \models A$, je-li A pravdivá v $\mathfrak{M}$ při libovolném ohodnocení e.

Z definice pravdivosti a definice $(\exists x)\, B$ pomocí $\neg$, $\forall$ je zřejmé, že d') lze odvodit z b) a d).

3.16 Podobně jako v případě termů lze ukázat nasledující tvrzení: Jsou-li všechny volné proměnné formule A mezi proměnnými $x_1, \ldots, x_n$ a jsou-li ohodnocení e, e' shodná na těchto proměnných, potom

$$\mathfrak{M} \models A[e] \quad \text{právě když} \quad \mathfrak{M} \models A[e'].$$

To lze snadno ověřit indukcí dle složitosti formule A. Z uvedeného faktu vyplývá, že při zkoumání pravdivosti formule (a realizace termu) vystačíme jen s ohodnocením konečného počtu proměnných, totiž těch, které jsou ve formuli (termu) volné.

Z definice pravdivosti d), d') vyplývá, že pokud proměnná x má v A jen vázané výskyty, potom pravdivost A v $\mathfrak{M}$ nezáleží na ohodnocení této proměnné. Speciálně, je-li A uzavřená formule, potom pravdivost formule A nezávisí na ohodnocení, to znamená, že $\mathfrak{M} \models A$ právě když $\mathfrak{M} \models A[e]$ při alespoň jednom ohodnocení. Je-li uzavřená formule A splněna v $\mathfrak{M}$, říkáme, že A *je pravdivá v* $\mathfrak{M}$. Z definice d) je zřejmé, že formule A je splněna v $\mathfrak{M}$, právě když je pravdivá formule $(\forall x_1) \ldots (\forall x_n)\, A$, kde $x_1, \ldots, x_n$ jsou všechny volné proměnné formule A v nějakém pořadí. Takové formuli říkáme *uzávěr formule* A.

3.17 Substituce termů za proměnné V matematické praxi je běžné dosazovat za proměnné termy, a tím získávat speciální případy (termů nebo) formulí. Z praktických důvodů musíme nejprve definovat substituci do termů.

Jsou-li $x_1, \ldots, x_n$ různé proměnné, t, $t_1, \ldots, t_n$ termy, potom symbolem $t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ označme výraz, který vznikne z termu t nahrazením každého výskytu proměnné x_i termem t_i pro $i \leq n$.

3.18 Příklad Je-li t tvaru $(x + y)$, t_1, t_2 a t_3 jsou po řadě $x + x$, $z \cdot y$, w, potom $t_{x,y}[t_1, t_2]$ je term $((x+x)+(z\cdot y))$, $t_{x,w}[t_1, t_3]$ je $((x+x)+y)$, $t_{x,y,z}[t_1, t_2, t_3]$

je $t_{x,y}[t_1,\ t_2]$. Indukcí dle složitosti termu t se můžeme přesvědčit, že $t[t_1, \ldots, t_n]$ je opět term.

3.19 Nyní můžeme přejít k formulím. Je-li A formule, t term, potom výraz, který vznikne z formule A nahrazením každého volného výskytu proměnné x termem t označme $A_x[t]$. Indukcí podle složitosti se snadno přesvědčíme, že $A_x[t]$ je opět formule. Je-li A atomická formule tvaru $p(t_1, \ldots, t_n)$ nebo $t_1 = t_2$, potom $t_1[t], \ldots, t_n[t]$ jsou opět termy a $A_x[t]$ je opět atomická formule. Je-li A tvaru $\neg B$, $(B \to C)$ nebo $(\forall z)\, B$, potom z indukčního předpokladu $B_x[t]$ a $C_x[t]$ jsou opět formule, proto $\neg B_x[t]$, $(B_x[t] \to C_x[t])$ jsou formule. Pokud z je proměnná x, pak $(\forall z) B$ neobsahuje x volně a substitucí se nemění, tedy zůstává formulí. Pokud z je proměnná různá od x, potom $(\forall z)\, B_x[t]$ je formule.

Zamysleme se nad smyslem substituce. Je-li A formule například tvaru $x + x = z \cdot x$, potom pro $t = \sin z$ je $A_x[t]$ formule $\sin z + \sin z = z \cdot \sin z$, která je speciálním případem – instancí formule A. Naším úmyslem je vždy, aby instance $A_x[t]$ "říkala" o t "totéž" co formule A "říká" o x, za které bylo substituováno. Budeme-li postupovat při substituování bez jakýchkoli omezení, náš záměr přitom může přijít zkrátka.

3.20 Příklad Uvažujme formuli A v jazyku elementární aritmetiky tvaru $(\exists y)\,(x = y + y)$ a term t tvaru $y + 1$, po substituci termu t za x do A dostáváme formuli A' tvaru $(\exists y)\,(y + 1 = y + y)$.

Jestliže formuli A jsme snadno interpretovali jako tvrzení "x je sudé", jsme na rozpacích, jak interpretovat A'. Jen jedno je zřejmé, že A' nelze chápat jako "$y + 1$ je sudé", protože proměnná y je ve formuli A vázaná. V tom je také hlavní závada uvedené substituce. Term, který byl substituován za *volný* výskyt proměnné x ve formuli A obsahuje proměnnou, která se po substituci termu do A stala vázanou. Proto při substituci termů do formulí se této situaci vždy vyhneme; výsledek naší úvahy shrnuje následující definice.

3.21 Substituovatelnost termu do formule Říkáme, že *term t je substituovatelný za proměnnou x do formule A*, jestliže pro každou proměnnou y obsaženou v t, žádná podformule tvaru $(\forall y)\, B$, $(\exists y)\, B$ formule A neobsahuje (z hlediska formule A) volný výskyt proměnné x. V dalším budeme označení $A_x[t]$ používat jen tehdy, je-li term t substituovatelný za x do formule A.

Substituci termů za proměnné budeme užívat i pro více proměnných současně; je-li term t_i substituovatelný za proměnnou x_i do formule A pro $i = 1,\ 2, \ldots, n$, výrazem $A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ budeme označovat formuli, která vznikne z formule A nahrazením každého volného výskytu proměnné x_i po řadě termem t_i pro $i = 1,\ 2, \ldots, n$. Výslednou formuli nazýváme *instance formule A*.

Snadno rozpoznáme dva případy, kdy je substituovatelnost termu t do formule A za proměnnou x bez jakýchkoli problémů.

V případě, že formule A je otevřená, potom každý term je substituovatelný za každou proměnnou vyskytující se v A. Podobně je tomu v obecnějším případě, kdy žádná proměnná obsažená v termu t není vázaná v A. Oba jednoduché případy substituovatelnosti nevyčerpávají celou škálu možností.

3.22 Příklad Je-li z proměnná, potom term t tvaru z je substituovatelný za x do formule $x = 0 \to \neg(\exists z)\,(z \neq 0)$.

Následující jednoduchý fakt je užitečný při zkoumání pravdivosti instancí formulí.

3.23 Lemma Je-li $\mathfrak{M}$ realizace jazyka L, A je formule, t, $t_1, \ldots, t_n$ jsou termy jazyka L a e je ohodnocení proměnných takové, že $t_i[e]$ je individuum m_i pro $i = 1, 2, \ldots, n$, potom

(i) $t_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e]$ je individuum $t[e(x_1/m_1, \ldots, x_n/m_n)]$.

(ii) $\mathfrak{M} \models A_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e]$, právě když $\mathfrak{M} \models A[e(x_1/m_1, \ldots, x_n/m_n)]$.

Důkaz. (i) Indukcí podle složitosti termu t. Označ t' term $t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$. Je-li t tvaru x, potom t' je t v případě, že x není v seznamu proměnných $x_1, \ldots, x_n$ a tvrzení platí, nebo t' je tvaru t_i, pokud x je proměnná x_i. V tomto případě je $t'[e]$ individuum m_i, tedy $t[e(x_1/m_1, \ldots, x_n/m_n)]$.

Je-li t tvaru $f(s_1, \ldots, s_r)$, potom z indukčního předpokladu

$$s_i[t_1, \ldots, t_n][e] = s_i[e(x_1/m_1, \ldots, x_n/m_n)]$$

platí pro $i = 1, 2, \ldots, r$ a $t'[e]$ je individuum

$$f_{\mathfrak{M}}(s_1[e(x_1/m_1, \ldots, x_n/m_n)], \ldots, s_r[e(x_1/m_1, \ldots, x_n/m_n)]),$$

tedy individuum $t[e(x_1/m_1, \ldots, x_n/m_n)]$.

(ii) Indukcí dle složitosti formule A. Označme A' instanci $A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$. Je-li A atomická formule tvaru $p(s_1, \ldots, s_r)$, kde p není $=$, potom

$$\begin{aligned}\mathfrak{M} \models A'[e], \text{ právě když } & (s_1[t_1, \ldots, t_n][e], \ldots, s_r[t_1, \ldots, t_n][e]) \in p_{\mathfrak{M}},\\ \text{právě když } & (s_1[e(x_1/m_1, \ldots)], \ldots, s_r[e(x_1/m_1, \ldots)]) \in p_{\mathfrak{M}},\\ \text{právě když } & \mathfrak{M} \models A[e(x_1/m_1, \ldots, x_n/m_n)].\end{aligned}$$

Je-li A tvaru $t_1 = t_2$, postupujeme stejně.

Je-li A tvaru $\neg B$ nebo $(B \to C)$, postupujeme podobně.

Je-li A tvaru $(\forall z)\,B$, z je některá z proměnných $x_1, \ldots, x_n$, například x_1, potom A' tvaru $A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ je formule $(\forall x_1)\,B_{x_2,\ldots,x_n}[t_2, \ldots, t_n]$.

$$\begin{aligned}\mathfrak{M} \models A'[e], \text{ právě když } & \mathfrak{M} \models B_{x_2,\ldots,x_n}[t_2, \ldots, t_n][e(x_1/m)] \text{ pro libovolné } m \in M,\\ \text{právě když } & \mathfrak{M} \models B[e(x_1/m, \ldots, x_n/m_n)] \text{ pro libovolné } m \in M,\\ \text{právě když } & \mathfrak{M} \models A[e(x_2/m_2, \ldots, x_n/m_n)].\end{aligned}$$

Poslední ekvivalence plyne z toho, že pravdivost formule A na ohodnocení proměnné x_1 vůbec nezávisí.

V případě, že z není v seznamu $x_1, \ldots, x_n$, jest A' tvaru $A[t_1, \ldots, t_n]$ a postup důkazu je zjednodušením předcházejícího případu.

3.3 Formální systém predikátové logiky 1. řádu

Vyslovíme nyní axiomy a odvozovací pravidla predikátové logiky. Část z nich již známe, jsou to axiomy, které určují vlastnosti logických spojek. Ukážeme, že při vhodné volbě množiny prvotních formulí spolu s nimi přechází do predikátové logiky celá výroková logika. Podobně jako ve výrokové logice budeme některé symboly chápat jako základní a jiné jako odvozené.

3.24 Redukce jazyka Z logických spojek budou základní symboly pro negaci $\neg$ a pro implikaci $\to$, ostatní spojky budou definovány ze základních pomocí zkratek stejným způsobem jako ve výrokové logice. Z obou kvantifikátorů chápeme symbol pro obecný (velký) kvantifikátor $\forall$ jako základní a symbol $\exists$ pro existenční (malý) kvantifikátor jako odvozený. Zavedeme jej následujícím způsobem.

3.25 Úmluva Je-li A formule, x proměnná, potom výraz $(\exists x)\, A$ je zkratka za formuli $\neg(\forall x)\, \neg A$.

Je zřejmé, že tímto způsobem lze každou formuli jazyka L vyjádřit jen pomocí obecného kvantifikátoru. Hlavním smyslem naší úmluvy je redukovat počet axiomů tím, že vlastnosti existenčního kvantifikátoru budou odvozeny z axiomů pro obecný kvantifikátor. Axiomy, které určují vlastnosti logického symbolu pro rovnost zavedeme později.

3.26 Axiomy pro logické spojky Je-li L jazyk 1. řádu a jsou-li A, B, C formule jazyka L, potom každá formule tvaru

$$A \to (B \to A) \tag{A1}$$

$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \tag{A2}$$

$$(\neg B \to \neg A) \to (A \to B) \tag{A3}$$

je axiom predikátové logiky.

Uvedené axiomy odpovídají schematům axiomů výrokové logiky. Vezmeme-li za množinu P prvotních formulí všechny formule jazyka L, které nelze ve výrokové logice dále rozkládat, to znamená, že P bude tvořena všemi atomickými formulemi a všemi formulemi tvaru $(\forall x)\, B$ a $(\exists x)\, B$ pro nějakou proměnnou x a libovolnou formuli B, potom každá formule jazyka L vznikne z prvotních formulí pomocí logických spojek. Všechny uvedené axiomy proto souhlasí s axiomy

výrokové logiky nad P. K axiomům výrokové logiky patří odvozovací pravidlo modus ponens, které je také odvozovacím pravidlem predikátové logiky.

Vztah mezi výrokovou a predikátovou logikou shrnuje následující věta.

3.27 Věta Nechť A je formule jazyka L, nechť P je množina všech atomických formulí jazyka L a všech formulí tvaru $(\forall x)\,B$ a $(\exists x)\,B$, kde x je nějaká proměnná a B formule jazyka L. Je-li A tautologie výrokové logiky nad P, potom A je větou predikátové logiky.

Důkaz. Podle definice množiny P každá formule jazyka L vznikne z formulí množiny P jen použitím výrokových spojek. Axiomy výrokové logiky nad P proto souhlasí s odpovídajícími axiomy predikátové logiky a pravidlo modus ponens náleží k oběma formálním systémům. Je-li A tautologie, podle Postovy věty je dokazatelná ve výrokové logice nad P a její důkaz je také důkazem v predikátové logice.

3.28 V dalším budeme běžně používat známých důkazových postupů výrokové logiky. Abychom zdůraznili výrokový charakter některého důkazu, například formule B z předpokladů $A_1, \ldots, A_n$, budeme říkat, že B je tautologickým důsledkem formulí $A_1, \ldots, A_n$. Při přenášení výrokových důkazů si povšimneme ještě jedné věci. Výrokové důkazy častokrát používají větu o dedukci výrokové logiky. Tento obrat se přenáší jen potud, pokud znak dokazatelnosti má stejný význam jako ve výrokové logice, tedy dokazatelnost z "výrokových axiomů" pomocí jediného pravidla modus ponens. Predikátová logika má také svou větu o dedukci, ale se silnějšími předpoklady o premisách. K tomu se vrátíme později.

3.29 Axiomy pro kvantifikátory Další axiomy určují vlastnosti obecného kvantifikátoru. Vyjádříme je ve dvou schematech:

Schema specifikace Je-li A formule, x proměnná a t term (substituovatelný za proměnnou x do formule A), potom formule

$$(\forall x)\,A \to A_x[t]$$

je axiom predikátové logiky.

Tento axiom má názorný smysl: pokud A platí pro "libovolné" x, pak platí i pro každý speciální případ $A_x[t]$.

Druhé schema, které vyslovíme, má spíše technický ráz a jeho smysl vynikne při studiu takzvaných prenexních operací:

Schema přeskoku Jsou-li A, B formule a je-li x proměnná, která nemá volný výskyt ve formuli A, potom formule

$$(\forall x)\,(A \to B) \to (A \to (\forall x)\,B)$$

je axiom predikátové logiky.

Predikátová logika má dvě odvozovací pravidla, *modus ponens* a *pravidlo generalizace*, které zní:

Pro libovolnou proměnnou x z formule A odvoď formuli $(\forall x)\, A$.

Jeho smysl je víceméně názorný a určuje úlohu volných proměnných ve větách: je-li dokazatelná formule A, která má (případně) volnou proměnnou x, potom je dokazatelná i formule "pro každé x platí A".

Uvedené axiomy a odvozovací pravidla tvoří formální systém predikátové logiky bez rovnosti. Predikátová logika s rovností vznikne z popsaného formálního systému již jen rozšířením jazyka o predikátový symbol rovnosti a přidáním axiomů pro tento predikát. Žádné další odvozovací pravidla se nepřidávají. V dalším textu bude $\vdash$ označovat *dokazatelnost* z axiomů predikátové logiky a případně z množiny předpokladů *pomocí obou odvozovacích pravidel.*

3.30 Základní věty o kvantifikátorech

Nyní odvodíme základní věty o vlastnostech kvantifikátorů. Postup, kterým to provádíme, je typický pro podobná odvození i v jiných formálních systémech: nejprve se odvozují další "pomocná" odvozovací pravidla, která rozšiřují paletu důkazových obratů a souběžně s tím se odvozují různé analogie určitých axiomů motivované buďto "symetrií" nebo jistou "dualitou" (například mezi obecným a existenčním kvantifikátorem). Při formulaci některých vět je patrná inspirace Gentzenovým kalkulem přirozené dedukce.

3.31 Lemma (pravidlo zavedení $\forall$)

Je-li $\vdash\ A \to B$ a proměnná x nemá volný výskyt ve formuli A, potom $\vdash\ A \to (\forall x)\, B$.

Důkaz. Je-li $\vdash\ A \to B$, potom užitím pravidla generalizace také

$$\vdash\ (\forall x)\,(A \to B) \tag{1}$$

Přitom

$$\vdash\ (\forall x)\,(A \to B) \to (A \to (\forall x)\, B) \tag{2}$$

je axiom predikátové logiky. Formule

$$A \to (\forall x)\, B$$

se odvodí z (1) a (2) pravidlem modus ponens.

3.32 Lemma Pro libovolné formule A, B a term t platí

(i) $\vdash\ A_x[t] \to (\exists x)\, A$

(ii) Je-li $\vdash\ A \to B$ a proměnná x nemá volný výskyt ve formuli B, potom také $\vdash\ (\exists x)\, A \to B$.

Tvrzení (i) je duální formou axiomu specifikace a (ii) je duální formou pravidla zavedení $\forall$. Toto pomocné odvozovací pravidlo budeme nazývat pravidlem (zavedení) $\exists$.

Důkaz. (i)

$\vdash\ (\forall x)\,\neg A \to \neg A_x[t]$ (axiom specifikace)
$\vdash\ \neg\neg(\forall x)\,\neg A \to (\forall x)\,\neg A$ (v3)

Složením obou implikací a použitím zkratky $(\exists x)\,A$ dostáváme $\vdash\ \neg(\exists x)\,A \to \neg A_x[t]$ jako jejich tautologický důsledek.

Odtud plyne tvrzení (i) jako tautologický důsledek obrácením implikace.

(ii) Je-li $\vdash\ A \to B$, potom

$\vdash\ \neg B \to \neg A$ (tautologický důsledek)
$\vdash\ \neg B \to (\forall x)\,\neg A$ (pravidlo $\forall$)
$\vdash\ (\exists x)\,A \to B$ (tautologický důsledek a zkratka $(\exists x)\,A$)

3.33 Lemma Nechť A' je instancí formule A, to znamená nechť A' je tvaru $A_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$ pro nějaké termy $t_1,\ldots,t_n$ a nějaké proměnné $x_1,\ldots,x_n$. Potom je-li $\vdash\ A$, pak také $\vdash\ A'$.

Jinými slovy: je-li dokazatelná formule A, pak je dokazatelná i každá instance formule A.

Důkaz. Indukcí dle počtu substituovaných termů. Je-li $n = 1$ a A' je tvaru $A_x[t]$, potom z $\vdash A$ pravidlem generalizace odvodíme $\vdash\ (\forall x)\,A$.

Dále $\vdash\ (\forall x)\,A \to A_x[t]$ (axiom specifikace)

a formuli A' lze odvodit z posledních dvou pravidlem modus ponens.

Následující příklad ukazuje, že pro $n > 1$ nelze přímočaře použít dokázaného případu pro $n = 1$, protože sekvenční dosazování nemusí dávat stejný výsledek jako paralelní.

3.34 Příklad Nechť A je formule $x < y$, nechť t je proměnná y a s je proměnná x. Potom $A_{x,y}[t,\ s]$ je formule $y < x$, ale dosazováním po jedné proměnné obdržíme formuli $x < x$, dosadíme-li nejprve t za x a potom s za y. Zvolíme-li obrácené pořadí substitucí, dostaneme formuli $y < y$.

Proto k důkazu lemmatu zvolíme jiný postup. Nechť $z_1,\ldots,z_n$ jsou proměnné, které se nevyskytují v A ani v termech $t_1,\ldots,t_n$, potom z předpokladu $\vdash\ A$ dostáváme $\vdash\ A_{x_1}[z_1]$ a snadno se přesvědčíme, že další substitucí z_2 za x_2 obdržíme formuli $A_{x_1,x_2}[z_1,\ z_2]$. postupujeme-li stejným způsobem, dokážeme nakonec $A_{x_1,\ldots,x_n}[z_1,\ldots,z_n]$. Označíme poslední formuli jako B, v této formuli nemají $x_1,\ldots,x_n$ volný výskyt a proměnné $z_1,\ldots,z_n$ jsou právě na těch místech, kde ve formuli A byly volné výskyty $x_1,\ldots,x_n$. Pro každé $i = 1,2,\ldots,n$ je term t_i substituovatelný za z_i do B, protože t_i byl substituovatelný za x_i do B. Z $\vdash\ B$ odvodíme $\vdash\ B_{z_1}[t_1]$ a protože $z_1,\ldots,z_n$ se nevyskytují v t_1, je snadné přesvědčit se, že substitucí t_2 za z_2 do poslední formule vznikne formule $B_{z_1,z_2}[t_1,t_2]$. Postupujeme-li tímto způsobem, dokážeme nakonec formuli $B_{z_1,\ldots,z_n}[t_1,\ldots,t_n]$, která je shodná s formulí A'.

Předchozí lemma ukazuje, že volné proměnné mohou být zaměněny.

Následující lemma zobecňuje axiom specifikace pro případ substituce za více proměnných.

3.35 Lemma Pro libovolnou formuli A, proměnné $x_1, \ldots, x_n$ a termy $t_1, \ldots, t_n$ platí

(i) $\vdash (\forall x_1) \ldots (\forall x_n)\, A \to A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$

(ii) $\vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \to (\exists x_1) \ldots (\exists x_n)\, A$

Důkaz. (i) Z axiomu specifikace dostáváme pro libovolnou proměnnou x a formuli C (kde $C_x[x]$ je C)

$$\vdash (\forall x)\, C \to C\,. \tag{3}$$

Z (3) postupně dostaneme

$$\begin{aligned} &\vdash (\forall x_n)\, A \to A \\ &\vdash (\forall x_{n-1})(\forall x_n)\, A \to (\forall x_n)\, A \\ &\vdots \\ &\vdash (\forall x_1) \ldots (\forall x_n)\, A \to\ (\forall x_2) \ldots (\forall x_n)\, A \end{aligned} \tag{4}$$

Přitom

$$(\forall x_1) \ldots (\forall x_n)\, A \to A \tag{5}$$

je tautologickým důsledkem předchozích formulí, vznikne složením všech implikací (4), tedy je dokazatelná. Nakonec (i) je instancí (5).

(ii) Z lemmatu 3.32 (i) pro libovolnou formuli C a proměnnou x plyne

$$\vdash C \to (\exists x)\, C \tag{6}$$

Užijeme-li (6) obdobně jako při důkazu (i), dostaneme

$$\vdash A \to (\exists x_1) \ldots (\exists x_n)\, A \tag{7}$$

a (ii) je instancí formule (7).

3.36 Z formulí (5) a (7) užitím pravidla zavedení $\forall$ a pravidla $\exists$ lze dokázat

$$\begin{aligned} &\vdash (\forall x_1) \ldots (\forall x_n)\, A \leftrightarrow (\forall x_{\pi(1)}) \ldots (\forall x_{\pi(n)})\, A \\ &\vdash (\exists x_1) \ldots (\exists x_n)\, A \leftrightarrow (\exists x_{\pi(1)}) \ldots (\exists x_{\pi(n)})\, A \end{aligned}$$

pro libovolnou permutaci π na množině indexů $\{1,\ 2, \ldots, n\}$. Na pořadí proměnných v bloku stejných kvantifikátorů tedy nezáleží. Tím je ospravedlněna následující definice.

3.37 Uzávěr formule Jsou-li $x_1, \ldots, x_n$ všechny proměnné s volným výskytem ve formuli A v nějakém pořadí, potom formuli $(\forall x_1) \ldots (\forall x_n)\, A$ nazveme uzávěrem formule A.

3.38 Věta o uzávěru
Je-li A' uzávěr A, potom $\vdash A$ právě když $\vdash A'$.

Důkaz. a) Je-li $\vdash A$, potom pravidlem generalizace odvodíme $\vdash A'$.

b) Z lemmatu 3.35 (i) plyne $\vdash A' \to A$, je-li $\vdash A'$, pak $\vdash A$ odvodíme pravidlem modus ponens.

Věta o uzávěru charakterizuje volné proměnné v dokazatelných formulích, mají stejný význam, jako kdyby byly uzavřeny obecným kvantifikátorem. Dokážeme-li $\vdash x = 0$, je tím dokázáno $\vdash (\forall x)\,(x = 0)$.

3.39 Lemma (distribuce kvantifikátorů)
Je-li $\vdash A \to B$, potom

$$\vdash (\forall x)\,A \to (\forall x)\,B \text{ a } \vdash (\exists x)\,A \to (\exists x)\,B$$

Důkaz.

a)	$\vdash (\forall x)\,A \to A$	axiom specifikace
	$\vdash (\forall x)\,A \to B$	tautologický důsledek předpokladu a předchozí formule
	$\vdash (\forall x)\,A \to (\forall x)\,B$	pravidlo zavedení $\forall$.
b)	$\vdash B \to (\exists x)\,B$	lemma 3.32 (i)
	$\vdash A \to (\exists x)\,B$	tautologický důsledek předpokladu a předchozí formule
	$\vdash (\exists x)\,A \to (\exists x)\,B$	pravidlo $\exists$.

3.40 Věta o ekvivalenci Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $B_1, \ldots, B_n$ po řadě formulemi $B'_1, \ldots, B'_n$. Je-li $\vdash B_i \leftrightarrow B'_i$ pro $i = 1, 2, \ldots, n$, potom $\vdash A \leftrightarrow A'$.

Důkaz. Věta 3.40 je obdobou věty o ekvivalenci, kterou jsme dokázali pro výrokovou logiku. Dokazuje se indukcí dle složitosti formule A. Základní případy jsou stejné jako ve výrokové logice. Navíc je jen případ, kdy A je tvaru $(\forall x)\,B$ nebo tvaru $(\exists x)\,B$. Potom A' je tvaru $(\forall x)\,B'$ nebo tvaru $(\exists x)\,B'$ a z indukčního předpokladu pro formuli B dostáváme

$$\vdash B \leftrightarrow B'.$$

Odkud $\vdash B \to B'$ a $\vdash B' \to B$.

Podle lemmatu 3.39 pak dostáváme $\vdash A \to A'$ a $\vdash A' \to A$. Odtud tvrzení věty plyne jako tautologický důsledek.

3.41 Záměna vázaných proměnných Vázané proměnné ve formuli mohou být za jistých předpokladů zaměněny. Je to obdoba případů „vázaných“ proměnných známých z různých oborů matematiky: například $\int_0^\pi \sin x\,dx$ je stejné číslo jako $\int_0^\pi \sin z\,dz$. Nejprve zavedeme pojem varianty formule.

Říkáme, že *formule* A' *je variantou formule* A, jestliže A' vznikne z A postupným nahrazením podformulí tvaru

$$(Qx)\,B \tag{8}$$

formulemi

$$(Qy)\,B_x[y] \tag{9}$$

kde y není volná ve formuli B a Q je obecný nebo existenční kvantifikátor.

3.42 Příklad Formule $(\forall x)\,((\exists y)\,(x = y \cdot z) \to d(z,x))$ je variantou formule $(\forall v)\,((\exists w)\,(v = w \cdot z) \to d(z,v))$. Nejprve nahradíme podformuli $(\exists y)\,(x = y \cdot z)$ formulí $(\exists w)\,(x = w \cdot z)$ a formuli $(\forall x)\,((\exists w)\,(x = w \cdot z) \to d(z,x))$ nahradíme uvedenou variantou.

3.43 Věta o variantách Je-li A' varianta formule A, potom $\vdash A \leftrightarrow A'$.

Důkaz. Podle věty 3.40 stačí dokázat, že formule (8) a (9) jsou ekvivalentní. Provedeme důkaz pro případ, že Q je $\forall$. Případ, kdy Q je $\exists$ se dokáže obdobně. Předpokládáme, že ve formuli (9) jsou x, y různé proměnné, v opačném případě není co dokazovat. Potom

$\vdash (\forall x)\,B \to B_x[y]$	axiom specifikace
$\vdash (\forall x)\,B \to (\forall y)\,B_x[y]$	pravidlo $\forall$, y nemá volný výskyt v B.

Označíme-li B' formule $B_x[y]$, zjistíme snadno, že x nemá volný výskyt v B' a je substituovatelné za y i do B'. Stejně jako v první části důkazu dostaneme $\vdash (\forall y)\,B' \to (\forall x)\,B'_y[x]$. Ale $B'_y[x]$ je formule B. Tím je dokázána i opačná implikace.

3.44 Věta o dedukci Nechť T je množina formulí, A je uzavřená formule a B je libovolná formule. Potom $T \vdash A \to B$, právě když $T,\ A \vdash B$.

Důkaz. Důkaz implikace zleva doprava je stejný jako ve výrokové logice. Při důkazu implikace zprava doleva postupujeme indukcí podle důkazu $B_1, \ldots, B_n$ formule B z $T,\ A$. Navíc je třeba uvažovat jen případ, kdy B_i je odvozena z formule B_j, $j < i$, pravidlem generalizace. To znamená, že B_i je tvaru $(\forall x)\,B_j$ pro nějakou proměnnou x. Z indukčního předpokladu

$$T \vdash A \to B_j$$

a protože A je uzavřená formule a neobsahuje volný výskyt proměnné x, pravidlem $\forall$ odvodíme

$$T \vdash A \to B_i$$

Tím je věta dokázána.

Z důkazu věty o dedukci je zřejmé, že předpoklad uzavřenosti formule A je příliš omezující. Stačilo by vědět, že v důkazu formule B z $T,\ A$ nebylo použito

pravidlo generalizace na žádnou proměnnou, která je volná v A, jinými slovy, že žádná proměnná volně se vyskytující v A nebyla jako proměnná v důkazu využita. Tuto okolnost je možné pro jednotlivé důkazy ověřit, ale nelze dosti dobře formulovat jako předpoklad věty o dedukci. Dokážeme nyní větu, která dovolí podobné případy řešit a je sama zajímavá.

3.45 Věta o konstantách Nechť T je množina formulí jazyka L a nechť A je formule jazyka L. Nechť jazyk L' vznikne z L rozšířením o nové symboly pro konstanty. Jsou-li $c_1, \ldots, c_m$ nové konstanty a $x_1, \ldots, x_m$ jsou proměnné, potom

$$T \vdash A_{x_1,\ldots,x_m}[c_1, \ldots, c_m] \text{ právě když } T \vdash A$$

Důkaz. a) Je-li $T \vdash A$, potom $T \vdash A_{x_1,\ldots,x_m}[c_1, \ldots, c_m]$ podle lemmatu 3.33.

b) Je-li $T \vdash A_{x_1,\ldots,x_m}[c_1, \ldots, c_m]$, označme tuto formuli A'. Nechť $A'_1, \ldots, A'_n$ je důkaz A' z T, nechť $y_1, \ldots, y_m$ jsou proměnné, které se nevyskytují nikde v důkazu A' ani ve formuli A. Nechť formule A_i vznikne z A'_i nahrazením každého výskytu konstanty c_j proměnnou y_j pro $j = 1, 2, \ldots, m$ a $i = 1, 2, \ldots, n$. Potom

$$A_1, \ldots, A_n \text{ je důkazem } A_{x_1,\ldots,x_m}[y_1, \ldots, y_m] \text{ z } T \tag{10}$$

Je-li A'_i axiomem predikátové logiky, potom A_i je axiomem predikátové logiky stejného druhu. Například, je-li A'_i formule $C' \to (D' \to C')$, potom A_i je tvaru $C \to (D \to C)$. Je-li A'_i formule z T, potom A_i je táž formule, protože A'_i neobsahuje konstanty $c_1, \ldots, c_m$. Je-li A'_i odvozena z předchozích formulí pravidlem modus ponens nebo pravidlem generalizace, potom A_i je odvozena stejným pravidlem z odpovídajících formulí posloupnosti (10). Proto $T \vdash A_{x_1,\ldots,x_m}[y_1, \ldots, y_m]$ a formule A je instancí dokázané formule.

3.46 Pokud A není uzavřená a má volné proměnné $y_1, \ldots, y_n$, chceme-li dokázat implikaci $A \to B$ z předpokladů T, rozšíříme jazyk o nové konstanty $c_1, \ldots, c_n$. Potom

$$\begin{aligned} T \vdash A \to B \text{ právě když } & T \vdash A_{y_1,\ldots,y_n}[c_1, \ldots, c_n] \to B_{y_1,\ldots,y_n}[c_1, \ldots, c_n] \\ \text{právě když } & T,\ A_{y_1,\ldots,y_n}[c_1, \ldots, c_n] \vdash B_{y_1,\ldots,y_n}[c_1, \ldots, c_n] \end{aligned}$$

První ekvivalence plyne z věty o konstantách a druhá z věty o dedukci. K důkazu implikace $A \to B$ z T tedy stačí dokázat formuli $B_{y_1,\ldots,y_n}[c_1, \ldots, c_n]$ z T, $A_{y_1,\ldots,y_n}[c_1, \ldots, c_n]$.

Substituce nových konstant za volné proměnné z formule A má zajistit, že při důkazu formule B z předpokladů T, A se nepoužije pravidlo generalizace na žádnou proměnnou, která má volný výskyt v A.

Následující tvrzení je zobecněním věty o dedukci.

3.47 Věta o redukci Je-li A formule, T množina formulí, potom

$$T \vdash A \tag{11}$$

právě když existuje přirozené číslo n a formule $B_1, \ldots, B_n$, z nichž každá je uzávěrem nějaké formule z T, takové, že platí

$$\vdash B_1 \to (B_2 \to \ldots (B_n \to A) \ldots) \tag{12}$$

Důkaz. a) Pokud formule $B_1, \ldots, B_n$ splňují podmínky věty, potom

$$T \vdash B_i \text{ pro } i = 1, 2, \ldots, n \tag{13}$$

podle věty o uzávěru se tvrzení (11) odvodí ze (12) a (13) pravidlem modus ponens.

b) Je-li A dokazatelná z předpokladů T, nechť $A_1, \ldots, A_n$ jsou všechny formule z T užité v důkazu formule A jako předpoklady. Je-li B_i uzávěrem A_i pro $i = 1, 2, \ldots, n$, potom

$T \vdash B_i$ podle věty o uzávěru a

$B_1, \ldots, B_n \vdash A$

protože každá z formulí A_i je dokazatelná z B_i podle věty o uzávěru. Nakonec (12) plyne z předchozího tvrzení podle věty o dedukci.

3.48 Předchozí věta ukazuje, že dokazatelnost formule A z nějaké množiny předpokladů je ekvivalentní dokazatelnosti jiné formule z redukované množiny předpokladů. Podle (12) lze redukovat dokazatelnost formule A v teorii T na dokazatelnost jiné formule v predikátové logice. Tento výsledek ukazuje významné postavení predikátové logiky mezi teoriemi, nemá však praktický význam, protože nedává návod, jak utvořit formuli (12).

Na závěr odvodíme ještě jeden důsledek věty o dedukci. Připomeňme, že množina formulí T jazyka L je sporná, je-li z T dokazatelná každá formule jazyka L. Z věty (v2) výrokové logiky plyne, že T je sporná, právě když z T je dokazatelná nějaká formule B i její negace $\neg B$.

3.49 Důsledek Nechť A' je uzávěr formule A, nechť T je množina formulí, potom

$T \vdash A$, právě když $T \cup \{\neg A'\}$ je sporná.

Důkaz. a) Je-li A dokazatelná z T, podle věty o uzávěru totéž platí o A'. Proto $T \cup \{\neg A'\}$ je sporná.

b) Je-li $T \cup \{\neg A'\}$ je sporná, potom z ní lze dokázat libovolnou formuli, tedy i formuli A'. Potom podle věty o dedukci

$$T \vdash \neg A' \to A'$$

odkud z věty (v7) výrokové logiky dostáváme

$$T \vdash A'$$

Poslední krok důkazu plyne opět z věty o uzávěru.

Předchozí tvrzení ukazuje, že důkaz nějaké formule lze nahradit důkazem spornosti nějaké množiny formulí. Takový postup se nazývá nepřímým důkazem a je obvyklý v matematické praxi. Užívá se i v některých metodách dokazování vět pomocí počítačů.

3.4 Prenexní tvary formulí

Ve výrokové logice jsme ukázali, že ke každé formuli lze sestrojit ekvivalentní formuli v jednom ze dvou syntaktických tvarů: konjunktivním nebo disjunktivním. V obou tvarech se používají jen spojky vyjadřující negaci, konjunkci a disjunkci, navíc jen v určitém pořadí. Ve stejném duchu je i definice *prenexního tvaru* formulí predikátové logiky, která požaduje, aby se kvantifikátory při výstavbě formule uplatnily až nakonec.

Dříve, než vyslovíme definici, připomeňme, že formule, které neobsahují žádnou vázanou proměnnou, nazýváme otevřené. To znamená, že otevřené jsou právě ty formule, které vzniknou z atomických podformulí jen pomocí logických spojek.

3.50 Prenexní tvar formulí Řekneme, že *formule* A *je v prenexním tvaru*, jestliže A má tvar

$$(Q_1 x_1)(Q_2 x_2)\ldots(Q_n x_n)\, B \tag{14}$$

kde

1. $n \geq 0$ a pro každé $i = 1, 2, \ldots, n$ Q_i je buď kvantifikátor $\forall$ nebo $\exists$.
2. B je otevřená formule a $x_1, \ldots, x_n$ jsou navzájem různé proměnné.

Formule B se nazývá *otevřené jádro* formule A a posloupnost kvantifikací, která předchází B se nazývá *prefix*.

3.51 Příklad Formule $(\forall x)(\forall y)(\exists z)\,(x = y + z)$ je v prenexním tvaru.

Otevřené jádro formule (14) představuje její největší otevřenou podformuli a prefix obsahuje všechny její kvantifikátory. V případě $n = 0$ prefix odpadá a formule (14) splývá s B. Požadavek, aby všechny proměnné v prefixu byly navzájem různé, omezuje zbytečné kvantifikace.

Ukážeme, že každou formuli predikátové logiky lze transformovat do prenexního tvaru.

3.52 Věta Ke každé formuli A lze sestrojit formuli A' v prenexním tvaru tak, že

$$\vdash A \leftrightarrow A' \tag{15}$$

Formule A', o které mluví věta 3.52, se sestrojí z formule A pomocí *prenexních operací*. Při popisu prenexních operací použijeme toto značení: Zastupuje-li symbol Q kvantifikátor $\forall$, potom symbol $\overline{Q}$ zastupuje kvantifikátor $\exists$. Podobně když Q zastupuje kvantifikátor $\exists$, $\overline{Q}$ zastupuje kvantifikátor $\forall$.

Prenexní operace provádějí záměnu podformulí formule A jinými formulemi podle některého z následujících vzorů

(a) podformuli B nahraď nějakou její variantou B',

(b) podformuli $\neg(Qx)\,B$ nahraď formulí $(\overline{Q}x)\,\neg B$,

(c) pokud proměnná x není volná ve formuli B, podformuli $B \to (Qx)\,C$ nahraď formulí $(Qx)\,(B \to C)$,

(d) pokud proměnná x není volná ve formuli C, podformuli $(Qx)\,B \to C$ nahraď formulí $(\overline{Q}x)\,(B \to C)$,

(e) pokud symbol $\square$ zastupuje symbol & nebo $\vee$ a proměnná x není volná ve formuli C, potom podformuli $(Qx)\,B \,\square\, C$, případně podformuli $C \,\square\, (Qx)\,B$ nahraď formulí $(Qx)\,(B \,\square\, C)$.

Jádrem důkazu věty je následující tvrzení.

3.53 Lemma Pro libovolné formule B, C a každou proměnnou x platí
(pb) $\vdash (\overline{Q}x)\,\neg B \leftrightarrow \neg(Qx)\,B$,

(pc) $\vdash (Qx)\,(B \to C) \leftrightarrow (B \to (Qx)\,C)$, pokud x není volná v B,

(pd) $\vdash (\overline{Q}x)\,(B \to C) \leftrightarrow ((Qx)\,B \to C)$, pokud x není volná v C,

(pe) $\vdash (Qx)\,(B \,\square\, C) \leftrightarrow ((Qx)\,B \,\square\, C)$, pokud symbol $\square$ zastupuje & nebo $\vee$ a proměnná x není volná v C.

Prenexní operace tedy nahrazují podformule ekvivalentními formulemi. Tvrzení (pe) dává ekvivalenci pro obě operace z (e), uvědomíme-li si, že spojky konjunkce a disjunkce jsou komutativní.

Důkaz. (pb) Zastupuje-li symbol Q kvantifikátor $\forall$, potom

$$\vdash \neg(\forall x)\,B \leftrightarrow \neg(\forall x)\,\neg\neg B$$

protože formule B a $\neg\neg B$ jsou ekvivalentní. Přitom formuli na pravé straně ekvivalence lze vyjádřit zkratkou $(\exists x)\,\neg B$.

Případ, kdy Q zastupuje kvantifikátor $\exists$ je analogický.

(pc) Nejprve předpokládejme, že symbol Q zastupuje kvantifikátor $\forall$. Pokud proměnná x není volná ve formuli B, implikace

$$\vdash (\forall x)\,(B \to C) \to (B \to (\forall x)\,C) \tag{16}$$

je axiom. Abychom dokázali obrácenou implikaci, uvědomme si, že formule $B \to C$ vznikne složením implikací

$$B \to (\forall x)\, C \tag{17}$$
$$(\forall x)\, C \to C \tag{18}$$

To znamená, že implikace

$$((\forall x)\, C \to C) \to [(B \to (\forall x)\, C) \to (B \to C)]$$

je tautologie.

Navíc (18) je případem axiomu specifikace. Pravidlem modus ponens odvodíme

$$\vdash (B \to (\forall x)\, C) \to (B \to C)$$

Odtud pravidlem $\forall$ dostáváme

$$\vdash (B \to (\forall x)\, C) \to (\forall x)\, (B \to C) \tag{19}$$

protože formule (17) nemá volný výskyt proměnné x. Z formulí (16) a (19) lze odvodit (pc).

Zbývá případ, že Q je kvantifikátor $\exists$. Podle lemmatu 3.32 (i) je

$$\vdash C \to (\exists x)\, C \tag{20}$$

Dále

$$\vdash (C \to (\exists x)\, C) \to [(B \to C) \to (B \to (\exists x)\, C)] \tag{21}$$

protože formule (21) je tautologie. Z (20), (21) pravidlem modus ponens odvodíme

$$\vdash (B \to C) \to (B \to (\exists x)\, C)$$

odkud

$$\vdash (\exists x)\, (B \to C) \to (B \to (\exists x)\, C) \tag{22}$$

lze odvodit pravidlem $\exists$, protože $B \to (\exists x)\, C$ neobsahuje volně proměnnou x.

K důkazu obrácené implikace využijeme fakt, že pro libovolné formule D, E, F je formule

$$(\neg D \to F) \to [(E \to F) \to ((D \to E) \to F)] \tag{23}$$

tautologie.

Nejprve odvodíme

$$(\exists x)\, C \to (\exists x)\, (B \to C) \tag{24}$$

distribucí kvantoru $\exists$ z axiomu (A1).

Dále

$$\vdash (B \to C) \to (\exists x)\,(B \to C) \tag{25}$$

podle lemmatu 3.32 (i) a

$$\vdash \neg B \to (B \to C) \tag{26}$$

je větou výrokové logiky. Složením obou implikací (25), (26) dostáváme

$$\vdash \neg B \to (\exists x)\,(B \to C) \tag{27}$$

jako tautologický důsledek. Dosadíme-li B, $(\exists x)\,C$, $(\exists x)\,(B \to C)$ po řadě za D, E, F do (23) , pak pravidlem modus ponens pomocí (24) a (27) odvodíme

$$\vdash (B \to (\exists x)\,C) \to (\exists x)\,(B \to C) \tag{28}$$

Ekvivalence (pc) pro případ, že Q zastupuje kvantifikátor $\exists$, plyne potom z (22) a (28).

(pd) Předpokládejme nejprve, že Q zastupuje kvantifikátor $\forall$. Platí

$$\begin{aligned}
\vdash ((\forall x)\,B \to C) &\leftrightarrow (\neg C \to \neg(\forall x)\,B) && \text{(tautologie)}\\
&\leftrightarrow (\neg C \to \neg(\forall x)\,\neg\neg B) && \text{(Věta o ekvivalenci)}\\
&\leftrightarrow (\neg C \to (\exists x)\,\neg B) && \text{(definice } \exists\text{)}\\
&\leftrightarrow (\exists x)\,(\neg C \to \neg B) && \text{(operace pc)}\\
&\leftrightarrow (\exists x)\,(B \to C) && \text{(tautologie)}
\end{aligned}$$

Případ, že Q je $\exists$ je analogický.

Poslední tvrzení lemmatu se dokáže tak, že rozepíšeme spojku $\Box$ pomocí negace a implikace a užijeme prenexní operace (b) – (d).

Důkaz věty 3.52. provedeme indukcí podle složitosti formule A. Je-li A atomická, pak A je v prenexním tvaru a za A' zvolíme A.

Je-li A tvaru $\neg B$ a již umíme sestrojit prenexní tvar B' formule B, potom A' vznikne z $\neg B'$ za pomoci operací (b).

Pokud A je tvaru $B \to C$ a již umíme sestrojit prenexní tvary B', C' formulí B, C, potom $A \leftrightarrow (B' \to C')$. Sestrojme varianty B'', C'' formulí B', C' takové, že žádná volná proměnná formule C' (a tedy ani C'') není vázaná ve formuli B'' a také žádná volná proměnná ve formuli B' (a tedy ani v B'') není vázaná ve formuli C''. Z Věty o variantách platí

$$A \leftrightarrow (B'' \to C'')$$

a prenexní tvar formule $B'' \to C''$ (a tedy i formule A) odvodíme z formule $B'' \to C''$ pomocí operací (c), (d).

Nakonec, je-li A tvaru $(\forall x)\,B$ a B' je prenexní tvar formule B, potom $(\forall x)\,B'$ je prenexní tvar formule A, pokud proměnná x není vázaná ve formuli B', jinak je prenexním tvarem formule B formule B'.

Pokud formule A obsahuje logické spojky $\&$, $\vee$, můžeme tyto symboly buď eliminovat rozepsáním zkratek, nebo použijeme prenexní operace (e). Z prenexních operací (c), (d) je zřejmé, že pro spojku $\leftrightarrow$ není přímá analogie operací (c), (d) možná, ekvivalenci proto eliminujeme rozepsáním na konjunkci dvou implikací.

3.54 Příklad Nechť x není volná ve formuli B a proměnná y se nevyskytuje v B ani v C. Potom následující formule jsou ekvivalentní (napravo uvádíme použité prenexní operace).

$B \leftrightarrow (\forall x)\, C$	
$(B \to (\forall x)\, C)\ \&\ ((\forall y)\, C_x[y] \to B)$	definice ekvivalence, (a)
$(\forall x)\, (B \to C)\ \&\ (\exists y)\, (C_x[y] \to B)$	(c), (d)
$(\forall x)(\exists y)\, [(B \to C)\ \&\ (C_x[y] \to B)]$	(e)

3.55 Příklad Následující formule jazyka aritmetiky jsou ekvivalentní

$(\exists x)\, (x = y) \to (\exists x)\, (x = 0 \vee \neg(\exists y)\, (y < 0))$	
$(\exists x)\, (x = y) \to (\exists u)\, (u = 0 \vee \neg(\exists v)\, (v < 0))$	(a)
$(\exists x)\, (x = y) \to (\exists u)\, (u = 0 \vee (\forall v)\, \neg(v < 0))$	(b)
$(\exists x)\, (x = y) \to (\exists u)(\forall v)\, (u = 0 \vee \neg(v < 0))$	(e)
$(\forall x)(\exists u)(\forall v)\, [(x = y) \to (u = 0 \vee \neg(v < 0))]$	(c), (d)

Při konstrukci prenexního tvaru není pořadí prenexních operací jednoznačně určeno, proto je prenexním tvarem také formule

$$(\exists u)(\forall v)(\forall x)\, [(x = y) \to (u = 0 \vee \neg(v < 0))]$$

3.5 Predikátová logika s rovností

Při definici splňování jsme zdůraznili zvláštní postavení predikátu rovnosti v sémantice jazyka s rovností. Axiomy rovnosti, které syntakticky popisují vlastnosti predikátu rovnosti, vyjadřují přirozené požadavky, které matematika klade na rovnost: aby rovnost byla reflexivní, a aby sobě rovná individua měla stejné vlastnosti vůči každému predikátu jazyka a dávala stejné výsledky při použití libovolné operace.

V dalším budeme předpokládat, že jazyk, se kterým pracujeme, obsahuje predikátový symbol $=$ pro rovnost. Syntaktické vlastnosti tohoto predikátu jsou vyjádřeny ve třech následujících schematech axiomů.

Je-li x proměnná, potom formule

$$x = x \tag{R1}$$

je axiom identity.

Jsou-li $x_1, \ldots, x_k,\ y_1, \ldots, y_k$ proměnné a je-li f k-ární funkční symbol, potom formule

$$(x_1 = y_1 \to \ldots (x_k = y_k \to (f(x_1, \ldots, x_k) = f(y_1, \ldots, y_k)) \ldots)) \qquad \text{(R2)}$$

je axiom rovnosti pro funkční symbol f.

Jsou-li $x_1, \ldots, x_k,\ y_1, \ldots, y_k$ proměnné a je-li p k-ární predikátový symbol, potom formule

$$(x_1 = y_1 \to \ldots (x_k = y_k \to (p(x_1, \ldots, x_k) \to p(y_1, \ldots, y_k)) \ldots)) \qquad \text{(R3)}$$

je axiom rovnosti pro predikátový symbol p.

Symetrii a tranzitivnost rovnosti lze odvodit z axiomů (R3) pro predikát rovnosti.

Nejprve dokážeme symetrii, pro libovolné proměnné $x,\ y$ platí

$$\vdash x = y \to y = x \qquad (31)$$

Při důkazu (31) i v dalších aplikacích axiomů (R2), (R3) upustíme od psaní závorek při úmluvě, že chybějící závorky se kumulují doprava (tedy tak, jako v uvedených axiomech). Formule

$$\vdash x = y \to x = x \to x = x \to y = x \qquad (32)$$

je případ axiomu (R3) a pořadí prvních tří členů implikace (32) lze běžným obratem výrokové logiky zaměnit. Jinými slovy, formule

$$\vdash x = x \to x = x \to x = y \to y = x$$

je tautologickým důsledkem formule (32). Odtud již (31) plyne z axiomů (R1) podle pravidla modus ponens.

Formule

$$\vdash x = y \to y = z \to x = z \qquad (33)$$

vyjadřuje tranzitivnost rovnosti. Při důkazu vycházíme z následujícího případu axiomu (R3)

$$\vdash y = x \to z = z \to y = z \to x = z \qquad (34)$$

Opět

$$\vdash z = z \to y = x \to y = z \to x = z$$

je tautologickým důsledkem (34). Pravidlem modus ponens z axiomu $z = z$ odvodíme

$$\vdash y = x \to y = z \to x = z \qquad (35)$$

Formule (33) se odvodí složením implikací (31) a (35) jako jejich tautologický důsledek. Instance formulí (31), (35) a axiomu (R1) se běžně využívají při řešení rovnic. Následující věta rozšiřuje paletu takových obratů.

3.56 Věta Nechť $t_1, \ldots, t_n,\ s_1, \ldots, s_n$ jsou termy takové, že platí

$$\vdash\ t_i = s_i \text{ pro } i = 1, 2, \ldots, n \tag{36}$$

(i) Je-li t term a s je term, který vznikne z t záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom

$$\vdash\ t = s \tag{37}$$

(ii) Je-li A' formule, která vznikne z formule A záměnou některých výskytů termů t_i odpovídajícími termy s_i, kromě případů, kdy term t_i je proměnná x, která je součástí kvantifikace $(\forall x)\ldots$ nebo $(\exists x)\ldots$, potom

$$\vdash\ A \leftrightarrow A'$$

Důkaz. (i) Dokážeme indukcí podle složitosti termu t. Je-li t proměnná, nebo některý z termů $t_1, \ldots, t_n$ a term s vznikne záměnou celého termu t odpovídajícím termem, pak (37) je jeden z předpokladů (36).

Je-li term t tvaru $f(r_1, \ldots, r_k)$ a pro termy $r_1, \ldots, r_k$ již bylo tvrzení (i) dokázáno a je-li term s tvaru $f(r'_1, \ldots, r'_k)$, kde $r'_j,\ j = 1, 2, \ldots, k$ vznikne z r_j záměnou některých výskytů termů t_i odpovídajícími termy s_i, podle indukčního předpokladu platí

$$\vdash\ r_j = r'_j \text{ pro } j = 1, 2, \ldots, k \tag{38}$$

Dále formule

$$\vdash\ r_1 = r'_1 \to \ldots \to r_k = r'_k \to f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k) \tag{39}$$

je instancí axiomu (R2). Tvrzení (37) lze odvodit z (38) a (39) pomocí pravidla modus ponens.

(ii) Podle předpokladu se při přechodu od formule A k A' nenahrazují proměnné, které jsou součástí kvantifikací. Záměna termů tedy probíhá jen v atomických podformulích formule A. Stačí, když ukážeme, že libovolná atomická podformule $p(r_1, \ldots, r_k)$, kde p je predikát různý od rovnosti, případně podformule $r_1 = r_2$ je ekvivalentní se svou transformací $p(r'_1, \ldots, r'_k)$ nebo $r'_1 = r'_2$.

Podle (i) platí (38) a formule

$$\vdash\ r_1 = r'_1 \to r_2 = r'_2 \to \ldots \to r_k = r'_k \to p(r_1, \ldots, r_k) \to p(r'_1, \ldots, r'_k)$$

je instancí axiomu (R3). Odtud

$$p(r_1, \ldots, r_k) \to p(r'_1, \ldots, r'_k)$$

lze odvodit pomocí (38) a pravidla modus ponens. Obrácená implikace plyne podobným způsobem ze symetrie rovnosti (31) a (38). Obě atomické podformule jsou tedy ekvivalentní. Případ atomické podformule $r_1 = r_2$ se dokazuje obdobně. Podle věty o ekvivalenci je formule A' ekvivalentní s A, protože vznikla záměnou podformulí za ekvivalentní formule.

3.57 Věta Jsou-li $t,\ t_1,\ldots,t_n,\ s_1,\ldots,s_n$ termy a je-li A formule, potom platí

(i) $\vdash t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to t[t_1,\ldots,t_n] = t[s_1,\ldots,s_n]$

(ii) $\vdash t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to (A[t_1,\ldots,t_n] \leftrightarrow A[s_1,\ldots,s_n])$

Je-li navíc x proměnná, která není obsažena v termu t, potom

(iii) $\vdash A_x[t] \leftrightarrow (\forall x)\,(x = t \to A)$

(iv) $\vdash A_x[t] \leftrightarrow (\exists x)\,(x = t \,\&\, A)$

Důkaz. Pokud termy $t_1,\ldots,t_n,\ s_1,\ldots,s_n$ neobsahují žádnou proměnnou, (i) a (ii) plyne z odpovídajících tvrzení věty 3.56 podle věty o dedukci. V obecném případě je třeba proměnné v termech $t_i,\ s_i$ nahradit novými konstantami. Obě tvrzení plynou z věty 3.56 podle věty o dedukci a věty o konstantách.

(iii) Formule

$$\vdash (\forall x)\,(x = t \to A) \to (t = t \to A_x[t])$$

je případem axiomu specifikace. Záměnou prvních dvou podformulí implikace odvodíme

$$\vdash t = t \to ((\forall x)\,(x = t \to A) \to A_x[t])$$

jako tautologický důsledek. Nakonec

$$\vdash (\forall x)\,(x = t \to A) \to A_x[t]$$

odvodíme pravidlem modus ponens pomocí předchozí formule a instance $t = t$ axiomu (R1).

Abychom dokázali obrácenou implikaci, použijeme (ii)

$$\vdash x = t \to (A \leftrightarrow A_x[t])$$

Odkud

$$\vdash A_x[t] \to (x = t \to A)$$

odvodíme jako tautologický důsledek. Nakonec

$$\vdash A_x[t] \to (\forall x)\,(x = t \to A)$$

odvodíme pravidlem $\forall$, protože podle předpokladu formule $A_x[t]$ neobsahuje volně proměnnou x. Tvrzení (iv) se dokazuje podobným způsobem.

3.6 Cvičení A

Sémantika predikátové logiky prvního řádu

a) Ověřte zda následující formule jsou splněny v nějaké realizaci jazyka

$(\exists x)p(x)$

$(\forall x)p(x)$

$(\exists x)(\forall y)(q(x,x)\ \&\ \neg q(x,y))$

$(\exists x)(\exists y)(p(x)\ \&\ \neg p(y))$

$(\exists x)(\forall y)q(x,y) \to (\forall y)(\exists x)q(x,y)$

$(\exists x)(\forall y)q(x,y) \to (\forall z)R(x,y,z)$

$(Vx)(Ey)q(x,y) \to (Ey)(Vx)q(x,y)$

b) Ověřte, které z formulí v a) jsou logicky pravdivé, to znamená, že jsou splněny v každé realizaci jazyka.

Formální systém dokazování v predikátové logice

1) Dokažte

a) $(\forall x)(A \to B) \to (\exists xA \to B)$, pokud x nemá volný výskyt ve formuli B.

b) proměnná x nemá volný výskyt ve formuli A

$A \leftrightarrow (\forall x)A$

$A \leftrightarrow (\exists x)A$

$(\forall x)A \leftrightarrow (\exists x)A$

c) $QxQyB \leftrightarrow QyQxB$

kde Q označuje universální nebo existenční kvantifikátor.

$Qx_1Qx_2 \ldots Qx_nB \leftrightarrow Qx_{p_1}Qx_{p_2} \ldots Qx_{p_n}B,$

kde Q označuje universální nebo existenční kvantifikátor a $p_1, p_2, \ldots, p_n$ je libovolná permutace indexů $1, 2, \ldots n$.

d) $(\exists x)(\forall y)B \to (\forall y)(\exists x)B$

e) $\neg(\exists x)A \to \neg(\forall x)A$

f) $(\exists x)(A \,\&\, (B \to C)) \to (\forall x)(A \to \neg C) \to \neg B)$

Pokud proměnná x nemá volný výskyt ve formuli B.

2) Dokažte

a) $\forall x(A \,\&\, B) \leftrightarrow (\forall xA \,\&\, \forall xB)$

b) $\exists x(A \vee B) \leftrightarrow (\exists xA \vee \exists xB)$

c) $\exists x(A \,\&\, B) \to (\exists xA \,\&\, \exists xB)$

d) $(\exists xA \vee \exists xB) \to \exists x(A \vee B)$

e) $(\forall xA \to \forall xB) \to (\forall xA \to \forall xB)$

f) $(\forall xA \to \forall xB) \to (\exists xA \to \exists xB)$

Věta o korektnosti

1) Ověřte zda následující formule jsou dokazatelné v predikátové logice

a) $\forall x \exists y A \to \exists y \forall x A$

b) $(\exists xA \,\&\, \exists xB) \to \exists x(A \,\&\, B)$

c) $\forall x(A \vee B) \to (\forall xA \vee \forall xB)$

d) $(A \to B) \to (\forall xA \to \forall xB)$

e) $(A \to B) \to (\exists xA \to \exists xB)$

Věty o rovnosti

Dokažte

a) $t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to t[t_1, t_2, \ldots, t_n] = t[s_1, s_2, \ldots, s_n]$

b) $t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to$
$\to (A[t_1, t_2, \ldots, t_n] \leftrightarrow A[s_1, s_2, \ldots, s_n])$

c) Nechť x je proměnná a t je term, který neobsahuje proměnnou x.

Dokažte, že platí

$$A_x[t] \leftrightarrow \forall x(x = t \to A)$$

$$A_x[t] \leftrightarrow \exists x(x = t \,\&\, A)$$

transitivnost rovnosti

$x = x \to y = z \to x = y \to x = z$

3.7 Cvičení B

1. (Polský zápis termů)
   Je-li dán jazyk L prvního řádu, říkáme, že slovo t je bezzávorkovým zápisem termu, jestliže t vznikne podle následujících pravidel:

   (i) t sestává z jediného symbolu – symbolu pro proměnnou,

   (ii) t je tvaru $f\,t_1, \ldots, t_n$ (zřetězení $n+1$ slov), kde f je n-ární funkční symbol a $t_1, \ldots, t_n$ jsou bezzávorkové zápisy termů.

   (a) Dokažte obdobu tvrzení (a) – (c) ze cvičení 3, kapitola 1.

   (b) Modifikujte definici polského zápisu z citovaného cvičení první kapitoly tak, aby popisovala polský zápis všech formulí predikátove logiky. Dokažte obdobu tvrzení (a) – (c) z citovaného cvičení.

2. Jsou-li T, S množiny formulí, A, B formule, potom platí

   (a) Je-li $T \subset S$ a $T \vdash A$, potom $S \vdash A$.

   (b) $T \vdash A$ právě když pro nějakou konečnou podmnožinu $T' \subset T$ platí $T' \vdash A$.

   (c) Je-li $T \vdash C$ pro každou formuli C z množiny S a je-li $S \vdash A$, potom $T \vdash A$.

   (d) Je-li S množina všech uzávěrů formulí z T, potom $T \vdash A$, právě když $S \vdash A$.

   (e) Je-li $T \vdash A$ a $T \vdash A \to B$, potom $T \vdash B$.

3. Je-li A' uzávěr formule A, je-li B formule a T množina formulí, potom $T, A \vdash B$ právě když $T \vdash A' \to B$.

4. (a) Ukažte, že pravidlo zavedení $\forall$ (viz lemma 1) plně nahradí odvozovací pravidlo generalizace. Navíc je možné vynechat schema axiomů $(\forall x)\,(A \to B) \to (A \to (\forall x)\,B)$, kde proměnná x není volná ve formuli A.

   (b) Ukažte, že pravidlo zavedení $\exists$ (viz lemma 2 (ii)) a schema (i) z téhož lemmatu plně nahradí pravidlo zavedení $\forall$ a schema specifikace. Podle (a) vznikne formální systém ekvivalentní predikátové logice prvního řádu.

   Oba typy systémů uvedené v bodech (a), (b) byly používány Hilbertem a jeho žáky.

5. Je-li T množina formulí, T je sporná, právě když $\vdash \neg A_1 \vee \ldots \vee \neg A_n$, kde $A_1, \ldots, A_n$ jsou uzávěry (navzájem různých) formulí z množiny T.

6. Jsou-li $v_1, \ldots, v_n$ navzájem různé symboly pro proměnné, označme

   A_2 formuli $(\exists v_1)(\exists v_2)\,(v_1 \neq v_2)$

   a dále

   A_3 označuje formuli $(\exists v_1)(\exists v_2)(\exists v_3)\,(v_1 \neq v_2 \,\&\, v_1 \neq v_3 \,\&\, v_2 \neq v_3)$

   Je zřejmé, jak bychom zapsali formuli A_n, která tvrdí "existuje alespoň n různých individuí".

   Jsou-li x, y, z navzájem různé symboly pro proměnné, dokažte $\vdash (\exists x)\,(x \neq y \,\&\, x \neq z) \leftrightarrow ((y = z \,\&\, A_2) \vee (y \neq z \,\&\, A_3))$.

7. Dokažte tvrzení (i), (ii) a (iv) z věty 2 v §4.

8. Převeďte následující formule do prenexního tvaru

   (a) $(\forall x)((\forall y)\,(y < x \to P(y)) \to P(x)) \to (\forall x)P(x)$,

   (b) $(\exists x)\,P(x) \to (\exists x)\,(P(x) \,\&\, (\forall y)\,(y < x \to \neg P(y)))$, kde P je unární predikátový symbol.

9. Nechť L je jazyk prvního řádu, nechť c je symbol pro konstantu. který se nevyskytuje v L, nechť L' je jazyk, který vznikne z L rozšířením o symbol c. Ke každé formuli A jazyka L přiřaďme formuli $A^\star$ tak, že libovolný term ve formuli A nahradíme konstantou c a vynecháme všechny kvantifikátory a všechny proměnné, které jsou bezprostředně za kvantifikátorem.

   (a) Konstrukci formule $A^\star$ lze popsat indukcí dle složitosti:
   Je-li A atomická formule tvaru $p(t_1, \ldots, t_n)$, kde p je n-ární predikátový symbol různý od rovnosti a $t_1, \ldots, t_n$ jsou termy, pak $A^\star$ je formule $p(c, \ldots, c)$.
   Je-li A atomická formule tvaru $t_1 = t_2$, kde t_1, t_2 jsou termy, pak $A^\star$ je formule $c = c$.
   Je-li A tvaru $\neg B$, nebo $B \,\square\, C$, kde B, C jsou formule a $\square$ je symbol pro logickou spojku, potom $A^\star$ je formule $\neg B^\star$, nebo $B^\star \,\square\, C^\star$.
   Je-li A tvaru $(Qx)\,B$, kde Q je symbol pro kvantifikátor a X je nějaká proměnná, potom $A^\star$ je tvaru $B^\star$.

   (b) Je-li L jazyk bez rovnosti, A libovolná formule taková, že $\vdash A$, potom $A^\star$ je tautologie.

   (c) Je-li L jazyk s rovností, A libovolná formule taková, že $\vdash A$, potom $A^\star$ je tautologický důsledek formule $c = c$.

(d) Pro žádnou formuli A není $\vdash A$ a $\vdash \neg A$. Formální systém predikátové logiky je tedy bezesporný. Problém bezespornosti predikátové logiky byl převeden na bezespornost výrokové logiky.

Kapitola 4

Pravdivost a dokazatelnost

Zatím jsme sémantiku a formální systém (syntax) predikátové logiky zkoumali odděleně. Zavedli jsme jazyk prvního řádu a nejprve jsme se zabývali relačními strukturami, které jazyk realizují a definovali jsme splňování a pravdivost formulí v realizacích jazyka. Teprve potom jsme zavedli formální systém predikátové logiky, její axiomy a odvozovací pravidla. Z nich jsme dokázali základní věty predikátové logiky.

Nyní si položíme otázku, zda zvolený formální systém predikátové logiky dobře vystihuje její sémantiku, zejména zda věty predikátové logiky jsou logicky pravdivými formulemi a naopak. Tyto otázky budeme zkoumat nejen pro formální systém predikátové logiky, ale pro třídu všech teorií prvního řádu. Nejprve zavedeme potřebné pojmy.

4.1 Věta o korektnosti

4.1 Logicky pravdivé formule Je-li L jazyk, říkáme, že *formule* A *jazyka* L *je logicky pravdivá* a píšeme $\models A$, jestliže A je splněna v každé realizaci jazyka L.

Logicky pravdivé jsou ty formule, které jsou splněny bez ohledu na realizaci jazyka, tedy při libovolné interpretaci speciálních symbolů. Logicky pravdivým formulím říkáme také logicky platné formule.

4.2 Teorie prvního řádu Je-li L jazyk prvního řádu a T je množina formulí jazyka L, říkáme, že T *je teorie prvního řádu (v predikátové logice) s jazykem* L. Formulím z množiny T říkáme *speciální axiomy teorie* T. Predikátová logika je speciálním případem teorie prvního řádu, která nemá žádné speciální axiomy.

Předchozí definice odpovídá postupu, kterým v matematice zavádíme nějakou speciální teorii. Nejprve zvolíme jazyk vhodný k formálnímu popisu teorie a

všechny předpoklady o objektech, se kterými teorie pracuje, vyjádříme pomocí vhodných formulí zvoleného jazyka - speciálních axiomů.

Za zmínku stojí i s tím spojený posun zájmu. Při odvozování vět teorie nám jde především o takové, ve kterých se projeví speciální vlastnosti teorie. Méně se zajímáme o logicky pravdivé formule, které platí ve všech realizacích jazyka teorie, zajímáme se o formule, které jsou pravdivé v těch realizacích jazyka, ve kterých jsou splněny všechny speciální axiomu teorie.

4.3 Modely teorie (i) Je-li T teorie s jazykem L a $\mathfrak{M}$ je realizace jazyka L, říkáme, že $\mathfrak{M}$ *je modelem teorie* T a píšeme $\mathfrak{M} \models T$, je-li v $\mathfrak{M}$ splněn každý speciální axiom teorie T.

(ii) Říkáme, že *formule* A *je sémantickým důsledkem teorie* T nebo že A *je* T*-platná formule*, je-li A splněna v každém modelu teorie T. V takovém případě píšeme $T \models A$.

4.4 Příklad a) *Teorie uspořádání* má jazyk s rovností, který obsahuje jediný speciální symbol, binární predikát $<$ a dva speciální axiomy

$$\neg(x < x)$$

$$x < y \to (y < z \to x < z)$$

kde x, y, z jsou proměnné. Každý model této teorie je částečně uspořádaná množina.

Přidáme-li ještě axiom

$$x < y \vee x = y \vee y < x$$

potom každý model této teorie je lineárně uspořádaná množina. Takové teorii se říká *teorie lineárního uspořádání.*

b) *Teorie okruhů, oborů integrity a těles* Nechť $L = \{0, 1, +, \cdot\}$ je jazyk s rovností takový, že $0, 1$ jsou symboly pro konstanty a $+, \cdot$ jsou symboly pro binární funkce. *Teorie komutativních okruhů s jednotkou* má následující speciální axiomy

$$x + (y + z) = (x + y) + z \tag{o1}$$

$$x + 0 = x \qquad 0 + x = x \tag{o2}$$

$$(\exists y)(x + y = 0 \quad \& \quad y + x = 0) \tag{o3}$$

$$x + y = y + x \tag{o4}$$

$$1 \cdot x = x \qquad x \cdot 1 = x \tag{o5}$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \tag{o6}$$

$$x \cdot y = y \cdot x \tag{o7}$$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \tag{o8}$$

Přidáním axiomu

$$x \cdot y = 0 \to (x = 0 \vee y = 0) \tag{i1}$$

dostáváme axiomy *teorie oborů integrity*.

Přidáme-li k axiomům teorie okruhů dva axiomy

$$0 \neq 1 \tag{t1}$$

$$x \neq 0 \to (\exists y)(y \cdot x = 1) \tag{t2}$$

dostáváme axiomy *teorie těles*. Modelem teorie okruhů je okruh, modelem teorie oborů integrity je obor integrity a modelem teorie těles je těleso. V algebře se dokazuje, že axiom (i1) je větou teorie těles. Každé těleso je tedy oborem integrity.

c) *Elementární aritmetika* je teorie s jazykem s rovností a speciálními symboly 0, S, $+$, $\cdot$, kde 0 je konstanta označující nejmenší přirozené číslo, S je unární funkční symbol pro funkci následníka $S(x) = x + 1$, $+$ a $\cdot$ jsou binární pro operace součtu a součinu přirozených čísel. Elementární aritmetika má tyto speciální axiomy.

$$S(x) \neq 0$$
$$S(x) = S(y) \to x = y$$
$$x + 0 = x$$
$$x + S(y) = S(x + y)$$
$$x \cdot 0 = 0$$
$$x \cdot S(y) = (x \cdot y) + x$$

První dva axiomy tvrdí, že následník přirozeného čísla je nenulový a že S je prostá funkce, další čtyři axiomy podávají rekurzivní definici součtu a součinu.

Struktura $\mathfrak{N}$ z příkladu 3.12 c je určena množinou přirozených čísel v teorii množin s operacemi součtu a součinu přirozených čísel tak jak jsou definovány v teorii množin je modelem elementární aritmetiky. $\mathfrak{N}$ nazýváme *standardní model aritmetiky*.

4.5 Úplnost formálního systému predikátové logiky Hlavním výsledkem této kapitoly je věta o úplnosti predikátové logiky, která tvrdí, že pro libovolnou teorii T prvního řádu množina všech vět teorie T je rovna množině všech T-platných formulí. Speciálně pro predikátovou logiku to znamená, že libovolná formule je větou predikátové logiky, právě když je logicky platná.

Říkáme, že *formální systém predikátové logiky je úplný*, protože dovoluje odvodit právě všechny logicky platné formule. Prvním krokem na cestě k tomuto cíli je následující tvrzení.

4.6 Věta o korektnosti Je-li T teorie s jazykem L a je-li A formule jazyka L taková, že $T \vdash A$, potom $T \models A$. Každá věta teorie T je splněna ve všech modelech.

Důkaz se provádí indukcí podle délky důkazu formule A. V první části dokážeme, že všechny axiomy predikátové logiky jsou logicky pravdivé a tedy také T-platné a ve druhé části dokážeme, že odvozovací pravidla jsou korektní: z T-platných formulí odvozují zase T-platnou formuli a speciálně z logicky platných formulí odvozují zase logicky platnou formuli.

Nechť $A_1, A_2, \ldots, A_n$ je důkaz formule A z axiomů T. Nechť $\mathfrak{M}$ je libovolný model teorie T. Indukcí podle délky důkazu dokážeme, že $\mathfrak{M} \models A_i$ platí pro každé $i \leq n$. Je-li dáno i, předpokládejme, že každá formule A_j, $j < i$ je splněna v modelu $\mathfrak{M}$. Pro $i = 1$ je to prázdný předpoklad. Podle definice důkazu pro formuli A_i mohou nastat tyto případy

a) A_i je axiom z T, potom A_i je splněna v $\mathfrak{M}$, protože $\mathfrak{M}$ je model teorie T podle předpokladu.

b) A_i je axiom predikátové logiky. Případy jednotlivých schemat axiomů rozebereme každý zvlášť.

b1) A_i je axiom výrokové logiky. Víme, že A_i je tautologie. Je-li e libovolné ohodnocení proměnných v modelu $\mathfrak{M}$, ohodnocení e určuje pravdivostní hodnoty všech prvotních podformulí formule A_i. Formule A_i je tautologie, je tedy pravdivá v $\mathfrak{M}$ při ohodnocení e nezávisle na pravdivosti svých prvotních podformulí. Protože e je libovolné ohodnocení proměnných, A_i je splněna v $\mathfrak{M}$.

b2) A_i je axiom specifikace tvaru $(\forall x)B \to B_x[t]$. Nechť e je libovolné ohodnocení proměnných. Je-li podformule $(\forall x)B$ nepravdivá při ohodnocení e, podle definice pravdivosti implikace je formule A_i pravdivá při ohodnocení e. Předpokládejme, že podformule $(\forall x)B$ je pravdivá při ohodnocení e. Podle definice pravdivosti, potom $\mathfrak{M} \models B[e(x/m)]$ pro libovolné individuum m. Speciálně, je-li m individuum $t[e]$, podle lemmatu 3.23 je formule $B_x[t]$ pravdivá při ohodnocení e, a tedy také formule A_i je pravdivá při ohodnocení e. Ukázali jsme, že formule A_i je pravdivá v $\mathfrak{M}$ při libovolném ohodnocení proměnných, je tedy splněna v $\mathfrak{M}$.

b3) Je-li A_i axiom tvaru $(\forall x)(B \to C) \to (B \to (\forall x)C)$, kde formule B neobsahuje volně proměnnou x a je-li e libovolné ohodnocení proměnných, stejně jako v b2), zajímavý je jen případ, kdy podformule $(\forall x)(B \to C)$ je pravdivá při ohodnocení e. Podle definice splňování to znamená, že pro libovolné individuum m platí $\mathfrak{M} \models (B \to C)[e(x/m)]$. Podle definice pravdivosti implikace to znamená, že buď podformule B není pravdivá při ohodnocení $e(x/m)$, nebo podformule C je při tomto ohodnocení pravdivá. Protože B neobsahuje proměnnou x volně, B je pravdivá při ohodnocení $e(x/m)$, právě když je pravdivá při ohodnocení e. Přitom pravdivost C při ohodnocení $e(x/m)$ pro každé individuum m, podle definice pravdivosti znamená, že formule $(\forall x)C$ je pravdivá při ohodnocení e.

Ukázali jsme, že při ohodnocení e buď není pravdivá formule B nebo je pravdivá formule $(\forall x)C$, tedy formule $B \to (\forall x)C$ je pravdivá při ohodnocení e.

To znamená, že je pravdivá také implikace A_i. To vše při libovolném ohodnocení e, proto $\mathfrak{M} \models A_i$.

b4) Je-li A_i axiom identity tvaru $x = x$, potom A_i je pravdivá při každém ohodnocení e, protože obě strany rovnosti jsou realizovány stejným individuem $e(x)$.

Je-li A_i axiom rovnosti pro n-ární funkční symbol f, tedy axiom

$$x_1 = y_1 \to x_2 = y_2 \to \ldots \to x_n = y_n \to f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n)$$

mějme libovolné ohodnocení proměnných e. Zajímavý je pouze případ, kdy všechny předpoklady implikace $x_i = y_i$ jsou pravdivé při e. Potom je pro každé $i, 1 \leq i \leq n$ proměnným x_i, y_i přiřazeno stejné individuum $e(x_i) = m_i = e(y_i)$. To znamená, že oba termy v poslední rovnosti implikace jsou realizovány stejným individuem $f_{\mathfrak{M}}(m_1, m_2, \ldots, m_n)$. Podle definice pravdivosti je pak rovnost $f(x_1, x_2, \ldots, x_n) = f(y_1, y_2, \ldots, y_n)$ pravdivá při ohodnocení e a spolu s ní i axiom rovnosti A_i. Protože e bylo libovolné ohodnocení proměnných, axiom A_i je splněn v $\mathfrak{M}$. Podobně postupujeme Je-li A_i axiom rovnosti pro predikát.

Zbývají případy, kdy formule A_i je odvozena nějakým odvozovacím pravidlem.

c) Je-li formule A_i odvozena pravidlem modus ponens z formulí A_j, A_k, kde $j, k < i$ a A_k je tvaru $A_j \to A_i$, podle indukčního předpokladu jsou formule A_j, A_k pravdivé v $\mathfrak{M}$ při libovolném ohodnocení proměnných e. Z definice pravdivosti implikace pak dostáváme, že také formule A_i je pravdivá při libovolném ohodnocení e, je tedy splněna v modelu $\mathfrak{M}$.

d) Je-li formule A_i odvozena pravidlem generalizace z nějaké formule A_j pro $j < i$, potom A_i je tvaru $(\forall x)A_j$. Nechť e je libovolné ohodnocení proměnných. Podle indukčního předpokladu je formule A_j pravdivá při každém ohodnocení proměnných, speciálně také při každém ohodnocení $e(x/m)$ pro libovolné individuum m. Podle definice pravdivosti je pak formule $(\forall x)A_j$, tedy formule A_i pravdivá při ohodnocení e. Protože e je libovolné ohodnocení proměnných, A_i je splněna v modelu $\mathfrak{M}$. Tím je věta o korektnosti dokázána.

4.7 Důsledek Všechny axiomy predikátové logiky jsou logicky pravdivé formule. Z korektnosti odvozovacích pravidel plyne, že také všechny věty predikátové logiky jsou logicky pravdivé formule.

4.8 Příklad a) Věta o korektnosti dává metodu, jak ukázat že nějaká formule není větou predikátové logiky nebo větou nějaké teorie T. Uvažujme formuli $x = 0$ ve standardním modelu $\mathfrak{N}$ elementární aritmetiky. V něm je konstanta 0 realizována prázdnou množinou. Ohodnotíme-li proměnnou x kterýmkoli jiným individuem, formule $x = 0$ není pravdivá v $\mathfrak{N}$, není tam tedy ani splněna. Podle věty o korektnosti tato formule není větou elementární aritmetiky a tím méně větou predikátové logiky. Stejným způsobem bychom dokázali, že ani formule $x \neq 0$

není větou elementární aritmetiky. Tento výsledek nás nepřekvapí, uvědomíme-li si, že kdyby například formule $x = 0$ byla větou elementární aritmetiky, pak podle věty o uzávěru by větou byla také formule $(\forall x)(x = 0)$.

b) Nyní můžeme ukázat, že větu o dedukci nelze v predikátové logice vyslovit bez předpokladu o proměnných formule A. V predikátové logice dokážeme

$$x = 0 \vdash y = 0$$

protože $y = 0$ je instancí $x = 0$. Není však dokazatelná implikace

$$x = 0 \to y = 0$$

protože není splněna ve standardním modelu aritmetiky $\mathfrak{N}$. K tomu stačí vzít ohodnocení proměnných, které proměnné x přiřazuje prázdnou množinu a proměnné y kterékoliv jiné individuum.

4.9 Důsledek Má-li teorie T model, je bezesporná.

Důkaz. Nechť $\mathfrak{M}$ je model teorie T. Nechť A je nějaká uzavřená formule jazyka teorie T. Podle definice splňování je právě jedna z formulí A a $\neg A$ pravdivá v modelu $\mathfrak{M}$. Ta z obou formulí, která není pravdivá v $\mathfrak{M}$, nemůže být podle věty o korektnosti dokazatelná. To znamená, že teorie T je bezesporná.

4.10 Důsledek Predikátová logika je bezesporná.

Důkaz. Každá realizace jazyka je modelem predikátové logiky podle Důsledku 4.7. Tvrzení potom plyne z Důsledku 4.9.

4.11 Finitní a nefinitní důkazy Důkaz bezespornosti predikátové logiky podle Důsledku 4.10 se opírá o model, který může být sám nekonečný. Takovému důkazu říkáme nefinitní. Ve cvičeních ukážeme, že bezespornost predikátové logiky lze dokázat pomocí jednoprvkového, tedy finitního modelu. V obecném případě může být důkaz bezespornosti nějaké teorie podmíněn existencí nějakého modelu, který je nekonečný a existenci konečného modelu dané teorie neumíme dokázat nebo dokonce umíme dokázat, že daná teorie žádné konečné modely nemá (například aritmetika). Takovým důkazům bezespornosti se říká sémantické.

Na rozdíl od množinových struktur, které jsou modely teorií, formule a důkazy v jazyku dané teorie jsou syntaktické objekty, které jsou finitní. Finitní důkaz bezespornosti teorie T lze provést například tak, že popíšeme způsob, jak lze libovolný důkaz sporu v teorii T syntakticky transformovat na důkaz sporu v nějaké jiné teorii S, o které již víme, že je bezesporná. Potom T musí být také bezesporná teorie.

Finitní důkaz popsaného typu se opírá jen o syntax teorií T a S, proto se takovým důkazům říká syntaktické. Finitní (syntaktický) důkaz bezespornosti predikátové logiky redukcí sporu do výrokové logiky není obtížný. Stručný návod byl zařazen do cvičení.

4.2 Věta o úplnosti

Zatím jsme dokázali, že formální systém predikátové logiky je korektní, tedy že každá věta predikátové logiky je logicky platná. Nyní ukážeme, že formální systém predikátové logiky je také úplný, to znamená, že také každá logicky pravdivá formule je větou predikátové logiky. Tento výsledek vyslovíme v obecnější formě pro teorie prvního řádu.

4.12 Věta o úplnosti (Gödel) Nechť T je teorie s jazykem L. Potom platí

(i) je-li A libovolná formule jazyka L, potom

$T \vdash A$, právě když $T \models A$

tedy A je větou T, právě když A je splněna v každém modelu teorie T.

(ii) T je bezesporná teorie, právě když T má nějaký model.

Důkaz. Nejprve ukážeme, že tvrzení (i) je důsledkem tvrzení (ii). Nechť T je teorie, A je formule jazyka teorie T. Podle věty 3.49 je $T \vdash A$, právě když je $T \cup \{\neg A'\}$, kde A' je uzávěr formule A, sporná teorie. Podle (ii) je to ekvivalentní s tvrzením, že $T \cup \{\neg A'\}$ nemá model. Protože A' je uzavřená formule a v každém modelu teorie T (pokud nějaký existuje) musí být pravdivá jedna z formulí A' a $\neg A'$, znamená to, že v každém modelu teorie T je pravdivá formule A'. Podle definice splňování to je právě tehdy, když je v každém modelu teorie T splněna formule A. Tím je (i) dokázáno.

Povšimněme si, že implikace zleva doprava ve tvrzení (i) je znění věty o korektnosti a implikace zprava doleva ve tvrzení (ii) je znění Důsledku 4.9. K důkazu věty o úplnosti stačí, dokážeme-li že každá bezesporná teorie má nějaký model. Metodu důkazu, kterou použijeme, vytvořil L. Henkin.

Nejprve popíšeme konstrukci takzvané kanonické struktury pro teorii T a ukážeme, že kanonická struktura je modelem teorie T, pokud T splňuje určité další předpoklady. V dalších krocích ukážeme, že každou teorii T lze rozšířit do teorie T', která splňuje zmíněné předpoklady, a že omezením kanonické struktury pro T' získáme model teorie T. Důkaz rozdělíme do několika tvrzení.

4.13 Konstrukce kanonické struktury pro T Je-li T bezesporná teorie s jazykem L, máme sestrojit relační strukturu, která je modelem teorie T. To znamená, že máme sestrojit množinu individuí - univerzum takového modelu - a dále zobrazení a relace na tomto univerzu, které realizují funkční a predikátové symboly jazyka L tak, aby výsledná struktura byla modelem teorie T. K dispozici máme jen syntaktický materiál teorie T, jazyk, termy, formule a věty.

Základní myšlenka konstrukce je prostá, universum bude tvořeno z termů, protože ty odpovídají "objektům" teorie, a splňování formulí v konstruované struktuře bude dáno větami teorie. Univerzum struktury vytvoříme z termů bez

proměnných, protože jejich význam je určen jednoznačně bez ohledu na ohodnocení proměnných, funkční symboly na tomto univerzu budeme realizovat určitým kanonickým způsobem a predikáty budou realizovány relacemi podle vět teorie.

Při bližším zkoumání navrženého postupu zjistíme, že jsou zde některé problémy.

(i) Pokud jazyk L neobsahuje žádnou konstantu, nejsou žádné termy bez proměnných.

(ii) Je-li L jazyk s rovností, může se stát, že pro dva různé termy t, s bez proměnných platí $T \vdash s = t$, ale v konstruované struktuře nebude tato formule splněna protože oba termy chápeme jako dvě různa individua.

(iii) Je-li A uzavřená formule, v konstruované struktuře bude pravdivá jedna z formulí A a $\neg A$. Přitom žádná z nich nemusí být větou teorie T.

(iv) Je-li nějaká formule tvaru $(\exists x)B$ větou teorie T, chceme, aby tato formule byla splněna v konstruované struktuře. To podle definice splňování nastane když v dané struktuře najdeme individuum - term bez proměnných t, který existenci "dosvědčí", což by znamenalo, že $B_x[t]$ je také větou teorie T. Teorie T nemusí takový požadavek splňovat.

Na první pohled je zřejmé, že nejjednodušší je problém (ii). Protože rovnost je reflexivní, symetrický a tranzitivní predikát, stačí faktorizovat množinu termů podle rovnosti. V ostatních případech musíme požadovat, aby teorie T měla nějaké další vlastnosti. V případě (iii) je to úplnost a v případě (iv) požadujeme aby T byla takzvaná Henkinova teorie, tím je řešen i problém konstant (i). Nejprve zavedeme dva nové pojmy.

4.14 Úplné teorie Říkáme, že *teorie T s jazykem L je úplná*, jestliže T je bezesporná a pro každou uzavřenou formuli A jazyka L je jedna z formulí A, $\neg A$ dokazatelná v T.

Úplná teorie je bezesporná a pro každou uzavřenou formuli A rozhoduje, která z dvojice formulí A, $\neg A$ je dokazatelná. Z definice splňování plyne, že pro každou realizaci $\mathfrak{M}$ jazyka je množina $Th(\mathfrak{M})$ všech uzavřených formulí, které jsou pravdivé v $\mathfrak{M}$, úplná teorie.

4.15 Henkinovy teorie Říkáme, že *teorie T s jazykem L je Henkinova*, jestliže pro libovolnou uzavřenou formuli $(\exists x)B$ existuje konstanta c, taková, že platí

$$T \vdash (\exists x)B \to B_x[c]$$

4.16 Lemma Je-li T úplná Henkinova teorie, potom T má model.

Důkaz. Nechť T je úplná Henkinova teorie s jazykem L, označme $\mathcal{T}$ množinu všech termů bez proměnných jazyka L. Na množině $\mathcal{T}$ definujeme relaci $\equiv$ tak, že pro libovolné dva termy t_1, t_2 z $\mathcal{T}$ položíme

$t_1 \equiv t_2$, právě když $T \vdash t_1 = t_2$

Relace $\equiv$ je ekvivalence na množině $\mathcal{T}$, protože predikát rovnosti je reflexivní, symetrický a tranzitivní. Pro libovolný term t z $\mathcal{T}$ nechť $[t]$ označuje třídu ekvivalence termu t určenou relací $\equiv$, tedy

$$[t] = \{s | s \in \mathcal{T}, t \equiv s\}$$

Nechť univerzum M vznikne z $\mathcal{T}$ faktorizací podle relace ekvivalence $\equiv$, to znamená, že množina M je tvořena třídami ekvivalence $[t]$, $t \in \mathcal{T}$.

K určení relační struktury $\mathfrak{M}$, která realizuje jazyk L, stačí definovat zobrazení a relace na univerzu M, které realizují funkční a predikátové symboly jazyka L.

Je-li f n-ární funkční symbol a $[t_1], [t_2], \ldots, [t_n] \in M$, položíme

$$f_{\mathfrak{M}}([t_1], [t_2], \ldots, [t_n]) = [f(t_1, t_2, \ldots, t_n)]$$

Je-li p n-ární predikátový symbol různý od rovnosti, pro $[t_1], \ldots, [t_n] \in M$ definujeme

$$([t_1], [t_2], \ldots, [t_n]) \in p_{\mathfrak{M}} \text{ právě když } T \vdash p(t_1, t_2, \ldots, t_n)$$

Je třeba ukázat, že obě definice jsou korektní, že jejich pravé strany závisí jen na třídách ekvivalence $[t_i]$, $1 \leq i \leq n$ a ne na volbě jejich reprezentace termy t_i . Pro každé i, $1 \leq i \leq n$ zvolme libovolně $s_i \in [t_i]$. Potom $T \vdash t_i = s_i$ pro každé i, $1 \leq i \leq n$ a podle vět o rovnosti

$$T \vdash f(t_1, t_2, \ldots, t_n) = f(s_1, s_2, \ldots, s_n)$$
$$T \vdash p(t_1, t_2, \ldots, t_n) \leftrightarrow p(s_1, s_2, \ldots, s_n)$$

odkud dostáváme

$$[f(t_1, t_2, \ldots, t_n)] = [f(s_1, s_2, \ldots, s_n)]$$
$$T \vdash p(t_1, t_2, \ldots, t_n) \quad \text{právě když} \quad T \vdash p(s_1, s_2, \ldots, s_n)$$

Tím je korektnost obou definic dokázána a definice kanonické struktury $\mathfrak{M}$ pro teorii T je úplná. V dalším budeme potřebovat následující tvrzení.

Je-li t term takový, že všechny jeho proměnné jsou mezi proměnnými $x_1, x_2, \ldots, x_n$ a je-li e ohodnocení proměnných v $\mathfrak{M}$, takové, že $e(x_i) = [t_i]$ pro i, $1 \leq i \leq n$ a nějaké termy bez proměnných $t_1, t_2, \ldots, t_n$, potom pro realizaci $t[e]$ platí

$$t[e] = [t_{x_1, x_2, \ldots, x_n}[t_1, t_2, \ldots, t_n]]$$

Speciálně je-li t term bez proměnných, potom

$$t[e] = [t] \tag{1}$$

Dokazujeme indukcí podle složitosti termu t. Je-li t proměnná například x_i, potom

$$\begin{aligned} t[e] &= e(x_i) \\ &= [t_i] \\ &= [t_{x_1, x_2, \ldots, x_n}[t_1, t_2, \ldots, t_n]] \end{aligned}$$

Je-li t tvaru $f(s_1, s_2, \ldots, s_n)$, z indukční hypotézy plyne

$$s_i[e] = [s_i[t_1, t_2, \ldots, t_n]] \text{ pro } i, 1 \leq i \leq n$$

odkud

$$\begin{aligned} t[e] &= f_{\mathfrak{M}}(s_1[e], s_2[e], \ldots, s_n[e]) \\ &= f_{\mathfrak{M}}([s_1[t_1, t_2, \ldots, t_n]], \ldots, [s_n[t_1, t_2, \ldots, t_n]]) \\ &= [f(s_1, s_2, \ldots, s_n)[t_1, t_2, \ldots, t_n]] \\ &= [t_{x_1, x_2, \ldots, x_n}[t_1, t_2, \ldots, t_n]] \end{aligned}$$

Důkaz tohoto tvrzení je obdobou důkazu lemmatu 3.23 (i). Následující tvrzení se dokáže podobně jako tvrzení (ii) téhož lemmatu.

Je-li A formule jejíž volné proměnné jsou mezi proměnnými $x_1, x_2, \ldots, x_n$ a e je ohodnocení proměnných v $\mathfrak{M}$ takové, že $e(x_i) = [t_i]$ pro i, $1 \leq i \leq n$ a termy bez proměnných t_i, potom

$$\mathfrak{M} \models A[e] \quad \text{právě když} \quad \mathfrak{M} \models A_{x_1, x_2, \ldots, x_n}[t_1, t_2, \ldots, t_n] \tag{2}$$

Pro kanonickou strukturu $\mathfrak{M}$ pro teorii T a libovolnou uzavřenou formuli A platí

$$\mathfrak{M} \models A \quad \text{právě když} \quad T \vdash A \tag{3}$$

dokážeme to indukcí podle složitosti formule A. Připomeňme, že podle definice splňování je uzavřená formule pravdivá v nějaké realizaci jazyka, je-li tam pravdivá při alespoň jednom ohodnocení proměnných. V takovém případě je pravdivá při všech ohodnoceních proměnných. Nechť e je libovolné ohodnocení proměnných v $\mathfrak{M}$. Uvažujeme následující případy.

a) Je-li A atomická formule tvaru $p(t_1, t_2, \ldots t_n)$, potom termy t_i pro i, $1 \leq i \leq n$ neobsahují proměnné. Platí

$$\mathfrak{M} \models A \quad \text{právě když} \quad \mathfrak{M} \models A[e]$$

$$\begin{aligned}
&\text{právě když} \quad (t_1[e], t_2[e], \dots t_n[e]) \in p_{\mathfrak{M}} \\
&\text{právě když} \quad ([t_1], [t_2], \dots [t_n]) \in p_{\mathfrak{M}} && (1) \\
&\text{právě když} \quad T \vdash A && (\text{definice } p_{\mathfrak{M}})
\end{aligned}$$

Je-li A tvaru $t_1 = t_2$ důkaz je podobný.

b) Je-li A tvaru $\neg B$, potom

$$\begin{aligned}
\mathfrak{M} \models A \quad &\text{právě když} \quad \mathfrak{M} \not\models B \\
&\text{právě když} \quad T \not\vdash B && (\text{ind. předpoklad}) \\
&\text{právě když} \quad T \vdash \neg B && (\text{úplnost } T) \\
&\text{právě když} \quad T \vdash A
\end{aligned}$$

c) Je-li A tvaru $B \to C$, potom

$$\begin{aligned}
\mathfrak{M} \models A \quad &\text{právě když} \quad \mathfrak{M} \not\models B \text{ nebo } \mathfrak{M} \models C \\
&\text{právě když} \quad T \not\vdash B \text{ nebo } T \vdash C && (\text{ind. předpoklad}) \\
&\text{právě když} \quad T \vdash \neg B \text{ nebo } T \vdash C && (\text{úplnost } T) \\
&\text{právě když} \quad T \vdash A
\end{aligned}$$

Poslední ekvivalenci rozebereme podrobněji. Z výrokové logiky dostáváme

$$\vdash \neg B \to (B \to C) \qquad (\text{v2})$$

$$\vdash C \to (B \to C) \qquad (\text{axiom A1})$$

Je-li formule $\neg B$ nebo formule C větou T, potom $T \vdash B \to C$ odvodíme pravidlem modus ponens. Je-li naopak implikace $B \to C$ větou T, z úplnosti T plyne, že buď B nebo $\neg B$ je také větou T. V prvním případě odvodíme $T \vdash C$ pravidlem modus ponens a druhý případ vyhovuje.

d) Je-li A tvaru $(\forall x)B$, potom

$$\begin{aligned}
\mathfrak{M} \models A \quad &\text{právě když} \quad \mathfrak{M} \models A[e] \\
&\text{právě když} \quad \text{pro libovolný term bez proměnných } t \\
&\qquad \mathfrak{M} \models B[e(x/[t])] \\
&\text{právě když} \quad \text{pro libovolný term bez proměnných } t \\
&\qquad \mathfrak{M} \models B_x[t] && (2) \\
&\text{právě když} \quad \text{pro libovolný term bez proměnných } t \\
&\qquad T \vdash B_x[t] && (\text{indukční předpoklad}) \\
&\text{právě když} \quad T \vdash A
\end{aligned}$$

Poslední ekvivalenci rozebereme podrobněji. Z úplnosti teorie T plyne, že buď A nebo $\neg A$ je větou T. Je-li A větou T, potom podle axiomu specifikace

je také větou formule $B_x[t]$ pro každý term t bez proměnných. Je-li naopak větou T formule $\neg A$, potom užitím prenexní operace dostáváme

$$T \vdash (\exists x)\neg B \tag{4}$$

Protože T je Henkinova teorie a (4) je uzavřená formule, pro nějakou konstantu c dostáváme

$$T \vdash (\exists x)\neg B \to \neg B_x[c]$$

odkud pravidlem modus ponens z (4) plyne

$$T \vdash \neg B_x[c]$$

a z bezespornosti teorie T

$$T \nvdash B_x[c]$$

Ukázali jsme, že formule $(\forall x)B$ je větou T, právě když je pravdivá v kanonické struktuře $\mathfrak{M}$ pro T. Tím je dokončen případ d) a důkaz (3).

Nyní již snadno ukážeme, že kanonická struktura $\mathfrak{M}$ je modelem teorie T. Je-li A libovolný axiom T, nechť A' je uzávěr formule A. Podle věty o uzávěru je A' větou teorie T a podle (3) je to formule pravdivá v $\mathfrak{M}$. Podle definice splňování je také formule A splněna v $\mathfrak{M}$. To znamená že kanonická struktura $\mathfrak{M}$ pro T je modelem teorie T. Tím je lemma dokázána.

Na závěr poznamenejme, že první krok důkazu lemmatu lze provést pro libovolnou teorii T. To znamená, že (3) platí pro libovolnou atomickou formuli bez proměnných.

4.17 Rozšiřování teorií Zatím umíme dokázat větu o úplnosti jen pro teorie, které jsou úplné a Henkinovy. Je-li T bezesporná teorie s jazykem L, pak T nemusí být úplná ani Henkinova. Uvažujeme-li například predikátovou logiku s rovností a jazykem $L = \{0, 1, +, \cdot\}$, je to teorie, která jistě není úplná. Přidáním dalších speciálních axiomů mohou vzniknout *různé* algebraické teorie - *teorie okruhů, teorie oborů integrity, teorie těles* z příkladu 4.4b a další. Je zřejmé, že predikátová logika sama nerozhoduje pro každou uzavřenou formuli A jazyka L zda A nebo $\neg A$ je větou. Nelze se domnívat, že logicky pravdivé formule budou detailně určovat vlastnosti speciálních symbolů, vždyť logicky pravdivé formule byly definovány právě tím, že jejich pravdivost nezáleží na interpretaci speciálních symbolů.

Ukážeme, že každou bezespornou teorii T lze rozšířit do úplné a Henkinovy teorie T'. Z kanonické struktury, která je modelem teorie T', pak získáme model teorie T. Nejprve zavedeme potřebné pojmy.

4.18 Rozšíření jazyka Říkáme, že jazyk L' je rozšířením jazyka L, jestliže L' obsahuje každý speciální symbol (a případně i predikát rovnosti) jazyka L ve stejném významu a se stejnou četností.

To znamená, že každý predikátový symbol jazyka L je predikátovým symbolem jazyka L' a každý funkční symbol jazyka L je také funkčním symbolem jazyka L' v obou případech se stejnou četností.

4.19 Příklad Jazyk L' s rovností a speciálními symboly $0, <, \simeq$, kde 0 je konstanta a $<, \simeq$ jsou binární predikátové symboly, je rozšířením jazyka s rovností $L = \{<\}$ teorie uspořádání.

4.20 Rozšíření teorie (i) Říkáme, že *teorie T' s jazykem L' je rozšířením teorie T s jazykem L*, jestliže jazyk L' je rozšířením jazyka L a libovolná formule A jazyka L, která je větou teorie T, je také větou teorie T'.

(ii) Říkáme, že *teorie T' s jazykem L' je konzervativní rozšíření teorie T s jazykem L*, jestliže T' je rozšířením teorie T a každá formule A jazyka L, která je větou teorie T', je také větou teorie T.

Jinými slovy, T' je konzervativní rozšíření teorie T s jazykem L, je-li T' rozšíření teorie T, a pro libovolnou formuli A jazyka L platí

$$T \vdash A \quad \text{právě když} \quad T' \vdash A \tag{5}$$

4.21 Příklad a) Teorie okruhů, oborů integrity a teorie těles mají stejný jazyk s rovností $L = \{0, 1, +, \cdot\}$ a teorie těles je rozšířením teorie oborů integrity a ta je opět rozšířením teorie okruhů.

Snadno se nahlédne, že teorie T' je rozšířením T, právě když je každý speciální axiom teorie T *větou* teorie T'. Případ teorie těles a teorie oborů integrity ukazuje, že každý speciální axiom teorie T nemusí být axiomem teorie T'.

b) Věta o konstantách ukazuje, že rozšíření nějaké teorie T o nové konstanty je konzervativní.

4.22 Lemma (i) Je-li bezesporná teorie T' rozšířením teorie T, potom T je také bezesporná teorie.

(ii) Je-li T' konzervativní rozšíření teorie T, potom T je bezesporná, právě když T' je bezesporná teorie.

Důkaz. (i) Je-li T' bezesporné rozšíření teorie T, důkaz sporu se přenáší z T do T'. Kdyby T byla sporná teorie, pak nějaká formule A a její negace jsou větami teorie T. Protože T' je rozšíření teorie T, jsou obě formule i větami teorie T' a ta nemůže být bezesporná.

(ii) Tvrzení plyne z (5). Spor se přenáší oběma směry.

4.23 Věta (Henkin) Ke každé teorii T lze sestrojit Henkinovu teorii T_H, která je konzervativním rozšířením teorie T.

Důkaz. Teorii T_H sestrojíme z teorie T přidáním nových konstant a nových axiomů tak, aby každá uzavřená formule tvaru $(\exists x)B$ měla odpovídající konstantu, která existenci "dosvědčí".

Nechť T je teorie s jazykem L, ke každé uzavřené formuli tvaru $(\exists x)A$ přidejme konstantu $c_{(\exists x)A}$ a axiom

$$(\exists x)A \to A_x[c_{(\exists x)A}] \tag{6}$$

Konstantám $c_{(\exists x)A}$ říkame Henkinovy nebo dosvědčující konstanty. Říkáme, že axiom (6) je Henkinův axiom příslušný ke konstantě $c_{(\exists x)A}$. Vytvořili jsme množinu C_1 Henkinových konstant odpovídající všem uzavřeným formulím tvaru $(\exists x)A$ jazyka L. Označme L_1 rozšíření jazyka L, které vznikne přidáním všech Henkinových konstant z množiny C_1 a označme T_1 teorii s jazykem L_1, která vznikne přidáním všech Henkinových axiomů (6) ke všem konstantám z množiny C_1.

Teorie T_1 ještě nemusí být Henkinova, je-li $(\exists x)A$ uzavřená formule jazyka L_1, která obsahuje nějakou konstantu z množiny C_1, v T_1 není odpovídající Henkinův axiom (6). Uvedený postup je třeba iterovat. Konstanty z množiny C_1 nazveme Henkinovy konstanty prvního řádu a k uvedené formuli přidáme Henkinovu konstantu $c_{(\exists x)A}$ druhého řádu a odpovídající axiom (6).

Předpokládejme, že pro nějaké přirozené číslo n jsou již sestrojeny množiny C_i $i \leq n$ Henkinových konstant až do řádu n. Nechť L_n je jazyk, který vznikne z L přidáním všech Henkinových konstant z množin C_i, $i \leq n$. Ke každé uzavřené formuli tvaru $(\exists x)A$, která obsahuje alespoň jednu Henkinovu konstantu řádu n, přidáme příslušnou Henkinovu konstantu. Množinu všech takto sestrojených konstant označíme C_{n+1} a jejím prvkům říkáme Henkinovy konstanty řádu $n+1$. Jazyk, který vznikne z L_n přidáním všech Henkinových konstant z množiny C_{n+1} označíme L_{n+1}.

Sestrojíme-li popsaným způsobem množiny C_n pro pro všechna přirozená čísla n, nechť C je sjednocením všech množin C_n a $L(C)$ je rozšíření jazyka L o všechny Henkinovy konstanty z množiny C. Nechť T_H je teorie s jazykem $L(C)$, která vznikne z teorie T přidáním všech axiomů (6) příslušných k nějaké konstantě z množiny C. Teorie T_H je rozšířením teorie T.

Dokážeme, že T_H je konzervativní rozšíření teorie T. Nechť A je formule jazyka L, která je větou teorie T_H. Nechť $B_1, B_2, \ldots, B_n$ jsou všechny Henkinovy axiomy tvaru (6) použité v důkazu formule A. Potom

$$T, B_1, B_2, \ldots, B_n \vdash A$$

a protože $B_1, B_2, \ldots, B_n$ jsou uzavřené formule, z věty o dedukci dostáváme

$$T \vdash B_1 \to B_2 \to \ldots \to B_n \to A$$

Bez újmy na obecnosti můžeme předpokládat, že axiom B_1 přísluší k Henkinově konstantě, jejíž řád je větší nebo roven řádům konstant, ke kterým přísluší axiomy $B_2, \ldots, B_n$. Nechť B_1 je tvaru $(\exists x)D \to D_x[d]$. Podle předpokladu o řádech Henkinových konstant d není obsažena ve formulích $B_2, \ldots, B_n$ a přirozeně ani ve formuli A. Protože T neobsahuje žádný axiom o konstantě d, použijeme větu o konstantách a odvodíme

$$T \vdash ((\exists x)D \to D_x[w]) \to (B_2 \to \ldots \to B_n \to A)$$

kde w je nová proměnná. Potom pravidlem zavedení $\exists$ dostáváme

$$T \vdash (\exists w)((\exists x)D \to D_x[w]) \to (B_2 \to \ldots \to B_n \to A)$$

a prenexní operací

$$T \vdash ((\exists x)D \to (\exists w)D_x[w]) \to (B_2 \to \ldots \to B_n \to A)$$

Z Věty o variantách plyne

$$\vdash (\exists x)D \to (\exists w)D_x[w]$$

a pomocí pravidla modus ponens odvodíme

$$T \vdash B_2 \to \ldots \to B_n \to A$$

Opakováním tohoto postupu nakonec odvodíme, že A je větou T. Tím je Věta dokázána.

Popíšeme metodu jak získat úplné rozšíření teorie. K tomu potřebujeme jeden z principů maximality z teorie množin, který zde uvedeme bez důkazu. Nejprve uvedeme potřebné pojmy.

Je-li $\mathcal{S}$ nějaká množina a $\mathcal{B}$ je množina nějakých podmnožin množiny $\mathcal{S}$, říkáme, že $\mathcal{B}$ je množina s konečnou vlastností, jestliže pro libovolnou podmnožinu $S \subseteq \mathcal{S}$ platí, že $S \in \mathcal{B}$, právě když každá konečná podmnožina $S' \subseteq S$ je prvkem $\mathcal{B}$. Říkáme, že S je maximální prvek množiny $\mathcal{B}$ vzhledem k inkluzi, jestliže žádná nadmnožina $S' \supseteq S, \quad S \neq S'$ není prvkem $\mathcal{B}$.

4.24 Princip maximality (Teichmüller, Tukey). Každá neprázdná množina podmnožin nějaké množiny $\mathcal{S}$ s konečnou vlastností má maximální prvek vzhledem k inkluzi.

4.25 Věta (Lindenbaum) Každá T bezesporná teorie T, má úplné rozšíření se stejným jazykem.

Důkaz. Nechť T je bezesporná teorie s jazykem L. Nechť $\mathcal{S}$ je množina všech uzavřených formulí jazyka L. Nechť

$$\mathcal{B} = \{\, S \mid S \subseteq \mathcal{S}, \quad T \cup S \text{ je bezesporná} \,\}$$

Množina $\mathcal{B}$ je částečně uspořádaná inkluzí a prázdná množina je jejím prvkem, protože T je bezesporná. Množina $\mathcal{B}$ je tedy neprázdná. Ukážeme, že má konečnou vlastnost.

Nechť S je libovolná podmnožina $\mathcal{S}$. Je-li $S \in \mathcal{B}$, potom $T \cup S$ je bezesporná a totéž platí pro každou konečnou podmnožinu $S' \subseteq S$. Je-li naopak $S \notin \mathcal{B}$, potom $T \cup S$ je sporná tedy pro nějakou formuli A platí

$$T \cup S \vdash (A \,\&\, \neg A)$$

Nechť množinu S' tvoří všechny formule z S, které vystupují v důkazu $A \,\&\, \neg A$. Potom také

$$T \cup S' \vdash (A \,\&\, \neg A)$$

a $T \cup S'$ je také sporná teorie. To znamená, že S' je konečná podmnožina množiny S, která není prvkem $\mathcal{B}$. Množina $\mathcal{B}$ má konečnou vlastnost.

Nechť S_0 je maximální prvek množiny $\mathcal{B}$, položme $T' = T \cup S_0$. Teorie T' má stejný jazyk jako T, ukážeme, že je to úplná teorie. Nechť A je nějaká uzavřená formule. Kdyby A ani $\neg A$ nebyla větou T', potom $\neg A$ není prvkem T' (ani S_0). Protože A není větou T', podle důsledku 3.49 je $T' \cup \{\neg A\}$ bezesporná. To by znamenalo, že S_0 není maximální prvek $\mathcal{B}$. Teorie T' je tedy úplná. Tím je věta dokázána.

4.26 Redukce a expanze struktur Je-li L' rozšíření jazyka L a $\mathfrak{M}'$ je realizace jazyka L', *redukce struktury* $\mathfrak{M}'$ *do jazyka* L, kterou označíme $\mathfrak{M}' \mid L$, vznikne z $\mathfrak{M}'$ vynecháním těch zobrazení a relací, které realizují funkční a predikátové symboly, které nejsou v jazyce L.

Je-li $\mathfrak{M}$ realizace jazyka L a $\mathfrak{M}'$ je realizace jazyka L', říkáme, že $\mathfrak{M}'$ *je expanze struktury* $\mathfrak{M}$ *do jazyka* L', jestliže $\mathfrak{M} = \mathfrak{M}' \mid L$. Obě struktury mají stejné univerzum a $\mathfrak{M}'$ se liší od $\mathfrak{M}$ jen o realizace těch funkčních a predikátových symbolů jazyka L', které nejsou v jazyce L.

4.27 Lemma Nechť teorie T' je rozšíření teorie T, která má jazyk L. Je-li $\mathfrak{M}'$ model teorie T', potom $\mathfrak{M} = \mathfrak{M}' \mid L$ je model teorie T.

Důkaz. Obě struktury mají stejné univerzum, mají tedy stejnou množinu všech ohodnocení proměnných. Snadno se ověří, že pro každé ohodnocení proměnných e a každou formuli jazyka L platí

$$\mathfrak{M} \models A[e] \quad \text{právě když} \quad \mathfrak{M}' \models A[e]$$

tedy také

$$\mathfrak{M} \models A \qquad \text{právě když} \quad \mathfrak{M}' \models A \tag{7}$$

Je-li A axiom teorie T, potom A je větou teorie T' a podle věty o korektnosti je $\mathfrak{M}' \models A$. Tvrzení plyne ze (7).

4.28 Dokončení důkazu věty o úplnosti Je-li T bezesporná teorie, podle Věty 4.23 lze sestrojit Henkinovu teorii T_H, která je konzervativním rozšířením teorie T. Podle tvrzení (ii) lemmatu 4.22 je teorie T_H také bezesporná. Podle

Věty 4.25 existuje úplné rozšíření T' teorie T_H se stejným jazykem. Protože obě teorie se vztahují ke stejné množině formulí, T' je také Henkinova. Teorie T' je tedy úplná Henkinova teorie, která je rozšířením teorie T. Nechť $\mathfrak{M}'$ je model teorie T', potom podle lemmatu 4.27 je $\mathfrak{M} = \mathfrak{M}' \mid L$ model teorie T. Tím je věta o úplnosti dokázána.

4.3 Věta o kompaktnosti

Jednoduchým důsledkem věty o úplnosti je věta o kompaktnosti. Spolu s větou o úplnosti patří k několika větám, které v určitém smyslu charakterizují logiku prvního řádu.

4.29 Věta o kompaktnosti Množina formulí T má model, právě když každá její konečná podmnožina má model.

Důkaz. Podle věty o úplnosti má libovolná teorie S model právě když je bezesporná. Má-li každá konečná podmnožina $T' \subseteq T$ model, potom je každá konečná podmnožina $T' \subseteq T$ bezesporná. To znamená, že také teorie T je bezesporná, protože každý důkaz sporu používá jen konečně mnoho axiomů. Teorie T má tedy model. A naopak, každý model teorie T je modelem všech jejích konečných podmnožin.

4.30 Důsledek Je-li T teorie s jazykem L a A je libovolná formule jazyka L, potom

$T \models A$ právě když $T' \models A$ pro nějakou konečnou podmnožinu $T' \subseteq T$.

Důkaz. Podle Věty o úplnosti 4.12 (i) platí

$$T \models A \quad \text{právě když} \quad T \vdash A$$

přitom důkaz formule A používá jen konečně mnoho axiomů z množiny T.

Na příkladech teorie těles a Peanovy aritmetiky ukážeme dvě použití věty o kompaktnosti.

4.31 Příklady a) Nechť T je teorie těles z Příkladu 4.4 b s jazykem $L = \{0, 1, +, \cdot\}$ s rovností. Je-li x proměnná, budeme termy

$$x, (x + x), (x + (x + x)), \ldots, \underbrace{(x + (x + (x + \ldots (x + x) \ldots)))}_{n \text{ vskyt } x}$$

označovat zkratkami $1 \cdot x,\ 2 \cdot x,\ 3 \cdot x,\ \ldots, n \cdot x$ a budeme jim říkat *přirozené násobky* x.

Připomeňme, že přirozená čísla nemusí být prvky zkoumaného tělesa a přirozený násobek imituje součin jako opakované přičítání. Výraz $p \cdot x$, kde p je nějaké přirozené číslo může zastupovat term značné délky. Pokud pro nějaké nenulové přirozené číslo p v určitém tělese platí formule

$$p \cdot 1 = 0 \tag{7}$$

říkáme, že těleso má konečnou charakteristiku. Nejmenší nenulové číslo p, pro které platí (7), je *charakteristika tělesa*. Pokud pro žádné nenulové p neplatí (7), říkáme, že těleso má charakteristiku nula. Přidáme-li k T formule

$$p \cdot 1 \neq 0 \tag{8}_p$$

pro všechna nenulová přirozená čísla p, dostáváme axiomy teorie těles charakteristiky nula. Označme tuto teorii T'. Je přirozené položit si otázku, zda lze tělesa charakteristiky nula axiomatizovat také konečným počtem axiomů v logice prvního řádu. Negativní odpověď vyplývá z důsledku 4.30.

Předpokládejme, že by nekonečné schema axiomů $(8)_p$ bylo možné nahradit jedinou formulí A jazyka L. To znamená, že A je splněna ve všech tělesech charakteristiky nula a v žádném tělese konečné charakteristiky. Tedy $T' \models A$ a podle důsledku 4.30 existuje konečná podmnožina $T'' \subseteq T'$ taková, že formule A je splněna v každém modelu T''.

Přitom T'' obsahuje jen konečně mnoho axiomů $(8)_p$. Nechť r je přirozené číslo větší než indexy všech axiomů $(8)_p$, které patří do T''. Potom každé těleso konečné charakteristiky větší než r je modelem T'', a proto je v něm splněna formule A. V algebře se ukazuje, že existují tělesa libovolně velkých konečných charakteristik. To znamená, že axiom A necharakterizuje tělesa charakteristiky nula.

b) *Peanova aritmetika prvního řádu* je teorie P, která vznikne z elementární aritmetiky z příkladu 4.4 c přidáním následujícího *schematu axiomů indukce.*

Je-li A formule jazyka elementární aritmetiky a x je proměná, potom formule

$$A_x[0] \to ((\forall x)(A \to A_x[S(x)]) \to (\forall x)A)$$

je axiom indukce.

Snadno se ukáže, že standardní model aritmetiky $\mathfrak{N}$ je také modelem Peanovy aritmetiky P. Je přirozené položit si otázku, zda $\mathfrak{N}$ je (až na izomorfismus) jediným modelem Peanovy aritmetiky. Z Věty o kompaktnosti 4.29 plyne, že existují modely, které nejsou izomorfní se standardním modelem Peanovy aritmetiky. Takové modely nazveme nestandardní.

Pro libovolné přirozené číslo n budeme definovat term jazyka aritmetiky, který označíme $\overline{n}$.

$$\overline{0} = 0$$
$$\overline{1} = S(0)$$
$$\overline{2} = S(S(0))$$
$$\vdots$$
$$\overline{n+1} = S(\overline{n}) = \underbrace{S(S(S \ldots S(0) \ldots))}_{n+1 \text{ vskyt } S}$$
$$\vdots$$

Termy $\overline{n}$, n přirozené nazýváme *numerály*. Je zřejmé, že každé individuum standardního modelu je realizací nějakého numerálu.

Nyní nechť jazyk L_c vznikne z jazyka L Peanovy aritmetiky přidáním nové konstanty c a nechť P_c je rozšíření Peanovy aritmetiky o axiomy

$$c \neq \overline{n}$$

pro všechny numerály $\overline{n}$. Potom každá konečná podmnožina T, $T \subseteq P_c$ má model, který vznikne expanzí standardního modelu $\mathfrak{N}$ tak, že konstantu c realizujeme individuem, které není realizací žádného z konečně mnoha numerálů, o kterých se mluví v T. Podle věty o kompaktnosti existuje model $\mathfrak{M}$ teorie P_c. Podle lemmatu 4.27 je $\mathfrak{M} \mid L$ model Peanovy aritmetiky. Od standardního modelu se liší tím, že obsahuje individuum, které není realizací žádného numerálu. Takový model není izomorfní se standardním modelem $\mathfrak{N}$, je to *nestandardní model Peanovy aritmetiky*. Věta o kompaktnosti zaručuje existenci nestandardních modelů Peanovy aritmetiky, nedává však návod, jak takové modely sestrojit. Konstrukcemi modelů s nejrůznějšími vlastnostmi se zabývá *teorie modelů*, která je samostatným oborem matematické logiky.

4.4 Cvičení

1. Nechť t, t' jsou termy, nechť A' vznikne z formule A nahrazením některých výskytů termu t termem t' (ne však bezprostředně za kvantifikátorem). Nechť seznam $x_1, \ldots, x_n$ obsahuje všechny proměnné vyskytující se ve formuli $t = t'$ a vázané ve fromuli $A \leftrightarrow A'$.

   (a) $\vdash (\forall x_1) \ldots (\forall x_n)\,(t = t') \rightarrow (A \leftrightarrow A')$

   (b) Najděte termy t, t' a formule A, A' elementární aritmetiky, které vyhovují uvedeným podmínkám a přitom formule

   $$(t = t') \rightarrow (A \leftrightarrow A')$$

   není splněna ve standardním modelu aritmetiky.

2. Nechť formule A' vznikne z formule A nahrazením některých výskytů podformule B formulí B'. Nechť seznam $x_1, \ldots, x_n$ obsahuje každou proměnnou, která má volný výskyt v podformuli B (nebo B'), ale vázaný ve formuli A (nebo A').

   (a) Potom platí

   $$\vdash (\forall x_1) \ldots (\forall x_n)\,(B \leftrightarrow B') \rightarrow (A \leftrightarrow A')$$

   (b) Najděte formule A, A', B, B' elementární aritmetiky, které vyhovují podmínkám cvičení tak, aby implikace

   $$(B \leftrightarrow B') \rightarrow (A \leftrightarrow A')$$

   nebyla splněna ve standardním modelu $\mathfrak{N}$.

3. (a) Dokažte tvrzení (iv) věty 2 z §4 druhé kapitoly.

   (b) Najděte formule elementární aritmetiky tvaru

   $$A_x[t] \leftrightarrow (\forall x)\,(x = t \rightarrow A) \quad \text{a} \quad A_x[t] \leftrightarrow (\exists x)\,(x = t \,\&\, A)$$

   které nejsou splněny ve standardním modelu aritmetiky.

4. Nechť jazyk L' je rozšířením jazyka L, nechť $\mathfrak{M}'$ je struktura pro L' a $\mathfrak{M} = \mathfrak{M}'|L$.

   (a) Každý term jazyka L je také termem jazyka L', každá formule jazyka L je formulí jazyka L'.

   (b) Množiny všech ohodnocení proměnných ve strukturách $\mathfrak{M}$ a $\mathfrak{M}'$ jsou si rovny.

(c) Je-li A formule a t term jazyka L a je-li e ohodnocení proměnných ve struktuře $\mathfrak{M}$, potom realizace termu t při ohodnocení e je stejné individuum v $\mathfrak{M}$ i v $\mathfrak{M}'$. Dále platí

$$\mathfrak{M} \models A[e] \quad \text{právě když} \quad \mathfrak{M}' \models A[e]$$

a

$$\mathfrak{M} \models A \quad \text{právě když} \quad \mathfrak{M}' \models A$$

(d) Je-li T množina formulí jazyka L a A formule jazyka L, potom

$$\mathfrak{M} \models T \quad \text{právě když} \quad \mathfrak{M}' \models T$$

a

$$T \models_L A \quad \text{právě když} \quad T \models_{L'} A$$

kde $T \models_L A$ znamená, že formule A je splněna v každé realizaci jazyka L, která je modelem T.

5. Je-li T bezesporná teorie s jazykem, který má spočetně symbolů, potom T lze rozšířit do úplné teorie se stejným jazykem. Dokažte bez pomoci principů maximality (a axiomu výběru).

   [Návod: Ukažte, že množina všech formulí je spočetná. Je-li $\langle A_n; n \text{ přirozené}\rangle$ prostá posloupnost všech uzavřených formulí, indukcí sestrojte posloupnost teorií T_n, kde T_0 je teorie T a T_{n+1} vznikne z T_n přidáním sentence A_n nebo $\neg A_n$ tak, aby T_{n+1} byla bezesporná. T' je sjednocení všech T_n.]

6. Nechť T je množina všech uzavřených formulí jazyka L. Následující tvrzení jsou ekvivalentní:

   (a) T je úplná teorie s jazykem L.

   (b) Množina všech uzavřených formulí jazyka L, které jsou dokazatelné z T je maximální bezesporná množina uzavřených formulí.

   (c) T je bezesporná množina a pro libovolné uzavřené formule A, B jazyka L platí

   $$T \vdash A \vee B \quad \text{právě když} \quad T \vdash A \text{ nebo } T \vdash B.$$

7. Je-li T úplná Henkinova teorie, potom k libovolné uzavřené formuli A jazyka teorie T existuje uzavřená formule A' bez kvantifikátorů taková, že $T \vdash A \leftrightarrow A'$.

   [Návod: Sestrojte A' indukcí podle složitosti formule A, kvantifikátory eliminujte pomocí dosvědčujících konstant.]

8. Nechť T je úplná Henkinova teorie s jazykem L.

   (a) Pokud L je jazyk bez rovnosti, ukažte, že T má model takový, že každé jeho individuum realizuje nějaký term bez proměnných jazyka L a dva různé termy jsou realizovány dvěma různými individui.

   (b) Je-li L jazyk s rovností, ukažte, že T má model takový, že každé individuum je realizací nějaké konstanty jazyka L.

   [Návod:

   (a) Sestrojte kanonickou strukturu pro T, faktorizace množiny termů není nutná.

   (b) Pro libovolný term t bez proměnných a proměnnou x je formule $(\exists x)\,(x = t)$ dokazatelná (v predikátové logice). Použijte (a) a existenci dosvědčující konstanty pro uvedenou formuli.]

9. Nechť L je jazyk s rovností.

   (a) Žádná množina formulí T jazyka L necharakterizuje konečné realizace jazyka L. Jinými slovy: pro žádnou množinu T formulí jazyka L neplatí

   $$\mathfrak{M} \models T \quad \text{právě když univerzum struktury } \mathfrak{M} \text{ je konečná množina.}$$

   (b) Najděte množinu formulí T, která charakterizuje všechny nekonečné struktury pro L.

   [Návod: Předpokládejte, že T je množina formulí s uvedenou vlastností. Nechť jazyk L' vznikne z jazyka L přidáním spočetně mnoha konstant c_n, kde n je přirozené číslo. Nechť S je množina všech formulí tvaru $c_n \neq c_m$ pro $n \neq m$. Nechť T' je množina $T \cup S$, pomocí věty o kompaktnosti dokažte, že T' má nějaký model $\mathfrak{M}'$. Potom $\mathfrak{M} = \mathfrak{M}'|L$ je nekonečný model T.]

10. Nechť L je jazyk s rovností, který má jediný speciální symbol $<$ pro binární predikát. Ukažte, že žádná množina T formulí jazyka L necharakterizuje dobrá uspořádání relací $<$. Jinými slovy: pro žádnou množinu formulí T neplatí

    $$\mathfrak{M} \models T \quad \text{právě když relace } <_{\mathfrak{M}} \text{ je dobré uspořádání univerza } \mathfrak{M}.$$

    [Návod: Předpokládejte, že množina formulí T má uvedenou vlastnost. Nechť L' vznikne z L přidáním spočetně mnoha konstant c_n pro přirozená čísla n. Nechť S je množina všech formulí tvaru $c_{n+1} < c_n$ pro přirozené číslo n. Pomocí věty o kompaktnosti dokažte, že $T \cup S$ má nějaký model $\mathfrak{M}'$. Potom $\mathfrak{M} = \mathfrak{M}'|L$ je model T, ale $<_{\mathfrak{M}}$ není dobré uspořádání.]

Kapitola 5

Teorie prvního řádu

Teorie prvního řádu mají svou historii. Na počátku jsou jejich axiomy formulovány v co nejjednodušším jazyku a s rozvíjením teorie přibývají nové pojmy, konstanty, operace a predikáty. Ty jsou zaváděny pomocí formulí. Cílem této kapitoly je ukázat, že zavádění nových pojmů má pomocný charakter. Rozšíření teorie, které tak vznikne je konzervativní a definované pojmy lze vždy eliminovat.

Nejprve uvedeme výsledek, který charakterizuje rozšíření teorií pomocí modelů.

5.1 Lemma Nechť jazyk L' je rozšířením jazyka L. Nechť T je teorie s jazykem L a T' je teorie s jazykem L'. Potom platí

(i) T' je rozšířením teorie T, právě když pro každý model $\mathfrak{M}'$ teorie T' je $\mathfrak{M}'|L$ modelem teorie T.

(ii) Je-li T' rozšířením teorie T a každý model $\mathfrak{M}$ teorie T lze expandovat do modelu $\mathfrak{M}'$ teorie T', potom T' je konzervativní rozšíření teorie T.

Důkaz. (i) Je-li T' rozšířením teorie T, potom $\mathfrak{M}'|L$ je model teorie T podle lemmatu 4.27.

Naopak, nechť $\mathfrak{M}'$ je libovolný model teorie T'. Ukážeme, že T' je rozšířením teorie T. Nechť formule A je větou teorie T. Protože $\mathfrak{M}'|L$ je model teorie T, platí $\mathfrak{M}'|L \models A$, odkud také $\mathfrak{M}' \models A$. Tedy $T' \models A$ a podle Věty o úplnosti je A také větou teorie T'. To znamená, že T' rozšířením teorie T.

(ii) Nechť T' je rozšířením teorie T a nechť A je formule jazyka L, která je větou teorie T'. Nechť $\mathfrak{M}$ je libovolný model teorie T a nechť $\mathfrak{M}'$ je jeho expanze do modelu teorie T'. Potom $\mathfrak{M}' \models A$ podle Věty o korektnosti 4.6 odkud také $\mathfrak{M} = \mathfrak{M}'|L \models A$. Ukázali jsme, že formule A je splněna v každém modelu teorie T, podle Věty o úplnosti 4.12 (i) je A také větou T. To znamená, že T' je konzervativní rozšířením teorie T.

5.1 Rozšíření teorie o definici predikátu

Chceme-li do teorie uspořádání z Příkladu 4.4 a) zavést relaci neostrého uspořádání $\leq$ rozšíříme jazyk o nový binární predikát $\leq$ a přidáme axiom

$$x \leq y \leftrightarrow (x < y \vee x = y)$$

Chceme-li relaci $\leq$ zavést do elementární aritmetiky z Příkladu 4.4 c), rozšíříme jazyk o nový binární predikát $\leq$ a přidáme axiom

$$x \leq y \leftrightarrow (\exists z)(z + x = y) \tag{1}$$

Toto rozšíření elementární aritmetiky označíme E'. Říkáme, že (1) je definující axiom a pravá strana (1), kterou označíme D, je definující formule predikátu $\leq$. Každou instanci $t \leq s$ formule $x \leq y$ můžeme v E' nahradit formulí $D'_{x,y}[t, s]$, kde D' je vhodná varianta definující formule D. Nový symbol $\leq$ je v E' definován a může být v případě potřeby eliminován.

5.2 Věta o definici predikátového symbolu Nechť T je teorie s jazykem L. Nechť D je formule jazyka L a všechny její volné proměnné jsou mezi proměnnými $x_1, x_2, \ldots, x_n$. Nechť rozšíření L' jazyka L vznikne přidáním nového n-árního predikátového symbolu p a nechť rozšíření T' vznikne z teorie T přidáním axiomu

$$p(x_1, x_2, \ldots, x_n) \leftrightarrow D \tag{2}$$

Potom teorie T' s jazykem L' je konzervativním rozšířením teorie T. Navíc pro libovolnou formuli B' jazyka L' lze sestrojit formuli B jazyka L takovou, že

$$T' \vdash B \leftrightarrow B'$$

Důkaz. Nechť B' je libovolná formule jazyka L' a nechť D' je varianta definující formule D z (2) taková, že žádná proměnná z formule B' není vázaná v D'.

Nechť formule B vznikne z formule B' tak, že nahradíme každou podformuli $p(t_1, t_2, \ldots, t_n)$ formulí $D'_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$. Podle věty o variantách je

$$T' \vdash p(t_1, t_2, \ldots, t_n) \leftrightarrow D'_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$$

a z Věty o ekvivalenci potom

$$T' \vdash B \leftrightarrow B'$$

Nyní ukážeme, že T' je konzervativní rozšíření teorie T. K tomu stačí pro libovolnou formuli B' jazyka L' ukázat, že z $T' \vdash B'$ plyne $T \vdash B$, kde B je

formule sestrojená popsaným způsobem. Je-li B' z jazyka L, potom B' a B jsou shodné formule a z $T' \vdash B$ plyne $T \vdash B$.

Nechť $B'_1, B'_2, \ldots, B'_n$ je důkaz formule B' z T' a nechť pro každé i, $i \leq n$ formule B_i vznikne z B'_i popsaným způsobem. Ukážeme, že každá formule B_i je větou teorie T. Postupujeme indukcí podle délky důkazu. Uvažujeme následující případy.

Je-li B'_i axiom predikátové logiky kromě axiomu rovnosti pro predikát p, potom B_i je axiom stejného druhu, je tedy větou predikátové logiky a také T. Je-li B'_i axiom rovnosti tvaru

$$y_1 = y'_1 \to \ldots \to y_n = y'_n \to p(y_1, \ldots, y_n) \to p(y'_1, \ldots, y'_n)$$

potom B_i je tvaru

$$y_1 = y'_1 \to \ldots \to y_n = y'_n \to D'[y_1, \ldots, y_n] \to D'[y'_1, \ldots, y'_n]$$

a to důsledek Věty o rovnosti. Je-li B'_i speciální axiom teorie T, tedy formule jazyka L, potom B'_i je B_i a to je věta teorie T. Je-li B'_i definující axiom (2), potom B_i je formule $D' \leftrightarrow D$ a to je větou predikátové logiky a tedy také T podle Věty o variantách.

Je-li B'_i odvozena z formulí B'_j, B'_k, $j, k < i$ a B'_k je tvaru $B'_j \to B'_i$, potom B_k je tvaru $B_j \to B_i$ a B_i je také odvozena z formulí B_j a B_k pravidlem modus ponens.

Je-li B'_i odvozena z formule B'_j, $j < i$ pravidlem generalizace, potom B'_i je tvaru $(\forall x)B'_j$ a snadno se nahlédne, že formule B_i je tvaru $(\forall x)B_j$ a je také odvozena pravidlem generalizace. Indukcí podle délky důkazu jsme dokázali, že formule B je větou teorie T. To znamená, že T' je konzervativní rozšíření teorie T. Tím je věta dokázána.

5.2 Rozšíření teorie o funkční symboly

Teorii lze rozšířit o nový funkční symbol dvojím způsobem podle toho s jakou mírou určitosti jsou dány funkční hodnoty. Pokusíme se to přiblížit na příkladu aritmetiky přirozených čísel. V aritmetice lze dokázat, že ke každému přirozenému číslu x existuje prvočíslo p, $p > x$. Řekneme-li "nechť p je prvočíslo větší než x", zavádíme p jako hodnotu závislou na přirozeném čísle x, ale nezáleží nám na tom, které ze všech takových prvočísel bude p. Mluvíme o *zavedení nového funkčního symbolu* p, který pro každé přirozené číslo x označuje nějaké prvočíslo $p(x)$ větší než x. Řekneme-li "nechť p je nejmenší prvočíslo větší než x", hodnotu p jsme definovali jednoznačně. V takovém případě mluvíme o *definici nového funkčního symbolu* p. Oba postupy mají své oprávnění, zavedení funkčního symbolu je jedinou možností v situaci, kdy umíme dokázat, že pro každé x požadované hodnoty

existují, ale neumíme z nich žádnou jednoznačně definovat, definice funkčního symbolu odpovídá situaci, kdy se nám to podaří.

5.3 Věta o zavedení funkčního symbolu Nechť T je teorie s jazykem L, nechť $(\exists y)A$ je formule jazyka L taková, že každá její volná proměnná je některá z proměnných $x_1, x_2, \ldots, x_n$.
Je-li

$$T \vdash (\exists y)A$$

nechť T' je rozšíření teorie T, které vznikne rozšířením jazyka L o nový n-ární funkční symbol f a přidáním axiomu

$$A_y[f(x_1, x_2, \ldots, x_n)]$$

potom T' je konzervativní rozšíření teorie T.

Důkaz. T' je rozšíření teorie T, konzervativnost dokážeme podle Lemmatu 5.1 (ii) tím, že budeme expandovat každý model teorie T do modelu teorie T'. K tomu použijeme Větu o dobrém uspořádání z teorie množin, která je důsledkem axiomu výběru.

Připomeňe, že množina M je dobře uspořádaná relací $<$, jestliže každá neprázdná podmnožina M' množiny M má nejmenší prvek vzhledem uspořádání $<$.

Věta o dobrém uspořádání Na každé množině existuje relace dobrého uspořádání.

Nechť $\mathfrak{M}$ je libovolný model teorie T, nechť $<$ je relace dobrého uspořádání na jeho univerzu M. Podle předpokladu je formule $(\exists y)A$ větou teorie T, to znamená, že pro každou n-tici individuí $m_1, \ldots, m_n$, která je ohodnocením volných proměnnnných této formule existuje individuum m takové, že

$$\mathfrak{M} \models A[e]$$

kde e je ohodnocení proměnných takové, že $e(y) = m$ a $e(x_i) = m_i$ pro $i \leq n$. Množinu všech takových m označme $M(m_1, \ldots, m_n)$ a její nejmenší prvek označme $min(M(m_1, \ldots, m_n))$.

Položíme-li

$$f_{\mathfrak{M}'}(m_1, \ldots, m_n) = min(M(m_1, \ldots, m_n)) \tag{3}$$

potom $f_{\mathfrak{M}'}$ je realizací funkčního symbolu f a přidáním tohoto zobrazení vznikne expanze $\mathfrak{M}'$ modelu $\mathfrak{M}$. Z definice (3) snadno plyne

$$\mathfrak{M}' \models A_y[f(x_1, x_2, \ldots, x_n)]$$

To znamená, že $\mathfrak{M}'$ je model teorie T'. Podle lemmatu 5.1 (ii) je T' konzervativní rozšíření teorie T.

Důkaz věty o zavedení funkčního symbolu je nefinitní, opírá se o modely rozšiřované teorie. Tím se liší od důkazu věty o definici predikátu, který byl syntaktický a finitní. Věta o zavedení funkčního symbolu má také syntaktický finitní důkaz, který je složitější a opírá se o Větu Herbrandovu.

5.4 Skolemova varianta formule Věta 5.3 ukazuje, že pomocí nově zavedených funkčních symbolů je možné eliminovat existenční kvantifikátory. Tuto metodu použil T. Skolem k důkazu tvrzení, že každá teorie má konzervativní rozšíření, jehož speciálními axiomy jsou otevřené formule. Nejprve zavedeme potřebné pojmy.

5.5 Univerzální a existenční formule (i) Říkáme, že *formule* A *je univerzální*, je-li v prenexním tvaru a všechny její kvantifikátory jsou univerzální.

(ii) Říkáme, že *formule* A *je existenční*, je-li v prenexním tvaru a všechny její kvantifikátory jsou existenční.

5.6 Skolemova varianta formule Je-li A uzavřená formule v prenexním tvaru, indukcí podle počtu existenčních kvantifikátorů v prefixu formule A sestrojíme univerzální formuli A_S v jistém rozšíření jazyka. Formuli A_S nazveme *Skolemovou variantou formule* A.

(i) Je-li A univerzální, A_S je formule A.
(ii) Je-li A tvaru

$$(\forall x_1)\dots(\forall x_n)(\exists y)B$$

kde $n \geq 0$. Nechť f je nový n-ární funkční symbol a A^o je formule

$$(\forall x_1)\dots(\forall x_n)B_y[f(x_1,\dots,x_n)]$$

Formule A^o má o jeden existenční kvantifikátor méně než A. Formule A_S je $(A^o)_S$, kterou sestrojíme pomocí (i) a (ii).

Zřejmě platí

$$A^o \vdash A \quad \text{a tedy} \quad \vdash A_S \to A \tag{4}$$

5.7 Ekvivalentní a otevřené teorie (i) Nechť T a S jsou teorie se stejným jazykem. Říkáme, že T a S *jsou ekvivalentní teorie* a píšeme $T \equiv S$, jestliže obě teorie mají stejné věty.

T a S jsou ekvivalentní, právě když je každý speciální axiom teorie T větou teorie S a naopak. Podle Věty o úplnosti jsou dvě teorie ekvivalentní právě když mají stejné modely.

(ii) Říkáme, že T *je otevřená teorie*, jestliže všechny speciální axiomy teorie T jsou otevřené formule.

5.8 Věta (Skolem) K libovolné teorii lze sestrojit otevřenou teorii T', která je konzervativním rozšířením teorie T.

Důkaz. K teorii T sestrojíme několik dalších teorií, z nichž ta poslední bude otevřené konzervativní rozšíření teorie T. Nechť T_1 je teorie se stejným jazykem jako T, taková, že axiomy T_1 jsou právě uzávěry prenexních tvarů formulí z T. Z Věty o uzávěru a Věty o prenexním tvaru je zřejmé, že T a T_1 jsou ekvivalentní teorie.

Nechť T_2 vznikne z T_1 tak, že ke každému speciálnímu axiomu A z T_1 rozšíříme jazyk o nové funkční symboly ze Skolemovy varianty A_S a přidáme formuli A_S jako nový axiom. Potom T_2 je konzervativní rozšíření T_1. Každý důkaz v teorii T_2 může použít jen konečně mnoho nových funkčních symbolů a konečně mnoho přidaných axiomů. Navíc, je-li A axiom teorie T_1, potom přidáním axiomu A^o a nového funkčního symbolu vznikne podle Věty 5.3 konzervativní rozšíření teorie T_1. Opakováním tohoto postupu dokážeme, že přidáním Skolemovy varianty A_S dostaneme konzervativní rozšíření T_1. Přidáním Skolemových variant konečně mnoha axiomů z T_1 dostáváme vždy konzervativní rozšíření teorie T_1. Proto je také T_2 konzervativním rozšířením T_1.

Nechť teorie T_3 vznikne z T_2 vynecháním všech speciálních axiomů teorie T_1. Protože (4) je dokazatelné v predikátové logice, všechny vynechané axiomy teorie T_2 jsou dokazatelné v T_3, to znamená, že teorie T_2 a T_3 jsou ekvivalentní.

Nechť T_4 vznikne z T_3 tím, že každý speciální axiom T_3 nahradíme jeho otevřeným jádrem. Podle Věty o uzávěru jsou teorie T_3 a T_4 ekvivalentní. Celkem dostáváme

$$T \equiv T_1 \quad \text{a} \quad T_2 \equiv T_3 \equiv T_4$$

a T_2 je konzervativním rozšířením T_1. To znamená, že T_4 je konzervativním rozšířením teorie T. Tím je věta dokázána.

Skolemova konstrukce otevřeného konzervativního rozšíření je vhodná pro teorie s malým počtem existenčních kvantifikatorů. Má-li teorie axiomy s větším počtem existenčních kvantifikátorů, popsaným způsobem získáme otevřené konzervativní rozšíření v málo přehledném jazyku, který má mnoho nových funkčních symbolů.

5.9 Věta o definici funkčního symbolu Nechť L je jazyk a $x_1, \ldots, x_n, y$ jsou různé proměnné. Nechť T je teorie s jazykem L a D je formule jazyka L taková, že všechny její volné proměnné jsou mezi $x_1, x_2, \ldots, x_n, y$. Nechť platí

$$T \vdash (\exists y)D \tag{5}$$

$$T \vdash D \to (D_y[t] \to y = t) \tag{6}$$

Nechť L' vznikne z L přidáním nového n-árního funkčního symbolu f a nechť teorie T' vznikne z T přidáním definujícího axiomu

$$y = f(x_1, x_2, \ldots, x_n) \leftrightarrow D \tag{7}$$

Potom T' je konzervativní rozšíření teorie T a k libovolné formuli A' jazyka L' lze sestrojit formuli A v jazyce L, takovou, že

$$T' \vdash A \leftrightarrow A' \tag{8}$$

Říkáme, že (5) je podmínka existence a (6) je podmínka jednoznačnosti pro f.

Důkaz. Nejprve popíšeme způsob, jak k libovolné formuli A' jazyka L' sestrojit formuli A tak, aby platilo (8). Nový funkční symbol se vyskytuje jen v atomických podformulích. Stačí tedy sestrojit formuli A jen pro případ, že A' je atomická formule. Obecný případ tvrzení (8) potom plyne z Věty o ekvivalenci.

Nechť A' je atomická formule jazyka L'. Postupujeme indukcí podle počtu výskytů symbolu f ve formuli A'. Pokud f nemá výskyt ve formuli A' potom A je formule A'. Má-li f výskyt ve formuli A' uvažujeme nejvnitřnější z takových výskytů, tedy term $f(t_1, \ldots, t_n)$, kde termy $t_1, \ldots, t_n$ již neobsahují symbol f. Potom A' je tvaru

$$B'_z[f(t_1, \ldots, t_n)]$$

kde B' má o jeden výskyt symbolu f méně než A'. Můžeme předpokládat, že z je proměnná, která se nevyskytuje ani v A' ani v definující formuli D. Podle indukčního předpokladu umíme již sestrojit formuli B v jazyku L takovou, že

$$T' \vdash B \leftrightarrow B' \tag{8'}$$

a proto můžeme za formuli A položit formuli

$$(\exists z)(D'_{x_1,x_2,\ldots,x_n,y}[t_1, \ldots, t_n, z] \,\&\, B)$$

kde D' je varianta definující formule taková, že žádná proměnná vyskytující se ve formuli A' není vázaná v D'. Potom A je formule jazyka L, ukážeme, že platí (8). Z Věty o variantách a (7) dostáváme

$$T' \vdash z = f(t_1, \ldots, t_n) \leftrightarrow D'_{x_1,x_2,\ldots,x_n,y}[t_1, \ldots, t_n, z]$$

a z Věty o ekvivalenci

$$T' \vdash (\exists z)(z = f(t_1, \ldots, t_n) \,\&\, B) \leftrightarrow A$$

odkud z vět o rovnosti a (8')

$$T' \vdash B'_z[f(t_1, \ldots, t_n)] \leftrightarrow A$$

kde na levé straně ekvivalence je formule A'. Tím je (8) dokázáno.

K důkazu konzervativnosti rozšíření T' užijeme Větu 5.3. Nechť S je teorie s jazykem L', která vznikne z T přidáním axiomu

$$D_y[f(x_1, \ldots, x_n)] \tag{9}$$

Z předpokladu (5) a Věty 5.3 plyne, že S je konzervativní rozšíření teorie T. Ukážeme, že T' a S jsou ekvivalentní teorie. K tomu stačí ukázat, že (7) je větou S a (9) je větou T'.

Platí

$$T' \vdash f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \leftrightarrow D_y[f(x_1, \ldots, x_n)]$$

protože je to instance axiomu (7), tedy také

$$T' \vdash f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \rightarrow D_y[f(x_1, \ldots, x_n)]$$

Přitom levá strana implikace je instancí axiomu identity, pravidlem modus ponens dostaneme

$$T' \vdash D_y[f(x_1, \ldots, x_n)]$$

Zbývá dokázat, že axiom (7) je větou teorie S. Vyjdeme z následující věty o rovnosti

$$\vdash_{L'} y = f(x_1, \ldots, x_n) \rightarrow (D \leftrightarrow D_y[f(x_1, \ldots, x_n)])$$

a prostředky výrokové logiky dostaneme

$$\vdash_{L'} D_y[f(x_1, \ldots, x_n)] \rightarrow (y = f(x_1, \ldots, x_n) \rightarrow D)$$

odkud z (9) pravidlem modus ponens odvodíme

$$S \vdash y = f(x_1, \ldots, x_n) \rightarrow D$$

Obrácenou implikaci odvodíme z předpokladu (6). Záměnou prvních dvou členů implikace odvodíme

$$S \vdash D_y[f(x_1, \ldots, x_n)] \rightarrow (D \rightarrow y = f(x_1, \ldots, x_n))$$

protože S je rozšíření teorie T. Pravidlem modus ponens z (9) pak odvodíme

$$S \vdash D \rightarrow y = f(x_1, \ldots, x_n)$$

Ukázali jsme, že definující axiom (7) teorie T je větou teorie S. Teorie S a T' jsou ekvivalentní. T' je konzervativní rozšíření T, protože podle Věty 5.3 je S konzervativní rozšíření T. Tím je věta dokázána.

5.10 Důležitý je speciální případ definice funkčního symbolu, kdy definující formule D je tvaru $y = t$, kde t je term, který neobsahuje jiné proměnné než $x_1, x_2, \ldots, x_n$. V takovém případě vždy platí podmínky existence a jednoznačnosti a jsou dokazatelné jen v predikátové logice. Tak

$$\vdash D_y[t] \rightarrow (\exists y)D$$

je větou predikátové logiky a na levé straně implikace je instance $t = t$ axiomu identity. Podmínka existence odtud plyne pravidlem modus ponens. Podmínka jednoznačnosti

$$\vdash y = t \rightarrow t' = t \rightarrow y = t'$$

je důsledkem symetrie a tranzitivnosti rovnosti.

Přirozené násobky a numerály z Příkladů 4.31 a) b) byly zavedeny právě popsaným způsobem, nemusíme je tedy chápat jen jako zkratky, ale jako nově definované funkční symboly a konstanty.

5.11 Rozšíření teorie o definice Říkáme, že *teorie* T' *je rozšířením teorie* T *o definice* jestliže T' vznikne z T konečným počtem rozšíření o definice predikátů nebo funkcí.

Podle Věty 5.2 a Věty 5.9 je T' konzervativní rozšíření teorie T a pro každou formuli A' jazyka teorie T' existuje formule A bez definovaných symbolů taková, že $T' \vdash A \leftrightarrow A'$.

Tato definice odpovídá běžnému postupu při budování nějaké teorie. Jednoduchý jazyk původní axiomatiky se rozšiřuje o nově definované symboly pro funkce a predikáty, které slouží k přehlednému zápisu termů a formulí. Uvedené výsledky ukazují, že žádné nové věty v původním jazyce nelze z definic odvodit a že definované symboly mohou být v případě potřeby eliminovány.

5.3 Cvičení

1. (Eliminace funkčních symbolů). Je-li L jazyk prvního řádu, nechť L^r je jazyk, který nemá žádný funkční symbol, obsahuje všechny predikátové symboly jazyka L a ke každému n-árnímu funkčnímu symbolu f jazyka L nechť L^r obsahuje $(n+1)$-ární predikátový symbol p^f. *Jazyk L^r budeme nazývat relační verzí jazyka L, p^f nazýváme predikátový symbol sdružený s f.*
Ke každému predikátovému symbolu p^f přiřadíme dva axiomy, které naznačují, že p^f je predikátový symbol, který zastupuje funkci:
Je-li f n-ární funkční symbol a jsou-li $x_1, \ldots, x_n$, y, y' navzájem různé symboly pro proměnné, k predikátu p^f přiřadíme následující axiomy

$$(\exists y)\, p^f(x_1, \ldots, x_n, y)$$

$$p^f(x_1, \ldots, x_n, y) \to (p^f(x_1, \ldots, x_n, y') \to y = y')$$

První z nich zaručuje existenci a druhý jednoznačnost individua, které zastupuje $f(x_1, \ldots, x_n)$. Nechť $P(L^r)$ označuje množinu všech axiomů přiřazených všem sdruženým predikátovým symbolům jazyka L^r.
Je-li $\mathfrak{M}$ struktura pro L, nechť $\mathfrak{M}^r$ je struktura pro jazyk L^r, která vznikne nahrazením každého zobrazení f, které realizuje funkční symbol f, relací p^f, která je grafem zobrazení f: To znamená, že p^f je relace, která sestává ze všech uspořádaných $(n+1)$-tic tvaru $(m_1, \ldots, m_n, m)$, kde $m_1, \ldots, m_n, m$ jsou individua taková, že $f(m_1, \ldots, m_n) = m$. Říkáme, že *struktura $\mathfrak{M}^r$ je relační verzí struktury $\mathfrak{M}$*.
Popíšeme způsob, jak eliminovat funkční symboly jazyka L:
K libovolné formuli A jazyka L lze indukcí podle složitosti sestrojit formuli A^r následujícím způsobem:
Je-li A atomická formule tvaru $t_1 = t_2$ a termy t_1, t_2 neobsahují žádný funkční symbol (tedy na obou stranách rovnosti je proměnná), potom A^r je formule A. Je-li na pravé straně proměnná y a t_1 obsahuje funkční symboly, postupujeme podle složitosti termu t_1: je-li t_1 tvaru $f(s_1, \ldots, s_n)$ pro nějaký n-ární funkční symbol f a termy $s_1, \ldots, s_n$, nechť $x_1, \ldots, x_n$ jsou proměnné, které se nevyskytují ve formuli A, formule A^r je tvaru

$$(\exists x_1) \ldots (\exists x_n)\, ((s_1 = x_1)^r \;\&\; \ldots \;\&\; (s_n = x_n)^r \;\&\; p^f(x_1, \ldots, x_n))$$

V případě, že oba termy t_1, t_2 obsahují funkční symboly, zvolme proměnnou x, která se nevyskytuje ve formuli A a formuli A^r píšeme ve tvaru

$$(\exists x)\, ((t_1 = x)^r \;\&\; (t_2 = x)^r)$$

Je-li A atomická formule tvaru $p(t_1, \ldots, t_n)$, kde p je n-ární predikátový symbol různý od rovnosti a $t_1, \ldots, t_n$ jsou termy, zvolíme proměnné

$x_1, \ldots, x_n$, které se nevyskytují ve formuli A a A^r píšeme ve tvaru

$$(\exists x_1) \ldots (\exists x_n)\,((t_1 = x_1)^r \;\&\; \ldots \;\&\; (t_n = x_n)^r \;\&\; p(x_1, \ldots, x_n))$$

Jádrem problému byla eliminace funkčních symbolů z atomických formulí, ostatní případy jsou jednoduché:
Je-li A tvaru $\neg B$, potom A^r je formule $\neg B^r$. Je-li A tvaru $B \,\square\, C$, kde $\square$ zastupuje symbol $\rightarrow$, $\&$, $\vee$ nebo $\leftrightarrow$, potom A^r je formule $B^r \,\square\, C^r$. Je-li A tvaru $(Qx)\,B$, kde Q zastupuje existenční nebo univerzální kvantifikátor, potom A^r je formule $(Qx)\,B^r$.
Nechť L^r je relační verze jazyka L, nechť A je formule jazyka L a $\mathfrak{M}$ je realizace jazyka L. Platí:

(a) $\mathfrak{M}^r \models P(L^r)$

(b) Pokud A neobsahuje funkční symboly, formule A^r je shodná s A.

(c) Pro libovolné ohodnocení proměnných e ve struktuře $\mathfrak{M}$

$$\mathfrak{M} \models A[e] \quad \text{právě když} \quad \mathfrak{M}^r \models A^r[e]$$

(d) K libovolné formuli B jazyka L^r lze sestrojit formuli B^f jazyka L tak, že při každém ohodnocení proměnných e v $\mathfrak{M}$ platí

$$\mathfrak{M} \models B^f[e] \quad \text{právě když} \quad \mathfrak{M}^r \models B[e]$$

(e) Je-li $\mathfrak{N}$ realizace jazyka L^r, která je modelem $P(L^r)$, potom existuje realizace $\mathfrak{M}$ jazyka L taková, že $\mathfrak{N}$ je shodná s $\mathfrak{M}^r$.

(f) Je-li T teorie s jazykem L a T^r je množina všech formulí B^r pro všechna B z T, potom

$$T \vdash A \quad \text{právě když} \quad T^r \cup P(L^r) \vdash A$$

2. Nechť T je teorie s jazykem L a T' je teorie s jazykem L'.

(a) T' je rozšířením teorie T, právě když L' je rozšířením L a pro každý model $\mathfrak{M}'$ teorie T' je $\mathfrak{M}|L$ model teorie T.

(b) Je-li T' rozšíření teorie T a je-li možné každý model teorie T rozšířit do modelu $\mathfrak{M}'$ teorie T', potom T' je konzervativní rozšíření teorie T.

(c) Připomeňme, že teorie T a T' jsou ekvivalentní, pokud T' je rozšířením T a naopak.
Teorie T, T' jsou ekvivalentní, právě když T' je konzervativní rozšíření teorie T a naopak.
Teorie T, T' jsou ekvivalentní, právě když mají stejné modely.

3. Říkáme, že *teorie* T, T' *jsou slabě ekvivalentní*, jestliže nějaké rozšíření teorie T o definice je ekvivalentní nějakému rozšíření teorie T' o definice.

   (a) K libovolné teorii T existuje slabě ekvivalentní teorie T', která nemá žádné funkční symboly.

   (b) Je-li T otevřená teorie, potom teorie T' z bodu (a) má za axiomy jen existenční formule.

   [Návod:

   (a) Použijte výsledků cvičení 1.

   (b) Použijte (a) a větu o prenexním tvaru formulí.]

4. (a) Užijte výsledku cvičení 2 (b) k důkazu tvrzení, že rozšíření teorie zavedením funkčního symbolu je konzervativní.

   (b) Pomocí (a) a lemmatu 5 z §1 podejte nový důkaz Herbrandovy věty.

5. Je-li A otevřená formule bez rovnosti, potom platí

$$\vdash A \quad \text{právě když} \quad A \text{ je tautologie}$$

   [Návod: Užijte Herbrandovu větu.]

6. Je-li T otevřená teorie a A formule jejího jazyka, která je v prenexním tvaru, potom $T \vdash A$, právě když nějaká disjunkce instancí otevřeného jádra formule A je tautologickým důsledkem instancí axiomů rovnosti a axiomů teorie T.

7. Je-li A větou teorie T, pak formule A má důkaz, který obsahuje jen ty speciální symboly jazyka, které se vyskytují ve formuli A a v axiomech teorie T.

Literatura

[1] Bohuslav Balcar, Petr Štěpánek, *Teorie množin*, ACADEMIA, Praha 1986, 2001

[2] Petr Štěpánek, *Matematická logika*, skripta, SPN Praha 1982

[3] Petr Štěpánek, *Predikátová logika*, učební text na stránkách katedry teoretické informatiky a matematické logiky

[4] Petr Štěpánek, *Meze formální metody* učební text na stránkách katedry teoretické informatiky a matematické logiky