Obsah

1. Úvod

Intuitivní, neformální, živé myšlení většiny lidí v naprosté většině případů dodržuje zákony logiky, aniž by lidé tyto zákony nutně znali a jejich používání si explicitně uvědomovali. Podobně lidé dokáží gramaticky správně se vyjadřovat ve svém mateřském jazyce, aniž by nutně znali a uměli formulovat gramatická pravidla, jimiž se používání jazyka řídí. Je však proto znalost logiky nebo gramatiky zbytečná? Nikoliv, a to přinejmenším z těchto důvodů:

1. Intuitivní, podvědomá znalost selhává ve složitějších nebo neobvyklých případech. To se stalo např. v matematice na přelomu 19. a 20. století. V teorii množin, která se měla stát exaktním základem celé matematiky, se objevily logické spory (paradoxy, antinomie), se kterými si intuitivní logika nevěděla rady. Řada podobných logických paradoxů byla formulována již ve starém Řecku. To vedlo k požadavku formálně definovat samotný proces deduktivního myšlení tak, aby jeho korektnost v konkrétních případech mohla být dobře ověřována.

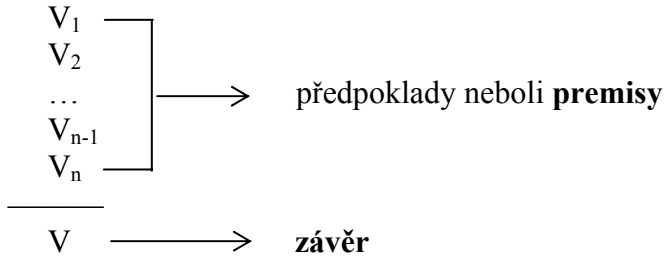
2. Má-li být proces deduktivního myšlení (dokazování a odvozování) přenesen na nevědomý stroj, jak se o to snaží metody umělé inteligence, musí být tento proces nutně formalizován. Stroj (počítač) nemůže být vybaven živým intuitivním myšlením. Toto myšlení lze na počítači nanejvýš simulovat. Podobně také komunikace člověka s počítačem může probíhat pouze na základě formálního jazyka s přesně definovanou formální gramatikou.

Tento text se zabývá základy matematické (formální, symbolické) logiky a jejím využitím ve formálních systémech. Prvá část je věnována výrokové logice (logice 0-tého řádu), ve které primitivní formule (výrokové symboly) nemají žádnou vnitřní stavbu a jediným jejich atributem je pravdivostní hodnota. Druhá část je věnována predikátové logice 1. řádu, která pracuje s primitivními formulemi (predikáty) vypovídajícími o vlastnostech a vztazích mezi předměty jistého univerza diskursu (individui). Logiky 2. řádu (uvažující vlastnosti vlastností, vlastnosti vztahů, vztahy mezi vlastnostmi a vztahy mezi vztahy) a vyšších řádů se v matematice používají méně často a není zde o nich pojednáváno. Predikátová logika 1. řádu postačuje v běžných případech k formalizaci většiny matematických i jiných teorií.

Dříve však, než přistoupíme k vlastnímu výkladu, pokusme se odpovědět na následující otázky:
O čem je logika? Čím se tato vědecká disciplína zabývá? Kde všude nám může logika pomoci?

Logika nám *může* pomoci všude tam, kde vstupuje do hry *jazyková komunikace,* ovšem pouze tehdy, pokud se o výsledku sporu či diskuse apod. rozhoduje silou *argumentu* a ne argumentem síly. Tato charakteristika nám však zatím příliš nepomohla k tomu, abychom odpověděli na zbylé otázky. Odpovíme tedy jinak. Velice pregnantně řečeno:
Logika je (především) **věda o správném usuzování, o umění správné argumentace.**
Ovšem ani tato odpověď nám příliš nepomůže, pokud nevíme, co je to *úsudek,* a co je to *správný (korektní, platný) logický úsudek,* neboli *argument.*

Obecně můžeme **úsudek** charakterizovat následujícím schématem:
Na základě pravdivosti výroků (soudů, tvrzení) V_1, …, V_n *soudím*, že je pravdivý rovněž výrok V.
Zapisujeme schématicky: V_1, …, V_n / V nebo častěji:



V praxi používáme různé druhy takovýchto úsudků, ovšem ne všemi se zabývá logika. Např. se obecně nezabývá tzv. **pravděpodobnostními** úsudky, např.:

Slunce doposud vyšlo každý den.
Tedy ----------
Slunce (pravděpodobně) vyjde i zítra.

Podobně se nezabývá úsudky **generalizací**:

Všechny labutě, které jsme dosud viděli, jsou bílé.
Tedy ----------
Všechny labutě jsou bílé.

Takovéto metody odvozování závěru (případně metody zobecnění – **indukce,** vysvětlení – **abdukce,** a jiné) jsou předmětem jiných disciplín, např. **Umělé inteligence,** nebo také tzv. **nemonotónní logiky,** která se zabývá metodami nemonotónního usuzování**.** V těchto případech je závěr spíše jakási *hypotéza,* a její pravdivost není zaručena pravdivostí premis, neboť z nich logicky nevyplývá.

My se zde budeme zabývat pouze tzv. **deduktivními úsudky** a definujeme:

Definice 1.1. (**logické vyplývání**):

Úsudek P_1, …, P_n / Z je deduktivně ***správný (platný),*** značíme $\mathbf{P_1, \ldots, P_n \models Z}$, jestliže závěr Z ***logicky vyplývá*** z předpokladů P_1, …, P_n, tj. za všech okolností takových, že jsou pravdivé všechny předpoklady P_1, …, P_n, je (za těchto okolností) pravdivý i závěr Z.

Tedy jinými slovy: Za žádných okolností, nikdy se nemůže stát, aby byly všechny předpoklady P_1, … , P_n pravdivé a zároveň závěr Z byl nepravdivý. Závěr Z je pravdivý za všech okolností takových, za kterých jsou pravdivé všechny předpoklady.

Deduktivní usuzování v praktickém životě všichni více či méně používáme, tedy usuzujeme logicky, aniž bychom si uvědomovali, že přitom používáme logiku. Tak např., jestliže víme, že všechny muchomůrky zelené jsou prudce jedovaté a zjistíme (např. za pomoci atlasu hub), že houba, kterou jsme nalezli, je muchomůrka zelená, pak jistě nebudeme tuto houbu ochutnávat a spolehneme se na logiku, neboť ta nám zaručuje, že houba, kterou jsme našli, je prudce jedovatá.

Příklady (jednoduchých, správných deduktivních úsudků).

1) Všechny kovy se teplem roztahují.
   Měď je kov.

   Měď se teplem roztahuje.

2) V seznamu novodobých římských císařů není žádná žena.
   Marie Terezie byla žena.

   Není pravda, že Marie Terezie byla římská císařovna.

3) B. Bolzano zavedl jako první pojem množiny do matematiky.
   B. Bolzano se narodil v Praze.

   Jako první zavedl pojem množiny do matematiky rodák z Prahy.

4) Je doma nebo odešel do kavárny.
   Je-li doma, pak nás očekává.

   Jestliže nás neočekává, pak odešel do kavárny.

5) Je-li tento kurs dobrý, pak je užitečný.
   Buď je přednášející shovívavý, nebo je tento kurs neužitečný.
   Ale přednášející není shovívavý.

   Tento kurs je špatný.

6) Všechny muchomůrky zelené jsou prudce jedovaté.
   Tato tužka je muchomůrka zelená.

   Tato tužka je prudce jedovatá.

7) Všichni muži mají rádi fotbal a pivo.
   Někteří milovníci piva nemají rádi fotbal.
   Xaver má rád pouze milovníky fotbalu a piva.

   Některé ženy nemá Xaver rád.

Správnost úsudku ověřujeme *bez empirického zkoumání* "stavu světa", tedy pouze tzv. *analytickými* metodami, neboť správnost úsudku je dána pouze *logickou strukturou* premis a závěru. Některé úsudky jsou natolik jednoduché a zřejmé, že se zdá, jako bychom žádnou logiku ani nepotřebovali. Ovšem ne vždy tomu tak je. Např. již úsudek ad 5) se nemusí jevit na první pohled zřejmý, i když je poměrně jednoduchý, ověřitelný na základě nejjednoduššího systému výrokové logiky. Rovněž jednoduchý naprosto správný úsudek ad 6) může některé čtenáře překvapit. V praxi (např. v oblasti práva, medicíny, nebo v informatice) se setkáváme s daleko složitějšími úsudky, potřebujeme řešit úlohy typu "co vyplývá z daných předpokladů?", apod., a pak již často nevystačíme s pouhou intuicí, potřebujeme se opřít o znalost logiky.

Logika tedy rovněž zkoumá *skladbu – konstrukci* jednotlivých složených výrazů (soudů) z jejich podvýrazů. Jednou z disciplín logiky je proto rovněž tzv. **logická analýza jazyka,** která spočívá v nalezení příslušné logické *konstrukce* vyjádřené daným výrazem. Ovšem ne všechny deduktivně správné úsudky můžeme ověřit pomocí daného logického systému. Proto hovoříme o *expresivní síle* logického systému, která je dána tím, do jaké míry podrobnosti můžeme analyzovat jednotlivé výrazy. Ideální logický systém by nám měl umožnit analyzovat premisy do takové hloubky, abychom mohli odvodit všechny závěry, které z těchto premis logicky vyplývají (provést všechny adekvátní *inference*) a ověřit všechny správné úsudky. Při nedostatečně jemné a přesné (případně nesprávné) analýze premis pak můžeme dojít k různým paradoxním závěrům (např. známé jsou *paradox analýzy, paradox lháře* a *paradox vševědoucnosti*).

Uvedeme nyní příklady logických systémů podle jejich expresivní síly.

Výroková logika (VL) umožňuje analyzovat pouze do úrovně elementárních výroků, jejichž strukturu již dále nezkoumá.

Predikátová logika 1. řádu (PL^1) umožňuje navíc analyzovat elementární výroky do úrovně vlastností jednotlivých objektů zájmu (tzv. individuí – prvků univerza diskursu) a jejich vztahů.

Predikátové logiky vyšších řádů (PL^n) umožňují navíc analyzovat vlastnosti vlastností, vlastnosti funkcí, atd.

Jedním z nejexpresivnějších logických systémů je tzv. **Transparentní intensionální logika (TIL)**, která pracuje s objekty libovolného řádu, umožňuje rozlišovat tzv. intenze a extenze, přesně explikuje pojem logické konstrukce, definuje, co je to pojem, pojmová analýza, atd. TIL je nyní stále populárnějším logickým systémem u nás i ve světě, a je využívána nejen v oblasti logické analýzy jazyka, ale také např. v oblasti *konceptuálního modelování.* TIL je předmětem samostatného kursu *Principy logické analýzy jazyka* na této fakultě, který vřele doporučujeme.

Z našich příkladů můžeme ověřit na základě výrokové logiky pouze úsudky 4) a 5). Pro analýzu všech ostatních příkladů potřebujeme alespoň predikátovou logiku 1. řádu.

Vlastnosti deduktivních úsudků

Uvědomme si některé důležité vlastnosti deduktivních úsudků. Především, ověříme-li (dokážeme-li) správnost (platnost) úsudku, *nedokážeme tím pravdivost závěru*! Závěr je pravdivý pouze *za předpokladu* pravdivosti premis. Tedy:

1) **Platný úsudek může mít nepravdivý závěr**.
   (V tom případě je ovšem alespoň jedna z premis nepravdivá.) Toto je evidentně případ úsudku ad 6) (ovšem je to logicky platný úsudek!). Ovšem rovněž např. v případě ad 4) správnost úsudku nedokazuje, že dotyčný je v kavárně, jestliže nás neočekává, klidně mohl jít třeba do kina. V tom případě by ovšem zřejmě nebyla pravdivá první premisa.
   Pozn.: V anglické literatuře se někdy rozlišuje *valid argument* (platný úsudek – dle naší definice) a *sound argument* (řádný argument – platný úsudek a premisy pravdivé, tedy i závěr pravdivý). Překlad možná není výstižný, avšak toto rozlišení zachycuje případ, kdy jsou premisy (a tedy i závěr) *pravdivé.*

To ovšem neznamená, že platný úsudek, jehož závěr není pravdivý, by byl ”bezcenný”. Vždyť takovýto způsob argumentace běžně používáme, chceme-li demonstrovat, že někdo neříká pravdu. Představme si dialog:

Vy tedy tvrdíte, že $X_1,\ldots,X_n$. Avšak z Vašich tvrzení plyne, že A. Z A dále plyne, že B, atd., až dostaneme závěr Z, který je evidentně nepravdivý. Tedy Vy tvrdíte Z, což není pravda. Proto alespoň jedno z Vašich původních tvrzení X_i není pravdivé.

2) **Monotónnost.** Jestliže $P_1, \ldots, P_n \models Z$, pak $P_1, \ldots, P_n, P_{n+1} \models Z$, pro libovolnou další premisu P_{n+1}.

Pozn.: Tuto vlastnost nemají jiné úsudky, které nejsou deduktivní, např. úsudky generalizací, kdy závěr nevyplývá z předpokladů. Jestliže např. na základě pozorování 10000 bílých labutí usoudíme (generalizujeme), že všechny labutě jsou bílé, a pak přijedeme do Austrálie a spatříme černou labuť (tedy přidáme premisu že Australská labuť je černá), náš závěr je evidentně nepravdivý, i když premisy jsou stále pravdivé. Tedy úsudky generalizací nejsou deduktivní a jsou nemonotónní. Tímto problémem se pak zabývají metody *umělé inteligence* (využívající tzv. *nemonotónní usuzování*) a provádějící tzv. revizi hypotéz (”belief revision”).

3) **Tranzitivita.**
Jestliže $P_1, \ldots, P_n \models Z$ a $Q_1, \ldots, Q_m, Z \models Z'$, pak $P_1, \ldots, P_n, Q_1, \ldots, Q_m \models Z'$.

4) **Reflexivita.** Je-li B rovna jedné z premis $P_1, \ldots, P_n$, pak $P_1, \ldots, P_n \models B$.

Na závěr zavedeme ještě dva důležité pojmy a jejich značení, a to pojem *analytické pravdivosti,* a pojem *kontradiktorické (sporné)* množiny výroků.

Definice 1.2. (analytická pravdivost, kontradikce)
Výrok V je ***analyticky pravdivý***, značíme $\models V$, je-li pravdivý za všech okolností, vždy. (Množina předpokladů je prázdná, V nemůže být nepravdivý.)
Množina $\{P_1, \ldots, P_n\}$ výroků je ***sporná (kontradiktorická, nesplnitelná),*** jestliže nemůže nikdy za žádných okolností nastat případ, že by byly všechny $P_1, \ldots, P_n$ pravdivé, značíme $P_1, \ldots, P_n \models$. (Tedy z této množiny logicky vyplývá jakýkoli výrok, i nepravdivý, proto musí být vždy alespoň jeden P_i nepravdivý.)

Nyní můžeme formulovat ještě jednu důležitou vlastnost deduktivních úsudků:

5) **Ze sporné** množiny předpokladů vyplývá **jakýkoli závěr.**

Příklady:

$\models 1+1=2$
$\models$ V Praze prší nebo neprší.

Pozn.: Všechny pravdivé matematické výroky jsou analyticky pravdivé. ”Běžné” výroky přirozeného jazyka nejsou analyticky pravdivé (jsou empirické, o ”stavu světa”, mohou být někdy pravdivé, jindy ne).

P_1: ”Jestliže A, pak B”. P_2: ”A a ne B”. $P_1, P_2 \models$ (kde A, B jsou libovolné výroky).
Nyní uvedeme příklad, který ilustruje vlastnost 5) – ze sporné množiny předpokladů vyplývá cokoliv.

Na schůzi výboru byla projednávána žádost pana X o zařazení do vyšší platové stupnice. Pan X si přál, aby ji mzdová komise doporučila. Ale výbor právě odstupoval a již předtím rozhodl, že doporučí pana X jako nového člena mzdové komise budoucího výboru. Takže by pak pan X byl členem komise, která bude posuzovat jeho vlastní žádost. Rozvinula se diskuse a bylo řečeno:

1. X přešel na kvalifikovanější práci.
2. X dobře rozumí mzdovým otázkám.
3. Jestliže X přešel na kvalifikovanější práci, pak je správné, aby jeho žádost byla projednána.
4. Jestliže je správné, aby jeho žádost byla v komisi projednána, pak by neměl být členem komise.
5. Rozumí-li výtečně mzdovým otázkám, měl by být členem komise.

Předseda nakonec řekl: "Všechny přednesené příspěvky jsou pravdivé. Teď jde o to, co z toho vyplývá." Po chvíli ticha prohlásil mladý zapisovatel (který náhodou studoval logiku na VŠB): "Z toho vyplývá, že můj pes právě hraje doma na piano."

Vyplývání je základním (veledůležitým) pojmem v logice, ale rovněž také v matematice. Matematikové formulují a **dokazují** tvrzení. Výsledkem jejich práce je tedy zpravidla (ne-li vždy) nalezení nějakého důkazu. Avšak důkazy a jejich analýza je to, co zajímá logiky, důkaz je rovněž jedním z nejdůležitějších logických pojmů. Co je to důkaz? Obecně řečeno, **důkaz tvrzení A z předpokladů $P_1,\ldots,P_n$** je posloupnost tvrzení $B_1,\ldots,B_m$ taková, že:

- $B_m = A$
- pro každé $i \leq m$ platí, že B_i je buď
  - jeden z předpokladů P_j nebo
  - B_i vznikne z předchozích $B_1,\ldots,B_{i-1}$ uplatněním nějakého **odvozovacího pravidla.**

Přitom je samozřejmě žádoucí, aby odvozovací pravidla byla volena tak, aby zachovávala pravdivost, tedy aby to, co dokážeme, logicky **vyplývalo** z daných předpokladů. Chceme-li charakterizovat určitou vědeckou disciplinu (například v matematice teorii přirozených čísel nebo teorii množin či grup apod.), můžeme se pokusit zvolit jistou množinu předpokladů, kterým říkáme **axiómy** a o kterých předpokládáme, že jsou pro tuto oblast pravdivé**,** a za použití vhodných odvozovacích pravidel dokázat mnohá (nebo dokonce v ideálním případě všechna) tvrzení, pravdivá v naší disciplině. (Pokud jsou axiómy analyticky pravdivé, pak tvrzení, která dokážeme, jsou rovněž analyticky pravdivá, tedy vždy, nejen ve zvolené disciplíně.) Takováto množina axiómů a odvozovacích pravidel (formulovaná v jistém formálním jazyce) se pak nazývá **logická teorie.** Vyhledávání a formulování axiómů a pravidel s cílem vytvořit teorii, která by pak mohla sloužit jako přesný základ pro další práci, by mohlo trvat velmi dlouho nebo dokonce donekonečna. Tato situace není vyloučena, ale typické je to, že nenastane. Např. jedna z nejdůležitějších matematických teorií, Goedel-Bernaysova teorie množin, má přehlednou množinu axiómů pozůstávající ze čtrnácti tvrzení. Můžeme tedy říct, že právě toto je rovněž jedna z okolností, které dělají z logiky přitažlivou disciplinu, a logiku v širším slova smyslu můžeme charakterizovat také jako **vědu o vytváření teorií.** Formalizovanými teoriemi a jejich vlastnostmi se zabývá kapitola 4. tohoto textu.

2. Výroková logika

2.1. Sémantický výklad výrokové logiky.

Výroková logika analyzuje věty až do úrovně elementárních výroků. Strukturu těchto elementárních výroků již dále nezkoumá. Přitom

Výrok je tvrzení, o němž má smysl prohlásit, zda je pravdivé či nepravdivé.

Tato "definice" se zdá být až banální, pokud si neuvědomíme, že ne každá věta vyjadřuje výrok. Např. věta *Francouzský král je holohlavý* nemůže být v současné době (kdy neexistuje francouzský král) ani pravdivá, ani nepravdivá. Kdyby totiž nastal jeden z těchto případů, vyplývala by z ní existence francouzského krále! Klasická výroková logika tedy ctí ***princip dvojhodnotovosti*** (*tercium non datur* – Chrisipos ze Solov).[1]

Výroky dělíme na jednoduché a složené. *Jednoduchý výrok* je takové tvrzení, jehož žádná vlastní část již není výrokem. *Složený výrok* pak má vlastní části – výroky. Výroková logika zkoumá strukturu těchto složených výroků v tom smyslu, že zkoumá způsob skládání jednoduchých výroků do složených pomocí *logických spojek.* Je to tedy teorie logických spojek. Přitom ovšem zachovává žádoucí *princip skladebnosti (kompozicionality),* podle něhož je pravdivostní hodnota složeného výroku jednoznačně určena jen pravdivostními hodnotami jeho složek a povahou spojení těchto složek (tj. logickou povahou spojek).

Příklad. Složené výroky.

V Praze prší a v Brně je hezky.

el. výrok — spojka — el. výrok

Není pravda, že v Praze prší.

spojka — el. výrok

Jazyk výrokové logiky musí proto obsahovat symboly zastupující jednotlivé elementární výroky (tzv. výrokové symboly (proměnné), které budou nabývat hodnot pravda, nepravda), symboly pro logické spojky a případné pomocné symboly.

Definice 2.1.1:

Abeceda jazyka výrokové logiky je množina následujících symbolů:

- Výrokové symboly: p, q, r, ... /případně s indexy/
- Symboly logických spojek /funktorů/: $\neg, \vee, \wedge, \supset, \equiv$
- Pomocné symboly /závorky/: (,) /případně [,],{,}/

  Symboly $\neg, \vee, \wedge, \supset, \equiv$ nazýváme po řadě funktory ***negace***, ***disjunkce***, ***konjunkce***, ***implikace***, ***ekvivalence***.

[1] TIL pracuje s parciálními funkcemi, tedy i s výroky bez pravdivostní hodnoty. Neklasické vícehodnotové a modální logiky pracují s intervalem pravdivostních hodnot.

Gramatika jazyka výrokové logiky rekurzivně definuje ***formule***:

(1) Výrokové symboly jsou formule /báze definice/.

(2) Jsou-li výrazy A, B formule, pak jsou formulemi i výrazy

$$(\neg A),\ (A \wedge B),\ (A \vee B),\ (A \supset B),\ (A \equiv B) \qquad (*)$$

/indukční krok definice/.

(3) Jiných formulí výrokové logiky, než podle bodů (1), (2) není /uzávěr definice/.

Jazyk výrokové logiky je množina všech formulí výrokové logiky.

Formule vzniklé podle bodu (1) nazýváme ***elementárními /atomárními***, ***primitivními/ formulemi***, formule vzniklé podle bodu (2) ***složenými formulemi***. Formule A, B jsou ***bezprostředními podformulemi*** formulí (∗). Maximální počet do sebe vnořených závorkových dvojic (,) vyskytujících se ve formuli udává ***/hierarchický/ řád formule***.

Poznámky 2.1.1:

1. Symboly A, B použité v indukčním kroku definice nejsou formulemi (nevyskytují se jako symboly v abecedě jazyka), ale ***metasymboly*** sloužící k označení formulí.
2. Používání závorek v zápisu formulí můžeme omezit přijetím následujících konvencí:
   - Složenou formuli nejvyššího řádu netřeba závorkovat.
   - Logické spojky uspořádáme do prioritní stupnice ¬, ∧, ∨, ⊃, ≡. Ze dvou funktorů váže silněji ten, který je v uvedené stupnici umístěn více vlevo.
     Pozn.: Tuto konvenci však příliš ”nezneužíváme” a závorky raději použijeme vždy, když chceme vyznačit strukturu formule.
   - V případě, že o prioritě vyhodnocení nerozhodnou ani závorky ani prioritní stupnice, vyhodnocujeme formuli zleva doprava. Tak např. formuli p⊃q⊃r⊃s vyhodnocujeme tak, jakoby byla zapsána ((p⊃q)⊃r)⊃s.
   - U vícečlenných konjunkcí nebo disjunkcí není třeba (vzhledem k jejich asociativitě – viz dále) uvádět závorky, tj. např. místo (p ∨ q) ∨ r nebo p ∨ (q ∨ r) lze psát pouze p ∨ q ∨ r. Tato konvence souvisí s předchozí konvencí (na pořadí vyhodnocování nezáleží a tedy lze standardně vyhodnocovat zleva doprava).
3. Symbolika není v literatuře jednotná. Následující tabulka udává alternativní značení spojek:

Symbol pro spojku	Alternativní Symboly
∧	&
⊃	→, ⇒
≡	↔, ⇔

Příklad 2.1.1:

Následující posloupnost formulí ilustruje postup konstrukce složené formule podle bodů (1) a (2). V prvém sloupci je zobrazen postup konstrukce složené formule striktně podle definice a v druhém s maximálním využitím konvencí šetřících závorky. V třetím sloupci je uveden hierarchický řád formulí uvedených v daném řádku.

Podle definice	S využitím konvencí	Hier.řád
p, q	p, q	0
$(\neg p), (\neg q), (p \wedge q)$	$\neg p, \neg q, p \wedge q$	1
$((\neg p) \vee (\neg q)), (\neg(p \wedge q))$	$\neg p \vee \neg q, \neg(p \wedge q)$	2
$(((\neg p) \vee (\neg q)) \equiv (\neg(p \wedge q)))$	$\neg p \vee \neg q \equiv \neg(p \wedge q)$	3

Definice 2.1.2:

Pravdivostní ohodnocení (valuace) výrokových symbolů je zobrazení *v*, které ke každému výrokovému symbolu přiřazuje pravdivostní hodnotu, tj. hodnotu z množiny {1,0}, která kóduje množinu {pravda, nepravda}.
Pravdivostní ohodnocení všech výrokových symbolů jazyka definuje ***model jazyka výrokové logiky***.

Pravdivostní funkce formule výrokové logiky je funkce *w*, která ke každému pravdivostnímu ohodnocení výrokových symbolů přiřazuje pravdivostní hodnotu celé formule. Tato hodnota je určena takto:

(1) Pravdivostní hodnota elementární formule je rovna pravdivostní hodnotě výrokového symbolu, tj.

$$w(p)_v = v(p) \text{ pro všechny výrokové proměnné p.}$$

(2) Jsou-li dány pravdivostní funkce formulí A, B, pak pravdivostní funkce formulí $\neg A$, $A \wedge B$, $A \vee B$, $A \supset B$, $A \equiv B$ jsou dány následující tabulkou 2.1:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \supset B$	$A \equiv B$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Tab. 2.1.

Převod z přirozeného jazyka do symbolického jazyka výrokové logiky:

Výrokově logická analýza.

Analýza na základě výrokové logiky nám umožňuje studovat strukturu vět z hlediska skládání jednoduchých výroků do složených výroků pomocí logických spojek. Elementární výroky zde považujeme za *nestrukturované "cihly",* které skládáme do strukturovaných bloků. Elementární výroky vstupují do spojení *jen* svou pravdivostní hodnotou a jsou navzájem zcela nezávislé. V dané větě proto označíme jednotlivé elementární výroky různými výrokovými symboly a místo spojek přirozeného jazyka použijeme odpovídající výrokové symboly pro spojky.

Výrokové spojky jsou zpřesněnou analogií příslušných spojek přirozeného jazyka (zejména v případě disjunkce a implikace), a to:

1. Spojka **negace** $\neg$ odpovídá "**není pravda, že**"
   Je to unární spojka, nespojuje dva výroky.
   Příklad: "Není pravda, že Praha je velkoměsto" (analyzujeme $\rightarrow$) $\neg$ p

2. Spojka **konjunkce** $\wedge$ odpovídá "**a**"
   Je to binární, komutativní spojka.
   Příklad:
   "Praha je hlavní město ČR a v Praze je sídlo prezidenta ČR" $\rightarrow$ p $\wedge$ q
   "Praha je hlavní město ČR a 2 + 3 = 5" $\rightarrow$ p $\wedge$ r

   Pozor! Ne každé "a" v přirozeném jazyce analyzujeme spojkou konjunkce, např.:
   "Jablka a hrušky se pomíchaly"
   "Přišel jsem domů a zatopil".

3. Spojka **disjunkce** $\vee$ odpovídá **"nebo"** (binární, komutativní spojka)

   Pozor! Spojka "nebo" se často používá v přirozeném jazyce ve *vylučujícím* smyslu "buď, anebo", pak při analýze použijeme jinou spojku – **alternativu** (neboli **nonekvivalenci**), viz tabulka všech binárních funkcí níže.
   "Osobní auta mají přední nebo zadní náhon" (nebo obojí) $\rightarrow$ p $\vee$ q
   "Napoleon diktoval nebo se procházel" (nebo obojí) $\rightarrow$ p $\vee$ q
   Ale: "Tento muž je ženatý nebo svobodný" $\rightarrow$ $\neg$ (p$\equiv$q)
   "Otec se zeptal, zda zůstanu doma nebo zda půjdu s ním" $\rightarrow$ $\neg$ (p$\equiv$q)

4. Spojka **implikace** $\supset$ odpovídá "**jestliže, pak", "když, tak", "je-li, pak**", apod.
   Je to jediná binární spojka, která není komutativní, proto nazýváme první člen implikace **antecedent**, druhý **konsekvent.** Implikace nepředpokládá *žádnou obsahovou souvislost* mezi antecedentem a konsekventem, proto bývá někdy nazývána *materiálová implikace* (středověk "*suppositio materialis"*).
   Implikace tedy (na rozdíl od častých případů v přirozeném jazyce) nezachycuje ani příčinnou ani časovou vazbu.
   "Jestliže 1+1=2, pak železo je kov" (pravdivý výrok) $\rightarrow$ p $\supset$ q
   "Jestliže existují ufoni, tak jsem papež" $\rightarrow$ p $\supset$ q
   Pozn.: Co tím dotyčný vlastně tvrdí? Jelikož předpokládáme, že říká pravdu, a evidentně není papež (konsekvent je nepravdivý), musí být nepravdivý rovněž antecedent, tedy dotyčný chce říct, že ufoni neexistují.

5. Spojka **ekvivalence** $\equiv$ odpovídá "**právě tehdy, když", "tehdy a jen tehdy, když"**, apod. , ale ne "tehdy, když" – to je implikace!
   "Řecká vojska vyhrávala boje tehdy (a jen tehdy), když o jejich výsledku rozhodovala fyzická zdatnost" $\rightarrow$ p $\equiv$ q
   a) "Dám ti facku, když mě oklameš" $\rightarrow$ okl $\supset$ facka
   b) "Dám ti facku tehdy a jen tehdy, když mě oklameš $\rightarrow$ okl $\equiv$ facka
   Situace: Neoklamal jsem. Ad a) – můžu dostat facku, ad b) – nemůžu dostat facku.
   Pozn.: V přirozeném jazyce se spojka ekvivalence používá zřídka, mnohem větší význam a častější použití má v exaktních vědách, zejména v matematice.

Pozn.: Převod z přirozeného do symbolické jazyka nemusí být vždy jednoznačný. (Proto také provádíme analýzu, abychom přirozené vyjádření zpřesnili, vybrali jeden z možných významů nejednoznačné věty.)

Příklad: ”Jestliže má člověk vysoký tlak a špatně se mu dýchá nebo má zvýšenou teplotu, pak je nemocen”.

p – ”X má vysoký tlak”
q – ”X se špatně dýchá”
r – ”X má zvýšenou teplotu”
s – ”X je nemocen”

1. analýza: $[(p \wedge q) \vee r] \supset s$ 2. analýza: $[p \wedge (q \vee r)] \supset s$

Obě formule jsou různé, ale ze zadání nepoznáme, jak bylo tvrzení myšleno.

Pozn.: Ne všechny gramaticky složené věty přirozeného jazyka je možno jednoduše analyzovat jako složené výroky.

Příklad: “Hokejisté prohráli kvalifikační zápas, proto se vrátili z mistrovství světa předčasně”.
Jelikož si můžeme strukturu věty zachytit schématicky jako “Protože prohráli (p), tedy se vrátili (v)” a toto spojení evidentně není komutativní, zdálo by se, že ji můžeme analyzovat pomocí spojky implikace: $p \supset v$. Ale pak by věta musela být pravdivá i v případě, že $\neg p$, tj. v případě, kdy hokejisté neprohráli kvalifikační zápas, což evidentně není pravda.
Spojce “protože” neodpovídá logická spojka implikace!
Jediný způsob, jak by bylo možno ve výrokové logice zachytit výše uvedené tvrzení, by bylo použití tzv. sémantického *modus ponens*: p, $p \supset v$. Z uvedené dvojice výroků pak vyplývá v.

Poznámky 2.1.2:

1. Pravdivostní funkce složených formulí, definované tabulkou 2.1, lze ekvivalentně definovat následujícími vzorci (tato definice je využívána v modálních logikách).

$$w(\neg A) = 1\text{-}w(A)$$
$$w(A \wedge B) = \min\{w(A), w(B)\}$$
$$w(A \vee B) = \max\{w(A), w(B)\}$$
$$w(A \supset B) = \max\{1\text{-}w(A), w(B)\}$$
$$w(A \equiv B) = \max\{\min\{w(A), w(B)\}, \min\{1\text{-}w(A), 1\text{-}w(B)\}\}$$

   (Tyto vztahy platí pro libovolné ohodnocení *v* výrokových proměnných, odkaz na *v* proto vynecháváme.)

2. Obor pravdivostních hodnot nemusí být nutně dvouprvkovou množinou {1, 0}, ale může být také např. tříprvkovou množinou {0, 1/2, 1}, nebo nekonečnou spojitou množinou danou reálným uzavřeným intervalem <0,1>. Pravdivostní funkce mohou být i nyní definovány výše uvedenými vzorci, ale také nějakým jiným způsobem. Výrokové logiky s takto definovanými pravdivostními funkcemi nazýváme ***vícehodnotovými***, resp. ***spojitěhodnotovými***. V dalším se však budeme zabývat pouze ***dvouhodnotovou*** logikou s výše definovanými pravdivostními funkcemi.

Příklad 2.1.2:

V následující tabulce jsou počítány pravdivostní funkce formulí:

$\neg p, \neg q, p \wedge q$ (sloupce označené 1),
$(\neg p \vee \neg q), \neg(p \wedge q)$ (sloupce označené 2),
$(\neg p \vee \neg q) \equiv \neg(p \wedge q)$ (3.sloupec) a
$\neg[(\neg p \vee \neg q) \equiv \neg(p \wedge q)]$ (4.sloupec).

Sloupce v tabulce vyplňujeme v pořadí vyznačeném pořadovými čísly uvedenými ve druhém řádku tabulky (tj. při určování pravdivostní funkce formule postupujeme ve směru rostoucího hierarchického řádu podformulí). Sloupce označené 0 obsahují všechny možné kombinace ohodnocení výrokových symbolů, n-té sloupce se počítají na základě sloupců (n-1)-ých.

¬	((¬	p	∨	¬	q)	≡	¬	(p	∧	q))
4.	**1.**	**0.**	**2.**	**1.**	**0.**	**3.**	**2.**	**0.**	**1.**	**0.**
0	1	0	1	1	0	1	1	0	0	0
0	1	0	1	0	1	1	1	0	0	1
0	0	1	1	1	0	1	1	1	0	0
0	0	1	0	0	1	1	0	1	1	1

Definice 2.1.3:

Je-li formule A vytvořena z *k* různých výrokových symbolů, pak existuje celkem 2^k různých ohodnocení (valuací) *v* formule A. Každé ohodnocení *v* výrokových symbolů obsažených ve formuli A, pro které je hodnota pravdivostní funkce rovna 1, tedy $w(A)_v = 1$, se nazývá ***model*** této ***formule***.

Formule A výrokové logiky je ***splnitelná***, je-li $w(A)_v = 1$ pro nějaké ohodnocení *v,* neboli existuje aspoň jeden model formule A.

Formule A výrokové logiky je ***tautologií /logickým zákonem/***, je-li $w(A)_v = 1$ pro všechna ohodnocení *v,* neboli každé ohodnocení je modelem formule A. Skutečnost, že formule A je tautologií, označujeme zápisem |= A.

Formule A výrokové logiky je ***kontradikcí***, jestliže neexistuje takové ohodnocení výrokových symbolů, pro které by hodnota pravdivostní funkce formule A byla rovna 1, tj. $w(A)_v = 0$ pro všechna ohodnocení *v,* formule nemá model.

Množina formulí M je ***splnitelná***, jestliže existuje valuace *v* taková, že $w(A)_v = 1$ pro *každou* formuli $A \in M$. Takové ohodnocení *v* se pak nazývá ***model množiny M.***

Formule A ***výrokově logicky vyplývá*** *z množiny formulí M,* značíme *M* |= A, jestliže A je pravdivá v každém modelu množiny *M.*

Poznámka 2.1.3:

Připomeňme si obecnou definici logického vyplývání (Definice 1.1.) z úvodní kapitoly. (Za všech *okolností* takových, že jsou pravdivé premisy, musí být pravdivý i závěr.) Vidíme tedy, že ty *okolnosti* mapujeme ve výrokové logice pouze jako ohodnocení výrokových proměnných (což odpovídá pravdivosti či nepravdivosti elementárních výroků).

Jestliže je množina formulí sporná, pak nemá model, a tedy (viz vlastnost 5) – kap. 1) z ní vyplývá jakákoli formule.

Jak jsme již naznačili v příkladě 2.1.2, pro zjištění pravdivostní hodnoty formule používáme tabulkové metody. Musíme prozkoumat všechny možné valuace *v*. Je-li *n* počet výrokově logických proměnných v A, pak počet valuací je 2^n a příslušná tabulka má 2^n řádků.

Příklad 2.1.3:

- Formule p, q, ¬p, ¬q, p∧q, ¬p ∨ ¬q, ¬(p ∧ q), (¬p ∨ ¬q) ≡ ¬(p ∧ q) jsou splnitelné. Např. formule ¬(p ∧ q) je pravdivá (má pravdivostní hodnotu 1) pro ohodnocení (0,1) výrokových symbolů (p,q)). Rovněž ohodnocení (1,0), (0,0) jsou její modely, ale ne (1,1).
- Formule (¬p ∨ ¬q) ≡ ¬(p ∧ q) je tautologií. Pro všechna možná ohodnocení (0,0), (0,1), (1,0), (1,1) výrokových symbolů (p, q) je tato formule pravdivá. Každé ohodnocení formuli splňuje, je jejím modelem.
- Formule ¬[(¬p ∨ ¬q) ≡ ¬(p ∧ q)] je kontradikcí. Neexistuje ohodnocení výrokových symbolů (p, q) pro které by byla formule pravdivá. Žádné ohodnocení formuli nesplňuje, formule nemá model.

Platnost uvedených tvrzení okamžitě plyne z tabulky předchozího příkladu 2.1.2.

- Zjistíme, zda množina formulí $M = \{p \supset r, q \supset r, p \vee q\}$ je splnitelná:

p	q	r	p ⊃ r	q ⊃ r	p ∨ q
1	1	1	**1**	**1**	**1**
1	1	0	0	0	1
1	0	1	**1**	**1**	**1**
1	0	0	0	1	1
0	1	1	**1**	**1**	**1**
0	1	0	1	0	1
0	0	1	1	1	0
0	0	0	1	1	0

Daná množina *M* je splnitelná a jejími modely jsou ohodnocení odpovídající 1., 3. a 5. řádku. Dále z tabulky vidíme, že z množiny *M* logicky vyplývá formule r. Pro každý model této množiny je r pravdivá. Tedy (závorky pro množinu premis není nutno uvádět): $p \supset r, q \supset r, p \vee q \models r$

Příklad 2.1.4 /některé důležité tautologie výrokové logiky/**:**

- Tautologie s jediným výrokovým symbolem:
  $\models p \equiv p$
  $\models p \vee \neg p$ zákon vyloučeného třetího
  $\models \neg(p \wedge \neg p)$ zákon sporu
  $\models p \equiv \neg\neg p$ zákon dvojí negace
- Algebraické zákony:
  $\models (p \vee q) \equiv (q \vee p)$ komutativní zákon pro $\vee$
  $\models (p \wedge q) \equiv (q \wedge p)$ komutativní zákon pro $\wedge$
  $\models (p \equiv q) \equiv (q \equiv p)$ komutativní zákon pro $\equiv$
  $\models (p \vee q) \vee r \equiv p \vee (q \vee r)$ asociativní zákon pro $\vee$
  $\models (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ asociativní zákon pro $\wedge$
  $\models ((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$ asociativní zákon pro $\equiv$
  $\models (p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$ distributivní zákon pro $\wedge,\vee$
  $\models (p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ distributivní zákon pro $\vee,\wedge$
- Zákony pro implikaci:
  $\models p \supset (q \supset p)$ zákon simplifikace
  $\models (p \wedge \neg p) \supset q$ zákon Dunse Scota
  $\models (p \supset q) \equiv (\neg q \supset \neg p)$ zákon kontrapozice
  $\models (p \supset (q \supset r)) \equiv ((p \wedge q) \supset r)$ spojování předpokladů
  $\models (p \supset (q \supset r)) \equiv (q \supset (p \supset r))$ na pořadí předpokladů nezáleží
  $\models (p \supset q) \supset ((q \supset r) \supset (p \supset r))$ hypotetický sylogismus
  $\models ((p \supset q) \wedge (q \supset r)) \supset (p \supset r)$ tranzitivita implikace
  $\models (p \supset (q \supset r)) \equiv ((p \supset q) \supset (p \supset r))$ Fregův zákon
  $\models (\neg p \supset p) \supset p$ reductio ad absurdum
  $\models ((p \supset q) \wedge (p \supset \neg q)) \supset \neg p$ reductio ad absurdum
  $\models (p \wedge q) \supset p$, $\models (p \wedge q) \supset q$
  $\models p \supset (p \vee q)$, $\models q \supset (p \vee q)$
- Zákony pro vzájemné převody funktorů:
  $\models (p \equiv q) \equiv (p \supset q) \wedge (q \supset p)$
  $\models (p \equiv q) \equiv (p \wedge q) \vee (\neg q \wedge \neg p)$
  $\models (p \supset q) \equiv (\neg p \vee q)$
  $\models \neg(p \supset q) \equiv (p \wedge \neg q)$ **Negace implikace**
  $\models \neg(p \wedge q) \equiv (\neg p \vee \neg q)$ De Morganovy zákony
  $\models \neg(p \vee q) \equiv (\neg p \wedge \neg q)$ De Morganovy zákony

Pozn.: Uvedené zákony snadno ověříme tabulkovou metodou.

Metoda protipříkladu – ověřování tautologií (vyplývání) sporem:

Tabulková metoda ověřování logického vyplývání či logických zákonů, splnitelnosti, atd. je vhodná pouze pro formule s malým počtem výrokových proměnných. Vždyť již při čtyřech proměnných má příslušná tabulka 16 řádků, při pěti 32 řádků! Proto jsou používány jiné, efektivnější metody. Jednou z nich je metoda protipříkladu, která je

zejména vhodná pro ověřování tautologií ve tvaru implikace a pro ověřování logického vyplývání. (S ostatními se seznámíme v dalším textu.)

Příklad 2.1.5

Ověříme zákon simplifikace $p \supset (q \supset p)$. Vycházíme z toho, že implikace je nepravdivá jen v jednom případě (Tab. 2.1), a to když je antecedent pravdivý a konsekvent nepravdivý. Prověříme tedy všechny valuace, pro něž je konsekvent nepravdivý a jestliže alespoň pro jednu z těchto valuací nastane případ, že by byl antecedent pravdivý, nemůže být daná formule tautologie a naopak, jestliže pro žádnou z těchto valuací není antecedent pravdivý, je uvažovaná formule tautologie. V našem případě bude konsekvent nepravdivý pouze při jedné valuaci, a to $q = 1$, $p = 0$. Ale v tom případě nemůže být antecedent $p = 1$, tedy celá formule je pravdivá i pro tuto valuaci. Nyní vše názorněji:

$$\begin{array}{llll} p \supset (q \supset p) & & & \\ 1 \quad\ 0 & & & \\ | \quad 1 \quad 0 & & & \\ 0 & & & \text{! spor !} \end{array}$$

Nyní ověříme, zda formule $\neg p$ logicky vyplývá z množiny $\{p \supset q, r \vee \neg q, \neg r\}$. Názorně tedy prověříme úsudkové schéma (všimněte si, že je to formalizace úsudku z kapitoly 1 "o kurzu a přednášejícím"):

$$\begin{array}{llllll} p \supset q, & r \vee \neg q, & \neg r & / & \neg p & \\ 1 \quad\ & 1 \quad\ & 1 & & 0 & \\ & & 0 & & 1 & \\ 1 \quad 1 & 0 \quad 1 & & & & \\ \quad |\!\!-\!\!-\!\!- & 0 & & & \text{! spor !} & \end{array}$$

Věta 2.1.1 /o substituci/**:**

Nechť A je tautologie výrokové logiky utvořená z výrokových symbolů $p_1, p_2,...,p_n$. Nechť formule B vznikne z tautologie A simultánním nahrazením výrokových symbolů $p_1, p_2,...,p_n$ formulemi $A_1,A_2,...,A_n$ (tj. substitucemi A_i za p_i pro $i = 1, 2,...,n$). Potom formule B je rovněž tautologií.

Důkaz:

Uvažujme libovolné pravdivostní ohodnocení výrokových symbolů obsažených ve formuli B a nechť při tomto ohodnocení mají formule $A_1,A_2,...,A_n$ pravdivostní hodnoty $h_1,h_2,...,h_n$. Udělíme-li tyto hodnoty výrokovým symbolům $p_1,p_2,...,p_n$ formule A, budou mít formule A i B stejnou pravdivostní hodnotu. Vzhledem k tomu, že A je tautologie, bude tato pravdivostní hodnota vždy 1.

Poznámka 2.1.4:

Věta o substituci umožňuje vytvořit k dané tautologii neomezeně mnoho dalších tautologií, které mají s danou výchozí tautologií společný tvar. Nahradíme-li v tautologii výrokové symboly p, q, r,... metasymboly A, B, C,... dostaneme z konkrétní výchozí tautologie ***schéma tautologií*** daného tvaru. Tak např. z tautologie $(p \wedge q) \supset p$ získáme tautologické schéma $(A \wedge B) \supset A$, pod které spadá nejenom původní formule $(p \wedge q) \supset p$, ale např. i formule $(q \wedge q) \supset q$, $(\neg p \wedge q) \supset \neg p$, $[(p \equiv r) \wedge \neg q] \supset (p \equiv r)$ a neomezené množství dalších formulí.

Věta 2.1.2 (sémantická varianta věty o dedukci):

Mějme formule $A_1, A_2, \ldots, A_n, B$, kde $n \geq 1$. Pak platí, že

$$A_1, A_{2, \ldots,} A_n \models B \text{ právě tehdy když } A_1, A_2, \ldots, A_{n-1} \models A_n \supset B.$$

Důkaz: Zřejmý (plyne z definice vyplývání – 2.1.3 a implikace – Tab. 2.1)

Pozn.: Uplatníme-li větu 2.1.2 *n*-krát, dostaneme

$$A_1, A_{2, \ldots,} A_n \models B \text{ právě tehdy, když } \models A_1, \supset (A_2 \supset \ldots \supset (A_{n-1} \supset (A_n \supset B))\ldots).$$

Nyní můžeme použít n–1 krát zákon o spojování předpokladů (viz Příklad 2.1.4) a dostaneme:

$$A_1, A_2, \ldots, A_n \models B \text{ právě tehdy, když } \models (A_1 \wedge A_2 \wedge \ldots \wedge A_{n-1} \wedge A_n) \supset B$$

Věta 2.1.3 o implikaci (sémantická varianta pravidla modus ponens)**:**

Jsou-li formule A, $A \supset B$ tautologie, pak je tautologií také formule B, neboli symbolicky zapsáno:

$$\text{Je-li } \models A, \models A \supset B, \text{ pak také } \models B.$$

Důkaz:

Sporem. Jestliže B není tautologií, pak existuje ohodnocení výrokových symbolů (obsažených ve formulích A, B), při kterém formule B není pravdivá. Formule A při tomto ohodnocení pravdivá je, neboť je tautologií a jako taková je pravdivá při každém ohodnocení. Při tomto ohodnocení však nemůže být pravdivá formule $A \supset B$, neboť podle definice pravdivostní funkce implikace není možné, aby současně w(A) = 1 a w(B) = 0. To je v rozporu s předpokladem podle kterého je formule $A \supset B$ tautologií.

Věta 2.1.4 /o ekvivalenci/**:**

Nechť formule B vznikne z formule A tak, že podformule C formule A je nahrazena formulí D. Potom platí:

$$\text{je-li } \models C \equiv D, \text{ pak také } \models A \equiv B.$$

Důkaz:

Je-li $\models C \equiv D$, pak formule C, D mají stejnou pravdivostní funkci a tedy záměnou D za C vznikne z formule A formule se stejnou pravdivostní funkcí. Tedy $\models A \equiv B$.

Definice 2.1.5:

Nechť formule F je utvořená z formulí A, B pouze pomocí funktorů $\neg, \wedge, \vee$. Formule F', která vznikne z formule F vzájemnou záměnou funktorů $\wedge$ a $\vee$, nazýváme ***duální formulí*** k formuli F. Vzhledem k tomu, že (F')' = F, jsou formule F a F' ***duálními navzájem***.

Věta 2.1.5:

Nechť formule F, G jsou utvořeny pouze pomocí funktorů $\neg, \wedge, \vee$. Potom platí následující věty o dualitě:

1. $\neg(F(p,q,\ldots)) \equiv F'(\neg p, \neg q, \ldots)$
2. $\models F \supset G$ právě tehdy, je-li $\models G' \supset F'$
3. $\models F \equiv G$ právě tehdy, je-li $\models G' \equiv F'$

Důkaz:

Bude uveden v kap.3.1. za obecnějších předpokladů (pro obecnější formule predikátové logiky).

Úplné systémy spojek výrokové logiky.

Ke každé formuli výrokové logiky je podle definice 2.1.2 jednoznačně přiřazena pravdivostní funkce. Na druhé straně k dané pravdivostní funkci (obecně skalární dvouhodnotové funkci o n dvouhodnotových proměnných) existuje mnoho formulí výrokové logiky, které ji mají za svou. Jsou to všechny navzájem ekvivalentní formule. Abychom tuto nejednoznačnost odstranili, budeme definovat ***standardní (kanonické) tvary*** formulí výrokové logiky. Každá třída navzájem ekvivalentních formulí bude reprezentována jedinou formulí ve standardním tvaru.

Definice 2.1.6:

- ***Literál*** je výrokový symbol nebo jeho negace.
- ***Elementární konjunkce*** (**EK)** je konjunkce literálů.
- ***Elementární disjunkce*** (**ED)** je disjunkce literálů.
- ***Úplná elementární konjunkce*** (**ÚEK)** dané množiny výrokových symbolů je elementární konjunkce, ve které se každý symbol z dané množiny vyskytuje právě jednou (buďto prostě nebo negovaný).
- ***Úplná elementární disjunkce*** (**ÚED**) dané množiny výrokových symbolů je elementární disjunkce, ve které se každý symbol z dané množiny vyskytuje právě jednou (buďto prostě nebo negovaný).
- ***Disjunktivní normální forma*** (**DNF**) dané formule je formule ekvivalentní s danou formulí a mající tvar disjunkce elementárních konjunkcí.
- ***Konjunktivní normální forma*** (**KNF**) dané formule je formule ekvivalentní s danou formulí a mající tvar konjunkce elementárních disjunkcí.
- ***Úplná disjunktivní normální forma*** (**UDNF**) dané formule je formule ekvivalentní s danou formulí a mající tvar disjunkce úplných elementárních konjunkcí.
- ***Úplná konjunktivní normální forma*** (**UKNF**) dané formule je formule ekvivalentní s danou formulí a mající tvar konjunkce úplných elementárních disjunkcí.
- ÚDNF a UKNF dané formule nazýváme ***kanonickými (standardním) tvary*** této formule.

Poznámky 2.1.5:

1. Elementární konjunkci splňuje právě jedno ohodnocení (model). Je jím ohodnocení, které přiřazuje prostým činitelům konjunkce pravdivostní hodnotu "1" a negovaným činitelům pravdivostní hodnotu "0".
2. Elementární disjunkci splňují všechna možná ohodnocení s výjimkou jediného a sice toho ohodnocení, které přiřazuje pravdivostní hodnotu "0" prostým sčítancům disjunkce a pravdivostní hodnotu "1" negovaným sčítancům disjunkce.

Věta 2.1.6:

1. Každou formuli, která není kontradikcí, lze vyjádřit ve tvaru UDNF.
2. Každou formuli, která není tautologií, lze vyjádřit ve tvaru UKNF.

Důkaz:

Důkaz je konstruktivní - ukážeme, jak se požadované tvary naleznou. K dané formuli nejdříve určíme její pravdivostní funkci (nejraději zapsanou ve tvaru tabulky) postupem vysvětleném v příkladu u definice 2.1.2. Dále se postup liší podle toho, zda hledáme 1. UDNF nebo 2. UKNF.

Ad 1.: Ke každému ohodnocení výrokových symbolů, pro které má pravdivostní funkce hodnotu "1" (takové ohodnocení existuje alespoň jedno, neboť podle předpokladu formule není kontradikcí) sestrojíme UEK, která nabývá hodnoty "1" pro toto (a jen toto) ohodnocení. Disjunkce všech těchto UEK představuje hledanou UDNF

Ad 2.: Ke každému ohodnocení výrokových symbolů, pro které má pravdivostní funkce hodnotu "0" (takové ohodnocení existuje alespoň jedno, neboť podle předpokladu formule není tautologií) sestrojíme UED, která nabývá hodnoty "0" pro toto (a jen toto) ohodnocení. Konjunkce všech těchto UED představuje hledanou UKNF.

Pozn.: Na množině formulí výrokové logiky můžeme zavést binární relaci ekvivalence $\Leftrightarrow$ (tj. reflexivní, symetrickou a transitivní relaci) definovanou takto: **A $\Leftrightarrow$ B** právě když A |= B a B |= A.
Jestliže platí A $\Leftrightarrow$ B, pak obě formule mají stejné modely, tj. mají stejnou pravdivostní funkci.
Navíc zřejmě platí: |= A $\equiv$ B právě když A $\Leftrightarrow$ B. Proto se v literatuře často nerozlišuje mezi $\equiv$ a $\Leftrightarrow$.

Příklad 2.1.7:

Nalézt UDNF a UKNF pro formuli $\neg(p \supset q)$:

1. *Metoda pravdivostní tabulky* (podle konstrukce popsané v důkaze):

p	q	$p \supset q$	$\neg(p \supset q)$	UEK	UED
0	0	1	0	-	$p \vee q$
0	1	1	0	-	$p \vee \neg q$
1	0	0	1	$p \wedge \neg q$	-
1	1	1	0	-	$\neg p \vee \neg q$

UDNF: $\neg(p \supset q) \Leftrightarrow p \wedge \neg q$, UKNF: $\neg(p \supset q) \Leftrightarrow (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$

2. *Metoda ekvivalentních úprav*:
UKNF: $\neg(p \supset q) \Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow (p \wedge \neg q) \Leftrightarrow [p \vee (q \wedge \neg q)] \wedge [\neg q \vee (p \wedge \neg p)] \Leftrightarrow$ ...
$\Leftrightarrow (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$

Příklad 2.1.8:

Alchymista je zavřen ve vězení, protože se mu stále nedaří přeměna olova ve zlato. Dostane pět motáků, z nichž první čtyři obsahují následující výroky:

p – Podaří se ti přeměna olova ve zlato
q – 1.4. bude tvůj švagr jmenován prokurátorem
r – Po 1.4. bude soud.

První moták zní: $p \wedge q \wedge r$

Druhý moták zní: $p \wedge q \wedge \neg r$
Třetí moták zní: $\neg p \wedge \neg q \wedge r$
Čtvrtý moták zní: $\neg p \wedge \neg q \wedge \neg r$
Pátý moták zní: Alespoň jeden z předchozích motáků je pravdivý.

Otázka: Co se vlastně nebohý alchymista dověděl?

Řešení: $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$. Máme tedy nalézt formuli, k níž je tato UDNF ekvivalentní. Dostaneme:

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

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

Odpověď: Podaří se ti přeměna olova ve zlato tehdy a jen tehdy, když bude 1.4. tvůj švagr jmenován prokurátorem.

Z věty 2.1.6 vyplývá, že všechny formule výrokové logiky mohou být převedeny na ekvivalentní formule obsahující pouze funktory $\neg, \wedge, \vee$. Funktory $\supset, \equiv$ jsou z pohledu věty 2.1.6 nadbytečné. V souvislosti s tím vznikají otázky:

a) Kolik pravdivostních funkcí (a jimi definovaných logických funktorů) vůbec existuje ?
b) Nelze množinu výchozích pravdivostních funkcí (a tím i množinu výchozích logických funktorů), nezbytných k vytvoření libovolné pravdivostní funkce, dále zredukovat ?

Seznam všech pravdivostních funkcí se dvěma argumenty:

X Y	0 0	0 1	1 0	1 1	
w0(X,Y)	0	0	0	0	dvouargumentová konstanta: "0"
w1(X,Y)	0	0	0	1	konjunkce: $X \wedge Y$
w2(X,Y)	0	0	1	0	inhibice: $\neg(X \supset Y)$
w3(X,Y)	0	0	1	1	1. proměnná: X
w4(X,Y)	0	1	0	0	inhibice: $\neg(Y \supset X)$
w5(X,Y)	0	1	0	1	2. proměnná: Y
w6(X,Y)	0	1	1	0	nonekvivalence: $\neg(X \equiv Y)$
w7(X,Y)	0	1	1	1	disjunkce: $X \vee Y$
w8(X,Y)	1	0	0	0	NOR (Peirce): $\neg(X \vee Y)$, $X \downarrow Y$ "ani ani"
w9(X,Y)	1	0	0	1	ekvivalence: $X \equiv Y$
w10(X,Y)	1	0	1	0	negace 2. proměnné: $\neg Y$
w11(X,Y)	1	0	1	1	implikace: $Y \supset X$
w12(X,Y)	1	1	0	0	negace 2. proměnné: $\neg X$
w13(X,Y)	1	1	0	1	implikace: $X \supset Y$
w14(X,Y)	1	1	1	0	NAND (Sheffer): $\neg(X \wedge Y)$, $X \uparrow Y$
w15(X,Y)	1	1	1	1	dvouargumentová konstanta: "1"

Seznam všech pravdivostních funkcí s jedním argumentem:

X	0	1	
w0(X)	0	0	jednoargumentová konstanta "0"
w1(X)	0	1	argument X
w2(X)	1	0	negace argumentu ¬X
w3(X)	1	1	jednoargumentová konstanta "1"

Vybrané pravdivostní funkce s více argumenty:

- pravdivostní funkce n-ární konjunkce a disjunkce
- pravdivostní funkce n-ární majoranty /n liché/

Věta 2.1.7:
Počet n-arních pravdivostních funkcí je 2 umocněno na 2^n.

Důkaz:
Každý argument může nabývat dvou hodnot nezávisle na hodnotě ostatních argumentů. Počet všech možných argumentových n-tic je tedy 2^n. Ke každé argumentové n-tici může funkce přiřadit jednu ze dvou hodnot a to nezávisle na přiřazení hodnoty k jiným n-ticím. Funkcí je tedy 2 umocněno na 2^n.

Definice 2.1.7:
Soustava pravdivostních funkcí je ***funkcionálně úplná***, jestliže jejich superpozicí (skládáním) lze vytvořit libovolnou pravdivostní funkci o libovolném počtu argumentů.

Věta 2.1.8:
Následující soustavy pravdivostních funkcí jsou funkcionálně úplné:
1. pravdivostní funkce příslušející funktorům $\{\neg, \wedge, \vee\}$,
2. pravdivostní funkce příslušející funktorům $\{\neg, \wedge\}$ nebo $\{\neg, \vee\}$,
3. pravdivostní funkce příslušející funktorům $\{\neg, \supset\}$,
4. pravdivostní funkce příslušející funktorům $\{\uparrow\}$ nebo $\{\downarrow\}$.

Důkaz:
Ad 1.: Vyplývá z věty 2.1.6 o UNDF a UNKF.
Ad 2.: Plyne z tvrzení 1. a z de Morganových zákonů výrokové logiky.
Ad 3.: Plyne z tvrzení 2. a z ekvivalence formulí $(A \vee B) \Leftrightarrow (\neg A \supset B)$.
Ad 4.: Plyne z tvrzení 2. a z ekvivalence formulí
$\neg A \Leftrightarrow A \uparrow A$, $A \wedge B \Leftrightarrow (A \uparrow B) \uparrow (A \uparrow B)$, kde $\uparrow$ značí NAND,
$\neg A \Leftrightarrow A \downarrow A$, $A \vee B \Leftrightarrow (A \downarrow B) \downarrow (A \downarrow B)$, kde $\downarrow$ značí NOR.

Příklad 2.1.9 /některé důležité rovnosti algebry výrokové logiky/**:**

$p \vee T \Leftrightarrow T$	$p \wedge T \Leftrightarrow p$	kde T je tautologie
$p \vee K \Leftrightarrow p$	$p \wedge K \Leftrightarrow K$	kde K je kontradikce
$p \vee p \Leftrightarrow p$	$p \wedge p \Leftrightarrow p$	idempotence
$p \vee q \Leftrightarrow q \vee p$	$p \wedge q \Leftrightarrow q \wedge p$	komutativita
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	asociativita
$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$	$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$	distributivita
$p \vee (p \wedge q) \Leftrightarrow p$	$p \wedge (p \vee q) \Leftrightarrow p$	absorpce
$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	de Morgan

$p \Leftrightarrow p \vee (q \wedge \neg q)$ $p \Leftrightarrow p \wedge (q \vee \neg q)$	rozšíření
$(p \supset q) \Leftrightarrow \neg p \vee q$ $(p \supset q) \Leftrightarrow \neg(p \wedge \neg q)$	eliminace $\supset$
$(p \equiv q) \Leftrightarrow (p \supset q) \wedge (q \supset p)$	eliminace $\equiv$
$(p \equiv q) \Leftrightarrow (p \wedge q) \vee (\neg q \wedge \neg p)$	eliminace $\equiv$
$\neg\neg p \Leftrightarrow p$	eliminace $\neg$

Poznámky 2.1.5:

1. Zápisy $A \supset B$, $A \equiv B$ představují formule, zatímco zápisy $A \models B$, $A \Leftrightarrow B$ reprezentují vztahy (binární relace) mezi formulemi. Vztah $\models$ je reflexivní a transitivní relace, vztah $\Leftrightarrow$ je binární relace typu ekvivalence (reflexivní, symetrická a tranzitivní) na množině všech formulí.
2. Na výrokovou logiku lze pohlížet jako na algebraickou a relační strukturu (***Booleova algebra***) s následujícími charakteristikami:
   - Nosičem struktury je podmnožina množiny všech formulí výrokové logiky, které nepoužívají spojek $\supset$, $\equiv$.
   - Na této množině jsou definovány operace:
     - $\neg$..... unární operace,
     - $\wedge$, $\vee$ ... binární operace.
   - Na této množině je definována binární relace:
     - $\Leftrightarrow$ ..... relace ekvivalence (formulí)
3. Faktorová algebra (algebra z bodu 2.) indukovaná relací ekvivalence $\Leftrightarrow$ je opět Booleovou algebrou a nazývá se ***Lindenbaumova algebra***. Jejími prvky jsou třídy navzájem ekvivalentních formulí. Na této množině lze definovat binární relaci (neostrého) uspořádání, tj. reflexivní, antisymetrickou a transitivní relaci na základě vztahu logického vyplývání.

Pozn.: Algebraické teorie a teorie relací jsou podrobněji studovány v Kapitole 4.1.

Shrnutí. V této kapitole jsme se naučili řešit *sémantickými* metodami základní úkoly výrokové logiky, především pak:

- Ověřit (dokázat), zda je daná formule **tautologie, kontradikce,** nebo **splnitelná** formule.
- Ověřit, zda je daný **úsudek správný** (platný), tedy zda závěr **vyplývá** z daných předpokladů.
- Ověřit, zda je daná **množina formulí splnitelná** či **kontradiktorická**.
- Zjistit, **co vyplývá** z daných předpokladů.

Poznali jsme dvě základní sémantické metody výrokové logiky: Tabulkovou metodu a metodu sporem. Jelikož jsou tyto metody při větším počtu výrokových proměnných neefektivní, byly vyvinuty metody, které jsou výhodnější a efektivnější (pro počítačové zpracování). Jednou z nejdůležitějších je **rezoluční metoda**, se kterou se seznámíme v následující kapitole.

2.2. Rezoluční metoda ve výrokové logice (Automatické dokazování)

Další důležitou metodou ověřování tautologií, logického vyplývání, řešení úlohy – co vyplývá z daných předpokladů, apod. je tzv. metoda **základní rezoluce.** Touto metodou dokazujeme **nesplnitelnost** dané formule (resp. množiny formulí) a je uplatnitelná na formuli v **konjunktivní normální formě (KNF).** Využívá dvou jednoduchých tvrzení:

1) Je-li formule A tautologie, pak formule $\neg A$ je kontradikce a naopak. (Důkaz zřejmý.) Symbolicky:

$\models A$ právě když $\models \neg A$

2) Rezoluční pravidlo odvozování: Nechť l je literál. Z formule $(A \vee l) \wedge (B \vee \neg l)$ odvoď $(A \vee B)$. Zapisujeme:

$$\frac{(A \vee l) \wedge (B \vee \neg l)}{(A \vee B)}$$

Toto pravidlo není přechodem k ekvivalentní formuli, ale zachovává **splnitelnost.**
Důkaz: Nechť je formule $(A \vee l) \wedge (B \vee \neg l)$ splnitelná, tedy pravdivá při nějaké valuaci v. Pak při této valuaci musí být pravdivé oba disjunkty (tzv. klausule) $A \vee l$ a $B \vee \neg l$. Nechť je dále $v(l) = 0$. Pak $w(A) = 1$ a tedy $w(A \vee B) = 1$. Nechť je naopak $v(l) = 1$. Pak $w(\neg l) = 0$ a musí být $w(B) = 1$, a tedy $w(A \vee B) = 1$. V obou případech je tedy formule $A \vee B$ pravdivá v modelu původní formule, a tedy splnitelná.

Uvědomme si, že důkaz byl proveden pro jakýkoli model v. Jinými slovy platí, že pravidlo zachovává i pravdivost:

$(A \vee l) \wedge (B \vee \neg l) \models (A \vee B)$.

(To nám poskytuje návod, jak řešit úlohu, **co vyplývá z** dané formule, resp. množiny formulí.)

Postup řešení.

Pozn.: Jednotlivé disjunkty v KNF nazýváme **klausule,** a proto je KNF také nazývána **klausulární forma.**

a) Důkaz, že formule A je tautologie: Formuli A znegujeme a převedeme do KNF. Nyní uplatňujeme pravidlo rezoluce. Pokud při postupném "vyškrtávání" literálů s opačným znaménkem dospějeme k prázdné klausuli, kterou značíme $\square$, je tato evidentně nesplnitelná, tedy také původní $\neg A$ je nesplnitelná a A je tautologie.

b) Důkaz správnosti úsudku $P_1,...,P_n \models Z$. Závěr Z znegujeme a dokazujeme, že množina $\{P_1,...,P_n, \neg Z\}$ je sporná.
Jinými slovy, dokazujeme, že formule $(P_1 \wedge P_2 \wedge ... \wedge P_n) \supset Z$ je tautologie (viz věta 2.1.2, která nás k tomu opravňuje), tedy že její negace $P_1 \wedge P_2 \wedge ... \wedge P_n \wedge \neg Z$ je kontradikce.

Příklad

1) Ověříme platnost úsudku $p \supset q,\ r \vee \neg q,\ \neg r\ /\ \neg p$. Jednotlivé klausule zapíšeme pod sebe (s negovaným závěrem) a uplatňujeme pravidlo rezoluce:

1. $\neg p \vee q$			
2. $r \vee \neg q$			
3. $\neg r$			
4. p		negovaný závěr	
---		alternativně:	
5. q	(1. a 4)	5' $\neg p \vee r$	(1.a 2.)
6. r	(2. a 5.)	6' $\neg p$	(5'a 3.)
7. □	(3. a 6.)	7' □	(6' a 4)

Dostali jsme prázdnou klausuli, která je nesplnitelná. Tedy negovaný závěr je ve sporu s předpoklady, proto je úsudek platný.

2) Ověříme platnost úsudku z kap. 1:

Je doma nebo odešel do kavárny.
Je-li doma, pak nás očekává.

Jestliže nás neočekává, pak odešel do kavárny.

Označíme jednotlivé elementární výroky: d – "je doma", k – "odešel do kavárny", o – "očekává nás" a formalizujeme:

$d \vee k$	1. $d \vee k$	
$d \supset o$	2. $\neg d \vee o$	
---	3. $\neg o$	
$\neg o \supset k$	4. $\neg k$	(klausule 3. a 4. tvoří negovaný závěr $\neg o \wedge \neg k$)
	---	
	5. d	(1. a 4.)
	6. o	(2. a 5.)
	7. □	(3. a 6.)

Dostali jsme prázdnou klausuli, která je nesplnitelná. Tedy negovaný závěr je ve sporu s předpoklady, proto je úsudek platný.

3) Dokažte, že formule $[(p \supset q) \wedge \neg q] \supset \neg p$ je tautologie.

Formuli znegujeme a převedeme do klausulární formy:

$[(\neg p \vee q) \wedge \neg q] \wedge p$

Klausule:

1. $\neg p \vee q$
2. $\neg q$
3. p
4. $\neg p$ rezoluce 1.2.
5. □

Negovaná formule je nesplnitelná, proto je původní formule tautologie.

4) Odvoďte logické důsledky formule $\neg a \downarrow (c \wedge (\neg b \vee a))$, kde $\downarrow$ je Pierceova spojka NOR (negace disjunkce, v přirozeném jazyce "ani, ani"). Formuli převedeme do KNF:
$[\neg a \downarrow (c \wedge (\neg b \vee a))] \Leftrightarrow \neg[\neg a \vee (c \wedge (\neg b \vee a))] \Leftrightarrow [\, a \wedge (\neg c \vee (b \wedge \neg a))] \Leftrightarrow$
$[\, a \wedge (b \vee \neg c) \wedge (\neg a \vee \neg c)]$.

1. a
2. $b \vee \neg c$
3. $\neg a \vee \neg c$
4. $\neg c$ (rezoluce 1 a 3)

Z dané formule vyplývají všechny klausule tvořící KNF a klausule obdržené rezolucí, tedy platí:

$\neg a \downarrow (c \wedge (\neg b \vee a)) \models a$
$\neg a \downarrow (c \wedge (\neg b \vee a)) \models b \vee \neg c$
$\neg a \downarrow (c \wedge (\neg b \vee a)) \models \neg a \vee \neg c$
$\neg a \downarrow (c \wedge (\neg b \vee a)) \models \neg c$

Pozn.: Pokud bychom chtěli obdržet všechny logické důsledky dané formule, museli bychom vycházet z UKNF. V našem případě je UKNF tvořena následujícími disjunkty (ověřte např. z tabulky pravdivostní funkce):

1. $a \vee b \vee c$
2. $a \vee b \vee \neg c$
3. $a \vee \neg b \vee c$
4. $a \vee \neg b \vee \neg c$
5. $\neg a \vee b \vee \neg c$
6. $\neg a \vee \neg b \vee \neg c$

---

7. $a \vee b$ (rezoluce 1, 2)
8. a (rezoluce 2, 3)
9. $a \vee \neg b$ (rezoluce 3, 4)
10. $\neg a \vee \neg c$ (rezoluce 5, 6)
11. $b \vee \neg c$ (rezoluce 7, 10)
12. $\neg c$ (rezoluce 8, 10)

Logickými důsledky naší formule jsou tedy všechny formule 1. až 12.

Vidíme tedy, že na rozdíl od sémantické metody pravdivostních funkcí (metody 0-1) popsané v kapitole 2.1, je rezoluční metoda formální čili syntaktická, tj. nepracuje s pravdivostními modely (s dalšími syntaktickými důkazovými metodami se seznámíme v kap. 2.3 a 2.4). Navíc je dobře zobecnitelná i pro teorémy predikátové logiky (jakož i teorémy libovolných širších formálních teorií, které vždy obsahují predikátovou logiku jako svou část). Tato metoda – *metoda automatického dokazování* – nalezla široké uplatnění v počítačovém dokazování (je na ní, resp. na obecné rezoluci pro predikátovou logiku, založen např. programovací jazyk PROLOG), v expertních systémech a v dalších oblastech umělé inteligence.

Metoda automatického dokazování se opírá o tři principy:

- ***Princip vyvrácení***, převádějící problém důkazu dané formule na problém důkazu nesplnitelnosti negace této formule. Viz věta 2.2.1.
- ***Rezoluční odvozovací pravidlo*** – jediné odvozovací pravidlo používané metodou. Viz věta 2.2.2.
- ***Robinsonův rezoluční princip*** umožňující vyvodit spor z nesplnitelné formule a tak dokázat její nesplnitelnost (a tím dokázat platnost původní formule). Viz věta 2.2.3.

Nyní popíšeme tuto metodu přesněji.

V následující definici zavedeme několik termínů většinou jen nově označujících již dříve zavedené pojmy.

Definice 2.2.1:

Klauzule je konečná disjunkce literálů. Připomeňme, že ***literál*** je výrokový symbol nebo jeho negace. Klauzule je tedy totéž co elementární disjunkce /ED/ - viz definice 2.1.6.

Prázdná klauzule je klauzule, která neobsahuje ani jeden literál. Prázdnou klauzuli označujeme symbolem □.

Hornova klauzule je klauzule s nejvýše jedním pozitivním (nenegovaným) literálem.

Klauzulární forma dané formule je ekvivalentní formule ve tvaru konjunkce klauzulí. Klauzulární forma je tedy totéž, co konjunktivní normální forma /KNF/ dané formule - viz definice 2.1.6.

Poznámky 2.2.1:

1. Vzhledem k asociativitě a komutativitě disjunkce nezáleží na pořadí literálů v klauzuli a klauzuli můžeme také pojímat jako ***disjunktivní množinu literálů***.
2. Vzhledem k tomu. že disjunkce je pravdivá, je-li pravdivý alespoň jeden její člen, představuje prázdná klauzule □ vždy nepravdivou, nesplnitelnou formuli, tj.spor.
3. Klauzuli
$$\neg q_1 \vee \neg q_2 \vee ... \vee \neg q_m \vee p_1 \vee p_2 \vee ... \vee p_n$$
můžeme přepsat, na základě de Morganova zákona, ve tvaru
$$\neg(q_1 \wedge q_2 \wedge ... \wedge q_m) \vee (p_1 \vee p_2 \vee ... \vee p_n)$$
a dále, na základě ekvivalence $\neg A \vee B \Leftrightarrow A \supset B$, ve tvaru implikace
$$(q_1 \wedge q_2 \wedge ... \wedge q_m) \supset (p_1 \vee p_2 \vee ... \vee p_n).$$
Často se používá pro zápis klauzule také následující množinová notace
$$\{q_1,q_2,...,q_m\} \Rightarrow \{p_1,p_2,...,p_n\},$$
kde $\{q_1,q_2,...,q_m\}$ je ***konjunktivní množina antecedentů*** a $\{p_1,p_2,...,p_n\}$ ***disjunktivní množina konsekventů*** klauzule. Klauzule je nepravdivá jedině tehdy, jsou-li všechny antecedenty pravdivé a současně všechny konsekventy nepravdivé.
4. Speciálními případy klauzulí jsou:
   - Klauzule bez antecedentů (m=0):
   $$\{\} \Rightarrow \{p_1, p_2,...,p_n\}, \text{ neboli } 1 \supset (p_1 \vee p_2 \vee ... \vee p_n).$$
   - Klauzule bez konsekventů (n=0), tj. Hornova klauzule se všemi literály negativními:

$$\{q_1,q_2,...,q_m\} \Rightarrow \{\ \}, \text{ neboli } (q_1 \wedge q_2 \wedge ... \wedge q_m) \supset 0.$$

- Klauzule s jediným konsekventem (n=1), tj. Hornova klauzule s jediným pozitivním literálem:

$$\{q_1,q_2,...,q_m\} \Rightarrow \{p_1\}, \text{ neboli } (q_1 \wedge q_2 \wedge ... \wedge q_m) \supset p_1.$$

- Prázdná klauzule (m=n=0):

$$\{\ \} \Rightarrow \{\ \}, \text{ neboli } 1 \Rightarrow 0, \text{ neboli } \square.$$

5. Vzhledem k asociativitě a komutativitě konjunkce nezáleží na pořadí klauzulí v klauzulární formě a klauzulární formu můžeme také pojímat jako ***konjunktivní množinu klauzulí***.
6. Podle věty 2.1.3 o normálním tvaru lze každou formuli výrokové logiky, která není tautologií, vyjádřit ve tvaru UKNF a tedy také KNF, tj. v klauzulární formě.

Věta 2.2.1 /*princip vyvrácení*/:

Formule B vyplývá z předpokladů $A_1, A_2,...,A_n$, značíme $A_1, A_2,..., A_n \models B$, právě tehdy, je-li formule $A_1 \wedge A_2 \wedge ... \wedge A_n \wedge \neg B$ kontradikcí.

Důkaz:

Následující tvrzení jsou ekvivalentní (věta 2.1.2):

1. $A_1, A_2,..., A_n \models B$
2. $A_1 \wedge A_2 \wedge ... \wedge A_n \supset B$ je tautologií
3. $\neg A_1 \vee \neg A_2 \vee ... \vee \neg A_n \vee B$ je tautologií
4. $\neg(A_1 \wedge A_2 \wedge ... \wedge A_n \wedge \neg B)$ je tautologií
5. $A_1 \wedge A_2 \wedge ... \wedge A_n \wedge \neg B$ je kontradikcí

Speciálně pro n=1:

1. $A \models B$
2. $A \supset B$ je tautologií
3. $\neg A \vee B$ je tautologií
4. $\neg(A \wedge \neg B)$ je tautologií
5. $A \wedge \neg B$ je kontradikcí

Věta 2.2.2 /*rezoluční odvozovací pravidlo*/:

Jsou-li splnitelné klausule

$$A_1 \vee A_2 \vee ... \vee A_m \vee L,\ B_1 \vee B_2 \vee ... \vee B_n \vee \neg L,$$

pak je splnitelná také klausule

$$A_1 \vee A_2 \vee ... \vee A_m \vee B_1 \vee B_2 \vee ... \vee B_n,$$

neboli:

$$A_1 \vee A_2 \vee ... \vee A_m \vee L,\ B_1 \vee B_2 \vee ... \vee B_n \vee \neg L \vdash A_1 \vee A_2 \vee ... \vee A_m \vee B_1 \vee B_2 \vee ... \vee B_n.$$

Důkaz: Viz ad 2) v úvodu této kapitoly.

Poznámky 2.2.2:

1. Klauzule na levé straně pravidla nazýváme ***rodičovskými klauzulemi*** a klauzuli na pravé straně ***rezolventou*** rodičovských klauzulí vzhledem k formuli L.

2. Speciálně ***platí***:

- m = 0, n = 0: $L, \neg L \vdash \square$ odvození sporu
- m = 0, n = 1: $L, \neg L \vee B \vdash B$ pravidlo MP
- m = 1, n = 1: $L \vee A, \neg L \vee B \vdash A \vee B$ zákl. tvar rezol. pravidla

Definice 2.2.2:

Nechť F je formule v klauzulárním tvaru (neboli konjunktivní množina klauzulí). Symbolem R(F) označme formuli F rozšířenou o všechny rezolventy všech rezoluce schopných dvojic klauzulí z F. ***Rezolučním uzávěrem formule*** F ***n-tého řádu*** nazveme formuli R_n(F) definovanou rekurzivně takto:

- R_0(F) = F,
- R_i(F) = $R(R_{i-1}$(F)), i=1,2,...,n

Věta 2.2.3 /*Robinsonův rezoluční princip*/:

Formule F v klauzulárním tvaru je kontradikcí (nesplnitelná) právě tehdy, existuje-li přirozené číslo n takové, že R_n(F) obsahuje prázdnou klauzuli $\square$

Důkaz /nástin/:

Důkaz se opírá o následující úvahy:

- Je-li aspoň jedna klauzule ve formuli F kontradikcí, pak je kontradikcí celá formule F.
- Prázdná klauzule $\square = L \wedge \neg L$ je kontradikcí.
- Při použití rezolučního pravidla (rozšíření formule F o rezolventu) se nemění pravdivostní funkce formule F. Metodou pravdivostních funkcí (metodou 0-1) se snadno přesvědčíme, že konjunkce rodičovských klauzulí $(A \vee L) \wedge (B \vee \neg L)$ má stejnou pravdivostní funkci jako konjunkce této konjunkce s rezolventou $(A \vee L) \wedge (B \vee \neg L) \wedge (A \vee B)$. Pravdivostní funkce formulí R_{i-1}(F) a R_i(F) jsou tedy totožné a tedy také pravdivostní funkce formule F a jejího rezolučního uzávěru libovolného řádu.

Příklad 2.2.1:

Dokažme nesplnitelnost následující konjunktivní množiny klauzulí

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

neboli následující konjunktivní normální formy

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

Důkaz:

1.	$p \vee q$	výchozí klauzule			
2.	$p \vee r$	výchozí klauzule			
3.	$\neg q \vee \neg r$	výchozí klauzule			
4.	$\neg p$	výchozí klauzule			
	Systematicky:		Optimálně:		
5.	$p \vee \neg r$	rezoluce: 1,3	5'. q	rezoluce: 1,4	
6.	q	rezoluce: 1,4	6'. r	rezoluce: 2,4	
7.	$p \vee \neg q$	rezoluce: 2,3	7'. $\neg q$	rezoluce: 3,6	
8.	r	rezoluce: 2,4	8'. $\square$	rezoluce: 5,7	Q.E.D.
9.	p	rezoluce: 2,5			
10.	$\neg r$	rezoluce: 3,6			

11. $\neg q$ rezoluce: 3,8
12. $\neg r$ rezoluce: 4,5
13. $\neg q$ rezoluce: 4,7
14. $\square$ rezoluce: 4,9 Q.E.D.

Příklad 2.2.2:

Dokažme, že z platnosti formulí $p \supset q \vee r$, $\neg s \supset \neg q$, $t \vee \neg r$ vyplývá platnost formule $p \supset (s \vee t)$, neboli dokažme platnost odvozovacího pravidla

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \vdash p \supset (s \vee t),$$

neboli - což je totéž - teorémů:

$$\vdash (p \supset q \vee r) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r) \supset [(p \supset (s \vee t)],$$
$$\vdash (p \supset q \vee r) \supset ((\neg s \supset \neg q) \supset ((t \vee \neg r) \supset (p \supset s \vee t))).$$

Podle principu vyvrácení budeme dokazovat, že formule

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

je nesplnitelná.

Formuli převedeme do klauzulárního tvaru

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

a z odpovídající konjunktivní množiny klauzulí

$$\{\neg p \vee q \vee r, s \vee \neg q, t \vee \neg r, p, \neg s, \neg t\}$$

odvodíme (rezolvujeme) spor (prázdnou klauzuli):

1. $\neg p \vee q \vee r$ výchozí klauzule
2. $s \vee \neg q$ výchozí klauzule
3. $t \vee \neg r$ výchozí klauzule
4. p výchozí klauzule
5. $\neg s$ výchozí klauzule
6. $\neg t$ výchozí klauzule
7. $q \vee r$ rezoluce: 1,4
8. $\neg q$ rezoluce: 2,5
9. $\neg r$ rezoluce: 3,6
10. r rezoluce: 7,8
11. $\square$ rezoluce: 9,10 Q.E.D

Poznámky 2.2.4 /strategie generování rezolvent/**:**

1. Generování rezolvent striktně podle Robinsonova rezolučního principu, tj. v posloupnosti F, $R_1(F)$, $R_2(F)$,... , může vést ke kombinatorické explozi a k zdlouhavému odvozování prázdné klauzule. Tato strategie generování rezolvent, tzv. ***generování do šířky***, je značně neefektivní. Efektivnější bývá opačná strategie, tzv. ***generování do hloubky***. (Viz příklad 2.2.5.)
2. Rezoluční metoda se výrazně zefektivní, je-li výchozí množina klauzulí tvořena výhradně Hornovými klauzulemi.
3. K zvýšení efektivnosti (zkrácení) rezolučního procesu byla navržena řada strategií, které stanoví pořadí provádění rezolucí (***strategie uspořádání***) nebo některé klauzule

z rezolučního procesu přímo vylučují (***strategie zjemňování***). Má-li být zvolená strategie ekvivalentní Robinsonovu rezolučnímu principu, musí platit:

- libovolná formule dokázaná při použití dané strategie je skutečně (logicky) pravdivá (strategie je ***korektní***),
- libovolná logicky pravdivá formule je při použití dané strategie dokazatelná (strategie je ***úplná***).

4. Nejpoužívanějšími strategiemi generování rezolvent jsou následující dvě metody:

   - ***Lineární metoda***. Rezolventy se řadí do lineární posloupnosti (v čele této posloupnosti jsou výchozí klauzule) a v každém kroku je jedním účastníkem rezoluce poslední člen této posloupnosti, tj. jednou z rodičovských klauzulí nové rezoluce je vždy rezolventa z předchozí rezoluce.
   - ***Metoda podpůrné množiny***. Předpokládá se, že množina výchozích klauzulí K je rozdělena na podmnožinu A, o které *a priori* víme, že tvoří bezesporný systém (např. je tvořena klauzulemi představující axiómy teorie, v jejímž rámci důkaz hledáme) a z podmnožiny B = K – A (tvořené klauzulemi vzniklými z formulí, které chceme z bezesporného systému axiómů dokázat). Strategie podpůrné množiny spočívá v tom, že nikdy nerezolvujeme klauzule z množiny A navzájem (je-li předpoklad o jejich bezespornosti správný, pak z nich spor neodvodíme a zbytečně ztrácíme čas).

Příklad 2.2.4:

Vyřešíme úlohu zadanou v příkladě 2.2.2 se současným užitím lineární metody a metody podpůrné množiny. Máme dokázat

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \vdash p \supset s \vee t,$$

což znamená dovodit spor z množiny klauzulí /viz přiklad 2.2.2/

$$\{\neg p \vee q \vee r, s \vee \neg q, t \vee \neg r, p, \neg s, \neg t\},$$

kterou můžeme rozdělit na dvě části:

A=$\{\neg p \vee q \vee r, s \vee \neg q, t \vee \neg r\}$ ... bezesporný systém předpokladů,

B=$\{p, \neg s, \neg t\}$ ..... závěr.

Důkaz (odvození sporu):

1.	$\neg p \vee q \vee r$	výchozí klauzule skupiny A
2.	$s \vee \neg q$	výchozí klauzule skupiny A
3.	$t \vee \neg r$	výchozí klauzule skupiny A
4.	p	výchozí klauzule skupiny B
5.	$\neg s$	výchozí klauzule skupiny B
6.	$\neg t$	výchozí klauzule skupiny B
7.	$\neg r$	rezoluce: 3,6
8.	$\neg p \vee q$	rezoluce: 1,7
9.	$\neg p \vee s$	rezoluce: 2,8
10.	s	rezoluce: 4,9
11.	$\square$	rezoluce: 5,10 Q.E.D

Příklad 2.2.5: Strategie prohledávání do hloubky a do šířky.

Uvažujme ”program” – množinu klausulí:

1. D
2. E
3. $B \vee \neg E$
4. $A \vee \neg D$
5. $A \vee \neg B$

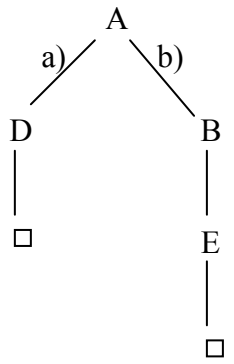
Položíme-li dotaz ”Kdy platí A?” neboli ”Vyplývá z dané množiny A?, pak vlastně připojíme 6. klausuli $\neg A$ a provádíme rezoluci. Máme zde dvě možnosti, jak dokázat A z předpokladů 1.-5.:

a)	7. $\neg D$	(rez. 6.,4.)	b)	7’ $\neg B$	(rez. 6.,5.)
	8. $\square$	(rez. 7.,1.)		8’ $\neg E$	(rez. 7’,3.)
				9 $\square$	(rez. 8’,2)

Pozn.: V programovacím jazyce Prolog bude uvedený program zapsán takto:

D.	fakt
E.	fakt
B :– E.	pravidlo (B pokud E)
A :– D.	pravidlo (A pokud D)
A :– B.	pravidlo (A pokud B)
?A.	cíl (dotaz)

Strategie prohledávání do hloubky spočívá v tom, že provedeme nejprve větev a), tj. zjistíme, že A platí za podmínky D (nový podcíl), která je splněna, a teprve poté (v procesu navracení) větev b), tj. zjistíme, že A platí za podmínky B (další podcíl) a ta platí za podmínky E (podcíl), která je splněna. V případě strategie do šířky se pokoušíme ”splnit obě větve paralelně”, tedy vygenerujeme klausule 7 a 7’, poté 8 a 8’, atd. Vše můžeme znázornit tzv. ***výpočtovým stromem*** programu:



Strategie do hloubky ”prohledá nejprve do hloubky” první větev a pak druhou. Je efektivnější, avšak program může ”uvíznout v tautologii” – nekonečné větvi. Kdybychom např. upravili náš program tak, že bychom přehodili 4. a 5. klausuli a druhou bychom změnili na $E \vee \neg B$, druhá větev b) by se stala nekonečnou a prováděla by se jako první. I když náš cíl A z programu vyplývá, nikdy bychom se to nedověděli.

2.3. Systém přirozené dedukce výrokové logiky

Přirozená dedukce je jednou z metod výstavby formálního systému logiky (podrobně o formálních systémech viz 2.4). Formální systémy logiky můžeme v zásadě rozdělit na systémy axiomatické a předpokladové. Axiomatickými systémy se budeme zabývat v kap. 2.4. a z předpokladových probereme právě jen přirozenou dedukci v alternativě polské, nikoliv gentzenovské. Formální systém je postaven výhradně na syntaktické bázi. To znamená, že jazyk logiky uvažujeme neinterpretovaný a všechny manipulace s ním jsou výhradně syntaktické, na základě odvozovacích pravidel. Takový souhrn nazýváme též ***logický kalkul.***

Tedy formální systém v tomto případě sestává ze dvou složek, a to

- *jazyk* – z jeho symbolů vytváříme konečné posloupnosti – formule (jimž zde nepřisuzujeme žádný smysl)
- *odvozovací pravidla* – operace na formulích, které umožňují ověřování ”platnosti výroků” prostřednictvím konstrukce důkazu.

Cílem tohoto postupu je získat v rámci formálního systému jistou jeho část – formální teorii jako souhrn dokazatelných formulí – ***teorémů.*** Interpretace formální teorie (která není součástí formálního systému) dodává teorii **význam** a činí ji vhodnou pro aplikace v usuzování.

Systém přirozené dedukce vychází z několika jednoduchých dedukčních (odvozovacích) pravidel, která se považují za výchozí a která se proto nedokazují. Na základě těchto výchozích pravidel se pak dokazují další složitější dedukční pravidla. Dedukční pravidla s nulovým počtem předpokladů jsou tzv. ***axiómy*** formálního systému (obdoby tautologií ze sémantického pojetí výrokové logiky). Jako axiómy zde používáme formule tvaru $A \vee \neg A$, popř. $A \supset A$. Pro dobře definovaný ***korektní*** formální systém (výrokové) logiky platí, že množina teorémů je totožná s množinou tautologií, tedy že axiómy jsou logicky pravdivé a odvozovací pravidla zachovávají pravdivost.

Zavedeme nyní přesné pojmy. Základním pojmem je pojem formule výrokové logiky, který zůstává beze změny tak, jak byl zaveden v definici 2.1.1. ***Dedukční pravidlo*** má obecně následující tvar:

$$F_1, F_2,...,F_m \vdash G_1, G_2,...,G_n.$$

Pravidlo ”interpretujeme” takto: ze současné platnosti všech formulí $F_1, F_2,...,F_m$ (předpokladů) plyne platnost libovolné z formulí $G_1, G_2,...,G_n$. Byly-li dokázány všechny formule z levé strany dedukčního pravidla, pak můžeme považovat za dokázánu i libovolnou formuli z pravé strany pravidla.

Definice 2.3.1:

Výchozími (nedokazovanými) dedukčními pravidly jsou:

Axiómy: $\vdash A \vee \neg A, \vdash A \supset A$

Zavedení konjunkce:	$A, B \vdash A \wedge B$	ZK
Eliminace konjunkce:	$A \wedge B \vdash A, B$	EK
Zavedení disjunkce:	$A \vdash A \vee B$ nebo $B \vdash A \vee B$	ZD

Eliminace disjunkce: $A \vee B, \neg A \vdash B$ nebo $A \vee B, \neg B \vdash A$ ED
(disjunktivní sylogismus)

Zavedení implikace: $B \vdash A \supset B$ ZI

Eliminace implikace: $A \supset B, A \vdash B$ EI *modus ponens* **MP**

Zavedení ekvivalence: $A \supset B, B \supset A \vdash A \equiv B$ ZE

Eliminace ekvivalence: $A \equiv B \vdash A \supset B, B \supset A$ EE

Uvedená pravidla ve svém souhrnu charakterizují význam funktorů $\neg, \wedge, \vee, \supset, \equiv$. Pravidlo zavedení implikace se používá zvláštním způsobem, který nazýváme *podmíněný důkaz* (nebo také důkaz z hypotézy), o němž bude řeč dále.

Definice 2.3.2:

Přímý důkaz formule B ***z předpokladů*** $A_1, A_2, \ldots, A_n$ je posloupnost formulí $B_1, B_2, \ldots, B_m$, kde

- každé B_i (i=1, 2,...,m-1) je:
  - rovno A_j pro některé $j \in \{1, 2, \ldots, n\}$ (předpoklad) nebo
  - axiom tvaru $(A \supset A)$ či $(\neg A \vee A)$
  - formule vzniklá užitím odvozovacích pravidel na předcházející členy posloupnosti,
- $B_m = B$.

Pozn.:

1. Jako členy důkazové posloupnosti můžeme použít rovněž takové formule, o kterých víme, že jsou to teorémy (byly již dokázány). Důkaz tím zkrátíme a zpřehledníme, neboť již neopakujeme znovu celou důkazovou sekvenci dříve dokázaného teorému.
2. Je-li $n = 0$, pak hovoříme o (*obyčejném*) ***přímém důkazu bez předpokladů***, kdy nelze stanovit předpoklady. Takový důkaz musí zřejmě začínat nějakým vhodným axiomem (např. $p \supset p$).
3. Má-li dokazovaná formule A tvar implikace, tj.
   $A_1 \supset \{A_2 \supset [A_3 \supset \ldots \supset (A_n \supset B) \ldots]\}$, (*)
   pak dle věty o dedukci (viz dále věta 2.3.1) můžeme provést přímý důkaz formule A tak, že dokážeme formuli B z předpokladů $A_1, A_2, A_3, \ldots, A_n$.
4. Má-li dokazovaná formule A tvar implikace (*), pak můžeme provést ***nepřímý důkaz (sporem) formule*** A: Nepřímý důkaz je posloupnost formulí $B_1, B_2, \ldots, B_m$, kde
   - $B_i = A_i$ pro i=1, 2,...,n /předpoklady/,
   - $B_{n+1} = \neg B$ a je-li $B = \neg C$, pak $B_{n+1} = C$ (předpoklad nepřímého důkazu),
   - B_i pro i=n+2, n+3,...,m-1 jsou:
     - dříve dokázané formule,
     - formule vzniklé užitím odvozovacích pravidel na předcházející členy posloupnosti,
   - $B_m = \neg B_k$ pro nějaké $k < m$ /spor/.

Teorém (***dokazatelná formule***) výrokové logiky je formule výrokové logiky k níž existuje důkaz bez předpokladů (tedy pouze z axiomu $A \vee \neg A$, popř. $A \supset A$). Skutečnost, že formule A je teorémem označujeme zápisem $\vdash A$. Skutečnost, že formule A je dokazatelná z předpokladů $A_1, A_2, \ldots, A_n$ označujeme zápisem $A_1, A_2, \ldots, A_n \vdash A$.

Příklad 2.3.1:

a) Teorém: $[(p \supset q) \wedge (q \supset r)] \supset (p \supset r)$
Důkaz /přímý/:

1.	$(p \supset q) \wedge (q \supset r)$	předpoklad	
2.	p	předpoklad	
3.	$p \supset q$	EK:1	
4.	$q \supset r$	EK:1	
5.	q	MP:3,2	
6.	r	MP:4,5	Q.E.D.

Tedy: $\vdash [(p \supset q) \wedge (q \supset r)] \supset (p \supset r)$

b) Teorém: $(p \supset q) \supset [(q \supset r) \supset (p \supset r)]$
Důkaz /přímý/:

1.	$p \supset q$	předpoklad	
2.	$q \supset r$	předpoklad	
3.	p	předpoklad	
4.	q	MP:1,3	
5.	r	MP:2,4	Q.E.D.

Tedy: $\vdash (p \supset q) \supset [(q \supset r) \supset (p \supset r)]$

c) Teorém: $(p \supset q) \supset (\neg q \supset \neg p)$
Důkaz /nepřímý/:

1.	$p \supset q$	předpoklad	
2.	$\neg q$	předpoklad	
3.	p	předpoklad nepřímého důkazu	
4.	q	MP:1,3	spor:2

Tedy: $\vdash (p \supset q) \supset (\neg q \supset \neg p)$

d) Slovní příklad:
Jsou známa následující fakta:
(1) A/dam/, B/edřich/ a C/yril/ jsou p/rogramátor/, t/echnik/ a v/ýzkumník/, ale nikoliv nutně v uvedeném pořadí. Každý má právě jednu profesi.
(2) Adam je starší než výzkumník.
(3) Technik je Adamův nejlepší přítel.
(4) Výzkumník dluží Bedřichovi 100Kč.
Kdo je kým?

Řešení:

1.	$\neg$(A je v)	předpoklad: (2)
2.	$\neg$(A je t)	předpoklad: (3)
3.	$\neg$(B je v)	předpoklad: (4)
4.	$\neg$(A je v) $\wedge$ $\neg$(A je t)	ZK:1,2
5.	$\neg$(A je v) $\wedge$ $\neg$(B je v)	ZK:1,3
6.	$\neg$(A je v) $\wedge$ $\neg$(A je t) $\supset$ (A je p)	předpoklad: (1)
7.	$\neg$(A je v) $\wedge$ $\neg$(B je v) $\supset$ (C je v)	předpoklad: (1)
8.	(A je p)	MP:6,4
9.	(C je v)	MP:7,5

10. (A je p) $\wedge$ (C je v)	ZK:8,9
11. (A je p) $\wedge$ (C je v) $\supset$ (B je t)	předpoklad: (1)
12. (B je t)	MP:11,10

Věta 2.3.1 /o dedukci/**:**

$$A_1, A_2,..., A_n \vdash B \qquad /**/$$

právě tehdy, je-li

$$A_1, A_2, \ldots, A_{n-1} \vdash A_n \supset B \qquad /*/$$

Aplikujeme-li větu o dedukci *n*-krát, dostaneme, že /*/ platí právě tehdy, když

$$\vdash A_1 \supset \{A_2 \supset [A_3 \supset ... \supset (A_n \supset B)..]\} \quad /***/$$

Důkaz:

Kvůli názornosti zapíšeme důkaz pro n = 2. Zobecnění důkazu pro libovolné n je nasnadě. Dokazujeme tedy:

$$\vdash A_1 \supset (A_2 \supset B) \text{ právě tehdy, je-li } A_1, A_2 \vdash B$$

1. Nechť platí $\vdash A_1 \supset (A_2 \supset B)$ /*/, dokážeme $A_1, A_2 \vdash B$ /**/:

(1) A_1	1. předpoklad /**/
(2) A_2	2. předpoklad /**/
(3) $A_1 \supset (A_2 \supset B)$	věta /*/, jejíž platnost se přepokládá
(4) $A_2 \supset B$	použití MP na (3) a (1)
(5) B	použití MP na (4) a (2), /**/ dokázáno

2. Nechť platí /**/, dokážeme /*/:

(1) A_1	1. předpoklad /*/
(2) A_2	2. předpoklad /*/
(3) B	použití /**/ na (1) a (2), /*/ dokázáno

Poznámka 2.3.1:

Z teorému tvaru /***/ věty 2.3.1 lze formulovat *n* odvozovacích pravidel:

$$A_1 \vdash A_2 \supset [A_3 \supset ... \supset (A_n \supset B)]$$
$$A_1, A_2 \vdash A_3 \supset ... \supset (A_n \supset B)$$
$$.....$$
$$A_1, A_2, A_3, ...,A_{n-1} \vdash A_n \supset B$$
$$A_1, A_2, A_3, ...,A_{n-1}, A_n \vdash B$$

Příklad 2.3.2:

Z teorému $\vdash (p \supset q) \supset [(q \supset r) \supset (p \supset r)]$ dokázaného v příkladu 2.3.1 plyne platnost následujících odvozovacích pravidel:

$p \supset q \vdash (q \supset r) \supset (p \supset r)$

$p \supset q, q \supset r \vdash p \supset r$ pravidlo tranzitivity implikace

Z teorému $\vdash (p \supset q) \supset (\neg q \supset \neg p)$ dokázaného v příkladu 2.3.1 plyne platnost následujících odvozovacích pravidel:

$p \supset q \vdash \neg q \supset \neg p$ pravidlo transpozice

$p \supset q, \neg q \vdash \neg p$ pravidlo modus tollens

Věta 2.3.2:

Následující odvozovací pravidla jsou platná:

Zavedení negace:	$A \vdash \neg\neg A$	ZN
Eliminace negace:	$\neg\neg A \vdash A$	EN
Negace disjunkce:	$\neg(A \vee B) \vdash \neg A \wedge \neg B$	ND
Negace konjunkce:	$\neg(A \wedge B) \vdash \neg A \vee \neg B$	NK
Negace implikace:	$\neg(A \supset B) \vdash A \wedge \neg B$	NI
Tranzitivita implikace:	$A \supset B, B \supset C \vdash A \supset C$	TI
Transpozice:	$A \supset B \vdash \neg B \supset \neg A$	TR
Modus tollens:	$A \supset B, \neg B \vdash \neg A$	MT

Důkaz:

Pravidla TI, TR, MT byla již dokázána v příkladech 2.3.1 a 2.3.2.

Na ukázku dokážeme ještě pravidlo ND /negace disjunkce/. Dokázat pravidlo ND je podle věty 2.3.1 totéž jako dokázat teorém

$$\neg(A \vee B) \supset \neg A \wedge \neg B.$$

Tento teorém dokážeme pomocí teorémů: $\neg(A \vee B) \supset \neg A$, $\neg(A \vee B) \supset \neg B$.

- Teorém: $\neg(A \vee B) \supset \neg A$

  Důkaz: 1. $\neg(A \vee B)$ předpoklad
  2. A předpoklad nepřímého důkazu
  3. $A \vee B$ ZD:2 spor:1 Q.E.D.

- Teorém $\neg(A \vee B) \supset \neg B$ se dokáže obdobně.

- Teorém: $\neg(A \vee B) \supset \neg A \wedge \neg B$

  Důkaz: 1. $\neg(A \vee B)$ předpoklad
  2. $\neg(A \vee B) \supset \neg A$ dříve dokázaný teorém
  3. $\neg(A \vee B) \supset \neg B$ dříve dokázaný teorém
  4. $\neg A$ MP:2,1
  5. $\neg B$ MP:3,1
  6. $\neg A \wedge \neg B$ ZK:4,5 Q.E.D.

Věta 2.3.3 (věta o **korektnosti a úplnosti** systému přirozené dedukce):

Každá formule dokazatelná v systému přirozené dedukce je tautologií a obráceně každá tautologie je dokazatelnou formulí (teorémem) systému přirozené dedukce. Neboli:

$$\models A \text{ právě tehdy, je-li } \vdash A$$

Důkaz:

Třeba dokázat:

1. Je-li $\vdash A$, pak také $\models A$. (korektnost)
2. Je-li $\models A$, pak také $\vdash A$. (úplnost)

Platnost prvého tvrzení vyplývá ze snadno prověřitelné skutečnosti, že všechna základní odvozovací pravidla (viz definice 2.3.1) mají tuto vlastnost: jsou-li všechny formule na levé straně tautologiemi, pak také každá formule na pravé straně je tautologií – tedy pravidla **zachovávají pravdivost**.

Důkaz druhého tvrzení je obtížnější, provedeme v kap. 2.4 pro Hilbertův systém.

Příklad 2.3.5:

- Teorém: $(p \supset r) \supset (\neg p \vee r)$

1.	$p \supset r$	předpoklad
2.	$\neg(\neg p \vee r)$	předpoklad nepřímého Dk.
3.	$\neg(\neg p \vee r) \supset (\neg\neg p \wedge \neg r)$	Teorém ND (de Morgan)
4.	$\neg\neg p \wedge \neg r$	MP: 2.3.
5.	$p \wedge \neg r$	EN: 4.
6.	p	
7.	$\neg r$	EK
8.	r	MP: 1.6. – spor, tedy
9.	$\neg p \vee r$	Q.E.D.

Příklad 2.3.6:

- Teorém: $[(p \supset r) \wedge (q \supset r)] \supset [(p \vee q) \supset r]$

1.	$[(p \supset r) \wedge (q \supset r)]$	předpoklad
2.	$(p \supset r)$	EK: 1
3.	$(q \supset r)$	EK: 1
4.	$p \vee q$	předpoklad
5.	$(p \supset r) \supset (\neg p \vee r)$	Teorém (Příklad 2.3.4)
6.	$\neg p \vee r$	MP: 2.5.
7.	$\neg r$	předpoklad nepřímého Dk.
8.	$\neg p$	ED: 6.7.
9.	q	ED: 4.8.
10.	r	MP: 3.9. – spor s 7., tedy
11.	r	Q.E.D

Technika hypotetických předpokladů (podmíněný důkaz):

V posloupnosti formulí tvořících důkaz může být za počáteční skupinou řádných předpokladů A_1, A_2, ..., A_n uveden další hypotetický předpoklad H. Jestliže na základě hypotetického a případně některých řádných předpokladů lze odvodit formuli D, pak formule $H \supset D$ může být připojena k řádnému důkazu jako teorém. Jestliže odvozená formule D je ve sporu s některým řádným předpokladem (je jeho negací), pak formuli $\neg H$ můžeme v důkaze použít jako větu.

Příklad 2.3.7:

- Teorém: $[(p \vee q) \supset r] \supset [(p \supset r) \wedge (q \supset r)]$

Přímý důkaz technikou hypotetických předpokladů:

1.	$(p \vee q) \supset r$	předpoklad	
	2.1. p	hypotéza	
	2.2. $p \vee q$	ZD:2.1	
	2.3. r	MP:1,2.2	
3.	$p \supset r$	ZI: $2.1 \supset 2.3$	
	4.1. q	hypotéza	
	4.2. $p \vee q$	ZD:4.1	
	4.3. r	MP:1,4.2	
5.	$q \supset r$	ZI: $4.1 \supset 4.3$	
6.	$(p \supset r) \wedge (q \supset r)$	ZK:3,5	Q.E.D

- Teorém: $\neg(p \vee q) \supset \neg p \wedge \neg q$

Nepřímý důkaz technikou hypotetických předpokladů:

1.	$\neg(p \vee q)$	předpoklad	
	2.1. p	hypotéza	
	2.2. $p \vee q$	ZD: 2.1	spor:1
3.	$\neg p$	neboť p vede ke sporu	
	4.1. q	hypotéza	
	4.2. $p \vee q$	ZD: 4.1	spor:1
4.	$\neg q$	neboť q vede ke sporu	
5.	$\neg p \wedge \neg q$	ZK: 3,4	Q.E.D.

Technika větveného důkazu z hypotéz:

Nechť v posloupnosti formulí tvořících důkaz dané formule se nachází formule ve tvaru disjunkce $C_1 \vee C_2 \vee ... \vee C_k$. Jestliže lze danou formuli dokázat na základě každého dodatečného předpokladu C_1, C_2,...,C_k, pak je daná formule dokázána. Vyskytuje-li se disjunkce dodatečných předpokladů v nepřímém důkaze a vede-li každý dodatečný předpoklad ke sporu, pak je daná formule dokázána (nepřímý důkaz dokončen). @

Příklad 2.3.8:

- Teorém: $(p \supset q) \supset [(p \vee r) \supset (q \vee r)]$

Přímý důkaz technikou větveného důkazu:

1.	$p \supset q$	předpoklad	
2.	$p \vee r$	předpoklad, disjunkce případů	
	3.1. p	hypotéza 1.případu	
	3.2. q	MP: 1, 3.1	
	3.3. $q \vee r$	ZD: 3.2	
3.	$p \supset q \vee r$	ZI	
	4.1. r	hypotéza 2.případu	
	4.2. $q \vee r$	ZD: 4.1	
4.	$r \supset q \vee r$	ZI	
5.	$(p \supset q \vee r) \wedge (r \supset q \vee r)$	ZK: 3.4.	
6.	$(p \vee r) \supset (q \vee r)$	Teorém: Příklad 2.3.6	Q.E.D.

- Teorém: $[(p \supset q) \wedge (r \supset s) \wedge \neg(q \vee s)] \supset \neg(p \vee r)$

Nepřímý důkaz technikou větveného důkazu:

1.	$p \supset q$	předpoklad	
2.	$r \supset s$	předpoklad	
3.	$\neg(q \vee s)$	předpoklad	
4.	$p \vee r$	předpoklad nepřímého důkazu ve tvaru disjunkce	
	5.1. p	1. hypotéza	
	5.2. q	MP: 1, 5.1	
	5.3. $q \vee s$	ZD: 5.2, spor:3	Q.E.D.
	6.1. r	2. hypotéza	
	6.2. s	MP: 2, 6.1	
	6.3. $q \vee s$	ZD: 6.2, spor:3	Q.E.D.

- Provedeme důkaz **pravidla rezoluce** (viz 2.2). Bez újmy na obecnosti stačí dokázat pravidlo v základním tvaru $[(L \vee A) \wedge (\neg L \vee B)] \supset (A \vee B)$:

  1. $L \vee A$ předpoklad
  2. $\neg L \vee B$ předpoklad
  3. $L \vee \neg L$ teorém, disjunkce případů
     - 4.1. L hypotéza, 1. případ
     - 4.2. $\neg\neg L$ ZN: 4.1
     - 4.3. B ED: 2, 4.2
     - 4.4. $A \vee B$ ZD: 4.3 Q.E.D.
     - 5.1. $\neg L$ hypotéza, 2. případ
     - 5.2. A ED: 1, 5.1
     - 5.3. $A \vee B$ ZD: 5.2 Q.E.D.

  (Srovnej se sémantickým důkazem v úvodu kap. 2.2.)

Poznámka 2.3.2:

Gentzenův systém přirozené dedukce (Gentzenovský výrokový kalkul) vychází z jediného axiómu, a to $A \supset A$ (resp. $\neg A \vee A$). Pravidla jsou pak obdobná jako v polském systému přirozené dedukce. Gentzenův důkaz tautologie získáme poměrně snadno tak, že formuli převedeme do KNF, zobrazíme tento převod ve formě stromu a důkaz pak začíná od ”listů” stromu.

Příklad 2.3.5:

Dokažme tautologii $[(p \supset q) \wedge \neg q] \supset \neg p$

$[(p \supset q) \wedge \neg q] \supset \neg p \Leftrightarrow (p \wedge \neg q) \vee q \vee \neg p \Leftrightarrow (p \vee q \vee \neg p) \wedge (\neg q \vee q \vee \neg p)$

Důkaz:

1. $p \vee \neg p$ axiom
2. $p \vee \neg p \vee q$ 1. ZD
3. $q \vee \neg q$ axiom
4. $q \vee \neg q \vee \neg p$ 3. ZD
5. $(p \wedge \neg q) \vee q \vee \neg p$ 2.,4. ZK

atd. s využitím již dokázaných teorémů.

2.4. Axiomatický systém výrokové logiky

2.4.a. Obecná charakteristika formálních systémů.

Formální axiomatický systém libovolné teorie (a speciálně také výrokové logiky) je zadán trojicí údajů:

- jazykem,
- množinou axiómů,
- množinou odvozovacích pravidel.

Jazyk teorie je množina všech (dobře utvořených) formulí jazyka. ***Množina axiómů*** teorie je vybraná podmnožina množiny všech formulí. Axiómy představují základní teorémy teorie, které jsou považovány za výchozí. ***Odvozovací pravidla*** umožňují odvozovat (dokazovat) nové ***teorémy*** na základě axiómů a teorémů již dokázaných. ***Formální teorie*** (v širším slova smyslu) je tvořena axiómy a všemi formulemi, které lze z nich pomocí odvozovacích pravidel odvodit. Formální teorie je ***deduktivním uzávěrem*** množiny axiómů, kterou proto někdy nazýváme teorií v užším slova smyslu. Označíme-li jednotlivé zmiňované množiny jako A – množina axiómů (teorie v užším slova smyslu, "v kostce"), T – množina teorémů (teorie v širším slova smyslu), DUF – množina všech dobře utvořených formulí (tj. jazyk) a S – množina všech slov v abecedě jazyka, pak platí následující vztahy:

$$A \subset T \subset DUF \subset S.$$

Postup budování axiomatické teorie (formálního systému či logického kalkulu) tedy sestává z těchto kroků:

1) Vymezení jazyka teorie, který je dán
   a. abecedou
   b. gramatikou – pravidla, jak tvořit DUF
2) Výběr jisté (vlastní) podmnožiny formulí jako axiómů
3) Stanovení pravidel odvozování
4) Demonstrace bezespornosti (korektnosti) teorie, tj. axiómů a pravidel
5) Interpretace formulí

ad 2) Množina axiómů je vždy neprázdná a musí být rozhodnutelná v množině DUF (jinak bychom nemohli v takovém systému nic dokazovat). To znamená, že existuje algoritmus, který pro každou DUF určí, zda je to axióm nebo ne. Může být konečná nebo nekonečná. Konečná množina axiómů je triviálně rozhodnutelná. Nekonečné množiny axiómů musí být charakterizovány algoritmem vytváření axiómů, nebo častěji konečnou množinou tzv. ***axiómových schémat***. Axiómy jsou voleny tak, aby byly pravdivé v každé interpretaci – *tautologie*. Navíc stanovujeme tzv. **speciální axiómy,** které charakterizují přímo danou teorii (např. aritmetiku přirozených čísel – viz kap. 4), a ty volíme tak, aby byly *pravdivé v zamýšlené interpretaci teorie*. (Výroková logika či predikátová logika 1. řádu – viz kap.3.4. – mohou být tedy považovány za teorie bez speciálních axiómů – ***logické kalkuly***.)

ad 3) Množina odvozovacích pravidel je tvořena několika nebo dokonce jen jedním pravidlem (jsou-li axiómy reprezentovány schématy). Tím se liší axiomatický systém od (polského) systému přirozené dedukce, který pracuje sice s prázdnou množinou axiómů, ale zato s podstatně větším počtem dedukčních pravidel. Odvozovací pravidla převádějí DUF na DUF a jsou volena tak, aby byla sémanticky ***korektní***, tj. aby "zachovávala pravdivosť" (jinak bychom obdrželi nekorektní systém, ve kterém je možno dokázat vše, a takový systém jistě není z praktického hlediska užitečný). Odvozovací pravidla tedy umožňují vytvářet teorémy, tj. dokazatelné formule. **Důkaz** je konečná posloupnost kroků – DUF, z nichž každá je buď axióm nebo vznikne z předchozích DUF pomocí odvozovacího pravidla. Posledním krokem je dokazovaná formule – teorém.

Někdy bývá stanoven ještě jeden přirozený "kosmetický" požadavek na množinu axiómů: Množina axiómů má být **nezávislá,** tj. žádný axióm není dokazatelný z ostatních axiómů.

ad 4) Přirozeným požadavkem je (syntaktická) **bezespornost (konzistence):** Alespoň jedna formule není dokazatelná (ve sporném systému dokážeme vše). (Ekvivalentním požadavkem v systémech obsahujících $\neg$, $\wedge$ je to, že není dokazatelná formule typu $A \wedge \neg A$, případně v systémech s $\neg$, $\supset$ formule typu $\neg(A \supset A)$.) S tímto souvisí rovněž sémantická bezespornost, neboli **korektnost** systému: Každý teorém je logicky pravdivá formule (v případě teorie bez speciálních axiómů), nebo logicky vyplývá ze speciálních axiómů (předpokladů). Tedy "to, co dokážeme, je pravdivé". Označíme-li množinu speciálních axiómů jako SA, můžeme požadavek korektnosti zapsat schematicky:
Jestliže $\vdash T$ pak $\models T$, resp. jestliže $SA \vdash T$ pak $SA \models T$.

Problém. Je dokazatelnost totéž co (logická) pravdivost? Jinými slovy, jsou dokazatelné **přesně** ty výroky, které jsou (logicky) pravdivé? Tímto problémem se budeme podrobně zabývat v kapitole 4, nyní jen stručně naznačíme. D. **Hilbert** (význačný matematik počátku 20. století) očekával kladnou odpověď na výše uvedené otázky a vytyčil tzv. program axiomatizace matematiky. Kurt **Gödel** (největší logik 20. století) dokázal **věty o úplnosti,** které dávají pozitivní odpověď na tyto otázky (pro výrokovou logiku a) pro predikátovou logiku 1. řádu (viz kap. 3), tedy "obrácené" tvrzení ke korektnosti:

Jestliže $\models T$ pak $\vdash T$, resp. jestliže $SA \models T$ pak $SA \vdash T$ (tzv.silná věta o úplnosti).

Hilbert však očekával ještě více, a to že všechny "matematické pravdy" lze "mechanicky" finitně dokázat (z vhodných axiomů), tedy že takové bezesporné teorie, které charakterizují aritmetiku přirozených čísel (např. Peanova aritmetika), jsou úplné v tom smyslu, že každá formule je v dané teorii **rozhodnutelná,** tj. na základě axiomů teorie můžeme dokázat buďto danou formuli nebo její negaci. Tedy že všechny formule, které jsou **pravdivé v** zamýšlené **interpretaci** nad množinou přirozených čísel jsou v této teorii dokazatelné.

Gödelovy **věty o neúplnosti** dávají velice překvapivou odpověď – existují **pravdivé leč nedokazatelné výroky aritmetiky** přirozených čísel. Tedy Hilbertův program není (v plné šíři) uskutečnitelný.

S (ne)úplností úzce souvisí problém **rozhodnutelnosti**: Existuje algoritmus, který o libovolné dobře utvořené formuli určí, zda je to teorém (dokazatelná DUF) čili (v korektním systému) logicky pravdivá formule?

Dá se dokázat a v dalších kapitolách ukážeme pro VL a PL^1, že

- pro výrokovou logiku lze vyvinout kalkuly, které jsou
  - bezesporné
  - úplné
  - rozhodnutelné
- pro predikátovou logiku 1. řádu lze vyvinout kalkuly, které jsou
  - bezesporné
  - úplné
  - jen parciálně rozhodnutelné (tj. pokud daná DUF je tautologie, pak algoritmus po konečném počtu kroků odpoví ANO, jinak nemusí vydat žádnou odpověď – může "cyklovat" či odpoví NE)
  - nelze vyvinout rozhodnutelný kalkul pro PL^1 (problém **logické pravdivosti je v PL^1 nerozhodnutelný)**
- pro predikátovou logiku 2. řádu (a vyšších) lze vyvinout
  - bezesporné kalkuly, ale každý takový je:
  - neúplný
  - nerozhodnutelný (ani parciálně)

Axiomatických systémů výrokové a predikátové logiky bylo vytvořeno velké množství. Liší se navzájem jazykem, množinou axiómů i odvozovacími pravidly. Všechny však představují jenom různé formalizace "intuitivní logiky". Všechny formalizace mají společnou vlastnost: Jsou korektní (každá dokazatelná formule /logický teorém axiomatického systému/ musí být tautologií). V tomto smyslu jsou všechny formalizace ekvivalentní.

K charakteristice dokazatelnosti byly vytvořeny dva typy formálních systémů:

a) Gentzenova typu
b) Hilbertova typu

Gentzenův systém přirozené dedukce je obdobný systému polskému, který jsme probrali v předchozí kapitole 2.3, vychází však z jediného (schématu) axiómu, a to $A \vee \neg A$ (resp. $A \supset A$) a pravidel obdobných polskému systému. Nebudeme jej zde podrobně probírat. Budeme se nyní (a v kap. 3.4) zabývat systémem Hilbertova typu.

2.4.b. Formální systém Hilbertova typu

Definice 2.4.1 /definice konkrétního axiomatického systému/:

- ***Jazyk***:
  - **Abeceda:**
    Výrokové symboly: p, q, r,... /případně s indexy/
    Logické funktory: $\neg, \supset$
    Závorky: (,) /případně [,],{,}/
  - **Gramatika (DUF)**:
    (1) p, q, r,... jsou formule.
    (2) Je-li A formule, pak $(\neg A)$ je formule.
    (3) Jsou-li A,B formule, pak $(A \supset B)$ je formule.
    (4) Jiných formulí než podle (1), (2), (3) není.
  - **Jazyk**: množina všech (dobře utvořených) formulí.
- ***Axiómová schémata***: A1: $A \supset (B \supset A)$
  A2: $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
  A3: $(\neg B \supset \neg A) \supset (A \supset B)$
- ***Odvozovací pravidlo***: MP: $A, A \supset B \vdash B$

Poznámky 2.4.1:

1. A, B nejsou formulemi, ale metasymboly sloužícími k označení formulí. Každé axiómové schéma označuje nekonečnou třídu axiómů daného tvaru. Kdybychom axiómová schémata nahradili axiómy
   1. $p \supset (q \supset p)$
   2. $(p \supset (q \supset r)) \supset ((p \supset q) \supset (p \supset r))$
   3. $(\neg q \supset \neg p) \supset (p \supset q)$

   museli bychom rozšířit množinu odvozovacích pravidel o další pravidlo, tzv. pravidlo substituce, abychom získali ekvivalentní axiomatický systém. ***Pravidlo substituce*** zní:
   Dosadíme-li v dokázané formuli za jednotlivé výrokové symboly jakékoliv jiné formule (za každý výskyt téhož výrokového symbolu vždy tutéž formuli), pak získáme opět dokázanou formuli (teorém).
2. Definovaný axiomatický systém pracuje pouze s funktory $\neg, \supset$. Vzhledem k tomu, že pravdivostní funkce příslušné k těmto funktorům tvoří funkcionálně úplný systém (viz věta 2.1.8), postačí tyto funktory k vytvoření sémanticky úplné logiky. Ostatní výrokotvorné funktory můžeme používat jako zkratky (zkracující a zpřehledňující zápis formulí) definované takto:
   $$A \wedge B =_{df} \neg(A \supset \neg B)$$
   $$A \vee B =_{df} \neg A \supset B$$
   $$A \equiv B =_{df} (A \supset B) \wedge (B \supset A)$$
   Symboly $\wedge, \vee, \equiv$ nepatří do jazyka definovaného axiomatického systému, jsou to metasymboly sloužící k označování složených formulí jistého typu.
3. Při psaní formulí lze vyžívat konvencí šetřících závorky – viz poznámka k definici 2.1.1.

Definice 2.4.2:

Důkaz formule A ***za předpokladů*** $A_1, A_2, ..., A_k$ /k ≥ 0/ je konečná posloupnost formulí $B_1, B_2,...,B_n$ taková, že:

- Pro i = 1, 2,...,n-1 je B_i
  1. buď předpoklad A_j (j ∈ {1,…,k})
  2. nebo axióm
  3. nebo formule, která vznikla aplikací pravidla MP na některé dvě formule z množiny $\{B_1, B_2,...,B_{i-1}\}$.
- B_n je dokazovaná formule A.

Skutečnost, že formule A je dokazatelná za předpokladů $A_1, A_2, ..., A_k$ označujeme zápisem $\mathbf{A_1, A_2, ..., A_k \vdash A}$.

Důkaz formule A je důkaz s prázdnou množinou předpokladů (k = 0). Neboli, *důkaz formule A* je důkaz pouze z (logických) axiómů daného systému.

Teorém je formule, pro kterou existuje důkaz (s prázdnou množinou předpokladů). Skutečnost, že formule A je teorémem označujeme zápisem $\vdash \mathbf{A}$.

Poznámky 2.4.2:

1. Hilbertův systém je **korektní**, tedy sémanticky bezesporný.
   a) Především, snadno ověříme, že všechny axiómy systému jsou ***tautologie***.
   b) Jediné pravidlo systému (MP) "***zachovává pravdivost***" v tom smyslu, že formule B, která vznikne aplikací pravidla na formule A_1, A_2 z těchto formulí logicky vyplývá. Tedy platí: Pokud $A_1, A_2 \vdash B$, pak $A_1, A_2 \models B$.
   Viz věta 2.4.4. – Postova.
2. Všimněme si, že z definice důkazu vyplývá, že i axióm je teorémem. Jeho důkaz je triviální: důkazem axiómu je axióm sám.
3. Důkaz $B_1, B_2,...,B_n$ formule A za předpokladů $A_1, A_2, ..., A_k$ je nejenom důkazem formule $A = B_n$, ale obsahuje i důkazy $B_1, B_2,...,B_i$ všech formulí B_i pro i = 1,2, ..., n-1.
4. Pro zkrácení důkazu můžeme použít jako kroky důkazu rovněž (kromě axiómů) dříve dokázané teorémy.

Příklady 2.4.1:

1. Důkaz formule /schématu formulí/ A ⊃ A:

1. (A ⊃ ((A ⊃ A) ⊃ A)) ⊃ ((A ⊃ (A ⊃ A)) ⊃ (A ⊃ A))	ax. A2	B/A ⊃ A, C/A
2. A ⊃ ((A ⊃ A) ⊃ A)	ax. A1	B/A ⊃ A
3. (A ⊃ (A ⊃ A)) ⊃ (A ⊃ A)	MP:2,1	
4. A ⊃ (A ⊃ A)	ax. A1	B/A
5. A ⊃ A	MP:4,3	Q.E.D.

V 1. formuli důkazu je použito ax.schéma A2, kde B je A ⊃ A a C je A, v 2. formuli je použito ax.schéma A1, kde B je A ⊃ A a ve 4.formuli je použito ax.schéma A1, kde B je A.

Tedy: $|- A \supset A$.

2. Důkaz formule $A \supset C$ za předpokladů $A \supset B$, $B \supset C$:

1. $A \supset B$	1.předpoklad	
2. $B \supset C$	2.předpoklad	
3. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$	A2	
4. $(B \supset C) \supset (A \supset (B \supset C))$	A1	$A/(B \supset C)$, B/A
5. $A \supset (B \supset C)$	MP:2,4	
6. $(A \supset B) \supset (A \supset C)$	MP:5,3	
7. $A \supset C$	MP:1,6	Q.E.D.

Tedy: $A \supset B, B \supset C |- A \supset C$.

Z uvedených příkladů je zřejmé, že nalezení důkazů, a to i velmi jednoduchých teorémů a dedukčních pravidel, nemusí být přímočaré. To souvisí s tím, že v axiomatickém systému jsou zpravidla minimalizovány počet axiómů a počet odvozovacích pravidel na počty nezbytně nutné. S přibývajícím množstvím dokázaných teorémů a odvozených odvozovacích pravidel se však neustále zlepšují možnosti pro hledání důkazů.

Věta 2.4.1 /o dedukci/:

$A_1, A_2,...,A_k |- A \supset B$ právě tehdy, když $A_1, A_2,...,A_k, A |- B$.

(Speciálně pro k=0: $|- A \supset B$ právě tehdy, když $A |- B$.)

Důkaz:

1. Nechť $A_1, A_2,...,A_k |- A \supset B$. Tedy existuje posloupnost formulí $B_1, B_2,...,B_n$, která je důkazem formule $A \supset B$ z předpokladů $A_1,A_2,...,A_k$. Důkazem formule B z předpokladů $A_1, A_2,...,A_k$, A bude pak posloupnost formulí $B_1, B_2,...,B_n$, A, B , kde $B_n = A \supset B$ a B je výsledkem aplikace pravidla MP na formule B_n a A.

2. Nechť $A_1, A_2,...,A_k$, $A |- B$. Tedy existuje posloupnost formulí $C_1,C_2,...,C_r = B$, která je důkazem formule B z předpokladů $A_1,A_2,...,A_k$, A. Dokážeme, že formule $A \supset C_i$ je platná pro všechna i = 1, 2,...,r. Tím bude speciálně dokázáno také $A \supset C_r$, což chceme dokázat. Důkaz provedeme matematickou indukcí podle délky důkazu.

   a) Je-li délka důkazu 1, pak pro jedinou formuli C_1 důkazu mohou nastat tři případy: C_1 je předpokladem A_i, C_1 je axiómem, C_1 je formulí A. V prvých dvou případech důkazem formule $A \supset C_1$ je posloupnost formulí:

   1. C_1 předpoklad nebo axióm
   2. $C_1 \supset (A \supset C_1)$ A1
   3. $A \supset C_1$ MP:1,2

   V třetím případě je třeba dokázat $A \supset A$. Důkaz této formule je uveden v příkladě 2.4.1.

   b) Dokážeme, že z předpokládané platnosti formule $A \supset C_n$ pro n = 1, 2,...,i-1 plyne její platnost také pro n=i. Pro C_i mohou nastat čtyři případy: C_i je předpokladem A_i, C_i je axiómem, C_i je formulí A, C_i je bezprostředním důsledkem

formulí C_j a $C_k = (C_j \supset C_i)$, kde j, k < i. V prvých třech případech probíhá důkaz formule $A \supset C_i$ stejným způsobem jako v bodě 1. V posledním čtvrtém případě je důkazem posloupnost formulí:

1.	$A \supset C_j$	indukční předpoklad
2.	$A \supset (C_j \supset C_i)$	indukční předpoklad
3.	$(A \supset (C_j \supset C_i)) \supset ((A \supset C_j) \supset (A \supset C_i))$	A2
4.	$(A \supset C_j) \supset (A \supset C_i)$	MP:2,3
5.	$A \supset C_i)$	MP:1,4 Q.E.D

Poznámka 2.4.3:

Podle věty o dedukci každému teorému (a speciálně také axiómu) ve tvaru implikace odpovídá odvozovací pravidlo (příp. několik odvozovacích pravidel) a naopak. Tak např.:

Teorém:	Pravidlo
$\vdash A \supset ((A \supset B) \supset B)$	$A, A \supset B \vdash B$ /pravidlo MP/
$\vdash A \supset (B \supset A)$ /ax.schéma A1/	$A \vdash B \supset A$, a $A, B \vdash A$
$\vdash A \supset A$ /příkl. 2.4.1/	$A \vdash A$
$\vdash (A \supset B) \supset ((B \supset C) \supset (A \supset C))$ /příkl. 2.4.1/	$A \supset B \vdash (B \supset C) \supset (A \supset C)$ $A \supset B, B \supset C \vdash A \supset C$ /pravidlo TI/

Příklad 2.4.2:

Několik jednoduchých teorémů a jim odpovídajících odvozovacích pravidel:

1.	$\vdash A \supset (\neg A \supset B)$ $\vdash \neg A \supset (A \supset B)$	$A, \neg A \vdash B$	
2.	$\vdash A \supset A \vee B$, $\vdash B \supset A \vee B$	$A \vdash A \vee B$, $B \vdash A \vee B$	ZD
3.	$\vdash \neg\neg A \supset A$	$\neg\neg A \vdash A$	EN
4.	$\vdash A \supset \neg\neg A$	$A \vdash \neg\neg A$	ZN
5.	$\vdash (A \supset B) \supset (\neg B \supset \neg A)$	$A \supset B \vdash \neg B \supset \neg A$	TR
6.	$\vdash A \wedge B \supset A$, $\vdash A \wedge B \supset B$	$A \wedge B \vdash A, B$	EK
7.	$\vdash A \supset (B \supset A \wedge B)$, $\vdash B \supset (A \supset A \wedge B)$	$A, B \vdash A \wedge B$,	ZK
8.	$\vdash A \supset (B \supset C) \supset (A \wedge B \supset C)$	$A \supset (B \supset C) \vdash A \wedge B \supset C$	

Několik **důkazů**:

Ad 1. $\vdash A \supset (\neg A \supset B)$, resp. $A, \neg A \vdash B$.

Důkaz:

1.	A	předpoklad
2.	$\neg A$	předpoklad
3.	$(\neg B \supset \neg A) \supset (A \supset B)$	A3
4.	$\neg A \supset (\neg B \supset \neg A)$	A1
5.	$\neg B \supset \neg A$	MP: 2,4
6.	$A \supset B$	MP: 5,3
7.	B	MP: 1,6 Q.E.D.

Ad 2. $\vdash A \supset A \vee B$, resp. $A \vdash A \vee B$.

Po eliminaci zkratky $\vee$ podle definice $A \vee B =_{df} \neg A \supset B$, dostáváme teorém $\vdash A \supset (\neg A \supset B)$ (resp. pravidlo $A, \neg A \vdash B$), který již byl dokázán.

Ad 3. $\vdash \neg\neg A \supset A$, resp. $\neg\neg A \vdash A$.

Důkaz:

1.	$\neg\neg A$	předpoklad
2.	$(\neg A \supset \neg\neg\neg A) \supset (\neg\neg A \supset A)$	axióm.schéma A3
3.	$\neg\neg A \supset (\neg A \supset \neg\neg\neg A)$	teorém 1. tohoto příkladu
4.	$\neg A \supset \neg\neg\neg A$	MP: 1,3
5.	$\neg\neg A \supset A$	MP: 4,2
6.	A	MP: 1,5 Q.E.D.

Ad 4. $\vdash A \supset \neg\neg A$, resp. $A \vdash \neg\neg A$.

Důkaz:

1.	A	předpoklad
2.	$(\neg\neg\neg A \supset \neg A) \supset (A \supset \neg\neg A)$	axióm.schéma A3
3.	$\neg\neg\neg A \supset \neg A$	teorém 3. tohoto příkladu
4.	$A \supset \neg\neg A$	MP: 3,2 Q.E.D.

Ad 5. $\vdash (A \supset B) \supset (\neg B \supset \neg A)$, resp. $A \supset B \vdash \neg B \supset \neg A$.

Důkaz:

1.	$A \supset B$	předpoklad
2.	$\neg\neg A \supset A$	teorém 3. tohoto příkladu
3.	$\neg\neg A \supset B$	TI: 2,1
4.	$B \supset \neg\neg B$	teorém 4. tohoto příkladu
5.	$A \supset \neg\neg B$	TI: 1,4
6.	$\neg\neg A \supset \neg\neg B$	TI: 2,5
7.	$(\neg\neg A \supset \neg\neg B) \supset \neg B \supset \neg A$	axióm.schéma A3
8.	$\neg B \supset \neg A$	MP: 6,7 Q.E.D.

Ad 6. $\vdash A \wedge B \supset A$, resp. $A \wedge B \vdash A$.

Po eliminaci zkratky $\wedge$ podle definice $A \wedge B =_{df} \neg(A \supset \neg B)$ dokazujeme teorém $\vdash \neg(A \supset \neg B) \supset A$, resp. pravidlo $\neg(A \supset \neg B) \vdash A$.

Důkaz:

1.	$\neg(A \supset \neg B)$	předpoklad
2.	$(\neg A \supset (A \supset \neg B)) \supset (\neg(A \supset \neg B) \supset \neg\neg A)$	teorém 5. tohoto příkladu
3.	$\neg A \supset (A \supset \neg B)$	teorém 1. tohoto příkladu
4.	$\neg(A \supset \neg B) \supset \neg\neg A$	MP: 3,2
5.	$\neg\neg A$	MP: 1,4
6.	$\neg\neg A \supset A$	teorém 3. tohoto příkladu
7.	A	MP: 5,6 Q.E.D.

Věta 2.4.2 /o metapravidlech/**:**

Nechť T značí libovolnou konečnou množinu formulí $T = \{A_1, A_2, .., A_n\}$. Potom platí:

(a) Je-li T, A |– B a A je logický teorém, pak T |– B.
Neboli: v množině předpokladů není třeba uvádět logické teorémy.

(b) Je-li A |– B , pak T, A |– B.
Neboli: přidání předpokladů nemůže změnit platnost platného pravidla. (Obdoba monotónnosti vyplývání, viz Kap. 1)

(c) Je-li T |– A a T, A |– B , pak T |– B.
Neboli: důsledek předpokladů není třeba uvádět mezi předpoklady.

(d) Je-li T |– A a A |– B , pak T |– B.
Neboli: důsledek důsledku množiny předpokladů je také důsledkem množiny předpokladů.

(e) Je-li T |– A , T |– B , A, B |– C , pak T |– C.
Neboli: důsledek důsledků množiny předpokladů je také důsledkem množiny předpokladů.

(f) Je-li T |– A a T |– B , pak T |– A ∧ B.
Neboli: konjunkce důsledků množiny předpokladů je také důsledkem množiny předpokladů.

(g) T |– A ⊃ (B ⊃ C) právě tehdy, když T |– B ⊃ (A ⊃ C).
Neboli: na pořadí předpokladů nezáleží.

(h) T, A ∨ B |– C právě tehdy, když současně T, A |– C a T, B |– C.
Věta o důkazu rozborem případů.

(i) Je-li T, A |– B a současně T, ¬A |– B , pak T |– B.
Věta o neutrální formuli /formule A je neutrální vzhledem k B/.

Poznámky 2.4.4:

1) (Odvozovací) pravidla představují vztah mezi formulemi, meta-pravidla představují vztah mezi pravidly.

2) Důkaz pravidla je (podle věty o dedukci) totéž co důkaz odpovídající formule (viz definice 2.4.2), tj. jistá posloupnost formulí. Důkaz metapravidla je naproti tomu posloupností pravidel (viz dále ukázky důkazů).

3) Množinu předpokladů T={A_1,A_2,..,A_n} z věty 2.4.2 interpretujeme nejčastěji jako množinu mimologických (speciálních) axiómů definujících obsahovou náplň konkrétní teorie.

Důkaz:

Ad (h):

Nechť T, A ∨ B |– C, dokážeme T, A |– C a T, B |– C.
Důkaz:

1.	A |– A ∨ B	pravidlo ZD	
2.	T, A |– A ∨ B	metapravidlo (b): 1	
3.	T, A ∨ B |– C	předpoklad	
4.	T, A |– C	metapravidlo (d): 2,3	Q.E.D.
5.	T, B |– C	dokáže se obdobně jako 4.	Q.E.D.

Nechť T, A |– C a T, B |– C, dokážeme T, A ∨ B |– C.

Důkaz:

1.	T, A |– C	předpoklad
2.	T |– A ⊃ C	věta o dedukci:1
3.	T |– ¬C ⊃ ¬A	metapravidlo (d): 2, pravidlo TR
4.	T, ¬C |– ¬A	věta o dedukci: 3
5.	T, ¬C |– ¬B	odvodí se obdobně jako 4.
6.	T, ¬C |– ¬A, ¬B	metapravidlo (f): 4,5
7.	¬A, ¬B |– ¬(A ∨ B)	pravidlo ekviv. teorému de Morgana
8.	T, ¬C |– ¬(A ∨ B)	metapravidlo (d): 6,7
9.	T |– ¬C ⊃ ¬(A ∨ B)	věta o dedukci: 8
10.	T |– A∨ B ⊃ C	metapravidlo (d): 9. pravidlo TR
11.	T, A ∨ B |– C	věta o dedukci: 10 Q.E.D.

Ad (i):

Nechť T, A |– B a T, ¬A |– B, dokážeme T |– B.

Důkaz:

1.	T, A |– B	předpoklad
2.	T, ¬A |– B	předpoklad
3.	T, A ∨ ¬A |– B	metapravidlo (h): 1,2
4.	T |– B	metapravidlo (a): 3

Věta 2.4.3 /pomocná věta pro důkaz Postovy věty/:

Nechť formule A je sestavena z výrokových symbolů p_1, p_2,...,p_n. V souladu s definicí 2.1.2 označme písmenem *v* pravdivostní ohodnocení (valuaci) těchto proměnných a zápisem w(A) pravdivostní ohodnocení formule A, jež je tímto ohodnocením indukováno. Potom platí:

$$p_1^v, p_2^v, ..., p_n^v \text{ |– } A^v, \qquad /*/$$

kde zápis A^v značí buď formuli ¬A (je-li w(A) = 0 při ohodnocení *v*), nebo formuli A (je-li w(A) = 1 při ohodnocení *v*).

Důkaz:

Důkaz provedeme matematickou indukcí podle konstrukce formule A. Ve formálním systému zadaném v definici 2.4.1 může mít formule A právě jeden z následujících třech tvarů:

1. A = p elementární formule
2. A = ¬B složená formule ve tvaru negace
3. A = B ⊃ C složená formule ve tvaru implikace

Báze indukce. Vztah /*/ má v případě elementární formule tvar p^v |– p^v a je tedy evidentně platný.

Indukční krok. Dokážeme, že z předpokladu platnosti vztahu /*/ pro komponenty B, C složené formule vyplývá platnost vztahu /*/ pro celé složené formule ¬B a B ⊃ C.

a) Složená formule má tvar ¬B. Podle indukčního předpokladu platí

$p_1^v, p_2^v,...,p_n^v \vdash B^v$. Máme dokázat $p_1^v, p_2^v,...,p_n^v \vdash (\neg B)^v$.

K tomu, abychom to dokázali, stačí dokázat $B^v \vdash (\neg B)^v$. Jsou dvě možnosti: buď $w(B) = 0$ a pak $\neg B \vdash \neg B$ a nebo $w(B) = 1$ a pak $B \vdash \neg\neg B$. Vztah $B^v \vdash (\neg B)^v$ je dokázaný.

b) Složená formule má tvar $B \supset C$. Podle indukčního předpokladu platí

$p_1^v, p_2^v, ..., p_n^v \vdash B^v$ a $p_1^v, p_2^v,...,p_n^v \vdash C^v$.

Máme dokázat $p_1^v, p_2^v,...,p_n^v \vdash (B \supset C)^v$.

K tomu, abychom to dokázali, stačí dokázat $B^v, C^v \vdash (B \supset C)^v$. Čtyřem různým ohodnocením formulí B, C odpovídají následující čtyři pravidla, jejichž platnost třeba ověřit:

a) $\neg B, \neg C \vdash B \supset C$

b) $\neg B, C \vdash B \supset C$

c) $B, \neg C \vdash \neg(B \supset C)$

d) $B, C \vdash B \supset C$

Důkaz a),b):

1.	$\neg B$	předpoklad
2.	$\neg B \supset (B \supset C)$	teorém /viz příklad 2.4.2/
3.	$B \supset C$	MP: 1,2 Q.E.D.

Důkaz c):

1.	B	předpoklad
2.	$\neg C$	předpoklad
3.	$((B \supset C) \supset C) \supset (\neg C \supset \neg(B \supset C))$	ax.schéma A3
4.	$B \supset ((B \supset C) \supset C)$	teorém /ekvivalent MP/
5.	$(B \supset C) \supset C$	MP: 1,4
6.	$\neg C \supset \neg(B \supset C)$	MP: 5,3
7.	$\neg(B \supset C)$	MP: 2,6 Q.E.D.

Důkaz d):

1.	C	předpoklad
2.	$C \supset (B \supset C)$	ax.schéma A1
3.	$B \supset C$	MP: 1,2 Q.E.D.

Věta 2.4.4 /Postova /: Úplnost a korektnost logického kalkulu výrokové logiky

Každá dokazatelná formule je tautologií a každá tautologie je dokazatelná, tj.

$$\vdash A \text{ právě tehdy, když } \models A.$$

Obecněji platí:

$$A_1, A_2,..,A_n \vdash B \text{ právě tehdy, když } A_1, A_2,..,A_n \models B.$$

Důkaz:

1. Nechť |– A, dokážeme |= A. (***Korektnost***)

   Formule A je buď axióm a nebo je dokazatelná z axiómů pomocí opakovaného používání odvozovacího pravidla MP. Je-li axiómem, pak je tautologií – o tom se přesvědčíme pro všechna tři axiómová schémata metodou pravdivostních funkcí /metodou 0-1/. Použití pravidla MP zachovává "tautologičnost": jsou-li formule B, $B \supset C$ tautologiemi, pak také formule C musí být tautologií /kdyby pro nějaké pravdivostní ohodnocení výrokových symbolů bylo w(B) = 1 a při tom w(C)=0, pak by pro toto ohodnocení bylo $w(B \supset C) = 0$ a formule $B \supset C$ by nebyla tautologií/. Protože všechny teorémy lze odvodit z axiómů pomocí opakovaného užití pravidla MP, jsou všechny teorémy tautologiemi.

2. Nechť |= A, dokážeme |– A. (***Úplnost***)

   Protože formule A je tautologií, je $A^v = A$ pro všechna pravdivostní ohodnocení výrokových symbolů *v*. Je tedy

   $$p_1^v, p_2^v,...,p_n^v \mid\!- A$$

   pro všechna ohodnocení *v*. Platí tedy speciálně také

   $$p_1, p_2^v,...,p_n^v \mid\!- A,$$
   $$\neg p_1, p_2^v,...,p_n^v \mid\!- A.$$

   Odtud podle věty o neutrální formuli dostáváme

   $$p_2^v, ..., p_n^v \mid\!- A$$

   pro všechna ohodnocení *v*. Speciálně opět platí

   $$p_2, ..., p_n^v \mid\!- A,$$
   $$\neg p_2,..., p_n^v \mid\!- A$$

   a počet předpokladů lze opět snížit o jeden. Tímto způsobem lze pokračovat až nakonec po n krocích nalezneme |– A. Tautologie A je tedy dokazatelnou formulí.

3. Predikátová logika 1. řádu

3.1. Sémantický výklad predikátové logiky

Úvodní poznámky:

1. Pouze jen malá část úsudků může být formalizována a dokázána v rámci výrokové logiky. Pokusme se např. ověřit typ (zjevně správného) úsudku charakterizovaný následujícím příkladem:

Každý člověk je omylný.
Jan je člověk.
_____
Jan je omylný.

Označíme-li uvedené tři věty symboly p, q, r, pak pokus o formalizaci v rámci výrokové logiky je dán následujícím úsudkem: p, q / r, což odpovídá formuli:

$$(p \wedge q) \supset r.$$

Tato formalizace je však zřejmě nedostačující, a to z těchto důvodů:

- Uvedené tři výroky jsou z hlediska VL elementární a navzájem nezávislé, avšak ve skutečnosti mají vnitřní komponenty, jsou strukturované, a existuje mezi nimi prostřednictvím těchto komponent vazba. Termín "člověk" se vyskytuje ve výrocích p i q, termín "omylný" ve výrocích p i r, a termín "Jan" ve výrocích q i r.
- Formule $(p \wedge q) \supset r$ není tautologií, úsudek p, q / r není platný, i když úsudek demonstrovaný příkladem evidentně platný je.

V predikátové logice, která je zobecněním výrokové logiky, je uvedený úsudek formalizován jako $\forall x\,[p(x) \supset q(x)]$, $p(J) \models q(J)$, resp. následující formulí

$$\{\forall x\,[p(x) \supset q(x)] \wedge p(J)\} \supset q(J),$$

kde,

- x je předmětová (individuová) proměnná probíhající určitou předmětnou oblast – universum diskursu,
- J je individuová konstanta z dané předmětné oblasti (v uvedeném příkladě konkrétní člověk Jan),
- p, q jsou určité vlastnosti předmětů z universa diskursu (v uvedeném příkladě je interpretujeme jako vlastnosti myslících bytostí "být člověkem" a "být omylný"), p(x), q(x) resp. p(J), q(J) značí, že x resp. J má vlastnost p resp. q ,
- zápis $\forall x[\ ]$ značí, že pro všechna individua z předmětné oblasti platí to, co je uvedeno v hranatých závorkách.

2. Predikátová logika 1.řádu.

V dalším se budeme zabývat pouze tzv. ***predikátovou logikou 1. řádu***, která formalizuje úsudky o vlastnostech předmětů a vztazích mezi předměty pevně dané předmětné oblasti (univerza). Nebudeme se zabývat formalizací úsudků, které navíc vypovídají i o vlastnostech vlastností a vztahů a o vztazích mezi vlastnostmi a vztahy. Tím se zabývají ***predikátové logiky druhého a vyšších řádů***. Predikátová logika 1. řádu je zobecněním výrokové logiky, kterou můžeme považovat za logiku nultého řádu. Predikátová logika 1. řádu je postačující pro formalizaci mnohých matematických i jiných teorií.

Definice 3.1.1 /jazyk predikátové logiky/**:**

I) ***Abeceda predikátové logiky*** je tvořena následujícími skupinami symbolů:
   a. Logické symboly
      i. předmětové (individuové) proměnné: *x, y, z*,... (příp. s indexy)
      ii. symboly pro spojky: $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$
      iii. symboly pro kvantifikátory $\forall$, $\exists$
      iv. případně binární predikátový symbol = (predikátová logika s rovností)
   b. Speciální symboly (určují specifiku jazyka)
      i. predikátové symboly: p, q, r,... /příp. s indexy/
      ii. funkční symboly: f, g, h,... /příp. s indexy/

      Ke každému funkčnímu a predikátovému symbolu je přiřazeno nezáporné číslo n ($n \geq 0$), tzv. ***arita***, udávající počet individuových proměnných, které jsou argumenty funkce nebo predikátu.
   c. Pomocné symboly /závorky/: (,) /případně i [,],{,}/

II) ***Gramatika,*** která udává, jak tvořit:
   a. ***termy*****:**
      i. každý symbol proměnné je term
      ii. jsou-li $t_1,\ldots,t_n$ ($n \geq 0$) termy a je-li f n-ární funkční symbol, pak výraz $f(t_1,\ldots,t_n)$ je term; pro $n = 0$ se jedná o nulární funkční symbol, neboli individuovou konstantu (značíme a, b, c, …)
      iii. jen výrazy dle i. a ii. jsou termy
   b. ***atomické formule***:
      i. je-li p n-ární predikátový symbol a jsou-li $t_1,\ldots,t_n$ termy, pak výraz $p(t_1,\ldots,t_n)$ je atomická formule
      ii. jsou-li t_1 a t_2 termy, pak výraz $(t_1 = t_2)$ je atomická formule
   c. ***formule*****:**
      i. každá atomická formule je formule
      ii. je-li výraz A formule, pak $\neg$A je formule
      iii. jsou-li výrazy A a B formule, pak výrazy (A $\vee$ B), (A $\wedge$ B), (A $\supset$ B), (A $\equiv$ B) jsou formule
      iv. je-li x proměnná a A formule, pak výrazy $\forall x$A a $\exists x$A jsou formule
      v. jen výrazy dle i. – iv. jsou formule

Poznámky 3.1.1

1. Jazyk predikátové logiky, jak byl vymezen výše, je jazyk logiky 1. řádu, pro niž je charakteristické to, že *jediný přípustný typ proměnných jsou individuové proměnné.* Pouze individuové proměnné lze vázat kvantifikátory. (V logice 2. řádu jsou povoleny i predikátové proměnné.)
2. Definice jazyka umožňuje formulaci speciálního jazyka (určité teorie) konkrétní volbou prvků (predikátových a funkčních konstant) dle bodu I)b. definice. Pro takový konkrétní jazyk budou platit obecné principy logické a mimo to – v závislosti na specifických vlastnostech (interpretacích) těchto prvků – i principy mimologické, které zadá tvůrce tohoto speciálního jazyka pomocí speciálních axiómů (dané teorie).

Je-li arita funkčního symbolu $n = 0$, pak se jedná o individuovou konstantu (značíme a, b, …), která však není pravou (logickou) konstantou, neboť podléhá (jako každý funkční symbol) interpretaci (viz Definice 3.1.3)

3. Zápis formulí můžeme zjednodušit na základě následujících konvencí o vynechávání závorek:
   - Elementární formule a formuli nejvyššího řádu netřeba závorkovat (vnější závorky vynecháváme).
   - Závorky je možné vynechávat v souladu s následující prioritní stupnicí funktorů: $(\forall, \exists)$, $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$. Každý funktor vlevo od vybraného funktoru váže silněji než vybraný funktor.
   - V případě, že o prioritě vyhodnocení nerozhodnou ani závorky ani prioritní stupnice, vyhodnocujeme formuli zleva doprava.
   - Speciálně vzhledem k asociativitě konjunkce a disjunkce, netřeba při zápisu vícečlenných konjunkcí a disjunkcí užívat žádné závorky.
   - Vedle závorek (,) lze užívat i závorky [,], {,}.

Příklad: Jazyk elementární aritmetiky je případem jazyka predikátové logiky 1. řádu s rovností. Má tyto (speciální) funkční symboly:

nulární symbol: 0 (konstanta nula)
unární symbol: s (funkce následník)
binární symboly: + a × (sčítání a násobení)

Příkladem termů jsou (používáme infixní notaci pro + a ×):

$0, s(x), s(s(x)), (x + y) \times s(s(0))$, atd.

Formulemi jsou např. výrazy:

$s(0) = (0 \times x) + s(0)$, $\exists x\,(y = x \times z)$, $\forall x\,[(x = y) \supset \exists y\,(x = s(y))]$

Definice 3.1.2

Výskyt proměnné x ***ve formuli*** A ***je vázaný***, jestliže je součástí nějaké podformule $\forall x B(x)$ nebo $\exists x B(x)$ formule A.

Proměnná *x* ***je vázaná ve formuli*** A, má-li v A vázaný výskyt. Výskyt proměnné x ve formuli A, který není vázaný, nazýváme ***volný***.

Proměnná *x* ***je volná ve formuli*** A, má-li v A volný výskyt.

Formule, v níž každá proměnná má buď všechny výskyty volné nebo všechny výskyty vázané, se nazývá ***formulí s čistými proměnnými***.

Formule se nazývá ***uzavřenou***, neobsahuje-li žádnou volnou proměnnou. Formule, která obsahuje aspoň jednu volnou proměnnou se nazývá ***otevřenou***.

Nechť $x_1, x_2, \ldots, x_n$ jsou všechny volné proměnné formule A. Potom uzavřenou formuli

$$\forall A =_{df} \forall x_1 \forall x_2 \ldots \forall x_n A \quad \text{resp.} \quad \exists A =_{df} \exists x_1 \exists x_2 \ldots \exists x_n A ,$$

nazýváme ***generálním*** resp. ***existenčním uzávěrem formule*** A.

Symbolem $A(x/t)$ označujeme formuli, která vznikne z formule A ***korektní substitucí termu*** t ***za proměnnou*** *x*. Má-li být substituce korektní musí splňovat následující dvě pravidla:

- Substituovat lze *pouze za volné výskyty* proměnné *x* ve formuli A a při substituci nahrazujeme *všechny volné výskyty* proměnné *x* ve formuli A.
- Žádná individuová proměnná vystupující v termu t se po provedení substituce *x*/t nesmí stát ve formuli A vázanou (v takovém případě je term t za proměnnou *x* ve formuli A ***nesubstituovatelný***).

Symbolem $A(x_1,x_2,...,x_n / t_1,t_2,...,t_n)$ označujeme formuli, která vznikne z formule A korektními substitucemi x_i/t_i pro i = 1, 2,...,n.

Všechny formule tvaru $A(x_1, x_2,...,x_n / t_1, t_2,...,t_n)$ nazýváme ***instancemi formule*** A.

Příklad: Nechť formulí A(*x*) je: $p(x) \supset \forall y\ q(x, y)$ a term t nechť je f(*y*). Provedeme-li substituci A(*x*/f(*y*)), dostaneme: $p(f(y)) \supset \forall y\ q(f(\boldsymbol{y}), y)$. Vidíme, že druhý (zvýrazněný) výskyt proměnné *y* není volný (přitom původně zde byla volná proměnná *x,* takže jsme změnili "smysl výrazu"). Tedy term f(*y*) není substituovatelný za *x* v dané formuli A, tj. $p(x) \supset \forall y\ q(x, y)$.

Převod z přirozeného jazyka do symbolického jazyka PL^1.

Jde o analýzu výrazů přirozeného jazyka v rámci PL^1. Volba predikátových (a funkčních) konstant je libovolná potud, že nesmí dojít ke "kolizi vlastností, funkcí či vztahů". Výrazy jako "všichni", "každý", "nikdo", apod. "překládáme" všeobecným kvantifikátorem ∀, výrazy jako "někdo", "někteří", apod. "překládáme" existenčním kvantifikátorem ∃. Dále budeme předpokládat, že jde o jazyk nad homogenním universem, proto v následujících příkladech považujeme za universum diskursu (obor proměnnosti proměnných) množinu všech individuí. Pro přehlednost budeme používat velká písmena pro predikátové symboly.

Příklad 3.1.1: Analyzujte v jazyce PL^1 následující výroky:

1) Nikdo, kdo není zapracován (P), nepracuje samostatně (S).
2) Ne každý talentovaný (T) spisovatel (Sp) je slavný (Sl).
3) Pouze zaměstnanci (Z) používají výtahu (V).
4) Ne každý člověk (C), který hodně mluví (M), nemá co říci (R).
5) Někdo je spokojen (Sn) a někdo není spokojen.
6) Někteří chytří lidé (Ch) jsou líní (L).
7) Všichni zaměstnanci (Z) používají výtahu (V).

Řešení:

Pozn.: Jako pomůcka k řešení může sloužit tato zásada: Po všeobecném kvantifikátoru ∀ následuje formule ve tvaru implikace (⊃), kdežto po existenčním kvantifikátoru formule ve tvaru konjunkce (∧).

1) $\forall x\ [\neg P(x) \supset \neg S(x)]$
2) $\neg\forall x\ \{[T(x) \wedge Sp(x)] \supset Sl(x)\}$
3) $\forall x\ [V(x) \supset Z(x)]$
4) $\neg\forall x\ \{[C(x) \wedge M(x)] \supset \neg R(x)\}$
5) $\exists x\ Sn(x) \wedge \exists x\ \neg Sn(x)$
6) $\exists x\ [Ch(x) \wedge L(x)]$
7) $\forall x\ [Z(x) \supset V(x)]$

Sémantika PL^1 – interpretace formulí.

Sémantika, neboli význam formulí predikátové logiky 1. řádu, je dána jejich interpretací. Než tento pojem přesně definujeme, uvedeme několik neformálních motivací a vysvětlení. Položíme-li si otázku, zda daná formule PL^1 je pravdivá či ne, pak taková otázka je v podstatě nesmyslná, pokud nevíme, co formule znamená, tedy jak je interpretována. Tak např. formule

$$\forall x \, \mathrm{p}(\mathrm{f}(x), x)$$

může "říkat", že pro všechna přirozená čísla platí, že jejich druhá mocnina je větší než to číslo, nebo že pro všechny lidi platí, že jejich otec je starší než dotyčný člověk, pak je samozřejmě v takových interpretacích pravdivá. Může ale také znamenat, že pro všechna přirozená čísla platí, že jejich druhá mocnina je menší než to číslo, nebo že pro všechny lidi platí, že jejich otec je mladší než dotyčný člověk, pak je samozřejmě (v takové interpretaci) nepravdivá.

Podobně např. formule, kterými jsme analyzovali věty 1. - 7. přirozeného jazyka v úvodním příkladu 3.1.1, mohou být interpretovány tak, aby zachycovaly význam těchto vět ("zamýšlená" interpretace), ale mohou být interpretovány úplně jinak. Např. formule, která je analýzou věty *Někteří chytří lidé jsou líní,* tedy

$$\exists x \, [\mathrm{Ch}(x) \wedge \mathrm{L}(x)],$$

může být interpretována jako zachycující význam věty *Některá lichá čísla jsou dělitelná dvěma,* a pak je evidentně (v této interpretaci) nepravdivá.

V čem tedy spočívá interpretace formule? Nejprve musíme stanovit, "o čem mluvíme", tedy jaká je předmětná oblast – obor proměnnosti (individuových) proměnných, tj. zvolíme jistou *neprázdnou* množinu – **universum diskursu,** jejíž prvky jsou **individua.** Jelikož predikátové symboly mají vyjadřovat vztahy mezi těmito předměty – prvky universa, přiřadíme každému *n*-árnímu **predikátovému symbolu** jistou *n*-ární **relaci** (tj. podmnožinu Kartézského součinu) nad universem. Specielně, jedná-li se o unární predikátový symbol ($n = 1$), pak přiřadíme podmnožinu universa. Podobně **funkční symboly** budou vyjadřovat *n*-ární **funkce** nad universem. Teprve poté, co je daná formule interpretována, můžeme **vyhodnotit** její **pravdivost** či nepravdivost **v dané interpretaci.** Je zde však ještě jeden problém, a to jsou proměnné. Proměnným jazyka PL^1 přiřazujeme **valuací** individua, tj. prvky universa. (Proměnným jazyka PL2 mohou být přiřazeny také vlastnosti či funkce.) Jak uvidíme dále z definice sémantiky kvantifikátorů, pravdivostní hodnota formule nezávisí na hodnotě vázaných proměnných (pouze volné proměnné jsou "skutečné" proměnné). Obsahuje-li však formule nějaké volné proměnné, můžeme vyhodnotit její pravdivost v interpretaci pouze v **závislosti na ohodnocení** (valuaci) **volných proměnných**. Při některé valuaci může být formule v dané interpretaci pravdivá, při jiné nepravdivá. Tak např. formule

$$\forall x \, \mathrm{p}(\mathrm{f}(x), \mathrm{y})$$

může být interpretována nad množinou celých čísel tak, že symbolu p je přiřazena relace větší nebo rovno ($\geq$), symbolu f funkce druhá mocnina (tedy $\mathrm{f}(x)$ "znamená" x^2). Pak formule "říká", že pro každé celé číslo x platí, že x^2 je větší než nebo rovno **jistému číslu *y*.** Tedy pravdivost formule v této interpretaci závisí na ohodnocení (valuaci) proměnné *y*. Přiřadíme-li např. *y* číslo 5, je formule nepravdivá, přiřadíme-li třeba číslo -3 nebo 0, je

formule pravdivá. Obecně bude formule pravdivá (v této interpretaci) pro každou valuaci proměnné *y,* která přiřadí *y* záporné číslo nebo nulu, nepravdivá pro všechny valuace, které přiřadí proměnné *y* číslo kladné.

Definice 3.1.3

Interpretace jazyka predikátové logiky 1. řádu je tato trojice objektů (která je někdy nazývána *interpretační struktura*):

A) *Neprázdná* množina M, která se nazývá **universum diskursu** a její prvky jsou **individua.**

B) Interpretace funkčních symbolů jazyka, která přiřazuje každému *n*-árnímu funkčnímu symbolu f určité **zobrazení f_M: $M^n \rightarrow M$**.

C) Interpretace predikátových symbolů jazyka, která přiřazuje každému *n*-árnímu predikátovému symbolu p jistou *n*-ární relaci $\mathbf{p_M}$ nad M, tj. **podmnožinu Kartézského součinu M^n.**

Poznámky 3.1.2

1. Každý *n*-ární funkční symbol je tedy interpretován jako funkce, která přiřazuje *n*-tici individuí právě jedno individuum, tj. zobrazení z M ×...× M do M. Specielně:
   - je-li $n = 0$, pak se jedná o nulární funkční symbol, tedy o individuovou konstantu, které je přiřazen prvek universa – individuum
   - je-li $n = 1$, pak se jedná o unární funkční symbol, kterému je přiřazena funkce o jednom argumentu (např. nad množinou čísel x^2, $x + 1$, nad množinou individuí otec(x), matka(x), atd.)
   - je-li $n = 2$, pak se jedná o binární funkční symbol, kterému je přiřazena binární funkce se dvěma argumenty (např. nad množinou čísel $x + y$, $x.y$, atd.)
2. Každý *n*-ární predikátový symbol p je interpretován jako *n*-ární relace p_M, tj. podmnožina Kartézského součinu M ×...× M, neboli zobrazení M ×...× M → {1,0}. Tato relace p_M se nazývá **obor pravdivosti** predikátu. Specielně:
   - je-li $n = 0$, pak se jedná o nulární predikátový symbol, kterému je přiřazena hodnota 1 nebo 0 (pravda, nepravda) tak, jak to již známe z výrokové logiky.
   - je-li $n = 1$, pak se jedná o unární predikátový symbol, kterému je přiřazena podmnožina universa M. (Vlastnosti tedy v PL^1 vyjadřujeme – poněkud nepřesně – jako podmnožiny universa.)
   - je-li $n = 2$, pak se jedná o binární predikátový symbol, kterému je přiřazena binární relace nad universem (např. relace větší, menší, apod.)
3. Výroková logika je tedy specielním (nejjednodušším) případem predikátové logiky, a to 0. řádu, ve které pracujeme pouze s nulárními predikáty a nepotřebujeme proto termy, funkční symboly, individuové proměnné ani universum diskursu (obor proměnnosti proměnných). Nulárním predikátům přiřazujeme pouze hodnoty pravda, nepravda.

Příklad 3.1.2:

Uvažujme jazyk predikátové logiky s následujícími konstantami:

- f_0, f_1 - nulární funkční symboly, g - unární funkční symbol, h, k - binární funkční symboly,
- p, q binární predikátové symboly.

Pro tento jazyk definujme interpretaci následujícím způsobem:

- Universum diskursu M je množina všech nezáporných celých čísel {0, 1, 2,...}.
- Realizace funkčních symbolů jsou definovány takto:
  f_0 ... předmětová konstanta: číslo 0 /nikoliv pravdiv. hodnota !/
  f_1 ... předmětová konstanta: číslo 1 /nikoliv pravdiv. hodnota !/
  g ... zobrazení $M \to M$ definované takto: $g(x) = x + 1$
  h ... zobrazení $M^2 \to M$ definované takto: $h(x, y) = x + y$
  k ... zobrazení $M^2 \to M$ definované takto: $k(x, y) = x \,.\, y$
- Realizace predikátových symbolů jsou definovány takto:
  p ... podmnožina množiny M^2 definovaná jako množina všech dvojic $\langle x,y \rangle$, pro které platí $x = y$,
  q ... podmnožina množiny M^2 definovaná jako množina všech dvojic $\langle x,y \rangle$, pro které platí $x < y$.

Skutečnost, že např. $(x + y).z = x.z + y.z$ pro všechna x, y, z zapíšeme standardní formulí predikátové logiky takto:

$$\forall x \forall y \forall z \, [p(k(h(x,y),z), h(k(x,z),k(y,z)))].$$

Můžeme přirozeně použít i obvyklého nestandardního zápisu

$$\forall x \forall y \forall z \, [(x+y).z = x.z+y.z],$$

který využívá speciální infixovovou notaci binárních funkcí a další speciální konvence (např. priorita násobení před sčítáním).

Poznatek, že ke každým dvěma číslům x, y existuje číslo z takové, že buď $x+z = y$ nebo $y+z = x$ zapíšeme formulí

$$\forall x \, \forall y \, \exists z \, [(x + z = y) \vee (y + z = x)],$$

neboli standardně

$$\forall x \, \forall y \, \exists z \, [p(h(x, z), y) \vee p(h(y, z), x))].$$

Definice 3.1.4:

Ohodnocení (valuace) individuových proměnných je zobrazení e, které každé proměnné x přiřazuje hodnotu $e(x) \in M$ (prvek univerza).

Ohodnocení termů e^* indukované ohodnocením proměnných e je induktivně definováno takto:

- $e^*(x) = e(x)$
- $e^*(f(t_1, t_2,...,t_n)) = f_M(e^*(t_1), e^*(t_2),...,e^*(t_n))$, kde f_M je funkce přiřazená v dané interpretaci funkčnímu symbolu f.

Pozn.: Hodnotou (realizací) termu t v interpretaci I je tedy vždy jistý *prvek universa.* Tedy funkční symboly jsou "jména funkcí – zobrazení", termy jsou "jména prvků

universa", zatímco predikátové symboly jsou "jména relací" a formule jsou "jména pravdivostních hodnot".

Definice 3.1.5:

Pravdivost formule A v interpretaci I pro ohodnocení e **e** individuových proměnných (což značíme $\models_I A[e]$ – formule A je pravdivá v I pro e, nebo také A ***je splněna v I ohodnocením e***), je definována v závislosti na tvaru formule:

1. Je-li A atomická formule tvaru
   a. $p(t_1, \ldots, t_n)$, kde p je predikátový symbol (různý od =) a $t_1, \ldots, t_n$ jsou termy, pak $\models_I A[e]$, jestliže platí $< e^*(t_1), e^*(t_2),\ldots,e^*(t_n)> \in p_M$, kde p_M je relace přiřazená interpretací I symbolu p – obor pravdivosti p. Tedy individua, která jsou hodnotou termů $t_1, \ldots, t_n$, jsou v relaci p_M.
   b. $(t_1 = t_2)$, pak $\models_I A[e]$, jestliže platí $e^*(t_1) = e^*(t_2)$, tj. oba termy jsou realizovány týmž individuem.
2. Je-li A složená formule dle bodu II. c) definice 3.1.1, tj. je-li tvaru
   a. $\neg B$, pak $\models_I A[e]$ jestliže neplatí $\models_I B[e]$
   b. $B \wedge C$, pak $\models_I A[e]$, jestliže platí $\models_I B[e]$ a $\models_I C[e]$
   c. $B \vee C$, pak $\models_I A[e]$, jestliže platí $\models_I B[e]$ nebo $\models_I C[e]$
   d. $B \supset C$, pak $\models_I A[e]$, jestliže neplatí $\models_I B[e]$ nebo platí $\models_I C[e]$
   e. $B \equiv C$, pak $\models_I A[e]$, jestliže platí $\models_I B[e]$ a $\models_I C[e]$, nebo neplatí $\models_I B[e]$ a neplatí $\models_I C[e]$
3. je-li A formule tvaru
   a. $\forall x$ B, pak $\models_I A[e]$, jestliže pro *libovolné* individuum $i \in M$ platí $\models_I B[e(x/i)]$, kde $e(x/i)$ je valuace stejná jako e až na to, že přiřazuje proměnné *x* individuum i.
   b. $\exists x$ B, pak $\models_I A[e]$, jestliže pro *alespoň jedno* individuum $i \in M$ platí $\models_I B[e(x/i)]$, kde $e(x/i)$ je valuace stejná jako e až na to, že přiřazuje proměnné *x* individuum i.

Pozn.: 1) Je-li universum diskursu konečná množina $M = \{a_1,\ldots,a_n\}$, pak platí následující ekvivalence formulí:

$$\forall x\, A(x) \Leftrightarrow A(a_1) \wedge \ldots \wedge A(a_n)$$
$$\exists x\, A(x) \Leftrightarrow A(a_1) \vee \ldots \vee A(a_n) .$$

2) Z definice kvantifikátorů je navíc zřejmé, že platí:

$$\forall x\, A(x) \Leftrightarrow \neg\exists x \neg A(x), \quad \exists x\, A(x) \Leftrightarrow \neg\forall x \neg A(x)$$

Definice 3.1.5a:

Formule A je splnitelná v interpretaci I, jestliže *existuje* ohodnocení e proměnných takové, že platí $\models_I A[e]$.

Formule A je pravdivá v interpretaci I, značíme $\models_I \mathbf{A}$, jestliže pro *všechna* možná ohodnocení e individuových proměnných platí, že $\models_I A[e]$.

Model formule A je interpretace I, ve které je A pravdivá.

Formule A je splnitelná, jestliže existuje interpretace I, ve které je splněna, tj. jestliže existuje interpretace I a valuace e takové, že $\models_I A[e]$.

Formule A je tautologií (logicky pravdivá), značíme $\models \mathbf{A}$, jestliže je pravdivá v každé interpretaci.

Formule A je kontradikcí, jestliže nemá model, tedy neexistuje interpretace I, která by formuli A splňovala.

Pozn.: Zjevně platí, že A je kontradikce, právě když negace A je tautologie, $\models \neg A$.

Model množiny formulí $\{A_1,\ldots,A_n\}$ je taková interpretace I, ve které jsou pravdivé *všechny* formule $A_1,...,A_n$.

Formule B logicky vyplývá z formulí $A_1, \ldots, A_n$, značíme $\mathbf{A_1,\ldots,A_n} \models \mathbf{B}$, jestliže B je pravdivá v každém modelu množiny formulí $A_1,\ldots,A_n$.
Tedy pro každou interpretaci I, ve které jsou pravdivé formule $A_1, \ldots, A_n$ ($\models_I A_1,\ldots, \models_I A_n$) platí, že je v ní pravdivá také formule B ($\models_I B$).

Pozn.:

1) Někdy bývá **model** formule definován jako interpretace I a valuace *e*, ve které je tato formule pravdivá (tedy platí $\models_I A[e]$). Pak také definice **logického vyplývání** v rámci PL^1 je příslušně upravena.

   Definice 3.1.5b: $A_1,\ldots,A_n \models B$, jestliže pro každou interpretaci I a vauaci e, ve které jsou předpoklady $A_1,\ldots,A_n$ pravdivé (tj. platí $\models_I A_1[e],\ldots, \models_I A_n[e]$), platí současně, že je v ní pravdivý i závěr B (tj. $\models_I B[e]$).

   Jestliže B vyplývá z $\{A_1,\ldots A_n\}$ podle "silnější" definice 3.1.5b, pak vyplývá i podle "slabší" definice 3.1.5a, ale ne naopak! Uvedené definice nejsou ekvivalentní. Např. podle definice vyplývání 3.1.5a platí, že

   $$p(x) \models \forall x\, p(x),$$

   avšak podle definice 3.1.5b to neplatí. Tedy definice 3.1.5b je přesnější, neboť formule $p(x) \supset \forall x\, p(x)$ **není tautologií.** Historicky se však vžila definice v podobě 3.1.5a, a také my ji budeme používat. Musíme si však být vědomi rozdílu mezi oběma definicemi.

   Pro uzavřené formule však obě definice splývají, neboť pravdivost uzavřené formule A v interpretaci I nezávisí dle bodu 3 definice 3.1.5 na valuaci proměnných. (Proto také bývají speciální axiómy teorie voleny pouze jako uzavřené formule, tzv. *sentence,* viz kapitola 4.)

Příklad 3.1.3:

Uvažujme jazyk predikátové logiky a jeho interpretaci, tak jak byly popsány v příkladu 3.1.2.

- Formule

$$p(h(x,y), x)), \text{ neboli } x + y = x$$

je pravdivá v uvedené interpretaci např. pro ohodnocení proměnných e(x)=3, e(y)=0 a nepravdivá např. pro ohodnocení e(x)=3, e(y)=2. Formule je splnitelná v dané interpretaci, není však v této interpretaci pravdivá.

- Formule

$$p(h(x,y), h(y,x)), \text{ neboli } x + y = y + x$$

je v uvedené interpretaci pravdivá pro každé ohodnocení a je tedy, stejně tak jako formule

$$\forall x \forall y\ [p(h(x,y), h(y,x))], \text{ neboli } \forall x \forall y\ [x + y = y + x]$$

pravdivá v této interpretaci. Není však univerzální logickou tautologií (interpretujeme-li např. binární predikát p jako ostrou nerovnost, pak uvedené formule jsou nepravdivé).

- Formule

$$\forall x\ \exists y\ q(x,y), \text{ neboli } \forall x\ \exists y\ [x < y]$$

je pravdivá v dané interpretaci a formule

$$\forall y\ \exists x\ q(x,y), \text{ neboli } \forall y\ \exists x\ [x < y]$$

je nesplnitelná v dané interpretaci jazyka predikátové logiky.

- Formule

$$p(x,y) \vee q(x,y) \vee q(y,x),\ \forall x \forall y\ [p(x,y) \vee q(x,y) \vee q(y,x)]$$

jsou pravdivé v dané interpretaci, nejsou však univerzálními logickými tautologiemi (o tom se přesvědčíme např. tak, že prohodíme interpretaci predikátů p a q).

- Formule

$$p(x, g(y)) \vee \neg p(x, g(y)),\ \ \forall x \forall y\ [p(x, g(y)) \vee \neg p(x, g(y))]$$

jsou univerzálními tautologiemi daného jazyka. Jejich pravdivost nezávisí na tom, jakou množinu probíhají předmětové proměnné, jak je interpretován funkční symbol g a jak je interpretován predikátový symbol p. Naproti tomu formule

$$p(x, g(y)) \wedge \neg p(x, g(y)),\ \ \forall x \forall y\ [p(x, g(y)) \wedge \neg p(x, g(y))]$$

nejsou splnitelné v žádné interpretaci a jsou tedy univerzálními kontradikcemi.

Úloha 3.1.1: Ukažte, že formule $\exists x\ p(x) \supset p(a)$, kde a je individuová konstanta, není tautologií, ale je splnitelná.

Řešení: Jelikož formule nemá volné proměnné, stačí nalézt interpretaci, ve které je pravdivá, a interpretaci, ve které není pravdivá.

I. Universum M = množina přirozených čísel
   - p_M = množina lichých čísel
   - $a_M = 3$

II. Universum M = množina přirozených čísel
   - p_M = množina lichých čísel
   - $a_M = 4$

III. Universum M = množina všech individuí
- p_M = množina studentů VŠB v r. 2001/2002
- a_M = Tomáš Konečný

IV. Universum M = množina všech individuí
- p_M = množina studentů VŠB v r. 2001/2002
- a_M = Marie Duží

Nyní platí, že naše formule je pravdivá v interpretacích I. a III., nepravdivá v II. a IV. Tedy je splnitelná, ale není to tautologie.

Definice 3.1.6:

Formule A, B ***jsou (sémanticky) ekvivalentní***, jestliže pro všechny interpretace I a všechny valuace e mají stejná pravdivostní ohodnocení. Skutečnost, že formule A, B jsou ekvivalentní zapisujeme: $A \Leftrightarrow B$.

Poznámka 3.1.3:

Dvě formule jsou ekvivalentní právě tehdy, je-li formule $A \equiv B$ tautologií, tj.:

$A \Leftrightarrow B$ právě tehdy, když $\models A \equiv B$.

Následující dvě věty umožňují nalézat nové tautologie predikátové logiky na základě již známých tautologií výrokové logiky.

Věta 3.1.1:

Nechť platí:
- A je formule výrokové logiky sestavená z výrokových symbolů $p_1, p_2,...,p_n$,
- $B_1,B_2,...,B_n$ jsou libovolné formule predikátové logiky,
- formule A' vznikne z formule A náhradami proměnných $p_1, p_2,...,p_n$ formulemi $B_1, B_2,...,B_n$ (po řadě, tj. B_i za p_i)

Potom platí: je-li A tautologií výrokové logiky, je A' tautologií predikátové logiky.

Důkaz:

Pravdivostní hodnota formule A nezávisí na pravdivostních hodnotách formulí $p_1, p_2,...,p_n$ a tedy ani pravdivostní hodnota formule A' nezávisí na pravdivostních hodnotách formulí $B_1, B_2,...,B_n$.

Věta 3.1.2:

Nechť platí:
- Formule A obsahuje podformule $B_1, B_2,...,B_n$,
- formule $B_1, B_2,...,B_n$ jsou po řadě ekvivalentní s formulemi $B_1', B_2',...,B_n'$ /tj. $B_i \Leftrightarrow B_i'$/,
- formule A' vznikne z formule A náhradami formulí $B_1, B_2,...,B_n$ formulemi $B_1', B_2',...,B_n'$ (po řadě, tj. B_i' za B_i).

Potom platí: je-li A tautologií predikátové logiky, je i A' tautologií predikátové logiky.

Důkaz:

Ve formuli A nahrazujeme podformule formulemi se stejným pravdivostním ohodnocením (pro všechny (I, e)). Tedy pravdivostní ohodnocení formule A' musí být pro

všechny (I, e) stejné jako pravdivostní ohodnocení formule A. Je-li tedy A tautologií, je tautologií i A'.

Příklad 3.1.4 /některé důležité tautologie predikátové logiky/**:**

- Všechny formule predikátové logiky mající tvar tautologií výrokové logiky (viz věta 3.1.1), např. formule $\forall x\ \mathrm{p}(x) \supset (\mathrm{q}(y) \supset \forall x\ \mathrm{p}(x))$ je tautologií, protože má tvar formule výrokové logiky $\mathrm{r} \supset (\mathrm{s} \supset \mathrm{r})$, která je tautologií výrokové logiky.
- 1. $\models \forall x\mathrm{A}(x) \supset \mathrm{A}(y)$ dictum de omni specielně
  $\models \forall x\mathrm{A}(x) \supset \mathrm{A}(x/\mathrm{t})$
  2. $\models \mathrm{A}(y) \supset \exists x\mathrm{A}(x)$

- ***De Morganovy zákony***:
  3. $\models \neg\forall x\mathrm{A}(x) \equiv \exists x\neg\mathrm{A}(x)$
  4. $\models \neg\exists x\mathrm{A}(x) \equiv \forall x\neg\mathrm{A}(x)$

- ***Zákony distribuce kvantifikátorů***:
  5. $\models \forall x[\mathrm{A}(x) \supset \mathrm{B}(x)] \supset [\forall x\mathrm{A}(x) \supset \forall x\mathrm{B}(x)]$
  6. $\models \forall x[\mathrm{A}(x) \supset \mathrm{B}(x)] \supset [\exists x\mathrm{A}(x) \supset \exists x\mathrm{B}(x)]$
  7. $\models \forall x[\mathrm{A}(x) \wedge \mathrm{B}(x)] \equiv [\forall x\mathrm{A}(x) \wedge \forall x\mathrm{B}(x)]$
  8. $\models \exists x[\mathrm{A}(x) \wedge \mathrm{B}(x)] \supset [\exists x\mathrm{A}(x) \wedge \exists x\mathrm{B}(x)]$
  9. $\models [\forall x\mathrm{A}(x) \vee \forall x\mathrm{B}(x)] \supset \forall \mathrm{x}[\mathrm{A}(x) \vee \mathrm{B}(x)]$
  10. $\models \exists x[\mathrm{A}(x) \vee \mathrm{B}(x)] \equiv [\exists x\mathrm{A}(x) \vee \exists x\mathrm{B}(x)]$

- ***Zákony prenexních operací*** (předpokládáme, že formule A neobsahuje volnou proměnnou x):
  11. $\models \forall x[\mathrm{A} \supset \mathrm{B}(x)] \equiv [\mathrm{A} \supset \forall x\mathrm{B}(x)]$
  12. $\models \exists x[\mathrm{A} \supset \mathrm{B}(x)] \equiv [\mathrm{A} \supset \exists x\mathrm{B}(x)]$
  13. $\models \forall x[\mathrm{B}(x) \supset \mathrm{A}] \equiv [\exists x\mathrm{B}(x) \supset \mathrm{A}]$
  14. $\models \exists x[\mathrm{B}(x) \supset \mathrm{A}] \equiv [\forall x\mathrm{B}(x) \supset \mathrm{A}]$
  15. $\models \forall x[\mathrm{A} \wedge \mathrm{B}(x)] \equiv [\mathrm{A} \wedge \forall x\mathrm{B}(x)]$
  16. $\models \exists x[\mathrm{A} \wedge \mathrm{B}(x)] \equiv [\mathrm{A} \wedge \exists x\mathrm{B}(x)]$
  17. $\models \forall x[\mathrm{A} \vee \mathrm{B}(x)] \equiv [\mathrm{A} \vee \forall x\mathrm{B}(x)]$
  18. $\models \exists x[\mathrm{A} \vee \mathrm{B}(x)] \equiv [\mathrm{A} \vee \exists x\mathrm{B}(x)]$

- ***Zákony komutace kvantifikátorů***:
  19. $\models \forall x\forall y\mathrm{A}(x,y) \equiv \forall y\forall x\mathrm{A}(x,y)$
  20. $\models \exists x\exists y\mathrm{A}(x,y) \equiv \exists y\exists x\mathrm{A}(x,y)$
  21. $\models \exists x\forall y\mathrm{A}(x,y) \supset \forall y\exists x\mathrm{A}(x,y)$

Poznamenejme, že obrácená implikace k implikaci 21. neplatí. O tom se můžeme přesvědčit na následujícím příkladě. Nechť x, y jsou proměnné probíhající množinu reálných čísel a predikát A je interpretován jako relace $<$. V této interpretaci je formule $\forall y\exists x\mathrm{A}(x,y)$ pravdivá (ke každému y existuje x menší než y) a formule $\exists x\forall y\mathrm{A}(x,y)$ nepravdivá (existuje x, které je menší než všechna y). Formule

$$\forall y\exists x\mathrm{A}(x,y) \supset \exists x\forall y\mathrm{A}(x,y)$$

je v dané interpretaci nepravdivá a tedy to není tautologie.

Nechť term t je substituovatelný za proměnnou x:

22. $\models \forall x A(x) \supset A(x/t)$ ***zákon konkretizace***
23. $\models A(x/t) \supset \exists x A(x)$ ***zákon abstrakce***
24. $\models \forall x A(x) \supset \exists x A(x)$ ***zákon partikularizace***

Poznámky 3.1.4:

1) Tautologie 3. a 4. vysvětlují, jak chápeme v PL^1 "totalitu" a existenci. Tvrdíme-li, že nějakou vlastnost mají všechna individua, znamená to, že neexistuje žádné individuum, které by tu vlastnost nemělo. A tvrdíme-li, že existuje alespoň jedno individuum s určitou vlastností, znamená to, že ne všechna individua této vlastnosti nevyhovují. S tím souvisí požadavek stanovený pro interpretaci – totiž že **obor interpretace – universum diskursu** musí být **neprázdný.**

   Představme si interpretaci formulí $\forall x\ p(x)$ a $\exists x\ (p(x)$ nad prázdným universem ($M = \Phi$). Formule $\forall x\ p(x)$ bude pravdivá (neexistuje žádné individuum, které nemá vlastnost p), ovšem stejně tak formule $\forall x\ \neg p(x)$ bude pravdivá (neexistuje žádné individuum, které má vlastnost p). Když nyní budeme interpretovat formuli $\exists x\ p(x)$, dospějeme k závěru, že je nepravdivá (nenajdeme individuum s vlastností p) a podobně je nepravdivá formule $\exists x\ \neg p(x)$ (neboť všechna – tj. žádné – individua mají vlastnost p). Tedy zákon partikularizace (tautologie 24) by byl nepravdivý. Tím se však dostáváme do rozporu s intuicí, protože tvrzení "co platí pro všechny, platí i pro některé" lze považovat za pravdivý "axióm". Jak vidíme, neplatilo by pro "pustý svět".

2) Každé tautologii predikátové logiky ve tvaru ekvivalence odpovídá ekvivalence formulí a obráceně. Tak např.ekvivalenci

   $$\neg\forall x\ A(x) \Leftrightarrow \exists x\ \neg A(x)$$

   odpovídá tautologie

   $$\models \neg\forall x\ A(x) \equiv \exists x\ \neg A(x).$$

   Na základě těchto ekvivalencí můžeme provádět ***ekvivalentní úpravy formulí*** predikátové logiky.

3) Každý jazyk predikátové logiky má nekonečně mnoho možných interpretací (už jenom universum diskursu lze stanovit nekonečně mnoha způsoby). Tím se liší od jazyka výrokové logiky, který má vždy jen konečný počet interpretací – valuací 0-1 výrokových symbolů (jazyk výrokové logiky pracující s n výrokovými symboly má 2^n interpretací). Tautologičnost formulí predikátové logiky nelze proto sémanticky dokazovat tak, že ukážeme, že každá možná interpretace jazyka je i modelem dané formule. Tímto způsobem jsme postupovali ve výrokové logice, když jsme zjišťovali pravdivostní hodnotu formule pro každou kombinaci pravdivostních hodnot výrokových symbolů.

4) Chceme-li nalézt sémantické zdůvodnění, zda je daná formule tautologie, či zda je daný úsudek platný, využíváme často tyto dvě metody:

   - ***"Důkaz" převodem na výrokovou logiku*** za předpokladu konečného univerza.

     $$\models \neg\forall x\ A(x) \equiv \exists x\ \neg A(x)$$

     "Důkaz" (za předpokladu M={a,b}):

     $$\neg\forall x\ A(x) \Leftrightarrow \neg[A(a) \wedge A(b)] \Leftrightarrow \neg A(a) \vee \neg A(b) \Leftrightarrow \exists x\ \neg A(x)$$

   - ***Množinový "důkaz"*** převodem na množinové úvahy o oborech pravdivosti predikátů. Platí totiž:

Je-li $\models_I \forall x\, p(x)$, pak $p_M = M$
Je-li $\models_I \exists x\, p(x)$, pak $p_M \neq \Phi$
Je-li $\models_I \forall x\, [p(x) \supset q(x)]$, pak $p_M \subseteq q_M$
Je-li $\models_I \exists x\, [p(x) \wedge q(x)]$, pak $(p_M \cap q_M) \neq \Phi$

Na ukázku dokažme 5. schéma tautologií z předchozího příkladu.
$\models \forall x[A(x) \supset B(x)] \supset [\forall x\, A(x) \supset \forall x B(x)]$

"Důkaz" /množinový/:
1. $\forall$x[A(x) $\supset$ B(x)] předpoklad
   obor pravdivosti A $\subseteq$ obor pravdivosti B
2. $\forall x$A(x) předpoklad
   obor pravdivosti A = celé univerzum M
3. $\forall x$B(x) z 1.a 2.
   obor pravdivosti B = celé univerzum M Q.E.D.

Příklad 3.1.5 /Sémantické ověření správnosti úsudku/

Sémantické ověření správnosti úsudku je v predikátové logice rovněž obtížnější než ve VL. Podle definice je úsudek správný, pokud je závěr pravdivý ve všech modelech předpokladů. Problémem v PL^1 je ovšem to, že takovýchto modelů je obecně nekonečně mnoho. Přesto je možno sémanticky ověřit platnost úsudku, a to přímo, nebo nejčastěji sporem (předpokládáme, že může nastat případ, kdy v nějaké interpretaci budou předpoklady pravdivé a závěr nepravdivý a ukážeme, že to možné není).

a) Marie má ráda pouze vítěze.
Karel je vítěz.
_____
Marie má ráda Karla.

$\forall x\, [R(M,x) \supset V(x)]$
$V(K)$
_____
$R(M,K)$

Aby byly předpoklady pravdivé, pak možné interpretace nad množinou individuí D musí mít tvar:

M_D : Marie, K_D : Karel (Pozor! realizací těchto konstant mohou být kterékoli jiné prvky D, třeba α, β, avšak celková úvaha se tím nijak nemění.)
$R_D \subset D \times D$: {… <Marie, i_1>, <Marie, i_2>, …, <Marie, i_n> …}
$V_D \subset D$: {…i_1, i_2, …, Karel,…, i_n…}

Vidíme, že závěr nevyplývá, neboť není zaručeno, že relace R_D bude obsahovat dvojici <Marie, Karel>.

b) Marie má ráda pouze vítěze.
Karel není vítěz.
_____
Marie nemá ráda Karla.

$\forall x\, [R(M,x) \supset V(x)]$
$\neg V(K)$

$\neg R(M,K)$

Aby byly předpoklady pravdivé, pak možné interpretace nad množinou individuí D musí mít tvar:

$R_D \subset D \times D$: {… <Marie, i_1>, <Marie, i_2>, …, <Marie, i_n> …}

$V_D \subset D$: {…i_1, i_2, …, ~~Karel~~,…, i_n…} – individuum Karel neleží v množině V_D, tedy Karel se nerovná žádnému z individuí i_1, i_2,…,i_n, které jsou v relaci R_D s individuem Marie.

Vidíme, že závěr vyplývá, neboť je zaručeno, že relace R_D nemůže obsahovat dvojici <Marie, Karel>.

c) Kdo zná Marii i Pavla, ten Marii lituje.
Někteří nelitují Marii, ačkoliv ji znají.

Někdo zná Marii, ale ne Pavla.

$\forall x\ (\ [Z(x,M) \wedge Z(x,P)] \supset L(x,M)\ )$
$\exists x\ [\ \neg L(x,M) \wedge Z(x,M)\ ]$

$\exists x\ [Z(x,M) \wedge \neg Z(x,P)\ ]$

Provedeme důkaz sporem, tedy budeme předpokládat, že nastane v nějaké interpretaci případ, kdy jsou předpoklady pravdivé a závěr nepravdivý, tedy je pravdivá formule $\forall x\ [Z(x,M) \supset Z(x,P)]$.

Aby byly předpoklady pravdivé, pak možné interpretace nad množinou individuí D musí mít tvar:

$Z_D \subset D \times D$: {… <i_1,Marie >, <i_2,Marie >, …, <i_n,Marie >, …,<α,Marie >
<i_1,Pavel >, <i_2,Pavel>, …, <i_n,Pavel>…}

$L_D \subset D \times D$: {… <i_1,Marie >, <i_2,Marie >, …, <i_n,Marie >, …,~~<α,Marie >~~…}

První předpoklad tvrdí, že všechna individua, která jsou v relaci Z_D s individui Marie i Pavel, nechť to jsou i_1, i_2,…,i_n, jsou také v relaci L_D s individuem Marie.

Dle druhého předpokladu existuje nějaké individuum, nechť je to α, které je v relaci Z_D spolu s Marií, ale tato dvojice není v relaci L_D. Tedy α nemůže být jedno z individuí i_1,…,i_n.

Je-li nyní pravdivá formule $\forall x\ [Z(x,M) \supset Z(x,P)]$, pak to znamená, že všechna taková individua i_j, která tvoří dvojici <i_j,Marie> v Z_D (tj. také individuum α), musí tvořit dvojici <i_j,Pavel>, která rovněž leží v Z_D. To však není možné, protože <α,Pavel> neleží v Z_D.

Poznámka 3.1.5.

Úsudek a) ilustruje poměrně častou chybu, které se můžeme v argumentaci dopustit. Z platnosti nutné podmínky nějakého tvrzení usuzujeme na pravdivost tohoto tvrzení. V našem příkladě je podmínka ”být vítězem” pouze ***nutná*****,** ne však ***dostatečná*** pro to, aby Marie měla dané individuum ráda (vítězové tedy mohou být i taková individua, která Marie nemá ráda). Uvažme následující dva úsudky:

Prvočísla mají přesně dva dělitele. (mít přesně dva dělitele je nutná podmínka)
Číslo 5 má přesně dva dělitele.
_____ **neplatný úsudek**
Číslo 5 je prvočíslo.

$\forall x\,[P(x) \supset D(x)]$ (”zamýšlená interpretace” predikátu D je
D(5) ‘mít přesně dva dělitele’)
_____ **neplatný úsudek**
P(5)

Pouze prvočísla mají přesně dva dělitele. (”mít přesně dva dělitele” je dostatečná podmínka pro ”být prvočíslem”)
Číslo 5 má přesně dva dělitele.
_____ **platný úsudek**
Číslo 5 je prvočíslo.

$\forall x\,[D(x) \supset P(x)]$
D(5)
_____ **platný úsudek**
P(5)

Pokud bychom chtěli pomocí počtu dělitelů množinu prvočísel ***definovat,*** pak musíme použít ***nutnou a dostatečnou*** podmínku:

Prvočísla jsou pouze a právě ta čísla, která mají přesně dva dělitele.

$\forall x\,[D(x) \equiv P(x)]$

Příklad 3.1.6 /ekvivalence a tautologie/:

a) Ověříme sémanticky, že následující věta je **tautologie**:

Existuje někdo takový, že je-li génius, pak jsou všichni géniové.

(Věta pochopitelně neříká, že jestliže existují géniové, pak jsou všichni géniové.)
Analýza: $\exists x\,[G(x) \supset \forall y\,G(y)]$
Uvažujme nyní možné interpretace. Ať je universum U jakékoli, máme dvě možnosti:

1. $G_U \subset U$ (G_U je vlastní podmnožinou $U - G_U \neq U$). V této interpretaci je formule pravdivá, neboť existuje valuace x taková, že $e(x) \notin G_U$. Pak je antecedent implikace nepravdivý, a tedy celá formule je pravdivá.
2. $G_U = U$. V této interpretaci je formule zřejmě rovněž pravdivá.

Tedy formule je pravdivá v každé interpretaci – tautologie.
Pozn.: Příklad demonstruje, jak je podmínka vyjádřená implikací za existenčním kvantifikátorem ”slabá”. Aby byla formule pravdivá, stačí za x zvolit kterýkoli prvek universa, který nesplňuje antecedent implikace.

b) Ověříme, že následující věty jsou **ekvivalentní** (tedy mají naprosto stejné pravdivostní podmínky):

Jana obdivuje pouze vítěze.

Jana neobdivuje nikoho, kdo není vítěz.
Neexistuje nikdo, kdo by nebyl vítěz a Jana jej obdivovala.

Analýza: $\forall x\,[O(J,x) \supset V(x)] \quad \Leftrightarrow \forall x\,[\neg O(J,x) \vee V(x)]$
$\forall x\,[\neg V(x) \supset \neg O(J,x)] \Leftrightarrow \forall x\,[V(x) \vee \neg O(J,x)]$
$\neg\exists x\,[\neg V(x) \wedge O(J,x)] \Leftrightarrow \forall x\,[V(x) \vee \neg O(J,x)]$
Tedy analýzou a pomocí ekvivalentních úprav jsme ověřili, že naše věty "říkají totéž", jsou ekvivalentní.

Příklad 3.1.7 /speciální kvantifikátory/:

Vedle základních standardních kvantifikací
$\forall x$ A(x) ... všechny prvky universa mají vlastnost A (obor pravdivosti A = celé univer. M)
$\exists x$ A(x) ...existuje (aspoň jeden) prvek universa s vlastností A (obor pravdivosti A je neprázdný)

zavedeme ještě následující nestandardní kvantifikace:
$(\forall B(x))A(x)$ ... všechny prvky s vlastností B mají vlastnost A
$(\exists B(x))A(x)$ ... existuje prvek s vlastností B, který má vlastnost A
$\exists_1 x A(x)$ ..... existuje právě jeden prvek s vlastností A ("existuje to jediné x, že A")

Nestandardní kvantifikátory mohou být definovány pomocí standardních kvantifikátorů takto:
$(\forall B(x))A(x) =_{df} \forall x\,[B(x) \supset A(x)]$ ohraničený obecný kvantifikátor
$(\exists B(x))A(x) =_{df} \exists x\,[B(x) \wedge A(x)]$ ohraničený existenční kvantifikátor
$\exists_1 x A(x) =_{df} \exists x A(x) \wedge [\forall y\, A(y) \supset (y = x)]$

Příklady na užití nestandardních kvantifikátorů v matematice:

- Reálná funkce f(x) je na intervalu (a,b) spojitá:
  $(\forall \varepsilon > 0)\,(\forall x \in (a,b))\,(\forall y \in (a,b))\,(\exists \delta > 0)\,[|x - y| < \delta \supset |f(x) - f(y)| < \varepsilon]$
- Reálná funkce f(x) je na intervalu (a,b) stejnoměrně spojitá:
  $(\forall \varepsilon > 0)\,(\exists \delta > 0)\,(\forall x \in (a,b))\,(\forall y \in (a,b))\,[|x - y| < \delta \supset |f(x) - f(y)| < \varepsilon]$
- Rovnice $a.x + b = 0$ má pro $a \neq 0$ jediné řešení:
  $(\forall a \neq 0)(\forall b)(\exists_1 x)[a.x + b = 0]$

Definice 3.1.7:

Nechť formule F je utvořena z elementárních formulí A, B,... pouze pomocí funktorů $\neg, \wedge, \vee, \forall, \exists$. Formuli F', která vznikne z formule F vzájemnými záměnami funktorů $\wedge$ a $\vee$ a vzájemnými záměnami funktorů $\forall$ a $\exists$, nazýváme ***duální formulí*** k formuli F.

Vzhledem k tomu, že F'' = F, jsou formule F a F´ ***duálními navzájem***.

Věta 3.1.3 /věty o dualitě/**:**

1. $\models \neg F(A, B,...) \equiv F'(\neg A, \neg B,...)$, neboli: $\neg F(A, B,...) \Leftrightarrow F'(\neg A, \neg B,...)$,
2. $\models F \supset G$ právě tehdy, když $\models G' \supset F'$,
3. $\models F \equiv G$ právě tehdy, když $\models F' \equiv G'$.

Důkaz:
Ad 1:

Důkaz provedeme matematickou indukcí podle struktury formule F. Nejdříve dokážeme platnost tvrzení v případě, že F je elementární formulí /báze indukce/. Potom z předpokládané platnosti tvrzení pro formule H, G dokážeme platnost tvrzení pro složenou formuli F tvaru $\neg H$, $H \wedge G$, $H \vee G$, $\forall H$, $\exists H$ /indukční krok/.

- Nechť $F(A, B,...) = A$. Potom
  $\neg F(A, B,...) \Leftrightarrow \neg A \Leftrightarrow (\neg A)' \Leftrightarrow F'(\neg A, \neg B,...)$
  a tvrzení je dokázáno.
- Nechť $F(A, B,...) = \neg H(A, B,...)$. Potom platí:
  $\neg F(A, B,...) \Leftrightarrow \neg\neg H(A, B,...) \Leftrightarrow$ podle předpokladu $F = \neg H$
  $\Leftrightarrow \neg H'(\neg A, \neg B,...) \Leftrightarrow$ podle indukčního předpokladu
  $\Leftrightarrow (\neg H(\neg A, \neg B,...))' \Leftrightarrow$ podle definice duální formule
  $\Leftrightarrow F'(\neg A, \neg B,...)$ podle předpokladu $F = \neg H$, Q.E.D.
- Nechť $F(A, B,...) = H(A, B,...) \wedge G(A, B,...)$. Potom platí:
  $\neg F(A, B,...) = \neg(H(A, B,...) \wedge G(A, B,...)) \Leftrightarrow$ podle předpokladu $F = H \wedge G$
  $\Leftrightarrow \neg H(A, B,...) \vee \neg G(A, B,...) \Leftrightarrow$ podle de Morganova zákona
  $\Leftrightarrow H'(\neg A, \neg B,...) \vee G'(\neg A, \neg B,...) \Leftrightarrow$ podle indukčního předpokladu
  $\Leftrightarrow (H(\neg A, \neg B,...) \wedge G(\neg A, \neg B,...))' \Leftrightarrow$ podle definice duální formule
  $\Leftrightarrow F'(\neg A, \neg B,...)$ podle předpokladu $F = H \wedge G$, Q.E.D.
- Nechť $F(A, B,...) = H(A, B,...) \vee G(A, B,...)$. Důkaz probíhá obdobně jako v předchozím bodě.
- Nechť $F(A, B,...) = \forall x\, H(A, B,...)$. Potom platí:
  $\neg F(A, B,...) = \neg\forall x\, H(A, B,...) \Leftrightarrow$ podle předpokladu $F = \forall x H$
  $\Leftrightarrow \exists x\, \neg H(A, B,...) \Leftrightarrow$ podle de Morganova zákona
  $\Leftrightarrow \exists x\, H'(\neg A, \neg B,...) \Leftrightarrow$ podle indukčního předpokladu
  $\Leftrightarrow (\forall x\, H(\neg A, \neg B,...))' \Leftrightarrow$ podle definice duální formule
  $\Leftrightarrow F'(\neg A, \neg B,...)$ podle předpokladu $F = \forall x H$, Q.E.D.
- Nechť $F(A, B,...) = \exists x\, H(A, B,...)$. Důkaz probíhá obdobně jako v předchozím bodě.

Ad 2:

1. $F(A, B,...) \supset G(A, B,...)$	předpoklad
2. $\neg G(A, B,...) \supset \neg F(A, B,...)$	podle pravidla: $F \supset G \Leftrightarrow \neg G \supset \neg F$
3. $G'(\neg A, \neg B,...) \supset F''(\neg A, \neg B,...)$	podle 1.věty o dualitě
4. $G'(A, B,...) \supset F'(A, B,...)$	substitucemi $\neg A/A$, $\neg B/B$, ...

Ad 3:

1. $F \equiv G$	předpoklad
2. $F \supset G$	EE: 1
3. $G \supset F$	EE: 1
4. $G' \supset F'$	podle 2.věty o dualitě: 2
5. $F' \supset G'$	podle 2.věty o dualitě: 3
6. $F' \equiv G'$	ZE: 4,5

Příklady 3.1.8 /k principům duality/**:**

Ad 1:

- $\models \neg(\forall x\, p(x) \vee p(y)) \equiv \exists x\, \neg p(x) \wedge \neg p(y)$
- $\models \neg\exists x\, \forall y\, p(x,y) \equiv \forall x\, \exists y\, \neg p(x,y)$

Ad 2:

- $\models \forall x\, p(x) \supset p(y)$,
  $\models p(y) \supset \exists x\, p(x)$
- $\models [\forall x\, p(x) \vee \forall x\, q(x)] \supset \forall x\, [p(x) \vee q(x)]$,
  $\models \exists x\, [p(x) \wedge q(x)] \supset [\exists x\, p(x) \wedge \exists x\, q(x)]$

Ad 3:

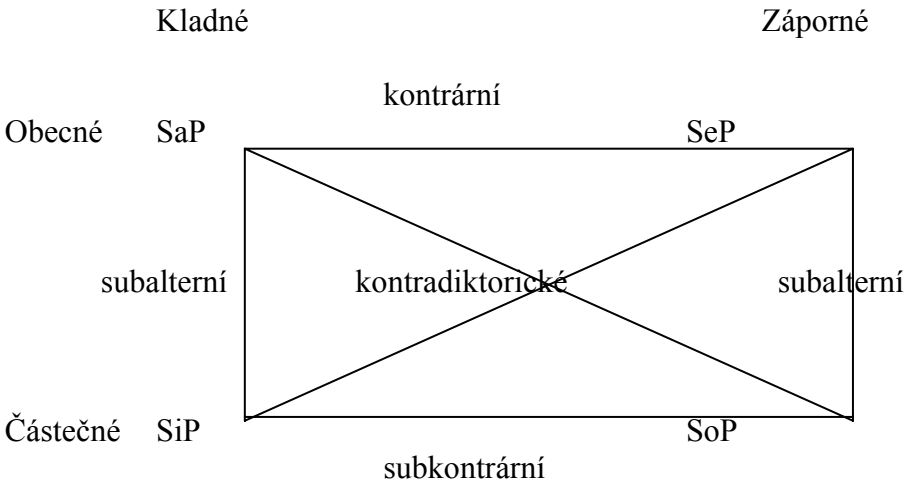
- $\models \forall x\, [p(x) \wedge q(x)] \equiv [\forall x\, p(x) \wedge \forall x\, q(x)]$,
  $\models \exists x\, [p(x) \vee q(x)] \equiv [\exists x\, p(x) \vee \exists x\, q(x)]$
- $\models \forall x\, [A \wedge B(x)] \equiv [A \wedge \forall x B(x)]$
  $\models \exists x\, [A' \vee B'(x)] \equiv [A' \vee \exists x\, B'(x)]$

3.1.1. Tradiční Aristotelova logika

Tradiční Aristotelova logika je fragment predikátové logiky 1. řádu, který je omezen pouze na jednomístné predikáty. Tato logika byla (v podstatě jako jediná) vyučována ještě v 19. století. Umožňuje kontrolovat správnost zvláštního typu jednoduchého úsudku, který se nazývá ***kategorický sylogismus***. Tyto úsudky zkoumal před více než 2000 lety řecký filosof a zakladatel logiky Aristoteles. Aristotelova logika vznikla kupodivu dříve než výroková logika, kterou zkoumali *stoici.* Stoici byli v jisté opozici vůči Aristotelovi a z jejich díla se zachovaly jen fragmenty, ze kterých je však zjevné, že používali rozvinutý systém výrokové logiky a v podstatě (i když poněkud v jiné formě) i systém predikátové logiky 1. řádu.

Aristotelova logika zkoumá tzv. ***subjekt – predikátové* výroky** (S-P výroky), kde S i P jsou nějaké vlastnosti (formalizované jako predikáty). Tyto výroky dělí na obecné a částečné, kladné a záporné. Všechny možnosti a jejich vzájemný vztah jsou znázorněny ***logickým čtvercem,*** kde význam zkratek je odvozen z latinského ***affirmo*** (tvrdím) a ***nego*** (popírám):

SaP – Všechna S jsou P
SeP – Žádné S není P
SiP – Některá S jsou P
SoP – Některá S nejsou P



Logický čtverec znázorňuje jednoduché úsudky platné mezi těmito výroky.

1) Kontradiktorické (protikladné, jeden je vždy ekvivalentní negaci druhého):
   SaP ≡ ¬SoP SeP ≡ ¬SiP
2) Kontrární (z jednoho vyplývá negace druhého):
   SaP |= ¬SeP SeP |= ¬SaP
   Může však být zároveň nepravda jak SaP tak SeP (tedy ani Sap ani Sep není pravda): Všechny houby jsou jedlé, všechny houby jsou nejedlé.
3) Subkontrární (podprotivné):
   ¬SiP |= SoP ¬SoP |= SiP

Může však být SiP i SoP pravdivé:
Některé labutě jsou černé, některé labutě nejsou černé

4) Subalterní (podřízený):
SaP |= SiP SeP |= Sop ¬SiP |= ¬SaP ¬SoP |= ¬SeP

Dále platí tzv. obraty:

5) Obraty.
SiP |= PiSSeP |= PeS
Někteří studenti jsou ženatí |= Někteří ženatí jsou studenti
Žádný člověk není strom |= Žádný strom není člověk
SaP |= PiS SeP |= PoS
Všichni učitelé jsou státní zaměstnanci |= Někteří státní zaměstnanci jsou učitelé
Žádné jedovaté houby nejsou jedlé |= Některé jedlé houby nejsou jedovaté

(Kategorické) ***Sylogismy*** jsou úsudky, které sestávají ze tří S-P výroků tvaru (4 figury):

M P	P M	M P	P M
S M	S M	M S	M S
I. ——	II. ——	III. ———	IV. ——
S P	S P	S P	S P

Kombinací a, e, i, o lze nyní vytvořit 64 tzv. modů, z nichž jen některé jsou platné.

Platné módy se pochopitelně neučíme nazpaměť (jako to kdysi dělali naši otcové), neboť jejich platnost můžeme snadno ověřit i sémanticky, na základě množinových úvah, které můžeme znázornit geometricky (např. metodou známých Vénových kroužků):
Obory pravdivosti predikátů S, P, M zakreslíme jako (vzájemně se protínající) kroužky. Poté znázorníme situaci, kdy jsou premisy pravdivé, tj.

1) Vyšrafujeme plochy, které odpovídají prázdným třídám objektů
2) Označíme křížkem plochy, které jsou jistě neprázdné (křížek přitom klademe jen tehdy, když neexistuje jiná plocha, "kam by mohl přijít")

Nakonec ověříme, zda vzniklá situace znázorňuje pravdivost závěru.

Příklad 3.1.9: (Ověřte graficky)

Všechny velryby jsou savci.
Někteří vodní živočichové jsou velryby.
U_1 ——————————————— Správný úsudek
Někteří vodní živočichové jsou savci.

Žádný učený z nebe nespadl
Všechno co spadlo z nebe je voda
U_2 ——————————————— Nesprávný úsudek
Žádná voda není učená

Všechna auta jsou dopravní prostředky

U_3
Všechna auta mají volant
———————————————
Některé dopravní prostředky mají volant
Nesprávný úsudek

U_4
Všechny myši jsou hranaté
Všechno hranaté je modré
———————————————
Všechny myši jsou modré
Správný úsudek

U_5
Nikdo s fialovými vlasy není starý
Někteří lidé, kteří mají fialové vlasy, pijí mléko
———————————————
Někteří lidé, kteří pijí mléko nejsou staří
Správný úsudek

U_6
Všichni jezevci jsou sběratelé umění
Někteří sběratelé umění žijí v norách
———————————————
Někteří jezevci žijí v norách
Nesprávný úsudek

Pozn.: Úsudek U_3 možná čtenáře překvapí. Jak je možné, že je tento úsudek neplatný? Vždyť přece za předpokladu pravdivosti premis musí platit, že některé dopravní prostředky mají volant, a to alespoň ta auta! Pokud si však situaci znázorníme Vénovými kroužky, zjistíme, že tomu tak není. Premisy nás opravňují pouze k vyšrafování ploch odpovídajících formulím:
$\neg\exists x\,[A(x) \wedge \neg V(x)]$, $\neg\exists x\,[A(x) \wedge \neg D(x)]$
("neexistují auta bez volantu" a "neexistují auta, která by nebyla dopravním prostředkem"), ale křížek na ploše odpovídající formuli $\exists x\,[A(x) \wedge V(x) \wedge D(x)]$, tedy průniku "aut, volantů a dopravních prostředků" se nenachází! Jistě, vždyť pravdivost premis nám ***nezaručuje existenci aut***! V době, kdy žádná auta neexistovala, byly premisy triviálně pravdivé, ale závěr být pravdivý nemusel.
Obdobný příklad (nyní již zjevně) nesprávného úsudku je znám od Bertranda Russella:

Všechny skleněné hory jsou hory
Všechny skleněné hory jsou skleněné
———————————————
Některé hory jsou skleněné
Nesprávný úsudek

Jde o běžnou a poměrně častou chybu, kdy ze všeobecných premis usuzujeme na existenci. R. M. Smullyan uvádí ve své velmi zdařilé knize "Jak se jmenuje tato knížka?" příklad uplatnění takovéhoto "argumentu", pomocí kterého "dokáže" existenci jednorožce.

Poznamenejme ještě, že v tradiční Aristotelově logice je tento mód (tedy úsudkové schéma) považován za ***platný.*** Je to proto, že Aristoteles dodává pro sylogismy podmínku, že ***všechny použité pojmy jsou neprázdné.*** Z tohoto pohledu není Russelův příklad sylogismem.

3.2. Automatické dokazování v predikátové logice (obecná rezoluční metoda)

Jak jsme uvedli v předchozí kapitole, sémantický důkaz logické pravdivosti, a tedy i logického vyplývání apod., zkoumáním všech možných interpretací, je v predikátové logice často obtížný. Jednou z efektivních metod je však rezoluční metoda, která je pro PL^1 zobecněním základní rezoluční metody výrokové logiky, kterou jsme se zabývali v kap. 2.2. Tato obecná rezoluční metoda se stala základem pro logické programování, zejména programovací jazyk PROLOG (Programming in Logic).

Rezoluční metoda je jedna z procedur (algoritmů), které parciálně rozhodují, zda daná formule PL^1 je nesplnitelná. Pro předloženou formuli A, která nesplnitelná je, tedy procedura v konečném čase tuto skutečnost zjistí a zastaví se. V případě, že A je splnitelná, algoritmus nemusí nikdy skončit svou činnost. Chceme-li tedy rozhodnout, zda daná formule A je logicky pravdivá, použijeme rezoluční metodu na formuli $\neg A$ a zjišťujeme, zda je nesplnitelná. Je-li tomu tak, procedura to zjistí a vydá kladnou odpověď. V opačném případě proces nemusí nikdy skončit. Specielně, chceme-li zjistit, zda $\{A_1,\ldots,A_n\} \models B$, aplikujeme rezoluční metodu na formuli $A_1 \wedge \ldots \wedge A_n \wedge \neg B$, neboť pokud je tato formule nesplnitelná, pak je formule $(A_1 \wedge \ldots \wedge A_n) \supset B$ tautologie a vztah vyplývání platí.

Rezoluční metodu lze aplikovat pouze na formule speciálního tvaru, v tzv. **klauzulární (Skolemově) formě**. Nejprve proto ukážeme, že každou formuli je možno převést do klauzulární formy tak, že výsledná formule je splnitelná, právě když výchozí formule je splnitelná. Potom uvedeme Herbrandovu větu, o niž se opírají první známé rozhodovací procedury pro dokazování nesplnitelnosti v predikátové logice 1. řádu. Uplatnění rezolučního pravidla výrokové logiky je totiž v PL^1 komplikováno tím, že v literálech se vyskytují termy obecně různého "tvaru", které je nutno nějak "unifikovat". Popíšeme tzv. základní rezoluční metodu pro PL^1, která je značně neefektivní. Průlomem v těchto metodách se však stal Robinsonův objev unifikačního algoritmu, který umožnil zobecnění základní rezoluční metody na mnohem účinnější rezoluční metodu, která se pak stala základem logického programování.

Automatické dokazování v predikátové logice zobecňuje postupy automatického dokazování výrokové logiky. Oproti situaci ve výrokové logice je situace v predikátové logice složitější a to z těchto důvodů:

- Komplikovanější je procedura převedení formule na klauzulární tvar. Oproti výrokové logice obsahuje navíc:
  - převod formule na prenexní tvar,
  - eliminaci kvantifikátorů z formule.
- Složitější je tvar rezolučního odvozovacího pravidla. Jeho použití vyžaduje simultánní úpravu literálů, tzv. unifikaci.

Definice 3.2.1:

Formule A predikátové logiky je v ***prenexním tvaru***, má-li podobu

$$Q_1x_1\ Q_2x_2 \ldots Q_nx_n\ B,$$

kde

- $n \geq 0$ a pro každé $i = 1, 2,\ldots,n$ je Q_i buď všeobecný kvantifikátor $\forall$ nebo existenční $\exists$,
- $x_1, x_2,\ldots,x_n$ jsou navzájem různé individuové proměnné,

- B je formule utvořená z elementárních formulí pouze užitím výrokových funktorů $\neg$, $\wedge$, $\vee$.

Výraz $Q_1x_1\ Q_2x_2...Q_nx_n$ se nazývá ***prefix (charakteristika)*** a B ***otevřeným jádrem (maticí)*** formule A v prenexním tvaru.

Věta 3.2.1:

Každou formuli lze přepsat do prenexního tvaru, tj. ke každé formuli predikátové logiky A existuje formule A^* v prenexním tvaru, která je s formulí A ekvivalentní (tj. $A \Leftrightarrow A^*$).

Důkaz:

Matematickou indukcí podle hierarchického řádu formule A.

1. Báze indukce. Formule řádu 0 (elementární formule) neobsahují žádné funktory (a tedy ani kvantifikátory) a jsou tedy automaticky v prenexním tvaru. Tvrzení věty tedy platí.
2. Indukční krok. Ukážeme, že platí-li tvrzení věty pro formule B, C, pak platí také pro formule $\forall x$B, $\exists x$B, $\neg$B, B $\wedge$ C, B $\vee$ C, B $\supset$ C, B $\equiv$ C (tj. platnost věty se přenáší z formulí nižšího řádu na formule řádu vyššího).
   - Je-li A = $\forall x$B nebo A = $\exists x$B, pak vzhledem k tomu, že B je v prenexním tvaru (indukční předpoklad), je i A v prenexním tvaru, tj. $A \Leftrightarrow A^*$.
   - Nechť A = $\neg$B. Formule B je podle indukčního předpokladu v prenexním tvaru, tj.
     $$B = Q_1x_1\ Q_2x_2...Q_nx_n\ D,$$
     kde Q_i jsou $\forall$ nebo $\exists$ a D je formule bez kvantifikátorů. Potom n-násobným použitím de Morganova zákona $\neg QxF \equiv Q'x\ \neg F$ (Q' je duální kvantifikátor ke Q), dostáváme
     $$A = \neg Q_1x_1\ Q_2x_2...Q_nx_n\ D \Leftrightarrow Q_1'x_1\ Q_2'x_2...Q_n'x_n\ \neg D \Leftrightarrow A^*$$
     a formule A je převedena do ekvivalentního prenexního tvaru A^*.
   - Nechť A = B $\wedge$ C. Formule B, C jsou podle indukčního předpokladu v prenexním tvaru, tj.
     $$B = Q_{1B}x_1\ Q_{2B}x_2...Q_{mB}x_m\ F,\ \ C = Q_{1C}y_1\ Q_{2C}y_2...Q_{nC}y_n\ G,$$
     kde F, G jsou formule bez kvantifikátorů. Máme dokázat, že existuje formule A^* ekvivalentní s formulí A. To zajisté platí, je-li k = n + m = 0. Tvrzení bude dokázáno, jestliže z předpokládané platnosti pro k = n + m - 1 dokážeme platnost pro k = n + m. Důkazem je následující řetěz ekvivalencí:
     $$A = B \wedge Q_{1C}y_1\ G_1 \Leftrightarrow Q_{1C}y_1\ B \wedge G_1 \Leftrightarrow Q_{1C}y_1\ (B \wedge G_1)^* \Leftrightarrow A^*.$$
     Formule B $\wedge$ G_1 obsahuje totiž jen n + m -1 kvantifikátorů a lze tedy na ni použít indukční předpoklad.
   - Pro složené formule B $\vee$ C, B $\supset$ C, B $\equiv$ C lze indukční krok dokázat podobným způsobem jako v předchozím bodě. Vzhledem k tomu, že
     $B \vee C \Leftrightarrow \neg(\neg B \wedge \neg C)$, $B \supset C \Leftrightarrow \neg(B \wedge \neg C)$, $B \equiv C \Leftrightarrow \neg(B \wedge \neg C) \wedge \neg(C \wedge \neg B)$,
     je však důkaz indukčního kroku pro $\vee$, $\supset$, $\equiv$ nadbytečný.

Algoritmus /převod formule do prenexního tvaru/**:**

(1) Eliminace funktorů $\supset$ a $\equiv$. Toho lze dosáhnout užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$$A \supset B \Leftrightarrow \neg A \vee B,$$
$$A \equiv B \Leftrightarrow (A \supset B) \wedge (B \supset A) \Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A).$$

(2) Převedení formule na tvar s čistými proměnnými.

a) Použijeme následující ekvivalence (náhrady levé strany pravou):
$(\forall x A \wedge \forall x B) \Leftrightarrow \forall x\,(A \wedge B)$ $\quad$ $(\exists x A \vee \exists x B) \Leftrightarrow \exists x\,(A \vee B)$

b) Přejmenování vázaných proměnných tak, aby žádná proměnná nebyla ve formuli současně volná i vázaná a tak, aby všechny vázané proměnné byly navzájem různé. To platí nejenom pro celou formuli, ale i pro každou její podformuli.

(3) Vypuštění nadbytečných kvantifikátorů, tj. kvantifikátorů jejichž oblast působnosti neobsahuje žádný výskyt kvantifikované proměnné.

(4) Přenesení všech výskytů funktoru negace bezprostředně před elementární formule. Toho lze dosáhnout opakovaným užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$$\neg\neg A \Leftrightarrow A,$$
$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B,$$
$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B,$$
$$\neg\forall x\, A(x) \Leftrightarrow \exists x\, \neg A(x),$$
$$\neg\exists x\, A(x) \Leftrightarrow \forall x\, \neg A(x).$$

(5) Přenesení všech kvantifikátorů na začátek formule. Toho lze dosáhnout opakovaným užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$\forall x A \wedge B \Leftrightarrow \forall x\,(A \wedge B)$	$\exists x A \vee B \Leftrightarrow \exists x\,(A \vee B)$	B neobsahuje volnou x
$A \wedge \forall x B \Leftrightarrow \forall x\,(A \wedge B)$	$A \vee \exists x B \Leftrightarrow \exists x\,(A \vee B)$	A neobsahuje volnou x
$\exists x A \wedge B \Leftrightarrow \exists x\,(A \wedge B)$	$\forall x A \vee B \Leftrightarrow \forall x\,(A \vee B)$	B neobsahuje volnou x
$A \wedge \exists x B \Leftrightarrow \exists x\,(A \wedge B)$	$A \vee \forall x B \Leftrightarrow \forall x\,(A \vee B)$	A neobsahuje volnou x

Příklad 3.2.1:

Nalézt prenexní formu formule na řádku 1.:

1.	$\forall x\,[p(x) \wedge \forall y \exists x\,(\neg q(x,y) \supset \forall z\, r(a,x,y))]$	výchozí formule
2.	$\forall x\,[p(x) \wedge \forall y \exists x\,(q(x,y) \vee \forall z\, r(a,x,y))]$	eliminace $\supset$
3.	$\forall x\,[p(x) \wedge \forall y \exists t\,(q(t,y) \vee \forall z\, r(a,t,y))]$	přejmenování proměnné
4.	$\forall x\,[p(x) \wedge \forall y \exists t\,(q(t,y) \vee r(a,t,y))]$	vypuštění nadbytečného kvantifikátoru
5.	$\forall x \forall y\,[p(x) \wedge \exists t\,(q(t,y) \vee r(a,t,y))]$	přesun kvantifikátoru doleva
6.	$\forall x \forall y \exists t\,[p(x) \wedge (q(t,y) \vee r(a,t,y))]$	přesun kvantifikátoru doleva

Poznámka 3.2.1:

Prenexní tvar formule není určen jednoznačně. Konečná podoba prenexní formule závisí na pořadí provádění úprav a na způsobu přejmenování vázaných proměnných. Všechny prenexní tvary jsou však ekvivalentní.

Definice 3.2.2:

Skolemova forma uzavřené formule je prenexní tvar této formule, která neobsahuje žádné existenční kvantifikátory. Skolemova forma vznikne z prenexní formy opakovaným použitím následujících dvou operací (***skolemizací***):

$\forall x_1\ \forall x_2 ... \forall x_n\ \exists y\ A(x_1, x_2, ..., x_n, y) \rightarrow$

$\rightarrow \forall x_1\ \forall x_2 ... \forall x_n\ A(x_1, x_2, ..., x_n, f(x_1, x_2, ..., x_n))$,

kde f je nový (v jazyce dosud nepoužitý) n-ární funkční symbol, tzv. ***Skolemova funkce***,

$\exists x\ \forall y_1\ \forall y_2 ... \forall y_n\ A(x, y_1, y_2, ..., y_n) \rightarrow \forall y_1\ \forall y_2 ... \forall y_n\ A(c, y_1, y_2, ..., y_n)$,

kde c je nová (v jazyce dosud nepoužitá) individuová konstanta, tzv. ***Skolemova konstanta***;

Každému eliminovanému existenčnímu kvantifikátoru odpovídá jiná Skolemova funkce nebo konstanta.

Skolemovu formu formule A označíme zápisem A^S.

Literál je atomická formule nebo negace atomické formule (např. $p(f(x))$, $\neg q(y)$).

Klausule je disjunkce literálů (např. $[p(f(x)) \vee \neg q(y)]$).

Konjunktivní normální tvar formule predikátové logiky je prenexní tvar formule, jejíž matice je konjunkce disjunkcí literálů (tj. konjunkce klauzulí).

Disjunktivní normální tvar formule predikátové logiky je prenexní tvar formule, jejíž matice je disjunkce konjunkcí literálů.

Klauzulární forma formule je Skolemova forma, jejíž matice je v klauzulárním tvaru, tj. je konjunkcí klausulí.

Poznámky 3.2.2:

1. Skolemovy konstanty a funkce představují předměty (reprezentanty předmětů), o jejichž existenci vypovídají původní formule. Tak např.
   - $\exists x \forall y\ A(x,y) \rightarrow \forall y\ A(c, y)$
     Je-li univerzem množina všech nezáporných celých čísel a realizací (interpretací) predikátu A je relace < (tedy $A(x,y)$ "chápeme jako" $x < y$), pak c interpretujeme jako 0. V tomto modelu je konstanta c jediná, ale v jiných modelech tomu tak být nemusí.
   - $\forall x \exists y\ A(x,y) \rightarrow \forall x\ A(x, f(x))$
     Je-li univerzem množina reálných čísel a oborem pravdivosti predikátu A je relace <, pak interpretací funkčního symbolu f může být např. funkce f', která je zadaná předpisem: $f'(x) = x + \sqrt{3}$.
2. Po provedené skolemizaci zůstávají v prefixu formule pouze obecné kvantifikátory. Nejdůležitější pro náš další výklad je ***klausulární forma*** formule: $\forall x_1\ \forall x_2 \ldots \forall x_n\ [C_1 \wedge C_2 \wedge \ldots C_k]$, kde C_i jsou klausule (disjunkce literálů). Vzhledem k tomu, že uvažujeme pouze uzavřené formule, není nutné tyto kvantifikátory explicitně uvádět.
3. Skolemova forma A^S uzavřené formule A není ekvivalentní s formulí A, ale platí:

$$\models A^S \supset A, \text{ neboli } A^S \models A.$$

Důkaz:
Nechť má formule $\forall x_1\ \forall x_2 ... \forall x_n\ A(x_1, x_2, ..., x_n, f(x_1, x_2, ..., x_n))$ model I. To znamená, že pro libovolnou *n*-tici $d_1, d_2, \ldots, d_n$ prvků universa platí, že (*n*+1)-tice prvků universa
$<d_1, d_2, \ldots, d_n, f_D(d_1, d_2, \ldots, d_n)> \in A_D$ (leží v oboru pravdivosti A), kde f_D je funkce přiřazená interpretací I symbolu f a A_D je relace – obor pravdivosti A v interpretaci I. Pak je ovšem interpretace I rovněž modelem formule $\forall x_1\ \forall x_2 \ldots \forall x_n\ \exists y\ A(x_1, x_2, \ldots x_n, y)$
Každý model formule A^S je tedy i modelem formule A, ale nikoliv naopak. Je-li tedy formule A nesplnitelná (kontradikce – nemá model), pak je nesplnitelná i formule A^S. Obráceně, je-li formule A splnitelná (má aspoň jeden model) je splnitelná i formule A^S. Obě formule A^S, A jsou současně splnitelné nebo nesplnitelné, nemusí však být ekvivalentní (tj. nemůžeme psát $A^S \Leftrightarrow A$ nebo $\models A^S \equiv A$).

Věta 3.2.2 (Skolem).
Každá formule A může být převedena na formuli A^S v *klauzulární* (Skolemově) *formě* takovou, že A je splnitelná, právě když A^S je splnitelná.

Důkaz: Uvedeme algoritmus převodu $A \rightarrow A^S$.

Krok 1. Utvoření existenčního uzávěru formule A. (Zachovává splnitelnost.)

Krok 2. Eliminace nadbytečných kvantifikátorů. (Ekvivalentní krok.)
Z formule A vypustíme všechny kvantifikátory $\forall x_i$, $\exists x_i$, v jejichž rozsahu se nevyskytuje proměnná x_i.

Krok 3. Přejmenování proměnných. (Ekvivalentní krok.)
Přejmenujeme všechny proměnné, které jsou v A kvantifikovány více než jednou tak, aby všechny kvantifikátory měly navzájem různé proměnné.

Krok 4. Eliminace spojek $\supset$, $\equiv$ podle těchto vztahů (Ekvivalentní krok.):
$(A \supset B) \Leftrightarrow (\neg A \vee B)$, $(A \equiv B) \Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A)$

Krok 5. Přesun spojek $\neg$ *dovnitř.* (Ekvivalentní krok.)

Krok 6. Přesun kvantifikátorů doprava. (Ekvivalentní krok.)
Provádíme náhrady podle těchto ekvivalencí (Q je kvantifikátor $\forall$ nebo $\exists$; © je symbol $\wedge$ nebo $\vee$; A, B neobsahují volnou proměnnou *x*):
$Qx\ (A \copyright B(x)) \Leftrightarrow A \copyright Qx\ B(x)$, $Qx\ (A(x) \copyright B) \Leftrightarrow Qx\ A(x) \copyright B$

Pozn.: Před provedením kroku 7. je vhodné provést ekvivalentní zjednodušující úpravy formule.

Krok 7. Eliminace existenčních kvantifikátorů (Zachovává splnitelnost.)
Provádíme postupně ***Skolemizaci podformulí*** $Qx\ B(x)$, $Qx\ A(x)$, které jsme obdrželi v předchozím kroku 6, tedy náhradu existenčně kvantifikovaných formulí formulemi bez existenčního kvantifikátoru dle Definice 3.2.2.

Krok 8. Přesun všeobecných kvantifikátorů doleva. (Ekvivalentní krok, neboť jsme již provedli krok 3. a platí ekvivalence dle 6.)

Krok 9. Použití distributivních zákonů. (Ekvivalentní krok.)

Provedeme postupné náhrady vlevo formulemi vpravo:

$(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$, $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

Poznámky 3.2.3:

- Z praktických důvodů (aby byl náš důkazový kalkul úplný) se snažíme minimalizovat počet argumentů zaváděných Skolemových funkcí. Krok 6 slouží tomuto účelu.
- Výslednou formuli můžeme ještě zjednodušit použitím úprav, které zachovávají splnitelnost.

Příklad 3.2.2:

6. Uvažujme formuli $A = \forall x\, \exists y\, \forall z\, \exists v\, [p(z,y) \wedge q(x,v)]$.
   Pokud bychom aplikovali Skolemizaci bez kroku 6, dostali bychom formuli:
   $A^{S'} = \forall x\, \forall z\, [p(z, f(x) \wedge q(x, h(x,z)]$, kde f, h jsou zavedené Skolemovy funkce.
   Použijeme-li však nejprve krok 6, dostaneme
   $A' = \exists y\, \forall z\, p(z,y) \wedge \forall x\, \exists v\, q(x,v)$ a z ní eliminací existenčních kvantifikátorů
   $A'' = \forall z\, p(z, a) \wedge \forall x\, q(x, h(x))$. Odtud pak přesunem kvantifikátorů doleva:
   $A^S = \forall z\, \forall x\, [p(z, a) \wedge q(x, h(x))]$, v níž zavedené Skolemovy funkce a, h jsou jednodušší.
7. Uvažme jednoduchou tautologii: $\neg\forall x\, P(x) \vee \forall y\, P(y)$.
   Na tomto místě chceme ještě jednou upozornit na ***důležitost kroku 6*** algoritmu převodu do klauzulární formy. Častým omylem je domněnka, že je možno provést převod tak, že formuli nejprve převedeme do prenexní konjunktivní formy, a pak provedeme Skolemizaci. Na jednoduchém příkladě ukážeme, že takovýto postup by nebyl úplným důkazovým kalkulem (nedokázali bychom všechny tautologie PL^1):
   Negací získáme formuli
   $$\forall x\, P(x) \wedge \exists y\, \neg P(y),$$
   která je nesplnitelná, což snadno dokážeme:
   Skolemizací obdržíme formuli $\forall x\, P(x) \wedge \neg P(a)$, a substitucí $\{x / a\}$ pak kontradikci $P(a) \wedge \neg P(a)$, tedy prázdnou klausuli.
   Provedeme-li (**chybně!**) nejprve převod do prenexní formy a pak Skolemizaci, dostaneme: $[\forall x\, P(x) \wedge \exists y\, \neg P(y)] \vdash \forall x\, [P(x) \wedge \exists y\, \neg P(y)] \vdash \forall x \exists y\, [P(x) \wedge \neg P(y)] \vdash \forall x\, [P(x) \wedge \neg P(f(x))]$. Nesplnitelnost této formule uvedenými důkazovými postupy *nedokážeme,* neboť literály $P(x)$ a $\neg P(f(x))$ nejsou unifikovatelné**.**
8. Nalezneme klausulární (Skolemovu) formu následující uzavřené prenexní formy (formule uvedené na řádku 1.):
   1. $\exists u \forall v \exists w \forall x \forall y \exists z\, A(u, v, w, x, y, z)$ výchozí forma
   2. $\forall v \exists w \forall x \forall y \exists z\, A(a, v, w, x, y, z)$ po eliminaci $\exists u$
   3. $\forall v \forall x \forall y \exists z\, A(a, v, f(v), x, y, z)$ po eliminaci $\exists w$
   4. $\forall v \forall x \forall y\, A(a, v, f(v), x, y, g(v,x,y))$ po eliminaci $\exists z$
   5. $A(a, v, f(v), x, y, g(v,x,y))$ bez explicitní obecné kvantifikace
9. Převedeme formuli A na formuli v klausulární (Skolemově) formě A^S:
   $A = \forall x\{p(x) \supset \exists z\{\neg\forall y[q(x,y) \supset p(f(x_1))] \wedge \forall y[q(x,y) \supset p(x)]\}\}$.

1.,2. Utvoření existenčního uzávěru a eliminace $\exists z$:
$A_2 = \exists x_1 \forall x \{p(x) \supset \{\neg \forall y[q(x,y) \supset p(f(x_1))] \wedge \forall y[q(x,y) \supset p(x)]\}\}$.

3. Přejmenování proměnné y:
$A_3 = \exists x_1 \forall x \{p(x) \supset \{\neg \forall y[q(x,y) \supset p(f(x_1))] \wedge \forall z[q(x,z) \supset p(x)]\}\}$.

4. Eliminace $\supset$:
$A_4 = \exists x_1 \forall x \{\neg p(x) \vee \{\neg \forall y[\neg q(x,y) \vee p(f(x_1))] \wedge \forall z[\neg q(x,z) \vee p(x)]\}\}$.

5. Přesun negace dovnitř:
$A_5 = \exists x_1 \forall x \{\neg p(x) \vee \{\exists y[q(x,y) \wedge \neg p(f(x_1))] \wedge \forall z[\neg q(x,z) \vee p(x)]\}\}$.

6. Přesun kvantifikátorů $\exists y$ a $\forall z$ doprava:
$A_6 = \exists x_1 \forall x \{\neg p(x) \vee \{[\exists y\, q(x,y) \wedge \neg p(f(x_1))] \wedge [\forall z\, \neg q(x,z) \vee p(x)]\}\}$.

7. Eliminace existenčních kvantifikátorů:
$A_7 = \forall x \{\neg p(x) \vee \{[q(x,h(x)) \wedge \neg p(f(a))] \wedge [\forall z\, \neg q(x,z) \vee p(x)]\}\}$.

8. Přesun $\forall z$ doleva:
$A_7 = \forall x \forall z \{\neg p(x) \vee \{[q(x,h(x)) \wedge \neg p(f(a))] \wedge [\neg q(x,z) \vee p(x)]\}\}$.

9. Použití distributivního zákona:
$A_8 = \forall x \forall z \{[\neg p(x) \vee q(x,h(x))] \wedge [\neg p(x) \vee \neg p(f(a))] \wedge [\neg p(x) \vee \neg q(x,z) \vee p(x)]\}$.

10. Provedeme zjednodušení:
   i) Vypustíme třetí klausuli (je to tautologie)
   ii) Odstraníme kvantifikátor $\forall z$ (stal se zbytečným)
   iii) Ve druhé klausuli odstraníme $\neg p(x)$, neovlivníme tím splnitelnost

$A^S = \forall x \{ [\neg p(x) \vee q(x,h(x))] \wedge \neg p(f(a)) \}$.

Herbrandova procedura.

Chceme-li dokázat logickou pravdivost formule A v PL^1, pak budeme postupovat obdobně jako ve VL:

a. Formuli A znegujeme
b. Formuli $\neg A$ převedeme do klausulární formy $(\neg A)^S$
c. Na formuli $(\neg A)^S$ budeme postupně uplatňovat resoluční pravidlo. Pokud získáme prázdnou klausuli $\square$, je důkaz úspěšně ukončen.

Tento třetí bod však v PL^1 nelze provést tak jednoduše jako ve výrokové logice. Problémem je to, že literály s opačným znaménkem, které bychom mohli při uplatňování rezoluce "vyškrtávat", mohou obsahovat různé termy.

Příklad 3.2.3:

Uvažujme formuli A v klausulární formě:

$\forall x\ \forall y\ \forall z\ \forall v\ [p(x, f(x)) \wedge q(y, h(y)) \wedge (\neg p(a, z) \vee \neg q(z, v))]$.

Dokážeme, že tato formule je nesplnitelná. Vypišme jednotlivé klausule pod sebe a pokusme se uplatňovat pravidlo rezoluce:

1. $p(x, f(x))$
2. $q(y, h(y))$
3. $\neg p(a, z) \vee \neg q(z, v)$

Klausule 1. a 3. obsahují literály s opačným znaménkem, avšak uplatnění rezoluce brání to, že p(x, f(x)) ≠ p(a, z). Uvědomíme-li si však, že všechny proměnné jsou univerzálně kvantifikovány a že platí zákon konkretizace (viz Příklad 3.1.4, tautologie 22: Je-li term t substituovatelný za x ve formuli A(x), pak $\forall x$ A(x) |= A(x/t), "co platí pro všechny, platí i pro t"), můžeme se pokusit najít vhodnou substituci termů za proměnné tak, abychom dostali shodné "*unifikované*" literály. V našem příkladě taková substituce existuje:

x / a, z / f(a).

Po provedení této substituce dostaneme klausule:

1'. p(a, f(a))
2. q(y, h(y))
3'. ¬p(a, f(a)) ∨ ¬q(f(a), v)

kde na 1' a 3' již lze uplatnit pravidlo rezoluce:

4. ¬q(f(a), v)

Abychom nyní mohli rezolvovat klausule 2. a 4., zvolíme opět substituci:

y / f(a), v / h(f(a)).

Dostaneme

2'. q(f(a), h(f(a)))
4'. ¬ q(f(a), h(f(a)))

a jejich rezolucí již obdržíme prázdnou klausuli. Tedy formule A je nesplnitelná.

V našem příkladu jsme se opřeli o zákon konkretizace, tedy postup byl korektní. Problémem ovšem je to, že příslušné substituce jsme hledali "zkusmo", intuitivně. Aby mohl být celý proces automatizován (a mohl tak sloužit jako základ pro logické programování), musíme najít nějaký *algoritmus,* jak provádět příslušné *unifikace.* Takové algoritmy existují. Uvedeme zde dva:

4. ***Herbrandova procedura***
5. ***Robinsonův unifikační algoritmus***

Podle definice je daná formule A nesplnitelná, právě když nabývá hodnoty *nepravda* ve *všech* interpretacích nad *všemi* možnými obory interpretace. Důkaz toho, že A je nesplnitelná, by samozřejmě usnadnilo, kdybychom našli jistý pevný obor interpretace D takový, že A je nesplnitelná, právě když nabývá hodnoty nepravda ve všech interpretacích nad tímto pevným oborem D. Takový obor ke každé formuli A existuje a nazývá se ***Herbrandovo universum H_A.*** Je tvořeno množinou všech termů, které mohou být sestrojeny z individuových konstant a_i a funkčních konstant f_i, které se vyskytují v A. (Pokud v A není žádná individuová konstanta, použijeme libovolnou, např. a.) V dalším výkladu budeme vyznačovat prvky Herbrandova universa kursivou, abychom je odlišili od funkčních symbolů formule.

Příklad 3.2.4:

6. Pro formuli A = $\forall x$ [p(a) ∨ q(b) ⊃ p(f(x))]
   je H_A = {*a, b, f(a), f(b), f(f(a)), f(f(b)), ...*}
7. Pro formuli B = $\forall x$ $\forall y$ p((f(x), y, g(x,y))
   je H_A = {*a, f(a), g(a,a), f(f(a)), g(a,f(a)), g(f(a),a), ...*}

Definice 3.2.3.

Buď A formule v klausulární formě: $\forall x_1\ \forall x_2\ \ldots\ \forall_{xn}\ [C_1 \wedge \ldots \wedge C_k]$. ***Základní instancí*** klausule C_i $(1 \le i \le k)$ rozumíme klausuli, která vznikne z C_i tím, že *všechny* individuové proměnné v C_i nahradíme nějakými prvky z H_A.

Věta 3.2.2 (Herbrand)

Formule A v klausulární formě je nesplnitelná, právě když existuje konečná konjunkce základních instancí jejích klausulí, která je nesplnitelná.

Příklad 3.2.4:

Uvažujme opět formuli A z příkladu 3.2.3:

$\forall x\ \forall y\ \forall z\ \forall v\ [p(x, f(x)) \wedge q(y, h(y)) \wedge (\neg p(a, z) \vee \neg q(z, v))]$.

Dokážeme pomocí Herbrandovy věty, že tato formule je nesplnitelná. Vypíšeme jednotlivé klausule pod sebe a budeme postupně generovat jejich základní instance:

1. $p(x, f(x))$
2. $q(y, h(y))$
3. $\neg p(a, z) \vee \neg q(z, v)$

V našem případě je $H_A = \{a, f(a), h(a), f(f(a)), f(h(a)), h(f(a)), h(h(a)), \ldots\}$.

Substituce 1: $\{x/a, y/a, z/a, v/a\}$
$p(a, f(a)) \wedge q(a, h(a)) \wedge [\neg p(a, a) \vee \neg q(a, a)]$

Substituce 2: $\{x/a, y/a, z/a, v/f(a)\}$
$p(a, f(a)) \wedge q(a, h(a)) \wedge [\neg p(a, a) \vee \neg q(a, f(a))]$

atd., až

Substituce *n*: $\{x/a, y/f(a), z/f(a), v/h(f(a))\}$
$p(a, f(a)) \wedge q(f(a), h(f(a))) \wedge [\neg p(a, f(a)) \vee \neg q(f(a), h(f(a)))]$

Rezoluční metodou výrokové logiky nyní snadno ověříme, že tato konjunkce je nesplnitelná. Tedy jsme nalezli protipříklad splnitelnosti formule A (matice formule nemůže "platit pro všechna *x, y, z, v*" – neboť neplatí pro valuaci, která těmto proměnným přiřadí individua z H_A dle substituce *n*), a proto je tato formule nesplnitelná.

Herbrandova procedura parciálně rozhoduje, zda je daná formule A nesplnitelná. K dané formuli postupně generujeme základní instance jejích klausulí a resoluční metodou vždy testujeme, zda je jejich konjunkce nesplnitelná. Jestliže tomu tak je, pak A je nesplnitelná a tato procedura to po konečném počtu kroků zjistí. V případě splnitelnosti A může procedura generovat donekonečna nové a nové základní instance a testovat jejich konjunkce.

Podstatným problémem této metody je skutečnost, že generování základních klausulí je neefektivní. Počet základních instancí, které musí být generovány, dokud nenarazíme na "protipříklad" – nesplnitelnou konjunkci, může být často tak velký, že nám přeplní paměť počítače, nehledě na časovou složitost takového algoritmu. **J.A. Robinson** navrhl v r. 1965 metodu, která na rozdíl od Herbrandovy procedury nevyžaduje generování základních instancí, ale rozhodne přímo, zda k *libovolné* konjunkci klausulí existuje

substituce taková, která unifikuje některé literály a umožní dokázat nesplnitelnost (pokud tato konjunkce nesplnitelná je).

Definice 3.2.4:

Nechť A je formule obsahující individuové proměnné x_i, i=1,2,...,n, a to buď přímo (jako bezprostřední argumenty) nebo zprostředkovaně (jako argumenty funkcí). Označme

$$\sigma = \{x_1/t_1, x_2/t_2, ..., x_n/t_n\}$$

simultánní substituci termů t_i za *(všechny výskyty)* předmětové proměnné x_i pro i=1,2,...,n. Potom zápisem

$$\mathbf{A\sigma}$$

označíme formuli, která vznikne z formule A *provedením substituce* σ. Poznamenejme, že substituce se může týkat všech, nebo jen některých, nebo dokonce žádné individuové proměnné obsažené v A (v tomto případě pro některá nebo všechna i substituujeme x_i/x_i).

Formule B je ***instancí*** formule A, jestliže existuje substituce σ taková, že $B = A\sigma$.

Poznámka 3.2.4:

Substituce lze skládat. Pro skládání (superpozici) substitucí platí:

- $(\sigma\rho)\tau = \sigma(\rho\tau) = \sigma\rho\tau$, tj. skládání substitucí je asociativní.
- Pro identickou substituci (tj. x_i/x_i pro všechna i) ε platí $\varepsilon\sigma = \sigma\varepsilon = \sigma$, tj. identická substituce hraje v algebře substitucí úlohu jednotkového prvku.
- $\sigma\rho \neq \rho\sigma$, tj. skládání substitucí není obecně komutativní.

Definice 3.2.5:

Unifikace (unifikační substituce, unifikátor) formulí A, B je substituce σ taková, že

$$A\sigma = B\sigma.$$

Nejobecnější unifikace formulí A, B je unifikace σ taková, že pro každou jinou unifikaci ρ formulí A, B platí $\rho = \sigma\tau$, kde $\tau \neq \varepsilon$, tj. každá unifikace vznikne z nejobecnější unifikace provedením další dodatečné substituce.

Poznámky 3.2.5:

1. Unifikace atomických formulí (literálů) A, B nemusí existovat, např.:
   - literály p(*x,y*), q(*z*,a) nelze unifikovat, protože se jedná o dva různé predikáty (byť se stejnou aritou),
   - literály p(*x*), p(f(*x*)) nelze unifikovat, přestože se jedná o stejné predikáty (neexistuje žádná unifikující substituce).
2. K daným dvěma formulím může existovat mnoho různých unifikací. Nechť např.

   $$A = p(x, y), B = p(u, 2).$$

   Potom:
   - $\sigma = \{x/u, y/2\}$ je unifikační substituce, neboť $A\sigma = B\sigma = p(u,2)$,
   - $\rho = \{x/3, y/2, u/3\}$ je unifikační substituce, neboť $A\rho = B\rho = p(3,2)$,
   - $\tau = \{x/f(y), y/2, u/f(y)\}$ je unifikační substituce, neboť $A\tau = B\tau = p(f(y), 2)$.

   $A\sigma$, $A\rho$, $A\tau$ jsou různými instancemi formule A, přitom formule $A\rho$ je základní instancí (podobně $B\tau$, $B\rho$, $B\sigma$ jsou různými instancemi formule B a $B\rho$ je základní instancí).

   σ, ρ, τ jsou různými unifikacemi formulí A, B. Unifikace σ je nejobecnější unifikace těchto formulí. Každou jinou unifikaci získáme z této dodatečnou substitucí, např.:

- $\rho = \sigma.\{u/3\}$,
- $\tau = \sigma.\{u/f(y)\}$.

(Tedy nejobecnější unifikace je ta "nejjednodušší", která ponechává co nejvíce proměnných volných.)

Algoritmus /*nalezení nejobecnější unifikace*/ - Robinson:

Formulace zcela obecného algoritmu je poměrně složitá (patří do výpočetních metod umělé inteligence) a jeho „ruční" simulace značně nepřehledná. Omezíme se proto pouze na případ, kdy unifikované elementární formule nemají na obou místech stejnolehlých argumentů současně nějaké funkční struktury (v tomto případě by bylo třeba rekurzivním algoritmem postupně tyto struktury rozkrývat).

Předpokládejme tedy

$$A = p(t_1, t_2,...,t_n),\ B = p(s_1,s_2,...,s_n),$$

kde $t_1, t_2,...,t_n, s_1, s_2,...,s_n$ jsou termy takové, že t_i, s_i nejsou současně funkční struktury dle Def. 3.1.1, bod II)a.ii (tedy alespoň jeden z nich je proměnná). Potom nejobecnější unifikaci získáme takto:

1. Pro i = 1,2,...,*n* prováděj:
   - Je-li $t_i = s_i$, pak polož $\sigma_i = \varepsilon$.
   - Není-li $t_i = s_i$, pak zjisti, zda jeden z termů t_i, s_i představuje nějakou individuovou proměnnou *x* a druhý nějaký term r, který proměnnou *x* *neobsahuje.*
     - Jestliže ano, pak polož $\sigma_i = \{x/r\}$.
     - Jestliže ne, pak ukonči práci s tím, že formule A, B nejsou unifikovatelné.
2. Po řádném dokončení cyklu urči $\sigma = \sigma_1\sigma_2...\sigma_n$. Substituce σ je nejobecnější unifikací formulí A, B.

Příklady 3.2.5:

1. Nechť $A = p(x, f(x), u)$, $B = p(y, z, g(x,y))$
   - $\sigma_1 = \{x/y\}$, $A\sigma_1 = p(y, f(y), u)$, $B\sigma_1 = p(y, z, g(y,y))$
   - $\sigma_2 = \{z/f(y)\}$, $A\sigma_1\sigma_2 = p(y, f(y), u)$, $B\sigma_1\sigma_2 = p(y, f(y), g(y,y))$
   - $\sigma_3 = \{u/g(y,y)\}$, $A\sigma_1\sigma_2\sigma_3 = p(y, f(y), g(y,y))$, $B\sigma_1\sigma_2\sigma_3 = p(y, f(y), g(y,y))$.

   Složená substituce $\sigma=\sigma_1\sigma_2\sigma_3$ je unifikací formulí A, B ($A\sigma = p(y, f(y), g(y,y)) = B\sigma$), a to nejobecnější unifikací.
2. Nechť $A = p(x, f(x), z)$, $B = p(y, z, g(x,y))$
   - $\sigma_1 = \{x/y\}$, $A\sigma_1 = p(y, f(y), z)$, $B\sigma_1 = p(y, z, g(y,y))$
   - $\sigma_2=\{z/f(y)\}$, $A\sigma_1\sigma_2 = p(y, f(y), f(y))$, $B\sigma_1\sigma_2 = p(y, f(y), g(y,y))$

   Termy $f(y)$ a $g(y,y)$ unifikovat nelze, neboť se jedná o dva různé funkční symboly. Formule A, B nelze tedy unifikovat.

Věta 3.2.3 (Robinson: *zobecněné rezoluční odvozovací pravidlo*):

Nechť A_i, B_i, L_i jsou atomické formule predikátové logiky. Potom platí následující odvozovací pravidlo:

$$A_1 \vee ... \vee A_m \vee L_1, B_1 \vee ... \vee B_n \vee \neg L_2 \ \vdash \ A_1\sigma \vee ... \vee A_m\sigma \vee B_1\sigma \vee ... \vee B_n\sigma ,$$

kde σ je unifikace formulí L_1, L_2, tj. $L_1\sigma = L_2\sigma$.

Klauzule na levé straně odvozovacího pravidla nazýváme ***rodičovskými klauzulemi*** a klauzuli na pravé straně ***rezolventou***.

Formule A^S v klausulární formě je nesplnitelná, právě když z ní lze opakovaným použitím obecného pravidla rezoluce odvodit prázdnou klausuli $\square$.

Poznámky 3.2.6:

1. Speciální případy rezolučního odvozovacího pravidla (předpokládáme $L_1\sigma = L_2\sigma$):
   - m=0, n=0: $L_1, \neg L_2 \vdash \square$ odvození sporu
   - m=0, n=1: $L_1, \neg L_2 \vee B \vdash B\sigma$ pravidlo MP
   - m=1, n=1: $L_1 \vee A, \neg L_2 \vee B \vdash A\sigma \vee B\sigma$ základní tvar rez. pravidla
2. Unifikace σ formulí L_1, L_2 může být jakákoliv; chceme-li však vyvodit z předpokladů (rodičovských klauzulí) nejobecnější závěr (rezolventu) je třeba použít nejobecnější unifikaci.

Důkaz (základního tvaru)**:**

Předpoklady $L_1 \vee A$, $\neg L_2 \vee B$ se transformují na tvar $L_1\sigma \vee A\sigma$, $\neg L_2\sigma \vee B\sigma$, kde σ je unifikací formulí L_1, $\neg L_2$. S těmito předpoklady se dále pracuje stejným způsobem jako s původními předpoklady $L_1 \vee A$, $\neg L_1 \vee B$ v důkazu vět 2.2.2 a 2.2.3.

Příklady 3.2.6 /*rezoluční metoda v predikátové logice*/:
Porovnejte tato řešení se sémantickým ověřováním správnosti úsudku, viz Příklad 3.1.5.

I. **Dokážeme správnost úsudku** (analytickou pravdivost věty):
Jistý filosof odporuje všem filosofům, tedy odporuje sám sobě.
Větu analyzujeme jako
(”zamýšlená” interpretace je nad množinou individuí, p $\rightarrow$ podmnožina filosofů, q $\rightarrow$ relace, ve které budou ty dvojice, kde první odporuje druhému)
$\exists x \ \{[p(x) \wedge \forall y \ (p(y) \supset q(x,y))] \supset q(x,x)\}$
Formuli znegujeme a převedeme na klausulární tvar:
$\forall x \ \forall y \ \{p(x) \wedge [\neg p(y) \vee q(x,y)] \wedge \neg q(x,x)\}$. K jednotlivým klausulím
1. $p(x)$
2. $\neg p(y) \vee q(x,y)$
3. $\neg q(x,x)$

je nejobecnějším unifikátorem substituce $\{y/x\}$:
4. $q(x,x)$ z 1. a 2.
5. $\square$ z 3. a 4.

Negovaná formule je nesplnitelná (kontradikce), proto je původní formule logicky pravdivá.

II. **Dokažme správnost úsudku:**

Kdo zná Pavla a Marii, ten Marii lituje.	$\forall x\ (\ [Z(x, P) \wedge Z(x, M)] \supset L(x, M)\ )$
Někteří nelitují Marii, ačkoli ji znají.	$\exists x\ [\neg L(x, M) \wedge Z(x, M)]$
Někdo zná Marii, ale ne Pavla.	$\exists x\ [Z(x, M) \wedge \neg Z(x, P)]$

$\forall x\ [\neg Z(x, P) \vee \neg Z(x, M) \vee L(x, M)]$	odstranění implikace (1. předpoklad)
$\neg L(a, M) \wedge Z(a, M)$	Skolemizace (2. předpoklad)
$\forall y\ [\neg Z(y, M) \vee Z(y, P)]$	negovaný závěr (přejmenování x)

Klausule:

1.	$\neg Z(x, P) \vee \neg Z(x, M) \vee L(x, M)$	
2.	$\neg L(a, M)$	
3.	$Z(a, M)$	
4.	$\neg Z(y, M) \vee Z(y, P)$	
5.	$\neg Z(a, P) \vee \neg Z(a, M)$	rezoluce 1., 2., substituce x/a
6.	$\neg Z(a, P)$	rezoluce 3., 5.
7.	$\neg Z(a, M)$	rezoluce 4., 6., substituce y/a
8.	$\square$	rezoluce 3., 7.

Negovaný závěr je ve sporu s předpoklady, tedy původní závěr z předpokladů vyplývá.

III. **Dokažme správnost úsudku:**

Všichni členové vedení jsou majiteli obligací nebo akcionáři.
Žádný člen vedení není zároveň majitel obligací i akcionář.
Všichni majitelé obligací jsou členy vedení.

Žádný majitel obligací není akcionář.

$\forall x\ [v(x) \supset (o(x) \vee a(x))]$
$\forall x\ [v(x) \supset \neg(o(x) \wedge a(x))]$
$\forall x\ [o(x) \supset v(x)]$

$\forall x\ [o(x) \supset \neg a(x)]$

Klausule:

1.	$\neg v(x) \vee o(x) \vee a(x)$	1. předpoklad
2.	$\neg v(x) \vee \neg o(x) \vee \neg a(x)$	2. předpoklad
3.	$\neg o(x) \vee v(x)$	3. předpoklad
4.	$o(k)$	negovaný závěr
5.	$a(k)$	(po Skolemizaci)
6.	$\neg o(x) \vee \neg a(x)$	rezoluce 2., 3.
7.	$\neg a(k)$	rezoluce 4., 6., substituce x/k
8.	$\square$	rezoluce 5., 7.

Pozn.: Všimněme si, že jsme první klausuli při důkazu nepoužili. Tedy závěr vyplývá již z druhého a třetího předpokladu (první je pro odvození důsledku nadbytečný).

IV. **Dokažme správnost úsudku:**

Každý, kdo má rád Jiřího, bude spolupracovat s Milanem.
Milan nekamarádí s nikým, kdo kamarádí s Láďou.
Petr bude spolupracovat pouze s kamarády Karla.

Jestliže Karel kamarádí s Láďou, pak Petr nemá rád Jiřího.

$\forall x\ [R(x, J) \supset S(x, M)]$
$\forall x\ [K(x, L) \supset \neg K(M, x)]$
$\forall x\ [S(P, x) \supset K(x, Kr)$

$K(Kr, L) \supset \neg R(P, J)$

Klausule:

1. $\neg R(x, J) \vee S(x, M)$	1. předpoklad
2. $\neg K(y, L) \vee \neg K(M, y)$	2. předpoklad
3. $\neg S(P, z) \vee K(z, Kr)$	3. předpoklad
4. $K(Kr, L)$	negovaný
5. $R(P, J)$	závěr
6. $\neg K(M, Kr)$	rezoluce 4., 2., substituce y/Kr
7. $\neg S(P, M)$	rezoluce 3., 6., substituce z/M
8. $\neg R(P, J)$	rezoluce 1., 7., substituce x/P
9. □	rezoluce 5., 8.

V. **Dokažme správnost úsudku:**

Každý muž má rád fotbal a pivo.
Xaver má rád pouze milovníky fotbalu a piva.
Někteří milovníci fotbalu nemají rádi pivo.
Kdo není muž, je žena. (musíme explicitně stanovit všechny předpoklady)

Některé ženy nemá Xaver rád.

$\forall x\ [M(x) \supset (R(x,f) \wedge R(x,p))]$	1. předpoklad
$\forall x\ [R(Xa,x) \supset (R(x,f) \wedge R(x,p))]$	2. předpoklad
$\exists x\ [R(x,f) \wedge \neg R(x,p)]$	3. předpoklad
$\forall x\ [\neg M(x) \supset Z(x)]$	4. předpoklad
$\forall x\ [\neg Z(x) \vee R(Xa,x)]$	negovaný závěr: $\neg\exists x\ [Z(x) \wedge \neg R(Xa,x)]$,

Klausule:

1. $\neg M(x) \vee (R(x,f)$
2. $\neg M(x) \vee (R(x,p)$
3. $\neg R(Xa,y) \vee (R(y,f)$
4. $\neg R(Xa,y) \vee (R(y,p)$
5. R(k,f)
6. $\neg$R(k,p)
7. $M(z) \vee Z(z)$

8. $\neg Z(u) \vee R(Xa,u)$

9.	$\neg R(Xa,k)$	rezoluce 4., 6. (y/k)
10.	$\neg Z(k)$	rezoluce 8., 9. (u/k)
11.	M(k)	rezoluce 7., 10. (z/k)
12.	R(k,p)	rezoluce 2., 11. (x/k)
13.	□	rezoluce 6., 12.

VI. **Dokažme**: $d(x,y) \supset p(x,y)$, $d(x,y) \wedge p(y,z) \supset p(x,z)$, d(a,b), d(b,c) |= p(a,c)

Jedna z možných interpretací použitého jazyka predikátové logiky je tato:
- a, b, c jsou individuové konstanty označující konkrétní lidi
- $d(x,y)$ je binární predikát s významem "x je dítětem y",
  $p(x,y)$ je binární predikát s významem "x je potomkem y"

Důkaz:
Užitím principu vyvrácení a převodem na klauzulární tvar získáme následující množinu klauzulí:

1. $\neg d(x,y) \vee p(x,y)$	předpoklad /pravidlo/
2. $\neg d(x,y) \vee \neg p(y,z) \vee p(x,z)$	předpoklad /pravidlo/
3. d(a,b)	předpoklad /fakt/
4. d(b,c)	předpoklad /fakt/
5. $\neg p(a,c)$	negace závěru /cíl/

Užitím rezolučního pravidla získáme po provedení potřebných unifikací následující rezolventy:

6. $\neg d(a,c)$	rezoluce: 5,1	{x/a,y/c}
7. $\neg d(a,y) \vee \neg p(y,c)$	rezoluce: 5,2	{x/a,z/c}
8. $\neg p(b,c)$	rezoluce: 7,3	{y/b}
9. $\neg d(b,c)$	rezoluce: 8,1	{x/b,y/c}
10. □	rezoluce: 9,4	

Odvodili jsme spor - tvrzení je dokázáno.

VII. **Dokažme**: p(a), $\forall y[p(y) \supset p(f(y))]$ |= p(f(f(a)))

Jedna z možných interpretací použitého jazyka predikátové logiky je tato:
- proměnná y probíhá množinu všech celých čísel,
- a je konstanta označující konkrétní celé číslo (např. 4),
- $p(y)$ je unární predikát s významem "y je sudé číslo",
- $f(y)$ je unární funkce s významem "druhá mocnina čísla y".

Důkaz:
Užitím principu vyvrácení a převodem na klauzulární tvar získáme následující množinu klauzulí:

1. p(a)	předpoklad /fakt/
2. $\neg p(y) \vee p(f(y))$	předpoklad /pravidlo/
3. $\neg p(f(f(a))$	negace závěru /cíl/

Užitím rezolučního pravidla získáme po provedení potřebných unifikací následující rezolventy:

4. $\neg p(f(a))$	rezoluce: 3, 2	{y/f(a)}

5. $\neg p(a)$ rezoluce: 4, 2 $\{y/a\}$
6. $\square$ rezoluce: 5, 1

Spor byl odvozen, tj. důkaz byl proveden.

Definice 3.2.6:

Metoda (čistého) ***logického programování*** je speciálním případem obecné rezoluční metody. Oproti obecné rezoluční metodě splňuje následující omezení:

- pracuje pouze s Hornovými klauzulemi (které mají nanejvýš jeden pozitivní literál),
- používá ***lineární strategii generování rezolvent*** (viz kapitola 2.2) spolu s tzv. ***navracením (backtrackingem)***.

Poznámky 3.2.7:

1. Logické programy používají následující notaci pro zápis klauzulí:

Hornovy klauzule	Ekvivalentní logický tvar	Zápis v logickém programu (Prolog)	
$\neg Q_1 \vee \neg Q_2 \vee ... \vee \neg Q_n \vee P$	$Q_1 \wedge Q_2 \wedge ... \wedge Q_n \supset P$	$P :- Q_1, Q_2, .., Q_n.$	1.
$\neg Q_1 \vee \neg Q_2 \vee P$	$Q_1 \wedge Q_2 \supset P$	$P:- Q_1, Q_2.$	2.
$\neg Q_1 \vee P$	$Q_1 \supset P$	$P:- Q_1.$	3.
P	P	$P.$	4.
$\neg Q_1 \vee \neg Q_2 \vee ... \vee \neg Q_n$	$\neg(Q_1 \wedge Q_2 \wedge ... \wedge Q_n)$	$?- Q_1, Q_2, .., Q_n.$	5.
$\neg Q_1 \vee \neg Q_2$	$\neg(Q_1 \wedge Q_2)$	$?- Q_1, Q_2.$	6.
$\neg Q_1$	$\neg Q_1$	$?- Q_1.$	7.
$\square$	$\square$	$\square$	8.

2. V logickém programování používáme následující terminologii:

Zápisy 1.,2.,3.: podmíněné příkazy (**pravidla**)
Zápis 4.: nepodmíněný příkaz (**fakt**)
Zápisy 5.,6.,7.: **cíle** /cílové klauzule/
Zápis 8.: $\square$ **spor** /prázdná klauzule/

- $P:- Q_1, Q_2, ..., Q_n$ ... podmíněný příkaz (deklarace procedury)
  $P = p(t_1, t_2, ..., t_r)$ ... hlava procedury
  p ..... jméno procedury
  t_i ..... formální parametr procedury
  $Q_1, Q_2, .., Q_n$ ..... tělo (příkazy) procedury
- $?- Q_1, Q_2, ..., Q_n$ .... množina cílů /množina volání procedur/
  $Q = q(s_1, s_2, ..., s_r)$ ... hlava cíle
  q ..... jméno volané procedury
  s_i ..... skutečný parametr volání

Definice 3.2.7:

Logický program je posloupnost příkazů (procedur) podmíněných (tj. pravidel) i nepodmíněných (tj. faktů). Cílová klauzule zadává ***otázky***, na které má program nalézt odpovědi.

Pozn.: Pojem příkazu chápeme ve smyslu předchozí poznámky. Logický program je tedy ***deklarativní*** *(ne imperativní)*. Specifikujeme, "**co** se má provést" a **ne**určujeme, "**jak** se to má provést".

Algoritmus (*interpretace logického programu*):

(1) Za aktuální cílovou klauzuli vezmi výchozí cílovou klauzuli.

(2) Je-li aktuální cílová klauzule prázdná, ukonči výpočet s odpovědí "ano" na otázky položenou výchozí cílovou klauzulí. (Byly-li ve výchozí cílové klausuli volné proměnné, pak poslední substituce termů za tyto proměnné je řešením – součást odpovědi.) Není-li aktuální cílová klauzule prázdná, přejdi k bodu (3).

(3) Vezmi nejlevější cíl v aktuální cílové klauzuli a hledej v programu příkaz se stejným jménem, který dosud nebyl s tímto cílem konfrontován (neúspěšně). Při hledání tohoto cíle postupuj v programu shora dolů (podle pořadí příkazů). Nenalezneš-li takový příkaz, ukonči výpočet s odpovědí "ne" na otázku položenou aktuální cílovou klauzulí. Nalezneš-li, přejdi k bodu (4).

(4) Pokus se unifikovat hlavu vybraného cíle s hlavou nalezeného stejnojmenného příkazu. Jestliže unifikace neexistuje, vrať se k bodu (3). Jestliže existuje, vezmi za novou aktuální cílovou klauzuli rezolventu dosavadní cílové klauzule s tělem nalezeného příkazu (při užití nejobecnější unifikace hlavy cíle a hlavy příkazu). Přejdi k bodu (2).

Příklad 3.2.7:

Program 1.:

1. p(x,y):-d(x,y)
2. p(x,y):-d(x,z), p(z,y)
3. d(a,b)
4. d(b,c)
5. d(f,c)

Poznámka:

Porovnej s předchozím příkladem 3.2.6, VI k rezoluční metodě. Oba příklady řeší shodnou úlohu.

Úloha 1.:

6. ?-p(a,c) zadání / dotaz

Výpočet 1. úlohy 1.programem:

7. ?-d(a,c) rezoluce: 6.,1.
6. ?-p(a,c) backtracking – navracení, neboť cíl 7. nelze splnit
7. ?-d(a,z), p(z,c) rezoluce: 6.,2. (*x*/a, *y*/c)
8. ?-p(b,c) rezoluce: 7.,3. (*z*/b)
9. ?-d(b,c) rezoluce: 8.,1. (*x*/b, *y*/c)
10. ano rezoluce: 9.,4.

Úloha 2.:

6. ?-p(f,a) zadání

Výpočet 2. úlohy 1.programem:

7. ?-d(f,a) rezoluce: 6.,1.
6. ?-p(f,a) backtracking
7. ?-d(f,z), p(z,a) rezoluce: 6.,2.
8. ?-p(c,a) rezoluce: 7.,5.
9. ?-d(c,a) rezoluce: 8.,1.
8. ?-p(c,a) backtracking
9. ?-d(c,z), p(z,a) rezoluce: 8.,2.
10. ne d(c,z) nelze rezolvovat s žádným příkazem, pro splnění cíle p(c,a) byly vyzkoušeny všechny /obě/ možnosti programu

Program 2.:

1. p(x,y):-d(x,y)
2. p(x,y):-p(x,z), d(z,y)
3. d(a,b)
4. d(b,c)
5. d(f,c)

Poznámka:

Program 2. řeší tutéž úlohu jako program 1., programy se liší pouze formálně pořadím příkazů v těle druhé procedury.

Výpočet 1. úlohy 2. programem:

7. ?-d(a,c) rezoluce: 6.,1.
6. ?-p(a,c) backtracking
7. ?-p(a,z), d(z,c) rezoluce: 6.,2.
8. ?-d(a,z), d(z,c) rezoluce: 7.,1.
9. ?-d(b,c) rezoluce: 8.,3.
10. ano rezoluce: 9.,4.

Výpočet 2.úlohy 2.programem:

7. ?-d(f,a) rezoluce: 6.,1.
6. ?-p(f,a) backtracking
7. ?-p(f,z), d(z,a) rezoluce: 6.,2.
8. ?-d(f,z), d(z,a) rezoluce: 7.,1.
9. ?-d(c,a) rezoluce: 8.,5.
7. ?-p(f,z), d(z,a) backtracking,
10. ?-p(f,u), d(u,z), d(z,a) rezoluce: 7.,2., nekonečný výpočet

Poznámky k výpočtu 2. úlohy 2. programem:

- Kdybychom generovali rezolventy do šířky místo do hloubky, skončil by výpočet po konečném počtu kroků. Druhý cíl cílové klauzule 8. je zřejmě nesplnitelný a tedy celá klauzule 8. je nesplnitelná a odpověď na otázku 2.úlohy je tedy záporná.
- Potřebná přejmenovávání vázaných proměnných tak, aby nedocházelo ke kolizím (viz např. vznik poslední 10. klauzule rezolucí z klauzulí 7.a 2.) provádí automaticky interpret Prologu.

Další typy možných úloh:

?-p(a,c), p(b,a)	platí současně p(a,c), p(b,a) ?
?-p(x,c)	existuje x takové, že p(x,c) ?
?-p(a,x)	existuje x takové, že p(a,x) ?
?-p(x,y)	existují x,y taková, že p(x,y) ?

Výpočet 2. cíle 2. programem:

6. ?-p(x,c)	
7. ?-d(x,c)	rezoluce 6, 1 (*y*/c)
8. ano *x* = b	rezoluce 7, 4 (*x*/b)

Zadáme-li středník ; pak se ptáme na další možné předky, vyvoláme backtracking:

6. ?-p(x,c)	
9. ?-p(x,z), d(z,c)	rezoluce 6, 2 (*y*/c)
10. ?-p(x,z)	
11. ?-d(x,z)	rezoluce 10, 1
12. ano	rezoluce 11, 3 (*x*/a, *z*/b)
13. ?-d(b,c)	
14. **ano, *x* = a**	

Příklad 3.2.8:

Program:

1. s(f(x,y)):-s(x)
2. s(f(x,y)):-s(y)
3. s(g(x,y)):-s(x),s(y)
4. s(a)
5. s(b)

Poznámka:

Jedna z možných interpretací použitého jazyka predikátové logiky je tato:

- *x*, *y* jsou proměnné probíhající množinu celých čísel,
- a, b jsou konstanty, tj. konkrétní celá čísla,
- funkce f, g mají význam: f(*x*, *y*) = *x*.*y*, g(*x*, *y*) = *x*+*y*,
- predikát s(*x*) má význam: číslo *x* je sudé.

Úloha:

6. ?-s(g(f(a,c),f(d,b)))	zadání (ptáme se, zda číslo a.c + d.b je sudé)

Výpočet:

7. ?-s((f(a,c)),s(f(d,b)))	rezoluce: 6.,3.
8. ?-s(a),s(f(d,b)))	rezoluce: 7.,1.
9. ?-s(f(d,b))	rezoluce: 6.,2.
10.?-s(d)	rezoluce: 9.,1.
9. ?-s(f(d,b))	backtracking
10.?-s(b)	rezoluce: 9.,2.
11. ano	rezoluce: 10.,5.

Příklad 3.2.9 /*Euklidův algoritmus*/:

Program:

1. nsd(x,x,x)
2. nsd(x,y,z):-p(x,y), nsd(f(x,y),y,z)
3. nsd(x,y,z):-p(y,x), nsd(x,f(y,x),z)

Poznámka:

Jedna z možných interpretací použitého jazyka predikátové logiky je tato:

- *x,y,z* jsou proměnné probíhající množinu celých čísel,
- funkce f má význam: f(*x,y*) = x - y,
- binární predikát p(*x,y*) má význam x > y,
- ternární predikát nsd(*x,y,z*) má význam: největším společným dělitelem čísel *x, y* je číslo *z*.

S užitím obvyklého matematického značení můžeme program přepsat v čitelnějším tvaru:

1. nsd(x,x,x)
2. nsd(x,y,z):-x>y, nsd(x-y,y,z)
3. nsd(x,y,z):-y>x, nsd(x,y-x,z)

Pozn.: Předpokládáme, že kromě těchto tří klausulí má náš program k dispozici vestavěné matematické procedury, které počítají běžné matematické fakty, jako 6-4, 4>2, apod.

Úloha:

4. ?-nsd(4,6,z) zadání (hledáme největšího společného dělitele čísel 4 a 6)

Výpočet:

5. ?-4>6, nsd(4-6,6,z)	rezoluce: 4.,2.
4. ?-nsd(4,6,z)	backtracking
5. ?-6>4, nsd(4,6-4,z)	rezoluce: 4,3.
6. ?-nsd(4,2,z)	„Výpočet“ klausule 5., fakt "6>4"
7. ?-4>2, nsd(4-2,2,z)	rezoluce: 6.,2.
8. ?-nsd(2,2,z)	„Výpočet“ klausule 7., fakt "4>2"
9. ano	rezoluce: 8.,1. **výsledek: z = 2**

Příklad 3.2.10 /*generování přirozených čísel*/:

Poznámka:

Interpretujme p(*x*) jako predikát "x je přirozené číslo" a f(*x*) jako funkci "následník čísla *x*".

Program:

1. p(0)	0 je přirozené číslo
2. p(f(*x*)):-p(*x*)	následník přirozeného čísla je přirozené číslo

Zadání:

3. ?-p(f(*x*))	jaká jsou všechna přirozená čísla ?

Výpočet:

4. ?-p(x)	rezoluce: 3.,2.
5. p(f(0))	neboť otázka 3. je splněna pro x=0
3. ?-p(f(x))	backtracking
4. ?-p(x)	rezoluce: 3.,5.
6. p(f(f(0)))	neboť otázka 3. je splněna pro x=f(0)

.....

Příklad 3.2.11 /*symbolické derivování polynomů*/:
Interpretace symbolů /model jazyka/:

x, y	předmětové proměnné, probíhající množinu reálných čísel
u, v, r, s	termy
a, 0, 1	předmětové konstanty /reálná čísla/
f(u, v)	binární funkce představující součet u + v
g(u, v)	binární funkce představující součin u.v
d(u, *x*, r)	ternární predikát s významem "derivace u podle *x* je r"

Program:

1. d(x,x,1)
2. d(a,x,0)
3. d(u+v,x,r+s):-d(u,x,r),d(v,x,s)
4. d(u.v,x,r.v+u.s):-d(u,x,r),d(v,x,s)

Poznámky:

Příkazy programu vyjadřují známá pravidla pro derivovaní nezávisle proměnné, konstanty, součtu a součinu.

Zadání:

5. ?-d(x.x,x,x+x) je derivací výrazu x.x výraz x+x ?

Výpočet:

6. ?-d(x,x,1),d(x,x,1)	rezoluce: 5.,4.	{u/x,v/x,r/1,s/1}
7. ?-d(x,x,1)	rezoluce: 6.,1.	
8. ano	rezoluce: 7.,1.	

Alternativní zadání:

5. ?-d(x.x,x,y)	co je derivací výrazu x.x podle x ?	

Výpočet:

6. ?-d(x,x,r),d(x,x,s)	rezoluce: 5.,4.	{u/x,v/x,r/1,y/r.x+x.s}, tj. y=r.x+x.s
7. ?-d(x,x,s)	rezoluce: 6.,1.	{r/1}, tj. r=1
8. ano	rezoluce: 7.,1.	{s/1}, tj. s=1, tj. y=1.x+x.1

Příklad 3.2.12 */z teorie grup/*:

Dokažte, že grupa, jejíž každý prvek je inverzní sám k sobě, je komutativní.

Předpoklady:

- $\forall x\ \forall y\ \forall z\ [(x.y).z = x.(y.z)]$ asociativita grupové operace
- $\forall x\ [x.\mathrm{e} = \mathrm{e}.x = x]$ existence jednotkového prvku e
- $\forall x\ [x.x = \mathrm{e}]$ autoinverze každého prvku

Závěr:

- $\forall x\ \forall y\ [x.y = y.x]$ komutativita grupové operace

Po převodu do klauzulárního tvaru dostáváme následující *množinu klauzulí* (p(*x,y,z*) je ternární predikát značící *x.y = z*):

1. $\neg p(x,y,u) \vee \neg p(y,z,v) \vee \neg p(u,z,w) \vee p(x,v,w)$
2. $\neg p(x,y,u) \vee \neg p(y,z,v) \vee \neg p(x,v,w) \vee p(u,z,w)$
3. p(*x*,e,*x*)
4. p(e,*x*,*x*)
5. p(*x*,*x*,e)

6. p(a,b,c)
7. ¬p(b,a,c)

Prvé dvě klauzule vyjadřují asociativitu (klauzule 1. říká, že (*x.y*).*z* lze přepsat na *x*.(*y.z*) a klauzule 2. postuluje možnost opačného přepisu), klauzule 3.a 4. vyjadřují vlastnost jednotkového prvku, klauzule 5. stanoví, že každý prvek je inverzní sám k sobě a konečně klauzule 6.a 7. vyjadřují neplatnost komutativního zákona. V souladu s principem vyvrácení chceme z klauzulí 1.-7. vyvodit spor. Uvedenou množinu klauzulí můžeme zapsat jako *logický program:*

1. p(x,v,w):-p(x,y,u),p(y,z,v),p(u,z,w)
2. p(u,z,w):-p(x,y,u),p(y,z,v),p(x,v,w)
3. p(x,e,x)
4. p(e,x,x)
5. p(x,x,e)
6. p(a,b,c)
7. ?-p(b,a,c)

@ doplnit Zlatuska SOFSEM‘99

3.3. Systém přirozené dedukce predikátové logiky

Úvodní poznámky:

Metoda přirozené dedukce predikátové logiky je zobecněním metody přirozené dedukce výrokové logiky. Od této metody se liší pouze tím, že pracuje s obecnějším jazykem predikátové logiky (viz definice 3.1.1) a v souvislosti s tím používá rozšířenou množinu výchozích dedukčních pravidel (viz následující definice 3.3.1).

Pojem důkazu (přímého, nepřímého), pojem teorému a způsoby dokazování, včetně speciálních dokazovacích technik (technika hypotetických předpokladů, technika větveného důkazu) – viz kapitola 2.3 – zůstávají beze změny.

V platnosti zůstávají rovněž věta 2.3.1 o dedukci (každému teorému ve tvaru implikace odpovídá dedukční pravidlo a každému dedukčnímu pravidlu teorém – přesná formulace viz věta 2.3.1) a věta 2.3.3 o korektnosti a úplnosti (každá dokazatelná formule je tautologií a obráceně každá tautologie je v systému přirozené dedukce dokazatelná).

Definice 3.3.1:

Výchozími (nedokazovanými, primárními) dedukčními pravidly jsou všechna dedukční pravidla uvedená v definici 2.3.1 pro práci s výrokovými funktory, tj.:

Zavedení konjunkce: $A, B \vdash A \wedge B$ ZK
Eliminace konjunkce: $A \wedge B \vdash A, B$ EK
Zavedení disjunkce: $A \vdash A \vee B$ nebo $B \vdash A \vee B$ ZD
Eliminace disjunkce: $A \vee B, \neg A \vdash B$ nebo $A \vee B, \neg B \vdash A$ ED
Zavedení implikace: $B \vdash A \supset B$ ZI
Eliminace implikace: $A \supset B, A \vdash B$ EI *modus ponens* **MP**
Zavedení ekvivalence: $A \supset B, B \supset A \vdash A \equiv B$ ZE
Eliminace ekvivalence: $A \equiv B \vdash A \supset B, B \supset A$ EE

a následující čtyři pravidla pro práci s kvantifikátory:

Zavedení obecného kvantifikátoru: $A(x) \vdash \forall x A(x)$ Z∀
Pravidlo lze použít pouze tehdy, jestliže formule $A(x)$ není odvozena z žádného předpokladu, který obsahuje x jako volnou proměnnou.@ rozvest

Eliminace obecného kvantifikátoru: $\forall x A(x) \vdash A(x/t)$ E∀
Formule $A(x/t)$ je výsledkem korektní substituce termu t za proměnnou x ve formuli $A(x)$, tedy term T musí být substituovatelný za x ve formuli A.

Zavedení existenčního kvantifikátoru: $A(x/t) \vdash \exists x A(x)$ Z∃

Eliminace existenčního kvantifikátoru: $\exists x A(x) \vdash A(x/c)$ E∃
Použijeme-li pravidlo E∃ pro různé formule A, musíme za proměnnou x substituovat vždy jinou konstantu c.
Obsahuje-li formule A, kromě kvantifikované proměnné x, ještě další volné proměnné, lze pravidlo eliminace existenčního kvantifikátoru formulovat obecněji takto:

$$\exists x\, A(x, y_1,...,y_n) \vdash A(\, x \,/\, f(y_1,...,y_n), y_1,...,y_n\,) \qquad E\exists$$

V tomto případě nelze za kvantifikovanou proměnnou x substituovat konstantu, ale funkci zbývajících (volných) proměnných. Použijeme-li pravidlo vícekrát pro různé formule A, musíme za proměnnou x substituovat vždy jinou funkci $f(y_1,...,y_n)$.

Poznámky 3.3.1:

1. Pravidlo eliminace disjunkce se v literatuře často nazývá *disjunktivní sylogismus.*
2. Speciálními případy pravidla eliminace obecného kvantifikátoru jsou pravidla: $\forall x A(x) \vdash A(x)$, $\forall x A(x) \vdash A(y)$, $\forall x A(x) \vdash A(a)$, $\forall x A \vdash A$.
3. Speciálními případy pravidla zavedení existenčního kvantifikátoru jsou pravidla: $A(x) \vdash \exists x A(x)$, $A(y) \vdash \exists x A(x)$, $A(a) \vdash \exists x A(x)$, $A \vdash \exists x\, A$.
4. Často jsou jako výchozí používána také následující dedukční pravidla (v našem systému přirozené dedukce, zavedeném definicí 3.3.1, jsou však odvoditelná z pravidel Z∀, Z∃, E∀, E∃):

   - Zavedení obecného kvantifikátoru do antecedentu
     $A(x) \supset B \vdash \forall x A(x) \supset B$, x není volná v B
   - Zavedení obecného kvantifikátoru do konsekventu
     $A \supset B(x) \vdash A \supset \forall x B(x)$, x není volná v A
   - Zavedení existenčního kvantifikátoru do antecedentu
     $A(x) \supset B \vdash \exists x A(x) \supset B$, x není volná v B
   - Zavedení existenčního kvantifikátoru do konsekventu
     $A \supset B(x) \vdash A \supset \exists x B(x)$
   - Eliminace obecného kvantifikátoru z konsekventu
     $A \supset \forall x B(x) \vdash A \supset B(x)$
   - Eliminace existenčního kvantifikátoru z antecedentu
     $\exists x A(x) \supset B \vdash A(x) \supset B$

Příklady 3.3.1 /*důkazy vybraných tautologií*/: @ doplnit priklady ze cviceni

1) $\vdash \forall x\, [A(x) \supset B(x)] \supset [\forall x A(x) \supset \forall x B(x)]$

Důkaz:

1.	$\forall x\, [A(x) \supset B(x)]$	předpoklad	
2.	$\forall x A(x)$	předpoklad	
3.	$A(x) \supset B(x)$	E∀:1	
4.	$A(x)$	E∀:2	
5.	$B(x)$	MP:3,4	
6.	$\forall x B(x)$	Z∀:5	Q.E.D.

(Porovnej se sémantickým "důkazem" v poznámce 3.1.4., ad 4))

Podle věty o dedukci odpovídá tomuto teorému následující odvozené (sekundární) dedukční pravidlo:

$$\forall x\, [A(x) \supset B(x)] \vdash [\forall x A(x) \supset \forall x B(x)]$$

2) $\vdash \neg\forall x\, A(x) \equiv \exists x\, \neg A(x)$ (De Morganovo pravidlo)

Důkaz:

⇒:	1.	$\neg\forall x\, A(x)$	předpoklad
	2.	$\neg\exists x\, \neg A(x)$	předpoklad nepřímého důkazu
	3.1.	$\neg A(x)$	hypotéza

3.2. $\exists x\, \neg A(x)$ Z∃: 3.1
4. $\neg A(x) \supset \exists x\, \neg A(x)$ ZI: 3.1, 3.2
5. $A(x)$ MT: 4,2
6. $\forall x\, A(x)$ Z∀:5 spor:1 Q.E.D.

⇐: 1. $\exists x\, \neg A(x)$ předpoklad
2. $\forall x\, A(x)$ předpoklad nepřímého důkazu
3. $\neg A(c)$ E∃:1
4. $A(c)$ E∀:2 spor:3 Q.E.D.

(Porovnej se sémantickým "důkazem" v poznámce 3.1.4, ad 4).)

Podle věty o dedukci odpovídají tomuto teorému následující odvozená (sekundární) dedukční pravidla:

$$\neg\forall x\, A(x) \vdash \exists x\, \neg A(x),\ \ \exists x\, \neg A(x) \vdash \neg\forall x\, A(x)$$

3) $\vdash \neg\exists x\, A(x) \equiv \forall x\, \neg A(x)$ (De Morganovo pravidlo)

Důkaz:

⇒: 1. $\neg\exists x\, A(x)$ předpoklad
2.1. $A(x)$ hypotéza
2.2. $\exists x\, A(x)$ Z∃:2.1
3. $A(x) \supset \exists x\, A(x)$ ZI:2.1,2.2
4. $\neg A(x)$ MT:3,1
5. $\forall x\, \neg A(x)$ Z∀:4 Q.E.D.

⇐: 1. $\forall x\, \neg A(x)$ předpoklad
2. $\exists x\, A(x)$ předpoklad nepřímého důkazu
3. $A(c)$ E∃:2
4. $\neg A(c)$ E∀:1 spor:3 Q.E.D.

Teorému odpovídají následující dedukční pravidla:

$$\neg\exists x\, A(x) \vdash \forall x\, \neg A(x),\ \ \forall x\, \neg A(x) \vdash \neg\exists x\, A(x)$$

Pozn.: Ve druhých částech důkazů 2) a 3) jsme použili pravidlo eliminace existenčního kvantifikátoru (E∃). Toto pravidlo není korektní v tom smyslu, že nemusí zachovávat pravdivost formule (formule $\exists x\, A(x) \supset A(c)$ není tautologií, srovnej se Skolemizací, viz kap. 3.2). Používáme je však nejčastěji v kombinaci s pravidlem E∀. V tom případě aplikujeme nejdříve pravidlo E∃ s nějakou novou konstantou a teprve pak E∀ se stejnou konstantou.

4) $\vdash \forall x\, [A(x) \supset B(x)] \supset [\exists x A(x) \supset \exists x B(x)]$ (6. tautologie z příkladu 3.1.4)

Důkaz:

1. $\forall x\, [A(x) \supset B(x)]$ předpoklad
2. $\exists x A(x)$ předpoklad
3. $A(a)$ E∃:2
4. $A(a) \supset B(a)$ E∀:1
5. $B(a)$ MP:3,4
6. $\exists x B(x)$ Z∃:5 Q.E.D.

5) $\vdash \forall x\,[A \vee B(x)] \equiv A \vee \forall x B(x)$, kde A neobsahuje volnou x

(17. tautologie z příkladu 3.1.4)

Důkaz:

$\Rightarrow$:	1.	$\forall x\,[A \vee B(x)]$	předpoklad	
	2.	$A \vee B(x)$	E$\forall$: 1	
	3.	$A \vee \neg A$	teorém	disjunkce hypotéz
	3.1.	A	1. hypotéza	
	3.2.	$A \vee \forall x B(x)$	ZD: 3.1	Q.E.D.
	4.1.	$\neg A$	2. hypotéza	
	4.2.	$B(x)$	ED: 2, 4.1	
	4.3.	$\forall x B(x)$	Z$\forall$: 4.2	
	4.4.	$A \vee \forall x B(x)$	ZD: 4.3.	Q.E.D.
$\Leftarrow$:	1.	$A \vee \forall x B(x)$	předpoklad, disjunkce hypotéz	
	2.1.	A	1. hypotéza	
	2.2.	$A \vee B(x)$	ZD: 2.1	
	2.3.	$\forall x\,[A \vee B(x)]$	Z$\forall$: 2.2	Q.E.D.
	3.1.	$\forall$xB(x)	2. hypotéza	
	3.2.	$B(x)$	E$\forall$: 3.1	
	3.3.	$A \vee B(x)$	ZD: 3.2	
	3.4.	$\forall x\,[A \vee B(x)]$	Z$\forall$: 3.3	Q.E.D.

6) $\vdash (A(x) \supset B) \supset (\forall x A(x) \supset B)$

Důkaz:

1.	$A(x) \supset B$	předpoklad
2.	$\forall x A(x)$	předpoklad
3.	$\neg A(x) \vee B$	podle pravidla $C \supset D \vdash \neg C \vee D$ z 1.
4.	$A(x)$	E$\forall$: 2
5.	B	ED: 3,4

Teorému odpovídá následující dedukční pravidlo (zavedení obecného kvantifikátoru do antecedentu - viz poznámky 3.3.1):

$$A(x) \supset B \vdash \forall x A(x) \supset B$$

Věta 3.3.1 /*o korektnosti*/:

Každý teorém (dokazatelná formule) systému přirozené dedukce predikátové logiky je tautologií predikátové logiky: Jestliže $\vdash A$, pak $\models A$.

Věta 3.3.2 /*o sémantické úplnosti*/:

Každá tautologie predikátové logiky je v systému přirozené dedukce dokazatelná (je teorémem): Jestliže $\models A$, pak $\vdash A$.

Definice 3.3.2 /*systém přirozené dedukce s identitou*/:

Systém přirozené dedukce predikátové logiky zavedený v definici 3.3.1 rozšíříme následujícím způsobem:

- Abecedu predikátové logiky zvětšíme o speciální binární predikátový symbol (predikátovou konstantu) "=", tzv. predikát ***základní rovnosti /identity/***. Místo standardního zápisu = (x, y), budeme však používat obvyklý infixový zápis $x = y$.

- Množinu výchozích (nedokazovaných) dedučních pravidel zvětšíme o následující dvě pravidla umožňující práci s predikátem rovnosti. Výrazy t, s jsou libovolné termy, výraz A(t) je výsledek korektní substituce A(x/t):

Zavedení identity	A |– $x = x$	ZId
Eliminace identity:	A(t), t = s |– A(s)	EId

Příklady 3.3.2 /důkazy teorémů a sekundárních pravidel s identitou/**:**

1) |– t = s ⊃ s = t neboli: t = s |– s = t (pravidlo **symetrie)**

Důkaz:

1. t = s	předpoklad	
2. t = t	ZId: 1	
3. s = t	EId: 2, 1 /A(x) je x = t/	Q.E.D.

2) |– t = s ⊃ (s = r ⊃ t = r) neboli: t = s, s = r |– t = r (pravidlo **tranzitivity)**

Důkaz:

1. t = s	předpoklad	
2. s = r	předpoklad	
3. s = t	pravidlo komutativity: 1	
4. t = r	EId: 2, 3 /A(x) je x = r/	Q.E.D.

3) |– t = s ⊃ (A(t) ≡ A(s)) neboli: t = s |– A(t) ⊃ A(s)

Důkaz:

⇒:	1. t = s	předpoklad	
	2. A(t)	předpoklad	
	3. A(s)	EId: 2, 1	Q.E.D.
⇐:	1. t = s	předpoklad	
	2. A(s)	předpoklad	
	3. s = t	pravidlo symetrie: 1	
	4. A(t)	EId: 2, 3	Q.E.D.

3.4. Axiomatický systém predikátové logiky

3.4.a. Úvodní poznámky:

Nebudeme zde znovu opakovat obecné charakteristiky formálních systémů, které jsme neformálně vyjádřili v 2.4.a, neboť axiomatická metoda v predikátové logice je zobecněním axiomatické metody ve výrokové logice. Od této se liší pouze tím, že pracuje s obecnějším jazykem (jazykem predikátové logiky – viz definice 3.1.1) a v souvislosti s tím používá rozšířenou množinu výchozích teorémů (axiómů, resp. axiomových schémat) a rozšířenou množinu výchozích odvozovacích pravidel – viz následující definice 3.4.1.

Pojem důkazu (s prázdnou nebo neprázdnou množinou předpokladů) a pojem teorému – viz kapitola 2.4 – zůstávají beze změny.

Přímočaře se zobecňují hlavní věty o axiomatickém systému výrokové logiky: věta o dedukci (každému teorému ve tvaru implikace odpovídá dedukční pravidlo a každému dedukčnímu pravidlu teorém), věta o korektnosti (každá formule dokazatelná s prázdnou množinou předpokladů je tautologií, nebo logicky vyplývá z množiny předpokladů v případě důkazu z předpokladů) a sémantické úplnosti (každá tautologie je dokazatelná).

3.4.b. Formální systém (logický kalkul) Hilbertova typu

Definice 3.4.1 /***definice axiomatického systému Hilbertova typu***/**:**

- ***Jazyk***:
  Viz definice 3.1.1 s jedinou výjimkou: množina funktorů je omezena na funktory $\neg$, $\supset$, $\forall$.
- ***Axiómová schémata***:
  A1: $A \supset (B \supset A)$
  A2: $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
  A3: $(\neg B \supset \neg A) \supset (A \supset B)$
  A4: $\forall x A(x) \supset A(x/t)$ Term t je substituovatelný za x v A
  A5: $(\forall x[A \supset B(x)]) \supset (A \supset \forall x B(x))$, x není volná v A
- ***Odvozovací pravidla***:
  MP: A, $A \supset B$ |– B (pravidlo odloučení, *modus ponens*)
  G: A |– $\forall x$A (pravidlo generalizace)@

Důkaz je konečná posloupnost kroků – dobře utvořených formulí (DUF) dle gramatiky jazyka, z nichž každá je buď axióm nebo vznikne z předchozích DUF pomocí odvozovacího pravidla. Posledním krokem je dokazovaná formule – ***teorém***.

Poznámky 3.4.1:

1. Právě definovaný axiomatický systém predikátové logiky je zobecněním axiomatického systému výrokové logiky zavedeného v definici 2.4.1.

2. Definovaný axiomatický systém pracuje pouze s funktory $\neg$, $\supset$, $\forall$. Ostatní funktory můžeme používat jako zkratky (zkracující a zpřehledňující zápis formulí) definované takto:

   Z1: $A \wedge B =_{df} \neg(A \supset \neg B)$

   Z2: $A \vee B =_{df} \neg A \supset B$

   Z3 $A \equiv B =_{df} (A \supset B) \wedge (B \supset A)$

   Z4 : $\exists x A =_{df} \neg \forall x \neg A$

   Symboly $\wedge$, $\vee$, $\equiv$, $\exists$ nepatří do jazyka definovaného axiomatického systému, jsou to metasymboly sloužící k označování složených formulí jistého typu.
   Axiomatických systémů predikátové logiky je mnoho a různé systémy pracují s různými množinami funktorů (a přirozeně i s různými množinami axiómů nebo axiómových schémat).

3. Při psaní formulí lze využívat konvencí šetřících závorky – viz poznámka 3. k definici 3.1.1.

4. **Volba axiómů** není pochopitelně zcela libovolná; aby byl systém ”rozumný”, tedy korektní, podléhá dvěma kritériím:
   - Každý **axióm je *tautologie***
   - Množina axiómů musí umožňovat, aby se z nich daly odvodit všechny logicky platné formule a přitom je rozumné, aby tato množina byla minimální, tedy žádný axióm není dokazatelný z jiných axiómů – ***nezávislá množina axiómů***.

5. Rovněž **volba odvozovacích pravidel** není libovolná. Aby byl systém korektní, musí pravidla ‘zachovávat pravdivost‘ v tom smyslu, že formule, kterou podle pravidla obdržíme, je pravdivá alespoň ve všech modelech předpokladů pravidla, tedy z těchto předpokladů vyplývá.

   Tedy pro každé pravidlo $A_1,\ldots,A_n \vdash B$ by mělo platit, že $A_1,\ldots,A_n \models B$. Pravidlo generalizace $A(x) \vdash \forall x A(x)$ však zjevně tento požadavek obecně nesplňuje, formule $A(x) \supset \forall x A(x)$ není tautologie. Přesto je Hilbertův kalkul korektní systém a formuli $A(x) \supset \forall x A(x)$ v něm *nedokážeme*. Jak je to možné? Intuitivní zdůvodnění tohoto pravidla je nasnadě: Máme-li dokázat nějakou vlastnost pro všechny objekty, je možno ji dokázat na jednom *libovolně* vybraném (při důkazu však nesmíme používat žádných dalších specifických vlastností tohoto objektu). Vzpomeňme si, jak jsme prováděli ve škole např. důkazy v geometrii. Nakreslíme *libovolný* trojúhelník a pro tento trojúhelník provedeme nějakou konstrukci, jejíž pomocí dokážeme zkoumanou vlastnost (tohoto) trojúhelníka, a protože to byl trojúhelník libovolný, prohlásíme, že tuto vlastnost mají všechny trojúhelníky. Musíme si však dát pozor, aby zvolený trojúhelník byl skutečně libovolný, tedy aby neměl nějakou další vlastnost, třeba rovnoramenný, protože takovéto specifické vlastnosti nesmíme – ani podvědomě – v důkazu využít. Jinak bychom naše tvrzení dokázali pouze pro všechny *rovnoramenné* trojúhelníky.

   Podrobně viz Věta 3.4.2 o korektnosti.

Příklady 3.4.1 /důkazy teorémů a sekundárních odvozovacích pravidel/**:**

1) $\vdash A(x/t) \supset \exists x A(x)$
(pravidlo zavedení existenčního kvantifikátoru ve tvaru teorému – viz def. 3.3.1)
Důkaz:

1.	$\forall x \neg A(x) \supset \neg A(x/t)$	ax. schéma A4
2.	$\neg\neg\forall x \neg A(x) \supset \forall x \neg A(x)$	teorém typu $\neg\neg C \supset C$
3.	$\neg\neg\forall x \neg A(x) \supset \neg A(x/t)$	$C \supset D, D \supset E \vdash C \supset E$: 2, 1 TI
4.	$\neg\exists x A(x) \supset \neg A(x/t)$	Z4: 3
5.	$[\neg\exists x A(x) \supset \neg A(x/t)] \supset [A(x/t) \supset \exists x A(x)]$	ax. schéma A3
6.	$A(x/t) \supset \exists x A(x)$	MP: 4, 5 Q.E.D.

2) $A \supset B(x) \vdash A \supset \forall x B(x)$ x není volná v A
(pravidlo zavedení obecného kvantifikátoru do konsekventu – viz poznámka 3. k definici 3.3.1/
Důkaz:

1.	$A \supset B(x)$	předpoklad
2.	$\forall x[A \supset B(x)]$	G: 1
3.	$\forall x[A \supset B(x)] \supset [A \supset \forall x B(x)]$	ax. schéma A5
4.	$A \supset \forall x B(x)$	MP: 2,3 Q.E.D.

Věta 3.4.1 /***o dedukci***/**:**
Pro *uzavřenou* formuli A a libovolnou formuli B platí:
$\vdash A \supset B$ právě tehdy, když $A \vdash B$.

Poznámka 3.4.2:
Tvrzení
"je-li $\vdash A \supset B$, pak také $A \vdash B$"
platí bez ohledu na to, zda formule A je, či není uzavřená (platnost tvrzení vyplývá ihned z pravidla MP). Naproti tomu opačné tvrzení
"je-li $A \vdash B$, pak také $\vdash A \supset B$"
pro otevřené formule A (tj. formule obsahující aspoň jednu volnou proměnnou x) platné není. To ukážeme na následujícím příkladě. Nechť formule A je $A(x)$ a formule B je $\forall x A(x)$. Potom dedukce $A \vdash B$ představuje obecně platné odvozovací pravidlo (pravidlo generalizace viz definice 3.4.1) $A(x) \vdash \forall x A(x)$, zatímco formule $A(x) \supset \forall x A(x)$ obecně platná není (není to tautologie a tedy – podle věty 3.4.2 o korektnosti – není ani dokazatelná) – srovnej s poznámkou k definici 3.1.5. a s poznámkou 3.4.1.

Věta 3.4.2 /***o korektnosti***/**:**
Každá dokazatelná formule predikátové logiky (tj. teorém kalkulu Hilbertova typu) je také tautologií predikátové logiky. Formálně: **Jestliže $\vdash A$, pak $\models A$**.

Důkaz /nástin/**:**
Všechny formule, které obdržíme z axiómových schémat A1–A5 jsou tautologiemi, tedy jsou pravdivé v každé interpretační struktuře I (při libovolné valuaci e volných proměnných). Korektnost pravidla MP (*modus ponens*) byla demonstrována v důkazu Postovy věty 2.4.4.

Korektnost pravidla generalizace $A(x) \vdash \forall x A(x)$ je zaručena definicí splňování formule $\forall x A$ ve struktuře I. Předpokládejme, že jsme v důkazové posloupnosti dosud

pravidlo generalizace nepoužili. Tedy formule A(x) musí být tautologií (neboť mohla vzniknout z axiómů – tautologií pouze použitím pravidla MP, které zachovává pravdivost). To znamená, že v libovolné struktuře I platí, že $\models_I$ A(x)[e] – formule A(x) je pravdivá v I pro libovolné ohodnocení e proměnné x. Tedy platí pro *libovolné* individuum i $\in$ M, kde M je universum zvolené v interpretační struktuře I, že formule A je pravdivá v I pro valuaci, která přiřazuje individuum i proměnné x, tedy $\models_I$ A[e(x/i)], kde e(x/i) je valuace stejná jako e až na to, že přiřazuje proměnné x individuum i. Tedy formule $\forall x$A(x) je pravdivá v I, $\models_I \forall x$A(x). Pravidlo generalizace je korektní v tom smyslu, že *zachovává* ***pravdivost formule v interpretaci.***

Poznámka 3.4.3. Jelikož pojmy *pravdivosti formule v interpretaci* (pravdivost pro *všechna* ohodnocení volných proměnných) a *splnitelnost formule v interpretaci* (pravdivost pro *alespoň jedno* ohodnocení volných proměnných) pro uzavřené formule splývají, bude se pravidlo generalizace "chovat korektně" vždy za předpokladu, že odvozujeme z *tautologických* axiómů nebo ze speciálních axiómů, které jsou všechny ***uzavřené formule.*** Proto jsou speciální axiómy teorií voleny vždy jako uzavřené formule, tzv. ***sentence*** či ***výroky.*** Viz kapitola 4.

Věta 3.4.3 /*o sémantické úplnosti axiomatického systému - K. Gödel*/:

Každá tautologie predikátové logiky je dokazatelná (v logickém kalkulu Hilbertova typu). Formálně, **je-li |= A pak |– A**.

Definice 3.4.2 /*axiomatický systém predikátové logiky s identitou*/:

Axiomatický systém zavedený v definici 3.4.1 rozšíříme následujícím způsobem:

- Abecedu predikátové logiky zvětšíme o speciální binární predikátový symbol (predikátovou konstantu) "=", tzv. predikát ***základní rovnosti (identity)***. Místo standardního zápisu =(x, y), budeme však používat obvyklý infixový zápis $x = y$.
- Množinu axiómových schémat zvětšíme o následující tři schémata charakterizující predikát rovnosti:

$$\vdash \forall x\,(x = x) \qquad \text{R1}$$

$$\vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\,[x_1 = y_1 \wedge \ldots \wedge x_n = y_n \supset f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)]$$

pro libovolný n-ární funkční symbol f R2

$$\vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\,[x_1 = y_1 \wedge \ldots \wedge x_n = y_n \supset p(x_1,\ldots,x_n) \equiv p(y_1,\ldots,y_n)]$$

pro libobolný n-ární predikátový symbol p R3

Poznámky 3.4.4:

1. Axiómová schémata R2, R3 říkají, že identické předměty nelze rozlišit pomocí žádné funkce nebo predikátu. Naplňují tak Leibnitzovo pojetí identity: identické je to, co nelze žádným způsobem rozlišit.
2. Rovnost (identitu) lze charakterizovat i jiným způsobem – viz např. zavedení identity v systému přirozené dedukce. Axiómová schémata R2, R3 můžeme také nahradit následujícími axiómy komutativity a tranzitivity rovnosti:

$$\vdash \forall x \forall y[x = y \supset y = x] \qquad \text{R2'}$$

$\vdash \forall x \forall y \forall z [x = y \wedge y = z \supset x = z]$ R3'

V systému predikátové logiky zavedeném definicí 3.4.2 jsou však formule R2', R3' dokazatelnými formulemi .

3. Podle toho, zda považujeme pojem rovnosti za univerzální logický pojem nebo za speciální (specifický) pojem konkrétního formálního systému (vztahující se ke konkrétní předmětné oblasti, např. k teorii přirozených čísel), dáváme přednost buď ***predikátové logice s rovností*** (podle definice 3.4.2) nebo ***predikátové logice bez rovnosti*** (definice 3.4.1).

Příklad 3.4.2 /důkazy formulí s rovností/**:**

1) $\vdash \forall x \forall y [x = y \supset y = x]$

Důkaz:

1. $\forall x \forall y \forall z \forall t\ [x=y \wedge z=t \supset (x=z \equiv y=t)]$ R3 (predikátem p je rovnost =)
2. $x=y \wedge x=x \supset x=x \equiv y=x$ 4-násobné použití "pravidla A4" na 1., subst. *x/x, y/y, z/x, t/x*
3. $x=y \wedge x=x \supset y=x$ pravidlo $A \wedge B \supset (B \equiv C) \vdash A \wedge B \supset C$ na 2
4. $\forall x[x=x]$ R1
5. $x = x$ "pravidlo A4" na 4., subst. *x/x*
6. $x=y \supset x=y \wedge x=x$ pravidlo $A \vdash B \supset B \wedge A$ na 5.
7. $x=y \supset y=x$ pravidlo $A \supset B, B \supset C \vdash A \supset C$ na 6., 3.
8. $\forall x \forall y[x=y \supset y=x]$ pravidlo G na 7.(dvakrát), Q.E.D.

2) $\vdash \forall x \forall y \forall z\ [x=y \wedge y=z \supset x=z]$

Důkaz:

1. $\forall x \forall y \forall z \forall t\ [x=y \wedge z=t \supset (x=z \equiv y=t)]$ R3 (predikátem p je rovnost =)
2. $x=y \wedge y=z \supset (x=z \equiv y=y)$ 4-násobné použití "pravidla A4" na 1., subst. *x/x, y/y, z/z, t/y*
3. $\forall x\ [x=x]$ R1
4. $y=y$ "pravidlo A4" na 4., subst. *y/y*
5. $x=y \wedge y=z \supset x=z$ pravid. $A, B \supset (C \equiv A) \vdash B \supset C$ na 4.,2.
6. $\forall x \forall y \forall z\ [x=y \wedge y=z \supset x=z]$ pravidlo G na 5./třikrát/, Q.E.D.

4. Formalizované teorie predikátové logiky 1. řádu.

Úvodní poznámky:

1. ***Historický vývoj teorií.***

a) Stadium empirické popisné teorie:
- Důraz je kladen na shromažďování faktů před hledáním souvislostí mezi nimi.
- Otázka "co platí?" předchází otázce "proč to platí?".
- Jsou dány pouze vzory řešení (paradigmata) typických úloh

b) Stadium neformalizované axiomatické teorie:
- Stanoveny primitivní pojmy, které se nedefinují, ale pomocí nichž se definují všechny ostatní pojmy. Stanoveny primitivní poznatky (axiómy), které se nezdůvodňují (nedokazují), ale ze kterých se odvozují všechny ostatní poznatky.
- Používání symbolů pro formální zápis poznatků.
- Prostředky odvozování a dokazování formalizovány nejsou, logika je používána na intuitivní úrovni.
- Příklady neformalizovaných axiomatických teorií:
  - Euklidovská geometrie (4. st. př. Kr.).
  - Všechny matematické teorie až do konce 19.století.
  - Fyzikální teorie: mechanika (klasická, relativistická, kvantová), termodynamika, teorie elektromagnetického pole, geometrická optika,...

c) Stadium formalizované axiomatické teorie:
- Zformalizovány jsou nejenom poznatky, ale i procesy odvozování jedněch poznatků z druhých. Logika je nedílnou součástí každé teorie.
- Formalizace dokazování není samoúčelná. Nutnost formálních důkazů byla vyvolána objevením antinómií (sporů) v základech matematiky (teorii množin). Proto se snažíme budovat korektní (bezespornou) teorii.
- Formalizovaná teorie může být rozvíjena automaticky (formálně) bez porozumění obsahovému smyslu (sémantice) dokazovaných tvrzení.

2. ***Antinomie (paradoxy).***

a) Antinomie **množiny všech množin**.

- Nechť M je množina všech množin. To znamená, že každá podmnožina množiny M je prvkem množiny M. Z toho plyne, že mohutnost (početnost, kardinalita) množiny M je alespoň rovna mohutnosti množiny všech podmnožin množiny M, neboli

$$\text{card}(M) \geq \text{card}(2^M).$$

- Na druhé straně je zřejmé, že množina všech podmnožin neprázdné množiny (a množina všech množin neprázdnou zajisté bude) má větší mohutnost než výchozí množina (kromě toho, že obsahuje všechny jednoprvkové podmnožiny, obsahuje navíc mnoho dalších podmnožin), neboli $\text{card}(M) < \text{card}(2^M)$.
  To je ve sporu s předchozí nerovností.

b) **Russellova antinomie**.

- Zřejmě není obecně vhodné, aby podmnožina dané množiny (a speciálně tedy i celá množina) byla prvkem dané množiny. Definujme proto jako *normální množinu* takovou množinu, která není svým vlastním prvkem. Položme otázku: je množina N všech normálních množin normální množinou?
- Je-li odpověď na položenou otázku ano, pak N neobsahuje sebe samu jako svůj prvek a tedy N není množinou všech normálních množin.
- Je-li odpověď na položenou otázku ne, pak N obsahuje sebe samu jako svůj prvek a tedy N – v rozporu se svou definicí – obsahuje jako prvek množinu, která není normální.
- Obě dvě možné odpovědi na položenou otázku jsou tedy špatné. Podstata sporu lépe vynikne z formálního zápisu. Symbolicky můžeme definici množiny N zapsat takto:

$$x \in N \Leftrightarrow \neg(x \in x) \quad .$$

Položená otázka vede ke sporné formuli (kontradikci)

$$N \in N \Leftrightarrow \neg(N \in N).$$

c) Podobných antinomií, jako jsou dvě výše uvedené, bylo formulováno více. O způsobech, jak se jim vyhnout, viz kap.4.3 o formalizovaných teoriích množin.

3. ***Hilbertův program*** (počátek 20. století)**.**

- Počátkem 20. století požadoval D. Hilbert vytvoření zformalizované teorie zahrnující celou matematiku a dokázání bezespornosti této teorie finitními prostředky.
- V 30. letech K. Gödel dokázal nemožnost naplnění Hilbertova programu:
  - bezespornost formální aritmetiky (a všech teorií, které aritmetiku přirozených čísel obsahují jako svou část) nelze dokázat finitními prostředky
  - každá bohatší formální teorie (zahrnující alespoň aritmetiku přirozených čísel) je neúplná, tj. existují dobře formulovaná tvrzení (reprezentovaná formulemi), která nejsou v rámci dané teorie ani dokazatelná, ani vyvratitelná.

4.1. Teorie relací a algebraické teorie 1. řádu.

Definice 4.1.1:

Formální teorie je zadána trojicí:

- formální jazyk teorie
- množina axiómů teorie
- množina dedukčních pravidel teorie

Formální jazyk teorie 1. řádu je jazyk predikátové logiky 1. řádu (viz definice 3.1.1). Formální jazyk je tedy množina všech dobře (syntakticky správně) utvořených formulí.

Množina axiómů teorie je podmnožina množiny všech dobře utvořených formulí. Sestává ze dvou částí:

- množiny ***logických*** axiómů (např. těch uvedených v definici 3.4.1 – tedy tautologií)
- množiny ***speciálních*** (specifických) axiómů. Množina speciálních axiómů charakterizuje pomocí formulí predikátové logiky vlastnosti (a vztahy mezi nimi) všech objektů určených primitivními pojmy teorie (tj. speciální predikátové a funkční symboly, spec. konstanty), které v jazyce teorie vystupují. Tedy speciální axiómy jsou voleny tak, aby byly pravdivé v "zamýšlené" interpretaci předmětné oblasti.

Množina dedukčních pravidel teorie splývá s množinou dedukčních pravidel použitého kalkulu predikátové logiky (viz např. definici 3.4.1).

Formální teorie (v širším slova smyslu) je množina všech formulí, které lze odvodit z axiómů teorie pomocí dedukčních pravidel teorie. Vzhledem k tomu, že teorie je plně charakterizována množinou T speciálních axiómů, ztotožňujeme někdy formální teorii T s množinou speciálních axiómů teorie (pojem formální teorie v užším slova smyslu). Proto bývá definován pojem důkazu z teorie takto:

Důkaz formule A z teorie T (značíme T |– A) je posloupnost dobře utvořených formulí (kroků důkazu) taková, že:

- poslední krok této posloupnosti je dokazovaná formule A
- každý krok důkazu je buďto
  - logický axióm, nebo
  - speciální axióm teorie, nebo
  - formule, která vznikla z předchozích kroků aplikací některého dedukčního pravidla teorie

Poznámky 4.1.1:

1. Axiomatický systém predikátové logiky (např. ten zavedený definicí 3.4.1) je speciálním případem formální teorie s prázdnou množinou speciálních axiómů. Axiomatický systém výrokové logiky (např. ten zavedený definicí 2.4.1) je rovněž speciálním případem formální teorie s prázdnou množinou speciálních axiómů a navíc s omezenou množinou logických axiómů. Viz úvod ke kapitole 2.4.

2. Formální teorie mohou být rovněž budovány např. na bázi přirozené dedukce. V Gentzenově systému je množina logických axiómů dána jediným schématem ($A \supset A$) a množiny dedukčních pravidel jsou obsáhlejší (viz např. definice 3.3.1 a 2.3.1).

Nejdůležitější matematické teorie, které jsou v moderní matematice budovány axiomaticky, jsou teorie relací (především ostrého a neostrého uspořádání, ekvivalence), dále všechny algebraické teorie (teorie grup, okruhů, těles, svazů, atd.) a aritmetické teorie.

Příklad 4.1.1 /T*eorie (ostrého) uspořádání/*:

1. varianta:

- Speciální konstanty:
  - = ... binární predikátová konstanta
  - < ... binární predikátová konstanta
- Logické axiómy: axiómy predikátové logiky bez rovnosti
- Speciální axiómy:

U1. $\forall x\ [x = x]$ reflexivita
U2. $\forall x\ \forall y\ [x=y \supset y=x]$ symetrie
U3. $\forall x\ \forall y\ \forall z\ [(x=y \wedge y=z) \supset (x=z)]$ transitivita
U4. $\forall x\ \forall y\ \forall z\ [(x=y \wedge x<z) \supset (y<z)]$
U5. $\forall x\ \forall y\ \forall z\ [(x=y \wedge z<x) \supset (z<y)]$
U6. $\forall x\ \forall y\ [(x<y) \supset \neg(y<x)]$ asymetrie
U7. $\forall x\ \forall y\ \forall z\ [(x<y \wedge y<z) \supset (x<z)]$ transitivita
U8. $\forall x\ \forall y\ [x=y \vee x<y \vee y<x]$
U9. $\forall x\ \exists y\ [x<y]$
U10. $\forall x\ \exists y\ [y<x]$
U11. $\forall x\ \forall y\ [x<y \supset \exists z\ [x<z \wedge z<y]]$

2. varianta:

- Speciální konstanta:
  < ... binární predikátový symbol /konstanta/
- Logické axiómy: axiómy predikátové logiky s rovností (viz definice 3.4.2)
- Speciální axiómy:

V1. $\forall x\ \forall y\ [x<y \supset \neg(y<x)]$ asymetrie
V2. $\forall x\ \forall y\ \forall z\ [x<y \wedge y<z \supset x<z]$ transitivita
V3. $\forall x\ \forall y\ [x=y \vee x<y \vee y<x]$
V4. $\forall x\ \exists y\ [x<y]$
V5. $\forall x\ \exists y\ [y<x]$
V6. $\forall x\ \forall y\ [x<y \supset \exists z\ (x<z \wedge z<y)]$

Různě obsáhlé teorie:

- **Teorie rovnosti**: U1-U3
  Modely: rovnost na množině přirozených (celých, racionálních, reálných) čísel, rovnost na množině všech matic daného typu,...
- **Teorie ostrého uspořádání** U1-U7 nebo V1-V2
  Modely: rovnost a ostré uspořádání na množině přirozených (celých, racionálních, reálných) čísel, rovnost a vlastní inkluze na množině všech podmnožin dané množiny,...

- **Teorie lineárního ostrého uspořádání**: U1-U8 nebo V1-V3
  Modely: rovnost a ostré uspořádání na množině přirozených (celých, racionálních, reálných) čísel, rovnost a lexikografické uspořádání na množině všech slov nad danou abecedou,...
- **Teorie hustého uspořádání**: U1-U11 nebo V1-V6
  Modely: rovnost a ostré uspořádání na množině racionálních (reálných) čísel,...

Příklad 4.1.2 /***Teorie částečného (neostrého) uspořádání/***
Struktura <M, ≤ > (tj. neprázdná množina M, na které je definována binární relace ≤, ≤ ⊆ M × M), která splňuje axiomy teorie částečného uspořádání, tj. množinu formulí i), ii), iii), se nazývá ***(částečně) uspořádaná množina*** neboli ***poset*[2]*.***

i) $\forall a\,(a \le a)$ reflexivita
ii) $\forall a \forall b\,[(a \le b \wedge b \le a) \supset (a = b)]$ antisymetrie
iii) $\forall a \forall b \forall c\,[(a \le b \wedge b \le c) \supset (a \le c)]$ transitivita

Pozn.: Relace, která splňuje pouze axiómy i) a iii), tedy není antisymetrická, se nazývá ***kvazi-uspořádání***.

Modely:
Množina N přirozených čísel při obvyklém uspořádání menší nebo roven.
Množina individuí uspořádaná relací "starší nebo stejně starý".
Množina N přirozených čísel s relací |, která je definována jako $m \mid n$ právě když m dělí n (beze zbytku).

Poslední příklad ilustruje, proč je toto uspořádání nazýváno 'částečné'. V množině M mohou totiž existovat tzv. nesrovnatelné prvky a,b, pro které neplatí ani $a \le b$ ani $b \le a$.

Poznámka: Na částečně uspořádaných množinách zavádíme dva důležité pojmy, a to pojem *supréma a infima.* Buď ⟨M, ≤⟩ částečně uspořádaná množina a N její podmnožina. Řekneme, že prvek $a \in M$ je ***suprémem množiny N v M***, značíme $a = \sup_M(N)$, jestliže prvek a je nejmenší horní závora množiny N v M, tj. platí, že

$$\forall x\,[(x \in N \supset a \ge x) \wedge \forall y\,(y \in M \wedge y \ge x) \supset (y \ge a)]$$

Analogicky definujeme ***infimum množiny N v množině M,*** značíme $a = \inf_M(N)$, jestliže prvek a je největší dolní závora množiny N v M, tj. platí, že

$$\forall x\,[(x \in N \supset a \le x) \wedge \forall y\,(y \in M \wedge y \le x) \supset (a \ge y)].$$

Často se stává, že relace, která se jeví jako částečné uspořádání, je ve skutečnosti kvazi-uspořádání, neboť nesplňuje axióm antisymetrie:
Model axiómů i) a iii) – *kvaziuspořádaná množina*:
Množina F formulí jazyka PL^1 uspořádaná relací logického vyplývání |=.
(Platí-li, že A |= B a B |= A, pak formule A, B jsou pouze ekvivalentní, avšak ne identické: např. A ⊃ B a ¬A ∨ B.)

Chceme-li přesto takovou množinu (částečně) uspořádat, použijeme následující "trik": Je-li relace |= kvazi-uspořádáním, pak definujeme na dané množině F relaci ***ekvivalence*** takto: A ⇔ B právě když A |= B a B |= A. (Připomínáme, že relace ekvivalence musí splňovat axiómy *reflexivity, symetrie a transitivity*.)

[2] Výraz "poset" je akronym pocházející z anglického "partially ordered set"

Je známo z teorie relací, že každá relace ekvivalence ≡ na množině M definuje ***rozklad*** množiny M na disjunktní podtřídy (podmnožiny M) takové, že jejich sjednocení pokrývá celou množinu M. Tedy do jedné třídy tohoto rozkladu patří všechny vzájemně ekvivalentní prvky a kterýkoli z nich může sloužit jako ***representant*** dané třídy (vzhledem k ekvivalenci). Množina těchto tříd rozkladu se nazývá ***faktorová množina*** a značí se obvykle M/≡, její prvky pak značíme [*m*], kde *m* je příslušný representant třídy.

Uvažme nyní množinu F formulí jazyka PL^1 a k ní příslušnou faktorovou množinu F/⇔. Na této množině nyní definujeme částečné uspořádání takto:

$[A_1] \le [A_2]$ právě tehdy když $A_1 \models A_2$.

Struktura < F/⇔, ≤ > nyní tvoří poset. Abychom to ukázali, musíme nejdříve ověřit, že relace ≤ je dobře (tj. korektně) definována a pak dokázat, že jsou splněny axiómy uspořádání i), ii), iii). Aby byla definice uspořádání korektní, nesmí daná relace záviset na výběru representantů tříd. Nechť tedy $A_1' \in [A_1]$ a $A_2' \in [A_2]$. Pak ovšem platí, že $A_1' \models A_1 \models A_2 \models A_2'$, tedy i $A_1' \models A_2'$ a definice je korektní. Reflexivita a transitivita relace ≤ jsou zřejmé. Ukážeme, že nyní je tato relace i antisymetrická. Je-li $[A_1] \le [A_2]$ a $[A_2] \le [A_1]$, pak $A_1 \models A_2$ a $A_2 \models A_1$. To znamená, že $A_1 \Leftrightarrow A_2$ a tedy $[A_1] = [A_2]$.

Příklad 4.1.3 ***/Teorie grup/*****:**
Struktura <G, f> (tj. neprázdná množina G, na které je definována binární operace – zobrazení f: G × G → G), která splňuje **axiomy teorie grup**, tj. množinu formulí i), ii), iii) (resp. i), ii), iii), iv)) se nazývá ***grupa*** (resp. ***komutativní, Abelova grupa***):

(f je binární funkční symbol)

i)	$\exists e \forall a\ f(e,a) = f(a,e) = a$	existence jednotkového prvku
ii)	$\forall a \forall b \forall c\ f(f(a,b),c) = f(a,f(b,c))$	asociativita
iii)	$\forall a \exists \hat{a}\ f(a,\hat{a}) = f(\hat{a},a) = e$	existence inverzního prvku
iv)	$\forall a \forall b\ f(a,b) = f(b,a)$	komutativita

Studium teorie grup ilustruje metodu axiomatického zkoumání. Zobecnění shodných ”situací” vede nejprve k vyjasnění podstaty této shody a potom k formulaci axiómů. Tím se získává soustava představující souhrn základních principů platných v kterémkoli ze souborů shodných situací (tedy řečeno ”jazykem logiky” – v kterékoli interpretační struktuře, která splňuje množinu axiómů). Ze soustavy axiómů se pak logickou dedukcí (na základě inferenčních pravidel axiomatického systému) buduje teorie zahrnující jako speciální ty ”situace”, které daly podnět k tvorbě axiómů. Tedy množina teorémů dané teorie je pravdivá v každé takové ”situaci”, tj. v každé interpretační struktuře, která je modelem axiómů. Mohou tak být objeveny i neočekávané ”shody”, tj. modely jiné než původní zamýšlené interpretace a jejich studium je pak usnadněno. Nemusíme znovu dokazovat všechna tvrzení platná v tomto modelu, víme, že platí všechny teorémy naší teorie.

Pozn.: Jako funkční symbol f volíme obvykle znak ”násobení” **‘.’,** nebo znak ”sčítání” **‘+’** v komutativní grupě, a to s infixní notací. Inversní prvek pak značíme a^{-1}, resp. -*a*, jednotkový prvek značíme 1, resp. 0.

Objasněme si tuto úlohu teorie grup na jednoduchém příkladu: Čtenáři jsou dobře známy vzorce

a) $u - v + v - w = u - w$
b) $u/v \,.\, v/w = u/w$

c) $\log_v u \,.\, \log_w v = \log_w u$

pro počítání s reálnými čísly.

Zkoumejme analogii těchto vzorců z jednotícího grupového hlediska. Především je zřejmé, že množina reálných čísel tvoří jak vzhledem k násobení tak vzhledem ke sčítání komutativní grupu. V kterékoli grupě platí teorém (grupovou operaci značíme nyní •, závorky vzhledem k asociativitě vynecháváme):

d) $u \bullet v^{-1} \bullet v \bullet w^{-1} = u \bullet w^{-1}$

Snadno nahlédneme, že vzorce a) i b) jsou speciálními případy tohoto teorému d) (vzorec a) pro aditivní grupu, b) pro multiplikativní grupu).

Označme nyní **R** množinu **R** – {0}**.** Abychom poznali, že i vzorec c) představuje přepis teorému d), uvažujme množinu **R** s binární operací • defunovanou takto:

$u \bullet v = \log U \,.\, \log V$, kde U, V jsou takové, že platí $u = \log U$, $v = \log V$.

Protože $u \bullet v = u.v$, je zřejmé, že <**R**, •> je komutativní grupa.
Uvědomíme-li si, že pro $v \neq 0$ je $u \bullet v^{-1} = \log U \,.\, (\log V)^{-1} = \log_{10} U \,.\, \log_V 10 = \log_V U$,
vidíme, že z d) dostáváme
$\log_V U \,.\, \log_W V = u \bullet v^{-1} \bullet v \bullet w^{-1} = u \bullet w^{-1} = \log_W U$ pro $v, w \neq 0$.

Příklad 4.1.3.1: Množina **Z** celých čísel tvoří vůči sčítání komutativní grupu <**Z**, +>.

Příklad 4.1.3.2: Uvažujme množinu **Z** celých čísel a definujme na této množině relaci ekvivalence takto: $a \equiv_n b$ modulo n právě tehdy když $n \mid (a - b)$, tj. čísla *a, b* mají "v kladné části" stejný zbytek po dělení číslem *n.* Tato ekvivalence definuje (jako každá ekvivalence) na **Z** rozklad na třídy celých čísel kongruentních modulo *n.* Označme tuto faktorovou množinu tříd jako $\mathbf{Z} / \equiv_n$ a její prvky označíme jako [i], kde i je representant příslušné třídy (kterýkoli prvek, nejčastěji ten, jehož absolutní hodnota je nejmenší, tedy reprezentanty budou čísla 0, 1, 2, ..., *n*-1). Pro názornost si zapíšeme např. množinu $\mathbf{Z} / \equiv_5$ modulo 5 výčtem jejích prvků:

[0] = {... -10, -5, 0, 5, 10, 15, ... }
[1] = {... -9, -4, 1, 6, 11, 16, ... }
[2] = {... -8, -3, 2, 7, 12, 17, ... }
[3] = {... -7, -2, 3, 8, 13, 18, ... }
[4] = {... -6, -1, 4, 9, 14, 19, ... }

Definujme na faktorové množině $\mathbf{Z} / \equiv_n$ binární operaci + jako sčítání tříd takto:
[i] + [j] = [i+j].
Toto sčítání je dobře definováno, neboť definovaný součet nezávisí na výběru representantů sčítaných tříd: Je-li [i] = [i'], [j] = [j'], pak $n \mid (i-i')$ a $n \mid (j-j')$, tedy $n \mid (i-i'+j-j')$, $n \mid (i+j - i'+j')$. To znamená, že [i+j] = [i'+j']. Snadno nahlédneme, že struktura $<\mathbf{Z}/\equiv_n, +>$ tvoří vůči takto definovanému sčítání komutativní grupu (je modelem axiómů grupy). Jednotkovým (či spíše nulovým) prvkem je třída [0] a inversním (opačným) prvkem k [*a*] je třída [-*a*].

Příklad 4.1.4 ***/Teorie svazů /*:**

Množina M, na které jsou definovány dvě binární operace (zobrazení $M \times M \rightarrow M$)

$\cap$ (průsek) a $\cup$ (spojení) takové, že tato struktura <M, $\cap$, $\cup$> splňuje následujících šest axiómů, se nazývá ***svaz***:

i)	$\forall(abc)\ (a \cup b) \cup c = a \cup (b \cup c)$	asociativita
ii)	$\forall(abc)\ (a \cap b) \cap c = a \cap (b \cap c)$	asociativita
iii)	$\forall(ab)\ a \cup b = b \cup a$	komutativita
iv)	$\forall(ab)\ a \cap b = b \cap a$	komutativita
v)	$\forall(ab)\ (a \cap b) \cup a = a$	Booleovy vlastnosti
vi)	$\forall(ab)\ a \cap (b \cup a) = a$	

V teorii svazů platí následující dva teorémy, které určují souvislost teorie svazů s teorií částečného (neostrého) uspořádání:

Věta: Jestliže S = <M, $\cap$, $\cup$> je svaz, pak binární relace $\leq$ definovaná na M předpisem

$a \leq b \Leftrightarrow_{df} a \cup b = b \equiv a \cap b = a$

je částečné uspořádání a navíc platí

$\forall(ab)\ [\sup\{a,b\} = a \cup b]$, $\forall(ab)\ [\inf\{a,b\} = a \cap b]$.

Věta: Je-li S = <M, $\leq$ > částečně uspořádaná množina taková, že pro každou dvou prvkovou podmnožinu množiny M existuje v M její suprémum a infimum, pak struktura S = <M, $\cap$, $\cup$> s operacemi průseku a spojení definovanými tak, že $a \cup b =_{df} \sup_M\{a,b\}$, $a \cap b =_{df} \inf_M\{a,b\}$, je modelem axiómů svazu, tedy tvoří svaz.

V každém svazu dále platí následující dva teorémy:

$\vdash\ (a \cap b) \cup (a \cap c) \leq a \cap (b \cup c)$

$\vdash\ (a \cup b) \cap (a \cup c) \geq a \cup (b \cap c)$

K uvedeným svazovým axiómům můžeme dle potřeby přidávat axiómy a zkoumat tak různé třídy svazů. Platí-li ve výše uvedených teorémech rovnost, pak se jedná o axióm ***distributivity*** a svazy, které jej splňují se nazývají *distributivní svazy*. Další důležitou třídou jsou ***modulární*** *svazy,* které splňují axióm

$\forall(a,b,c)\ (\ (a \leq c) \supset [a \cup (b \cap c) = (a \cup b) \cap c]\ )$

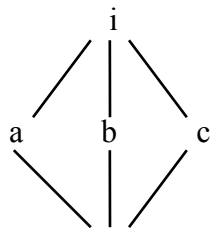
Příklady svazů:

Množina 2^M všech podmnožin dané množiny M, kde průsek je definován jako průnik množin a spojení jako sjednocení množin, tvoří (distributivní) svaz.

Faktorová množina F/$\Leftrightarrow$ tvoří (distributivní) svaz tříd ekvivalentních formulí, kde průsek a spojení jsou definovány takto:
$[A_1] \cup [A_2] = [A_1 \vee A_2]$, $[A_1] \cap [A_2] = [A_1 \wedge A_2]$,
tedy jako třída definována disjunkcí, resp. konjunkcí.

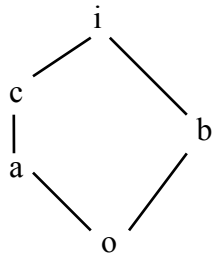
Každý distributivní svaz je modulární, ale ne naopak:

Množina {o, a, b, c, i} s uspořádáním definovaným takto:
a $\leq$ i, b $\leq$ i, c $\leq$ i, a $\geq$ o, b $\geq$ o, c $\geq$ o tvoří modulární svaz, který není distributivní, což snadno nahlédneme, znázorníme-li si tuto množinu Hasseovým diagramem:



o

Množina {i, a, b, c, o} s uspořádáním dle následujícího obrázku je svaz, který není modulární:



Teorie svazů je v poslední době hojně využívána i v oblastech ”mimo matematiku”, např. v informatice při sémantickém vyhledávání na webu jsou využívány tzv. konceptuální svazy.

Příklad 4.1.5 ***/Teorie rodokmenu a příbuzenských vztahů/*****:**

- Univerzum: množina všech individuí (žijících i zemřelých)
- Speciální primitivní symboly (funkční a predikátové) /se ”zamýšleným významem”/:
  - O ... unární funkční konstanta /O(x) ... otec x/
  - M ... unární funkční konstanta /M(x) ... matka x/
  - m ... unární predikátová konstanta /m(x) ... x je mužského pohlaví/
  - z ... unární predikátová konstanta /z(x) ... x je ženského pohlaví/
- Logické axiómy: axiómy predikátové logiky s rovností
- Odvozené funkce:
  - $DO(x) =_{df} O(O(x))$ ... děd po otci /otec otce/
  - $DM(x) =_{df} O(M(x))$ ... děd po matce /otec matky/
  - $BO(x) =_{df} M(O(x))$ ... bába po otci /matka otce/
  - $BM(x) =_{df} M(M(x))$ ... bába po matce /matka matky/
  - .....
- Odvozené predikáty:
  - $rod(x,y) \Leftrightarrow_{df} x=O(y) \vee x=M(y)$ ... x je rodičem y
  - $pred(x,y) \Leftrightarrow_{df} rod(x,y) \vee \exists z\,[pred(x,z) \wedge rod(z,y)]$ ... x je předkem y
  - $dit(x,y) \Leftrightarrow_{df} rod(y,x)$ ... x je dítětem y
  - $pot(x,y) \Leftrightarrow_{df} pred(y,x)$ ... x je potomkem y
  - $sour(x,y) \Leftrightarrow_{df} \exists z\,[rod(z,x) \wedge rod(z,y)]$ ... x,y jsou sourozenci
  - .....
- Speciální axiómy:

  A1. $\forall x \exists y\,[y = O(x)]$ každý má otce

  $\forall x \exists y\,[y = M(x)]$ každý má matku

  A2. $\forall (x,y,z)[y = O(x) \wedge z = O(x) \supset y=z]$ otec je jediný

$\forall(x,y,z)[y = M(x) \wedge z = M(x) \supset y=z]$ matka je jediná

A3. $\forall(x,y)\ [x = O(y) \supset m(x)]$ každý otec je muž

$\forall(x,y)\ [x = M(y) \supset z(x)]$ každá matka je žena

A4. $\forall x\ [m(x) \vee z(x)]$ každý je mužem nebo ženou

$\forall x\ \neg[m(x) \wedge z(x)]$ nikdo není mužem i ženou

A5. $\forall x\ \neg pred(x,x)$ nikdo není svým vlastním předkem

- Některé jednoduché věty dokazatelné z axiómů (všechny proměnné jsou obecně kvantifikovány):
  - $\vdash\ \neg rod(x,x)$
  - $\vdash\ sour(x,y) \equiv sour(y,x)$
  - $\vdash\ pot(x,y) \wedge pot(y,z) \supset pot(x,z)$
  - .....

Definice 4.1.2:

Teorie T' ***je silnější než teorie*** T, jestliže každá formule dokazatelná v T je dokazatelná i v T', ale ne naopak, tedy existuje alespoň jedna formule, která je v T' dokazatelná, ale v T nikoliv.

Teorie T ***a*** T' ***jsou ekvivalentní*** (stejně silné), jestliže každá formule, která je dokazatelná v jedné teorii, je dokazatelná i v druhé.

Teorie T' ***je rozšířením teorie*** T, jestliže používá větší množinu speciálních symbolů nebo vychází z větší množiny speciálních axiómů než teorie T. Je-li rozšířená teorie T' ekvivalentní s původní teorii T, pak hovoříme o ***nepodstatném (konzervativním) rozšíření***. Je-li teorie T' silnější než teorie T, pak hovoříme o ***podstatném rozšíření***.

Příklady 4.1.5:

Teorie (ostrého) uspořádání definovaná axiómy U1-U11 je silnější, než teorie definovaná axiómy U1-U8.

Teorie (ostrého) uspořádání definovaná axiómy U1-U11 (v predikátové logice bez rovnosti) je ekvivalentní s teorií uspořádání definovanou axiómy V1-V6 (v predikátové logice s rovností).

Přidání axiómu V6 k teorii V1-V5 má za následek její podstatné rozšíření. Zavedení nového speciálního symbolu $\leq$ novým speciálním axiómem $x \leq y \equiv x<y \vee x=y$, je však pouze konzervativním rozšířením.

Poznámky 4.1.2: /Syntaktická – lingvistická definice/

1. Nové symboly můžeme ve formální teorii definovat (zavést) dvojím způsobem:
   - ***Metasystémově*** pomocí metasymbolu "$=_{df}$" nebo $\Leftrightarrow_{df}$. V tomto případě není nový symbol součástí formálního systému, ale pouze zkratkou pro určitou formuli. Např. zápis $x \neq y$ můžeme považovat pouze za zkrácené označení formule $\neg x=y$. Neboli
   $$x \neq y \ =_{df}\ \neg x=y.$$
   - ***Systémově*** pomocí nového speciálního axiómu ve tvaru ekvivalence (rozšířením teorie). Např. symbol nerovnosti může být "implicitně definován" formulí
   $$x \neq y \equiv \neg x=y,$$
   která rozšiřuje množinu speciálních axiómů.
2. ***Korektnost systémové definice nové předmětové konstanty***.
   Platí-li současně (tj. lze-li v teorii odvodit)
   $$\vdash \exists x\ A(x),$$

$\vdash A(x) \wedge A(y) \supset x=y$,

pak lze konstantu c zavést novým axiómem ve tvaru

$\vdash A(x/c)$

(přitom předpokládáme, že symbol c nebyl dosud v teorii použit).

Příklad: Protože v teorii přirozených čísel platí

$\vdash \exists x\,[x = S(0)]$, (kde S je interpretován jako funkce následník)

$\vdash x = S(0) \wedge y = S(0) \supset x=y$,

lze definovat konstantu 1 novým axiómem

$\vdash 1 = S(0)$.

3. ***Korektnost systémové definice nového funkčního symbolu.***

Platí-li současně (tj. lze-li v teorii odvodit)

$\vdash \exists y\, A(x_1,x_2,...,x_n, y)$,

$\vdash A(x_1,x_2,...,x_n, z) \wedge A(x_1,x_2,...,x_n, t) \supset z=t$,

pak lze v této teorii definovat funkční symbol f (předpokládáme, že symbol f nebyl dosud v teorii použit) novým axiómem ve tvaru

$\vdash y = f(x_1,x_2,...,x_n) \equiv A(x_1,x_2,...,x_n, y)$.

Příklad: Protože v teorii přirozených čísel platí

$\vdash \exists y\,[y = x.x]$,

$\vdash z = x.x \wedge t = x.x \supset z=t$,

lze v této teorii zavést funkční symbol sqr novým axiómem

$\vdash y = sqr(x) \equiv y = x.x$.

4. ***Korektnost systémové definice nového predikátového symbolu.***

Nový predikátový symbol p (v teorii dosud nepoužívaný) lze zavést novým axiómem ve tvaru

$\vdash p(x_1,x_2,...,x_n) \equiv A(x_1,x_2,...,x_n)$

Příklad: V teorii uspořádání můžeme definovat nový predikátový symbol $\leq$ axiómem tvaru

$\vdash x \leq y \equiv x<y \vee x=y$

5. ***Obecné podmínky korektnosti definice.***

- Definovaný symbol obsažený v definiendu (levé části definice) je symbol, který se dosud v systému nevyskytoval.
- Definiens (pravá část definice) obsahuje jen dříve definované symboly. Výjimkou jsou rekurentní definice.
- V definiendu se každá proměnná vyskytuje jen jednou.
- Každá volná proměnná vyskytující se v jedné části definice se musí vyskytovat i v druhé části (podmínka homogenity).

4.2. Vlastnosti a význam formálních teorií – Gödelovy výsledky

Úvod.

David Hilbert (1862-1943) byl vynikající německý matematik, představitel formalistické školy, která považovala matematiku za jakousi ”hru se symboly”, která má svá pravidla, jako např. hra v šachy. Abychom to ilustrovali, zavedeme jednoduchý systém S:

Konstanty: ♣,♥
Predikáty: ♦ ♠
Axiomy systému S: (1) $\forall x\,(\diamondsuit x \supset \spadesuit x)$
$\exists x\ \spadesuit x \supset \diamondsuit \clubsuit$
$\spadesuit \heartsuit$
Inferenční pravidla: MP (modus ponens), E∀ (eliminace všeobecného kv.), Z∃ (zavedení existenčního kv.)
Teorém: ♠ ♣
Důkaz:

♠♥	(axiom 3)
$\exists x\ \spadesuit x$	(Z∃)
♦♣	(axiom 2 a MP)
♦♣ ⊃ ♠♣	(axiom 1 a E∀)
♠♣	(MP)

Symboly a celý systém S jsou zcela bez jakéhokoli významu. Axiomy nejsou ‘pravdivé’, jsou to jakási ”implicitní pravidla” pro práci se symboly. Podle (”pre-hilbertovských”) formalistů je celá matematika takováto hra se symboly, jenom trochu více komplikovaná a rafinovanější.

(Již Gottlob Frege (1884) napadl toto formalistické pojetí. Nemůžeme zde opakovat všechny jeho argumenty, uvedeme jen jeden: Hra v šachy nebo náš systém S mohou být jen hry bez jakéhokoli významu či pravdivosti. Avšak meta-teorie her může být smysluplná matematika. Např. to, že výše uvedený důkaz se skládá z pěti kroků, nebo to, že král a dva střelci nemohou vynutit mat, jsou *smysluplné,* objektivně *pravdivé* meta-teorémy.)

Hilbert si všiml, že paradoxy a konceptuální problémy matematiky jsou vždy spojeny s usuzováním zahrnujícím nekonečno. Jelikož se však veškerá naše zkušenost opírá pouze o konečné objekty, musíme v ”nekonečné klasické matematice” pracovat tak, že ji rozdělíme na bezproblémovou konečnou část, přidáme jakési ”ideální prvky”, které ”ukazují na nekonečno” a vše uděláme tak, abychom mohli s takovým systémem pracovat finitními prostředky s plnou důvěrou, že se nemohou objevit paradoxy. ”Ideální nekonečné prvky” nemůžeme samozřejmě přidávat libovolně. Absolutně nutnou podmínkou je to, že přidáním nevznikne nekonzistence. Jako příklad uvedeme analogii. Mějme dvě teorie T (tepla) a S (světla), o kterých víme, že jsou obě pravdivé (”o teple resp. o světle”). Tedy i jejich konjunktivní spojení, teorie T a S bude pravdivá. Ovšem jsou-li T a S ”dobré nástroje”, to znamená konzistentní teorie, nezaručuje to ještě, že i jejich spojení bude dobrým nástrojem, neboť některá tvrzení si mohou protiřečit (co platí o teple, nemusí platit o světle a obráceně). Tedy Hilbert chtěl dokázat, že jednotlivé části nekonečné matematiky mohou být přidány ke konečné matematice tak, aby nevznikla žádná nekonzistence. Navíc, takové důkazy chtěl obdržet bez ohledu na ***logické vyplývání, pravdivost, sémantiku,*** pouhou manipulací se symboly, jejichž konečná *struktura* je jasná, přehledná a rozpoznatelná.

Existuje mnoho způsobů, jak dokázat konzistenci. Jednoduchým způsobem je např. nalezení modelu. Chceme-li např. dokázat konzistenci transfinitní teorie množin, nemůžeme použít tuto teorii k důkazu její vlastní konzistence. Nemůžeme rovněž nijak demonstrovat, že existují (aktuálně) nekonečné množiny, které jsou touto teorií korektně popsány. Při každé takovéto demonstraci bychom vždy použili jen konečný počet objektů, i kdybychom mohli jít pokaždé "o krok dál" a to "potenciálně nekonečně daleko". Avšak jelikož je (syntaktický) důkaz pouze posloupnost symbolů manipulovaná podle určitých pravidel, stačilo by ukázat, že žádná takováto posloupnost symbolů nevyústí např. ve výraz "0 = 1" nebo "$\omega \neq \omega$".

Hilbertův program byl velice ambiciózní a měl mnoho cílů: Především, celá klasická matematika (která byla až do té doby směsicí formálních a neformálních přístupů) musí být důsledně zformalizována. (Část práce v tomto duchu odvedli již Whitehead s Russellem v *Principa Mathematica* (1910).) Dále, je nutno přesně definovat pojem '*finitní metody*'. Nakonec pak budou tyto finitní metody aplikovány na zformalizované verze klasické matematiky tak, že ukáží jasně a přehledně jednotlivé vlastnosti a vztahy a co především, dokáží jejich konzistenci. Mnoho vynikajících matematiků a filosofů 20. století (např. Ackermann, Bernays, von Neumann, atd.) pracovalo na tomto programu. To, že Gödelovy věty o neúplnosti dokázaly nemožnost jeho realizace (v plné šíři), je dnes všeobecně známo. Avšak některé "vedlejší produkty" programu (např. axiomatizace, teorie modelů, teorie rekursivních funkcí, teorie algoritmů a výpočetních metod, atd.) přinesly cenné výsledky a významně obohatily moderní matematiku.

Poznámky:

1. Studiem vlastností formálních teorií se zabývá věda zvaná metamatematika. ***Metamatematika*** je neformální teorie formálních teorií. Skutečnost, že odvozování v metamatematice je neformální (intuitivní) - a jiné být nemůže - je vyvážena tím, že metamatematika používá jen ***finitních*** (konečných) postupů, jejichž korektnost je bezprostředně evidentní. Není např. dovoleno pracovat s ***aktuálním nekonečnem*** (s nekonečnými množinami), tak jak je to v klasické matematice běžné.
2. Veškeré finitní prostředky metamatematiky mohou být reprezentovány pomocí aritmetiky přirozených čísel (poznamenejme, že aritmetika přirozených čísel pracuje pouze s tzv. ***potenciálním nekonečnem*** ve smyslu: ke každému přirozenému číslu existuje následník). Pomocí tzv. ***gödelizace*** lze přiřadit každé formuli formální teorie přirozené číslo a odvozování jedněch formulí z jiných formulí je pak převedeno na výpočet jistých aritmetických funkcí (***rekurzivních funkcí***).

Cílem této kapitoly je podat přehledně, mírně populárně, avšak přesně Gödelovy převratné výsledky. Jelikož jsou tyto výsledky chápány často chybně, někdy až "mysticky" a přitom původní Gödelovy formulace a důkazy jsou technicky poněkud obtížné, a tedy v rámci tohoto stručného učebního textu nereprodukovatelné, podáme výklad z pohledu dnešní matematické logiky a přitom využijeme z velké části velice zdařilého článku Petra Hájka (1996).

Pro úplnost zopakujeme nyní některé pojmy, se kterými jsme se již setkali v průběhu výkladu. V matematické logice pracujeme s *výroky* (neboli *sentencemi*) chápanými jako přesně definované matematické objekty. Definujeme, co to znamená, že nějaký výrok α je *dokazatelný* (z nějaké množiny výroků) a že nějaký výrok je *pravdivý* (při nějaké interpretaci jeho složek, tj. v nějakém modelu). Pojmy dokazatelnosti a pravdivosti jsou dva základní pojmy matematické logiky. Otázka, v jakém jsou tyto pojmy vztahu, tedy

Jsou dokazatelné přesně ty výroky, které jsou pravdivé?

je jednou z centrálních otázek matematické logiky. Aby měla tato otázka smysl, musí být přesně definováno, co je to výrok, pravdivost, dokazatelnost, a to lze udělat různými způsoby – v závislosti na expresivní síle logického systému. Jelikož je predikátový počet 1. řádu jedním ze základních logických kalkulů, náš výklad byl soustředěn na tento systém.

Tedy v PL^1:

uzavřené formule jsou *výroky*.

Znovu zdůrazněme, že nemá smysl říct, že výrok α je pravdivý (či nepravdivý), neboť bez interpretace jeho speciálních (funkčních a predikátových) symbolů nemá výrok α "smysl".

Tedy výrok α může být *pravdivý v* interpretační struktuře I_1 – v modelu výroku α, nepravdivý ve struktuře I_2.

Formule je *tautologie (logicky pravdivá),* je-li pravdivá v každé interpretační struktuře (při každé interpretaci).

Výrok φ je *dokazatelný z* výroků (axiómů) $\alpha_1,...,\alpha_n$, (značíme $\alpha_1,...,\alpha_n \vdash \varphi$), je-li posledním krokem *důkazu,* což je posloupnost formulí taková, že každý krok této posloupnosti je buď některý z axiomů $\alpha_1,...,\alpha_n$, nebo vznikl z předchozích kroků (formulí) aplikací některého z odvozovacích pravidel daného systému.

Má-li být kalkul "smysluplný", musí být důkaz *korektní (sémanticky bezesporný)*, tj. "zachovávat pravdivost": **Jestliže $\alpha_1,...,\alpha_n \vdash \varphi$, pak $\alpha_1,...,\alpha_n \models \varphi$**, tedy výrok φ je pravdivý v každém modelu množiny $\{\alpha_1,...,\alpha_n\}$.

Proto, jestliže chceme dokazovat tautologie, musí být všechny (tzv. logické) axiómy daného kalkulu *tautologie*; pak tyto logické axiómy (jako předpoklady důkazu) nevyznačujeme: **Jestliže $\vdash \varphi$, pak $\models \varphi$**.

V r. 1928 publikovali Hilbert a Ackermann práci *Grundlazüge der theoretischen Logik.* V ní dospěli k formulaci korektního logického kalkulu predikátového počtu 1. řádu s logickými axiómy a pravidly jen mírně odlišnými od těch, které jsme uvedli v kapitole 3.4. (tedy 5 axiómů a 2 pravidla: *modus ponens* a *generalizace*) a položili základní otázku – *problém úplnosti* takto definovaného *logického kalkulu*:

Jsou dokazatelné všechny tautologie PL^1?

Obsah disertace Kurta Gödela (publikované v r. 1930) dává positivní odpověď na tuto otázku:

Věta 4.2.1. /Gödelova věta o úplnosti PL^1/:
Predikátový počet 1. řádu (s axiómy a pravidly uvedenými v 3.4.1 nebo jinými korektními a vhodnými) je úplný logický kalkul, tj. dokazatelné jsou v něm právě všechny tautologie PL^1. Dokazatelnost je v PL^1 ekvivalentní logické pravdivosti: **$\models \varphi$ právě když $\vdash \varphi$**.

Větu lze ještě zesílit:

Silná Gödelova věta o úplnosti PL^1: Výrok φ je v kalkulu PL^1 dokazatelný ze speciálních axiomů $\alpha_1,...,\alpha_n$ dané teorie (tedy nejen z logických axiómů – tautologií) právě když φ z těchto axiomů logicky vyplývá (je pravdivý v každém modelu teorie):

$\alpha_1,...,\alpha_n \vdash \varphi$, právě když $\alpha_1,...,\alpha_n \models \varphi$.

Důkaz zde nemůžeme podrobně probrat (svou technickou náročností je mimo rámec tohoto učebního textu), proto jej pouze naznačíme. Poznamenejme, že dnes je běžný jiný důkaz než ten, který podal Gödel ve své disertaci. Základní myšlenka je však stejná

v originálním důkaze i v důkazech pozdějších. K jejímu vyslovení potřebujeme ještě několik nových pojmů a vět:

Definice 4.2.1:

Teorie T ***je*** *(syntakticky)* ***bezesporná (konzistentní)***, jestliže pro žádnou uzavřenou formuli A jazyka teorie neplatí současně |– A i |– ¬A, tj. formule A a ¬A nemohou být současně dokazatelné (dokazatelná je nejvýše jedna z těchto formulí).

Poznámky 4.2.1:

1. Požadavek uzavřenosti formule má následující význam. Uzavřená formule (bez volných předmětových proměnných) vypovídá pouze o vlastnostech objektů representovaných primitivními pojmy teorie, kdežto otevřená formule (s aspoň jednou volnou předmětovou proměnnou) vypovídá i o vlastnostech konkrétních předmětů. Tak např. uzavřená formule $\forall x \forall y\ [x+y = y+x]$ vypovídá pouze o vlastnostech funkcí representovaných primitivními symboly "+" a "=", kdežto otevřená formule $x+y = 6$ vypovídá i o vlastnostech předmětů x,y (definuje konkrétní množinu dvojic (x,y) splňující daný vztah). Formule $x+y = 6$ a $\neg(x+y = 6)$ definují různé množiny dvojic.
2. Bezespornost teorie nelze zaměňovat se zákonem sporu. Zákon sporu, tj. formule $\neg(A \wedge \neg A)$ je součástí teorie, kdežto bezespornost je vlastnost teorie. Ve sporné teorii, jak hned ukážeme, lze dokázat každou formuli a tedy speciálně i zákon sporu. Na druhé straně lze konstruovat bezesporné teorie ve kterých zákon sporu neplatí.

Věta 4.2.2:

Teorie je bezesporná právě tehdy, existuje-li aspoň jedna formule, kterou nelze z teorie odvodit (tj. která do teorie nepatří).

Důkaz:

1. Je-li teorie bezesporná, pak v ní nelze současně odvodit formule A, ¬A. Tedy existuje aspoň jedna formule, kterou nelze v teorii odvodit.
2. Je-li teorie sporná, pak v ní lze odvodit formule A, ¬A. Vzhledem k zákonu výrokové logiky $A \supset (\neg A \supset B)$, neboli $A,\neg A \vdash B$, lze pak v teorii odvodit libovolnou formuli B.

Poznámka 4.2.2:

Sporná teorie je naprosto jalová, bezespornost teorie je samozřejmým požadavkem. Bezespornost teorie je tedy velmi slabá vlastnost.

Definice 4.2.2:

Axióm A_i ***je nezávislý na axiómech***

$A_1,...,A_{i-1},A_{i+1},...,A_n$ (*)

jestliže A_i nelze na základě těchto axiómů dokázat.

Systém axiómů $A_1,A_2,...,A_n$ ***je nezávislý***, jestliže každý z nich je nezávislý na zbytku ostatních.

Věta 4.2.3:

Ke každému konečnému systému axiómů existuje nezávislý systém axiómů ekvivalentní s původním systémem.

Důkaz:

Vyloučením závislého axiómu ze systému axiómů vznikne ekvivalentní systém. Vzhledem ke konečnému počtu axiómů musí být proces eliminace závislých axiómů po konečném počtu kroků ukončen.

Věta 4.2.4:

Axióm A_i je nezávislý na axiómech (∗) právě tehdy, je-li teorie

$$A_1,...,A_{i-1},\neg A_i,A_{i+1},...,A_n \qquad (**)$$

bezesporná.

Důkaz:

1. Je-li teorie (∗∗) sporná, pak lze z (∗∗) odvodit jakoukoliv formuli a tedy i A_i. Platí-li však
$$A_1 \wedge ... \wedge A_{i-1} \wedge \neg A_i \wedge A_{i+1} \wedge ... \wedge A_n \supset A_i$$
pak platí také
$$A_1 \wedge ... \wedge A_{i-1} \wedge A_{i+1} \wedge ... \wedge A_n \supset A_i$$
což vyplývá ze zákona výrokové logiky $(P \wedge \neg Q \wedge R \supset Q) \supset (P \wedge R \supset Q)$. Je-li tedy teorie (∗∗) sporná, pak axióm A_i je závislý na axiómech (∗).
2. Je-li axióm A_i závislý na axiómech (∗), pak lze z (∗∗) odvodit A_i i $\neg A_i$ a teorie (∗∗) je sporná.

Příklady 4.2.1:

Uvažujme teorii hustého lineárního uspořádání zleva i zprava neomezené množiny, tj. teorii danou axiómy V1-V6 (příklad 4.1.1). Zde např. platí:

- Axióm V4 je nezávislý na zbylých axiómech. Nahradíme-li axióm V4 jeho negací, tj. formulí $\neg\forall x\exists y\ [x<y]$, vznikne bezesporná teorie. Jejím modelem může např. být přirozené uspořádání reálných čísel z intervalu (-∞, a>, kde a je nějaké reálné číslo.
- Podobně axióm V5 je nezávislý na zbylých axiómech.
- Podobně axióm V6 je nezávislý na zbylých axiómech. Nahradíme-li jej jeho negací, vznikne bezesporná teorie jejíž modelem může být např. přirozené uspořádání celých čísel.

Definice 4.2.3:

Teorie T ***je úplná***, jestliže pro každou uzavřenou formuli A jazyka teorie platí buď |– A nebo |– ¬A, tj. ze dvou formulí A, ¬A je vždy aspoň jedna dokazatelná.

Je-li teorie T navíc bezesporná (což zpravidla mlčky předpokládáme), pak ze dvou formulí A, ¬A této teorie je vždy dokazatelná právě jedna.

Poznámky 4.2.4:

1. **POZOR:** Právě definovanou **úplnost teorie** /definice 4.2.3/ nelze zaměňovat se (*sémantickou*) ***úplností*** **logického kalkulu** zavedenou v kapitolách 2. a 3. a formulovanou v Gödelových větách o úplnosti!
2. O požadavku uzavřenosti formule viz poznámku k definici 4.2.1.
3. Úplnost teorie nelze zaměňovat se zákonem vyloučeného třetího. Zákon vyloučeného třetího, tj. formule $A \vee \neg A$ je součástí teorie, kdežto úplnost je vlastnost teorie. Zákon vyloučeného třetího je jakožto tautologie dokazatelný i v neúplných teoriích.

4. V neúplné teorii existují dobře formulované otázky (reprezentované formulemi jazyka teorie), na které teorie nedává odpověď (formuli ani její negaci nelze dokázat). V úplné teorii existuje odpověď na každou smysluplnou otázku (tj. pro každou formuli jazyka teorie platí, že je dokazatelná tato formule nebo její negace).
5. Úplnost teorie není žádoucí, chceme-li studovat obecné rysy některých pojmů, které se v různých předmětných oblastech projevují značně odlišně (např. společné rysy pojmu uspořádání, které je někdy úplné jindy neúplné, někdy se týká konečných množin, jindy nekonečných, někdy je husté, jindy není, atd.). Chceme-li však vyčerpávajícím způsobem popsat určitou jedinečnou předmětnou oblast (např. aritmetiku přirozených nebo reálných čísel), pak je naopak ideálem úplná teorie. Bohužel Gödelovy věty o neúplnosti (viz dále) dokazují, že tento ideál nelze v případě aritmetiky naplnit.

Příklady 4.2.2:

- Úplnými teoriemi jsou např.:
  - Teorie uspořádání V1-V6 /viz příklad 4.1.1/
- Neúplnými teoriemi jsou např.:
  - Teorie uspořádání V1-Vk, kde k=2,3,4,5
- Teorie V1-V3 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V4 /např. přirozené uspořádání celých čísel/ a v druhém jeho negace /např. přirozené uspořádání všech záporných celých čísel/.
- Teorie V1-V4 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V5 /např. přirozené uspořádání celých čísel/ a v druhém jeho negace /např. přirozené uspořádání všech přirozených čísel/.
- Teorie V1-V5 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V6 /např. přirozené uspořádání racionálních čísel/ a v druhém jeho negace /např. přirozené uspořádání všech celých čísel/.

Věta 4.2.5:

Každá bezesporná teorie T má alespoň jeden model.

Náznak důkazu silné věty o úplnosti (viz 4.2.1):

Z věty 4.2.5 již lehce plyne silná věta o úplnosti: Když teorie T nedokazuje nějakou formuli φ (φ je uzavřená), pak teorie $T \cup \{\neg\varphi\}$ je bezesporná a tedy má model M. To je však model teorie T, ve kterém není pravdivá formule φ. "Zformalizujeme-li" tuto úvahu, je důkaz zřejmý: Jestliže není pravda, že $T \vdash \varphi$, pak není pravda, že $T \models \varphi$, což je ekvivalentní s: Jestliže $T \models \varphi$, pak $T \vdash \varphi$.

Náznak důkazu věty 4.2.5: Potřebujeme ještě pojem ***Henkinovské úplnosti*:**
Teorie T je Henkinovská, jestliže pro každou uzavřenou formuli tvaru $\exists x\ \varphi(x)$ existuje konstanta c taková, že T dokazuje formuli $\exists x\ \varphi(x) \supset \varphi(c)$.
(Připomeňme, že tato formule pochopitelně není tautologie – srovnej se Skolemizací, kap. 3.2.1. Konstanta c se nazývá *svědek* pro formuli $\varphi(x)$.)

Lze ukázat, že ke každé bezesporné teorii T existuje silnější (ve smyslu definice 4.1.2) bezesporná T', která je Henkinovská a úplná. K teorii T' se už snadno sestrojí model. Za množinu M (universum – srovnej s Herbrandovým universem) vezmeme množinu všech konstant této teorie. Předpokládejme pro jednoduchost, že T má jediný binární predikát P. Jeho interpretací bude relace $R \subseteq M \times M$ taková, že $\langle c,d\rangle \in R$ právě když T' dokazuje formuli $P(c,d)$. Tím máme strukturu $\langle M, R\rangle$, která je modelem T', a tedy

i teorie T. (K ověření skutečnosti, že tato struktura je modelem T' je ovšem nutný fakt, že T' je Henkinovsky úplná.)

Hilbert očekával větu o úplnosti. Gödelův výsledek z r. 1930 byl velmi cenný, ale nebyl vlastně překvapením. Hilbert však očekával ve svém programu "formalizace aritmetiky" ještě daleko více. Především očekával, že se podaří ukázat, že predikátový počet 1. řádu je *rozhodnutelný* v tom smyslu, že se podaří najít algoritmus, který o každé formuli rozhodne (tedy v konečném počtu kroků odpoví ano či ne na otázku), zda je daná formule tautologie. Dále očekával, že se podaří nalézt "přirozenou" úplnou teorii, která bude plně charakterizovat aritmetiku, tedy bude dokazovat všechny pravdivé výroky o přirozených číslech. Gödelovy věty o neúplnosti (publikované v roce 1931) ukazují, že tato očekávání jsou nesplnitelná. A to byl ve své době zcela nečekaný výsledek, který změnil zásadním způsobem "tvář moderní matematické logiky". Abychom tyto neformální úvahy formulovali přesně, potřebujeme ještě několik definic:

Definice 4.2.4:

Teorie je rozhodnutelná, jestliže existuje algoritmus, který o každé formuli φ jazyka teorie rozhodne (v konečném počtu kroků), zda φ je platným výrokem teorie T (dokazatelnou formulí v T – patřící do teorie) či nikoliv.

Pozn.: Zde předpokládáme, že pojem algoritmu je dostatečně přesně určen (např. pomocí Turingova stroje).

Příklady 4.2.3:

- Rozhodnutelnými teoriemi jsou např.:
  - Výroková logika
  - Teorie uspořádání V1-V6
- Nerozhodnutelnými teoriemi jsou např. (jak za chvíli ukážeme):
  - Predikátová logika
  - Formální aritmetika

Nyní budeme zkoumat teorie, které mají za svůj model následující strukturu **N**, která je jednou ze základních matematických struktur. Tedy teď nebudeme hledat společné rysy v různých "situacích", ale budeme se snažit plně charakterizovat – axiomatizovat jednu předmětnou oblast, tj. množinu přirozených čísel spolu s přirozenými operacemi sčítání, násobení a relací uspořádání. (Funkce, relace, atd. na množině přirozených čísel budeme značit tučně, abychom je odlišili od příslušných symbolů jazyka teorie, kterým jsou tyto funkce, relace, atd. přiřazeny v zamýšlené interpretaci.)

N = <N, **0, S, +, ., =, ≤**>

kde N bude universum diskursu – množina přirozených čísel 0, 1, 2, ...
0 je číslo nula
S je unární funkce z N do N – operace *následník*
+ je binární funkce sčítání přirozených čísel
. je binární funkce násobení přirozených čísel
= je binární relace rovnosti
≤ je binární relace "menší nebo roven"

Abychom mohli tuto strukturu popisovat jazykem teorie PL^1, musí tento jazyk obsahovat symboly odpovídající výše uvedeným funkcím a relacím. Budeme je pro přehlednost značit stejně, jen ne tučně.

Nyní nás nebudou zajímat tautologie, tj. výroky pravdivé v *každé* interpretaci našeho jazyka, ale výroky pravdivé v jedné *standardní* interpretaci, tj. ve struktuře **N** přirozených čísel. Budeme studovat teorie, které mají **N** za svůj model a umožňují dokázat (pokud možno všechny "rozumné") výroky o přirozených číslech. Tedy nyní se záměry a postup axiomatizace poněkud liší např. od případu axiomatických algebraických teorií. Nebudeme hledat společné rysy různých "situací", ale budeme zkoumat jednu "situaci" – aritmetiku přirozených čísel. V takovém případě postupujeme tak, že si všímáme toho, jak provádíme jednotlivé důkazy neformálně, či intuitivně, především pak toho, kterou minimální množinu předpokladů potřebujeme nutně a vždy. Tyto společné předpoklady pak formulujeme jako množinu (speciálních) axiomů. Uvedeme jako příklad dvě takové teorie, a to Robinsonovu aritmetiku Q a Peanovu aritmetiku PA.

Příklad 4.2.4 / ***Robinsonova aritmetika Q*** a ***Peanova aritmetika PA*** **/:**

Robinsonova aritmetika je teorie o následujících sedmi axiómech (které jsou generální uzávěry následujících formulí):

Q_1 $\neg\, S(x) = 0$ neboli $S(x) \neq 0$
Q_2 $S(x) = S(y) \supset x = y$
Q_3 $x + 0 = x$
Q_4 $x + S(y) = S(x + y)$
Q_5 $x \,.\, 0 = 0$
Q_6 $x \,.\, S(y) = (x \,.\, y) + x$
Q_7 $x \leq y \equiv \exists z\, (z + x = y)$

Tyto axiómy popisují základní vlastnosti aritmetických operací. Přidáme-li k nim schéma *axiómů indukce (Ind)*, dostaneme Peanovu aritmetiku PA:

Ind $\{\varphi(0) \wedge \forall x\, [\varphi(x) \supset \varphi(S(x))]\} \supset \forall x\, \varphi(x)$

Pozn.: Všimněme si, že Q je konečně axiomatizovaná teorie (má konečný počet axiómů), PA však ne, neboť jsme přidali schéma axiómů indukce.

Zřejmě jsou všechny axiómy teorie PA (a tedy i Q) pravdivé ve struktuře **N**. Tedy je tato struktura modelem obou teorií. Říkáme mu *standardní model aritmetiky*. Každé přirozené číslo $n \in N$ má své "jméno" v jazyce aritmetiky, totiž term S(S...(S(0)...)) označovaný jako $\underline{n}$ a zvaný *n*-tý *numerál.* Tedy např. číslo 1 je přiřazeno termu S(0), číslo 2 termu S(S(0)), atd. Teorie Q je dosti slabá, PA je hodně silná a dokazuje spoustu známých tvrzení o přirozených číslech.

Některé jednoduché věty a jejich důkazy (metodou přirozené dedukce)

Ukažme si dvě jednoduchá použití axiomu indukce.

$\vdash \forall x\, (0 + x = x)$

Nejprve označíme $\varphi(x)$ formuli $0 + x = x$.
Nechť $0 + x = x$. Pak $S(0 + x) = S(x)$ /Def. 3.4.2 ax. R2/
$S(0 + x) = 0 + S(x)$ axiom Q_4
$0 + S(x) = S(x)$ /transitivita a komutativita identity/
$\forall x\, [(0 + x = x) \supset 0 + S(x) = S(x)]$ ZI, Z∀
Tedy jsme v Q dokázali výrok $\forall x\, [\varphi(x) \supset \varphi(S(x))]$
Výrok $\varphi(0)$, tj. $0 + 0 = 0$, je snadno dokazatelný dle axiomu Q_3.
V axiomu Ind máme tedy dokazatelné obě premisy.

To znamená, že PA |– $\forall x\ (0 + x = x)$

To není triviální výsledek, protože zatím nevíme, zda z axiomů Robinsonovy nebo Peanovy aritmetiky plyne komutativita sčítání. Dokážeme nyní asociativitu sčítání.

|– $\forall(x,y,z)\ [(z + y) + x = z + (y + x)]$

Označíme $\varphi(x,y,z)$ formuli $(z + y) + x = z + (y + x)$.
Nechť y a z jsou dána. Axiom Q_3 dává $\varphi(0,y,z)$.
Nechť dále x je dáno a nechť $(z + y) + x = z + (y + x)$.
Pak $S((z + y) + x) = S(z + (y + x))$.
Užijeme axiom Q_4 jednou na levou stranu a dvakrát na pravou stranu:
$S((z + y) + x) = (z + y) + S(x)$
$S(z + (y + x)) = z + S(y + x) = z + (y + S(x))$
Dohromady: $(z + y) + S(x) = z + (y + S(x))$
Ověřili jsme, že $\forall x\ (\ \varphi(x,y,z) \supset \varphi(S(x),y,z)\ )$.
Tedy dle axiomu Ind máme $\forall x\ \varphi(x,y,z)$.
Protože čísla y a z byla libovolná, máme $\forall(x,y,z)\ \varphi(x,y,z)$.

Následující teorémy – *vlastnosti aritmetických operací* jsou dokazatelné v PA (teorémy jsou generální uzávěry formulí):

$(z + y) + x = z + (y + x)$	$(z \,.\, y) \,.\, x = z \,.\, (y \,.\, x)$
$0 + x = x$	$z \,.\, (y + x) = z \,.\, y + z \,.\, x$
$S(y) + x = S(y + x)$	$\neg(x = S(x))$
$y + x = x + y$	$y + x = z + x \supset y = z$
$0 \,.\, x = 0$	$(x + y = 0) \supset (x = 0 \wedge y = 0)$
$S(y) \,.\, x = y \,.\, x + x$	$(x \,.\, y = 0) \supset (x = 0 \vee y = 0)$
$y \,.\, x = x \,.\, y$	$\exists u\ (u + x = y \vee u + y = x)$

Dále uvedeme explicitní definice některých ***neprimitivních*** (odvozených, složených) pojmů pomocí pojmů primitivních.

Predikátové symboly:

- $x \neq y \Leftrightarrow_{df} \neg(x=y)$ binární predik. symbol
- $x<y \Leftrightarrow_{df} \exists z\ [x+ S(z) = y]$ binární predik. symbol
- $x>y \Leftrightarrow_{df} y<x$ binární predik. symbol
- $x<y<z \Leftrightarrow_{df} x<y \wedge y<z$ ternární predik. symbol ($<(x,y,z)$)
- $x|y \Leftrightarrow_{df} \exists z\ [y = z.x]$ binární predik. symbol ("x dělí y")
- $sd(x,y,z) \Leftrightarrow_{df} x|y \wedge x|z$ ternární predik.symbol
  ("x je společným dělitelem y,z")
- $prv(x) \Leftrightarrow_{df} (x>1) \wedge \neg\exists y\ [y\neq 1 \wedge y\neq x \wedge y|x]$
  unární predik. symbol
  ("x je prvočíslo")

Funkční symboly:

- $1 =_{df} S(0),\ 2 =_{df} S(S(0)),\ 3 =_{df} S(S(S(0))),\ ...$
  nulární funkční symboly (předmětové konstanty)
- $y = x^2 \Leftrightarrow_{df} y = x.x$ unární funkční symbol (druhá mocnina)

- $y = x^3 \Leftrightarrow_{df} \exists z\,[z = x^2 \wedge y = z.x]$ unární funkční symbol (třetí mocnina)
- $x = \mathrm{nsd}(y,z) \Leftrightarrow_{df} \mathrm{sd}(x,y,z) \wedge \forall t\,[\mathrm{sd}(t,y,z) \supset t \le x]$
  binární funkční symbol ("x je nejv. společný dělitel čísel y,z")

Vlastnosti relace < (opět generální uzávěry):

$x < y \wedge y < z \supset x < z$
$x < y \vee x = y \vee y < x$
$\neg(x < x)$

Vztah relací ≤ a < k sobě navzájem a k operacím:

$x \le y \equiv x < y \vee x = y$
$x < y \supset x + z < y + z$
$x < S(y) \equiv x < y \vee x = y$
$x < y \wedge z \neq 0 \supset x \,.\, z < y \,.\, z$

*Některé další teorémy aritmetiky přirozených čísel***:**

- $\vdash x \neq 0 \supset \exists q \exists r\,[y = x.q+r \wedge r<x]$
  existence celočíselného podílu a zbytku
- $\vdash y = x.q_1+r_1 \wedge r_1<x \wedge y = x.q_2+r_1 \wedge r_2<x \supset q_1=q_2 \wedge r_1=r_2$
  jednoznačnost celočíselného podílu a zbytku
- $\vdash x \neq 0 \supset (\exists_1 q)(\exists_1 r)[y = x.q+r \wedge r<x]$
  existence a jednoznačnost celočíselného podílu a zbytku
- $\vdash \forall x \exists y\,[y>x \wedge \mathrm{prv}(y)]$
  Euklidova věta: ke každému číslu exist. prvočíslo, které je větší než dané číslo ⇒ prvočísel je nekonečně mnoho.
- $\vdash n>2 \supset \neg(\exists x,y,z)\,[(S(x))^n + (S(y))^n = (S(z))^n]$
  Fermatova věta – byla dokázána.

V PA tedy lze dokázat, že operace s přirozenými čísly mají očekávané vlastnosti: sčítaní a násobení jsou asociativní a komutativní operace, násobení je distributivní vůči sčítání, relace ≤ a < jsou skutečně neostré a ostré uspořádání, nula je nejmenší přirozené číslo, největší přirozené číslo neexistuje, číslo S(x) je vždy nejmenší mezi čísly většími než x, atd.

Teorie Q je dosti slabá, neboť při důkazu mnohých všeobecných aritmetických tvrzení potřebujeme právě axiomy indukce. PA je již hodně silná teorie a dokazuje spoustu známých tvrzení o přirozených číslech. PA však není úplná teorie: Existuje výrok φ, který je pravdivý v **N**, avšak není dokazatelný v PA (a pochopitelně ani ¬φ není dokazatelný v PA, neboť ¬φ není pravdivý v **N** a PA je korektní).

Ještě jednou shrneme: Co to znamená, že teorie T je neúplná? Jelikož je každá formule φ v dané zamýšlené interpretaci (v našem případě **N**) pravdivá či nepravdivá, přáli bychom si, aby naše teorie dokazovala jednu z φ či ¬φ (tu pravdivou – T je korektní). Tedy neúplná teorie "dokazuje málo". Na druhé straně může "mít příliš mnoho modelů" v tom smyslu, že dokazuje formule takové, které jsou sice pravdivé v **N**, ale jsou pravdivé i v jiných interpretacích našich axiomů, třeba i značně odlišných od té zamýšlené (tedy neizomorfních s **N**), neboť dle věty o úplnosti kalkulu musí dokazovat všechny formule vyplývající z axiomů. Tedy množina axiomů je nedostatečná, slabá. Mohli bychom říct: Dobrá, tak nějaké axiomy (konzistentně) přidáme tak, abychom charakterizovali přirozená

čísla úplně, vyčerpávajícím způsobem. To by sice bylo možné, ovšem pak bychom nedosáhli toho, aby teorie byla "rozumná" v tom smyslu, že vždy poznáme, zda daná formule je či není axiomem (rekurzivně axiomatizovaná teorie). Následující věta ukazuje, že v případě aritmetiky nelze splnit oba požadavky – úplnost a rekurzivitu. Neúplnost není specielní vlastnost teorie PA.

Definice 4.2.5:

Teorie je rekurzivně axiomatizovaná, jestliže existuje algoritmus, který o každé formuli φ jazyka teorie rozhodne (v konečném počtu kroků), zda φ je či není axiomem teorie.

Věta 4.2.6 /První Gödelova věta o neúplnosti/:

Nechť T je teorie, obsahující Q (tj. jazyk teorie T obsahuje jazyk aritmetiky a T dokazuje všechny axiomy teorie Q). Nechť T je rekurzivně axiomatizovaná a nechť **N** je jejím modelem. Pak T je neúplná teorie.

Pozn.: Podle pozdějších výsledků lze předpoklad, že **N** je modelem teorie T nahradit slabším předpokladem, že T je bezesporná (*Rosserova věta*).

Upřesnili jsme tedy, co je to "přirozená" nebo "rozumná" teorie, v níž by byly dokazatelné všechny pravdivé výroky o přirozených číslech. Rozumná je jistě jen taková teorie, která je bezesporná (jinak bychom v ní dokázali vše). A k přirozenosti zajisté patří to, že jsme schopni rozpoznat, zda daná formule je či není axiomem, tedy že je ***rekurzivně axiomatizovatelná***, jinak bychom v té teorii nemohli dokazovat nic. Ale žádná taková teorie neexistuje podle věty 4.2.6.

V dalším naznačíme jednotlivé kroky důkazu Gödelovy věty o neúplnosti. Především poznamenejme, že Gödelův důkaz byl inspirován známým Epimenidovým paradoxem lháře: Věta, která říká "já jsem nepravdivá", není ani pravdivá ani nepravdivá. Nemá totiž vůbec žádný smysl (stejně jako věta "já jsem pravdivá"). Ovšem zatímco Epimenidovu "větu" nelze v jazyce aritmetiky vůbec zapsat, v Gödelově důkazu není vůbec žádný paradox a formule g, kterou nalezl Gödel, je dobře utvořená, lze ji zapsat a ukázat o ní, že je pravdivá v **N**, ale nedokazatelná z teorie T. Navíc, Gödelův důkaz je konstruktivní, tedy Gödel příslušnou formuli opravdu zkonstruoval. V roce 1989 publikoval Boolos nový důkaz, který je snad jednodušší, ale není konstruktivní, je to důkaz sporem. Boolův důkaz je inspirován jiným známým paradoxem, a to Berryho paradoxem (*Nejmenší celé číslo nepojmenovatelné méně než dvaceti sedmi slabikami* – spor, právě jsme takové číslo pojmenovali dvaceti šesti slabikami). My zde vyložíme hlavní ideje původního Gödelova důkazu.

Nejprve musíme aritmetizovat syntaxi aritmetiky. Formule jazyka aritmetiky jsou jisté posloupnosti znaků, důkazy jsou jisté posloupnosti formulí. Lze definovat jednoduché *očíslování* všech formulí a důkazů (v dané teorii T), tj. funkci gn (Gödel number) přiřazující každé formuli φ a každému důkazu d v teorii T číslo gn(φ) a gn(d), a to jedno-jednoznačně (různé vzory mají různé obrazy). Kromě toho je funkce gn efektivní v tom smyslu, že existuje algoritmus, který ji počítá, a také algoritmus, který ke gn(*x*) počítá jeho vzor *x*.

Další potřebný pojem je Σ-*úplnost teorie* Q. Dokazujeme, že Q a žádná rozumná silnější teorie není úplná. Na druhé straně však existuje třída formulí (Σ-formule – jsou v úzkém vztahu k algoritmům) takových, že každý Σ-výrok pravdivý v **N** je dokazatelný

v Q. Přitom z rekurzivní axiomatizovanosti teorie T plyne, že množina Gödelových čísel formulí dokazatelných v T je definovatelná v N jistou Σ-formulí, kterou označíme Dok(x). Tedy: Teorie T dokazuje φ právě když Dok(gn(φ)) je pravdivé v **N**. (gn(φ) je numerál, jehož významem je Gödelovo číslo formule φ.)

Třetí ingrediencí je *Gödelovo diagonální lemma.* Pro každou formuli φ(x) jazyka aritmetiky existuje uzavřená formule ψ taková, že v Q je dokazatelná formule ψ ≡ φ (gn(ψ)). Tedy gn(ψ) je jméno Gödelova čísla formule ψ a formule φ (gn(ψ)) "říká", že toto číslo má vlastnost φ. Navíc je tato formule ekvivalentní s ψ, a to dokazatelně v Q. Tedy ψ "říká" – "já mám vlastnost φ".

Zbývá poslední nápad: Aplikovat diagonální lemma na formuli ¬Dok(x). Dostaneme *Gödelovu diagonální formuli*, označme ji g, takovou, že Q dokazuje formuli g ≡ ¬Dok (gn(g)). Tedy g "říká" – "já jsem nedokazatelná". Zde je ona podobnost s Epimenidovým paradoxem. Avšak ještě jednou: Zde není žádný paradox. Gödelova formule má smysl, lze ji zkonstruovat a lze ukázat, že je pravdivá v **N**, ale nedokazatelná v T (pochopitelně ani její negace nemůže být dokazatelná).

Kdyby teorie T dokazovala g, pak by formule Dok (gn(g)) byla pravdivá v **N** a tato formule je Σ-formule; tedy by ji Q (a tím spíše T) dokazovalo, tj. T by dokazovalo ¬g, což je spor. Avšak teorie T je bezesporná, tedy nedokazuje g, tedy ¬Dok (gn(g)) je pravdivá v **N**, tedy g je pravdivá v **N**.

(Když vše ještě jednou shrneme s trochou metafory: g "říká" – "já jsem nedokazatelná", a to je pravda, protože kdyby byla dokazatelná, pak by byla nepravdivá a teorie T by dokazovala nepravdivou formuli, což není možné, protože T je bezesporná.) Pro každou rozumnou aritmetiku T najdeme výrok g, který je pravdivý v **N**, ale nedokazatelný z T.

Důsledky:

Jelikož platí silná Gödelova věta o úplnosti (viz 4.2.1), nemůže Gödelova formule g logicky vyplývat z teorie T (neboť kdyby T |= g, pak by T |– g), a tedy ani z PA. Tedy tato formule *není pravdivá v každém modelu* PA. Jelikož je pravdivá ve standardním modelu **N**, musí existovat nestandardní modely PA, a to takové, které nejsou isomorfní s **N**. (Připomeňme, že isomorfní modely jsou takové struktury, které se liší pouze přejmenováním, jinak se "chovají" stejně.)

Každá "rozumná" aritmetika T (tj. ***rekursivně axiomatizovatelná***, obsahující Q a má model **N**) je ***nerozhodnutelná*** (neexistuje algoritmus, který by pro každou formuli rozhodl, zda je či není dokazatelná v T)**.** Kdybychom měli takovou rozhodnutelnou teorii T, mohli bychom ji pomocí "rozhodovacího algoritmu" rozšířit na úplnou. To je však nemožné podle Rosserova vylepšení Gödelovy věty o neúplnosti.

Predikátový počet 1. řádu je teorie PL^1 s prázdnou množinou speciálních axiomů. Proto je PL^1 *nerozhodnutelný.* Neexistuje algoritmus, který by rozhodoval, zda je daná formule φ v PL^1 dokazatelná (a tedy tautologie). Je tomu tak proto, že Q je konečně axiomatizovaná: Jsou-li $Q_1,\ldots,Q_7$ její axiomy, pak je podle věty o dedukci rozhodnutí, zda φ je dokazatelná v Q ekvivalentní rozhodnutí, zda je formule $Q_1 \wedge Q_2 \wedge \ldots \wedge Q_7 \supset \varphi$ dokazatelná v PL^1.

Tedy **problém logické pravdivosti je v PL^1 nerozhodnutelný.**

Situace však není tak beznadějná (vždyť funguje rezoluční metoda!). Church dokázal, že tento problém je **parciálně rozhodnutelný** v následujícím smyslu:

Existují algoritmy (např. rezoluční metoda) takové, že je-li předložená formule φ tautologie, pak algoritmus vydá v konečném počtu kroků odpověď ANO. Pokud však φ není tautologie, pak algoritmus buďto odpoví NE, nebo nemusí vydat nikdy *žádnou* odpověď (”cykluje”).

Definice 4.2.6:

Teorie je kategorická, jestliže každé dva její modely jsou izomorfní (tj. odhlédneme-li od různosti značení existuje jen ”jediný” model teorie).

Poznámky 4.2.5:

1. Formální aritmetika 1. řádu není kategorickou teorií. (Formální aritmetika 2. řádu je kategorická, avšak za cenu ***neúplnosti kalkulu PL2***.)
2. Existují i úplné teorie, které jsou nekategorické (např. teorie uspořádání).
3. Většina bezesporných teorií může mít modely o různé kardinalitě (s různou mohutností univerzální množiny). Tato skutečnost motivuje zavedení slabšího pojmu, tzv. α-kategoričnosti. ***Teorie je α-kategorická***, jestliže všechny její modely o kardinalitě α jsou izomorfní. Dá se ukázat, že formální aritmetika není v 1. řádu ani α-kategorická.

Příklady 4.2.4:

Příkladem nekategorické teorie je teorie uspořádání V1-V6. Ukážeme, že existují dva neizomorfní modely této teorie. Jedním modelem je přirozené uspořádání $<$ na množině reálných čísel. Druhým modelem je uspořádání $<<$ na množině reálných čísel definované takto (Q je zde množina racionálních čísel):

$$x<<y \Leftrightarrow_{df} [(x\in Q) \wedge (y\in Q) \wedge (x<y)] \vee [(x\in Q) \wedge (y\notin Q)] \vee [(x\notin Q) \wedge (y\notin Q) \wedge (x<y)].$$

V tomto uspořádání jsou všechna racionální čísla před všemi iracionálními čísly a v rámci každé skupiny platí přirozené uspořádání. V tomto uspořádání platí $20<<\sqrt{2}$, ačkoliv $\sqrt{2}<20$. Obě uspořádání (oba modely) splňují všechny axiómy V1-V6 a přitom nejsou izomorfní.

Zbývá pojednat o druhé Gödelově větě o neúplnosti.

Věta 4.2.7 /Druhá Gödelova věta o neúplnosti/: Žádná rozumná aritmetika T (splňující další rozumné podmínky, např. tedy Q, PA) nedokazuje svou vlastní bezespornost.

Důkaz (náznak): Uvnitř teorie T lze vyjádřit tvrzení o bezespornosti teorie pomocí predikátu Dok, např. výrokem $\neg Dok(\underline{gn}(\varphi)) \vee \neg Dok(\underline{gn}(\neg\varphi))$ pro nějakou uzavřenou formuli φ. Označme výrok vyjadřující bezespornost symbolem KON. Gödel si všiml, že za jistých dalších podmínek je formule KON ekvivalentní jeho diagonální formuli g, tj. T dokazuje KON ≡ g. Protože T nedokazuje g, nedokazuje ani KON.

Shrnutí: Důsledky obou Gödelových vět jsou známy. Především, naděje formalistů, že sémantická pravdivost bude redukovatelná na syntaktickou dokazatelnost, byly zmařeny na základě první věty. Jelikož tento výsledek se týká každé teorie dostatečně silné, aby obsahovala aritmetiku, týká se celé klasické matematiky. Druhá věta však byla ještě více destruktivní pro Hilbertův program: Nemožnost dokázat konzistenci klasické matematiky

absolutním finitním důkazem. Tedy matematika nemůže být redukována na mechanickou práci se symboly, na pouhou syntax. Sémantické pojmy jako **pravdivost, logické vyplývání** jsou v matematice základními nezastupitelnými pojmy.
(Kurt Gödel sám zastával Platonský pohled na filosofii matematiky. Tvrdil, že existují abstraktní entity jako množiny, třídy, funkce, atd., které jsou označovány matematickými symboly, tedy matematické symboly mají svůj význam. Navíc, jak tvrdil, "lidská mysl nemůže být stroj", tvořivá činnost matematika, matematické objevování, se neobejde bez jisté matematické intuice …)

LITERATURA

Sochor, A.: *Klasická matematická logika.* Karolinum Praha, 2001.
Švejdar, V.: *Logika, neúplnost a složitost.* Academia Praha, 2002.
Brown, J.R.: *Philosophy of Mathematics.* Routledge, 1999.
Hájek, P.: *Kurt Gödel, matematik a logik.* In: Malina, J., Novotný, J. (ed), Brno 1996.
Štěpán, J.: *Logika a logické systémy.* Votobia Olomouc, 1992.
Manna, Z.: *Matematická teorie programů.* SNTL Praha, 1981.
Markl, J.: *Matematická logika.* Sylaby VŠB Ostrava. 2001.