VŠB–Technická univerzita Ostrava

Logika pro informatiky

(a příbuzné obory)

učební text

Doc. RNDr. Marie Duží, CSc.

Ostrava 2012

Vydavatelství VŠB-TU Ostrava

Vydání této publikace je spolufinancováno
Evropským sociálním fondem a státním rozpočtem České republiky

Projekt ESF OPVK reg. č. CZ.1.07/2.2.00/07.0217
ORGANON – LMS pro výuku logiky

Název: Logika pro informatiky
Autor: Doc. RNDr. Marie Duží, CSc.
Vydání: první, 2012, ***errata 2014***
Počet stran: 183
Náklad: 250 ks
Vydavatel: Ediční středisko VŠB-TUO

Studijní materiály pro obor Informatika a výpočetní technika Fakulty elektrotechniky a informatiky.

Jazyková korektura: nebyla provedena

Vydavatelství VŠB-TU Ostrava – Ostrava 2012

ISBN 978-80-248-2662-2

Předmluva

Tato skripta pojednávají o logice a jsou určena studentům bakalářského i magisterského studia technických oborů jako informační technologie, komputační lingvistika, ale nejen jim. Mohou zde čerpat také studenti filosofických oborů a všech spřízněných disciplin. Předložený učební text vznikl na základě dlouhodobých zkušeností s výukou logiky na Katedře Informatiky Fakulty elektrotechniky a informatiky, VŠB-Technická univerzita Ostrava, a to v kursech *Úvod do logiky*, *Matematická logika*, *Matematické základy informatiky*, *Úvod do teoretické informatiky*, *Funkcionální a logické programování*.

Pokouším se představit logiku jako disciplínu, kterou potřebuje téměř každý. Proto úvodní kapitola nejprve pojednává o tom, co je to logika, kde a v čem nám může logika pomoci, a co je předmětem studia logiky.

Další kapitola je věnována snad nejsnadnějšímu logickému systému, a tím je výroková logika. Ovšem již zde ukazuji, že i ve výrokové logice můžeme najít zajímavé problémy, při jejichž řešení nám formální aparát pomůže. Ačkoliv je výroková logika rozhodnutelný systém, neboť možných interpretací je vždy konečně mnoho, a v podstatě sestavení tabulky pravdivostních hodnot jednotlivých formulí a kontrola této tabulky nám umožní dokázat vše, co potřebujeme, je takový důkaz pracný a často málo efektivní. Proto se již zde čtenář seznámí s různými důkazovými metodami, které jsou efektivnější a navíc je možno je snadno zobecnit pro systémy složitější, kde již tabulková metoda není použitelná, neboť možných interpretací jednotlivých formulí je nekonečně mnoho. Navíc, systém výrokové logiky je základem všech klasických logik a bez jeho znalosti pak nelze pochopit např. systém predikátové logiky.

Následující kapitola se zabývá výkladem predikátové logiky prvního řádu, tj. snad nejrozšířenějšího logického systému, který se dnes stal již téměř těsnopisem matematiky. Opět nejprve ukazuji, kde a jak nám formalizace v systému predikátové logiky pomáhá, ale zároveň poukazuji na meze tohoto systému. Velká pozornost je věnována sémantickému výkladu predikátové logiky, neboť bez důkladného porozumění tomu, co je to sémantiKa neboli význam formulí, může čtenář jen těžko porozumět dalšímu výkladu. Následuje zobecnění důkazových metod, jejichž základy jsme poznali při výkladu výrokové logiky, pro tento složitější systém. Jedná se především o obecnou rezoluční metodu, systém přirozené dedukce a důkazový kalkul Hilbertova typu.

Dá se tedy říct, že druhá a třetí kapitola představují klasické logické kalkuly. V následující závěrečné kapitole pak ukazuji, jak je možno v rámci těchto kalkulů budovat jednotlivé teorie určitých partikulárních problémů. Seznámíme se zde s teorií relací a funkcí, dále pak s některými algebraickými teoriemi a na závěr pak s teorií aritmetiky a s výsledky Kurta Gödela. Tato část je z celého výkladu nejobtížnější a bývá obsahem kursů pro pokročilé, přesto jsem se rozhodla ji zde zařadit, neboť pochopení možností a mezí automatického či mechanického dokazování je důležité zejména pro informatiky a programátory. Pro studenty filosofických oborů pak přinese zajímavé úvahy o filosofickém dopadu těchto velikých objevů.

Každá kapitola je doprovázena cvičeními tak, aby si čtenář mohl ihned ověřit, že vše dobře pochopil a získal potřebnou zručnost při řešení jednotlivých úloh.

Ostrava, 2012

Marie Duží

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 se lidé dokáží gramaticky správně 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 důkazových systémech a při vytváření teorií. Prvá část je věnována výrokové logice (logice 0-tého řádu), ve které primitivní formule (výrokové proměnné) 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) $V_1, \ldots, V_n$ *soudím*, že je pravdivý rovněž výrok V. Zapisujeme schematicky: $V_1, \ldots, V_n \ / \ V$ nebo častěji:

V_1
V_2
…
V_{n-1}
V_n
——— → předpoklady neboli ***premisy***

V → ***závěr***

V praxi používáme různé druhy takovýchto úsudků, ovšem ne všemi se zabývá logika. Např. se obecně nezabývá tzv. *Pravděpodobnostními* či *induktivními* 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*, tj. takovými, kde závěr z předpokladů logicky vyplývá. Proto definujeme:

Definice 1.1 (***deduktivně platný úsudek***):
Úsudek $P_1, \ldots, P_n \ / \ Z$ je deduktivně *platný (správný),* značíme $\boldsymbol{P_1, \ldots, P_n \models Z}$, jestliže závěr Z *analyticky vyplývá* z předpokladů $P_1, \ldots, P_n$, tj. za všech okolností takových, že jsou pravdivé všechny předpoklady $P_1, \ldots, P_n$, je (za těchto okolností) pravdivý i závěr Z.

Tedy jinými slovy: Za žádných okolností, nikdy se nemůže stát, aby byly všechny předpoklady $P_1, \ldots, P_n$ 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.
   Kdo není muž, je žena.
   _____
   Některé ženy nemá Xaver rád.

8) Žádné prvočíslo větší než 2 není sudé.
   Číslo 3 je prvočíslo větší než 2.
   _____
   Číslo 3 není sudé.

Správnost úsudku ověřujeme *bez empirického zkoumání* stavu světa, tedy pouze tzv. *analytickými* metodami, neboť správnost úsudku je dána pouze *logickou strukturou* premis a závěru. Jinými slovy, to, zda jsou předpoklady pravdivé či nikoliv musíme zjišťovat. Ať už empiricky zkoumáním toho, jaká fakta aktuálně platí, či v případě matematických úsudků např. tak, že si pravdivost předpokladů dokážeme nebo se poradíme s nějakou učebnicí matematiky. Avšak jakmile již víme, že jsou předpoklady pravdivé, nemusíme a zřejmě nebudeme stejným způsobem ověřovat pravdivost závěru, neboť ta je již zaručena pravdivostí všech předpokladů.

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*).

Tak např. následující úsudek je evidentně nesprávný:

Jan Švejnar kandiduje na prezidenta České republiky.
Prezident České republiky je manžel Livie Klausové.

Jan Švejnar kandiduje na manžela Livie Klausové.

Přijetím kandidatury na prezidenta jistě příslušný kandidát nepřijímá zároveň kandidaturu na manžela současného prezidenta. Avšak využili jsme zde pouze jeden z nejzákladnějších logických zákonů, a tím je Leibnizův zákon substituce identit. Jestliže je prezident ČR *identický* s manželem Livie Klausové, pak by dosazení druhého za první mělo být vždy platné. Avšak zde to nefunguje – paradox? Jistěže ne, pouze je nutno rozlišit *úřad* prezidenta ČR od té osoby, která jej náhodně zastává. Ovšem v běžných logických systémech predikátové logiky prvního řádu je právě takovéto rozlišení jistým problémem. Potřebujeme nějaký systém logiky vyšších řádů. Ovšem v těchto skriptech se budeme zabývat pouze predikátovou logikou prvního řádu. Silnější systémy, např. Transparentní intenzionální logika, jsou pak obsahem nadstavbových kursů pro pokročilé.

Uvedeme nyní příklady logických systémů podle jejich expresivní síly.

Výroková logika (VL) umožňuje analyzovat věty 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 výroky do úrovně vlastnosti vlastností, vlastnosti funkcí, atd.

Jedním z nejexpresivnějších logických systémů je tzv. ***Transparentní intenzionální 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. Zejména pak umožňuje rozlišovat tři úrovně abstrakce, a to úroveň *extenzionální* (na které jsou objektem predikace *hodnoty* funkcí, jakožto zobrazení), *intenzionální* (Kde objektem predikace jsou celé funkce) as *hyperintensionální* (kde objektem predikace je příslušná konstrukce funkce). TIL se nyní stává 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*, tvorby ontologií, komunikace v multi-agentních systémech, umělé inteligenci, atd. TIL je předmětem samostatného kursu *Inteligentní systémy* na katedře Informatiky FEI, VŠB-Technické university Ostrava, a také kursu Transparentní intenzionální logika na katedře logiky Filosofické fakulty University Karlovy, či na fakultě Informatiky MUNI Brno, a lze jej zájemcům vřele doporučit.

Vraťme se k výše uvedeným příkladům platných úsudků *ad* 1) až 8). Z těchto 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 však z Definice 1.1 plyne, že alespoň jedna z premis je 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, jehož premisy jsou 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 tvrzení 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 (anglicky *belief revision*).

3) ***Tranzitivita.***
Jestliže $P_1, \ldots, P_n \models Z$ a $Q1, \ldots, Q_m, Z \models Z'$, pak $P_1, \ldots, P_n, Q_1, \ldots, Q_m \models Z'$.

4) ***Reflexivita.*** Je-li tvrzení B rovno 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 byla všechna tvrzení $P_1, \ldots, P_n$ pravdivá. Značíme $P_1, \ldots, P_n \models$.
(Tedy z této množiny logicky vyplývá jakýkoli výrok, i nepravdivý, proto musí být vždy alespoň jedno P_i nepravdivé.)

***Příklady*:**
Analyticky pravdivé výroky:
$\models$ 1+1= 2
$\models$ V Praze prší nebo neprší.
Sporné výroky:
P_1: ”Jestliže A, pak B”. P_2: ”A a ne B”. $P_1, P_2 \models$ (kde A, B jsou libovolné výroky).

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

Nyní můžeme formulovat ještě jednu důležitou vlastnost deduktivních úsudků:

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

Příklad: 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 ≤ 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 důkazový postup zachovával 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 budeme zabývat kapitola 4. tohoto textu.

Cvičení ke kapitole 1.

Rozhodněte, které z následujících úsudků jsou platné.

a) Všechny myši jsou hranaté.
Všechno hranaté je modré.
_____
Všechny myši jsou modré.

b) Někteří psi rádi přednášejí básně.
Všichni psi jsou laviny.
_____
Některé laviny rády přednášejí básně.

c) Všichni žáci jsou ryby.
Někteří žáci jsou mloci.
_____
Někteří mloci jsou ryby.

d) Všechny žáby jsou modré.
Tento kůň je modrý.
_____
Tento kůň je žába.

e) Některé mraky mají černé puntíky.
Všechny domy mají černé puntíky.
_____
Některé mraky jsou domy.

f) Všechny ovce jsou sloni.
Někteří sloni jsou čápi.
_____
Všechny ovce jsou čápi.

g) Nikdo s červeným nosem nemůže být premiér.
Všichni muži mají červené nosy.
_____
Žádný muž nemůže být premiérem.

h) Všichni jezevci jsou sběratelé umění.
Někteří sběratelé umění žijí v norách.
_____
Někteří jezevci žijí v norách.

i) Nikdo s fialovými vlasy není mladý.
Někteří s fialovými vlasy pijí mléko.

Někteří, kteří pijí mléko, nejsou mladí.

j) Někdo má rád Alici, ale není šachista.
Všichni, kdo mají rádi Alici a Roberta, jsou šachisté.

Někdo má rád Alici, ale nemá rád Roberta.

Řešení: Pokud jste usoudili, že platné úsudky jsou a), b), c), g), i), a j), a ostatní jsou neplatné, pak Vám to výborně logicky myslí a můžete se směle pustit do studia následujících kapitol. Z toho ovšem neplyne, že pokud jste se v tomto cvičení dopustili nějaké chyby, či s tímto řešením nesouhlasíte, nemůžete se pustit do studia následujících kapitol. Právě naopak, věřím, že poté, co si následující kapitoly prostudujete, snadno si ověříte platnost či neplatnost těchto úsudků pomocí metod, které se naučíme.

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. Pravdivá zřejmě není. Kdyby byla nepravdivá, pak by bylo pravda, že francouzský král není holohlavý, což rovněž není možné, protože francouzský král neexistuje. Tedy kdyby nastal jeden z těchto případů (pravdivost či nepravdivost), vyplývala by z této věty existence francouzského krále! Klasická výroková logika tedy ctí ***princip dvojhodnotovosti*** (*tercium non datur* – Chrisipos ze Solov).[1]

Výroky dělíme na jednoduché a složené. *Elementární (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. Každý jazyk je nejlépe definován abecedou a gramatikou. Abeceda určuje typy symbolů, které mohou být v jazyce použity, gramatika pak zadává pravidla tvorby (nekonečně mnoha) dobře utvořených výrazů, tj. v tomto popřípadě *formulí.*

[1] TIL pracuje s parciálními funkcemi, tedy i s výroky bez pravdivostní hodnoty. Neklasické vícehodnotové a modální logiky pracují s intervalem pravdivostních hodnot. V tomto textu se však budeme zabývat pouze dvouhodnotovou logikou totálních funkcí.

Definice 2.1.1 (*jazyk výrokové logiky*):
Abeceda jazyka výrokové logiky je množina následujících symbolů:

- Výrokové symboly: $p, q, r, \ldots$ (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 spojky ***negace***, ***disjunkce***, ***konjunkce***, ***implikace***, ***ekvivalence***.

Gramatika jazyka výrokové logiky rekurzivně definuje nekonečnou množinu ***formulí***:
(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 jakékoli formule.
2. Používání závorek v zápisu formulí můžeme omezit přijetím následujících konvencí:
   - Složenou formuli nejvyššího řádu netřeba závorkovat.
   - Logické spojky uspořádáme do prioritní stupnice $\neg, \wedge, \vee, \supset, \equiv$. Ze dvou funktorů váže silněji ten, který je v uvedené stupnici umístěn více vlevo.
     Pozn.: Tuto konvenci však doporučujeme příliš nezneužívat 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 $p \supset q \supset r \supset s$ vyhodnocujeme tak, jakoby byla zapsána ve tvaru $((p \supset q) \supset r) \supset s$.
   - U vícečlenných konjunkcí nebo disjunkcí není třeba (vzhledem k jejich asociativitě – viz dále) uvádět závorky, tj. např. místo $(p \vee q) \vee r$ nebo $p \vee (q \vee r)$ lze psát pouze $p \vee q \vee r$. Tato konvence souvisí s předchozí konvencí (na pořadí vyhodnocování nezáleží a tedy lze standardně vyhodnocovat zleva doprava).
3. Symbolika pro výrokové spojky není v literatuře jednotná. Následující tabulka 2.1. udává alternativní značení spojek:

Symbol pro spojku	Alternativní Symboly
$\wedge$	&
$\supset$	$\rightarrow, \Rightarrow$
$\equiv$	$\leftrightarrow, \Leftrightarrow$

Tab. 2.1.

***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

Tab. 2.2.

Definice 2.1.2 (*pravdivostní vyhodnocování formulí*):

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 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 valuaci výrokového symbolu, tj.
$w(p)_v = v(p)$ 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 2.3:

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. 2.3.

2.1.1. Převod z přirozeného jazyka do jazyka výrokové logiky

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**, značíme $\neg$, 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**, značíme $\wedge$, 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 lze analyzovat spojkou konjunkce, např.:
   "Jablka a hrušky se pomíchaly".
   "Přišel jsem domů a zatopil".

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

   Příklady:

   "Osobní auta mají přední nebo zadní náhon" (nebo obojí) $\rightarrow p \vee q$
   "Napoleon diktoval nebo se procházel" (nebo obojí) $\rightarrow p \vee q$

   Pozor! Spojka "nebo" se často používá v přirozeném jazyce ve *vylučujícím* smyslu "buď, anebo". V tom případě bychom měli při analýze použít jinou spojku – ***alternativu*** (neboli ***nonekvivalenci***), viz tabulka všech binárních funkcí níže.

   Příklady: "Tento muž je buď ženatý, nebo svobodný" $\rightarrow \neg(p \equiv q)$
   "Zůstanu doma, nebo půjdu do školy" $\rightarrow \neg(p \equiv q)$

4. Spojka **implikace**, značíme $\supset$, 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.

   Příklady:
   "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**, značíme ≡, odpovídá ”**právě tehdy, když”, ”tehdy a jen tehdy, když”**, apod. , ale ne ”tehdy, když” – to je implikace!

Příklady:
”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. Ve kterém případě mohu dostat facku?
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”. Označme jednotlivé výroky takto:

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

Existují dvě možné analýzy.
1. analýza: $[(p \wedge q) \vee r] \supset s$
2. analýza: $[p \wedge (q \vee r)] \supset s$
Obě formule jsou různé a nejsou ekvivalentní (tj. nemají shodnou pravdivostní funkci), 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 schematicky jako “Protože prohráli (p), tedy se vrátili z mistrovství předčasně (v)” a toto spojení evidentně není komutativní, zdálo by se, že větu 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. Proto si zapamatujeme:

***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 2.3, lze ekvivalentně definovat následujícími vzorci (tato definice je využívána v modálních logikách).

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

(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.

2.1.2. Sémantické dokazování ve výrokové logice

V tomto odstavci nejprve definujeme přesně, kdy je daná formule tautologií (tj. logicky pravdivá), kontradikcí či je splnitelná, a pak si představíme sémantické metody, jak sémanticky ověřovat či dokazovat logickou pravdivost a logické vyplývání ve výrokové logice. Jednou z nejjednodušších metod je ***tabulková metoda.***

***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),
$(\neg p \vee \neg q) \equiv \neg(p \wedge q)$ (sloupec 3)
$\neg[(\neg p \vee \neg q) \equiv \neg(p \wedge q)]$ (sloupec 4).
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).

¬	((¬	*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

Tab. 2.4.

Nyní tedy můžeme definovat model dané formule, kdy je formule splnitelná, tj. kdy má model, co je to tautologie a kontradikce, a konečně snad nejdůležitější definice této kapitoly, a tou je *výrokově logické vyplývání.*

Definice 2.1.3 (*model formule, splnitelnost a nesplnitelnost, tautologie a kontradikce*):

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 $\models A$.

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 $\mathbf{M}$ 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.***

Definice 2.1.4 (*výrokově logické vyplývání*):

Formule A ***výrokově logicky vyplývá*** *z množiny formulí M,* značíme $M \models A$, 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. Je tomu tak proto, že sporná množina předpokladů nemá žádný model. Tedy ať už je závěr jakýkoli, pravdivý či nepravdivý, nemůže to narušit platnost úsudku. Ta je dána podmínkou, že závěr musí být pravdivý za všech okolností, kdy jsou pravdivé všechny předpoklady. Jestliže tedy nejsou pravdivé za žádných okolností, „nezavazuje“ to závěr k ničemu. Je to možná trochu neintuitivní, ale dle definice to platí. Existují tzv. relevantní logiky, které takovýto úsudek za platný nepovažují. Nicméně, v klasických logikách opravdu ze sporné množiny předpokladů vyplývá deduktivně jakýkoli závěr. Proto se snažíme vždy udržet konzistenci báze znalostí, tj. množiny zjištěných faktů (předpokladů), ze kterých dále odvozujeme patřičné důsledky. Jakmile se nám vloudí nekonzistence, důkazový kalkul prakticky kolabuje.

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:**

a) Z tabulky předchozího příkladu 2.1.2 okamžitě plyne:

- Formule p, q, $\neg p$, $\neg q$, $p \wedge q$, $\neg p \vee \neg q$, $\neg(p \wedge q)$, $(\neg p \vee \neg q) \equiv \neg(p \wedge q)$ jsou splnitelné.

- Např. formule $\neg(p \wedge q)$ 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 $(\neg p \vee \neg q) \equiv \neg(p \wedge q)$ 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, což snadno ověříme tabulkovou metodou
- Formule $\neg[(\neg p \vee \neg q) \equiv \neg(p \wedge q)]$ je kontradikcí. Neexistuje ohodnocení výrokových symbolů p, q, pro které by byla formule pravdivá. Žádné ohodnocení formuli nesplňuje, formule nemá model.

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

p	q	r	$p \supset r$	$q \supset r$	$p \vee q$
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. V každém modelu množiny M je formule r pravdivá. Tedy (závorky pro množinu premis není nutno uvádět):

$$p \supset r, q \supset r, p \vee q \models r$$

Tedy tabulková metoda je tou nejzákladnější metodou dokazování ve výrokové logice. Jelikož je tabulka pravdivostní funkce dané formule vždy konečná, lze v konečném počtu kroků rozhodnout o platnosti úsudku, tautologičnosti dané formule, atd. Říkáme proto, že výroková logika je rozhodnutelná.

***Příklad* 2.1.4** (některé důležité tautologie výrokové logiky).

Níže uvedené tautologie snadno ověříme tabulkovou metodou. Ty nejpoužívanější a nejdůležitější z nich vyznačujeme tučným písmem:

- 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

Jsou-li 1 a 0 atomické formule s významem 1 = konstanta Pravda a 0 = Nepravda, pak dále platí:

$\models p \vee 1$
$\models \neg(p \wedge 0)$
$\models (p \vee 0) \equiv p$
$\models (p \wedge 1) \equiv p$

- 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
$\models \mathbf{(p \supset q) \equiv (\neg q \supset \neg p)}$	zákon kontrapozice
$\models \mathbf{(p \supset (q \supset r)) \equiv ((p \wedge q) \supset r)}$	spojování předpokladů (pozor na uzávorkování!)
$\models (p \supset (q \supset r)) \equiv (q \supset (p \supset r))$	na pořadí předpokladů nezáleží
$\models (p \supset q) \supset ((q \supset r) \supset (p \supset r))$	hypotetický sylogismus
$\models \mathbf{((p \supset q) \wedge (q \supset r)) \supset (p \supset r)}$	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:

$\models \mathbf{(p \equiv q) \equiv (p \supset q) \wedge (q \supset p)}$
$\models \mathbf{(p \equiv q) \equiv (p \wedge q) \vee (\neg q \wedge \neg p)}$
$\models \mathbf{(p \supset q) \equiv (\neg p \vee q)}$

- Zákony pro negování:

$\models \mathbf{\neg(p \supset q) \equiv (p \wedge \neg q)}$	Negace implikace
$\models \mathbf{\neg(p \wedge q) \equiv (\neg p \vee \neg q)}$	De Morganovy zákony
$\models \mathbf{\neg(p \vee q) \equiv (\neg p \wedge \neg q)}$	De Morganovy zákony

Metoda protipříkladu: ověřování tautologií a logického 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! Složitost takového rozhodování roste exponenciálně. Proto jsou používány jiné, efektivnější metody. Jednou z nich je metoda protipříkladu, čili sporem, která je zejména vhodná pro ověřování tautologií ve tvaru implikace a pro ověřování logického vyplývání.

a) ***Dokazování tautologií sporem***. Princip je tento. Chceme-li dokázat logickou pravdivost formule A, pak využijeme tento zákon:

$$\models A \text{ právě když } \neg A \not\models$$

Jistě, je-li opravdu formule *a* tautologie, $\models A$, musí být formule $\neg A$ kontradikcí, neboť je-li A pravdivá při každém ohodnocení svých výrokových proměnných, pak negovaná formule $\neg A$ nemůže být pravdivá při žádném ohodnocení, tedy je to kontradikce.

Předpokládáme tedy, že $\neg A$ není kontradikce, tedy že může být při nějakém ohodnocení pravdivá a pokoušíme se dojít ke sporu, tj. ukázat, že tato negovaná formule model nemá, tedy je to kontradikce.

***Příklad* 2.1.5**

Ověříme sporem zákon simplifikace $p \supset (q \supset p)$. Předpokládáme tedy, že tato formule není tautologie. Vycházíme z toho, že implikace je nepravdivá jen v jednom případě (Tab. 2.3), a to tehdy, 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:

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

b) ***Dokazování platnosti úsudku sporem***.

Chceme-li ověřit platnost úsudku sporem, předpokládáme, že úsudek platný není. Dle definice je úsudek neplatný, jestliže existuje ohodnocení výrokových proměnných vyskytujících se v předpokladech a závěru takové, že jsou v něm všechny předpoklady pravdivé a závěr nepravdivý. Jinými slovy, úsudek je neplatný, jestliže existuje model množiny předpokladů ve kterém je závěr nepravdivý.

Příklad.

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”):

```
p ⊃ q,  r ∨ ¬q,  ¬r  /  ¬p
  1        1       1      0
                     0      1
1    1  0    1
     |——— 0          spor !
```

Na závěr těchto úvah uvedeme ještě několik užitečných poznatků. Následující věta vypovídá o zcela zřejmé skutečnosti, že je-li nějaká formule tautologie, pak je tautologií také každá formule stejné logické formy.

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 společnou logickou formu. Nahradíme-li v tautologii výrokové symboly p, q, r,... metasymboly A, B, C,..., dostaneme z konkrétní výchozí tautologie ***schéma tautologií*** dané formy.

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, …, 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 – 2.1.4 a implikace – Tab. 2.3)

Důsledek.: 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:

$$\mathbf{A_1, A_2, \ldots, A_n \models B} \text{ právě tehdy, když } \mathbf{\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \supset B}$$

Vidíme tedy, že dokazování platnosti úsudku je ekvivalentní dokazování příslušné tautologie ve tvaru implikace.

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:

Je-li $\models A$, $\models A \supset B$, 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:

Je-li $\models (C \equiv D)$, 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 (***duální formule***): Nechť formule F je utvořená z formulí A, B pouze pomocí funktorů $\neg$, $\wedge$, $\vee$. Formuli 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 pravidla o dualitě:

1. $\neg(F(p, q,...)) \equiv F'(\neg p, \neg q,...)$
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. 3.3. pro obecnější formule predikátové logiky. Viz Věta 3.3.3.

2.1.3 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 (*normální formy formulí*).

- ***Literál*** je výroková proměnná (tj. atomická formule) nebo její negace.
- ***Elementární konjunkce*** (**EK)** je konjunkce literálů.
- ***Elementární disjunkce*** (**ED)** je disjunkce literálů.

- ***Úplná elementární konjunkce*** **(UEK)** dané množiny výrokových proměnných je elementární konjunkce, ve které se každá proměnná z dané množiny vyskytuje právě jednou (buďto prostě nebo negovaná).
- ***Úplná elementární disjunkce*** **(UED)** dané množiny výrokových proměnných je elementární disjunkce, ve které se každá proměnná z dané množiny vyskytuje právě jednou (buďto prostě nebo negovaná).
- ***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, tj. ukážeme, jak se požadované tvary naleznou. K dané formuli nejdříve určíme její pravdivostní funkci (zapsanou ve tvaru tabulky) postupem vysvětleným v příkladu u definice 2.1.2. Dále se postup liší podle toho, zda hledáme UDNF nebo UKNF.

UDNF: 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. Čili je-li ohodnocení dané proměnné 1, pak proměnnou ponecháme. Je-li 0, pak ji negujeme a dostaneme opět 1. Konjunkce 1 a 1 dává hodnotu 1. Disjunkce všech těchto UEK představuje hledanou UDNF.

UKNF: 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 $A \models B$ a $B \models A$, tj. formule A a B mají stejnou pravdivostní funkci, stejné modely.

Navíc zřejmě platí: $\models (A \equiv B)$ právě když $A \Leftrightarrow B$. Proto se v literatuře často nerozlišuje mezi $\equiv$ a $\Leftrightarrow$.

***Příklad* 2.1.7**: Nalezneme UDNF a UKNF pro formuli $\neg(p \supset q)$: Provedeme to dvojím způsobem. Jednak využijeme postup, popsaný v důkaze předchozí věty, tj. metodu pravdivostní tabulky, a za druhé, ukážeme, jak najít normální formy pomocí ekvivalentních úprav dané formule.

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	-	$\neg p \vee \neg q$

Jako výsledek dostaneme:

UDNF je disjunkce úplných elementárních konjunkcí. V našem případě je takováto konjunkce pouze jedna, a to $p \wedge \neg q$. Tedy platí:

$$\neg(p \supset q) \Leftrightarrow (p \wedge \neg q).$$

UKNF je konjunkce úplných elementárních disjunkcí. V našem případě jsou to tři disjunkce, a to $(p \vee q)$, $(p \vee \neg q)$, $(\neg p \vee \neg q)$. Tedy platí:

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

2. *Metoda ekvivalentních úprav* (využijeme tautologie z příkladu 2.1.4):

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

UKNF: $\neg(p \supset q) \Leftrightarrow (p \wedge \neg q) \Leftrightarrow (p \vee 0) \wedge (\neg q \vee 0) \Leftrightarrow [p \vee (q \wedge \neg q)] \wedge [\neg q \vee (p \wedge \neg p)]$
$\Leftrightarrow (p \vee q) \wedge (p \vee \neg q) \wedge (\neg q \vee p) \wedge (\neg q \vee \neg p) \Leftrightarrow (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$

Pozn.: Ve třetím kroku jsme použili zákon o tautologii $\models (p \vee 0) \equiv p$. Ve čtvrtém kroku pak jsme využili ekvivalencí $(q \wedge \neg q) \equiv 0$, $(p \wedge \neg p) \equiv 0$ a věty o substituci. Další krok je pak uplatněním distributivního zákona, viz příklad 2.1.4, algebraické zákony. Nakonec jsme využili komutativnosti disjunkce ke zjednodušení výsledku.

Opačnou úlohou k nalezení normální formy je úloha, kdy chceme nalézt co nejjednodušší formuli ekvivalentní dané formuli v normální formě. Ukážeme si to na příkladě.

***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 spojky $\neg$, $\wedge$, $\vee$. Spojky $\supset$, $\equiv$ 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 spojek), nezbytných k vytvoření libovolné pravdivostní funkce, dále zredukovat ?

Abychom na tyto otázky odpověděli, zamysleme se nejprve nad tím, kolik je všech jedno- a dvou-argumentových pravdivostních funkcí. Následující tabulky dávají odpověď. Nechť X, Y jsou libovolné formule.

X	0	1	
$w_0(X)$	0	0	jednoargumentová konstanta Nepravda
$w_1(X)$	0	1	argument X
$w_2(X)$	1	0	negace argumentu: $\neg X$
$w_3(X)$	1	1	jednoargumentová konstanta Pravda

Seznam všech pravdivostních funkcí s jedním argumentem

Vidíme, že již pro pravdivostní funkce s jedním argumentem existují čtyři možnosti. Pro pravdivostní funkce se dvěma argumenty je pak těchto možností šestnáct.

X	0	0	1	1	
Y	0	1	0	1	
$w_0(X,Y)$	0	0	0	0	dvouargumentová konstanta: 0
$w_1(X,Y)$	0	0	0	1	konjunkce: $X \wedge Y$
$w_2(X,Y)$	0	0	1	0	inhibice: $\neg(X \supset Y)$
$w_3(X,Y)$	0	0	1	1	1. proměnná: X
$w_4(X,Y)$	0	1	0	0	inhibice: $\neg(Y \supset X)$
$w_5(X,Y)$	0	1	0	1	2. proměnná: Y
$w_6(X,Y)$	0	1	1	0	nonekvivalence: $\neg(X \equiv Y)$
$w_7(X,Y)$	0	1	1	1	disjunkce: $X \vee Y$
$w_8(X,Y)$	1	0	0	0	NOR (Peirce): $\neg(X \vee Y)$, $X \downarrow Y$ "ani ani"
$w_9(X,Y)$	1	0	0	1	ekvivalence: $X \equiv Y$
$w_{10}(X,Y)$	1	0	1	0	negace 2. proměnné: $\neg Y$
$w_{11}(X,Y)$	1	0	1	1	implikace: $Y \supset X$
$w_{12}(X,Y)$	1	1	0	0	negace 1. proměnné: $\neg X$
$w_{13}(X,Y)$	1	1	0	1	implikace: $X \supset Y$
$w_{14}(X,Y)$	1	1	1	0	NAND (Sheffer): $\neg(X \wedge Y)$, $X \uparrow Y$
$w_{15}(X,Y)$	1	1	1	1	dvouargumentová konstanta: 1

Seznam všech pravdivostních funkcí se dvěma argumenty

Věta 2.1.7: Počet n-árních pravdivostních funkcí je 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 jiným n-ticím. Funkcí je tedy 2 umocněno na n, tj. 2^n.

Definice 2.1.7 (*funkcionální úplnost*): 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

$$\neg A \Leftrightarrow A \uparrow A,\ A \wedge B \Leftrightarrow (A \uparrow B) \uparrow (A \uparrow B), \text{ kde } \uparrow \text{ značí NAND,}$$

$$\neg A \Leftrightarrow A \downarrow A,\ A \vee B \Leftrightarrow (A \downarrow B) \downarrow (A \downarrow B), \text{ kde } \downarrow \text{ značí NOR.}$$

Na výrokovou logiku lze tedy 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 dále definována binární relace:

$\Leftrightarrow$ ..... ekvivalence (formulí)

Faktorová algebra indukovaná relací ekvivalence $\Leftrightarrow$ je opět Booleovou algebrou a nazývá se Lindenbaumova algebra. Jejími prvky jsou třídy navzájem ekvivalentních formulí. Na této množině tříd ekvivalentních formulí 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.

Cvičení ke kapitole 2.1.

1) U následujících formulí rozhodněte, o jakou formuli se jedná (splnitelná, tautologie, kontradikce). Použijte jak tabulkovou metodu, tak metodu ekvivalentních úprav formulí.

   a) $(p \wedge \neg q) \supset (\neg p \supset (q \vee p))$
   b) $(q \wedge p) \supset [(p \supset q) \wedge (\neg p \vee q)]$
   c) $[(p \supset q) \wedge (q \vee p)\ ] \supset (\neg p \vee q)$
   d) $(p \supset q) \equiv (\neg q \supset \neg p)$
   e) $[(p \vee \neg q) \wedge \neg(p \wedge q)] \supset (\neg p \vee q)$
   f) $[(p \vee \neg(p \wedge q)) \supset (\neg p \vee q \vee p)]\ \supset (p \equiv \neg q)$

Návod:
Ad a)
Metoda ekvivalentních úprav (využíváme logické zákony z příkladu 2.1.4):
$(p \wedge \neg q) \supset (\neg p \supset (q \vee p)) \Leftrightarrow [\neg(p \wedge \neg q) \vee (p \vee q \vee p)] \Leftrightarrow [\neg p \vee q \vee p \vee q \vee p] \Leftrightarrow$
$[\neg p \vee p \vee q] \Leftrightarrow (1 \vee q) \Leftrightarrow 1$
Tedy formule je tautologie.

Tabulková metoda:

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

Pravdivostní funkce má pro všechny valuace hodnotu Pravda (1), tedy formule je tautologie.

2) *Úsudky*: Ověřte správnost či nesprávnost, v případě nesprávného úsudku upravte předpokladu tak, aby úsudek byl správný, a to **a)** sporem **b)** tabulkou:

   a) Má přednášku nebo se toulá po škole.
      Jestliže má přednášku, pak se jedná o vzorného studenta.

      Jestliže se nejedná o vzorného studenta, pak se toulá po škole.

   b) Nefunguje-li program jak má, je chyba v programu nebo není v pořádku systém.
      Je-li chyba v programu, musím se poradit se svým cvičícím.
      Program funguje, jak má.

      Nefunguje-li program, musím se poradit se svým cvičícím.

c) Není pravda, že student umí Javu a C++.
Student neumí Javu.

Student neumí C++.

d) Jestliže se problému věnuji, tak ten problém vyřeším.
Jestliže se problému nevěnuji, pak mám na práci něco jiného.

Vyřeším ten problém nebo mám na práci něco jiného.

e) Jestliže pracuji, potom vydělávám peníze, ale jestliže jsem líný, pak si užívám.
Buď pracuji, nebo jsem líný.
Nicméně, jestliže jsem líný, pak nevydělávám, zatímco jestliže pracuji, pak si neužívám.

Proto si užívám.

Návod:

Ad a) Nejprve si označíme jednotlivé elementární výroky.

p = má přednášku

t = toulá se po škole

v = je vzorný student

Nyní zapíšeme jednotlivé formule, které zachycují skladbu složených výroků:

$$p \vee t, p \supset v \,/\, \neg v \supset t$$

Řešení sporem: Předpokládáme, že úsudek není platný, tedy, že může existovat ohodnocení výrokových proměnných, při kterém by byly předpoklady byly pravdivé a závěr nepravdivý.

$$\begin{array}{l} p \vee t, p \supset v \,/\, \neg v \supset t \\ \quad 1 \quad\; 1 \quad\;\; 0 \\ \qquad\quad\; 1 \quad\; 0 \\ 0 \;|\; 0\,0 \quad 0 \quad 0 \\ \quad 0 \\ \text{Spor.} \end{array}$$

Tedy takové ohodnocení existovat nemůže, úsudek je platný.

Ad b) Řešení tabulkou:
Všímáme si pouze sloupců, ve kterých jsou všechny předpoklady pravdivé. Jsou to sloupce 1, 3, 5 a 6. Tedy modely předpokladů jsou tyto:

$p = 1, t = 1, v = 1$
$p = 1, t = 0, v = 1$
$p = 0, t = 1, v = 0$
$p = 0, t = 1, v = 0$

V těchto modelech předpokladů je pravdivý také závěr $\neg v \supset t$.

	p	t	v	$p \vee t$	$p \supset v$	$\neg v$	$\neg v \supset t$	
1	1	1	1	1	1	0	1	⇐
2	1	1	0	1	0	1	1	
3	1	0	1	1	1	0	1	⇐
4	1	0	0	1	0	1	0	
5	0	1	1	1	1	0	1	⇐
6	0	1	0	1	1	1	1	⇐
7	0	0	1	0	1	0	1	
8	0	0	0	0	1	1	0	

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.* Tato metoda je uplatnitelná na formule v *konjunktivní normální formě (KNF).*

Obecně, jak se dovíme v kapitole 3, je rezoluční metoda důkaz sporem. Ovšem ve výrokové logice ji můžeme použít také pro přímý důkaz. Je tomu tak proto, že rezoluční pravidlo zachovává pravdivost. Tedy rezolventa, kterou z daných předpokladů odvodíme, z nich *vyplývá.* A nyní přesněji:

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

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

Toto pravidlo není přechodem k ekvivalentní formuli, ale zachovává *pravdivost* tedy rezolventa z daných předpokladů vyplývá**.**

Důkaz: Nechť je formule $(A \vee l) \wedge (B \vee \neg l)$ 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 je pravdivá v každém modelu předpokladů, neboť jsme zkoumali *libovolnou* valuaci v:

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

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) *Nepřímý 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, je tato evidentně nesplnitelná, tedy také původní $\neg A$ je nesplnitelná a A je tautologie.

b) *Nepřímý 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

$$(P_1 \wedge ... \wedge P_n) \supset Z$$

je tautologie (viz věta 2.1.2, která nás k tomu opravňuje), tedy že její negace

$P_1 \wedge ... \wedge P_n \wedge \neg Z$ je kontradikce.

Příklad

1) Ověříme platnost úsudku $p \supset q$, $r \vee \neg q$, $\neg r$ / $\neg p$ nepřímým důkazem. 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.

1a) Nyní provedeme přímý důkaz platnosti výše uvedeného úsudku:

1. $\neg p \vee q$	
2. $r \vee \neg q$	
3. $\neg r$	
————	
4. $\neg q$	rezoluce 2, 3
5. $\neg p$	rezoluce 1, 4

Alternativně:

1. $\neg p \vee q$	
2. $r \vee \neg q$	
3. $\neg r$	
————	
4. $\neg p \vee r$	rezoluce 1, 2
5. $\neg p$	rezoluce 3, 4

2) Ověříme platnost úsudku č. 4 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.

2a) Nyní provedeme přímý důkaz.

$d \vee k$	1. $d \vee k$
$d \supset o$	2. $\neg d \vee o$
-------	3. $k \vee o$ rezoluce 1, 2
$\neg o \supset k$	

Klauzule 3 je ekvivalentní závěru, který jsme chtěli odvodit: $\neg o \supset k \Leftrightarrow o \vee k \Leftrightarrow k \vee o$

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 (*klauzulární forma*):

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.
2. *Prázdná klauzule* je klauzule, která neobsahuje ani jeden literál. Prázdnou klauzuli označujeme symbolem □.
3. *Hornova klauzule* je klauzule s nejvýše jedním pozitivním (nenegovaným) literálem.
4. *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 ($m = 0$):
   $$\{\ \} \Rightarrow \{p_1, p_2, ..., p_n\}, \text{ neboli } 1 \supset \{p_1, p_2, ..., p_n\}.$$
   - 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 ($m = n = 0$):
   $$\{\ \} \Rightarrow \{\ \}, \text{ neboli } 1 \supset 0, \text{ neboli } \#.$$
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 – důkaz sporem*): 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 v nějaké valuaci v pravdivé 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 v této valuaci pravdivá také klausule

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

neboli:

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

***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*:
   - $m = 0, n = 0$: $l, \neg l \vdash \#$ odvození sporu
   - $m = 0, n = 1$: $l, \neg L \vee B \vdash B$ pravidlo MP
   - $m = 1, n = 1$: $l \vee A, \neg l \vee B \vdash A \vee B$ základní tvar rezolučního pravidla

Definice 2.2.2 (*Rezoluční uzávěr*): 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.

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 $\# = l \wedge \neg l$ 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 ekvivalentní a tedy také jsou pravdivostní funkce formule F a jejího rezolučního uzávěru libovolného řádu ekvivalentní.

***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'. □	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.	□	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 tohoto odvozovacího pravidla:

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \mid\!- p \supset (s \vee t),$$

neboli tohoto teorému:

$$\mid\!= (p \supset q \vee r) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r) \supset [(p \supset (s \vee t)]$$

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.	#	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 následující příklad 2.2.4.)
2. Rezoluční metoda se výrazně zefektivní, je-li výchozí množina klauzulí tvořena výhradně *Hornovými klauzulemi*, tj. klauzulemi s nanejvýš jedním pozitivním literálem.
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 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* 2.2.3**: Vyřešíme úlohu zadanou v příkladě 2.2.2 se současným užitím lineární metody a metody podpůrné množiny. Máme dokázat

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \mid\!- p \supset (s \vee t),$$

což znamená odvodit spor z množiny těchto klauzulí:

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

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.	#	rezoluce: 5,10	Q.E.D

***Příklad* 2.2.4:** 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. $A \vee \neg B$

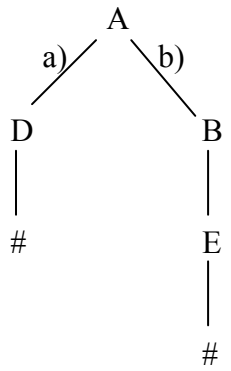
Položíme-li dotaz ”Kdy platí A?” neboli ”Vyplývá z dané množiny A?, pak vlastně připojíme 6. klausuli $\neg A$ a provádíme rezoluci. Máme zde dvě možnosti, jak dokázat A z předpokladů 1 – 5:

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

Pozn.: Jak jsme již zmínili, rezoluční metoda je základem automatického dokazování, a to především v programovacím jazyce Prolog. V Prologu zapíšeme uvedené klauzule 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) provedeme větev b), 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:

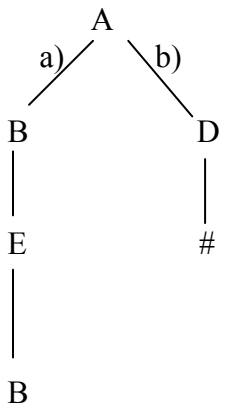


Strategie do hloubky ”prohledá nejprve do hloubky” první větev a pak druhou. Je efektivnější, avšak program může ”uvíznout v tautologii” – nekonečné větvi. Kdybychom např. upravili náš program tak, že bychom přehodili 4. a 5. klausuli a druhou bychom změnili na $E \vee \neg B$, druhá větev b) by se stala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

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

V programovacím jazyce Prolog bude uvedený program zapsán takto:

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



atd., nekonečná větev.

Cvičení ke kapitole 2.2.

1. Ověřte rezoluční metodou platnost těchto úsudků

Jestliže studuji, dosáhnu dobrého postavení.
Jestliže nestuduji, užívám si.
_____
Dosáhnu dobrého postavení, nebo si užívám.

Jestliže pracuji, pak vydělávám peníze, ale jsem-li líný, pak si užívám.
Buď pracuji nebo jsem líný.
Nicméně, jestliže pracuji, potom si neužívám, zatímco jestliže jsem líný, potom nevydělávám peníze.
_____
Proto si užívám.

Neběží-li motor, je vada v motoru nebo nejde proud.
Je-li vada v motoru, je třeba volat opraváře.
Proud jde.
_____
Neběží-li motor, je třeba volat opraváře.

Není pravda, že uchazeč umí anglicky i německy.
Uchazeč neumí anglicky.
_____
Uchazeč neumí německy.

Návod: Uvažme první úsudek. Nejprve jej formalizujeme a pak provedeme důkaz rezoluční metodou:

Jestliže studuji (s), dosáhnu dobrého postavení (p).
Jestliže nestuduji, užívám si (u).
_____
Dosáhnu dobrého postavení, nebo si užívám.

$s \supset p$
$\neg s \supset u$
_____
$p \vee u$

Převedeme nyní uvedené formule do klauzulární formy a provedeme přímý důkaz:

1) $\neg s \vee p$
2) $s \vee u$
3) $p \vee u$ rezoluce 1, 2

Tedy úsudek je platný.

2. *Co vyplývá* z následujících předpokladů?

Karel pojede autobusem nebo vlakem.
Jede-li Karel autobusem nebo svým vozem, pak přijede pozdě a zmešká schůzku.
Karel nepřišel pozdě.

Je-li úterý, je přednáška, ale není cvičení.
Dnes je přednáška i cvičení.
Je-li cvičení, pak nepotřebujeme projektor.

Je-li Karel v Praze, je Helena v Brně.
Je-li úterý, není Helena v Brně.
Je úterý nebo středa.

Návod: Vyřešíme první úlohu takto:

1) Karel pojede autobusem (a) nebo vlakem (v).
2) Jede-li Karel autobusem nebo svým vozem (s), pak přijede pozdě (p) a zmešká schůzku (z).
3) Karel nepřišel pozdě.

1. $a \vee v$
2. $[(a \vee s) \supset (p \wedge z)$
3. $\neg p$

Nyní převedeme uvedené formule do klauzulární formy. Nejprve upravíme druhou formuli:

$[\neg(a \vee s) \vee (p \wedge z)] \Leftrightarrow [(\neg a \wedge \neg s) \vee (p \wedge z)] \Leftrightarrow [\neg a \vee (p \wedge z)] \wedge [(\neg s \vee (p \wedge z)] \Leftrightarrow$
$[(\neg a \vee p) \wedge (\neg a \vee z)] \wedge [(\neg s \vee p) \wedge (\neg s \vee z)]$

1. $a \vee v$
2. $\neg a \vee p$
3. $\neg a \vee z$
3. $\neg s \vee p$
4. $\neg s \vee z$
5. $\neg p$
6. $v \vee p$ rezoluce 1, 2 Karel jel vlakem nebo přišel pozdě
7. $v \vee z$ rezoluce 1, 3 Karel jel vlakem nebo zmeškal schůzku
8. $\neg a$ rezoluce 2, 5 Karel nejel autobusem
9. $\neg s$ rezoluce 3, 5 Karel nejel svým vozem
10. v rezoluce 5, 6 Karel jel vlakem

3. Najděte ***chybějící předpoklad*** v následujících úsudcích tak, aby úsudek byl platný:

   $p \vee \neg r, q \supset (p \wedge r),$ **?** $\models \neg q \vee \neg r$

   $p \supset r, \neg q \vee \neg r, r \supset (q \vee s),$ **?** $\models p \wedge s$

   $(p \vee r) \supset (q \wedge s), q \supset \neg r,$ **?** $\models p \supset \neg s$

   Návod na řešení první úlohy sporem:

   1. $p \vee \neg r$
   2. $\neg q \vee p$
   3. $\neg q \vee r$
   4. q negovaný závěr
   5. r negovaný závěr
   6. p rezoluce 1, 5
   7. r rezoluce 3, 4
   8. $\neg r$ (chybějící předpoklad)
   9. # rezoluce 7, 8

2.3. Systém přirozené dedukce výrokové logiky

Přirozená dedukce je jednou z metod výstavby formálního systému čili důkazového kalkulu 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, podobně jako rezoluční metoda. 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 (*přirozená dedukce pro VL*):
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 $A \vee B, \neg B \vdash A$ (disjunktivní sylogismus)	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	

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

- každé B_i (i=1, 2,...,m-1) je:
  - rovno A_j pro některé $j \in \{1, 2,...,n\}$ (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.

   $$A_1 \supset \{A_2 \supset [A_3 \supset \ldots \supset (A_n \supset B) \ldots]\}, \qquad (*)$$

   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 $B_1, B_2,...,B_m$, 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) $\vdash [(p \supset q) \wedge (q \supset r)] \supset (p \supset r)$

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) $\vdash (\mathrm{p} \supset \mathrm{q}) \supset [(\mathrm{q} \supset \mathrm{r}) \supset (\mathrm{p} \supset \mathrm{r})]$

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

Důkaz (nepřímý):

1.	$p \supset q$	předpoklad	
2.	$\neg q$	předpoklad	
3.	p	předpoklad nepřímého důkazu	
4.	q	MP: 1,3	spor s 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(etnik) 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) + 5
7.	$\neg$(A je v) $\wedge$ $\neg$(B je v) $\supset$ (C je v)	předpoklad: (1) + 6
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

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

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, že $A_1, A_2 \vdash B$ /**/:

(1) A_1	1. předpoklad /**/
(2) A_2	2. předpoklad /**/
(3) $A_1 \supset (A_2 \supset B)$	teorém /*/, jehož 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 (de Morganův zákon)
Negace konjunkce:	$\neg(A \wedge B) \vdash \neg A \vee \neg B$	NK (de Morganův zákon)
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 s 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: Je 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* 2.3.3:**

- 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	EK: 5
7.	$\neg r$	EK: 5
8.	r	MP: 1.6. – spor, tedy předpoklad nepřímého důkazu je nepravdivý
9.	$\neg p \vee r$	Q.E.D.

***Příklad* 2.3.4:**

- 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 teorém.

***Příklad* 2.3.5:**

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

  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

- $\vdash \neg(p \vee q) \supset (\neg p \wedge \neg q)$

  Nepřímý důkaz technikou hypotetických předpokladů:

1.	$\neg(p \vee q)$	předpoklad	
	2.1. p	hypotéza	
	2.2. $p \vee q$	ZD: 2.1	spor s 1
3.	$\neg p$	neboť p vede ke sporu	
	4.1. q	hypotéza	
	4.2. $p \vee q$	ZD: 4.1	spor s 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 hypotetického 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 2.3.6*:**

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

  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.

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

  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 s 3
6.1. r 2. hypotéza
6.2. s MP: 2, 6.1
6.3. $q \vee s$ ZD: 6.2, spor 3

- Provedeme důkaz ***pravidla rezoluce*** (viz 2.2) technikou větveného důkazu. 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
4. $l \supset A \vee B$ ZI
   5.1. $\neg l$ hypotéza, 2. případ
   5.2. A ED: 1, 5.1
   5.3. $A \vee B$ ZD: 5.2
5. $\neg l \supset A \vee B$ ZI
6. $(l \supset A \vee B) \wedge (\neg l \supset A \vee B)$ ZK
7. $(l \vee \neg l) \supset (A \vee B)$ teorém
8. $(A \vee B)$ MP 3, 7

(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 ⊃ A (resp. ¬A ∨ 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* 2.3.7:** Dokažme tautologii $[(p \supset q) \wedge \neg q] \supset \neg p$

a) *Metodou ekvivalentních úprav*:

$\neg[(p \supset q) \wedge \neg q] \supset \neg p \Leftrightarrow [p \wedge \neg q \vee q] \vee \neg p \Leftrightarrow (p \wedge 1) \vee \neg p) \Leftrightarrow (p \vee \neg p)$, což je tautologie.

b) *Důkaz* dle Gentzenova systému:

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. $(p \vee \neg p \vee q) \wedge (q \vee \neg q \vee \neg \mathrm{p})$ 2.,4. ZK
6. $(1 \vee q) \wedge (1 \vee \neg p)$
7. $(1 \wedge 1)$
8. 1 tautologie

Cvičení ke kapitole 2.3.

Ověřte přirozenou dedukcí platnost těchto úsudků:

Jestliže studuji, dosáhnu dobrého postavení.
Jestliže nestuduji, užívám si.
_____
Dosáhnu dobrého postavení, nebo si užívám.

Jestliže pracuji, pak vydělávám peníze, ale jsem-li líný, pak si užívám.
Buď pracuji nebo jsem líný.
Nicméně, jestliže pracuji, potom si neužívám, zatímco jestliže jsem líný, potom nevydělávám peníze.
_____
Proto si užívám.

Neběží-li motor, je vada v motoru nebo nejde proud.
Je-li vada v motoru, je třeba volat opraváře.
Proud jde.
_____
Neběží-li motor, je třeba volat opraváře.

Není pravda, že uchazeč umí anglicky i německy.
Uchazeč neumí anglicky.
_____
Uchazeč neumí německy.

Je-li pan X otcem Jirky a má krevní skupinu A a také Jirkova matka má krevní skupinu A, pak Jirka má některou z krevních skupin A nebo 0.
Pan X i Jirkova matka mají krevní skupinu A.
Jirka nemá krevní skupinu A.
Jirka nemá krevní skupinu 0.
_____
Pan X není otcem Jirky.

Je-li Karel v Praze, je Helena v Brně.
Je-li úterý, není Helena v Brně.
Je úterý nebo středa.
_____
Je-li Karel v Praze, je středa. (Avšak *ne*, že „ve středu je Karel v Praze!)
V úterý není Karel v Praze.

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:

$$A \subset T \subset \mathrm{DUF} \subset S.$$

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. ***axiomových 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 důkazové kalkuly***.)

ad 3) ***Množina odvozovacích pravidel*** je tvořena několika nebo dokonce jen jedním pravidlem (jsou-li axiómy reprezentovány schématy). Jak jsme viděli v předchozí kapitole, systém přirozené dedukce pracuje pouze se dvěma axiómy, 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. minimální v tom smyslu, že žádný axióm není dokazatelný z ostatních axiómů.

ad 4) Přirozeným požadavkem je ***syntaktická bezespornost (konzistence)***, tj. 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 teorému v důkazovém kalkulu 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. Těmito problémy se však budeme podrobně zabývat až v kap. 4.

S (ne)úplností úzce souvisí problém (ne)***rozhodnutelnosti***: Existuje algoritmus, který o libovolné dobře utvořené formuli určí, zda je to teorém (dokazatelná DUF) čili (v korektním důkazovém kalkulu bez speciálních axiomů) 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 neboli důkazových kalkulů 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, tj. logický teorém důkazového kalkulu musí být tautologií). V tomto smyslu jsou všechny formalizace ekvivalentní.

K charakteristice dokazatelnosti byly vytvořeny dva hlavní typy formálních systémů:

a) Gentzenova typu
b) Hilbertova typu

Nyní (a v kap. 3.7) se budeme zabývat systémem Hilbertova typu.

2.4.b. Formální systém Hilbertova typu pro výrokovou logiku

Definice 2.4.1 (*definice důkazového kalkulu Hilbertova typu*):

- ***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.
- ***Axiomová 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***: Modus ponens (MP): $A, A \supset B \vdash B$

***Poznámky* 2.4.1:**

1. A, B nejsou formulemi, ale metasymboly sloužícími k označení formulí. Každé axiomové schéma označuje nekonečnou třídu axiómů daného tvaru. Kdybychom axiomová 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 důkazový kalkul. ***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 z předpokladů*):

Důkaz formule A ***z 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 $\in$ {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

$$\boldsymbol{A_1, A_2, ..., A_k \vdash A}.$$

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 $\vdash \boldsymbol{A}$.

***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 $A_1, A_2 \models B$.
2. Všimněme si, že z definice důkazu vyplývá, že i axióm je teorémem. Jeho důkaz je triviální: důkazem axiómu je axióm sám.
3. Důkazový postup $B_1, B_2,...,B_n$ formule A z 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) $A \supset A$:

a)	$(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A))$	ax. A2	$B/A \supset A$, C/A
b)	$A \supset ((A \supset A) \supset A)$	ax. A1	$B/A \supset A$
c)	$(A \supset (A \supset A)) \supset (A \supset A)$	MP: b), a)	
d)	$A \supset (A \supset A)$	ax. A1	B/A
e)	$A \supset A$	MP: d), c) Q.E.D.	

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. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$	ax. 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: $A \supset B, B \supset C \vdash A \supset C$.

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***)**:**

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

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

Důkaz:

1. Nechť $A_1, A_2,...,A_k \vdash A \supset B$. 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 $A_1, A_2,...,A_k, A \vdash B$. 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.	$\vdash \neg\neg\neg A \supset A$	$\neg\neg A \vdash A$	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.	$(\neg B \supset \neg A) \supset (A \supset B)$	ax. A3
4.	$\neg A \supset (\neg B \supset \neg A)$	ax. 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.

Pozn.: Tento důkaz ilustruje skutečnost, že *ze sporných předpokladů* lze dokázat libovolnou formuli.

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 $T, A \vdash B$ a A je logický teorém, pak $T \vdash B$.
Neboli: v množině předpokladů není třeba uvádět logické teorémy.

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

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

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

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

(f) Je-li $T \vdash A$ a $T \vdash B$, pak $T \vdash A \wedge B$.
Neboli: konjunkce důsledků množiny předpokladů je také důsledkem množiny předpokladů.

(g) $T \vdash A \supset (B \supset C)$ právě tehdy, když $T \vdash B \supset (A \supset C)$.
Neboli: na pořadí předpokladů nezáleží.

(h) $T, A \vee B \vdash C$ právě tehdy, když současně $T, A \vdash C$ a $T, B \vdash C$.
Věta o důkazu rozborem případů.

(i) Je-li $T, A \vdash B$ a současně $T, \neg A \vdash B$, pak $T \vdash B$.
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.

Některé ***Důkazy*:**

Ad (h): Nechť $T, A \vee B \vdash C$, dokážeme $T, A \vdash C$ a $T, B \vdash C$.

Důkaz:

1.	$A \vdash A \vee B$	pravidlo ZD	
2.	$T, A \vdash A \vee B$	metapravidlo (b): 1	
3.	$T, A \vee B \vdash C$	předpoklad	
4.	$T, A \vdash C$	metapravidlo (d): 2,3	Q.E.D.
5.	$T, B \vdash C$	dokáže se obdobně jako 4.	Q.E.D.

Nechť $T, A \vdash C$ a $T, B \vdash C$, dokážeme $T, A \vee B \vdash C$.

Důkaz:

1.	$T, A \vdash C$	předpoklad
2.	$T \vdash A \supset C$	věta o dedukci: 1
3.	$T \vdash \neg C \supset \neg A$	metapravidlo (d): 2, pravidlo TR
4.	$T, \neg C \vdash \neg A$	věta o dedukci: 3
5.	$T, \neg C \vdash \neg B$	odvodí se obdobně jako 4.
6.	$T, \neg C \vdash \neg A, \neg B$	metapravidlo (f): 4,5
7.	$\neg A, \neg B \vdash \neg(A \vee B)$	pravidlo ekviv. teorému de Morgana
8.	$T, \neg C \vdash \neg(A \vee B)$	metapravidlo (d): 6,7
9.	$T \vdash \neg C \supset \neg(A \vee B)$	věta o dedukci: 8
10.	$T \vdash A \vee B \supset C$	metapravidlo (d): 9. pravidlo TR
11.	$T, A \vee B \vdash C$	věta o dedukci: 10 Q.E.D.

Ad (i): Nechť $T, A \vdash B$ a $T, \neg A \vdash B$, dokážeme $T \vdash B$.

Důkaz:

1.	$T, A \vdash B$	předpoklad
2.	$T, \neg A \vdash B$	předpoklad
3.	$T, A \vee \neg A \vdash B$	metapravidlo (h): 1,2
4.	$T \vdash B$	metapravidlo (a): 3

Věta 2.4.3 (*pomocná věta pro důkaz následující 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:

$$p_1^v, p_2^v, ..., p_n^v \vdash A^v, \qquad /*/$$

kde zápis $A^{'v}$ značí buď formuli $\neg A$ (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 stupně syntaktické složitosti 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.	$A = \neg B$	složená formule ve tvaru negace
3.	$A = B \supset C$	složená formule ve tvaru implikace

Báze indukce. Vztah /∗/ má v případě elementární formule tvar $p^v \mid\!- p^v$ a je tedy evidentně platný.

Indukční krok. Dokážeme, že z předpokladu platnosti vztahu /∗/ pro komponenty B, C složené formule vyplývá platnost vztahu /∗/ také pro složené formule $\neg B$ a $B \supset C$.

a) Složená formule má tvar $\neg B$. Podle indukčního předpokladu platí

$p_1^v, p_2^v,...,p_n^v \mid\!- B^v$. Máme dokázat $p_1^v, p_2^v,...,p_n^v \mid\!- (\neg B)^v$.
K tomu, abychom to dokázali, stačí dokázat $B^v \mid\!- (\neg B)^v$. Jsou dvě možnosti: buď $w(B) = 0$ a pak $\neg B \mid\!- \neg B$ a nebo $w(B) = 1$ a pak $B \mid\!- \neg\neg B$. Vztah $B^v \mid\!- (\neg B)^v$ je dokázaný.

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

$p_1^v, p_2^v,...,p_n^v \mid\!- B^v$ a $p_1^v, p_2^v,...,p_n^v \mid\!- B^v \mid\!- C^v$.

Máme nyní dokázat, že $p_1^v, p_2^v,...,p_n^v \mid\!- (B \supset C)^v$.
K tomu, abychom to dokázali, stačí dokázat B^v, $C^v \mid\!- (B \supset C)^v$. Čtyřem různým ohodnocením formulí B, C odpovídají následující čtyři pravidla, jejichž platnost třeba ověřit:

a) $\neg B, \neg C \mid\!- B \supset C$

b) $\neg B, C \mid\!- B \supset C$

c) $B, \neg C \mid\!- \neg(B \supset C)$

d) $B, C \mid\!- B \supset C$

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.

$$\mid\!- A \text{ právě tehdy, když } \mid= A.$$

Obecněji platí:

$$A_1, A_2,..,A_n \mid\!- B \text{ právě tehdy, když } A_1, A_2,..,A_n \mid= B.$$

Důkaz:

1. Nechť $\vdash A$, dokážeme $\models A$. (*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 axiomová 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, neboť 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, což je spor. Protože všechny teorémy lze odvodit z axiómů pomocí opakovaného užití pravidla MP, jsou všechny teorémy tautologiemi.

2. Nechť $\models A$, dokážeme $\vdash A$. (*Úplnost*)

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

   $$p_1^v, p_2^v, \ldots, p_n^v \vdash A$$

   pro všechna ohodnocení v. Platí tedy speciálně také

   $$p_1^v, p_2^v, \ldots, p_n^v \vdash A,$$
   $$\neg p_1^v, p_2^v, \ldots, p_n^v \vdash A.$$

   Odtud podle věty o neutrální formuli dostáváme

   $$p_1^v, p_2^v, \ldots, p_n^v \vdash A$$

   pro všechna ohodnocení v. Speciálně opět platí

   $$p_2, \ldots, p_n^v \vdash A,$$
   $$\neg p_2, \ldots, p_n^v \vdash A$$

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

Cvičení ke kapitole 2.4.

Dokažte zbylé teorémy z příkladu 2.4.2., tj. teorémy *ad* 7 a 8.

Dokažte metapravidla a) – g) z ***Věty 2.4.2*** **(**o metapravidlech**)**.

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, tedy dle VL 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 takto:

   $$\forall x\, [P(x) \supset Q(x)],\, P(\mathrm{j}) \models q(\mathrm{j})$$

   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. $P(\mathrm{j})$, $Q(\mathrm{j})$ 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.

   Tedy uvedenou formalizaci můžeme číst takto:
   Pro všechna individua x taková, že má-li x vlastnost P, pak má také vlastnost Q. Individuum j má vlastnost P. Tedy j má také vlastnost Q.

2. Predikátová logika 1.řádu. V dalším se budeme zabývat pouze tzv. ***predikátovou logikou 1. řádu (PL^1)***, 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.

Jako obvykle, definujeme nejprve jazyk predikátové logiky 1. řádu. Tento jazyk bude obsahovat jazyk výrokové logiky, avšak navíc potřebujeme označovat individua z daného universa diskursu, k tomu nám slouží tzv. termy (konstanty, proměnné a funkční termy) a dále vlastnosti individuí a vztahy mezi individui, k tomu nám slouží tzv. predikátové symboly jako P, Q, atd. Abychom pak mohli mluvit o všech individuích nebo o některých individuích, zavedeme také tzv. kvantifikátory, a to všeobecný $\forall$ (pro všechna) a existenční $\exists$ (pro některá).

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 funkčního symbolu nebo predikátu.
   c) Pomocné symboly (závorky): (,) (případně i [,],{,})

II. ***Gramatika,*** která udává, jak tvořit:
   a) ***termy*****:**
      i) každý symbol proměnné je *atomický term*
      ii) jsou-li $t_1,...,t_n$ ($n \geq 0$) termy a je-li f n-ární funkční symbol, pak výraz $f(t_1,...,t_n)$ je term; pro $n = 0$ se jedná o nulární funkční symbol, neboli individuovou *konstantu* (značíme a, b, c, …); pro $n > 0$ se jedná o *složený term*.
      iii) jen výrazy dle i. a ii. jsou termy
   b) ***atomické formule***:
      i) je-li P n-ární predikátový symbol a jsou-li $t_1,...,t_n$ termy, pak výraz $P(t_1,...,t_n)$ je *atomická formule*
      ii) jsou-li t_1 a t_2 termy, pak výraz $(t_1 = t_2)$ je *atomická formule*
   c) ***(složené) 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 Definici 3.3.1)
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:

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

Definice 3.1.2 (*volné a vázané proměnné*)

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

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

nazýváme *obecným* 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: $P(f(y)) \supset \forall y\ Q(f(\mathbf{y}), y)$. 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.

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 $\forall$, výrazy jako "někdo", "někteří", apod. překládáme existenčním kvantifikátorem $\exists$. Dále budeme předpokládat, že jde o jazyk nad homogenním universem, proto v následujících příkladech považujeme za universum diskursu (obor proměnnosti proměnných) množinu všech individuí.

***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) Všichni zaměstnanci (*Z*) používají výtahu (*V*).
5) Ne každý člověk (*C*), který hodně mluví (*M*), nemá co říci (*R*).
6) Někdo je spokojen (*Sn*) a někdo není spokojen.
7) Někteří chytří lidé (*Ch*) jsou líní (*L*).

***Řešení*:**
Pozn.: Jako pomůcka k řešení může sloužit tato zásada: Po všeobecném kvantifikátoru $\forall$ následuje (většinou) formule ve tvaru implikace ($\supset$), kdežto po existenčním kvantifikátoru (většinou) formule ve tvaru konjunkce ($\wedge$). Vysvětlení podáme níže.

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) $\forall x\,[Z(x) \supset V(x)]$
5) $\neg\forall x\,\{[C(x) \wedge M(x)] \supset \neg R(x)\}$
6) $\exists x\, Sn(x) \wedge \exists x\, \neg Sn(x)$
7) $\exists x\,[Ch(x) \wedge L(x)]$

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, neboť formule je pouze posloupnost symbolů. Tak např. formule

$$\forall x\, P(f(x), x)$$

může "říkat", že pro všechna přirozená čísla x platí, že jejich druhá mocnina je větší než toto číslo x, 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 x platí, že jejich druhá mocnina je menší než toto číslo x, 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

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

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, tj. 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 PL^2 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 dané 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

$$\forall x\, P(f(x), y)$$

může být interpretována nad množinou celých čísel tak, že symbolu P je přiřazena relace větší nebo rovno ($\geq$), symbolu f funkce druhá mocnina (tedy $f(x)$ pak 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. valuací proměnné 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 proměnné y záporné číslo nebo nulu, nepravdivá pro všechny valuace, které přiřadí proměnné y číslo kladné.

Cvičení ke kapitole 3.1.

Převeďte následující věty z přirozeného jazyka do jazyka PL1. Poté je znegujte a opět formalizujte. Proveďte kontrolu správnosti pomocí de Morganových zákonů.

1) Někteří studenti nemají hudební nadání
2) Někteří studenti nejsou ani nadaní ani pilní
3) Každé číslo dělitelné 8 je dělitelné 4
4) Kdo seje vítr, ten sklízí bouři
5) Psi, kteří štěkají, nekoušou
6) Žádný tyran není spravedlivý
7) Každý člověk má otce i matku
8) Každý, kdo má otce, má i matku
9) Každý člověk je mladší než jeho rodiče
10) Žádný dobrý učitel nikoho zbytečně nepotrestal
11) Někdo má rád každého
12) Není všechno zlato, co se třpytí
13) Nutnou podmínkou toho, aby rovnice $y = 2653 / x$ měla řešení y, je nenulové x.

Návod:

- Výrazy jako „všichni“, „žádný“, „nikdo“, apod. formalizujeme pomocí všeobecného kvantifikátoru: $\forall$
- Výrazy jako „někdo“, „něco“, „někteří“, „existuje“, apod. formalizujeme pomocí existenčního kvantifikátoru: $\exists$
- Často je užitečné větu nejprve přeformulovat tak, aby měla stejné pravdivostní podmínky, tedy aby byla ekvivalentní s původní větou, ale její formalizace pak bude snazší. Použijeme přitom ***de Morganovy zákony*** (podrobně viz kapitola 3.3):

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

Není pravda, že všechna x jsou A $\Leftrightarrow$ Existuje x, které není A

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

Není pravda, že existuje x, které je A $\Leftrightarrow$ Žádné x není A

- ***Pozor***: v češtině máme poněkud „nelogicky“ dvojí zápor.
  - Tedy např. větu

    „Žádný člověk není dokonalý“

    formalizujeme takto:

    $$\forall x\, [C(x) \supset \neg D(x)].$$

    Použili jsme tedy pouze jednu negaci.
  - Kdybychom předchozí formuli četli s jedním záporem

    „Všichni lidé nejsou dokonalí“,

    dostáváme jinou, neekvivalentní větu s tímto významem:

    „Ne všichni lidé jsou dokonalí“,

    jejíž formalizací bude formule

    $$\neg\forall x\, [C(x) \supset D(x)] \Leftrightarrow \exists x\, [C(x) \wedge \neg \mathrm{D}(x)],$$

    kterou lze interpretovat jako

    „Někteří lidé nejsou dokonalí“.

- ***Pomocné pravidlo***: $\forall + \supset$, $\exists + \wedge$ (většinou), což je snadno odůvodnitelné právě použitím de Morganových zákonů.

  - $\neg\forall x\, [\mathrm{P}(x) \supset \mathrm{Q}(x)] \Leftrightarrow \exists x\, [\mathrm{P}(x) \wedge \neg \mathrm{Q}(x)]$
    Není pravda, že všechna P jsou Q $\Leftrightarrow$ Některá P nejsou Q
  - $\neg\exists x\, [\mathrm{P}(x) \wedge \mathrm{Q}(x)] \Leftrightarrow \forall x\, [\mathrm{P}(x) \supset \neg \mathrm{Q}(x)]$
    Není pravda, že některá P jsou Q $\Leftrightarrow$ Žádné P není Q
    - Vzpomeňme si přitom na pravidla výrokové logiky:
    - $(p \supset q) \Leftrightarrow (\neg p \vee q)$
    - $\neg(p \supset q) \Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow (p \wedge \neg q)$

    Tedy:
  - $\neg\forall x\, [\mathrm{P}(x) \supset \mathrm{Q}(x)] \Leftrightarrow \exists x\, \neg[\mathrm{P}(x) \supset \mathrm{Q}(x)] \Leftrightarrow \exists x\, [\mathrm{P}(x) \wedge \neg \mathrm{Q}(x)]$
  - $\neg\exists x\, [\mathrm{P}(x) \wedge \mathrm{Q}(x)] \Leftrightarrow \forall x\, [\neg \mathrm{P}(x) \vee \neg \mathrm{Q}(x)] \Leftrightarrow \forall x\, [\mathrm{P}(x) \supset \neg \mathrm{Q}(x)]$

Příklady:

a)

Pouze zaměstnanci (Z) používají výtah (V): $\forall x\,[V(x) \supset Z(x)]$

Pokud někdo používá výtah, pak je to zaměstnanec: $\forall x\,[V(x) \supset Z(x)]$

Není pravda, že někdo používá výtah a není to zaměstnanec:
$\neg\exists x\,[V(x) \wedge \neg Z(x)] \Leftrightarrow \forall x\,[\neg V(x) \vee Z(x)] \Leftrightarrow \forall x\,[V(x) \supset Z(x)]$

b)

Všichni zaměstnanci používají výtah: $\forall x\,[Z(x) \supset V(x)]$

Není pravda, že některý zaměstnanec výtah nepoužívá:
$\neg\exists x\,[Z(x) \wedge \neg V(x)] \Leftrightarrow \forall x\,[\neg Z(x) \vee V(x)] \Leftrightarrow \forall x\,[Z(x) \supset V(x)]$

c)

Marie (m) má ráda (R) pouze vítěze (V): $\forall x\,[R(\mathrm{m}, x) \supset V(x)]$

Pokud má Marie někoho ráda, pak je to vítěz: $\forall x\,[R(\mathrm{m}, x) \supset V(x)]$

Neexistuje někdo, koho by měla Marie ráda a nebyl to vítěz:
$\neg\exists x\,[R(\mathrm{m}, x) \wedge \neg V(x)] \Leftrightarrow \forall x\,[\neg R(\mathrm{m}, x) \vee V(x)] \Leftrightarrow \forall x\,[R(\mathrm{m}, x) \supset V(x)]$

Pozn.: „mít rád“ je binární vztah, ne vlastnost

d)

Nutnou podmínkou toho, aby rovnice $y = 2653/x$ měla řešení y, je nenulové x.

$$\forall x\,[\exists y\,(y = \mathit{Podíl}\,(2653, x)) \supset \neg(x{=}0)]$$

Je-li $x = 0$, pak neexistuje y takové, že $y = 2653/x$.

$$\begin{gathered}\forall x\,[(x{=}0) \supset \neg\exists y\,(y = \mathit{Podíl}\,(2653, x))] \Leftrightarrow \\ \forall x\,[\neg(x{=}0) \vee \neg\exists y\,(y = \mathit{Podíl}\,(2653, x))] \Leftrightarrow \\ \forall x\,[\neg\exists y\,(y = \mathit{Podíl}\,(2653, x)) \vee \neg(x{=}0)] \Leftrightarrow \\ \forall x\,[\exists y\,(y = \mathit{Podíl}\,(2653, x)) \supset \neg(x{=}0)]\end{gathered}$$

3.2. Základní pojmy teorie množin, relací a funkcí.

Dříve, než definujeme přesně interpretaci (sémantiku čili význam) formulí predikátové logiky 1. řádu, uvedeme na tomto místě podkapitolu, ve které zopakujeme základní pojmy tzv. naivní (Cantorovy) teorie množin, funkcí a relací. Důvod je ten, že ne všichni čtenáři jsou s tímto obeznámeni a přitom je znalost těchto teorií nesmírně důležitá právě pro pochopení způsobu, jakým provádíme interpretaci formulí predikátové logiky 1. řádu, tedy jak jim rozumět.

3.2.1. Teorie množin

Nejprve si položíme otázku: *Co je to množina?*

- *Množina* je soubor prvků a je svými prvky plně určena; množinu s prvky *a, b, c* značíme: $\{a, b, c\}$. To, že např. *a* je prvkem množiny $\{a, b, c\}$, značíme $a \in \{a, b, c\}$.
- Prvkem množiny může být *opět množina* a množina nemusí mít *žádné prvky*. Množina, která nemá žádné prvky, se nazývá *prázdná množina*, značíme Ø nebo také $\{\ \}$.
- *Množiny jsou identické*, právě když mají přesně stejné prvky (princip extenzionality)

Příklady:

1. *množiny*: Ø, $\{a, b\}$, $\{b, a\}$, $\{a, b, a\}$, $\{\{a, b\}\}$, $\{a, \{b, a\}\}$, $\{$ Ø, $\{$Ø$\}$, $\{\{$Ø$\}\}$
2. *být prvkem*: $a \in \{a, b\}$, $a \notin \{\{a, b\}\}$, $\{a, b\} \in \{\{a, b\}\}$, Ø $\in$ {Ø, {Ø}, {{Ø}}}, Ø $\in$ {Ø, {Ø}}, {{Ø}} $\in$ {Ø, {Ø}, {{Ø}}}
3. $x \notin$ Ø pro žádné *x*.
4. *identita množin*: $\{a, b\} = \{b, a\} = \{a, b, a\}$, ale: $\{a, b\} \neq \{\{a, b\}\} \neq \{a, \{b, a\}\}$

Množinové operace vytvářejí z množin nové množiny:

- ***Sjednocení*****:** $A \cup B = \{x \mid x \in A$ ***nebo*** $x \in B\}$
  čteme: „Množina všech *x* takových, že *x* je prvkem *A* nebo *x* je prvkem *B*.“
  - $\{a, b, c\} \cup \{a, d\} = \{a, b, c, d\}$
  - {sudá čísla} $\cup$ {lichá čísla} = {přirozená čísla} – značíme většinou ***N***

  Operaci sjednocení lze zobecnit takto: Nechť *I* je nějaká (spočetná) množina. Pak
  $\bigcup_{i \in I} A_i = \{x \mid x \in A_i$ pro *nějaké* $i \in I\}$
  Čteme: Sjednocení množin A_i je množina všech *x* takových, že *x* patří do A_i pro nějaké $i \in I$.
  Příklad: Nechť $I=\mathbf{N}$, $A_i = \{x \mid x = 2.i\}$. Pak $\bigcup_{i \in I} A_i$ = *množina sudých čísel*
- ***Průnik***: $A \cap B = \{x \mid x \in A$ ***a*** $x \in B\}$
  čteme: „Množina všech *x* takových, že *x* je prvkem *A* ***a současně*** *x* je prvkem *B*.“
  - $\{a, b, c\} \cap \{a, d\} = \{a\}$
  - {sudá čísla} $\cap$ {lichá čísla} = Ø

Operaci průniku lze zobecnit takto: Nechť I je nějaká (spočetná) množina. Pak
$\bigcap_{i\in I} A_i = \{x \mid x \in A_i \text{ pro } \textit{každé } i \in I\}$
Čteme: Průnik množin A_i je množina všech x takových, že x patří do A_i pro každé $i \in I$.
Příklad: Nechť $I=\mathbf{N}$, $A_i = \{x \mid x \geq i\}$. Pak $\bigcap_{i\in I} A_i = \emptyset$

Vztahy mezi množinami:

- Množina A je ***podmnožinou*** množiny B, značíme $A \subseteq B$, právě když každý prvek A je také prvkem B.
- Množina A je ***vlastní podmnožinou*** množiny B, značíme $A \subset B$, právě když každý prvek A je také prvkem B, ale *ne naopak*.
  Příklad: $\{a\} \subseteq \{a\} \subset \{a, b\} \not\subset \{\{a, b\}\}$

Tvrzení: $A \subset B$, právě když $A \subseteq B$ a $A \neq B$
$A \subseteq B$, právě když $A \cup B = B$ nebo $A \cap B = A$

Další ***množinové operace***:

- ***Rozdíl***: $A \setminus B = \{x \mid x \in A \text{ a } x \notin B\}$
  Příklady: $\{a, b, c\} \setminus \{a, b\} = \{c\}$;
  $\{a, b, c, d\} \setminus \{a, b, e\} = \{c, d\}$

- ***Doplněk*** (komplement):
  Nechť $A \subseteq M$. ***Doplněk A vzhledem k M*** je množina $\overline{A} = M \setminus A$
  Příklad: Množina $\{c\}$ je doplňkem množiny $\{a, b\}$ vzhledem k $\{a, b, c\}$.

- ***Kartézský součin***: $A \times B = \{\langle a,b\rangle \mid a\in A, b\in B\}$, kde $\langle a,b\rangle$ je ***uspořádaná dvojice***, tj. množina dvou prvků, ve které ***záleží na pořadí.***
  Příklady: $\langle a,b\rangle = \langle c,d\rangle$ právě když $a = c, b = d$
  $\langle a,b\rangle \neq \langle b,a\rangle$, ačkoliv $\{a,b\} = \{b,a\}$

  Opět můžeme učinit zobecnění: Kartézský součin množin $A_1 \times \ldots \times A_n$ je množina uspořádaných n-tic: $\{\langle a_1,a_2, \ldots, a_n\rangle \mid a_1\in A_1, a_2\in A_2, \ldots, a_n\in A_n,\}$.
  Jedná-li se o Kartézský součin jedné a téže množiny, tj. $A \times \ldots \times A$, pak užíváme také značení A^n.

- ***Potenční množina***: $2^A = \{B \mid B \subseteq A\}$, tj. množina všech podmnožin množiny A. Značíme je někdy také $P(A)$.
  Příklady: $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
  $2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
  $2^{\{a,b\} \times \{a\}} = \{\emptyset, \{\langle a,a\rangle\}, \{\langle b,a\rangle\}, \{\langle a,a\rangle, \langle b,a\rangle\}\}$

  Kolik prvků má množina 2^A?
  Je-li $|A|$ počet prvků (kardinalita) množiny A, pak 2^A má $2^{|A|}$ prvků (proto užíváme takové značení pro potenční množinu).

Nyní vyložíme (zatím na intuitivní úrovni), jaká je souvislost mezi teorií množin a predikátovou logikou 1. řádu. Zpřesnění pak provedeme poté, co v následující kapitole definujeme, co je to interpretace formulí PL^1 a vyložíme způsob vyhodnocování jejich pravdivosti.

V kapitole 3.1. jsme uvedli, že predikátové symboly jazyka slouží k označení vlastností individuí (nebo vztahů mezi individui) a proměnné k označení individuí v závislosti na jejich valuaci. Vlastnosti individuí zde považujeme právě za množiny.

Pozn.: V případě jazyka matematiky je to uspokojivé, avšak v případě „normálního" empirického jazyka je to jisté zjednodušení. Je však mimo rámec tohoto kurzu provést zpřesnění.

Tak například vlastnost čísla být prvočíslem je prostě množina prvočísel, tj. podmnožina množiny všech přirozených čísel. Vlastnost individua „být studentem" můžeme považovat prostě za množinu studentů, tj. podmnožinu všech individuí.

Nechť tedy P je nějaká množina, a jistý prvek. Nejprve si ukážeme, jak můžeme v jazyce PL^1 zapsat skutečnost, že prvek $a \in P$. Symbol P můžeme považovat za jednoargumentový predikátový symbol a skutečnost, že prvek a patří do množiny P, zapíšeme v jazyce PL^1 prostě takto: $P(a)$. Tedy prvek a splňuje podmínku (čili má vlastnost) P.

Sjednocení množin A a B, které jsme v jazyce teorie množin definovali jako

$$A \cup B = \{x \mid x \in A \textbf{ nebo } x \in B\}$$

definujeme v jazyce PL^1 takto:

$$A(x) \vee B(x).$$

Tato formule bude pravdivá pro všechna ohodnocení proměnné x taková, která mají vlastnost A nebo B, tedy patří do množiny A nebo do množiny B.

Podobně průnik

$$A \cap B = \{x \mid x \in A \textbf{ a } x \in B\}$$

definujeme v PL^1 formulí

$$A(x) \wedge B(x).$$

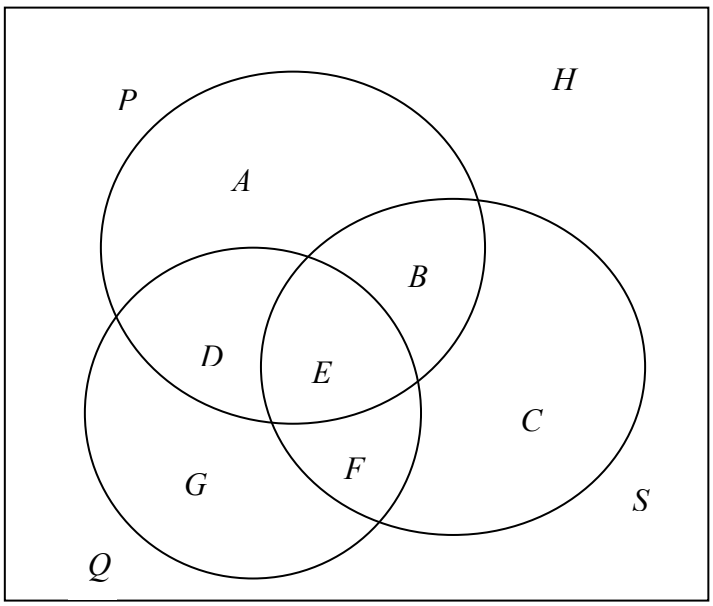
Rozdíl

$$A \setminus B = \{x \mid x \in A \text{ a } x \notin B\}$$

definujeme v PL^1 formulí

$$A(x) \wedge \neg B(x).$$

***Příklad 3.2.1*:** Definici množin v jazyce PL^1 nyní ilustrujeme následujícím obrázkem:



Celý obdélník na obrázku nechť je nějaké universum diskursu U.
Dále jsme znázornili tři podmnožiny universa, P, Q a S.
Vznikly nám tedy další podmnožiny universa, a to A, B, C, D, E, F, G a H.
Nyní definujeme tyto množiny jak v jazyce teorie množin, tak v jazyce PL^1:

A) množinově: $P \setminus (Q \cup S) = (P \setminus Q) \cap (P \setminus S)$
v jazyce PL^1: $P(x) \wedge \neg(Q(x) \vee S(x)) \Leftrightarrow P(x) \wedge \neg Q(x) \wedge \neg S(x)$

B) množinově: $(P \cap S) \setminus Q$
v jazyce PL^1: $P(x) \wedge S(x) \wedge \neg Q(x)$

C) množinově: $S \setminus (P \cup Q) = (S \setminus P) \cap (S \setminus Q)$
v jazyce PL^1: $S(x) \wedge \neg(P(x) \vee Q(x)) \Leftrightarrow S(x) \wedge \neg P(x) \wedge \neg Q(x)$

D) množinově: $(P \cap Q) \setminus S$
v jazyce PL^1: $P(x) \wedge Q(x) \wedge \neg S(x)$

E) množinově: $(P \cap Q \cap S)$
v jazyce PL^1: $P(x) \wedge Q(x) \wedge S(x)$

F) množinově: $(Q \cap S) \setminus P$
v jazyce PL^1: $Q(x) \wedge S(x) \wedge \neg P(x)$

G) množinově: $Q \setminus (P \cup S) = (Q \setminus P) \cap (Q \setminus S)$
v jazyce PL^1: $Q(x) \wedge \neg(P(x) \vee S(x)) \Leftrightarrow Q(x) \wedge \neg P(x) \wedge \neg S(x)$

H) množinově: $U \setminus (P \cup Q \cup S) = (U \setminus P \cap U \setminus Q \cap U \setminus S)$
v jazyce PL^1: $\neg(P(x) \vee Q(x) \vee S(x)) \Leftrightarrow \neg P(x) \wedge \neg Q(x) \wedge \neg S(x)$

Nyní si ukážeme, jak vyjádříme v jazyce PL^1 výše uvedené *vztahy* mezi množinami:

- Množina A je *podmnožinou* množiny B, značíme $A \subseteq B$, právě když každý prvek A je také prvkem B. Tedy $A \subseteq B$ zapíšeme v jazyce PL^1 takto: $\forall x\,[A(x) \supset B(x)]$
- Množina A je *vlastní podmnožinou* množiny B, značíme $A \subset B$, právě když každý prvek A je také prvkem B, ale *ne naopak*. V jazyce PL^1 zapíšeme tento vztah takto: $\forall x\,[A(x) \supset B(x)] \wedge \neg\forall x\,[B(x) \supset A(x)] \Leftrightarrow \forall x\,[A(x) \supset B(x)] \wedge \exists x\,[B(x) \wedge \neg A(x)]$

Pozn.: Řekli jsme, že množina je soubor (jakýchkoli) prvků. V případě konečného počtu prvků můžeme zapsat danou množinu prostě výčtem jejích prvků, např. $\{a, b, c, d\}$.

V případě *nekonečného* počtu prvků však nekonečný výčet takto zapsat nelze. Musíme zadat množinu nějakým pravidlem, jak ji vytvořit z již známých prvků. Např. nekonečnou množinu kladných celých čísel zapíšeme takto: $\{x \mid x \in \boldsymbol{N} \text{ a } x > 0\}$. Přitom předpokládáme, že víme, co je to množina přirozených čísel, číslo 0 a relace být větší >. Tedy není pravda, že každý (tj. libovolným způsobem *zadaný*) soubor prvků lze považovat za množinu.

Souvisí to se známým ***Rusellovým paradoxem***.

Sir Bertrand Arthur William Russell (1872 – 1970) byl významný britský matematik, filosof, logik a spisovatel, nositel Nobelovy ceny za literaturu za rok 1950. V matematice je znám svým paradoxem v naivní teorii množin.

Paradox se dá zjednodušeně vyložit takto:
Normální je, že množina a její prvky jsou objekty různých typů. Tedy „normální množina“ není prvkem sebe sama. Nechť tedy η je množina ***všech*** normálních množin:

$$\eta = \{M \mid M \notin M\}.$$

Nyní si však Russell položil otázku: Je $\eta \in \eta$?

Pokud zní odpověď Ano, tj. $\eta \in \eta$, pak dle zadání platí, že η je normální, tj. $\eta \notin \eta$.

Pokud zní odpověď Ne, tj. $\eta \notin \eta$, pak η je normální a patří do η, tj. $\eta \in \eta$.

Obě odpovědi vedou ke sporu, jedná se o „špatné zadání“, které nezadává takový soubor prvků, jenž bychom mohli považovat za množinu.

Cvičení ke kapitole 3.2.1.

Dokažte výše uvedená tvrzení:

a) $A \subset B$, právě když $A \subseteq B$ a $A \neq B$

b) $A \subseteq B$, právě když $A \cup B = B$ nebo $A \cap B = A$

Návod: Vyjádřete tyto vztahy v jazyce PL^1 a proveďte důkaz pomocí ekvivalentních úprav s využitím de Morganových zákonů a zákonů pro výrokovou logiku.

3.2.2. Základy teorie relací a funkcí

Opět zásadní otázka: Co je to relace? Studenti většinou odpoví, "no, nějaký vztah". Taková odpověď nám však nepostačuje, protože pak následuje otázka "a co je to vztah?" Potřebujeme přesnou definici. Je pravda, že v predikátové logice 1. řádu pojmy relace a vztah v podstatě ztotožňujeme, což je opět jisté zjednodušení či nepřesnost. Ovšem výklad rozdílu mezi relací a vztahem je nad rámec možností predikátové logiky (i vyšších řádů). Potřebovali bychom k tomu logiku intenzionální, a to je již jiná kapitola. Spokojíme se tedy s tím, že pojmy vztah a relace budeme ztotožňovat. Přesněji, budeme mluvit pouze o relacích.

Binární relace R mezi množinami A, *B* je podmnožina kartézského součinu $A \times B$:

$$R \subseteq A \times B$$

Jak jsme již uvedli, kartézský součin $A \times B$ je množina všech uspořádaných dvojic $\langle a, b \rangle$, kde $a \in A$, $b \in B$.

Binární relace S na množině M je pak podmnožina Kartézského součinu $M \times M$:

$$S \subseteq M \times M.$$

Příklady:

a) Binární relace na množině přirozených čísel ***N*** být ostře menší (<) je množina dvojic: $\{\langle 0,1\rangle,\langle 0,2\rangle,\langle 0,3\rangle,\ldots,\langle 1,2\rangle,\langle 1,3\rangle, \langle 1,4\rangle, \ldots, \langle 2,3\rangle,\langle 2,4\rangle,\ldots,\langle 3,4\rangle,\ldots,\langle 5,7\rangle,\ldots,\langle 115,119\rangle, \ldots.\}$
Tedy např. dvojice $\langle 5,7\rangle \in <$, dvojice $\langle 8,3\rangle \notin <$.

Přitom jsme použili zápis v jazyce teorie množin. Obvykle však píšeme $5<7$, $\neg(8<3)$. Používáme tedy jazyk predikátové logiky v infixní notaci. Obecně však můžeme zapsat skutečnost, že např. dvojice $\langle a, b \rangle$ patří do relace *R* prefixním způsobem, tedy *R(a,b)*.

b) Binární relace mezi množinami $\{a,b,c,d\}$ a $\{1,2,3\}$ může být např. množina těchto dvojic: $\{\langle a,1\rangle,\langle c,2\rangle,\langle d,3\rangle\}$.

c) Binární relace *R* (mít rád) mezi množinami {Petr, Marie, Jan, Tom} a {Alík, Minka, Milka} je např. množina {⟨Marie, Minka⟩, ⟨Tom, Alík⟩, ⟨Jan, Alík⟩}. Tedy Marie má ráda (kočičku) Minku, Tom a Jan mají rádi (pejska) Alíka, Petr nemá rád nic z druhé množiny a (čokoládu) Milku nemá rád nikdo z první množiny.

Definici můžeme snadno zobecnit na Kartézský součin *n* množin, dostaneme *n*-ární relaci P^n mezi množinami $A_1,\ldots,A_n$:

$$P^n \subseteq A_1 \times \ldots \times A_n$$

n-ární relace R^n na množině *M*:

$$R^n \subseteq M \times \ldots \times M$$

Je to množina *n*-tic prvků množiny *M*.

Příklad:

a) Ternární relace na $\boldsymbol{N}$:
$\{\langle 0,0,0\rangle,\langle 1,0,1\rangle,\langle 1,1,0\rangle,\ldots, \langle 2,0,2\rangle, \langle 2,1,1\rangle,\langle 2,2,0\rangle, \ldots, \langle 3,0,3\rangle, \langle 3,1,2\rangle, \langle 3,2,1\rangle,\langle 3,3,0\rangle,\ldots,\langle 115,110,5\rangle, \ldots.\}$
Je to množina trojic přirozených čísel takových, že 1. číslo je větší než druhé a 3. číslo je rozdíl 1. číslo minus 2. číslo.

b) Relace „adresa osoby“: {⟨Jan Novák, Praha 5, Bellušova 1831⟩, ⟨Marie Duží, Praha 5, Bellušova 1827⟩,...,}

Funkce je také relace. Avšak ne každá relace je funkce. Aby daná relace byla funkcí, musí být „zprava jednoznačná“.

Přesněji: *n-ární funkce F* je $(n+1)$-ární relace mezi množinami $A_1,\ldots,A_n, B$, tedy

$$F \subseteq A_1 \times ... \times A_n \times B$$

taková, že platí

$$\forall a_1 \ldots a_n \forall b \ \forall c \ [((F(a_1,\ldots,a_n,b) \wedge (F(a_1,\ldots,a_n,c)) \supset b=c]$$

kde $a_1 \in A_1,\ldots, a_n \in A_n, b,c \in B$.

Tedy ke každé *n-tici* prvků $a_1,\ldots,a_n$ existuje *nanejvýš jeden* prvek $b \in B$ takový, že $(F(a_1,\ldots,a_n,b)$. Říkáme také, že takováto funkce je *zobrazení* z $A_1 \times ... \times A_n$ do b. Značíme

$$F: A_1 \times ... \times A_n \rightarrow B.$$

Množinu $A_1 \times ... \times A_n$ nazýváme *definiční obor (doména)* funkce F, množinu B pak *obor hodnot (range)*. Místo $F(a_1,\ldots,a_n,b)$ píšeme $F(a_1,\ldots,a_n) = b$.

Všimněme si, že nyní jsme definovali funkci, která každému prvku ze svého definičního oboru přiřazuje *nanejvýš* jeden prvek z oboru hodnot. Může se tedy stát, že nějaký prvek dané domény nemá *žádný obraz* v oboru hodnot funkce. Takovéto funkce nazýváme *parciální*.

Příklad:

Funkce *Minus* (odečítání) je na množině *přirozených čísel parciální*. Toto zobrazení typu $\boldsymbol{N} \times \boldsymbol{N} \rightarrow \boldsymbol{N}$ některým dvojicím přirozených čísel nepřiřadí žádné přirozené číslo. Budou to ty dvojice, ve kterých je první prvek menší než druhý, neboť jejich rozdíl je číslo záporné, tedy to není číslo přirozené.

Funkce *Minus* je však *totální* na množině $\boldsymbol{C}$ *celých* čísel. Zobrazení *Minus*: $\boldsymbol{C} \times \boldsymbol{C} \rightarrow \boldsymbol{C}$ přiřadí každé dvojici $\langle m,n\rangle$ obraz v $\boldsymbol{C}$, totiž číslo *Minus*$(\langle m,n\rangle)$, značíme $m - n$. Např. dvojici $\langle 3,5\rangle$ přiřadí funkce číslo –2, neboť 3 – 5 = –2.

Funkce *Dělení* je na množině $\boldsymbol{C}$ *celých* čísel *parciální.* Zobrazení *Dělení*: $\boldsymbol{C} \times \boldsymbol{C} \rightarrow \boldsymbol{C}$ některým dvojicím $\langle m,n\rangle$ nepřiřadí žádné číslo z $\boldsymbol{C}$, neboť např. 2:5 = 0,4 a číslo 0,4 není celé číslo, je to číslo racionální.

Funkce *Dělení* je však *totální* na množině $\boldsymbol{R}$ čísel *racionálních.* Zobrazení *Dělení*: $\boldsymbol{R} \times \boldsymbol{R} \rightarrow \boldsymbol{R}$ přiřadí *každé* dvojici racionálních čísel $\langle m,n\rangle$ nějaké racionální číslo z $\boldsymbol{R}$, totiž podíl $m:n$.

Jak uvidíme v další kapitole, predikátová logika pracuje pouze s *totálními* funkcemi. Proto definujeme:

Funkce F: $A_1 \times ... \times A_n \rightarrow B$ je *totální*, jestliže toto zobrazení přiřadí *každému* prvku z $A_1 \times ... \times A_n$ *právě jeden* prvek z *B*. Formálně,

$$\forall a_1 \ldots a_n \forall b \; \forall c \; \{[((F(a_1,\ldots,a_n,b) \wedge (F(a_1,\ldots,a_n,c)) \supset b{=}c] \wedge$$
$$\forall a_1 \ldots a_n \exists b \; F(a_1,\ldots,a_n,b)\}$$

Často také potřebujeme rozlišit různé typy (totálních) funkcí, tj. zobrazení. Proto ***definujeme***:

- Zobrazení f: A $\rightarrow$ B je ***surjekce*** (neboli zobrazení A ***na*** B), jestliže k libovolnému prvku $b \in$ B existuje vzor $a \in$ A takový, že $f(a) = b$. Formálně:
$$\forall b \; [\mathrm{B}(b) \supset \exists a \; (\mathrm{A}(a) \wedge f(a){=}b)]$$
- Zobrazení f: A $\rightarrow$ B je ***injekce*** (neboli ***prosté*** zobrazení A ***do*** B), jestliže pro všechny prvky $a \in$ A, $b \in$ B takové, že $a \neq b$ platí, že $f(a) \neq f(b)$. Formálně:
$$\forall a \forall b \; [(\mathrm{A}(b) \wedge \mathrm{A}(a) \wedge (a \neq b)) \supset (f(a) \neq f(\mathrm{b}))]$$
- Zobrazení f: A $\rightarrow$ B je ***bijekce*** (neboli ***prosté*** zobrazení A ***na*** B), jestliže f je surjekce a injekce.

Bijekce, neboli také *vzájemně jednoznačné zobrazení* je důležitý typ zobrazení, neboť pomocí bijekce lze jednak definovat *izomorfismus* mezi dvěma strukturami (jak ukážeme v Kap. 4) a navíc stejnou kardinalitu dvou množin.

3.2.2.1. Spočetné a nespočetné množiny

Kardinalita konečných množin je počet jejich prvků. Jak je to však v případě nekonečných množin? Zde nemůžeme mluvit prostě o počtu prvků. Nejprve však definujeme, kdy je množina nekonečná:

Množina A je *nekonečná*, jestliže existuje bijekce na její vlastní podmnožinu.

Tak např. množina přirozených čísel ***N*** je nekonečná, neboť existuje bijekce na její vlastní podmnožinu ***S*** sudých čísel: $f(n) = 2n$. Jedná se o jeden z malých paradoxů teorie množin, neboť množina sudých čísel je vlastní podmnožinou množiny přirozených čísel, $\boldsymbol{S} \subset \boldsymbol{N}$.

V případě nekonečných množin sice nemůžeme hovořit o počtu prvků, můžeme však porovnávat jejich *kardinalitu* (neboli *mohutnost*) právě pomocí bijekce. Jistě, existuje-li bijekce, neboli vzájemně jednoznačné zobrazení množiny A na množinu B (a obráceně, neboť ke každé bijekci existuje inverzní zobrazení, které je také bijekce), pak řekneme, že množiny A, B mají *stejnou kardinalitu* neboli mohutnost: *Card(A) = Card (B)*.

Jelikož základní a jistým způsobem nejjednodušší nekonečná množina je množina přirozených čísel ***N***, porovnáváme kardinalitu nekonečných množin s touto množinou, a ***definujeme***:

Množina *A*, pro kterou existuje bijekce $A \rightarrow \boldsymbol{N}$ (tedy *A* má stejnou kardinalitu jako množina ***N***), se nazývá nekonečně *spočetná*.

Pozn.: Konečné množiny se rovněž považují za (triviálně) spočetné.

Spočetná množina je tedy taková množina, jejíž prvky lze očíslovat, tj. seřadit do prosté posloupnosti (ve které se prvky neopakují). Specielně, každá nekonečná podmnožina spočetné množiny je spočetná. Důkaz těchto dvou tvrzení ponecháváme na čtenáři.

Příklad:

- **Množina *S* sudých přirozených čísel je spočetná**: *Card(**S**) = Card(**N**).*

  Bijekce *f: **N*** na ***S*** je definována předpisem *f(n) = 2n.* Inverzní bijekce f^{-1}: ***S*** na ***N*** je definována jako $f^{-1}(n) = n/2$.

- **Množina *Z* celých čísel je spočetná:** *Card(**Z**) = Card(**N**).*

  Množinu ***Z*** očíslujeme např. takto:

  f(0)=0, f(1)= –1, f(2)= 1, f(3)= –2, f(4)= 2, f(5)= –3, f(6) = 3, …

  Tedy bijekce *f*: $\boldsymbol{Z} \rightarrow \boldsymbol{N}$ je dána tímto předpisem: $f(n) = (-1^n)[(n+1)/2]$, kde $[x]$ značí celou část (racionálního) čísla *x*.

- **Kartézský součin $\boldsymbol{N} \times \boldsymbol{N}$ je rovněž spočetná množina**. Její prvky očíslujeme např. takto:

  1 2 3 4 5 6 …
  ⟨1,1⟩ ⟨2,1⟩ ⟨1,2⟩ ⟨3,1⟩ ⟨2,2⟩ ⟨1,3⟩ …

  Totiž Kartézský součin, tj. množinu všech možných uspořádaných dvojic přirozených čísel, si můžeme znázornit dvourozměrnou tabulkou:

⟨1,1⟩	⟨1,2⟩	⟨1,3⟩	⟨1,4⟩	…
⟨2,1⟩	⟨2,2⟩	⟨2,3⟩	⟨2,4⟩	…
⟨3,1⟩	⟨3,2⟩	⟨3,3⟩	⟨3,4⟩	…
⟨4,1⟩	⟨4,2⟩	⟨4,3⟩	⟨4,4⟩	…
…	…	…	…	…

  Prvky tabulky číslujeme „cik-cak“

- Obecně, jsou-li *A* a *B* spočetné množiny, pak $\boldsymbol{A} \times \boldsymbol{B}$ **je rovněž spočetná množina**.
  Důkaz: jelikož *A*, *B* jsou spočetné, můžeme jejich prvky seřadit do posloupností
  $A = \{a_1, a_2, \ldots, a_n\}$, $b = \{b_1, b_2, \ldots, b_n\}$
  Nyní je snadné sestrojit bijekci *f*: $\boldsymbol{A} \times \boldsymbol{B} \rightarrow \boldsymbol{N} \times \boldsymbol{N}$, a to takto:
  $f\langle a_1,b_1\rangle = \langle 1,1\rangle$, $f\langle a_2,b_1\rangle = \langle 2,1\rangle$, $f\langle a_1,b_2\rangle = \langle 1,2\rangle$, $f\langle a_3,b_1\rangle = \langle 3,1\rangle$, …
  Obecně tedy $f\langle a_n,b_m\rangle = \langle n,m\rangle$.
  Jelikož je $\boldsymbol{N} \times \boldsymbol{N}$, spočetná, existuje bijekce *g*: $\boldsymbol{N} \times \boldsymbol{N} \rightarrow \boldsymbol{N}$. Složení *gf* obou bijekcí je pak bijekce $\boldsymbol{A} \times \boldsymbol{B} \rightarrow \boldsymbol{N}$.

- **Množina racionálních čísel *Q* je** (překvapivě) rovněž **spočetná**: *Card(**Q**) = Card(**N**).*
  Důkaz tohoto tvrzení není již tak triviální jako v předchozích příkladech. Nejprve potřebujeme definovat, kdy je kardinalita jedné množiny menší nebo rovna kardinalitě druhé množiny.
  Definice je jednoduchá:

  Mějme množiny *A*, *B*. Pak *Card (A)* ≤ *Card (B)* právě když existuje *injekce* (čili prosté zobrazení) z množiny *A* do množiny *B*.

  Dále budeme potřebovat *Cantor-Bernstein*ovu větu, která říká, že jestliže $|A| \leq |B|$ *a* $|B| \leq |A|$, pak $|A| = |B|$. Jinými slovy, jestliže existuje injekce *f*: $A \rightarrow B$ a zároveň injekce *g*: $B \rightarrow A$, pak existuje *bijekce h*: $A \rightarrow B$.

Ačkoliv se toto tvrzení zdá být zcela zřejmé, jeho důkaz je poměrně složitý a nebudeme jej zde prezentovat. Zájemci však mohou najít poměrně přehlednou verzi důkazu zde: http://www.cut-the-knot.org/WhatIs/Infinity/Bernstein.shtml.[2]

Nyní můžeme podat *důkaz* tvrzení, že *Card(**Q**) = Card(**N**)*.

a) $|\boldsymbol{N}| \leq |\boldsymbol{Q}|$, neboť každé přirozené číslo je racionální, tedy existuje injekce $\boldsymbol{N}$ do $\boldsymbol{Q}$.

b) Nyní chceme dokázat, že $|\boldsymbol{Q}| \leq |\boldsymbol{N}|$. Uděláme to opět v několika krocích:

- Především, jelikož množina celých čísel $\boldsymbol{Z}$ je spočetná, je spočetná také množina $\boldsymbol{Z} \times \boldsymbol{N}$. Injekci $\boldsymbol{Q}$ do $\boldsymbol{Z} \times \boldsymbol{N}$ dostaneme tak, že každému racionálnímu číslu a/b přiřadíme dvojici $\langle a,b \rangle$.
- Tedy $|Q| \leq |\boldsymbol{Z} \times \boldsymbol{N}| = |\boldsymbol{N}|$, tj. $|\boldsymbol{Q}| \leq |\boldsymbol{N}|$

c) Dle Cantor-Bernsteinovy věty je $|\boldsymbol{Q}| = |\boldsymbol{N}|$

Existují však *nespočetné množiny*, které nelze bijektivně zobrazit na množinu přirozených čísel. Všeobecně přijímaná hypotéza je, že ***nejmenší nespočetná množina je množina reálných čísel***. Dá se ukázat, že již v intervalu $\langle 0,1 \rangle$ je reálných čísel „více než“ je všech přirozených, ale „stejně mnoho“ jako všech reálných čísel!

Cantorův diagonální důkaz:

Jedná se o důkaz sporem. Předpokládejme tedy, že existuje bijekce f z množiny $\boldsymbol{N}$ *na* množinu *všech* reálných čísel v intervalu $\langle 0,1 \rangle$, tedy že reálných čísel je v tomto intervalu spočetně mnoho. Každé z těchto čísel je tvaru $0,i_1i_2i_3\ldots$, kde $i_1i_2i_3\ldots$ je desetinný rozvoj čísla. Můžeme tedy tato čísla uspořádat do tabulky, která bude vypadat např. takto:

n	*f(n)*								
1	0,	**3**	1	4	1	5	9	…	π/10
2	0,	3	**7**	3	7	3	7	…	37/99
3	0,	1	4	**2**	8	5	7	…	1/7
4	0,	7	0	7	**1**	0	6	…	√2/2
5	0,	3	3	3	3	**3**	3	…	1/3
…	…								

Vezměme nyní cifry, které leží v diagonále (v tabulce jsou zvýrazněny tučně) a ke každé přičteme 1. Pokud je touto cifrou 9, nahradíme ji nulou. Např. v našem případě jsme z čísla 0,37213… získali číslo 0,48324… Může se toto číslo nacházet v tabulce? Nemůže. Jeho první desetinná cifra je různá od první desetinné cifry čísla *f(1)*, druhá je různá od druhé desetinné cifry čísla *f(2)*, atd. Čili toto nové číslo se nemůže rovnat žádnému *f(n)* pro žádné *n*, tedy v tabulce se nenachází. To je ovšem spor s předpokladem, že *f* je bijekce, tj. zobrazení *na* množinu *všech* čísel z intervalu $\langle 0,1 \rangle$.

[2] A. Bogomolny: *A short "about" (from Interactive Mathematics Miscellany and Puzzles)*. ***http://www.cut-the-knot.org/wanted.shtml***, Accessed 03 September 2015

Důkaz, který jsme zde ilustrovali je aplikací obecnějšího ***Cantorova diagonálního argumentu***, pomocí kterého Cantor dokázal jednu z nejvýznamnějších vět Cantorovy teorie množin. Abychom ji formulovali, musíme definovat:

> Kardinalita množiny M je ostře menší než kardinalita množiny N, $Card\ (M) < Card(N)$, právě když existuje injekce f z M do N a neexistuje bijekce M na N.

Cantorův teorém: Množina všech podmnožin $P(M)$ množiny M má kardinalitu ostře větší než M, tj. $Card\ (M) < Card\ P(M)$.

Důkaz:
Nechť f: $M \rightarrow P(M)$ je injekce a definujeme $X = \{a \in M \mid a \notin f(a)\}$. Zřejmě $X \subseteq M$, tedy $X \in P(M)$. Kdyby f byla bijekce, musel by existovat prvek $b \in M$ takový, že $X = f(b)$. Pak ale buď $b \in X$ nebo $b \notin X$. Pokud $b \in X$, pak dle definice X platí, že $b \notin X$. Naopak, jestliže $b \notin X$, pak dle definice X platí, že $b \in X$. V obou případech dojdeme ke sporu, tedy takový prvek b neexistuje, tj. zobrazení f nemůže být bijekce *na* $P(M)$.

Pozn.: V důkazu zmíněnou injekci zkonstruujeme snadno. Stačí zobrazit každý prvek m množiny M na jednoprvkovou množinu $\{m\}$.

Z tohoto teorému pak plyne jako důsledek jiný důkaz nespočetnosti množiny R reálných čísel, neboť R se dá ztotožnit s množinou všech podmnožin množiny přirozených čísel N.

Dalším důsledkem je pak to, že dostáváme vzrůstající nekonečnou posloupnost kardinalit množin: $N < P(N) < P(P(N)) < P(P(P(N))) < ...$

Cvičení ke kapitole 3.2.2.

1) *Rozhodněte*, zda jsou následující relace funkcemi, případně jakými. Budeme pracovat s množinami $A=\{a_1,a_2,a_3,a_4\}$, $B=\{b_1,b_2,b_3\}$ a $C=\{c_1,c_2,c_3\}$ jejichž prvky jsou různé.

a) $R \subseteq A \times B$, $R = \{\langle a_1,b_3\rangle, \langle a_2,b_2\rangle, \langle a_1,b_1\rangle\}$

b) $R \subseteq B \times A$, $R = \{\langle b_1,a_4\rangle, \langle b_2,a_4\rangle, \langle b_3,a_4\rangle\}$

c) $R \subseteq A \times C$, $R = \{\langle a_1,c_2\rangle, \langle a_2,c_3\rangle, \langle a_3,c_1\rangle\}$

d) $R \subseteq A \times B$, $R = \{\langle a_1,b_1\rangle, \langle a_2,b_2\rangle, \langle a_3,b_3\rangle, \langle a_4,b_3\rangle\}$

e) $R \subseteq B \times A$, $R = \{\langle b_1,a_3\rangle, \langle b_2,a_2\rangle, \langle b_3,a_1\rangle\}$

f) $R \subseteq A \times B \times C$, $R=\{\langle a_1,b_1,c_1\rangle, \langle a_2,b_2,c_1\rangle, \langle a_1,b_2,c_3\rangle\}$

2)

a) Je funkce druhá mocnina (x^2) na množině přirozených čísel totální?

b) Na jaké množině je funkce druhá odmocnina ($\sqrt{x}$) totální?

3) *Vyjádřete slovně* následující skutečnosti za předpokladu, že predikát P znamená „mít rád“ (kdo, koho), individuová konstanta m znamená Marie a individuová konstanta k Karel.

a) $\exists x \exists y\, P(x,y)$

b) $\exists x \forall y\, \mathrm{P}(x,y)$

c) $\exists y \forall x\, P(x,y)$

d) $\forall x \exists y\, P(x,y)$

e) $\forall x \forall y\, \mathrm{P}(x,y)$

f) $\forall x\, P(x,m)$

g) $\forall y\, P(k,y)$

3.3. Interpretace a modely

Po těchto neformálních úvodních kapitolách nyní budeme definovat všechny pojmy potřebné pro sémantický výklad predikátové logiky 1. řádu, o kterých jsme až dosud mluvili na intuitivní úrovni, formálně a přesně.

Definice 3.3.1 (*Interpretace*): *Interpretace jazyka predikátové logiky 1. řádu* je tato trojice objektů (která je někdy nazývána *interpretační struktura*):

A) *Neprázdná* množina U, 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 (*totální funkci*) f^U: $U^n \to U$.

C) *Interpretace predikátových symbolů* jazyka, která přiřazuje každému n-árnímu predikátovému symbolu P jistou n-ární relaci P^U nad U, tj. $P^U \subseteq U^n$.

Poznámky:

1. Každý n-ární funkční symbol je tedy interpretován jako funkce, která přiřazuje n-tici individuí právě jedno individuum, tj. zobrazení z $U \times ... \times U$ do U. Specielně:
   - je-li $n = 0$, pak se jedná o nulární funkční symbol, tedy o *individuovou konstantu*, které je interpretací 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 funkce druhá mocnina x^2, funkce následník $x + 1$, nad množinou živých individuí funkce (biologický) otec, (biologická) matka, atd.)
   - je-li $n = 2$, pak se jedná o binární funkční symbol, kterému je přiřazena binární funkce se dvěma argumenty (např. nad množinou čísel funkce sčítání $x+y$, funkce násobení $x \,.\, y$, atd.)
2. Každý n-ární predikátový symbol P je interpretován jako n-ární relace P^U. Tato relace P^U se nazývá *obor pravdivosti* predikátu P. 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 U. (Jak jsme již zmínili, vlastnosti 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, mít rád, 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 3.3.1:
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 U je množina všech nezáporných celých čísel {0, 1, 2,...}.
- Interpretace funkčních symbolů jsou definovány takto:

  f_0 ... konstanta: číslo 0 (nikoliv pravdivostní hodnota)
  f_1 ... individuová konstanta: číslo 1 (nikoliv pravdivostní hodnota)
  g ... zobrazení $U \to U$ definované takto: $g(x) = x + 1$ (tj. funkce následník)
  h ... zobrazení $U \times U \to U$ definované takto: $h(x, y) = x + y$ (tj. funkce sčítání)
  k ... zobrazení $U \times U \to U$ definované takto: $k(x, y) = x \,.\, y$ (tj. funkce násobení)

- Interpretace predikátových symbolů jsou definovány takto:
  P ... podmnožina množiny $U \times U$ definovaná jako množina všech dvojic $\langle x,y \rangle$, pro které platí $x = y$
  Q ... podmnožina množiny $U \times U$ 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 zápisu

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

který využívá speciální infixovovou notaci binárních funkcí a další konvence jazyka matematiky (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

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

neboli standardně s využitím konvencí jazyka matematiky

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

Definice 3.3.2 (*ohodnocení termů*):

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

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

$$e^*(x) = e(x)$$

$$e^*(f(t_1, t_2, ..., t_n)) = f^U (e^*(t_1), e^*(t_2),...,e^*(t_n)),$$

kde f^U 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 3.3.3 (*vyhodnocení pravdivosti formule*):
Pravdivost formule A v interpretaci I pro ohodnocení e individuových proměnných (což značíme $\models_I A[e]$ a čteme formule A je splněna v interpretaci 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 $\langle e^*(t_1), e^*(t_2),...,e^*(t_n)\rangle \in P^U$, kde P^U je relace přiřazená interpretací I symbolu P, tj. obor pravdivosti P. Tedy individua, která jsou hodnotou termů $t_1, \ldots, t_n$, jsou v relaci P^U.
   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 3.3.1, 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 $\in U$ platí $\models_I B[e(x/\mathrm{i})]$, kde $e(x/\mathrm{i})$ 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 $\in U$ platí $\models_I B[e(x/\mathrm{i})]$, kde $e(x/\mathrm{i})$ 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:
$$\forall x\, A(x) \Leftrightarrow A(a_1) \wedge \ldots \wedge A(a_n)$$
$$\exists x\, A(x) \Leftrightarrow A(a_1) \vee \ldots \vee A(a_n).$$
Tedy všeobecný kvantifikátor je zobecněním konjunkce pro nekonečné universum a existenční kvantifikátor je zobecněním disjunkce pro nekonečné universum diskursu.
2) Z definice kvantifikátorů je navíc zřejmé, že platí *de Morganovy zákony* tak, jak jsme je poznali v kapitole 3.1:
$$\forall x\, A(x) \Leftrightarrow \neg\exists x\, \neg A(x),$$
$$\exists x\, A(x) \Leftrightarrow \neg\forall x\, \neg A(x).$$

Definice 3.3.4 (*splnitelnost a pravdivost*):

- *Formule A je splnitelná v interpretaci I*, jestliže *existuje* ohodnocení *e* proměnných takové, že platí $\models_I A[e]$.
- *Formule A je splnitelná*, jestliže existuje interpretace I a ohodnocení proměnných *e* takové, že $\models_I A[e]$.
- *Formule A je pravdivá v interpretaci I*, značíme $\models_I A$, jestliže pro *všechna* možná ohodnocení *e* individuových proměnných platí, že $\models_I A[e]$.
- *Formule A je tautologií* (*logicky pravdivá*), značíme $\models A$, jestliže je pravdivá v každé interpretaci I (tj. pro všechna ohodnocení *e*).
- *Formule A je kontradikcí*, jestliže neexistuje interpretace I ani ohodnocení proměnných *e*, pro které by byla formule *A* pravdivá, tj. formule *A* není splnitelná v žádné interpretaci I, je *nesplnitelná.*
- *Model formule A* je interpretace I, ve které je *A* pravdivá.
- *Model množiny formulí* $\{A_1,\ldots,A_n\}$ je taková interpretace I, ve které jsou pravdivé *všechny* formule $A_1,\ldots,A_n$.

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

Definice 3.3.5 (*logické vyplývání*):
Formule B logicky vyplývá z formulí $A_1,\ldots,A_n$, značíme $A_1,\ldots,A_n \models B$, jestliže *B* je pravdivá v každém modelu množiny formulí $A_1,\ldots,A_n$.

Důsledek: Tedy pro každou interpretaci I, ve které jsou pravdivé formule $A_1,\ldots,A_n$ (tj. $\models_I A_1,\ldots, \models_I A_n$) platí, že je v ní pravdivá také formule *B* ($\models_I B$).

Pozn.: Kdyby byl *model* formule definován jako interpretace I a valuace *e*, pro kterou je tato formule splněna (tedy $\models_I A[e]$), pak také definice *logického vyplývání* v rámci PL^1 by musela být příslušně upravena:

> $A_1,\ldots,A_n \models B$, jestliže pro každou interpretaci I a valuaci *e*, která splňuje všechny předpoklady $A_1,\ldots,A_n$ (tj. platí $\models_I A_1[e]$, …, $\models_I A_n[e]$), platí současně, že je splněn i závěr *B* (tj. $\models_I B[e]$).

Jestliže *B* vyplývá z $\{A_1,\ldots,A_n\}$ podle této "silnější" definice, pak vyplývá i podle definice 3.3.5, ale ne naopak! Uvedené definice nejsou ekvivalentní. Např. podle definice 3.3.5 platí, že

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

avšak podle této silnější definice to neplatí. Tedy takováto silnější definice je jistým způsobem přesnější, neboť formule $P(x) \supset \forall x\, P(x)$ není tautologií. Historicky se však vžila definice v podobě 3.3.5, a také my ji budeme používat. Musíme si však být vědomi rozdílu mezi oběma definicemi.

Pro *otevřené* formule s volnými proměnnými tedy *neplatí sémantická věta o dedukci*:

$$A_1,\ldots,A_n \models B \Leftrightarrow \models (A_1 \wedge \ldots \wedge A_n) \supset B$$

Pro uzavřené formule však obě definice splývají, neboť pravdivost uzavřené formule *A* v interpretaci I nezávisí dle bodu 3 definice 3.3.3 na valuaci proměnných. (Proto také bývají speciální axiómy teorie voleny pouze jako uzavřené formule, tzv. *sentence,* viz kapitola 4.)

Příklad 3.3.2: Uvažujme jazyk predikátové logiky a jeho interpretaci, tak jak byly popsány v příkladu 3.3.1.

Formule $P(h(x,y), x))$, neboli $x+y = x$ je splněna v uvedené interpretaci např. ohodnocením 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 $P(h(x,y), h(y,x))$, neboli $x+y = y+x$ je v uvedené interpretaci splněna každým ohodnocením a je tedy v této interpretaci pravdivá. Není to však logicky pravdivá formule: interpretujeme-li např. binární predikát P jako ostrou nerovnost, pak uvedená formule není v takové interpretaci pravdivá.

Totéž platí pro formuli $\forall x \forall y\ [P(h(x,y), h(y,x))]$, neboli $\forall x \forall y\ (x+y = y+x)$. Formule je pravdivá v této interpretaci. Není však to však logicky pravdivá formule: interpretujeme-li např. binární predikát P jako ostrou nerovnost, pak uvedená formule není v této interpretaci nepravdivá.

Formule $\forall x \exists y\ Q(x,y)$, neboli $\forall x \exists y\ (x < y)$ je pravdivá v dané interpretaci.

Formule $\forall y \exists x\ Q(x,y)$, neboli $\forall y \exists x\ (x < y)$ je nesplnitelná v dané interpretaci jazyka predikátové logiky, neboť valuace $e(y) = 0$ formuli nesplňuje.

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 logicky pravdivé (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 logicky pravdivé. Jejich pravdivost nezávisí na tom, jakou množinu probíhají individuové proměnné (čili jaké volíme universum U), jak je interpretován funkční symbol g a jak je interpretován predikátový symbol P. Formule „má tvar“ tautologie výrokové logiky $p \vee \neg p$.

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, jsou to kontradikce.

Definice 3.3.6 (*ekvivalence formulí*):
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: Dvě formule jsou ekvivalentní právě tehdy, je-li formule $A \equiv B$ tautologií, tj.:

$$A \Leftrightarrow B \text{ právě tehdy, když } \models (A \equiv B).$$

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

Věta 3.3.1: Nechť A je formule výrokové logiky sestavená z výrokových symbolů $p_1,\ldots, p_n$ a nechť $B_1,\ldots,B_n$ jsou libovolné formule predikátové logiky. Nechť dále formule A' vznikne z formule A náhradami proměnných $p_1,\ldots, p_n$ po řadě formulemi $B_1,\ldots,B_n$. Potom platí: je-li A tautologií výrokové logiky, je A' tautologií (logicky pravdivou formulí) predikátové logiky.

Důkaz: Pravdivostní hodnota formule A nezávisí na pravdivostních hodnotách formulí $p_1,\ldots, p_n$ (neboť A je pravdivá pro všechny pravdivostní hodnoty těchto formulí). Proto ani pravdivostní hodnota formule A' nezávisí na pravdivostních hodnotách formulí $B_1,\ldots,B_n$ (v libovolné interpretaci).

Věta 3.3.2: Nechť platí, že
- formule A obsahuje podformule $B_1,\ldots,B_n$
- formule $B_1,\ldots,B_n$ jsou po řadě ekvivalentní s formulemi $B'_1,\ldots,B'_n$ (tj. $B_i \Leftrightarrow B'_i$)
- formule A' vznikne z formule A náhradami formulí $B_1,\ldots,B_n$ po řadě formulemi $B'_1,\ldots,B'_n$

Potom platí: je-li A logicky pravdivá formule predikátové logiky, je i A' logicky pravdivá formule.

Důkaz: Ve formuli A nahrazujeme podformule formulemi se stejným pravdivostním ohodnocením (pro všechny interpretace I a valuace e). Tedy pravdivostní ohodnocení formule A' musí být pro všechny interpretace I a valuace e stejné jako pravdivostní ohodnocení formule A. Je-li tedy A logicky pravdivá, je také A' logicky pravdivá.

***Příklad* 3.3.3 (*některé důležité tautologie predikátové logiky*)**:

Všechny formule predikátové logiky mající tvar tautologií výrokové logiky (viz věta 3.1.1) jsou logicky pravdivé. Např. formule $\forall x\ \mathrm{p}(x) \supset (\mathrm{q}(y) \supset \forall x\ \mathrm{p}(x))$ je logicky pravdivá, protože má tvar formule výrokové logiky $\mathrm{r} \supset (\mathrm{s} \supset \mathrm{r})$, která je tautologií výrokové logiky.

Dále nechť A, B jsou libovolné formule predikátové logiky a nechť term t je substituovatelný za proměnnou x. Pak

1. $\models \forall x\mathrm{A}(x) \supset \mathrm{A}(y)$ *dictum de omni* specielně
   $\models \forall x\mathrm{A}(x) \supset \mathrm{A}(x/t)$ pravidlo *konkretizace*
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. $\models [\forall x\mathrm{A}(x) \vee \forall x\mathrm{B}(x)] \supset \forall x\ [\mathrm{A}(x) \vee \mathrm{B}(x)]$
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. $\models \exists x\,[B(x) \supset A] \equiv [\forall x B(x) \supset A]$
15. $\models \forall x\,[A \wedge B(x)] \equiv [A \wedge \forall x B(x)]$
16. $\models \exists x\,[A \wedge B(x)] \equiv [A \wedge \exists x B(x)]$
17. $\models \forall x\,[A \vee B(x)] \equiv [A \vee \forall x B(x)]$
18. $\models \exists x\,[A \vee B(x)] \equiv [A \vee \exists x B(x)]$

Zákony komutace kvantifikátorů:

19. $\models \forall x \forall y A(x,y) \equiv \forall y \forall x A(x,y)$
20. $\models \exists x \exists y A(x,y) \equiv \exists y \exists x A(x,y)$
21. $\models \exists x \forall y A(x,y) \supset \forall y \exists x A(x,y)$

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 *P* je interpretován jako relace <. V této interpretaci je formule $\forall y \exists x P(x,y)$ pravdivá (ke každému *y* existuje *x* menší než *y*) a formule $\exists x \forall y P(x,y)$ nepravdivá (existuje *x*, které je menší než všechna *y*). Tedy formule $\forall y \exists x P(x,y) \supset \exists x \forall y P(x,y)$ 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 existenční generalizace***
24. $\models \forall x A(x) \supset \exists x A(x)$ ***zákon partikularizace***

***Poznámky*:**

1) Tautologie 3. a 4. vysvětlují, jak chápeme v PL^1 všeobecnost 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 ($U = \emptyset$). Formule $\forall x P(x)$ bude v této interpretaci 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 i formule $\exists x \neg P(x)$ (neboť žádné individuum, které by nemělo vlastnost *P*, neexistuje). 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 logicky pravdivé formuli 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, tj. valuací 0, 1 výrokových symbolů (jazyk výrokové logiky pracující s n výrokovými symboly má tedy 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 logicky pravdivá, či zda je daný úsudek platný, využíváme často tyto dvě metody:

   Ověření převodem na výrokovou logiku za předpokladu konečného univerza. Např. za předpokladu, že U={a,b}, pak tautologii

   $$\models \neg\forall x\, \mathrm{A}(x) \equiv \exists x\, \neg\mathrm{A}(x)$$

   lze ověřit takto:

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

   Množinový důkaz úvahou o oborech pravdivosti predikátů. Platí totiž:

   Je-li $\models_I \forall x\, P(x)$, pak $P^U = U$

   Je-li $\models_I \exists x\, P(x)$, pak $P^U \neq \emptyset$

   Je-li $\models_I \forall x\, [P(x) \supset Q(x)]$, pak $P^U \subseteq Q^U$

   Je-li $\models_I \exists x\, [P(x) \wedge Q(x)]$, pak $(P^U \cap Q^U) \neq \emptyset$

   Na ukázku ověřme 5. schéma tautologií z předchozího příkladu:

   $$\models \forall x\, [\mathrm{A}(x) \supset \mathrm{B}(x)] \supset [\forall x\mathrm{A}(x) \supset \forall x\mathrm{B}(x)]$$

1. $\forall x\, [\mathrm{A}(x) \supset \mathrm{B}(x)]$ předpoklad
   tj. obor pravdivosti A $\subseteq$ obor pravdivosti B
2. $\forall x\mathrm{A}(x)$ předpoklad
   tj. obor pravdivosti A = celé univerzum U
3. $\forall x\mathrm{B}(x)$ z 1.a 2.
   tj. obor pravdivosti B musí být také celé univerzum U

Sémantické ověření správnosti úsudku je v predikátové logice rovněž obtížnější než ve VL. Podle definice je úsudek správný, tj. platný, 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 sporem (tj. předpokládáme, že může nastat případ, kdy v nějaké interpretaci budou předpoklady pravdivé a závěr nepravdivý a ukážeme, že to možné není). Provedem to množinovými úvahami o oborech pravdivosti jednotlivých predikátů. Nejprve znázorníme množiny, které jsou modelem předpokladů. Pak ověříme, že je v těchto modelech pravdivý i závěr.

***Příklad* 3.3.4** (*Sémantické ověření správnosti úsudku*):

a)	Marie má ráda pouze vítěze.	$\forall x\,[R(m,x) \supset V(x)]$
	Karel je vítěz.	$V(k)$
	———	———
	Marie má ráda Karla.	$R(m,k)$

Aby byly předpoklady pravdivé, pak možné interpretace nad množinou D individuí i_1, i_2,…, Marie, Karel, …, i_n, … musí mít tvar:

1. Interpretace termů: 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.)
2. Interpretace predikátových symbolů:

$R^D \subseteq D \times D$: {… ⟨Marie, i_1⟩, ⟨Marie, i_2⟩, …, ⟨Marie, i_n⟩, …}
$V^D \subseteq D$: {…i_1, i_2, …, Karel,…, i_n,…}

Vidíme, že závěr z uvedených předpokladů logicky nevyplývá, neboť není zaručeno, že relace R^D bude obsahovat dvojici ⟨Marie, Karel⟩. To, že někdo je vítěz, *není postačující podmínkou* toho, aby jej Marie měla ráda, pouze podmínkou *nutnou.* Úsudek je *neplatný.*

Nyní změníme druhý předpoklad a dostaneme tak platný úsudek:

b)	Marie má ráda pouze vítěze.	$\forall x\,[R(m,x) \supset V(x)]$
	Karel není vítěz.	$\neg V(k)$
	———	———
	Marie nemá ráda Karla.	$\neg R(m,k)$

Aby byly předpoklady pravdivé, pak možné interpretace nad množinou D individuí i_1, i_2,…, Marie, Karel, …, i_n, … musí mít tvar:

1. Interpretace termů: m^D = Marie, k^D = Karel
2. Interpretace predikátových symbolů:

$R^D \subseteq D \times D$: {… ⟨Marie, i_1⟩, ⟨Marie, i_2⟩, …, ⟨Marie, i_n⟩, …}
$V^D \subseteq D$: {…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. Dle prvního předpokladu je totiž *nutnou podmínkou* toho, aby Karel byl v relaci R^D s Marií, právě to, že Karel musí být v množině vítězů V^D.

Vidíme, že závěr z předpokladů vyplývá, neboť je zaručeno, že relace R^D nemůže obsahovat dvojici ⟨Marie, Karel⟩. Tedy *úsudek je platný.*

c)	Kdo zná Marii i Pavla, ten Marii lituje.	$\forall x\,([Z(x,m) \wedge Z(x,p)] \supset L(x,m))$
	Někteří nelitují Marii, ačkoliv ji znají.	$\exists x\,[\neg L(x,m) \wedge Z(x,m)]$
	———	———
	Někdo zná Marii, ale ne Pavla.	$\exists x\,[Z(x,m) \wedge \neg Z(x,p)]$

Provedeme důkaz sporem, tedy budeme předpokládat, že nastane v nějaké interpretaci případ, kdy jsou předpoklady pravdivé a závěr nepravdivý, tedy je v takové interpretaci pravdivá formule $\forall x\,[Z(x,m) \supset Z(x,p)]$, tj. negace závěru:

$$\neg\exists x\,[Z(x,m) \wedge \neg Z(x,p)] \Leftrightarrow \forall x\,[\neg Z(x,m) \vee Z(x,p)] \Leftrightarrow \forall x\,[Z(x,m) \supset Z(x,p)]$$

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

$Z^D \subseteq D \times D$: {… ⟨i_1,Marie⟩, ⟨i_2,Marie⟩, …, ⟨i_n,Marie⟩, …,⟨α,Marie⟩, ...,
⟨i_1,Pavel⟩, ⟨i_2,Pavel⟩, …, ⟨i_n,Pavel⟩…}
$L^D \subseteq D \times D$: {… ⟨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 a 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:
Úsudek *ad* 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:

Je-li číslo prvočíslem, pak má přesně dva dělitele.
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')
——————————
$P(5)$

Pouze prvočísla mají přesně dva dělitele.
Číslo 5 má přesně dva dělitele.
——————————————————————— *platný úsudek*
Číslo 5 je prvočíslo.

$\forall x\ [D(x) \supset P(x)]$
$D(5)$
——————————
$P(5)$

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

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

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

V definicích stanovujeme vždy nutnou a dostatečnou podmínku, zejména v matematice.

Příklad 3.3.5 *(ekvivalence a tautologie)*:

a) Ověříme sémanticky, že následující věta je *analyticky pravdivá*:

„*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 $U \setminus G^U \neq U$). 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, je logicky pravdivá.
   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 (zamýšlená interpretace je zřejmá):

$$\forall x\,[O(j,x) \supset V(x)] \Leftrightarrow \forall x\,[\neg O(j,x) \vee V(x)]$$
$$\forall x\,[\neg V(x) \supset \neg O(j,x)] \Leftrightarrow \forall x\,[V(x) \vee \neg O(j,x)]$$
$$\neg\exists x\,[\neg V(x) \wedge O(j,x)] \Leftrightarrow \forall x\,[V(x) \vee \neg O(j,x)]$$

Tedy analýzou a pomocí ekvivalentních úprav jsme ověřili, že naše věty ”říkají totéž”, jsou ekvivalentní.

Příklad 3.3.6 **(***speciální kvantifikátory***):**

Vedle standardních kvantifikátorů (A, B libovolné formule)
$\forall x\mathrm{A}(x)$ ... všechny prvky universa mají vlastnost A (obor pravdivosti A = celé universum)
$\exists x\mathrm{A}(x)$ ...existuje (aspoň jeden) prvek universa s vlastností A (obor pravdivosti A je neprázdný)

Jsou někdy užívány následující nestandardní kvantifikace (zejména např. v tzv. deskripční logice):
$(\forall \mathrm{B}(x))\mathrm{A}(x)$: všechny prvky s vlastností B mají vlastnost A
$(\exists \mathrm{B}(x))\mathrm{A}(x)$: existuje prvek s vlastností B, který má vlastnost A
$\exists! x\mathrm{A}(x)$: existuje právě jeden prvek s vlastností A (”existuje to jediné x, že A”)

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

Příklady 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:
  $(\forall a \neq 0)(\forall b)(\exists! x)[a \,.\, x + b = 0]$

Definice 3.3.7 (*duální formule*):
Nechť formule F je utvořena z elementárních formulí A, B,... pouze pomocí funktorů $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$. Formuli F^d, 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 $F^{dd} = F$, jsou formule F a F^d *duálními navzájem*.

Věta 3.3.3 (dualitě):

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

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
  $\neg F(A, B,...) \Leftrightarrow \neg A \Leftrightarrow (\neg A)^d \Leftrightarrow F^d(\neg A, \neg B,...)$
  a tvrzení je dokázáno.

- Nechť $F(A, B,...) = \neg H(A, B,...)$.
  $\neg F(A, B,...) \Leftrightarrow \neg\neg H(A, B,...) \Leftrightarrow$ podle předpokladu $F = \neg H$
  $\Leftrightarrow \neg H^d(\neg A, \neg B,...) \Leftrightarrow$ podle indukčního předpokladu
  $\Leftrightarrow (\neg H(\neg A, \neg B,...))^d \Leftrightarrow$ podle definice duální formule
  $\Leftrightarrow F^d(\neg A, \neg B,...)$ podle předpokladu $F = \neg H$, Q.E.D.

- Nechť $F(A, B,...) = H(A, B,...) \wedge G(A, B,...)$.
  $\neg F(A, B,...) = \neg(H(A, B,...) \wedge G(A, B,...)) \Leftrightarrow$ podle předpokladu $F = H \wedge G$
  $\Leftrightarrow \neg H(A, B,...) \vee \neg G(A, B,...) \Leftrightarrow$ podle *de Morganova* zákona
  $\Leftrightarrow H^d(\neg A, \neg B,...) \vee G^d(\neg A, \neg B,...) \Leftrightarrow$ podle indukčního předpokladu
  $\Leftrightarrow (H(\neg A, \neg B,...) \wedge G(\neg A, \neg B,...))^d \Leftrightarrow$ podle definice duální formule
  $\Leftrightarrow F^d(\neg A, \neg B,...)$ 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 $F(A, B,...) = \forall x\, H(A, B,...)$.
  $\neg F(A, B,...) = \neg \forall x\, H(A, B,...) \Leftrightarrow$ podle předpokladu $F = \forall x H$
  $\Leftrightarrow \exists x\, \neg H(A, B,...) \Leftrightarrow$ podle *de Morganova* zákona

$\Leftrightarrow \exists x\, H^d(\neg A, \neg B,...) \Leftrightarrow$	podle indukčního předpokladu
$\Leftrightarrow (\forall x\, H(\neg A, \neg \mathrm{B},...))^d \Leftrightarrow$	podle definice duální formule
$\Leftrightarrow F^d(\neg A, \neg B,...)$	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. $G^d(\neg A, \neg B,...) \supset F^{dd}(\neg A, \neg B,...)$	podle 1.věty o dualitě
4. $G^d(A, B,...) \supset F^d(A, B,...)$	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. $G^d \supset F^d$	podle 2.věty o dualitě: 2
5. $F^d \supset G^d$	podle 2.věty o dualitě: 3
6. $F^d \equiv G^d$	ZE: 4,5

Příklad 3.3.7 (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:

- $\models \forall x\, P(x) \supset P(y)$
  $\models P(y) \supset \exists x\, P(x)$
- $\models [\forall x\, P(x) \vee \forall x\, Q(x)] \supset \forall x\, [P(x) \vee Q(x)]$
  $\models \exists x\, [P(x) \wedge Q(x)] \supset [\exists x\, P(x) \wedge \exists x\, Qx)]$

Ad 3:

- $\models \forall x\, [P(x) \wedge Q(x)] \equiv [\forall x\, P(x) \wedge \forall x\, Q(x)]$,
  $\models \exists x\, [P(x) \vee Q(x)] \equiv [\exists x\, P(x) \vee \exists x\, Q(x)]$
- $\models \forall x\, [A \wedge B(x)] \equiv [A \wedge \forall x\, B(x)]$
  $\models \exists x\, [A^d \vee B^d(x)] \equiv [A^d \vee \exists x\, B^d(x)]$

Cvičení ke kapitole 3.3.

1) Ukažte, že formule $\exists x\ P(x) \supset P(a)$, kde a je individuová konstanta, není logicky pravdivá, ale je splnitelná.

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

2) Dokažte, že *neplatí* $\exists x\ P(x) \models P(a)$, tedy že formule $P(a)$ *nevyplývá* za formule $\exists x\ P(x)$. Využijte přitom řešení úlohy 1).

3) Zapište v jazyce PL^1 následující výroky a najděte jejich *modely* a také interpretace, ve kterých *nejsou* pravdivé:
   a) Množiny A a B mají neprázdný průnik. Některá A jsou B.
   b) Všechna čísla jsou sudá nebo lichá.
   c) Množina A je podmnožinou množiny B. Všechna A jsou B.
   d) Žádné A není B. Množina A je podmnožinou komplementu množiny B.
   e) Některá A nejsou B.

4) Najděte modely následujících formulí:
   a) $\exists x\ R(x,f(x))$
   b) $\forall x\ R(x,f(x))$
   c) $\forall x \forall y\ [P(x,y) \supset Q(f(x),y)]$
   d) $\forall x \forall y\ [P(x,y) \supset \neg Q(f(x),y)]$
   e) $\exists x \forall y\ [P(x,y)]$
   f) $\forall y \exists x\ [\neg P(x,y)]$

5) Převeďte následující věty do formulí jazyka PL^1 a ověřte jejich ekvivalenci pomocí *de Morganových* zákonů:

   a) Všechna prvočísla větší než 2 jsou lichá.
      Je-li prvočíslo větší než 2, pak je liché.
      Neexistuje prvočíslo větší než 2, které by nebylo liché.
      Není-li číslo liché, pak to není prvočíslo větší než 2.

   b) Některá prvočísla nejsou lichá.
      Není pravda, že všechna prvočísla jsou lichá.

   c) Někteří studenti nejsou líní.
      Ne všichni studenti jsou líní.

   d) Žádné prvočíslo není sudé.
      Je-li číslo sudé, pak to není prvočíslo.
      Neexistuje sudé prvočíslo.

   e) Žádný učený z nebe nespadl.
      Kdo spadl z nebe, není učený.
      Neexistuje učený spadlý z nebe.

f) Některá čísla jsou menší než jejich druhá mocnina.
Není pravda, že žádné číslo není menší než jeho druhá mocnina.

g) Někteří mají rádi svou matku.
Není pravda, že nikdo nemá rád svou matku.

h) Neexistuje největší přirozené číslo.
Neexistuje přirozené x takové, že je větší nebo rovno než všechna y.
Ke každému číslu x existuje číslo y takové, že je-li x přirozené, pak není větší nebo rovno y.

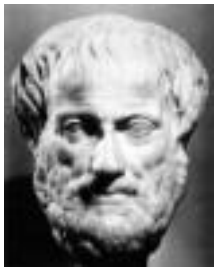
6) Určete, ***pro které interpretace jsou pravdivé*** formule (tedy charakterizujte jejich modely):

a) $\exists x \forall y\ [P(y) \supset (x=y)]$
$\exists x\ [P(x) \wedge \forall y\ [P(y) \supset (x=y)]]$
$\forall x \exists y \exists z\ \{[(x=y) \vee (x=z)] \wedge (y \neq z)\}$

b) Sémanticky ověřte, že následující formule jsou *logicky pravdivé*:
$\forall x\ [P(x) \wedge Q(x)] \equiv [\forall x\ P(x) \wedge \forall x\ Q(x)]$
$\exists x\ [P(x) \vee Q(x)] \equiv [\exists x\ P(x) \vee\ \exists x\ Q(x)]$
$\forall x \forall y\ R(x,y) \equiv \forall y \forall x\ R(x,y)$
$\exists x \exists y\ R(x,y) \equiv \exists y \exists x\ R(x,y)$
$[\forall x\ P(x) \vee \forall x\ Q(x)] \supset \forall x\ [P(x) \vee Q(x)]$
$\exists x\ [P(x) \wedge Q(x)] \supset [\exists x\ P(x) \wedge \exists x\ Q(x)]$
$\forall x\ [P(x) \supset Q(x)] \supset [\forall x\ P(x) \supset \forall x\ Q(x)]$
$[\exists x\ P(x) \supset \exists x\ Q(x)] \supset \exists x\ [P(x) \supset Q(x)]$

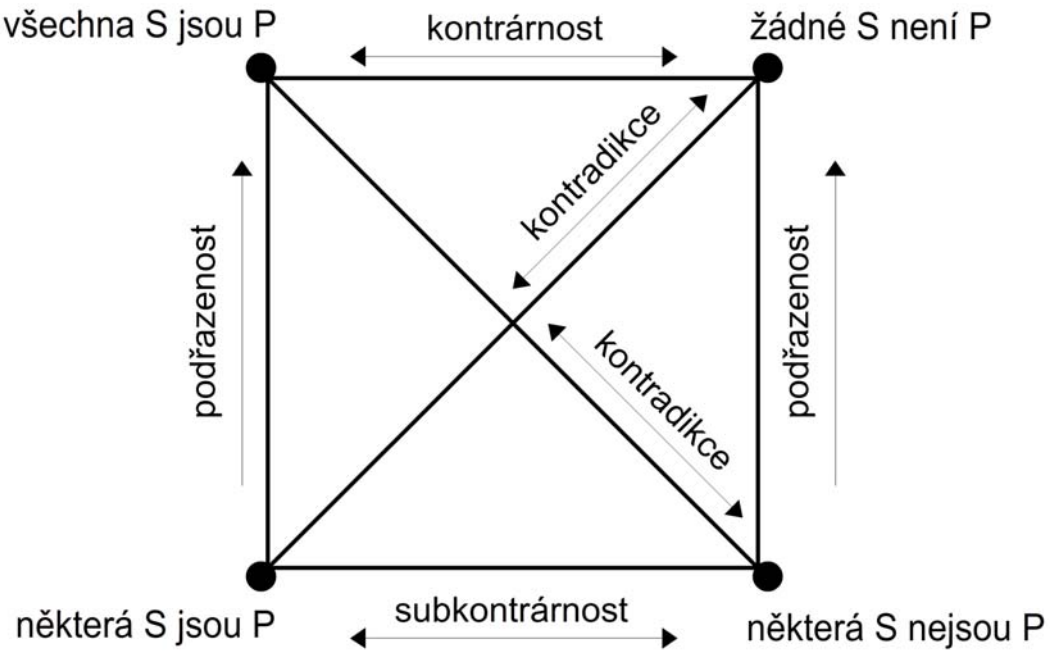
c) Zdůvodněte, proč *nejsou logicky pravdivé* formule:
$\forall x\ [P(x) \vee Q(x)] \supset [\forall x\ P(x) \vee \forall x\ Q(x)]$
$[\exists x\ P(x) \wedge \exists x\ Q(x)] \supset \exists x\ [P(x) \wedge Q(x)]$
$\forall x\ [P(x) \supset \forall x\ P(x)]$
$[\forall x\ P(x) \supset \forall x\ Q(x)] \supset \forall x\ [P(x) \supset Q(x)]$
$\exists x\ [P(x) \supset Q(x)] \supset [\exists x\ P(x) \supset \exists x\ Q(x)]$

3.4. Tradiční Aristotelova logika



Aristotelés ze Stageiry byl řecký filozof, jeden z nejvýznamnějších myslitelů ve starověku, žák (a později odpůrce) Platónův. Narodil se v roce 384 př. n. l. ve Stageiře v Thrákii (v dnešním severním Řecku) v rodině lékaře. Byl dvacet let žákem Platónovy Akademie, později založil v Aténách svoji vlastní filosofickou školu, zvanou Lykeion (Lyceum). Aristotelovo dílo je velice rozsáhlé a mnohostranné. Zachovalo se několik stovek Aristotelových spisů, které obsahují spisy filosofické, přírodovědné, metafyzické, etické, o literatuře a rétorice, a v neposlední řadě spisy o logice, tj. *Organon*, neboli „nástroj“ ke správnému, filosofickému uvažování, myšlení.

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*:



Tradiční Aristotelova logika je dnes považována za fragment predikátové logiky 1. řádu, který je omezen pouze na jednomístné predikáty jejichž interpretací (oborem pravdivosti) je vždy *neprázdná* podmnožina universa. Tato logika byla (v podstatě jako jediná) vyučována ještě v 19. století. Umožňuje kontrolovat správnost zvláštního typu jednoduchého úsudku, který se nazývá ***kategorický sylogismus***. 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.[3] Pro subjekt–predikátové výroky jsou často užívány zkratky, které jsou odvozeny 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

   Důkazy těchto vztahů provedeme snadno tak, že si jednotlivé úsudky zapíšeme v jazyce PL^1 a použijeme *de Morganovy* zákony:

   Všechna S jsou P ⇔ Není pravda, že některá S nejsou P
   Důkaz (de Morgan): $\forall x\,[S(x) \supset P(x)] \Leftrightarrow \neg\exists x\,[S(x) \wedge \neg P(x)]$
   Žádné S není P ⇔ Není pravda, že některá S jsou P
   Důkaz (de Morgan): $\forall x\,[S(x) \supset \neg P(x)] \Leftrightarrow \neg\exists x\,[S(x) \wedge P(x)]$

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 nemusí být pravda): Všechny houby jsou jedlé, všechny houby jsou nejedlé.)

   Opět, zapíšeme-li tyto úsudky v jazyce PL^1, snadno ověříme jejich platnost. Nyní to provedeme na základě množinových úvah:

   Všechna S jsou P |= Není pravda, že žádné S není P
   $\forall x\,[S(x) \supset P(x)] \models \neg\forall x\,[S(x) \supset \neg P(x)]$

   Důkaz (sémanticky): Je-li $S^U \subseteq P^U$, pak S^U nemůže být podmnožinou komplementu P^U, tedy *není* $S^U \subseteq \neg P^U$

   Žádné S není P |= Není pravda, že všechna S jsou P
   $\forall x\,[S(x) \supset \neg P(x)] \models \neg\forall x\,[S(x) \supset P(x)]$

   Důkaz (sémanticky): *Je-li* $S^U \subseteq \neg P^U$ (komplementu P^U), pak S^U nemůže být podmnožinou P^U, tedy *není* $S^U \subseteq P^U$

3) *Subkontrární* (podprotivné):
   ¬SiP |= SoP ¬SoP |= SiP
   (Může však být SiP i SoP pravdivé: Některé labutě jsou černé, některé labutě nejsou černé.)

   Zapíšeme tyto úsudky v jazyce PL^1 a ověříme jejich platnost:

   Není pravda, že některá S jsou P |= Některá S nejsou P
   $\neg\exists x\,[S(x) \wedge P(x)] \models \exists x\,[S(x) \wedge \neg P(x)]$
   Jelikož platí ekvivalence $\neg\exists x\,[S(x) \wedge P(x)] \Leftrightarrow \forall x\,[S(x) \supset \neg P(x)]$, ověříme platnost tohoto úsudku:
   $\forall x\,[S(x) \supset \neg P(x)] \models \exists x\,[S(x) \wedge \neg P(x)]$

[3] Viz Gahér (2006).

Důkaz: Je-li $S^U \subseteq \neg P^U$ (komplementu P^U) a $S^U \neq Ø$ (předpoklad ***neprázdnosti oborů pravdivosti***), pak je neprázdný také průnik S^U a komplementu P^U, tj. $\exists x\,[S(x) \wedge \neg P(x)]$.

4) *Subalterní* (podřazené):
SaP |= SiP SeP |= SoP

Důkaz platnosti druhého subkontrárního úsudku a subalterních úsudků je zcela analogický.

Dále platí tzv. obraty:

5) *Obraty*.
SiP |= PiS SeP |= 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.

Pro platné módy existují mnemotechnické pomůcky, které se naši otcové učili nazpaměť:

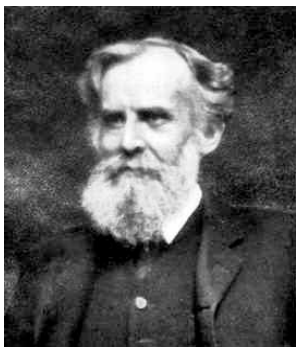
I. aaa, eae, aii, eio (barbara, celarent, darii, ferio)

II. aoo, aee, eae, eio (baroco, camestres, cesare, festino)

III. oao, aai, aii, iai, eao, eio (bocardo, darapti, datisi, disamis, felapton, ferison)

IV. aai, aee, iai, eao, eio (bamalip, calemes, dimatis, fesapo, fresison)

My se je pochopitelně nemusíme učit nazpaměť, neboť jejich platnost můžeme snadno dokázat nebo ověřit sémanticky, na základě množinových úvah. Za tím účelem je nejčastěji používána metoda tzv. *Vennových diagramů*.



John Venn (1834 – 1923), anglický matematik, logik a filosof.

Metoda Vennových diagramů

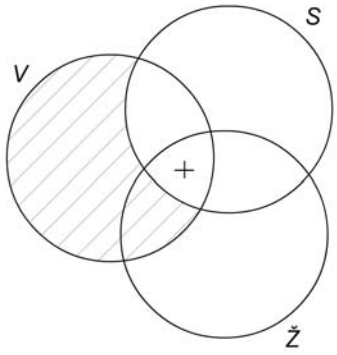
Obory pravdivosti predikátů *S*, *P*, *M* zakreslíme jako (vzájemně se protínající) kroužky (viz *Příklad* 3.2.1, kapitola 3.2). Poté znázorníme situaci, kdy jsou premisy pravdivé, a to v *tomto pořadí*:

1) Vyšrafujeme plochy, které odpovídají prázdným třídám objektů
2) Označíme křížkem plochy, které jsou jistě neprázdné (křížek přitom klademe jen tehdy, když jeho umístění je *jednoznačné*, tj. neexistuje jiná plocha, kam by mohl být umístěn)

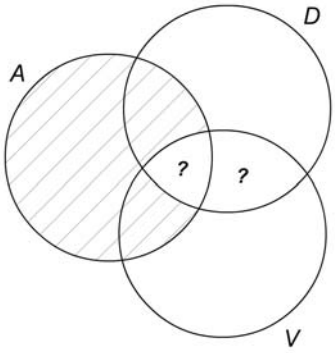
Nakonec ověříme, zda vzniklá situace znázorňuje pravdivost závěru.

Příklad 3.4.1:

a) Všechny velryby (*V*) jsou savci (*S*).
Někteří vodní živočichové (*Ž*) jsou velryby.
_____ Správný úsudek
Někteří vodní živočichové jsou savci.



b) Všechna auta (*A*) jsou dopravní prostředky (*D*)
Všechna auta mají volant (*V*)
_____ Nesprávný úsudek
Některé dopravní prostředky mají volant



Pozn.: Neplatnost tohoto úsudku možná některého 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 Vennovými kroužky, zjistíme, že tomu tak není. Premisy nás opravňují pouze k vyšrafování ploch odpovídajících těmto 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"). Avšak křížek na ploše odpovídající formuli $\exists x\,[D(x) \wedge V(x)]$, tedy průniku " 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 zjevně nesprávného úsudku je znám od Bertranda Russella:

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

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 jak jsme již zmínili, Aristoteles pracuje pouze s ***neprázdnými pojmy***. Dodáme-li další předpoklad, a to že existují skleněné hory, bude úsudek platný. Podobně, dodáme-li v úsudku *ad* b) příkladu 3.4.1 předpoklad *existence aut*, bude poté úsudek platný.

Cvičení ke kapitole 3.4.

Ověřte metodou Vennových diagramů platnost úsudků z úvodní kapitoly 1:

U_1

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

U_2

Všechny myši jsou hranaté
Všechno hranaté je modré
———————————————
Všechny myši jsou modré

U_3

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

U_4

Všichni jezevci jsou sběratelé umění
Někteří sběratelé umění žijí v norách
———————————————
Někteří jezevci žijí v norách

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

Jak jsme demonstrovali v předchozích kapitolách, sémantický důkaz logické pravdivosti, a tedy i logického vyplývání, platnosti úsudku apod., zkoumáním všech možných interpretací, je v predikátové logice často obtížný ne-li nemožný. 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 pouze splnitelná (ale ne logicky pravdivá), 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 po konečném počtu kroků vydá kladnou odpověď. V případě, že A je pouze splnitelná, 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. Jinými slovy, v případě dokazování platnosti úsudku $\{A_1,\ldots,A_n\} \models B$ stačí dokázat nesplnitelnost množiny formulí $\{A_1,\ldots,A_n, \neg B\}$.

Pozn.: Musíme mít ovšem na paměti, že uvedené ekvivalence, tj. $\{A_1,\ldots,A_n\} \models B$ právě když $\models (A_1 \wedge \ldots \wedge A_n) \supset B$, právě když $(A_1 \wedge \ldots \wedge A_n \wedge \neg B)$ je kontradikce, platí pouze pro uzavřené formule bez volných proměnných.

Rezoluční metodu lze aplikovat pouze na formule ve speciálním 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 obecnou rezoluční metodu, která se pak stala základem logického programování.

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

- Komplikovanější je procedura převedení formule na klauzulární tvar, tj. do Skolemovy klauzulární formy. Skolemova klauzulární forma je formule v konjunktivní normální formě, která má v prefixu pouze všeobecné kvantifikátory a matice formule je konjunkce *klauzulí*, kde klauzule je disjunkce literálů. Proto oproti výrokové logice je tato metoda složitější. Zejména si musíme poradit s kvantifikátory, a to tak, aby všeobecné kvantifikátory byly v prefixu a existenční se nevyskytovaly vůbec. Musíme tedy provést

  - převod formule do konjunktivní normální formy
  - eliminaci existenčních kvantifikátorů z formule (tzv. Skolemizace).
- Složitější je tvar rezolučního odvozovacího pravidla. Jeho použití vyžaduje simultánní úpravu literálů, tzv. unifikaci.

Než uvedeme přesné definice, ukážeme si postup nejprve na jednoduchých příkladech. Připomeňme si sémantická ověření platnosti úsudků v Příkladu 3.3.4. Takovéto ověřování je poněkud složité a nedá se automatizovat. Ukážeme nyní, jak elegantním způsobem dokázat platnost úsudků *ad* b) a c) tohoto příkladu za pomoci rezoluční metody:

Marie má ráda pouze vítěze.	$\forall x\,[R(m,x) \supset V(x)]$
Karel není vítěz.	$\neg V(k)$
Marie nemá ráda Karla.	$\neg R(m,k)$

Nejprve negujeme závěr úsudku: $R(m,k)$. Pak převedeme jednotlivé formule do klauzulární formy. Je to taková formule, která má v prefixu pouze všeobecné kvantifikátory a matice formule je v *konjunktivní normální formě*, tedy je to konjunkce disjunkcí literálů (klauzulí). Připomeňme, že literál je atomická formule nebo její negace. Formule $R(m,k)$ je již v klauzulární formě (té nejjednodušší): obsahuje pouze jeden literál $R(m,k)$. Druhý předpoklad $\neg V(k)$ je rovněž v klauzulární formě. Jedná se opět o jeden literál, tentokrát je to negace atomické formule $V(k)$. Zbývá upravit první předpoklad. Formule neobsahuje žádné existenční kvantifikátory, proto je naše situace jednoduchá. Stačí převést formuli $[R(m,x) \supset V(x)]$ do konjunktivní formy $[\neg R(m,x) \vee V(x)]$. Je to opět velice jednoduchá konjunktivní forma, která obsahuje jedinou klauzuli, tj. disjunkci dvou literálů $\neg R(m,x)$ a $V(x)$. Nyní sepíšeme klauzule pod sebe a snažíme se aplikovat rezoluční pravidlo „vyškrtávání literálů s opačným znaménkem“.

1. $\neg R(m,x) \vee V(x)$
2. $\neg V(k)$
3. $R(m,k)$

Nyní bychom mohli uplatnit rezoluční pravidlo např. na klauzule 1 a 2, neboť literály $V(x)$ a $\neg V(k)$ mají „opačná znaménka“. Avšak atomické formule $V(x)$ a $V(k)$ nejsou identické. Pomoc je jednoduchá. Uvědomme si, že proměnná x je v prvním předpokladu vázána všeobecným kvantifikátorem. Můžeme tedy uplatnit pravidlo konkretizace „co platí pro všechny, platí i pro některé“ (viz Příklad 3.3.3 pravidlo 1) a dosadit za proměnnou x konstantu k. Tím provedeme *unifikaci* termů $V(x)$ a $\neg V(k)$. Výsledkem bude nová klausule:

4. $\neg R(m,k)$ 1, 2, substituce x/k
5. # 3, 4

Došli jsme k prázdné klausuli, která je nesplnitelná. Tedy negovaný závěr je ve sporu s předpoklady, *úsudek je platný.*

c)	Kdo zná Marii i Pavla, ten Marii lituje.	$\forall x\,([Z(x,m) \wedge Z(x,p)] \supset L(x,m))$
	Někteří nelitují Marii, ačkoliv ji znají.	$\exists x\,[\neg L(x,m) \wedge Z(x,m)]$
	Někdo zná Marii, ale ne Pavla.	$\exists x\,[Z(x,m) \wedge \neg Z(x,p)]$

Provedeme důkaz sporem, tedy budeme předpokládat, že nastane v nějaké interpretaci případ, kdy jsou předpoklady pravdivé a závěr nepravdivý, tedy je pravdivá jeho negace: $\forall x\ [Z(x,m) \supset Z(x,p)]$. Nyní převedeme jednotlivé formule do klauzulární formy (všeobecný kvantifikátor vynecháváme, protože víme, že zůstanou pouze proměnné vázané všeobecným kvantifikátorem, na které pak můžeme uplatňovat substituci za účelem unifikace literálů).

1. *předpoklad*: $([Z(x,m) \wedge Z(x,p)] \supset L(x,m)) \Leftrightarrow \neg[Z(x,m) \wedge Z(x,p)] \vee L(x,m) \Leftrightarrow$

$\neg Z(x,m) \vee \neg Z(x,p) \vee L(x,m)$. Obdrželi jsme jednu klausuli.

2. *předpoklad*: Nyní máme problém. Formule je uzavřena *existenčním* kvantifikátorem, který potřebujeme odstranit. Jediná možnost, která se nabízí, je tato: Pokud existuje nějaké individuum x, předpokládejme, že je to např. nějaké individuum a. *Pozor*! Musíme však použít takovou konstantu, která dosud ještě nebyla použita, neboť toto individuum a jistě nemusí být totožné s individuem p nebo m. Převedeme tedy tento předpoklad na formuli

$[\neg L(a,m) \wedge Z(a,m)]$

Obdrželi jsme *dvě* jednoduché klausule, literály $\neg L(a,m)$ a $Z(a,m)$. Pozor, jsou to opravdu dvě klausule, neboť klausulární forma je *konjunkce* disjunkcí literálů.

3. *negovaný závěr*: $\neg Z(y,m) \vee Z(y,p)$. Přitom jsme vázanou proměnnou x přejmenovali na y, neboť tato proměnná je jistě jiná, než to x v prvním předpokladu.

Opět sepíšeme klausule pod sebe a budeme se pokoušet generovat resolventy za pomoci unifikace literálů (substituce vhodných termů za (všeobecně kvantifikované) proměnné):

1.	$\neg Z(x,m) \vee \neg Z(x,p) \vee L(x,m)$	
2.	$\neg L(a,m)$	
3.	$Z(a,m)$	
4.	$\neg Z(y,m) \vee Z(y,p)$	
5.	$\neg Z(a,m) \vee \neg Z(a,p)$	1, 2, substituce x/a
6.	$\neg Z(a,p)$	3, 5
7.	$\neg Z(a,m)$	4,6, substituce y/a
8.	#	3, 7 prázdná klausule

Tedy negovaný závěr je ve sporu s předpoklady, *úsudek* je *platný*.

Pozn.:

a) Unifikace je vždy dosazování termů za proměnné (ne naopak!)
b) Při unifikaci musíme vždy dosadit substituovaný term za *všechny výskyty* dané proměnné ve formuli, do které substituujeme.
c) Odstranění existenčního kvantifikátoru (tj. úprava druhého předpokladu) jistě *není přechod* k *ekvivalentní* formuli (viz cvičení 3.3, úlohy 1 a 2). Situace však není tak špatná, neboť provádíme *důkaz sporem*, a tento přechod sice nezachovává pravdivost, zachovává však *splnitelnost*, což pro důkaz sporem postačuje. Jistě, je-li např. formule $\exists x$ A(x) splnitelná, pak alespoň jeden prvek universa splňuje podmínku A, tedy formule A(a) bude také splnitelná, protože *existuje taková interpretace konstanty a*, pro kterou nabude formule A(a) hodnoty pravda. Musíme však volit pokaždé *novou konstantu*, která dosud nebyla v jazyce použita.

Po těchto úvodních příkladech přejdeme k přesným definicím. První definice je spíše pomocnou, pro ilustraci dalšího postupu.

Definice 3.5.1 (*prenexní tvar formule*): Formule A predikátové logiky je v *prenexním tvaru*, má-li tvar $Q_1x_1\ Q_2x_2\ ...\ Q_nx_n$ B, kde $n \geq 0$ a pro každé i = 1, 2,...,n je Q_i buď všeobecný kvantifikátor $\forall$ nebo existenční $\exists$, $x_1, x_2,...,x_n$ jsou navzájem různé individuové proměnné, B je formule utvořená z elementárních formulí pouze užitím výrokových spojek $\neg, \wedge, \vee$. 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 3.5.1: Každou formuli lze ekvivalentně 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 ⇔ A∗.

Důkaz: Matematickou indukcí podle hierarchického řádu formule A.
1. *Báze indukce*. Formule řádu 0 (elementární formule) neobsahují žádné spojky 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 ⇔ 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 Qi 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 ⇔ $Q1'x_1\ Q_2'x_2\ ...\ Q_n'x_n\ \neg$D ⇔ 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 = $Q_1x_1\ Q_2x_2\ ...\ Q_mx_m$ F, C = $Q_1y_1\ Q_2y_2\ ...\ Q_ny_n$ 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_1y_1 G_1 ⇔ Q_1y_1 B $\wedge$ G_1 ⇔ Q_1y_1 (B $\wedge$ G_1)∗ ⇔ 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 ⇔ $\neg(\neg$B $\wedge$ $\neg$C), B $\supset$ C ⇔ $\neg$(B $\wedge$ $\neg$C), B $\equiv$ C ⇔ $\neg$(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 $\equiv$. Použijeme ekvivalence:
A $\supset$ B ⇔ $\neg$A $\vee$ B,
A $\equiv$ B ⇔ (A $\supset$ B) $\wedge$ (B $\supset$ A) ⇔ ($\neg$A $\vee$ B) $\wedge$ ($\neg$B $\vee$ A).
(2) Převedení formule na tvar s čistými proměnnými.

a) Použijeme následující ekvivalence (náhrady levé strany pravou):
$(\forall x\mathrm{A} \wedge \forall x\mathrm{B}) \Leftrightarrow \forall x\,(\mathrm{A} \wedge \mathrm{B})$ $\quad$ $(\exists x\mathrm{A} \vee \exists x\mathrm{B}) \Leftrightarrow \exists x\,(\mathrm{A} \vee \mathrm{B})$
b) Přejmenování vázaných proměnných tak, aby žádná proměnná nebyla ve formuli současně volná i vázaná a tak, aby všechny proměnné vázané různými kvantifikátory byly navzájem různé. To platí nejenom pro celou formuli, ale i pro každou její podformuli.

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

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

$\neg\neg\mathrm{A} \Leftrightarrow \mathrm{A}$,
$\neg(\mathrm{A} \wedge \mathrm{B}) \Leftrightarrow \neg\mathrm{A} \vee \neg\mathrm{B}$, (*de Morgan*)
$\neg(\mathrm{A} \vee \mathrm{B}) \Leftrightarrow \neg\mathrm{A} \wedge \neg\mathrm{B}$, (*de Morgan*)
$\neg\forall x\ \mathrm{A}(x) \Leftrightarrow \exists x\ \neg\mathrm{A}(x)$, (*de Morgan*)
$\neg\exists x\ \mathrm{A}(x) \Leftrightarrow \forall x\ \neg\mathrm{A}(x)$. (*de Morgan*)

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

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

Příklad 3.5.1: Nalezneme 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.	$\forall x\,[P(x) \wedge \forall y\exists x_1\,(Q(x_1,y) \vee \forall z\,R(a,x_1,y))]$	přejmenování proměnné
4.	$\forall x\,[P(x) \wedge \forall y\exists x_1\,(Q(x_1,y) \vee R(a,x_1,y))]$	vypuštění nadb. kvantifikátoru
5.	$\forall x\forall y\,[P(x) \wedge \exists x_1\,(Q(x_1,y) \vee R(a,x_1,y))]$	přesun kvantifikátoru doleva
6.	$\forall x\forall y\exists x_1\,[P(x) \wedge (Q(x_1,y) \vee R(a,x_1,y))]$	přesun kvantifikátoru doleva

Pozn.: 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 3.5.2 (*Skolemova klauzulární forma*):

1) *Literál* je atomická formule nebo negace atomické formule (např. $P(f(x))$, $\neg Q(y)$).
2) *Klausule* je disjunkce literálů (např. $[P(f(x)) \vee \neg Q(y)]$).
3) *Konjunktivní normální tvar* formule predikátové logiky je prenexní tvar formule, jejíž matice je konjunkce disjunkcí literálů (tj. konjunkce *klauzulí*).
4) *Skolemova klauzulární forma* uzavřené formule je prenexní tvar této formule, která neobsahuje žádné existenční kvantifikátory a matice formule je konjunkce klausulí.

Skolemovu formu formule A označíme zápisem A^{S}.

Eliminace existenčních kvantifikátorů *(Skolemizace).*
Skolemova forma vznikne z formule opakovaným použitím následujících dvou operací (***skolemizací***):

a) $\exists x \forall y_1 ... \forall y_n \, A(x, y_1,...,y_n) \rightarrow \forall y_1 ... \forall y_n \, A(c, y_1,...,y_n)$,
kde c je nová (v jazyce dosud nepoužitá) individuová konstanta, tzv. *Skolemova konstanta*

b) $\forall x_1 \forall x_2 ... \forall x_n \, \exists y \, A(x_1, x_2,...,x_n, y) \rightarrow \forall x_1 \forall x_2 ... \forall x_n \, A(x_1, x_2,...,x_n, f(x_1, x_2,..., x_n))$,
kde f je nový (v jazyce dosud nepoužitý) n-ární funkční symbol, tzv. ***S****kolemova funkční konstanta*.

Thoralf Albert Skolem (23.5.1887 – 23.3. 1963) byl norský matematik a logic. Publikoval více než 180 článků (matematika – teorie grup, svazů, matematická logika, atd.).

Pozn.: Každému eliminovanému existenčnímu kvantifikátoru odpovídá jiná Skolemova konstanta.

1. Skolemovy konstanty představují individua, o jejichž existenci vypovídají původní formule. Tak např.
   - $\exists x \forall y \, P(x,y) \rightarrow \forall y \, P(\mathrm{c}, y)$
     Je-li univerzem množina všech přirozených čísel a realizací (interpretací) predikátu P je relace $\leq$ (tedy $P(x,y)$ chápeme jako $x \leq y$), pak konstantu c lze interpretovat jako číslo 0. Tedy, je-li formule na levé straně v této interpretaci pravdivá, pak je i formule na pravé straně pravdivá v této interpretaci. V tomto modelu je konstanta c jediná, ale v jiných modelech tomu tak být nemusí. Ovšem toto pravidlo nezachovává pravdivost. Kdybychom interpretovali konstantu c např. číslem 3, pak formule na levé straně je v této interpretaci pravdivá, kdežto formule na pravé straně je nepravdivá.
   - $\forall x \exists y \, P(x,y) \rightarrow \forall x \, P(x,f(x))$
     Důležité: jestliže je existenčně vázaná proměnná y v dosahu nějakých všeobecných kvantifikátorů vázajících proměnné $x_1, x_2,...,x_n$, pak musíme volit *funkční* symbol f arity n a za proměnnou y dosadíme term $f(x_1, x_2,..., x_n)$, neboť hodnoty y závisí na $x_1, x_2,...,x_n$.
     Je-li např. univerzem množina reálných čísel a oborem pravdivosti predikátu P je relace $<$, pak interpretací funkčního symbolu f může být např. funkce F, která je zadaná předpisem: $F(x) = x + \sqrt{3}$. V tomto modelu jsou obě formule pravdivé. V jiné interpretaci tomu tak být nemusí, pravidlo *nezachovává pravdivost*, není ve shodě s vyplýváním. Avšak zachovává *splnitelnost.* Je-li formule na levé straně pravdivá v nějaké interpretaci, pak lze vždy volit interpretaci symbolu f, tedy nalézt funkci $F(x)$, takovou, aby byla pravdivá i formule vpravo.

Tedy *Skolemova* ***klausulární forma*** formule má tento tvar:

$$\forall x_1 \forall x_2 \ldots \forall x_n \, [C_1 \wedge C_2 \wedge \ldots C_k],$$

kde C_i jsou klausule (disjunkce literálů). Vzhledem k tomu, že uvažujeme pouze uzavřené formule, není nutné všeobecné kvantifikátory explicitně uvádět.

Věta 3.5.2. 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 $\forall x_1 \ \forall x_2 ... \forall x_n \ P(x_1, x_2,...,x_n, f(x_1, x_2,..., x_n))$ libovolný 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

$$\langle d_1, d_2,\ldots,d_n, f^U(d_1, d_2,\ldots,d_n)\rangle \in P^U$$

(leží v oboru pravdivosti *P*), kde f^U je funkce přiřazená interpretací I symbolu *f* a P^U je relace – obor pravdivosti *P* v interpretaci I. Pak je ovšem interpretace I rovněž modelem formule $\forall x_1 \ \forall x_2 \ldots \forall x_n \ \exists y \ P(x_1, x_2,\ldots x_n, y)$. Každý model formule A^S je tedy i modelem formule A. Je-li tedy formule A nesplnitelná (kontradikce – nemá model), pak je nesplnitelná i formule A^S, což pro důkaz sporem postačuje.

Věta 3.5.3 (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.

Z předchozí věty vyplývá, že je-li A^S splnitelná, pak je splnitelná i A. Obráceně, je-li formule A splnitelná (má aspoň jeden model) je splnitelná i formule A^S, neboť pak lze vždy nalézt takovou interpretaci symbolu *f*, aby v ní byla A^S pravdivá. Obě formule A^S, A jsou současně splnitelné nebo nesplnitelné, nemusí však být ekvivalentní (tj. nemůžeme psát $A^S \Leftrightarrow A$ nebo $\models (A^S \equiv A)$).

Algoritmus převodu $\mathbf{A \rightarrow A^S}$.

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

Krok 2. Eliminace nadbytečných kvantifikátorů. (ekvivalentní krok)
Z formule A vypustíme všechny kvantifikátory $\forall x_i$, $\exists x_i$, v jejichž dosahu 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 ve svém dosahu 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* dle de Morganových zákonů. (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 (krok zachovává splnitelnost.)
Provádíme postupně *Skolemizaci podformulí* $Qx\ \mathrm{B}(x)$, $Qx\ \mathrm{A}(x)$, které jsme obdrželi v předchozím kroku 6, tedy náhradu existenčně kvantifikovaných formulí formulemi bez existenčního kvantifikátoru dle Definice 3.5.2 (část Skolemizace).

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:
$(\mathrm{A} \wedge \mathrm{B}) \vee \mathrm{C} \Leftrightarrow (\mathrm{A} \vee \mathrm{C}) \wedge (\mathrm{B} \vee \mathrm{C}),\ \ \mathrm{A} \vee (\mathrm{B} \wedge \mathrm{C}) \Leftrightarrow (\mathrm{A} \vee \mathrm{B}) \wedge (\mathrm{A} \vee \mathrm{C})$

Rezoluční metoda je tedy metoda nepřímého důkazu, *sporem*:

a) Důkaz logické pravdivosti formule A: dokazujeme nesplnitelnost negované formule $\neg$A.

b) Důkaz platnosti úsudku $\mathrm{A}_1,\ldots,\mathrm{A}_n \models Z$: dokazujeme nesplnitelnost množiny formulí $\{\mathrm{A}_1,\ldots,\mathrm{A}_n, \neg Z\ \}$

***Příklad 3.5.2*:**

1) Uvažujme formuli $\mathrm{A} = \forall x \exists y \forall z \exists v\ [P(z,y) \wedge Q(x,v)]$.
Pokud bychom aplikovali Skolemizaci bez kroku 6, dostali bychom formuli:
$\mathrm{A}^{S'} = \forall x \forall z\ [P(z, f(x)) \wedge Q(x, h(x,z))]$, kde f, h jsou zavedené Skolemovy funkční konstanty. Použijeme-li však nejprve krok 6, dostaneme
$\mathrm{A}' = \exists y \forall z\ P(z,y) \wedge \forall x\ \exists v\ Q(x,v)$ a z ní eliminací existenčních kvantifikátorů
$\mathrm{A}'' = \forall z\ P(z, a) \wedge \forall x\ Q(x, h(x))$. Odtud pak přesunem kvantifikátorů doleva:
$\mathrm{A}^{S} = \forall z \forall x\ [P(z, a) \wedge Q(x, h(x))]$, v níž zavedené Skolemovy konstanty a, h jsou mnohem jednodušší.

2) Krok 6 však je důležitý nejen proto, že výsledná klauzulární forma je jednodušší. Na tomto místě chceme 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):

   Uvažme jednoduchou tautologii:

   $$\neg \forall x\ P(x) \vee \forall y\ P(y).$$

   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 $\mathrm{P}(a) \wedge \neg \mathrm{P}(a)$, tedy spor, 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: nelze nalézt takovou substituci termu $f(x)$ za proměnnou x, která by tyto literály unifikovala.

3) Převedeme formuli A na formuli v klausulární (Skolemově) formě A^S:

$$A = \forall x\{P(x) \supset \exists z\{\neg \forall y[Q(x,y) \supset P(f(x_1))] \wedge \forall y[Q(x,y) \supset P(x)]\}\}.$$

Kroky 1. a 2. Utvoření existenčního uzávěru a eliminace $\exists z$:

$$\exists x_1 \forall x\{P(x) \supset \{\neg \forall y[Q(x,y) \supset P(f(x_1))] \wedge \forall y[Q(x,y) \supset P(x)]\}\}.$$

Krok 3. Přejmenování proměnné y:

$$\exists x_1 \forall x\{P(x) \supset \{\neg \forall y[Q(x,y) \supset P(f(x_1))] \wedge \forall z[Q(x,z) \supset P(x)]\}\}.$$

Krok 4. Eliminace $\supset$:

$$\exists x_1 \forall x\{\neg P(x) \vee \{\neg \forall y[\neg Q(x,y) \vee P(f(x_1))] \wedge \forall z[\neg Q(x,z) \vee P(x)]\}\}.$$

Krok 5. Přesun negace dovnitř:

$$\exists x_1 \forall x\{\neg P(x) \vee \{\exists y[Q(x,y) \wedge \neg P(f(x_1))] \wedge \forall z[\neg Q(x,z) \vee P(x)]\}\}.$$

Krok 6. Přesun kvantifikátorů $\exists y$ a $\forall z$ doprava:

$$\exists x_1 \forall x\{\neg P(x) \vee \{[\exists y\, Q(x,y) \wedge \neg P(f(x_1))] \wedge [\forall z\, \neg Q(x,z) \vee P(x)]\}\}.$$

Krok 7. Eliminace existenčních kvantifikátorů:

$$\forall x\{\neg P(x) \vee \{[Q(x,h(x)) \wedge \neg P(f(a))] \wedge [\forall z\, \neg Q(x,z) \vee P(x)]\}\}.$$

Krok 8. Přesun $\forall z$ doleva:

$$\forall x \forall z\{\neg P(x) \vee \{[Q(x,h(x)) \wedge \neg P(f(a))] \wedge [\neg Q(x,z) \vee P(x)]\}\}.$$

Krok 9. Použití distributivního zákona:

$$\forall x \forall z\{[\neg P(x) \vee Q(x,h(x))] \wedge [\neg P(x) \vee \neg P(f(a))] \wedge [\neg P(x) \vee \neg Q(x,z) \vee P(x)]\}.$$

Nyní můžeme ještě formuli zjednodušit:

i) Vypustíme třetí klausuli, protože je to tautologie
ii) Odstraníme kvantifikátor $\forall z$ (stal se zbytečným)
iii) Ve druhé klausuli odstraníme $\neg P(x)$, neovlivníme tím splnitelnost

Výsledná Skolemova klauzulární forma je:

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

Příklad 3.5.3: 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 $P(x, f(x)) \neq P(a, z)$. Uvědomíme-li si však, že všechny proměnné jsou univerzálně kvantifikovány a že platí zákon konkretizace (viz Příklad 3.3.3, pravidlo 1: Je-li term t substituovatelný za proměnnou x ve formuli $A(x)$, pak $\forall x A(x) \models A(x/t)$, "co platí pro všechny, platí i pro t"), můžeme se pokusit najít vhodnou substituci termů za proměnné tak, abychom dostali shodné, tj. *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'. $\neg P(a, f(a)) \vee \neg Q(f(a), v)$

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

4. $\neg Q(f(a), v)$

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'. $\neg Q(f(a), h(f(a)))$

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 z nich, a to Herbrandovu proceduru a Robinsonův unifikační algoritmus. *Herbrandova procedura* byl historicky první takový algoritmus, avšak není příliš efektivní. Teprve objev Robinsonův umožnil prudký rozvoj automatického dokazování teorémů a logického programování.

Jacques Herbrand (12.2.1908 – 27.7.1931) byl velice nadaný francouzský matematik a logik. Již v 17 letech absolvoval École Normale Superiore. Doktorandskou práci obhájil v 21 letech, poté musel narukovat do armády. V r. 1931 publikoval významnou studii na téma obecných rekurzivních funkcí a odjel na dovolenou jako horolezec do Alp. Zde však měl smrtelnou nehodu.

3.5.1 Herbrandova procedura

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* formule A (budeme značit 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 ve formuli A není žádná individuová konstanta, použijeme libovolnou, např. a.)

***Příklad 3.5.4*:**
a) Pro formuli A = $\forall x\,[P(a) \vee Q(b) \supset P(f(x))]$
je $H_A = \{a, b, f(a), f(b), f(f(a)), f(f(b)), \ldots\}$
b) Pro formuli B = $\forall x \forall y\, P((f(x), y, g(x,y))$
je $H_A = \{a, f(a), g(a,a), f(f(a)), g(a,f(a)), g(f(a),a), \ldots\}$

Definice 3.5.3 (*Základní instance*).
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 3.5.4 (Herbrand)
Formule A v klausulární formě je nesplnitelná, právě když existuje konečná konjunkce základních instancí jejích klausulí, která je nesplnitelná.

Příklad 3.5.5: Uvažujme opět formuli A z příkladu 3.5.3:

$$\forall x \forall y \forall z \forall v\,[P(x, f(x)) \wedge Q(y, h(y)) \wedge (\neg P(a, z) \vee \neg Q(z, v))]$$

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 $H_A = \{a, f(a), h(a), f(f(a)), f(h(a)), h(f(a)), h(h(a)), \ldots\}$. Nyní budeme po řadě dosazovat prvky Herbrandova universa za proměnné x, y, z, v tak dlouho, dokud nenalezneme "protipříklad", čili spor.

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 být pravdivá pro všechna *x, y, z, v*, neboť není splněna valuací, 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, tj. 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).

3.5.2 Robinsonův unifikační algoritmus.

Pozn.: *John Alan Robinson* (narozen v r. 1928) je vzděláním filosof, dále matematik a zabývá se teoretickou informatikou. Je emeritním profesorem na Syracuse universitě v USA. Jeho nejdůležitější výsledky se týkají automatizovaného dokazování teorémů, logického programování založeného na rezolučním principu a unifikaci termů (r. 1965). Robinson obdržel v r. 1996 Herbrandovu cenu za významný přínos k automatickému usuzování a dokazování.

Definice 3.5.3 (*substituce a instance formule*):
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)* individuové 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 $B = A\sigma$.

Pozn.: 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 3.5.4 (*unifikace*):
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.

Pozn.:

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 více 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.)

***Robinsonův* algoritmus *nalezení nejobecnější unifikace*:**
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 složené termy (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 složené termy (dle Def. 3.1.1, bod II a), tedy alespoň jeden z těchto termů 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.

***Příklad 3.5.6*:**

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 3.5.5 (*Robinsonovo 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 #.

Poznámky:

1. Speciální případy rezolučního odvozovacího pravidla (předpokládáme $L_1\sigma = L_2\sigma$):

   - m=0, n=0: $L_1, \neg L_2 \mid\!-\ \#$ odvození sporu
   - m=0, n=*1*: $L_1, \neg L_2 \vee B \mid\!- B\sigma$ pravidlo MP
   - m=1, n=1: $L_1 \vee A, \neg L_2 \vee B \mid\!- A\sigma \vee B\sigma$ 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 unifikace 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 věty 2.2.3.

Příklad 3.5.7 (*rezoluční metoda v predikátové logice*):

I. *Dokážeme 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. $Q(x,x)$ 1. a 2.
5. # 3. a 4.

Negovaná formule je nesplnitelná (kontradikce), proto je původní formule logicky pravdivá.

II. *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.	#	rezoluce 5., 7.

Negovaný závěr je ve sporu s předpoklady, proto závěr z předpokladů vyplývá, *úsudek je platný.*

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).

III. *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.

Negovaný závěr je ve sporu s předpoklady, proto závěr z předpokladů vyplývá, *úsudek je platný.*

IV. *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.

Konstanty: *f*-fotbal, *p*-pivo, *a*-Xaver; Predikáty: *M*-muž, *R*-mít rád, *Z*-žena

$\forall x\,[M(x) \supset (R(x,f) \wedge R(x,p))]$	1. předpoklad
$\forall x\,[R(a,x) \supset (R(x,f) \wedge R(x,p))]$	2. předpoklad
$\exists x\,[R(x,f) \wedge \neg R(x,p)]$	3. předpoklad
$\forall x\,[\neg M(x) \supset Z(x)]$	4. předpoklad
$\forall x\,[\neg Z(x) \vee R(a,x)]$	negovaný závěr: $\neg\exists x\,[Z(x) \wedge \neg R(a,x)]$

Klausule:

1.	$\neg M(x) \vee R(x,f)$	1. premisa
2.	$\neg M(x) \vee R(x,p)$	1. premisa
3.	$\neg R(a,y) \vee R(y,f)$	2. premisa
4.	$\neg R(a,y) \vee R(y,p)$	2. premisa
5.	$R(k,f)$	3. premisa po Skolemizaci x/k
6.	$\neg R(k,p)$	3. premisa po Skolemizaci x/k
7.	$M(z) \vee Z(z)$	4. premisa
8.	$\neg Z(u) \vee R(a,u)$	negovaný závěr
9.	$\neg R(a,k)$	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.

V. *Dokažme*:
$\forall x\forall y\,(D(x,y) \supset P(x,y))$, $\forall x\forall y(D(x,y) \wedge P(y,z) \supset P(x,z))$, $D(a,b)$, $D(b,c)$ $\models$ $P(a,c)$

Jedna z možných interpretací nad universem lidí 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*"

Klausule:

1. $\neg D(x,y) \vee P(x,y)$	1. předpoklad
2. $\neg D(x,y) \vee \neg p(y,z) \vee p(x,z)$	2. předpoklad
3. $D(a,b)$	3. předpoklad
4. $D(b,c)$	4. předpoklad
5. $\neg P(a,c)$	negace závěru

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 – závěr z předpokladů vyplývá.

VI. *Dokažme*: $P(a), \forall y\,[P(y) \supset P(f(y))] \models p(f(f(a)))$

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 funkční symbol s významem "druhá mocnina čísla y".

Klauzule:

1. $P(a)$	předpoklad	
2. $\neg P(y) \vee P(f(y))$	předpoklad	
3. $\neg P(f(f(a))$	negace závěru	
rezolventy:		
4. $\neg P(f(a))$	rezoluce: 3, 2	$\{y/f(a)\}$
5. $\neg P(a)$	rezoluce: 4, 2	$\{y/a\}$
6. #	rezoluce: 5, 1	

Spor byl odvozen, tj. závěr z předpokladů vyplývá.

3.5.3 Základní principy logického programování

Definice 3.5.5 (*metoda logického programování*):
Metoda logického programování (v Prologu) 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: Nechť $Q_1,\ldots,Q_n$, P jsou klausule.

1. Logické programy používají následující notaci pro zápis klauzulí:

Hornovy klauzule	Ekvivalentní logický tvar	Zápis v logickém programu (Prolog)	
$\neg Q_1 \vee \neg Q_2 \vee \ldots \vee \neg Q_n \vee P$	$Q_1 \wedge Q_2 \wedge \ldots \wedge Q_n \supset P$	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.
$\neg Q_1 \vee \neg Q_2 \vee \ldots \vee \neg Q_n$	$\neg(Q_1 \wedge Q_2 \wedge \ldots \wedge Q_n)$	?– 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.
#	#	#	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.: # ***spor*** /prázdná klauzule/

   - P:– Q_1, Q_2,..,Q_n. — podmíněný příkaz (deklarace procedury)
     - $P = R(t_1, t_2,\ldots,t_k)$ — hlava procedury
       - P — jméno procedury
       - t_i — formální parametry procedury
     - Q_1, Q_2,..,Q_n. — tělo (příkazy) procedury
   - ?– Q_1, Q_2,..,Q_n. — množina cílů (volání podprocedur)
     - $Q = S(s_1, s_2,\ldots,s_m)$ — hlava cíle
       - Q — jméno volané procedury
       - s_i — skutečné parametry volání

Definice 3.5.6 (*logický program*):
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".

V logických programech platí navíc tyto notační konvence a zásady:
- Proměnné začínají Velkým písmenem
- Jména predikátů, funkcí a konstanty začínají malým písmenem
- Klausule ukončujeme tečkou nebo středníkem;
- Středník vyvolává proces navracení a program se pokouší odvodit další důsledky
- Je-li ve vstupním dotazu volná proměnná, pak program vypíše ty hodnoty proměnné, pro které daný dotaz vyplývá, tedy odpověď je Ano.

Algoritmus (*interpretace logického programu*):

(1) Za aktuální cílovou klauzuli vezmi výchozí cílovou klauzuli (dotaz).

(2) Je-li aktuální cílová klauzule prázdná, ukonči výpočet s odpovědí "ano" na otázky položené 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 3.5.8: Přepíšeme důkaz platnosti úsudku z předchozí kapitoly, příklad V, do logického programu s tím, že přidáme ještě jeden fakt – d(f,c).

Program 1.:
1. p(X,Y):–d(X,Y).
2. p(X,Z):–d(X,Y), p(Y,Z).
3. d(a,b).
4. d(b,c).
5. d(f,c)

Úloha 1.:
6. ?–p(a,c). cíl / dotaz

Výpočet úlohy 1 *programem* 1:

7. ?–d(a,c).	rezoluce: 6.,1.
6. ?–p(a,c).	backtracking – navracení, neboť cíl 7. nelze splnit
7. ?–d(a,Y), p(Y,c).	rezoluce: 6.,2. (*X*/a, *Z*/c)
8. ?–p(b,c).	rezoluce: 7.,3. (*Y*/b)
9. ?–d(b,c).	rezoluce: 8.,1. (*X*/b, *Y*/c)
10. ano	rezoluce: 9.,4.

Úloha 2.:

6. ?–p(f,a).	zadání – cíl

Výpočet úlohy 2 *programem* 1:

7. ?–d(f,a).	rezoluce: 6.,1.
6. ?–p(f,a).	backtracking
7. ?–d(f,Y), p(Y,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,Y), p(Y,a).	rezoluce: 8.,2.
10. ne	d(c,Y) 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).
6. ?–p(a,c). cíl / dotaz

Výpočet úlohy 1 *programem* 2:

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 úlohy 2 *programem* 2:

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 úlohy 2 *programem* 2*:*

- 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, dotazů:

?-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 druhého dotazu programem 2*:*

6. ?-p(X,c).
7. ?-d(X,c). rezoluce 6, 1 (*Y*/c)
8. **ano X = b** rezoluce 7, 4 (*X*/b)

Program vydá jako odpověď poslední substituci za volnou proměnnou obsaženou v dotazu. Tedy odpověď zní, ano, cíl p(X,c) je splněn pro X=b. Zadáme-li středník ; pak se ptáme na další možné odpovědi, vyvoláme proces navracení (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 3.5.9.

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: 9.,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 3.5.10* (*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 úlohy, 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)	fakt "6>4", výpočet klausule 5.
7. ?-4>2, nsd(4-2,2,Z)	rezoluce: 6.,2.
8. ?-nsd(2,2,Z)	fakt "4>2", výpočet“ klausule 7.
9. **ano, Z = 2**	rezoluce: 8.,1.

***Příklad 3.5.11* (*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)**
.....	X=f(f(0)), …

Na závěr této kapitoly uvedeme jednoduchý příklad toho, jak zapsat v jazyce PL^1 a v logickém programu (Prologu) dané znalosti a dotazy na to, co z nich vyplývá.

Příklad 3.5.12
Všichni studenti mají daňové úlevy.
Kdo má daňové úlevy, je na tom dobře.
Všichni studenti jsou mladší než Karlova matka.
Tom a Petr jsou studenti.
Je Karel student?
Kdo je mladší než Karlova matka?
Kdo je na tom dobře?

PL^1	Klausule	
$\forall x\,[S(x) \supset U(x)]$	1. $\neg S(x) \vee U(x)$	
$\forall x\,[U(x) \supset D(x)]$	2. $\neg U(x) \vee D(x)$	
$S(t) \wedge S(p)$	5. $S(t)$	
	6. $S(p)$	
$\forall x\,[S(x) \supset M(x,m(k))]$	7. $\neg S(x) \vee M(x,m(k))$	
$S(k)$	8. $\neg S(k)$	Ne, nelze unifikovat
$M(x,m(k))$	9. $\neg M(x,m(k))$	
	10. $\neg S(x)$	rez. 9,7
	11. $x=t$	rez. 5, 10
	12. $x=p$	rez. 6, 10
$D(x)$	13. $\neg D(x)$	
	14. $\neg U(x)$	rez. 2, 13
	15. $\neg S(x)$	rez. 1, 14
	16. $x=t$	rez. 5, 15
	17. $x=p$	rez. 6, 15

Program:

```
1.  uleva(X):–student(X).
2.  dobre(X):–uleva(X).
3.  mladsi(X,m(k)):–student(X).
4.  student(tom).
5.  student(petr).
6.  ?-student(karel).                 Je Karel student?
7.  NE
8.  ?-mladsi(X,m(k)).                 Kdo je mladší než Karlova matka?
9.  ANO, X=tom;                       Tom; a ještě někdo?
10. ANO, X=petr;                      Petr; a ještě někdo?
11. NE
12. ?-dobre(X).                       Kdo je na tom dobře?
13. ?-uleva(X).                       Kdo má úlevy na daních?
14. ?-student(X).                     Kdo je student?
15. ANO, X=tom;                       Tom je na tom dobře; a ještě někdo?
16. ANO, X=petr;                      Petr; a ještě někdo?
17. NE
```

Cvičení ke kapitole 3.5.

1. Převeďte do *Skolemovy klauzulární formy* následující formule:

a) $\exists x \forall y \forall z [P(x,y,z)]$

b) $\exists x \exists y \forall z [P(x,y,z)]$

c) $\exists x \forall y \exists z [P(x,y,z)]$

d) $\forall x \exists y \forall z [P(x,y,z)]$

e) $\forall x \exists y \exists z [P(x,y,z)]$

f) $\forall x \forall y \exists z [P(x,y,z)]$

g) $\forall x \exists y \forall z \exists v [P(z,y) \wedge Q(x,v)]$

h) $\forall x \exists y \forall z \exists v [P(z,y) \supset Q(x,v)]$

i) $\forall x \exists y \forall z \exists v [P(z,y) \wedge Q(x,y)]$

j) $\forall x \exists y \forall z [(P(x,y) \supset Q(y,z)) \vee Q(x,y)]$

k) $[\forall x (P(x) \supset \exists y \forall z (P(y) \wedge Q(y,z) \wedge Q(x,z)))] \supset \exists x Q(x,a)$

l) $\forall x [P(x) \supset \exists z [\neg \forall y [Q(x,y) \supset P(f(v))] \wedge \forall y [Q(x,y) \supset P(x)]]]$

2. *Unifikujte***:**

a) $P(x,y)$; $P(z, g(t))$

b) $P(f(x), z, g(y, a))$; $P(y, x, g(f(a), z))$

c) $P(x, b, f(x))$; $P(a, y, f(y))$

d) $P(x, f(x,z), h(a))$; $P(y, f(y,y), w)$

3. ***Rezoluční metodou ověřte platnost úsudků, popřípadě upravte tak, aby byly platné*:**

a) Nikdo, kdo trpí klaustrofobií nemůže pracovat jako liftboy.
Všichni horolezci trpí klaustrofobií.

Proto žádný horolezec nemůže pracovat jako liftboy.

b) Všechny dřevěné stoly jsou stoly.
Všechny dřevěné stoly jsou ze dřeva.

Některé stoly jsou ze dřeva.

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

Tato tužka je jedovatá.

d) Každý, kdo miluje jachting a moře, cítí k moři respekt
Někteří respekt k moři necítí, ačkoli ho milují.

Zřejmě existují takoví, kteří milují moře, ale nikoli jachting.

e) Každý někomu pije krev.
Komu pije krev Drákula, ten brzo zemře.

Někdo brzo zemře.

f) Každý horolezec má rád pěkné počasí a pivo.
Michal má rád pouze milovníky pěkného počasí a piva.¨
Někteří milovníci pěkného počasí nemají rádi pivo.
Kdo není horolezec, ten se bojí výšek.

Michal nemá rád některé lidi, kteří se bojí výšek.

4. Pomocí rezoluční metody ověřte logickou platnost formulí:

a) $\exists x P(x) \vee \exists x \neg P(x)$
b) $\forall x\, [\exists y Q(x,y) \vee \forall z \neg Q(x,z)]$
c) $[\exists x P(x) \supset \exists x Q(x)] \supset \exists x\, [P(x) \supset Q(x)]$
d) $\forall x\, [[\neg P(x) \vee Q(x,h(x))] \wedge \neg P(f(a))]$
e) $\forall x_1 \forall x_2 \exists y\, \{[P(x_1) \supset Q(x_2,y)] \supset \forall z\, [[Q(x_2,y) \supset R(z)] \supset [P(x_1) \supset R(z)]\ ]\ \}$
f) $\exists x \exists y\, [P(x,y) \wedge \forall r\, \neg Q(x,r)] \vee \forall s \forall t \exists z\, [\neg P(s,t) \vee Q(t,z) \vee [Q(s,z) \wedge \neg P(t,z)]]$

5. Použijte ***rezoluční metodu*** ke stanovení odpovědi na následující „hlavolam“:

Tom, Milan a Jan jsou členy jistého sportovního klubu. Každý člen tohoto klubu je lyžař nebo horolezec. Žádný horolezec nemá rád déšť, všichni lyžaři mají rádi sníh. Milan nemá rád to, co má rád Tom a má rád to, co Tom rád nemá. Tom má rád déšť a sníh.

a) Existuje v klubu sportovec, který je horolezec, ale nikoliv lyžař?
b) Pokud ano, který z nich to je?
c) „Minimalizujte“ předpoklady nutné pro odvození odpovědi. Jinými slovy, které předpoklady jste při odvození odpovědi nepotřebovali?

6. Dokažte *rezoluční* metodou, že každý predikát P, který splňuje předpoklady A_1, A_2 a A_3, je reflexivní, tedy pro něj platí také R).

A_1)	$\forall x \forall y\, [P(x,y) \supset P(y,x)]$	symetrie
A_2)	$\forall x \forall y \forall z\, [(P(x,y) \wedge P(y,z)) \supset P(x,z)]$	transitivita
A_3)	$\forall x \exists y\, p(x,y)$	
R)	$\forall x\, p(x,x)$	reflexivita

Jinými slovy dokažte, že $(A_1 \wedge A_2 \wedge A_3) \supset R$ je logicky pravdivá formule.
Najděte *model* množiny předpokladů $\{A_1, A_2, A_3\}$.

7. Zapište následující předpoklady jako program v Prologu a vyřešte dotaz.

Každý horolezec má rád pěkné počasí a pivo.
Michal má rád pouze milovníky pěkného počasí a piva.
Tom a Petr mají rádi pěkné počasí, ale nemají rádi pivo.
Kdo není horolezec, ten se bojí výšek.

Existuje někdo, kdo se bojí výšek a Michal jej nemá rád?

8. Použijte ***rezoluční metodu*** k tomu, abyste zodpověděli otázky:
George, Tim, John a Bill jsou fotbaloví fanoušci. Nick a John podporují Baník, Tim podporuje Spartu. Nick má rád každého, kdo podporuje Baník, zatímco George má rád každého, kdo je sice fotbalový fanoušek, ale nepodporuje Spartu.
Otázky:
   a) Koho má rád Nick?
   b) Má George rád Billa?
   c) Koho má rád George?

9. V databázi jsou tři tabulky, DODAVATEL, VÝROBEK a DODÁVKA:

DODAVATEL

Kód-dod	Jméno	Profese	Město
001	Novák	Dovozce	Praha
110	Brown	Výrobce	Londýn
003	Pinkava	obch.zástupce	Plzeň

VÝROBEK

Kód-výr	Název	Model	Váha	MJ
003	Olej	30	300	litr
004	Pneumatiky	157/75	2500	ks
013	Olej	50	500	litr
005	Lampy	RAAI	10	ks

DODÁVKA

Kód-dod	Kód-výr	Množství
001	004	2500
110	013	130

i) ***Zapište obsah těchto tabulek jaka fakta v Prologu.***

ii) ***Formulujte následující dotazy v Prologu:***

a) Jaká jsou jména dodavatelů oleje?
b) Ve kterém městě sídlí dodavatelé pneumatik a ve kterém městě dodavatelé oleje?
c) Co dodává pan Brown?
d) Kteří dodavatelé oleje dodávají méně než 300 tun a sídlí v Londýně?
e) Kdo dodává olej a kdo lampy?

Návod: Použijte predikáty, např.

jméno(X,Y), profese(X,Y), město(X,Y), výrobek(X,Y), typ(X,Y), váha(X,Y), mj(X,Y), dodává(K_1,K_2,Y),

kde proměnná X probíhá vždy přes příslušné kódy a proměnná Y přes hodnoty příslušného atributu v tabulce.

Nebo druhá možnost: dodavatel(X,Y,U,V), výrobek(X,Y,Z,U,V), dodává(K_1,K_2,Y).

3.6. Systém přirozené dedukce predikátové logiky

Úvodní poznámky:

Metoda přirozené dedukce pro predikátovou logiku je zobecněním metody přirozené dedukce, jak jsme ji poznali ve výrokové logice. 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, a to zejména pravidel pro práci s kvantifikátory.

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 3.6.1: (*pravidla přirozené dedukce*)
Výchozími (nedokazovanými, primárními) dedukčními pravidly jsou všechna dedukční pravidla uvedená v definici 2.3.1 pro práci s výrokovými spojkami, 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 proměnnou x jako volnou proměnnou.

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 $y_1,\ldots,y_n$ takové, že leží v dosahu všeobecných kvantifikátorů, je nutno 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 funkční term f s argumenty $y_1,\ldots,y_n$. Použijeme-li pravidlo vícekrát pro různé formule A, musíme za proměnnou x substituovat vždy jinou funkci $f(y_1,...,y_n)$.

Poznámky 3.6.1:

1. Pravidlo eliminace disjunkce se v literatuře často nazývá *disjunktivní sylogismus.*
2. Speciálními případy pravidla eliminace obecného kvantifikátoru jsou pravidla: $\forall x\mathrm{A}(x) \vdash \mathrm{A}(x)$, $\forall x\mathrm{A}(x) \vdash \mathrm{A}(y)$, $\forall x\mathrm{A}(x) \vdash \mathrm{A}(a)$, $\forall x\mathrm{A} \vdash \mathrm{A}$.
3. Pravidlo zavedení obecného kvantifikátoru (tj. *generalizace*) *nezachovává pravdivost*, zachovává *pouze pravdivost v interpretaci.* To znamená, že je-li formule $\mathrm{A}(x)$ s volnou proměnnou x v nějaké interpretaci pravdivá (tj. pro *všechna* ohodnocení x), pak je v této interpretaci pravdivá také formule $\forall x\mathrm{A}(x)$. Avšak je-li $\mathrm{A}(x)$ pravdivá v interpretaci I pouze pro některá ohodnocení proměnné x, pak pravidlo nelze použít. Speciálními případy pravidla zavedení existenčního kvantifikátoru jsou pravidla: $\mathrm{A}(x) \vdash \exists x\mathrm{A}(x)$, $\mathrm{A}(y) \vdash \exists x\mathrm{A}(x)$, $\mathrm{A}(a) \vdash \exists x\mathrm{A}(x)$, $\mathrm{A} \vdash \exists x\,\mathrm{A}$.
4. Pravidlo *eliminace existenčního* kvantifikátoru rovněž *nezachovává pravdivost* (ani pravdivost v interpretaci). Jak jsme viděli při výkladu obecné rezoluční metody (kap. 3.5), zachovává pouze *splnitelnost.* Proto jej lze použít v přímém důkazu pouze jako jakýsi mezikrok. V dalším průběhu důkazu je nutno opět provést existenční generalizaci, tj. zavedení existenčního kvantifikátoru.
5. Často jsou jako výchozí používána také následující dedukční pravidla (v našem systému přirozené dedukce, zavedeném definicí 3.6.1, jsou však odvoditelná z pravidel Z∀, Z∃, E∀, E∃):
   - Zavedení obecného kvantifikátoru do antecedentu
     $$\mathrm{A}(x) \supset \mathrm{B} \vdash \forall x\mathrm{A}(x) \supset \mathrm{B},\ x \text{ není volná v B}$$
   - Zavedení obecného kvantifikátoru do konsekventu
     $$\mathrm{A} \supset \mathrm{B}(x) \vdash \mathrm{A} \supset \forall x\mathrm{B}(x),\ x \text{ není volná v A}$$
   - Zavedení existenčního kvantifikátoru do antecedentu
     $$\mathrm{A}(x) \supset \mathrm{B} \vdash \exists x\mathrm{A}(x) \supset \mathrm{B},\ x \text{ není volná v B}$$
   - Zavedení existenčního kvantifikátoru do konsekventu
     $$\mathrm{A} \supset \mathrm{B}(x) \vdash \mathrm{A} \supset \exists x\mathrm{B}(x)$$
   - Eliminace obecného kvantifikátoru z konsekventu
     $$\mathrm{A} \supset \forall x\mathrm{B}(x) \vdash \mathrm{A} \supset \mathrm{B}(x)$$
   - Eliminace existenčního kvantifikátoru z antecedentu
     $$\exists x\mathrm{A}(x) \supset \mathrm{B} \vdash \mathrm{A}(x) \supset \mathrm{B}$$

***Příklady 3.6.1* (*důkazy vybraných tautologií*)**

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 (proměnná x je ve výchozí fomruli vázána)	
	Q.E.D.		

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.

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:

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

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. 3.5). Používáme je 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) $\vdash \forall x\ [A(x) \supset B(x)] \supset [\exists x A(x) \supset \exists x B(x)]$

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

Důkaz:

⇒:	1.	$\forall x\ [A \vee B(x)]$	předpoklad
	2.	$A \vee B(x)$	E∀: 1
	3.	$A \vee \neg A$	axiom
		3.1. A	1. hypotéza
		3.2. $A \vee \forall x B(x)$	ZD: 3.1
	4.	$A \supset (A \vee \forall x B(x))$	
		5.1. $\neg A$	2. hypotéza
		5.2. $B(x)$	ED: 2, 5.1
		5.3. $\forall x B(x)$	Z∀: 5.2
		5.4. $A \vee \forall x B(x)$	ZD: 5.3.
	5.	$\neg A \supset (A \vee \forall x B(x))$	
	6.	$(A \vee \neg A) \supset (A \vee \forall x B(x))$	4,5 (teorém, viz Příklad 2.3.6)
	7.	$A \vee \forall x B(x)$	MP: 3, 6 Q.E.D.
⇐:	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∀: 2.2
	2.	$A \supset \forall x\ [A \vee B(x)]$	
		3.1. $\forall x B(x)$	2. hypotéza
		3.2. $B(x)$	E∀: 3.1
		3.3. $A \vee B(x)$	ZD: 3.2
		3.4. $\forall x\ [A \vee B(x)]$	Z∀: 3.3
	3.	$\forall x B(x) \supset \forall x\ [A \vee B(x)]$	
	4.	$(A \vee \forall x B(x)) \supset \forall x\ [A \vee B(x)]$	Teorém: 2,3
	5.	$\forall x\ [A \vee B(x)]$	MP: 1, 4 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.	$\neg A(x) \vee B$	pravidlo $C \supset D \vdash \neg C \vee D$ (Dk. viz 2.3)
4.	$A(x)$	E∀: 2
5.	B	ED: 3,4

Teorému odpovídá následující dedukční pravidlo (zavedení obecného kvantifikátoru do antecedentu - viz poznámky 3.6.1):

$$A(x) \supset B \vdash \forall x A(x) \supset B$$

Příklad 3.6.2 *(důkaz platnosti úsudku)*

Kdo se bojí vody, ten nechodí plavat.	$\forall x\,[B(x,v) \supset \neg P(x)]$
Kdo chodí plavat, ten má rád léto.	$\forall x\,[P(x) \supset R(x,l)]$
Někdo chce být zdráv a proto chodí plavat.	$\exists x\,[Z(x) \wedge P(x)]$
———	
Někdo se nebojí vody a má rád léto.	$\exists x\,[\neg B(x,v) \wedge R(x,l)]$

1.	$\forall x\,[B(x,v) \supset \neg P(x)]$	předpoklad
2.	$\forall x\,[P(x) \supset \neg R(x,l)]$	předpoklad
3.	$\exists x\,[Z(x) \wedge P(x)]$	předpoklad
4.	$[Z(a) \wedge P(a)]$	ED: 3
5.	$[B(a,v) \supset \neg P(a)]$	E∀: 1
6.	$[P(a) \supset R(a,l)]$	E∀: 2
7.	$Z(a)$	EK: 4
8.	$P(a)$	EK: 4
9.	$R(a,l)$	MP: 6, 8
10.	$\neg B(a,v)$	MT: 5, 8
11.	$\neg B(a,v) \wedge R(a,l)$	ZK: 10, 9
12.	$\exists x\,[\neg B(x,v) \wedge R(x,l)]$	Z∃: 11

Následujícící dvě věty uvádíme bez důkazu. Nicméně, důkazy sémantické konzistence a úplnosti důkazového kalkulu budou alespoň v náznaku provedeny pro Hilbertův kalkul v kapitole 3.7.

Věta 3.6.1 (*o korektnosti – sémantické konzistenci*):
Každý teorém (dokazatelná formule) systému přirozené dedukce predikátové logiky je tautologií predikátové logiky: Jestliže $\vdash A$, pak $\models A$.

Věta 3.6.2 (*o sémantické úplnosti*):
Každá logicky pravdivá formule predikátové logiky je v systému přirozené dedukce dokazatelná (je teorémem): Jestliže $\models A$, pak $\vdash A$.

Definice 3.6.2 (***systém přirozené dedukce s identitou***)**:**
Systém přirozené dedukce predikátové logiky zavedený v definici 3.6.1 nyní 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	$A \vdash x = x$	ZId
Eliminace identity:	$A(t), t = s \vdash A(s)$	EId

Příklady 3.6.3 (důkazy teorémů a sekundárních pravidel s identitou):

1) $\vdash t = s \supset s = t$ neboli: $t = s \vdash s = t$ (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) $\vdash t = s \supset (s = r \supset t = r)$ neboli: $t = s, s = r \vdash t = r$ (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) $\vdash t = s \supset (A(t) \equiv A(s))$ neboli: $t = s \vdash A(t) \equiv A(s)$

Důkaz:

$\Rightarrow$:	1. $t = s$	předpoklad	
	2. A(t)	předpoklad	
	3. A(s)	EId: 2, 1	Q.E.D.
$\Leftarrow$:	1. $t = s$	předpoklad	
	2. A(s)	předpoklad	
	3. $s = t$	pravidlo symetrie: 1	
	4. A(t)	EId: 2, 3	Q.E.D.

Cvičení ke kapitole 3.6.

1) *Metodou přirozené dedukce dokažte logickou pravdivost formulí*:
$\forall x\,[P(x) \wedge Q(x)] \equiv [\forall x\,P(x) \wedge \forall x\,Q(x)]$
$\exists x\,[P(x) \vee Q(x)] \equiv [\exists x\,P(x) \vee \exists x\,Q(x)]$
$\forall x \forall y\,R(x,y) \equiv \forall y \forall x\,R(x,y)$
$\exists x \exists y\,R(x,y) \equiv \exists y \exists x\,R(x,y)$
$[\forall x\,P(x) \vee \forall x\,Q(x)] \supset \forall x\,[P(x) \vee Q(x)]$
$\exists x\,[P(x) \wedge Q(x)] \supset [\exists x\,P(x) \wedge \exists x\,Q(x)]$
$\forall x\,[P(x) \supset Q(x)] \supset [\forall x\,P(x) \supset \forall x\,Q(x)]$
$[\exists x\,P(x) \supset \exists x\,Q(x)] \supset \exists x\,[P(x) \supset Q(x)]$

2) *Metodou přirozené dedukce dokažte platnost úsudků*:

a) Nikdo, kdo trpí klaustrofobií nemůže pracovat jako liftboy.
Všichni horolezci trpí klaustrofobií.

Proto žádný horolezec nemůže pracovat jako liftboy.

b) Všechny dřevěné stoly jsou stoly.
Všechny dřevěné stoly jsou ze dřeva.

Některé stoly jsou ze dřeva.

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

Tato tužka je jedovatá.

d) Každý, kdo miluje jachting a moře, cítí k moři respekt
Někteří respekt k moři necítí, ačkoli ho milují.

Zřejmě existují takoví, kteří milují moře, ale nikoli jachting.

e) Každý někomu pije krev.
Komu pije krev Drákula, ten brzo zemře.

Někdo brzo zemře.

f) Každý horolezec má rád pěkné počasí a pivo.
Michal má rád pouze milovníky pěkného počasí a piva.¨
Někteří milovníci pěkného počasí nemají rádi pivo.
Kdo není horolezec, ten se bojí výšek.

Michal nemá rád některé lidi, kteří se bojí výšek.

3.7. Logický kalkul predikátové logiky Hilbertova typu

Nebudeme zde znovu opakovat obecné charakteristiky formálních systémů, které jsme neformálně vyjádřili v kapitole 2, neboť axiomatická metoda dokazování 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 3.7.1. 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 logicky pravdivá, nebo logicky vyplývá z množiny předpokladů v případě důkazu z předpokladů) a sémantické úplnosti (každá logicky pravdivá formule je dokazatelná).

Definice 3.7.1 (***definice důkazového kalkulu Hilbertova typu***)**:**

- ***Jazyk***:
  Jazyk predikátové logiky (viz definice 3.1.1) s těmito omezeními: množina spojek je omezena na spojky $\neg$, $\supset$ a pracujeme pouze s obecným kvantifikátorem $\forall$.
- ***Axiómová schémata***:
  A_1: $A \supset (B \supset A)$
  A_2: $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
  A_3: $(\neg B \supset \neg A) \supset (A \supset B)$
  A_4: $\forall x A(x) \supset A(x/t)$ kde term t je substituovatelný za x v A
  A_5: $(\forall x\, [A \supset B(x)]) \supset (A \supset \forall x B(x))$ proměnná x není volná v A
- ***Odvozovací pravidla***:
  MP: $A, A \supset B \vdash B$ (pravidlo odloučení, *modus ponens*)
  G: $A \vdash \forall x A$ (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 3.7.1:

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:

$$Z1: \quad A \wedge B =_{df} \neg(A \supset \neg B)$$
$$Z2: \quad A \vee B =_{df} (\neg A \supset B)$$
$$Z3 \quad A \equiv B =_{df} (A \supset B) \wedge (B \supset A)$$
$$Z4: \quad \exists x A =_{df} \neg \forall x \neg A$$

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 spojek (a přirozeně i s různými množinami axiómů nebo axiómových schémat).

3. *Volba axiómů* není pochopitelně zcela libovolná; aby byl systém "rozumný", tedy korektní, podléhá dvěma kritériím:
   - Každý *axióm* je *logicky pravdivá formule*
   - 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*.

4. 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? Je-li formule $A(x)$ pravdivá v nějaké interpretaci I, pak je v této interpretaci pravdivá také formule $\forall x A(x)$. Tedy platí, že $A(x) \models \forall x A(x)$.

   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 3.7.2 o korektnosti.

Příklady 3.7.1 (důkazy teorémů a sekundárních odvozovacích pravidel):

1) $\vdash A(x/t) \supset \exists x A(x)$
   Důkaz:

1.	$\forall x \neg A(x) \supset \neg A(x/t)$	axiom 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.	$[\neg\exists x A(x) \supset \neg A(x/t)] \supset [A(x/t) \supset \exists x A(x)]$	axiom 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)
Důkaz:

1.	$A \supset B(x)$	předpoklad
2.	$\forall x\,[A \supset B(x)]$	G: 1
3.	$\forall x\,[A \supset B(x)] \supset [A \supset \forall x B(x)]$	axiom A5
4.	$A \supset \forall x B(x)$	MP: 2,3 Q.E.D.

Věta 3.7.1 (*o dedukci*) Pro *uzavřenou* formuli A a libovolnou formuli B platí:
$\vdash A \supset B$ právě tehdy, když $A \vdash B$.

Poznámka 3.7.2: 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 3.7.2 o korektnosti – není ani dokazatelná).

Věta 3.7.2 (*o korektnosti* neboli *sémantické konzistenci*):
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 logicky pravdivá (neboť mohla vzniknout z axiómů – tautologií pouze použitím pravidla MP, které zachovává pravdivost). To znamená, že v libovolné struktuře I platí pro libovolné ohodnocení e proměnné x, že $\models_I A(x)[e]$. Tedy platí pro *libovolné* individuum $i \in U$, kde U 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 3.7.3 (***o sémantické úplnosti axiomatického systému - K. Gödel***)**:**
Každá tautologie predikátové logiky je dokazatelná (v logickém kalkulu Hilbertova typu). Formálně, ***je-li*** **|= A** ***pak*** **|– A**.

Důkaz: bude proveden v kapitole 4.

Definice 3.7.2 (***axiomatický systém predikátové logiky s identitou***)**:**
Axiomatický systém zavedený v definici 3.7.1 rozšíříme následujícím způsobem:

- Abecedu predikátové logiky rozšíříme 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 rozšíříme o následující tři schémata charakterizující predikát rovnosti:

R_1 $\quad \vdash \forall x\,(x = x)$

R_2 $\quad \vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\,[x_1 = y_1 \wedge \ldots \wedge x_n = y_n \supset f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)]$
pro libovolný *n*-ární funkční symbol *f*

R_3 $\quad \vdash \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n\,[x_1 = y_1 \wedge \ldots \wedge x_n = y_n \supset P(x_1,\ldots,x_n) \equiv P(y_1,\ldots,y_n)]$
pro libobolný *n*-ární predikátový symbol *P*

Poznámky 3.7.4:

1. Axiómová schémata R_2, R_3 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 R_2, R_3 můžeme také nahradit následujícími axiómy komutativity a tranzitivity rovnosti:

   $\vdash \forall x \forall y\,[x = y \supset y = x]$ $\qquad R_2'$

   $\vdash \forall x \forall y \forall z\,[x = y \wedge y = z \supset x = z]$ $\qquad R_3'$

   V systému predikátové logiky zavedeném definicí 3.7.2 jsou však formule R_2', R_3' 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 3.7.2) nebo ***predikátové logice bez rovnosti*** (definice 3.7.1).

***Příklad* 3.7.2** (důkazy formulí s rovností):

1) $\vdash \forall x \forall y\, [x = y \supset y = x]$
Důkaz:
1. $\forall x \forall y \forall z \forall t\, [x=y \wedge z=t \supset (x=z \equiv y=t)]$ R_3 (predikátem P je rovnost =)
2. $x=y \wedge x=x \supset x=x \equiv y=x$
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. $\forall x\, [x=x]$ R_1
5. $x = x$ 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. $\forall x \forall y \forall z \forall t\, [x=y \wedge z=t \supset (x=z \equiv y=t)]$ R_3 (predikátem p je rovnost =)
2. $x=y \wedge y=z \supset (x=z \equiv y=y)$ subst. *x/x, y/y, z/z, t/y*
3. $\forall x\, [x=x]$ R_1
4. $y=y$ 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.

Cvičení ke kapitole 3.7.

Mějme bizardní jazyk „gibberish“, který mluví o dvou objektech: ***ponk*** a ***lonk*** a jedné relaci ***zonkovat.*** Zapište následující tvrzení ve formě axiómů PL1 a dokažte, že tato množina axiomů je bezesporná, tj. najděte její model.

a) Pro libovolné dva *lonky* existuje nanejvýš jeden *ponk,* který *zonkuje* oba tyto *lonky.*
b) Pro libovolné dva *ponky* existuje právě jeden *lonk,* který *zonkuje* oba tyto *ponky.*
c) Ke každému *lonku* existují alespoň tři *ponky,* které *zonkují* tento *lonk.*

Dokažte, že z těchto axiomů nelze dokázat toto tvrzení:

d) Existuje *lonk* s právě jedním *ponkem,* který jej *zonkuje.*

Návod: Představte si *ponky* jako nějaké body a *lonky* jako nějaké linky (čáry, trasy, apod.)

4. Formalizované teorie predikátové logiky 1. řádu.

V této kapitole se budeme zabývat logickými *teoriemi*, které jsou budovány v rámci příslušného důkazového kalkulu. Ukážeme si, že zatímco v daném logickém kalkulu dokazujeme *logicky pravdivé* formule, teorie je budována k tomu, abychom dokazovali formule *pravdivé v* určité *interpretaci*, což reprezentuje zkoumanou oblast zájmu. Uvidíme, že to, co jsme dosud poznali (tj. pojem axiomu, důkazu, důkazu z předpokladů, teorému, atd.), se beze zbytku přenáší i do logických teorií, a jde vlastně o to, že k logickým axiomům kalkulu přidáme *speciální axiomy* pro danou teorii a provádíme *důkaz z* (těchto dodatečným) *předpokladů*. Nejprve si však povíme něco málo z historie.

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:
   - Formalizovány 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 *antinomií* (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. Přitom však máme na mysli zamýšlenou interpretaci s tím, že takto vybudovaná teorie pak může být aplikována v kterékoli jiné interpretaci, která splňuje axiomy teorie.

Proč však vlastně takovéto logické formální teorie vyvíjíme? Odpovědí je více. Jednak si tím ušetříme práci. Dokážeme-li nějaké teorémy pro danou teorii, pak tyto teorémy platí v kterékoli jiné interpretaci, která splňuje axiomy dané teorie. Stačí tedy např. rozpoznat společné rysy dvou zdánlivě zcela rozdílných relací, ukázat, že obě tyto relace splňují např. axiomy částečného uspořádání (viz níže), a není již nutno dokazovat pro každou relaci zvlášť teorémy, které platí obecně v teorii částečného uspořádání.

Druhý důvod, který je rovněž nasnadě, je ten, že takováto formalizace přesně definuje množinu modelů dané teorie, tedy to, co je pro danou zkoumanou oblast typické.

Za třetí, snažíme se budovat *konzistentní* teorie, tj. takové, které mají model. Tím se vyhneme různým paradoxům, a co hlavně, náš důkazový kalkul nekolabuje tak, jak je tomu v teoriích nekonzistentních, kde lze dokázat vše, tedy kalkul a teorie se stávají bezcennými. Tato snaha je vedena také tím, že jakmile pracujeme s (aktuálním) nekonečnem, začínají se objevovat různé paradoxy/antinomie, z nichž některé sice byly známy už ve starověku, ale jakmile chceme rigorosně budovat matematiku, pak tyto antinomie závažně narušují celý systém.

Antinomie (paradoxy).

a) Antinomie ***množiny všech množin***
   - Nechť M je množina všech množin. To znamená, že každá (pod)množina 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

     $$Card(M) \geq Card(2^M).$$

   - 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

     $$Card(M) < Card(2^M).$$

     To je ve sporu s předchozí nerovností.

b) ***Russellova antinomie*** (Russellův paradox).

   S tímto paradoxem jsme se již setkali v závěru kapitoly 3.2.1. Zopakujeme stručně:
   - Zřejmě není obecně vhodné, aby podmnožina dané množiny (a speciálně tedy i celá množina) byla prvkem dané množiny. Je nutno rozlišovat mezi *prvkem* množiny a *podmnožinou* dané množiny, jsou to rozdílné vztahy. Definujme proto jako *normální množinu* takovou množinu, která není svým vlastním prvkem. Položme otázku: je množina η všech normálních množin normální množinou?
     - Je-li odpověď na položenou otázku ano, pak η neobsahuje sebe samu jako svůj prvek a tedy η není množinou *všech* normálních množin.
     - Je-li odpověď na položenou otázku ne, pak η obsahuje sebe samu jako svůj prvek a tedy η – 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 η zapsat takto:

       $$x \in \eta \Leftrightarrow \neg(x \in x)$$

       Položená otázka vede ke sporné formuli (kontradikci)

       $$\eta \in \eta \Leftrightarrow \neg(\eta \in \eta)$$

Podobných antinomií, jako jsou dvě výše uvedené, bylo formulováno více a jsou v matematice závažné, neboť jak jsme viděli v předchozích kapitolách, ve sporném systému dochází ke kolapsu důkazového kalkulu, neboť vše je dokazatelné.

Proto formuloval počátkem 20. století německý matematik a logik David Hilbert tzv. *program formalizace matematiky*. Myšlenka je jednoduchá: zvolíme množinu „zaručených pravd“ (axiomů), které zapíšeme ve tvaru formulí predikátové logiky, které jsou pravdivé buď logicky (tj. ve všech interpretacích) nebo alespoň v zamýšlené interpretaci. Dále najdeme množinu odvozovacích pravidel takových, aby jejich aplikace vyústila v důkazový postup, který zachovává pravdivost. Jak množina axiomů tak množina odvozovacích pravidel musí být zadána dobrým tj. *finitním* způsobem tak, abychom vždy mohli v konečném počtu kroků rozhodnout zda daná formule či pravidlo je axiomem či pravidlem daného důkazového kalkulu. V tom případě tedy budeme dokazovat pouze teorémy, které jsou pravdivé (logicky nebo v dané interpretaci) a nemůže dojít ke sporu čili paradoxu. Konzistence systému je zaručena.

Hilbert předpokládal, že tímto (finitním) způsobem lze dokázat *všechny* matematické pravdy. Bohužel, tento předpoklad se ukázal jako nesplnitelný. Udržíme sice systém konzistentní, ale dokážeme jenom podmnožinu všech pravdivých tvrzení matematicky, a to dokonce již v nejjednodušším matematickém systému jako je aritmetika přirozených čísel. Ačkoliv se jedná o negativní výsledek, je to jeden z největších objevů v dějinách matematiky. Jedná se o dvě zásadní věty Kurta Gödela, tzv. *věty o neúplnosti*, který ve 30. letech minulého století 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.

Těmito problémy se budeme zabývat v závěrečné kapitole této knihy. Nejprve však definujeme, co je to teorie a pak představíme nejdůležitější teorie, které ve své praxi potřebujeme, a to teorii relací a algebraické teorie.

David Hilbert (1862 – 1943) byl významný německý matematik. Dosáhl řady velkých výsledků v oblasti axiomatizace geometrie, v základech funkcionální analýzy (Hilbertův prostor) a v matematické logice. Je znám seznam jeho 23 otevřených matematických problémů z roku 1900, z nichž některé nebyly dodnes vyřešeny.

Definice 4.1 (***Formální teorie***): 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 3.7.1 – tedy tautologií)
- množiny *speciálních* axiómů teorie. Množina speciálních axiómů charakterizuje pomocí formulí predikátové logiky vlastnosti (a vztahy mezi nimi) 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 3.7.1).

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 teorií *T*, pak hovoříme o *nepodstatném (konzervativním) rozšíření*. Je-li teorie *T*' silnější než teorie *T*, pak hovoříme o *podstatném rozšíření*.

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 (formální teorie v užším slova smyslu, tj. teorie „v kostce"). Proto bývá definován pojem důkazu z teorie takto:

Důkaz formule A z teorie T (značíme $T \vdash A$) 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

Tedy důkaz z teorie (nebo také v teorii) je *důkaz z předpokladů*, kde předpoklady jsou speciální axiomy teorie *T*.

Poznámky 4.1:

- Axiomatický systém predikátové logiky (např. důkazový kalkul zavedený definicí 3.7.1) 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.
- 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 3.6.1 a 2.3.1).

Příklad *(Teorie rodokmenu a příbuzenských vztahů)*: Zavedeme speciální symboly jazyka PL^1, které budou mít tuto zamýšlenou interpretaci:

Univerzum: množina všech individuí (žijících i zemřelých)
Speciální primitivní symboly (funkční a predikátové):

- o ... unární funkční konstanta ($o(x)$ — otec x)
- m ... unární funkční konstanta ($m(x)$ — matka x)
- M ... unární predikátová konstanta ($M(x)$ — x je muž)
- Z ... unární predikátová konstanta ($Z(x)$ — x je žena)

- 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
  - $Dite(x,y) \Leftrightarrow_{df} Rod(y,x)$ — 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 teorémy dokazatelné z axiómů (všechny proměnné jsou obecně kvantifikovány):
  - $\vdash \neg Rod(x,x)$
  - $\vdash Sour(x,y) \equiv Sour(y,x)$
  - $\vdash Pot(x,y) \wedge Pot(y,z) \supset Pot(x,z)$
  - .....

(Dokažte uvedená tvrzení např. přirozenou dedukcí.)

4.1. Teorie binárních relací.

Nyní se budeme zabývat pouze *binárními* relacemi na dané množině M, tj. relacemi, které jsou podmnožinou $M \times M$. Z nich nejdůležitější pro nás jsou relace uspořádání (zejména částečné uspořádání) a ekvivalence.

***Příklad* 4.1. (*teorie uspořádání*):**

1. *varianta*:

- Speciální binární predikátové symboly:
  = ... zamýšlená interpretace: identita
  < ... zamýšlená interpretace: být menší
- Logické axiómy: axiómy predikátové logiky bez rovnosti
- Speciální axiómy:

U_1.	$\forall x\,[x = x]$	reflexivita =
U_2.	$\forall x\,\forall y\,[x=y \supset y=x]$	symetrie =
U_3.	$\forall x\,\forall y\,\forall z\,[(x=y \wedge y=z) \supset (x=z)]$	tranzitivita =
U_4.	$\forall x\,\forall y\,\forall z\,[(x=y \wedge x<z) \supset (y<z)]$	
U_5.	$\forall x\,\forall y\,\forall z\,[(x=y \wedge z<x) \supset (z<y)]$	
U_6.	$\forall x\,\forall y\,[(x<y) \supset \neg(y<x)]$	asymetrie <
U_7.	$\forall x\,\forall y\,\forall z\,[(x<y \wedge y<z) \supset (x<z)]$	tranzitivita <
U_8.	$\forall x\,\forall y\,[x=y \vee x<y \vee y<x]$	
U_9.	$\forall x\,\exists y\,[x<y]$	
U_{10}.	$\forall x\,\exists y\,[y<x]$	
U_{11}.	$\forall x\,\forall y\,\ [x<y \supset \exists z\,[x<z \wedge z<y]]$	

2. *varianta*:

- Speciální binární predikátový symbol: <
- Logické axiómy: axiómy predikátové logiky s rovností (viz definice 3.4.2)
- Speciální axiómy:

V_1.	$\forall x\,\forall y\,[x<y \supset \neg(y<x)]$	asymetrie
V_2.	$\forall x\,\forall y\,\forall z\,[x<y \wedge y<z \supset x<z]$	tranzitivita
V_3.	$\forall x\,\forall y\,[x=y \vee x<y \vee y<x]$	
V_4.	$\forall x\,\exists y\,[x<y]$	
V_5.	$\forall x\,\exists y\,[y<x]$	
V_6.	$\forall x\,\forall y\,[x<y \supset \exists z\,(x<z \wedge z<y)]$	

Z takto zadaných teorií nyní můžeme vybírat různě obsáhlé teorie, např.:

- *Teorie rovnosti*: U_1–U_3
  Modely: identita na množině přirozených (celých, racionálních, reálných) čísel, identita na množině všech matic daného typu, ...
- *Teorie ostrého uspořádání*: U_1–U_7 nebo V_1–V_2
  Modely: relace rovnost a ostře menší na množině přirozených (celých, racionálních, reálných) čísel, rovnost a relace vlastní inkluze (podmnožiny) na množině všech podmnožin dané množiny, ...
- *Teorie lineárního ostrého uspořádání*: U_1–U_8 nebo V_1–V_3
  Modely: relace rovnost a ostře menší na množině přirozených (celých, racionálních, reálných) čísel, rovnost a lexikografické uspořádání na množině všech slov nad danou abecedou, ...
- *Teorie hustého uspořádání*: U_1–U_{11} nebo V_1–V_6
  Modely: rovnost a ostré uspořádání na množině racionálních nebo reálných čísel.

Zřejmě platí, že teorie (ostrého) uspořádání definovaná axiómy U_1-U_{11} je silnější, než teorie definovaná axiómy U_1-U_8. Teorie (ostrého) uspořádání definovaná axiómy U_1-U_{11} (v predikátové logice bez rovnosti) je ekvivalentní s teorií uspořádání definovanou axiómy V_1-V_6 (v predikátové logice s rovností). Přidání axiómu V_6 k teorii V_1-V_5 má za následek její podstatné rozšíření. Zavedení nového speciálního symbolu $\leq$ novým speciálním axiómem $x \leq y \Leftrightarrow x<y \vee x=y$, je však pouze konzervativním rozšířením.

Definice 4.2 (*Teorie částečného (neostrého) uspořádání*):
Axiomy teorie *částečného uspořádání* tvoří tato množina formulí:

i)	$\forall a\, R(a, a)$	reflexivita
ii)	$\forall a \forall b\, [(R(a, b) \wedge R(b, a)) \supset (a = b)]$	antisymetrie
iii)	$\forall a \forall b \forall c\, [(R(a, b) \wedge R(b, c)) \supset R(a, c)]$	tranzitivita

Struktura $\langle M, \leq \rangle$, tj. neprázdná množina M, na které je definována binární relace $\leq$, $\leq \subseteq M \times M$), která splňuje axiomy teorie částečného uspořádání, tj. množinu formulí i), ii), iii), se nazývá *(částečně) uspořádaná množina* neboli *poset.*[4]

Řekneme, že struktury $\langle M, \leq_1 \rangle$, $\langle N, \leq_2 \rangle$ jsou *izomorfní* vzhledem k uspořádání, jestliže existuje bijekce f: $M \to N$ taková, že pro všechny prvky $m_1, m_2 \in M$ platí:

$$m_1 \leq_1 m_2 \supset f(m_1) \leq_2 f(m_2)$$

Tedy isomorfní struktury mají nosiče o stejné mohutnosti a jsou strukturálně stejné, čili daná bijekce zachovává uspořádání.

Příklad 4.2. (*modely*, tj. částečně uspořádané množiny):

Množina $\boldsymbol{N}$ přirozených čísel při obvyklém uspořádání menší nebo rovno ($\leq$): $\langle \boldsymbol{N}, \leq \rangle$.
Množina všech podmnožin dané množiny M uspořádaná relací být podmnožinou ($\subseteq$): $\langle 2^M, \subseteq \rangle$.
Množina individuí uspořádaná relací "starší nebo stejně starý".

[4] Výraz "poset" je akronym pocházející z anglického "partially ordered set".

Množina $\boldsymbol{N}$ přirozených čísel s relací |, která je definována jako $m \mid n$ právě když m dělí n (beze zbytku).

První dva příklady ilustrují, proč je toto uspořádání nazýváno ‘částečné’. V množině M mohou totiž existovat tzv. nesrovnatelné prvky a,b, pro které neplatí ani $R(a, b)$ ani $R(b, a)$. Všimněme si tedy, že struktury $\langle \boldsymbol{N}, \leq \rangle$ a $\langle 2^M, \subseteq \rangle$ nejsou isomorfní ani pro nosiče stejné kardinality. V první struktuře jsou všechna čísla srovnatelná, ve druhé struktuře existují nesrovnatelné prvky.

Jsou-li dva prvky množiny M v relaci $\leq$, používáme obvyklý infixní zápis tvaru $a \leq b$. Na částečně uspořádaných množinách zavádíme dva důležité pojmy, a to pojem *suprema a infima*. K tomu však potřebujeme pomocnou ***definici***:

Nechť $\langle M, \leq \rangle$ částečně uspořádaná množina a N její podmnožina. Pak

- *nejmenší prvek* N je $a \in N$ takový, že $\forall x \in N\ (a \leq x)$.
- *největší prvek* N je $b \in N$ takový, že $\forall x \in N\ (b \geq x)$.
- *minimální prvek* N je $min \in N$ takový, že $\neg \exists x \in N\ (x < min)$.
- *maximální prvek* N je $max \in N$ takový, že $\neg \exists x \in N\ (x > min)$.

Zřejmě platí, že každý nejmenší prvek je zároveň minimální, ale ne naopak. Podobně každý největší prvek je maximální, ale nemusí tomu být naopak. Minimální či maximální prvek, pokud existuje, je právě jeden. Množina však může mít více minimálních či maximálních prvků. Množina, která má nejmenší a největší prvek, značíme často O resp. I, se nazývá *ohraničená.*

Definice 4.3 (*supremum a infimum*):
Buď $\langle M, \leq \rangle$ částečně uspořádaná množina a N její podmnožina.
Řekneme, že prvek $a \in M$ je *supremem množiny* N *v* M, značíme $a = \sup_M(N)$, jestliže prvek a je *nejmenší horní závora* množiny N v M, tj. platí, že

$$\forall x\ [(x \in N \supset a \geq x) \wedge \forall y\ (y \in M \wedge y \geq x) \supset (y \geq a)]$$

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

$$\forall x\ [(x \in N \supset a \leq x) \wedge \forall y\ (y \in M \wedge y \leq x) \supset (a \geq y)].$$

Příklad 4.3:
- Množina $\boldsymbol{N}$ přirozených čísel nemá v množině racionálních čísel (ani v žádné jiné množině) supremum, neboť nemá horní závoru, je shora neohraničená. Infimem a nejmenším prvkem této množiny je číslo 0.
- Množina všech podmnožin 2^M dané množiny M má supremum i infimum v M: $\sup_M(2^M) = M$, $\inf_M(2^M) = \emptyset$.

Pozn.: Relace, která splňuje pouze axiómy i) a iii), tedy není antisymetrická, se nazývá *kvazi-uspořádání*. Často se stává, že relace, která se jeví jako částečné uspořádání, je ve skutečnosti kvazi-uspořádání, neboť nesplňuje axióm antisymetrie:

Příklad 4.4: Model axiómů *kvaziuspořádání*:
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. $A \supset B$ a $\neg A \vee B$.)

Chceme-li přesto takovou množinu uspořádat, použijeme k tomu relaci ekvivalence a uspořádáme množinu ekvivalenčních tříd. Proto definujeme:

Definice 4.4 (*teorie ekvivalence*):
Axiomy teorie *ekvivalence* tvoří tato množina formulí:

iv)	$\forall a\, R(a, a)$	reflexivita
v)	$\forall a \forall b\, [R(a, b) \supset R(b, a)]$	symetrie
vi)	$\forall a \forall b \forall c\, [(R(a, b) \wedge R(b, c)) \supset R(a, c)]$	tranzitivita

Struktura $\langle M, \Leftrightarrow \rangle$, tj. neprázdná množina *M*, na které je definována binární relace $\Leftrightarrow$, $\Leftrightarrow \subseteq M \times M$), která splňuje axiomy teorie ekvivalence, je struktura s ekvivalencí.

Příklad 4.5 *(modely teorie ekvivalence)*:

- Množina ***N*** přirozených čísel s relací *identity* (=).
- Relace být *stejně starý*, *stejně vysoký*, apod. na množině individuí jsou ekvivalence.
- Množina ***N*** přirozených čísel s relací Mod_5, která je definována jako *mít stejný zbytek po dělení číslem 5*.
- Množina formulí s relací $\Leftrightarrow$ definovanou takto: formule A, B jsou ekvivalentní, značíme $A \Leftrightarrow B$, právě když mají přesně *stejné modely*.

Jsou-li dva prvky množiny *M* v relaci $\Leftrightarrow$, používáme obvyklý infixní zápis tvaru $a \Leftrightarrow b$.

Definice 4.5 (***rozklad množiny***)**:** Množina vzájemně disjunktních vlastních podmnožin dané množiny *M* takových, že jejich sjednocení je identické s *M*, se nazývá *rozklad množiny M.* Prvky rozkladu nazýváme *třídy* rozkladu.

Věta 4.1:
a) Každý rozklad na množině *M* definuje na *M* relaci ekvivalence, kde ekvivalentní jsou právě a jen prvky jedné a téže třídy.
b) Každá relace ekvivalence $\Leftrightarrow$ na množině *M* definuje rozklad množiny *M* tak, že do jedné třídy rozkladu patří všechny vzájemně ekvivalentní prvky.

Důkaz:
a) Nechť *R* je rozklad na *M*, dále $A_1, A_2, \ldots, A_i, \ldots$ jsou třídy rozkladu *R* a nechť pro každé dva prvky a_{i1}, a_{i2} z *M* platí, že $a_{i1} \Leftrightarrow a_{i2}$ právě když $a_{i1} \in A_i$, $a_{i2} \in A_i$.
Reflexivita: $a_{i1} \Leftrightarrow a_{i1}$ (zřejmé)
Symetrie: Je-li $a_{i1} \in A_i$, $a_{i2} \in A_i$, pak také $a_{i2} \in A_i$, $a_{i1} \in A_i$.
Tranzitivita: Je-li $a_{i1} \in A_i$, $a_{i2} \in A_i$ a $a_{i2} \in A_i$, $a_{i3} \in A_i$, pak také $a_{i1} \in A_i$, $a_{i3} \in A_i$.

b) Nechť $\Leftrightarrow$ je relace ekvivalence na M a nechť $A_i \subset M$ taková, že pro všechny prvky $a, b \in M$ platí: $a \in A_i$, $b \in A_i$ právě když $a \Leftrightarrow b$.
$\bigcup_{i \in I} A_i = M$ – zřejmé, neboť každý prvek M je ekvivalentní alespoň sám se sebou, tedy patří do nějaké (alespoň jednoprvkové) třídy A_i.
Je-li $A_i \subset M$, $A_j \subset M$, $a \in A_i$, $b \in A_j$ a není pravda, že $a \Leftrightarrow b$, pak dle definice podmnožin A_i nepatří prvky a, b do stejné třídy. Tedy $A_i \neq A_j$.

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 dle ekvivalence $\Leftrightarrow$ se nazývá ***faktorová množina*** a značí se obvykle $M/\Leftrightarrow$. Její prvky, tj. třídy rozkladu, pak značíme $[m]$, kde m je příslušný representant třídy.

Příklad 4.6: Na množině přirozených čísel $\boldsymbol{N}$ definujeme relaci ekvivalence $\Leftrightarrow_5$ (čteme: modulo 5) takto: čísla m, n jsou ekvivalentní právě když mají stejný zbytek po dělení 5. Tato ekvivalence rozloží množinu $\boldsymbol{N}$ na pět tříd, tj. faktorová množina $\boldsymbol{N}/\Leftrightarrow_5$ obsahuje tyto prvky, třídy rozkladu:

$$[0] = \{0, 5, 10, 15, \ldots.\}$$
$$[1] = \{1, 6, 11, 16, \ldots\}$$
$$[2] = \{2, 7, 12, 17, \ldots\}$$
$$[3] = \{3, 8, 13, 18, \ldots\}$$
$$[4] = \{4, 9, 14, 19, \ldots\}$$

Tedy $\boldsymbol{N}/\Leftrightarrow_5 = \{[0], [1], [2], [3], [4]\}$.

Příklad 4.7: Uvažme množinu F formulí jazyka PL^1 a k ní příslušnou faktorovou množinu $F/\Leftrightarrow$, kde relace $\Leftrightarrow$ je definována jako „mít přesně stejné modely“. Na této množině nyní definujeme částečné uspořádání takto:

$$[A_1] \leq [A_2] \text{ právě tehdy, když } A_1 \models A_2.$$

Struktura $\langle F/\Leftrightarrow, \leq \rangle$ tvoří poset. Abychom to ukázali, musíme nejdříve ověřit, že relace $\leq$ 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 $A_1' \models A_1$, $A_1 \models A_2$, $A_2 \models A_2'$, tedy i $A_1' \models A_2'$ a definice je korektní. Reflexivita a tranzitivita relace $\leq$ jsou zřejmé. Ukážeme, že tato je relace antisymetrická:
Je-li $[A_1] \leq [A_2]$ a $[A_2] \leq [A_1]$, pak $A_1 \models A_2$ a $A_2 \models A_1$. To znamená, že $A_1 \Leftrightarrow A_2$ a tedy $[A_1]=[A_2]$.

Cvičení ke kapitole 4.1

a) Dokažte teorémy teorie rodokmeny z úvodního příkladu této kapitoly:

$$\vdash \neg Rod(x,x)$$
$$\vdash Sour(x,y) \equiv Sour(y,x)$$
$$\vdash Pot(x,y) \wedge Pot(y,z) \supset Pot(x,z)$$

b) Ověřte a dokažte, že struktury z příkladu 4.2 splňují axiomy teorie částečného uspořádání.

c) Dokažte, že každá konečná neprázdná podmnožina X částečně uspořádané množiny má minimální a maximální prvek.

d) Dokažte, že inverzní relace k libovolnému částečnému uspořádání je opět částečné uspořádání. Inverzní relace R^{-1} k relaci R je množina všech dvojic $\langle y, x\rangle$ takových, že $\langle x, y\rangle \in R$.

e) Dokažte, že pokud je relace $<$ na množině M ireflexivní (tj. $\neg\exists x\ (x < x)$) a tranzitivní, pak relace $\leq$ definovaná tak, že $x \leq y$ právě když $x < y$ nebo $x = y$, je částečným uspořádáním.

f) Ověřte a dokažte, že struktury z Příkladu 4.5 splňují axiomy teorie ekvivalence.

g) Dokažte, že relace „modulo 5“ definovaná v Příkladu 4.6 je relace ekvivalence.

h) Definujte na množině $\boldsymbol{N}/\Leftrightarrow_5$ (viz Příklad 4.6) částečné uspořádání a ukažte, že vaše definice je korektní.

i) Dokažte, že je-li nějaká relace R ireflexivní a tranzitivní, pak je také asymetrická.

Tedy
$$\forall x\ \neg(x < x)$$
$$\forall xyz\ [(x < y) \supset ((y < z) \supset (x < z)]$$
$$\forall xy\ [(x < y) \supset \neg(y < x)]$$

Dále dokažte, že je-li R je asymetrická, pak je ireflexivní.

To znamená, že ostré uspořádání stačí definovat pouze dvěma axiomy, a to ireflexivita a tranzitivita nebo asymetrie a tranzitivita.

4.2. Algebraické teorie

Algebry jsou struktury typu $\langle N, f^n, g^m, \ldots \rangle$, kde na dané neprázdné množině N (*nosiči*) jsou definovány operace f^n, g^m,…, tj. zobrazení $N \times \ldots \times N \to N$. V této kapitole stručně představíme teorie algeber s jednou binární operací (grupoidy, pologrupy, monoidy a grupy) a se dvěma binárními operacemi (svazy).

Definice 4.6 (*grupoidy*):
Nechť G je neprázdná množina. Pak struktura $\langle G, f \rangle$, kde f: $G \times G \to G$ je zobrazení na množině G, se nazývá *grupoid.*

Pozn.: Operaci f často značíme $\bullet$ a užíváme infixní notaci, tj. místo $f(a,b)$ píšeme: $a \bullet b$.

Definice 4.7 (*monoidy, grupy*):
Nechť $\boldsymbol{G} = \langle G, \bullet \rangle$ je grupoid. Pak $\boldsymbol{G}$ se nazývá

- *komutativní*, platí-li:
  - $(\forall a,b \in G)(a \bullet b = b \bullet a)$
- *asociativní*, platí-li:
  - $(\forall a,b,c \in G)((a \bullet b) \bullet c = a \bullet (b \bullet c))$
- S *jednotkovým* (neutrálním) *prvkem*, platí-li:
  - $(\exists e \in G\ \forall a \in G)(a \bullet e = a = e \bullet a)$
- S *nulovým* (agresivním) *prvkem*, platí-li:
  - $(\exists o \in G\ \forall a \in G)(a \bullet o = o = o \bullet a)$
- S *inverzními* prvky, platí-li:
  - $(\forall a \in G\ \exists a^{-1} \in G)(a \bullet a^{-1} = e = a^{-1} \bullet a)$

Grupoid $\boldsymbol{G}$ se nazývá

- *pologrupa*, je-li asociativní
- *monoid*, jestliže $\boldsymbol{G}$ je pologrupa s jednotkovým prvkem
- *grupa*, jestliže $\boldsymbol{G}$ je monoid s inverzními prvky
- *Abelova grupa*, jestliže $\boldsymbol{G}$ je komutativní grupa

Tedy *grupa* $\boldsymbol{G}$ je struktura $\langle G, \bullet \rangle$ taková, že operace $\bullet$ je *asociativní*, a navíc existuje v G *jednotkový* prvek a ke každému prvku $a \in G$ existuje *inverzní* prvek a^{-1}.

Příklad 4.8:

- Struktura $\langle Z, - \rangle$, kde $-$ je odečítání na množině celých čísel, je grupoid, není to pologrupa (odečítání není asociativní)
- Struktura $\langle \boldsymbol{N} \setminus \{0\}, + \rangle$, kde $+$ je sčítání na množině přirozených čísel, je pologrupa, není to monoid (nemá jednotkový prvek)
- Struktura $\langle \boldsymbol{N}, + \rangle$, kde $+$ je sčítání na množině přirozených čísel, je monoid, ale není to grupa (0 je neutrální, tj. jednotkový prvek, ale nejsou inverzní prvky)

- Struktura $\langle \boldsymbol{Z}, + \rangle$, kde + je sčítání na množině celých čísel, je Abelova grupa: sčítání je asociativní a komutativní, neutrální (jednotkový) prvek je 0, inverzní prvek k libovolnému číslu m je $-m$.
- $(N, \mathbf{.})$ – kde **.** je násobení na množině přirozených čísel, je pouze komutativní monoid: jednotkový prvek je 1, chybí však inverzní prvky.
- $(R, \mathbf{.})$ – kde **.** je násobení na množině racionálních čísel, je Abelova grupa: násobení je asociativní a komutativní, jednotkový prvek je číslo 1, inverzní prvek k libovolnému číslu m je $1/m$.

Na příkladu teorie grup můžeme ilustrovat metodu axiomatického zkoumání a důvody, proč vytvářet takovéto logické teorie. 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 – teorii v kostce). Ze soustavy axiómů se pak logickou dedukcí (na základě inferenčních pravidel axiomatického systému) buduje teorie v širším slova smyslu 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, a to v každém jejím modelu.

Pozn.: Jako funkční symbol f volíme obvykle znak pro násobení '**.**', nebo znak pro sčítání '+' v komutativní grupě, a to s infixní notací. Inversní prvek pak značíme pro násobení a^{-1}, resp. pro sčítání $-a$, jednotkový prvek značíme 1 (násobení), resp. 0 (sčítání).

Objasněme si úlohu logické teorie na jednoduchém příkladu grupy: Čtenáři jsou jistě dobře známy matematické 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 $\bullet$, 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 $\underline{\boldsymbol{R}}$ množinu reálných čísel bez čísla nula: $\boldsymbol{R}\backslash\{0\}$. Abychom poznali, že i vzorec c) představuje přepis teorému d), uvažujme množinu $\underline{\boldsymbol{R}}$ s binární operací $\bullet$ definovanou takto:

$u \bullet v = \log U \,.\, \log V$, kde U, V jsou čísla taková, že platí $u = \log U$, $v = \log V$.

Protože $u \bullet v = u.v$, je zřejmé, že $\langle \underline{\boldsymbol{R}}, \bullet \rangle$ 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

$$\log_V U \,.\, \log_W V = u \bullet v^{-1} \bullet v \bullet w^{-1} = u \bullet w^{-1} = \log_W U \text{ pro } v,\ w \neq 0.$$

Příklad 4.9: Uvažujme množinu $\boldsymbol{Z}$ celých čísel a definujme na této množině relaci ekvivalence modulo n takto: $a \Leftrightarrow_n b$ právě tehdy když číslo n dělí beze zbytku rozdíl a – b, značíme $n \mid (a - b)$, tj. čísla a, b mají v kladné části stejný zbytek po dělení číslem n. Tato ekvivalence definuje (jako každá ekvivalence) na $\boldsymbol{Z}$ rozklad na třídy celých čísel kongruentních modulo n. Označme tuto faktorovou množinu tříd jako $\boldsymbol{Z}/\Leftrightarrow_n$ 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 $\boldsymbol{Z}/\Leftrightarrow_5$ 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 $\boldsymbol{Z}/\Leftrightarrow_n$ 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 $\langle \boldsymbol{Z}/\Leftrightarrow_n, + \rangle$ 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].

Definice 4.8 (*svaz*):
Množina M, na které jsou definovány dvě binární operace (tj. zobrazení $M \times M \to M$), které nazýváme $\cap$ (*průsek*) a $\cup$ (*spojení*) takové, že tato struktura $\langle M, \cap, \cup \rangle$ 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)	$\forall ab\ [(a \cap b) \cup a = a]$	absorpce
vi)	$\forall ab\ [a \cap (b \cup a) = a]$	absorpce

V teorii svazů platí následující dva teorémy, které určují souvislost teorie svazů a teorií částečného (neostrého) uspořádání:

Věta 4.2: Jestliže $S = \langle M, \cap, \cup \rangle$ je svaz, pak binární relace $\leq$ definovaná na M předpisem

$a \leq b \Leftrightarrow_{df} a \cup b = b$ nebo

$a \leq b \Leftrightarrow_{df} a \cap b = a$

je částečné uspořádání a navíc platí

$$\forall ab\ (\mathrm{Sup}\{a,b\} = a \cup b),\ \forall ab\ (\mathrm{Inf}\{a,b\} = a \cap b).$$

Věta 4.3: Je-li $S = \langle M, \leq \rangle$ částečně uspořádaná množina taková, že pro každou dvouprvkovou podmnožinu množiny M existuje v M její supremum a infimum, pak struktura $S = \langle M, \cap, \cup \rangle$ s operacemi průseku a spojení definovanými tak, že

$$a \cup b =_{df} \mathrm{Sup}_M\{a,b\}$$
$$a \cap b =_{df} \mathrm{Inf}_M\{a,b\}$$

je modelem axiómů svazu, tedy tvoří svaz.

Věta 4.4: V každém svazu dále platí následující dva teorémy:

$$\vdash (a \cap b) \cup (a \cap c) \leq a \cap (b \cup c)$$
$$\vdash (a \cup b) \cap (a \cup c) \geq a \cup (b \cap c)$$

Důkaz:

a) Platí, že $(a \cap b) \leq a$, $(a \cap b) \leq b \leq (b \cup c)$, tedy $(a \cap b) \leq a \cap (b \cup c)$. Podobně platí, že $(a \cap c) \leq a$, $(a \cap c) \leq c \leq (b \cup c)$, tedy $(a \cap c) \leq a \cap (b \cup c)$. Jelikož spojení *nejmenší horní závora*, platí také $(a \cap b) \cup (a \cap c) \leq a \cap (b \cup c)$.

b) Důkaz je zcela obdobný.

Příklad 4.10 (svazy):

- Množina 2^M všech podmnožin dané množiny M, kde průsek je definován jako průnik množin a spojení jako sjednocení množin, tvoří (distributivní) svaz. Největší prvek tohoto svazu je M, nejmenší je prázdná množina $\emptyset$.
- 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 formulí, resp. konjunkcí.
- Množina přirozených čísel, kde průsek dvou čísel m, n je $min\{m, n\}$, spojení je $max\{m, n\}$. Tento svaz má nejmenší prvek, číslo 0, ale nemá největší.

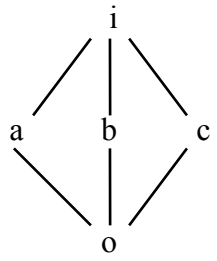
K uvedeným svazovým axiómům můžeme dle potřeby přidávat další axiómy a zkoumat tak různé třídy svazů. Platí-li ve výše uvedené větě 4.4 rovnost, pak se jedná o axióm *distributivity* a svazy, které jej splňují se nazývají ***distributivní*** *svazy*. Další důležitou třídou jsou ***modulární*** *svazy,* které splňují axióm

$$\forall a,b,c\ [(a \leq c) \supset [a \cup (b \cap c) = (a \cup b) \cap c]]$$

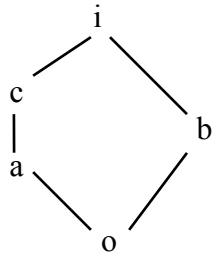
Každý distributivní svaz je modulární, ale ne naopak. Množina $\{o, a, b, c, i\}$ s uspořádáním definovaným takto

$$a \leq i, b \leq i, c \leq i, a \geq o, b \geq o, c \geq o$$

tvoří *modulární svaz*, který *není distributivní*, což snadno nahlédneme, znázorníme-li si tuto množinu Hasseovým diagramem (význam je zřejmý):



Množina $\{i, a, b, c, o\}$ s uspořádáním dle následujícího obrázku je svaz, který není modulární:



Cvičení ke kapitole 4.2:

1) Dokažte, že struktura $\langle \boldsymbol{Z}/\Leftrightarrow_n, +\rangle$ z příkladu 4.9 je komutativní (tj. Abelova) grupa.
2) Dokažte Věty 4.2 a 4.3.
3) Dokažte, že v každém svazu platí pro všechna x, y: $(x \leq y) \Leftrightarrow x \cap y = x, x \cup y = y$.
4) Dokažte, že v každém svazu jsou operace průseku a spojení izotónní, tj.:

   Jestliže $y \leq z$, pak $x \cap y \leq x \cap z$ a $x \cup y \leq x \cup z$.

4.3. Teorie aritmetiky – Gödelovy výsledky

David Hilbert (1862-1943) byl vynikající německý matematik, kterého jsme již stručně představili. Formalistická škola před Hilbertem 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) $\forall x$ (♦$x \supset$ ♠x)
(2) $\exists x$ ♠$x \supset$ ♦♣
(3) ♠♥
Inferenční pravidla: MP (modus ponens), E∀ (eliminace ∀), Z∃ (zavedení ∃)

Teorém: ♠ ♣
Důkaz:

♠♥	(axiom 3)
$\exists x$ ♠x	(Z∃)
♦♣	(axiom 2 a MP)
♦♣ $\supset$ ♠♣	(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.

Nicméně, 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 v zamýšlené interpretaci (tj. o teple resp. o světle). 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 nalezení modelu, neboť každá teorie, která má model, je konzistentní. Avšak tento způsob často selhává v tom případě, že teorie má pouze nekonečné modely. Nemůžeme ověřit konzistenci pouze na základě toho, že teorie má nekonečný model, neboť pak bychom předpokládali, že známe aktuální nekonečno (model). 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 "$\omega \neq \omega$".

Důležitý v Hilbertově přístupu je zejména *finitismus*: nemůžeme poznat aktuální nekonečno, neboť nemáme k dispozici nekonečné zdroje. Nicméně, můžeme smysluplně a korektně zkoumat *potenciální nekonečno*, a to tak, že vyjdeme od známých konečných objektů a podle přesného a korektního pravidla budeme generovat další a další objekty vyhovující kritériím příslušnosti do nekonečného souboru objektů. Takto můžeme potenciálně postupovat do nekonečna, nicméně v každém kroku máme za sebou pouze konečný počet kroků a je vygenerován konečný počet objektů.

Hilbertův program formalizace matematiky 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 formalizované verze klasické matematiky tak, že ukážou jasně a přehledně jednotlivé vlastnosti a vztahy a co především, dokážou 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 rekurzivních 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* v tomto 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*, tj. *uzavřenými formulemi*) 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.

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. Výrok α může být *pravdivý v* interpretační struktuře I_1 tj. 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. důkazový postup musí 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 logicky pravdivé formule, musí být všechny logické axiómy daného kalkulu *logicky pravdivé*; pak tyto logické axiómy (jako předpoklady důkazu) nevyznačujeme a píšeme: **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 3.7 (tedy 5 axiómů a 2 pravidla: *modus ponens* a *generalizace*) a položili základní otázku – *problém úplnosti* takto definovaného *logického kalkulu*:

Jsou dokazatelné všechny logicky pravdivé formule PL^1?

Obsah disertace Kurta Gödela (publikované v r. 1930) dává positivní odpověď na tuto otázku:

Věta 4.5 (*Gödelova věta o úplnosti PL*^{1}, 1930):
Predikátový kalkul 1. řádu (s axiómy a pravidly uvedenými v 3.7 nebo jinými korektními a vhodnými) je úplný důkazový kalkul, tj. dokazatelné jsou v něm právě všechny tautologie PL^1. Dokazatelnost je v PL^1 ekvivalentní logické pravdivosti:

$$\models \varphi \textbf{ právě když } \vdash \varphi.$$

Větu lze ještě zesílit (a Gödel to učinil):
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):

$$\alpha_1,...,\alpha_n \vdash \varphi, \textbf{ právě když } \alpha_1,...,\alpha_n \models \varphi.$$

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 4.9 (*syntaktická bezespornost*):
Teorie T *je (syntakticky) bezesporná (konzistentní)*, jestliže pro žádnou uzavřenou formuli A jazyka teorie neplatí současně $\vdash A$ i $\vdash \neg A$, tj. formule A a ¬A nemohou být současně dokazatelné (dokazatelná je nejvýše jedna z těchto formulí).

*Pozn.***:**
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 4.6: Teorie je bezesporná právě tehdy, existuje-li aspoň jedna formule, kterou nelze v teorii dokázat (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.

Sporná teorie je naprosto jalová, bezespornost teorie je samozřejmým požadavkem. Bezespornost teorie je tedy velmi slabá vlastnost, ovšem je zásadní. Ve sporné teorii se důkazový kalkul hroutí, dochází ke kolapsu, neboť dokazatelné je cokoli. Proto Hibert tolik usiloval o důkaz konzistence teorie aritmetiky.

Definice 4.10 (*nezávislost axiomů*): Axióm A_i je nezávislý na axiómech A_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 4.7: Ke každému konečnému systému (schémat) axiomů existuje nezávislý systém ekvivalentní s původním systémem.

Důkaz: Vyloučením závislého axiomu vznikne ekvivalentní systém. Vzhledem ke konečnému počtu (schémat) axiomů musí být proces eliminace závislých axiomů po konečném počtu kroků ukončen.

Věta 4.8: Axióm A_i je nezávislý na axiómech A_1, ..., A_n právě tehdy, jestliže přidáním $\neg$Ai nevznikne sporná množina axiomů, tj. teorie A_1, ..., A_{i-1}, $\neg A_i$, A_{i+1},..., A_n je bezesporná.

Důkaz:
1) Je-li teorie A_1, ..., A_{i-1}, $\neg A_i$, A_{i+1},..., A_n sporná, pak v ní lze dokázat jakoukoli formuli a tedy také A_i. V tom případě (dle věty o dedukci) platí

$$\models A_1, ..., A_{i-1}, \neg A_i, A_{i+1},..., A_n \supset A_i$$

A proto také $$\models A_1, ..., A_{i-1}, A_{i+1},..., A_n \supset A_i$$

Což vyplývá ze zákonů výrokové logiky. V tom případě je tedy A_i závislý na A_1, ..., A_n.

2) Je-li axiom A_i závislý na axiomech A_1, ..., A_n, pak lze z A_1, ..., A_{i-1}, $\neg A_i$, A_{i+1},..., A_n dokázat jak A_i tak i $\neg A_i$, tedy teorie je sporná.

Příklad 4.11:
Uvažujme teorii hustého lineárního uspořádání zleva i zprava neomezené množiny, tj. teorii danou axiómy V_1–V_6 (příklad 4.1, kapitola 4.1). Zde např. platí:

- Axióm V_4 je nezávislý na zbylých axiómech. Nahradíme-li axióm V_4 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 $(-\infty, a\rangle$, kde a je nějaké reálné číslo.
- Podobně axióm V_5 je nezávislý na zbylých axiómech.
- Rovněž axióm V_6 je nezávislý na zbylých axiómech. Nahradíme-li jej jeho negací, vznikne bezesporná teorie jejímž modelem může být např. přirozené uspořádání celých čísel.

Věta 4.9: Každá bezesporná teorie *T* má alespoň jeden model.

K důkazu věty 4.9 potřebujeme ještě jednu ingredienci – 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 $\exists x\ \varphi(x) \supset \varphi(c)$. Konstanta c se nazývá *svědek* pro formuli $\varphi(x)$.

(Připomeňme, že tato formule pochopitelně není tautologie – srovnej se Skolemizací, kap. 3.5.)

Důkaz (věty 4.9 – náznak): Lze ukázat, že ke každé bezesporné teorii *T* existuje silnější (ve smyslu definice 4.1) 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 ⟨*M*, *R*⟩, 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.)

Důkaz (věty 4.5 – o úplnosti): Z věty 4.9 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 $T \vdash \varphi$.

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 4.11 (*úplnost teorie*): Teorie *T* je *úplná*, jestliže pro každou uzavřenou formuli A jazyka teorie platí buď $\vdash$ A nebo $\vdash \neg$A, tj. formule A je dokazatelná nebo vyvratitelná. Je-li *T* navíc bezesporná, pak ze dvou formulí A, ¬A je vždy dokazatelná právě jedna.

Poznámky:

1. Právě definovanou *úplnost teorie* nelze zaměňovat se (*sémantickou*) *úplností logického kalkulu* zavedenou v kapitolách 2. a 3. a formulovanou v Gödelových větách o úplnosti.
2. Úplnost teorie nelze zaměňovat se zákonem vyloučeného třetího. Zákon vyloučeného třetího, tj. formule $A \vee \neg A$ je součástí teorie (axiom), kdežto úplnost je vlastnost teorie. Zákon vyloučeného třetího je jakožto tautologie dokazatelný i v neúplných teoriích.
3. V neúplné teorii existují dobře formulované otázky (reprezentované formulemi jazyka teorie), na které teorie nedává odpověď (formuli ani její negaci nelze dokázat). Říkáme, že neúplná teorie má nezávislé teorémy, které do ní nepatří. V úplné teorii existuje odpověď na každou smysluplnou otázku (tj. pro každou formuli jazyka teorie platí, že ji teorie rozhoduje, je dokazatelná tato formule nebo její negace).
4. 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 lineární či 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.

Příklad 4.12:

- Teorie uspořádání V_1–V_6 (viz příklad 4.1) je úplná.
- Neúplnými teoriemi jsou např.:
  - Teorie uspořádání V_1-V_k, kde $k = 2, 3, 4, 5$
- Teorie V_1–V_3 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V_4 (např. přirozené uspořádání celých čísel) a v druhém jeho negace (např. přirozené uspořádání všech záporných celých čísel).
- Teorie V_1–V_4 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V_5 (např. přirozené uspořádání celých čísel) a v druhém jeho negace (např. přirozené uspořádání všech přirozených čísel).
- Teorie V_1–V_5 je neúplná. Lze nalézt dva modely takové, že v jednom platí axióm V_6 (např. přirozené uspořádání racionálních čísel) a v druhém jeho negace (např. přirozené uspořádání všech celých čísel).
- Rovněž teorie částečného uspořádání (viz Definici 4.2) je neúplná. Existují modely, ve kterých jsou všechny prvky srovnatelné, tj. platí $\forall x \forall y\ (x \leq y \vee y \geq x)$ (například uspořádání přirozených čísel dle velikosti) a modely, ve kterých tato formule pravdivá není (např. uspořádání množiny všech podmnožin dané množiny dle množinové inkluze).

Definice 4.12 (***rozhodnutelnost teorie***): Teorie T je *rozhodnutelná*, jestliže existuje algoritmus, který o každé uzavřené formuli φ jazyka teorie rozhodne v *konečném* počtu kroků, zda φ je platným výrokem teorie T, tj. zda $T \vdash \varphi$, či nikoliv.

Pozn.: Zde předpokládáme, že pojem algoritmu je dostatečně přesně určen (např. pomocí Turingova stroje).

Příklad 4.13**:**

- 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" (čili v strukturálně různých modelech), 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.)

$$\mathbf{N} = \langle N, \mathbf{0}, \boldsymbol{S}, +, ., =, \leq \rangle$$

kde N je 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
$\leq$ 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 tedy nebudou zajímat tautologie, tj. výroky pravdivé v *každé* interpretaci našeho jazyka, ale výroky pravdivé v jedné *standardní* interpretaci, tj. ve struktuře **N** *aritmetiky 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 či relačních teorií. Nebudeme hledat společné rysy různých modelů, ale budeme zkoumat jeden model – 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*.

Definice 4.13 (*Robinsonova aritmetika Q a Peanova aritmetika PA*):

Robinsonova aritmetika Q 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) v těchto teoriích.

Ukažme si dvě jednoduchá použití axiomu indukce:

1) $\vdash \forall x\ (0 + x = x)$

Nejprve označíme $\varphi(x)$ formuli $0 + x = x$.
Nechť $0 + x = x$. Pak $s(0 + x) = s(x)$ axiom Q_3
$s(0 + x) = 0 + s(x)$ axiom Q_4
$0 + s(x) = s(x)$ (tranzitivita a komutativita identity)
$\forall x\ [(0 + x = x) \supset 0 + s(x) = s(x)]$ ZI, Z$\forall$

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 $PA \vdash \forall x\ (0 + x = x)$

To není triviální výsledek, protože zatím nevíme, zda z axiomů Robinsonovy nebo Peanovy aritmetiky plyne komutativita sčítání. Dokážeme nyní asociativitu sčítání.

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

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):

$(z + y) + x = z + (y + x)$	$(z \cdot y) \cdot x = z \cdot (y \cdot x)$
$0 + x = x$	$z \cdot (y + x) = z \cdot y + z \cdot x$
$s(y) + x = s(y + x)$	$\neg(x = s(x))$
$y + x = x + y$	$y + x = z + x \supset y = z$
$0 \cdot x = 0$	$(x + y = 0) \supset (x = 0 \wedge y = 0)$
$s(y) \cdot x = y \cdot x + x$	$(x \cdot y = 0) \supset (x = 0 \vee y = 0)$
$y \cdot x = x \cdot y$	$\exists u\ (u + x = y \vee u + y = x)$

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 (individuové 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)
- $x = Nsd(y,z) \Leftrightarrow_{df} Sd(x,y,z) \wedge \forall t\,[Sd(t,y,z) \supset t \leq x]$ 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 $\leq$ a $<$ k sobě navzájem a k operacím:

$x \leq y \equiv x < y \vee x = y$

$x < y \supset x + z < y + z$

$x < s(y) \equiv x < y \vee x = y$

$x < y \wedge z \neq 0 \supset x \,.\, z < y \,.\, z$

*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
- $\vdash x \neq 0 \supset (\exists! q)(\exists! r)[y = x.q + r \wedge r < x]$ existence a jednoznačnost celočíselného podílu a zbytku
- $\vdash \forall x \exists y\,[y > x \wedge Prv(y)]$ Euklidova věta: ke každému číslu existuje prvočíslo, které je větší než dané číslo $\Rightarrow$ 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, násobení je distributivní vůči sčítání, relace $\leq$ 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 formulí φ či ¬φ (tu pravdivou, neboť *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). Jistě, kdyby toto nebylo splněno, nemohli bychom v takovéto teorii dokazovat. Následující věta ukazuje, že v případě aritmetiky nelze splnit oba požadavky – úplnost a rekurzivitu. Neúplnost není specielní vlastnost teorie *PA*.

Definice 4.15 (*rekurzivní axiomatizace*): Teorie je *rekurzivně axiomatizovaná*, jestliže existuje algoritmus, který o každé formuli φ jazyka teorie v konečném počtu kroků rozhodne, tj. vydá odpověď Ano/Ne, zda φ je či není axiomem teorie.

Věta 4.10 ***(První Gödelova věta o neúplnosti, 1931):***
Nechť *T* je teorie, obsahující *Q* (tj. jazyk teorie *T* obsahuje jazyk aritmetiky a *T* dokazuje všechny axiomy Robinsonovy 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 axiomatizovaná*, jinak bychom v té teorii nemohli dokazovat nic. Ale žádná taková teorie neexistuje podle věty 4.10.

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 $\mathsf{gn}(\varphi)$ a $\mathsf{gn}(d)$, 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 $\mathsf{gn}(x)$ 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 $\mathbf{N}$ 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 $\mathsf{Dok}(x)$. Tedy: Teorie T dokazuje φ právě když $\mathsf{Dok}(\underline{\mathsf{gn}(\varphi)})$ je pravdivé v $\mathbf{N}$. ($\underline{\mathsf{gn}(\varphi)}$ je numerál, jehož významem je Gödelovo číslo formule φ.)

Třetí ingrediencí je *Gödelovo diagonální lemma.* Pro každou formuli $\varphi(x)$ jazyka aritmetiky existuje uzavřená formule ψ taková, že v Q je dokazatelná formule

$$\psi \equiv \varphi(\underline{\mathsf{gn}(\psi)}).$$

Tedy $\underline{\mathsf{gn}(\psi)}$ je jméno Gödelova čísla formule ψ a formule $\varphi(\underline{\mathsf{gn}(\psi)})$ ”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 geniální nápad: Aplikovat diagonální lemma na formuli $\neg\mathsf{Dok}(x)$. Dostaneme *Gödelovu diagonální formuli*, označme ji g, takovou, že Q dokazuje formuli

$$\mathsf{g} \equiv \neg\mathsf{Dok}\,(\underline{\mathsf{gn}(\mathsf{g})}).$$

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 $\mathbf{N}$, ale nedokazatelná v T (pochopitelně ani její negace nemůže být dokazatelná).

Kdyby teorie T dokazovala g, pak by formule $\mathsf{Dok}(\underline{\mathsf{gn}(\mathsf{g})})$ byla pravdivá v $\mathbf{N}$ a tato formule je Σ-formule; tedy by ji Q (a tím spíše T) dokazovalo, tj. T by dokazovalo $\neg\mathsf{g}$, což je spor. Avšak teorie T je bezesporná, tedy nedokazuje g, tedy $\neg\mathsf{Dok}(\underline{\mathsf{gn}(\mathsf{g})})$ je pravdivá v $\mathbf{N}$, tedy g je pravdivá v $\mathbf{N}$.

(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 $\mathbf{N}$, ale nedokazatelný v T.

Důsledky *(mírně zjednodušeno)*:

1) Jelikož platí silná Gödelova věta o úplnosti (viz 4.2.1), nemůže Gödelova formule g logicky vyplývat z teorie T (neboť kdyby $T \models \mathsf{g}$, pak by $T \vdash \mathsf{g}$), 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.)

2) Každá "rozumná" aritmetika T (tj. *rekurzivně 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.

3) Predikátový důkazový kalkul 1. řádu je teorie PL^1 s prázdnou množinou speciálních axiomů. Proto je PL^1 *nerozhodnutelná.* Neexistuje algoritmus, který by rozhodoval, zda je daná formule φ v PL^1 dokazatelná (a tedy logicky pravdivá). 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 logicky pravdivá, pak algoritmus vydá v konečném počtu kroků odpověď ANO. Pokud je však φ pouze splnitelná (tedy není to ani tautologie ani kontradikce), pak algoritmus buďto odpoví NE, nebo nemusí vydat nikdy *žádnou* odpověď ("cykluje").

Definice 4.16 (*kategorická teorie*): Teorie je *kategorická*, jestliže každé dva její modely jsou izomorfní (tj. odhlédneme-li od různosti značení, existuje strukturálně jen jeden model).

Pozn:

1. Formální aritmetika 1. řádu není kategorickou teorií. (Formální aritmetika 2. řádu je kategorická, avšak za cenu ***neúplnosti kalkulu PL^2***.)
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.

Příklad 4.13:
Příkladem nekategorické teorie je teorie uspořádání V_1–V_6. Ukážeme, že existují dva neizomorfní modely této teorie. Jedním modelem je přirozené uspořádání ostře menší (<) na množině reálných čísel. Druhým modelem je uspořádání << na množině reálných čísel definované takto (*R* je zde množina racionálních čísel):

$$x<<y \Leftrightarrow_{df} [(x\in Q) \wedge (y\in R) \wedge (x<y)] \vee [(x\in R) \wedge (y\notin R)] \vee [(x\notin R) \wedge (y\notin R) \wedge (x<y)].$$

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 V_1–V_6 a přitom nejsou izomorfní.

Zbývá stručně pojednat o druhé Gödelově větě o neúplnosti.

Věta 4.11 (*Druhá Gödelova věta o neúplnosti*):
Žádná rozumná aritmetika *T* (splňující další rozumné podmínky, tj. rekurzivně axiomatizovaná, např. *Q*, *PA*) nedokazuje svou vlastní bezespornost.

Důkaz (náznak): Uvnitř teorie *T* lze vyjádřit tvrzení o bezespornosti teorie pomocí predikátu Dok, např. výrokem $\neg\mathrm{Dok}(\underline{gn(\varphi)}) \vee \neg\mathrm{Dok}(\underline{gn(\neg\varphi)})$ 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.

Tato druhá věta byla ve své době ještě více překvapivá než první věta o neúplnosti. Její důsledky na Hilbertův program byly téměř zničující. Nemáme tedy rozumný prostředek, jak dokázat jednou provždy konzistenci matematiky. Nevíme, jak „opravdu vypadají“ přirozená čísla, zda se nechovají někde „za horizontem“ příliš velká čísla nějak jinak, než předpokládáme. Jistě, to je vše pravda. Přesto to neznamená, že bychom přestali provozovat matematiku a logiku, vždyť nám slouží dobře již několik tisíciletí. A věříme, že budet sloužit i nadále a že se neobjeví nějaká zničující nekonzistence.

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.

Nicméně, Hilbertův program měl v dějinách vědy svůj nezastupitelný význam. Jeho pojem finitní metody dokazování je dnes rozvíjen především v tzv. intuicionistických či konstruktivistických logikách. Navíc, tento program spolu s velkými objevy Kurta Gödela v podstatě daly impuls ke vzniku nových disciplín, jako je teorie rekurzivních funkcí, teorie algoritmů, výpočtové složitosti, apod., a při troše nadsázky můžeme říct, že daly impuls ke vzniku teoretické informatiky. Ne náhodou byl von Neumann jeden z prvních, kdo pochopil Gödelovy objevy a jejich obrovský, převratný význam.

Kurt Gödel (nar. 28.4. 1906 v Brně, zemřel 14. ledna 1978 v Princeton, USA). 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:

"*Either mathematics is too big for the human mind*
or the human mind is more than a machine".

LITERATURA

(další zdroje ke studiu)

Brown, J.R.: *Philosophy of Mathematics.* Routledge, 1999.
Cmorej, P.: *Úvod do logickej syntaxe a sémantiky.* Bratislava: IRIS, 2001.
Gahér, F.: *Logika pre každého* (3. doplněné vydání). Bratislava: IRIS, 2003.
Gahér, F.: *Stoická sémantika a logika.* Univerzita Komenského Bratislava, 2006.
Hájek, P.: *Kurt Gödel, matematik a logik.* In: Malina, J., Novotný, J. (ed), Brno 1996.
Manna, Z.: *Matematická teorie programů.* SNTL Praha, 1981.
Smullyan, R.: *Jak se jmenuje tahle knížka?* Mladá Fronta, 1986.
Sochor, A.: *Klasická matematická logika.* Karolinum Praha, 2001.
Štěpán, J.: *Logika a logické systémy.* Votobia Olomouc, 1992.
Švejdar, V.: *Logika – neúplnost složitost a nutnost.* Academia Praha, 2002.