FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
UNIVERZITA KOMENSKÉHO
KATEDRA INFORMATIKY

Vybrané partie z logiky

EDUARD TOMAN

Bratislava 2005

Obsah

1 Úvod

Prirodzené východisko pre štúdium informatiky predstavuje matematická logika, ktorá charakterizuje zo všeobecného hľadiska vyjadrovacie prostriedky a pracovné postupy matematiky.

Jednou z charakteristických stránok matematiky je práca s abstraktnými objektami, či už sú to čísla, funkcie, relácie, plochy, štruktúty, prípadne niečo iné.

Matematická logika dáva skúmaniu takýchto objektov nový rozmer tým, že študuje jazyk matematiky, spôsoby, akými sú abstraktné objekty definované a zákonitosti, ktorými sa matematik riadi, pokiaľ uvažuje o matematických objektoch. Treba povedať, že matematická logika je v porovnaní s inými partiami matematiky pomerne mladá disciplína. Rok 1879, keď G. Frege publikoval svoj spis o predikátovej logike býva niekedy spájaný so zrodom tejto novej disciplíny.

Poznamenávame, že by bolo nesprávne sa domnievať, že až so vznikom matematickej logiky dostáva matematika logickú výstavbu a pevné usporiadanie. Pojem dôkazu, ktorý rozhodujúcim spôsobom ovplyvnil výstavbu matematiky, patrí už starovekej Gréckej matematike. Znamenal vznik matematiky ako deduktívnej vedy. Pripomeňme len známe Euklidove knihy, kde je geometria budovaná na základe niekoľko postulátov, z ktorých sú postupne odvodzované všetky ďalšie tvrdenia euklidovskej geometrie.

Každá matematická veta musí mať dôkaz, ktorý vychádza z explicitne vyjadrených predpokladov. Dôkaz musí ukázať, že veta je odvodená z predpokladov len rozumovou (logickou) úvahou. Matematik (mlčky) predpokladá, že rozumie pojmu dôkaz a že bude schopný presvedčiť sa o správnosti každého kroku odvodenia. Úlohou rozhodcu v sporných prípadoch od začiatku hrala klasická logika, ktorej konečnú podobu formuloval Aristoteles. Matematická logika vzniká až neskôr, v dobe, keď vrcholí snaha po presnom vyjadrení základov matematiky vyjadrením pojmu čísla, funkcie a ďalších pojmov, ktoré sa dostali do popredia záujmu už rozvinutej matematickej analýzy, algebry a geometrie.

Nový a nečakaný impulz k rozvoju matematickej logiky dali objavy paradoxov teórie množín na prelome storočia. Otázku paradoxov, z ktorých menujeme aspoň Russellov paradox, už nebolo možné riešiť prostriedkami klasickej logiky. Jedno z prvých riešení podal Russell sám v rámci tzv. teórie typov. Dnes najrozšírenejším riešením je axiomatická výstavba teórie množín na základe predikátovej logiky prvého rádu.

Matematická logika prešla od počiatku minulého storočia rýchlym vývojom, rozvinula mnoho účinných metód, ktoré prispeli k vyjasneniu základov matematiky a nachádzajú svoje uplatnenie v rôznych častich matematiky, matematickej informatiky i v technike. V súčasnom období jazyku i metódam matematickej logiky venujú zvýšenú pozornosť lingvisti, fyziológovia, ekonómovia i predstavitelia rôznych ďalších vedeckých disciplín.

V prednáške z matematickej logiky si kladieme cieľ vhodnou formou vyložiť pojmy a metódy matematickej logiky, najmä syntax a sémantiku logiky prvého rádu. Ukážeme použitie predikátového počtu prvého rádu na zápis vlastností matematických štruktúr.

Predložený text vznikol prepísaním prednášok z logiky pre študentov odboru informatika. Aj touto cestou vyjadrujem srdečnú vďaku študentovi *Martinovi Dzurenkovi*, ktorý sa podujal túto prácu vykonať.

Bratislava, na Jozefa 2004 Eduard Toman

1.1 Jazyk logiky

Najprv budeme analyzovať jazyk matematiky, aby sme ukázali na jeho podstatné súčasti, ktoré musí logika zachytiť, pokiaľ chce k základom matematiky niečo podstatné povedať.

V matematike pracujeme s množstvom rôznych objektov, napríklad to môžu byť čísla, body, geometrické útvary, zobrazenia alebo zložitejšie matematické štruktúry. Niektoré objekty majú svoje vlastné mená, napríklad nula, imaginárna jednotka, identické zobrazenie, Eulerove číslo, Ludolfovo číslo, ktoré označujú jeden celkom určitý matematický objekt. K označeniu týchto špeciálnych objektov sa často používajú ustálené symboly, napríklad 0, i, i_d, e, π, ktorým hovoríme *konštanty*.

V matematike taktiež používame všeobecné názvy, ktoré určujú povahu objektov, napríklad číslo, bod, štvorec, ale inak neurčujú, o ktoré číslo, bod a štvorec sa jedná. Také všeobecné názvy používame aj v bežnom jazyku. K označeniu takých všeobecných názvov sa v matematike používajú symboly, ktorým hovoríme *premenné*. Ide spravidla o písmená z konca abecedy $x, y, z, \ldots$ Pri práci s objektami v matematike používame *operácie*, napríklad ak pracujeme s číslami, používame operáciu súčtu, súčinu, rozdielu, prípadne iné. Často používané operácie majú svoje zvláštne označenie, napríklad $+, \cdot, -$. Operácia (povedzme súčet) je vlastne zobrazenie, funkcia, ktorá niekoľkým objektom (napríklad číslam) priraďuje výsledok (ich súčet). Jazyk logiky bude teda obsahovať symboly pre operácie, ktorým budeme hovoriť *funkčné symboly*. Ku každému funkčnému symbolu je dané prirodzené číslo, ktoré vyjadruje árnosť symbolu, teda počet argumentov, na ktoré je symbol aplikovaný. Ak je árnosť symbolu rovná prirodzenému číslu n, hovoríme, že symbol je n-árny. Pre $n \leq 3$ sa používajú zaužívané názvy: symboly pre súčet a súčin sú *binárne* (majú árnosť dva), stretávame sa s *unárnymi* symbolmi (majú árnosť jedna), napríklad symbol S, ktorý označuje funkciu, ktorej hodnota pre dané prirodzené číslo x je nasledujúce prirodzené číslo, teda $S(x) = x + 1$. Symboly, ktoré majú árnosť tri sa nazývajú *ternárne*. Vo všeobecnom prípade sa stretávame s n-árnymi symbolmi, ktoré označujú funkciu n premenných. Je prirodzené chápať konštanty, ktoré určujú konkrétny objekt (nezávislý na iných objektoch) ako 0-árne funkčné symboly, teda symboly, ktoré nevyžadujú žiadny argument.

V matematike vyjadrujeme taktiež vzťahy medzi objektami, napríklad *"číslo x je rovné dvojnásobku y"*, *"x je menšie ako 1"*. Pre niektoré vzťahy sa používajú ustálené označenia, napríklad = alebo <. Výrazy $x = 2y$ a $x < 1$ sú symbolickým vyjadrením vzťahov medzi číslami x, y, ktorých slovnú podobu sme uviedli v uvodzovkách.

Všimnime si, že každý z týchto výrazov zastupuje jednoduchú vetu slovenského jazyka. V danom prípade išlo o vzťah medzi dvoma číslami, sú možné aj všeobenejšie vzťahy, napríklad "číslo x leží medzi y a z", ktorý určuje vzťah medzi troma číslami. Jazyk logiky teda bude obsahovať symboly, ktoré vyjadrujú vzťah medzi indivíduami. Hovoríme im *predikátové symboly*. Ku každému predikátovému symbolu je dané prirodzené číslo, árnosť symbolu, ktoré udáva počet argumentov. Teda symboly = a < sú binárne, vyjadrujú vzťah medzi dvoma číslami, vo všeobecnosti sa môžeme stretnúť s n-árnymi predikátovými symbolmi pre $n \geq 1$. Obdobou 0-árnych funkčných symbolov by mohli byť "logické konštanty" označujúce pravdu a nepravdu, ale nebudeme ich používať.

Jazyk logiky bude tiež obsahovať symboly pre logické spojky, ktoré sú obdobou spojek v bežnom jazyku a dovoľujú spájať jednoduché výrazy do zložitejších. K logickým spojkám patria symboly $\wedge$ pre kojunkciu, $\vee$ pre disjunkciu, $\rightarrow$ pre implikáciu, $\leftrightarrow$ pre ekvivalenciu a symbol $\neg$, ktorý označuje negáciu.

Ak použijeme predošlé výrazy, môžeme úlohu logických spojok ilustrovať nasledujúcim príkladom:

$\neg x = 2y$	čítame	"neplatí $x = 2y$"
$x = 2y \wedge x < 1$	čítame	"$x = 2y$ a $x < 1$"
$x = 2y \vee x < 1$	čítame	"$x = 2y$ alebo $x < 1$"
$x = 2y \rightarrow x < 1$	čítame	"$x = 2y$ implikuje $x < 1$"
$x = 2y \leftrightarrow x < 1$	čítame	"$x = 2y$ práve vtedy, keď $x < 1$"

Matematika používa taktiež fomulácie *"pre každé x platí ..."* alebo *"existuje x také, že ..."*. Také jazykové obraty budeme nazývať kvantifikácia premenných: Jazyk logiky bude obsahovať aj symboly $\forall$ a $\exists$, ktorým hovoríme *všeobecný* (univerzálny alebo veľký) kvantifikátor a *existenčný* (alebo malý) kvantifikátor.

V jazyku logiky uplatňujeme aj pomocné symboly, ktoré používame k zlepšeniu čitateľnosti výrazov. Pomocné symboly sú spravidla rôzne druhy zátvoriek $(,), [,], \{, \}$ atď. Ak x je premenná, potom výrazy

$(\forall x)(x < 1)$	čítame	"pre každé x platí $x < 1$"
$(\exists x)(x = 2y)$	čítame	"existuje x také, že $x = 2y$"

Ukazuje sa, že všetky dôležité obraty jazyka matematiky môžeme zachytiť vhodnou voľbou odpovedajúcich symbolov v umelom symbolickom jazyku. Matematické tvrdenia sú potom vyjadrené určitými výrazmi tohoto symbolického jazyka. Pre potreby rôznych matematických teórií je možné zostrojiť rôzne formálne jazyky.

Predchádzajúce úvahy môžeme zhrnúť nasledujúcou definíciou:

Definícia: *Jazyk 1. rádu obsahuje tieto symboly:*

1. *premenné* $x_1, x_2, \ldots, y_1, y_2, \ldots$ *ktorých je nekonečne veľa*
2. *funkčné symboly* $f, g, h, \ldots$ *ku každému symbolu je priradené prirodzené číslo väčšie alebo rovné* 0*, ktoré vyjadruje jeho -árnosť*
3. *predikátové symboly* $P, Q, R, \ldots$ *ku každému symbolu je priradené prirodzené číslo väčšie alebo rovné* 1*, ktoré vyjadruje jeho -árnosť*
4. *logické spojky* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$*, ktoré vyjadrujú v uvedenom poradí negáciu, konjunkciu, disjunkciu, implikáciu a ekvivalenciu*
5. *kvantifikátory* $\forall, \exists$ *– všeobecný (veľký, univerzálny) kvantifikátor, existenčný (malý) kvantifikátor*
6. *pomocné symboly – zátvorky*

Niektoré symboly sú spoločné pre všetky formálne jazyky – takéto symboly nazývame logické – sú to symboly pre premenné, logické spojky, kvantifikátory, pomocné symboly a symbol $=$, ktorý vyjadruje rovnosť (pokiaľ je v jazyku obsiahnutý).

Zostávajúce symboly, teda symboly pre funkcie a predikáty (mimo $=$) nazývame špeciálne. Sú to symboly, ktoré označujú špeciálne operácie a vzťahy v jednotlivých oblastiach matematiky. Je zrejmé, že jazyk je určený udaním svojich špeciálnych symbolov.

Pokiaľ jazyk obsahuje symbol $=$ pre predikát rovnosti, hovoríme, že ide o jazyk s rovnosťou. V opačnom prípade ide o jazyk bez rovnosti. Napríklad jazyk teórie množín je jazyk prvého rádu s rovnosťou, ktorý má jediný špeciálny symbol $\in$, binárny predikátový symbol, ktorý vyjadruje patričnosť prvku do množiny.

Zo symbolov jazyka sa podľa istých pravidiel tvoria *termy* a *formuly*. Zatiaľ nebudeme popisovať syntaktické pravidlá pre termy alebo formuly. Obmedzíme sa na konštatovanie, že termy zodpovedajú "dobre uzátvorkovaným" výrazom, ktoré označujú výsledok po vykonaní naznačených operácií a formuly zodpovedajú matematickým tvrdeniam.

Napríklad výraz $f(g(x,y),h(x),x)$, kde x,y, sú premenné a f,g,h sú postupne v uvedenom poradí ternárny, binárny a unárny funkčný symbol, je term. Výrazy $x=2y$ a $x<1$ sú jednoduché formuly.

Jazyky, ktoré sme popísali sa nazývajú *jazyky prvého rádu*. Premenné jazyka prvého rádu sú všeobecné názvy pre indivíduá (napríklad číslo). Jazyk neobsahuje premenné pre množiny indivíduí (napríklad množiny čísel, zobrazení, relácií a podobne). Kvantifikovať môžeme teda len premenné pre indivíduá. Tým sa jazyky prvého rádu líšia od jazykov vyšších rádov, kde napríklad jazyky druhého rádu obsahujú premenné pre množiny indivíduí, jazyky tretieho rádu obsahujú premenné pre množiny množín indivíduí a dovoľujú kvantifikovať napríklad relácie, zobrazenia a podobne.

Logika, ktorá pracuje len s jazykmi prvého rádu sa nazýva *logika prvého rádu*. Je celý rad dôvodov, pre ktoré možno logiku prvého rádu považovať za základný jazyk matematiky. Vzhľadom na logiky vyšších rádov má jednoduchší jazyk, ktorý sa neodvoláva na pojem množiny. Preto logika prvého rádu môže slúžiť ako základná teória aj pre teóriu množín. Pokúsime sa ilustrovať možnosti (i obmedzenia) logiky prvého rádu na niekoľkých príkladoch z algebry a teórie množín.

Na popísanie usporiadaných množín nám stačí jeden špeciálny symbol $<$, binárny predikátový symbol pre usporiadanie. Pracujeme s jazykom s rovnosťou, ktorý obsahuje symbol $<$. Čiastočné usporiadanie je charakterizované formulami:

$$(\forall x)(\neg(x<x))$$

$$(\forall x)(\forall y)(\forall z)[(x<y\wedge y<z)\rightarrow x<z]$$

Prvá z nich stanovuje, že usporiadanie nie je reflexívne a druhá vyjadruje tranzitívnosť usporiadania.

K štúdiu telies je možno použiť jazyk s rovnosťou, ktorý obsahuje špeciálne symboly $0,1,+,\cdot$. Prvé dva z nich sú konštanty označujúce nulu a jednotku, druhé dva sú binárne funkčné symboly označujúce operácie sčítania a násobenia. V tomto jazyku je možné vyjadriť obvyklé axiómy telesa; to nechávam čitateľom ako cvičenie. Ak x je premenná, potom termy $x,(x+x),x+(x+x),x+(x+(x+x)),\ldots$ budeme označovať $1\times x,2\times x,3\times x,4\times x,\ldots$ a budeme im hovoriť prirodzené násobky x, výraz $p\times x$, kde p je prirodzené číslo, zastupuje term, ktorý môže byť dosť dlhý. Pokiaľ pre nejaké nenulové prirodzené číslo p v určitom telese platí formula $p\times 1=0$ hovoríme, že teleso má konečnú charakteristiku. Najmenšie číslo p, pre ktoré tento vzťah platí je charakteristikou telesa. Ak pre žiadne nenulové p vzťah neplatí hovoríme, že teleso má charakteristiku nula. Ak pridáme k axiómam telesa všetky formuly tvaru $p\times 1\neq 0$ pre nenulové prirodzené čísla p, dostávame axiómy telesa charakteristiky nula. Je prirodzené, keď si položíme otázku, či telesá charakteristiky nula je možné axiomatizovať konečným počtom axióm. Negatívna odpoveď je obsiahnutá v nasledovnom tvrdení.

Tvrdenie 1: *Každá konečná množina formúl, ktoré sú splnené vo všetkých telesách charakteristiky nula, platí aj vo všetkých telesách dosť veľkej konečnej charakteristiky.*

Toto tvrdenie je jednoduchým dôsledkom vety o kompaktnosti predikátovej logiky prvého rádu. S vetou o kompaktnosti sa zoznámime neskôr. Vráťme sa ešte k príkladu telies charakteristiky nula, všimnime si, že tieto telesá je možné charakterizovať jedinou axiómou, ak zavedieme ešte jeden druh premenných pre prirodzené čísla a dovolíme ich kvantifikáciu. Ak p je premenná pre prirodzené čísla, potom namiesto predošlých formúl vystačíme s jedinou formulou $(\forall p)(p \neq 0 \rightarrow p \times 1 \neq 0)$.

Slabá logika druhého rádu je teda silnejšia než logika prvého rádu. Z toho, čo sme povedali o dôkaze Tvrdenia 1 vyplýva, že veta o kompaktnosti neplatí pre slabú logiku druhého rádu. Zostaneme ešte v jazyku prvého rádu teórie telies. Poznamenávame, že niektoré vlastnosti, napríklad, že ide o teleso reálnych čísel, nie je možné v tomto jazyku vyjadriť ani nekonečným počtom formúl. Dôsledkom Löwenheim-Skolemovej vety je aj nasledujúce tvrdenie.

Tvrdenie 2: *Žiadna množina formúl jazyka prvého rádu teórie telies neurčuje teleso reálnych čísel jednoznačne až na izomorfizmus.*

Uvedené výsledky so stúpajúcou gradáciou ukazujú na obmedzenia dané jazykom prvého rádu. Môže teda logika prvého rádu vyhovieť všetkým požiadavkám tak, aby bola spoľahlivým východiskom k budovaniu matematiky? Prv než odpovieme, vráťme sa k uvedeným príkladom. V prípade telies charakteristiky nula spočíva obtiaž v tom, že použitý jazyk prvého rádu mal premenné len pre prvky telesa a nie pre prirodzené čísla. V prípade telesa reálnych čísel ide o to, že nemáme možnosť hovoriť o množinách reálnych čísel a vyjadriť tak vetu o supréme, ktorá je dôležitou charakteristikou telesa reálnych čísel. Tieto obtiaže odpadnú, ak použijeme jazyk teórie množín. V ňom môžeme pomocou jediného druhu premenných (pre množiny) popisovať jednotlivé čísla (prvky telesa), množiny čísel a prirodzené čísla. Tým sa vraciame k našej počiatočnej téze, že logika prvého rádu môže byť chápaná ako základ k budovaniu matematiky. Téza je plne oprávnená, pokiaľ budujeme matematiku na množinovom základe. Tento fakt poukazuje na špecifickú úlohu teórie množín v matematike. Predchádzajúca úvaha naznačuje, že redukcia logických systémov vyššieho rádu do logiky prvého rádu je možná prostredníctvom teórie množín.

1.2 Formálne systémy logiky

Popísali sme jazyk logiky prvého rádu a zoznámili sme sa s jeho vyjadrovacími možnosťami. Na vhodnom mieste podrobne popíšeme pravidlá, ktorými sa riadi syntax dvoch dôležitých typov výrazov - termov a formúl. Zatiaľ sa uspokojíme s konštatovaním, že termy označujú určité indivíduá, ktoré sú výsledkom naznačených operácií a formuly sú výrazy, ktoré vyjadrujú matematické tvrdenia. Povedali sme, že každé tvrdenie – *veta*, musí mať dôkaz, ktorý je odvodený z explicitne vyjadrených predpokladov, len logickou úvahou. Takéto vymedzenie si kladie prinajmenšom dve prirodzené otázky:

Je možné pojem dôkazu presne definovať?
Aké sú logické pravidlá, ktorými sa riadi odvodzovanie?

Odpoveď na prvú otázku je jednoduchšia, už máme pripravený jazyk logiky, v ktorom bude možné dôkazy vyjadrovať. Ako sme už prv ukázali jazyk prvého rádu je symbolický a matematické tvrdenia sú vyjadrené konečnými postupnosťami symbolov – formulami. Prirodzený jazyk, v našom prípade slovenčina, ktorým o matematike hovoríme, je odlišný a zostáva v úlohe *metajazyka*. Tým sa vyhneme nebezpečiu sémantických paradoxov, ku ktorým môže dôjsť, ak používame prirodzený jazyk v oboch rovinách teda ako jazyk matematickej teórie i ako metajazyk, ktorým o teórii hovoríme (paradox klamára a iné). Zvolený prístup zdôrazňuje finitné hľadisko, predmetom štúdia sú formuly, teda konečné postupnosti symbolov, ktoré máme (aspoň v princípe) plne pod kontrolou.

Dôkaz možno definovať ako konečnú postupnosť formúl, ktorej každý člen je buď nejaké základné tvrdenie – *axióma* alebo je z niektorých predchádzajúcich členov postupnosti odvodená jedným z odvodzovacích pravidiel.

Definícia: *Formálny systém tvoria nasledovné zložky:*

1. *jazyk, z ktorého symbolov vytvárame konečné postupnosti, najmä termy a formuly*
2. *axiómy – sú isté formuly, ktoré pokladáme za základné pravdivé tvrdenia*
3. *odvodzovacie pravidlá – sú to syntaktické pravidlá, pomocou ktorých sa z jednej alebo viacej formúl vytvára ďalšia odvodená formula*

Definícia: *Dôkazom vo formálnom systéme je konečná postupnosť formúl, ktorej členmi sú niektoré axiómy a formuly odvodené z predchádzajúcich členov postupnosti podľa odvodzovacích pravidiel*

Definícia: *Hovoríme, že formula A je teorémou formálneho systému alebo že je odvoditeľná vo formálnom systéme, ak existuje jej dôkaz; t.j. konečná postupnosť formúl, ktorej posledným členom je formula A (počet členov postupnosti sa nazýva dĺžka dôkazu)*

Uvedená definícia vcelku ideálne vyjadruje intuitívny pojem dôkazu. Odvodzovanie vychádza z predpokladov a postupuje podľa presných syntaktických pravidiel, ktoré sú kontrolovateľné v každom kroku.

Prejdime teraz k druhej otázke, aké sú logické pravidlá, ktorými sa riadi odvodzovanie? Na rozdiel od prvej predstavuje druhá otázka hlboký problém základov matematiky a má i filozofický rozmer. V intuitívnom pojatí sa jednotlivé kroky dôkazu odvodzujú z predpokladov len rozumovou (logickou) úvahou. Tá je vo formálnom odvodzovaní zastúpená voľbou odvodzovacích pravidiel a voľbou niektorých axióm. Stojíme teda pred otázkou, aké axiómy logiky a aké odvodzovacie pravidlá máme voliť. Ich voľbou ovplyvňujeme triedu formúl, ktoré je možné v danom formálnom systéme odvodiť. V matematike najzaužívanejšia takzvaná klasická predikátová logika prvého rádu rieši túto otázku odkazom na sémantiku. Logické axiómy sú "univerzálne platné" formuly, to znamená formuly, ktoré sú "pravdivé" pri každej interpretácii symbolov jazyka a odvodzovacie pravidlá sú "korektné" v tom zmysle, že z pravdivej formuly odvodzujú vždy opäť "pravdivú" formulu. Je zrejmé, že za axiómy logiky nemusíme brať všetky "univerzálne platné" formuly, pokiaľ sa nám z nich podarí vybrať určitú podmnožinu a zvolíme odvodzovacie pravidlá tak, že z vybraných formúl môžeme všetky ostatné "univerzálne platné" formuly dokázať. formálny systém predikátovej logiky, ktorý vznikne popísaným spôsobom si vyslúžil prívlastok klasický, pretože je v istom zmysle rozšírením klasickej logiky.

Budovanie logiky je účelné rozdeliť do niekoľkých etáp, ktoré tvoria ucelené časti logiky a majú aj svoje určité názvy. Najprv popíšeme axiómy a odvodzovacie pravidlá, ktoré určujú vlastnosti logických spojok. Odpovedajúci formálny systém sa nazýva *výroková logika*. V ďalšom pridáme axiómy a odvodzovacie pravidlá pre kvantifikátory, čím vznikne *predikátová logika bez rovnosti*. Nakoniec pridaním axióm pre predikát rovnosti je daná *predikátová logika s rovnosťou*. V jednotlivých krokoch sa dozvieme, aký obsah majú pojmy "pravdivý", "korektný" a ďalšie pojmy, ktoré sme doposiaľ používali v uvodzovkách. Adekvátnosť formálneho systému na riešenie druhej otázky bude vyjadrená vetou o úplnosti, ktorá tvrdí, že formálny systém logiky odvodzuje práve všetky "univerzálne platné" formuly.

2 Výroková logika

2.1 Syntax výrokovej logiky

Pri štúdiu vlastností logických spojok odhliadneme od ostatných symbolov, to znamená od špeciálnych symbolov, kvantifikátorov a symbolov pre rovnosť. To čo robíme pripomína rozbor súvetia, pri ktorom sa nepúšťame do rozboru jednotlivých viet. Jednotlivé vety chápeme ako nedeliteľný celok, ako základné komponenty súvetia. V jazyku výrokovej logiky sa tento prístup prejavuje tým, že je daná množina takzvaných prvotných formúl, ktoré sú základnými zložkami všetkých ostatných formúl. Každá formula vznikne z konečného počtu prvotných formúl použitím logických spojok.

Definícia: *Nech P je neprázdna množina; jej prvky nazveme prvotné formuly. Môžu to byť vety prirodzeného jazyka, slová nejakého formálneho jazyka alebo len písmená* $(p, q, r, \ldots, p_1, p_2, \ldots)$

Definícia: *Jazyk L(P) výrokovej logiky nad množinou P obsahuje okrem prvkov množiny P symboly pre logické spojky $(\neg, \wedge, \vee, \rightarrow, \leftrightarrow)$, ďalej pomocné symboly (rôzne typy zátvoriek). Hovoríme, že P je množina prvotných formúl jazyka L(P) resp. L_p*

Definícia: *Výrokové formuly jazyka L_p definujeme pomocou nasledujúcich syntaktických pravidiel:*

1. *každá prvotná formula $p \in P$ je výroková formula*
2. *ak sú výrazy A, B výrokové formuly, potom výrazy $\neg A, (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$ sú výrokové formuly*
3. *každá výroková formula vznikne konečným použitím pravidiel (1) a (2)*

Poznámka: Iné výrokové formuly vo výrokovej logike neexistujú.

Uvedená definícia popisuje spôsob, akým sa zložitejšie formuly tvoria z jednoduchších. Hovoríme, že ide o induktívnu definíciu. Formula je popísaná ako výraz, ktorý vznikne z konečného počtu prvotných formúl, symbolov pre logické spojky a pomocných symbolov podľa pravidiel 1—3. Toto pojatie zdôrazňuje finitné hľadisko. Každá formula je konečný objekt, ktorý máme (aspoň v princípe) plne pod kontrolou. Množina formúl, pravdivosť a dokázateľnosť formúl sú predmetom štúdia.

Zo všeobecného hľadiska je toto vymedzenie príliš špeciálne. Pri mnohých logických úvahách nezáleží na tom, čo vlastne formuly sú. Môžeme pracovať namiesto výrazov s prirodzenými číslami, ktoré sú ich kódy a podobne. Zvolené pojatie sa neodvoláva na žiadne zložitejšie štruktúry a plne vyhovuje požiadavkám presného vymedzenia základov matematiky.

Definícia: *Nech A je formula L_p výrokovej logiky. Jej podformulou je:*

1. *ona sama; ak A je prvotná formula jazyka L_p*
2. *ona sama; a každá podformula B, ak $A = (\neg B)$*
3. *ona sama; a každá podfomula formúl B a C, ak $A = (A \wedge B)$, $A = (A \vee B)$, $A = (A \rightarrow B)$ alebo $A = (A \leftrightarrow B)$*

4. *žiadnych iných podformúl okrem tých, čo sú opísané v bodoch 1—3 niet*

Príklad: Ak $P = \{p, q, r, s\}$, potom p, q, r, s sú formuly jazyka L_p podľa (1), výrazy $(p \vee q)$ a $(q \wedge r)$ sú formuly podľa (2) a nakoniec výraz $((p \vee q) \to (q \wedge r))$ je taktiež formula podľa (3). Všetky sú zároveň podformuly formuly $((p \vee q) \to (q \wedge r))$. Podobne výraz $(p \to (q \to (t \to s)))$ je výroková formula, ktorej podformuly okrem jej samej sú formuly p, q, r, s a formuly $(r \to s)$, $q \to (r \to s)$. Je zrejmé, že výrazy $(\to p)$, $(\to\to p)$, $pq\wedge$ nie sú výrokové formuly.

Poznámka: Pri zápise formúl prihliadneme k tomu, že pomocné symboly (zátvorky) majú predovšetkým zlepšiť čitateľnosť formúl. Pri písaní zátvoriek dovoľujeme určitú voľnosť, pokiaľ to nie je na ujmu zrozumiteľnosti. Je napríklad obvyklé vynechávať krajné zátvorky, ktoré sú definíciou formuly predpísané, ale v skutočnosti nič neoddeľujú. Píšeme napríklad $p \to (q \to r)$ namiesto $(p \to (q \to r))$. Podľa potreby budeme zavádzať ďalšie podobné dohody.

2.2 Sémantika výrokovej logiky

Ďalším naším cieľom je ukázať ako pravdivosť formuly závisí na pravdivosti jej prvotných zložiek.

Definícia:

- *Pravdivostné ohodnotenie (valuácia) prvotných formúl jazyka L_p je každé zobrazenie v: $P \to \{0,1\}$, ktoré každej prvotnej formule $p \in P$ priradí hodnotu 0 (nepravda) alebo hodnotu 1 (pravda)*

- *Indukciou podľa dĺžky formuly definujeme rozšírenie $\overline{v}$ zobrazenia v na množine všetkých formúl jazyka L_p:*

$\overline{v}(A) = v(A)$	ak A je prvotná formula		
$\overline{v}(\neg A) = 0$	ak $\overline{v}(A) = 1$	ináč	$\overline{v}(\neg A) = 1$
$\overline{v}(A \wedge B) = 1$	ak $\overline{v}(A) = \overline{v}(B) = 1$	ináč	$\overline{v}(A \wedge B) = 0$
$\overline{v}(A \vee B) = 0$	ak $\overline{v}(A) = \overline{v}(B) = 0$	ináč	$\overline{v}(A \vee B) = 1$
$\overline{v}(A \to B) = 0$	ak $\overline{v}(A) = 1$ a $\overline{v}(B) = 0$	ináč	$\overline{v}(A \to B) = 1$
$\overline{v}(A \leftrightarrow B) = 1$	ak $\overline{v}(A) = \overline{v}(B)$	ináč	$\overline{v}(A \leftrightarrow B) = 0$

- *Hovoríme, že $\overline{v}(A)$ je pravdivostná hodnota formuly A pri ohodnotení v. Formula A je pravdivá pri ohodnotení v, ak $\overline{v}(A) = 1$, inak je formula A nepravdivá.*

Definícia:

1. *Výroková formula A je tautológia, ak $\overline{v}(A) = 1$ pre ľub. ohodnotenie v.*

2. *Výroková formula A je splniteľná, ak $\overline{v}(A) = 1$ pre nejaké ohodnotenie v. Ohodnotenie s touto vlastnosťou nazývame model formuly A.*

3. *Množina formúl T je splniteľná, ak existuje v také, že $\overline{v}(A) = 1$ pre ľubovoľnú formulu $A \in T$. Takéto ohodnotenie v nazývame model T.*

4. *$T \models A$ (čítame "A je tautologický dôsledok T"), ak $\overline{v}(A) = 1$ pre každé ohodnotenie v, ktoré je modelom T.*

Poznámka: Ak T je prázdna množina, tak namiesto T $\models$ A píšeme $\models$ A (t.j. $\overline{v}(A) = 1$ pre ľubovoľné ohodnotenie v prvotných formúl L_p)

Poznámka:

1. Modelom prázdnej množiny formúl je ľubovoľné ohodnotenie. Preto $\models A \leftrightarrow A$ je tautológia.
2. Ak T nie je splniteľná (je nesplniteľná), potom ľubovoľná formula je jej tautologickým dôsledkom.
3. Ak je T_0 nesplniteľná množina formúl a $T_0 \subseteq T$, potom aj T je nesplniteľná.
4. Ľahko sa vidí, že ak $T \models A \rightarrow B$ a $T \models A$, tak potom $T \models B$, špeciálne ak $\overline{v}(A \rightarrow B) = 1 = \overline{v}(A)$, tak potom $\overline{v}(B) = 1$.

Príklad: Základné tautológie:

- $(A \vee \neg A)$ – *zákon vylúčenia tretieho*
- $\neg(A \wedge \neg A)$ – *zákon vylúčenia sporom*
- $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$ – *De Morganove pravidlá*
- $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$ – *De Morganove pravidlá*
- $\neg\neg A \leftrightarrow A$ – *zákon dvojitej negácie*

2.3 Veta o kompaktnosti

Lema: *Množina všetkých výrokových formúl utvorených zo spočítateľnej množiny prvotných formúl je spočítateľná množina.*

Dôkaz: Nech f je prosté zobrazenie množiny P všetkých prvotných formúl na množinu prirodzených čísel. Definujme zobrazenie f' na množine $P' = P \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$. Pre $x \in P$ nech $f'(x) = f(x) + 10$, pre $x \notin P$ je funkcia daná tabuľkou

x	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\neg$	$($	$)$
$f'(x)$	1	2	3	4	5	6	7

Nech $\{q_i\}_{i \in N}$ je nekonečná rastúca množina prvočísel. Nech $s_1, s_2, \ldots, s_k$ je slovo z abecedy P'. Definujme funkciu F nad všetkými slovami z abecedy P' takto:

$$F(s_1 s_2 \ldots s_k) = q_1^{f'(s_1)} q_2^{f'(s_2)} \ldots q_k^{f'(s_k)}$$

Táto funkcia je prostá, teda formúl je najviac toľko ako prir. čísel. Keďže existuje nekonečne veľa formúl, tak podľa Cantor–Bernsteinovej vety je ich práve $\aleph_0$.

Veta: *Množina T formúl výrokovej logiky je splniteľná práve vtedy, keď ľubovoľná konečná $T_0 \subseteq T$ je splniteľná.*

Dôkaz: Nech T je splniteľná, teda existuje aspoň jedno ohodnotenie v prvotných formúl

jazyka L_p, že $\forall A \in T : \overline{v}(A) = 1$. Pre každú podmnožinu $T_0 \subseteq T$ to musí samozrejme platiť tiež.

Obrátene: Nech množina formúl T má model; teda $\exists v\ \forall A \in T : \overline{v}(A) = 1$. Nech $S = \{B | B \in L_p \wedge \overline{v}(B) = 1\}$. Potom množina S má tieto vlastnosti:

1. $S \supseteq T$
2. každá podmnožina množiny S je splniteľná
3. pre ľuboboľnú formulu A uvažovaného jazyka L_p je buď $A \in S$ alebo $\neg A \in S$, ale nikdy nie súčasne

Ak každá podmnožina T_0 množiny T je splniteľná, tak je aj množina formúl T splniteľná. Dôkaz rozdelíme na 2 časti:

1. najprv sa presvedčíme, že ak existuje množina S s vlastnosťami (1), (2) a (3) potom pomocou nej ľahko možno definovať model T
2. skonštruujeme takú množinu S

1. Nech v je ohodnotenie také, že pre ľubovoľnú prvotnú formulu p platí $v(p) = 1 \leftrightarrow p \in S$. Indukciou vzhľadom na dĺžku konštrukcie formuly A ukážeme, že pre ľubovoľnú formulu A platí: $\overline{v}(A) = 1 \leftrightarrow A \in S$ (uvedomme si, že formula je konečný objekt).

1. báza indukcie: platí vďaka výberu v
2. indukčný krok: keďže spojky $\neg, \wedge$ tvoria úplný systém, stačí nám uvažovať iba formuly tvorené práve týmito spojkami
   - Uvažujme $\neg A$.
     Platí $\overline{v}(\neg A) = 0$, ak $\overline{v}(A) = 1$ a zároveň $\overline{v}(\neg A) = 1$, ak $\overline{v}(A) = 0$. S využitím indukčného predpokladu $\overline{v}(A) = 1 \leftrightarrow A \in S$ dostávame $\overline{v}(\neg A) = 1 \leftrightarrow \neg A \in S$
   - Uvažujme $A_1 \wedge A_2$.
     Nech $\overline{v}(A_1 \wedge A_2) = 1$. Potom $\overline{v}(A_1) = 1$ aj $\overline{v}(A_2) = 1$. Podľa IP teda $A_1 \in S$ aj $A_2 \in S$. Chceme dokázať, že aj $A_1 \wedge A_2 \in S$. Postupujme sporom: Nech $A_1 \wedge A_2 \notin S$, teda $\neg(A_1 \wedge A_2) \in S$. Uvažujme množinu $\{A_1, A_2, \neg(A_1 \wedge A_2)\} \subseteq S$. Táto množina nie je splniteľná, čo nám dáva požadovaný spor.
     Obrátene nech $A_1 \wedge A_2 \in S$. Teda $A_1 \in S$ a $A_2 \in S$. Podľa IP teda $\overline{v}(A_1) = 1$ aj $\overline{v}(A_2) = 1$. Zo sémantických vlastností spojky $\wedge$ teda dostávame $\overline{v}(A_1 \wedge A_2) = 1$.

Teda existuje model S, ktorý je zároveň modelom pre T.

2. Na základe predošlej lemy vieme, že formúl výrokovej logiky je spočítateľne veľa a teda sa dajú zoradiť do postupnosti. Nech je to postupnosť $\{A_i\}_{i \in N}$. Zostrojme množiny S_i nasledovne:

$S_0 = T$

$S_{i+1} = S_i \cup \{A_i\}$ ak každá konečná podmnožina množiny $S_i \cup \{A_i\}$ je splniteľná

$S_{i+1} = S_i \cup \{\neg A_i\}$ v opačnom prípade

Potom množina $S = \bigcup_{i \geq 0} S_i$ má požadované vlastnosti. ♣

Dôsledok: *Nech T je množina formúl a A je formula výrokovej logiky. Potom $T \models A \leftrightarrow T' \models A$ platí pre nejakú konečnú podmnožinu $T' \subseteq T$.*

Dôkaz: Platí: $T \models A \leftrightarrow T \cup \{\neg A\}$ *je nesplniteľná.* Z predošlej vety vyplýva, že musí existovať konečná nesplniteľná množina $T_0 \subseteq T \cup \{\neg A\}$. Definujme $T' = T_0 \setminus \{\neg A\}$. Potom platí: $T_0 = T' \cup \{\neg A\}$ *je nesplniteľná* $\leftrightarrow T' \models A$.

Príklad: Usporiadanú dvojicu (V, R) nazveme neorientovaný graf, ak R je symetrická a antireflexívna relácia na množine V, t.j. ak R spĺňa podmienky:

$$(\forall x)(\forall y)(xRy \rightarrow yRx) \qquad a \qquad (\forall x)\neg(xRx)$$

Graf (V', R') je podgraf grafu (V, R), ak platí:

$$V' \subseteq V \wedge R' \subseteq \{(x, y), x \in V' \wedge y \in V' \wedge (xRy)\}$$

Funkcia $h : V \rightarrow \{1, 2, \ldots, n\}$ je zafarbenie grafu (V, R) n-farbami, ak platí:

$$(\forall x)(\forall y)(xRy \rightarrow h(x) \neq h(y))$$

Čísla $1, 2, \ldots, n$ reprezentujú n-farieb. Zafarbenie je pridelenie farieb vrcholom grafu tak, aby vrcholom, ktoré sú spojené hranou nebola nikdy priradená tá istá farba, teda ide o regulárne zafarbenie.

Uvažujme nasledujúce tvrdenie: Ak pre každý konečný podgraf grafu (V, R) existuje jeho regulárne zafarbenie n-farbami, potom aj pre celý graf (V, R) existuje jeho regulárne zafarbenie n-farbami.

Toto tvrdenie dokážeme prevedením na vetu o kompaktnosti. Nech graf $G = (V, R)$ je daný, môžeme zvoliť množinu T výrokových formúl a dokonca aj množinu P prvotných formúl. Zvoľme ju takto: $P = \{p_{x,i}, x \in V \wedge 1 \leq i \leq n\}$. Každá dvojica (x, i) je taká, že x je vrchol grafu a farba i má v množine P prvotnú formulu $p_{x,i}$, ktorá reprezentuje tvrdenie, že vrcholu x bola priradená farba i. Za množinu T zvoľme zjednotenie nasledujúcich troch množín výrokových formúl:

$$\begin{aligned} \{p_{x,1} \vee p_{x,2} \vee \ldots \vee p_{x,n}; x \in V\} &\leftrightarrow \text{každý vrchol má nejakú farbu} \\ \{p_{x,i} \rightarrow \neg p_{x,j}; i \neq j\} &\leftrightarrow \text{ale len jednu} \\ \{p_{x,i} \rightarrow \neg p_{y,i}; xRy\} &\leftrightarrow \text{susedné vrcholy majú rôzne farby} \end{aligned}$$

Nech v je ľubovoľné pravdivostné ohodnotenie, ktoré je modelom pre množinu formúl T. Z ohodnotenia v môžeme zostrojiť funkciu h takto: $h(x)$ definujeme ako to i, pre ktoré platí $v(p_{x,i}) = 1$. Je zrejmé, že číslo i je jednoznačne určené a že h je zafarbenie grafu (V, R). Zdôvodnili sme, že ak je T splniteľná, tak graf (V, R) je možné zafarbiť n-farbami.

Podobne môžeme zdôvodniť, že ak existuje pre ľubovoľný konečný podgraf grafu (V, R) regulárne zafarbenie n-farbami, potom každá konečná časť F množiny T je splniteľná. Naše tvrdenie teda vyplýva bezprostredne z vety o kompaktnosti.

Poznámka: Predpokladajme, že T je množina, ktorej prvky sú uzavreté podmnožiny intervalu $\langle 0, 1\rangle$ chápaného ako podmnožina množiny $\mathcal{R}$ všetkých reálnych čísel. Ak má každých konečne veľa prvkov množiny T neprázdny prienik, t.j. platí $\bigcap F \neq \emptyset$ pre každú

konečnú podmnožinu $F \subseteq T$, potom existuje aspoň jedno reálne číslo, ktoré je súčasne prvkom všetkých prvkov množiny T, t.j. platí $\bigcap T \neq \emptyset$.

Práve uvedené tvrdenie sa v topológii nazýva princíp kompaktnosti, reálny interval $\langle 0, 1\rangle$ z topologického hľadiska je kompaktnou množinou. Ak nahradíme v princípe kompaktnosti termíny podľa nasledujúcej tabuľky dostávame taktiež pravdivé tvrdenie, ktoré sa nazýva vetou o kompaktnosti vo výrokovej logike.

uzavretá podmnožina intervalu $\langle 0, 1\rangle$	$\rightarrow$	výroková formula
množina uzavretých množín	$\rightarrow$	množina výrokových formúl
prienik množiny je neprázdny	$\rightarrow$	množina je splniteľná

2.4 Formálny systém výrokovej logiky

Existujú dva hlavné prístupy k formálnemu systému logiky pomenované podľa dvoch významných matematikov. Prvý prístup — Gentzenovský — presadzuje menší počet axióm a väčší počet odvodzovacích pravidiel vo formálnom systéme. Naopak druhý prístup — Hilbertovský — presadzuje väčší počet axióm a menší počet odvodzovacích pravidiel. Na tejto prednáške sa budeme pridržiavať práve Hilbertovského prístupu.

Definícia:

1. *Hovoríme, že konečná postupnosť formúl $A_1, A_2, \ldots, A_n$ je dôkazom (odvodením) formuly A, ak A_n je formula A a pre ľubovoľné $i \leq n A_i$ je buď axióma alebo vyplýva z predchádzajúcich formúl $A_j, j < i$ podľa niektorého z odvodzovacích pravidiel.*

2. *Ak existuje dôkaz formuly A hovoríme, že A je dokázateľná a píšeme $\vdash A$. Hovoríme taktiež, že A je teoréma (veta) formálneho systému.*

Definícia: *Formálny systém výrokovej logiky pozostáva z nasledujúcich zložiek:*

1. *Jazyk tvoria množina P prvotných formúl, symboly pre logické spojky a pomocné symboly*

2. *Tri schémy axióm (Nech A, B, C sú ľubovoľné formuly výrokovej logiky):*

$$\begin{array}{ll} (A \rightarrow (B \rightarrow A)) & \textit{(A1)} \\ ((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))) & \textit{(A2)} \\ ((\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)) & \textit{(A3)} \end{array}$$

3. *Pravidlo odvodenia "modus ponens":*

$$\frac{A,\ A \rightarrow B}{B} \quad \textit{(MP)}$$

Slovom: z formúl A, $A \rightarrow B$ odvoď formulu B

Príklad: $\vdash A \rightarrow A$

Dôkaz:

1. krok	$\vdash A \rightarrow ((A \rightarrow A) \rightarrow A)$	(A1)
2. krok	$\vdash A \rightarrow ((A \rightarrow A) \rightarrow A) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$	(A2)
3. krok	$\vdash (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$	(1, 2, MP)
4. krok	$\vdash (A \rightarrow (A \rightarrow A))$	(A1)
5. krok	$\vdash A \rightarrow A$	(3, 4, MP)

Definícia: *Nech T je množina formúl výrokovej logiky a $A, A_1, \ldots, A_n$ sú formuly výrokovej logiky. Hovoríme, že postupnosť formúl $A_1, \ldots, A_n$ je dôkazom (odvodením) formuly A z predpokladov T, ak A_n je formula A a pre ľubovoľné $i \leq n$ je A_i buď axióma výrokovej logiky alebo formula z množiny T alebo A_i je odvodená z formúl $A_1, A_2, \ldots, A_{i-1}$ pomocou niektorého pravidla odvodenia. Hovoríme, že formula A je odvoditeľná z predpokladov T, ak existuje dôkaz (odvodenie) A z predpokladov T a označujeme $T \vdash A$.*

2.5 Veta o dedukcii

Veta: *Nech T je množina formúl výrokovej logiky; A, B sú formuly. Potom*

$$T \vdash A \to B \leftrightarrow T, A \vdash B$$

Dôkaz:

Predpokladajme, že platí $T \vdash A \to B$. Teda existuje $A_1, A_2, \ldots, A_n(A \to B)$, čo je dôkaz formuly $A \to B$. Rozšírme T o formulu A ($T \cup \{A\} \equiv T, A$). Použijeme pravidlo modus ponens a dostávame $T, A \vdash B$.

Predpokladajme, že platí $T, A \vdash B$, chceme dokázať $T \vdash A \to B$. Použijeme matematickú indukciu vzhľadom na dĺžku odvodenia formuly B z predpokladov T, A.

- báza indukcie: n = 1
  rozlíšime 3 prípady:
  1. formula B je totožná s formulou A
     Platí $\vdash A \to A$ teda bude platiť aj $T \vdash A \to A$
  2. formula B je axióma
     Platí $\vdash B \to (A \to B)$ aj $\vdash B$. Pomocou pravidla modus ponens odvodíme $\vdash A \to B$. A teda aj $T \vdash A \to B$.
  3. formula B je niektorá z formúl z množiny T
     Platí $\vdash B \to (A \to B)$ aj $T \vdash B$. Pomocou pravidla modus ponens odvodíme $T \vdash A \to B$.
- indukčný krok:
  Prepokladajme, že tvrdenie vety platí pre každé $s < n$. Máme dokázať, že tvrdenie platí aj pre n. Vieme, že $T, A \vdash B$, teda existuje postupnosť $A_1, A_2, \ldots, A_n(B)$ – dôkaz formuly B. Rozoberme možnosti ako sa do tejto postupnosti mohla dostať posledná formula $A_n \equiv B$:
  1. formula B je totožná s formulou A (už sme dokazovali)
  2. formula B je axióma (už sme dokazovali)
  3. formula B je niektorá z formúl z množiny T (už sme dokazovali)
  4. formula B vznikla použitím pravidla modus ponens na niektoré dve formuly $A_i, A_j \equiv A_i \to B$ $(i, j < n)$
     Z indukčného predpokladu dostávame $T \vdash A \to A_j$ a $T \vdash A \to A_i$. Použitím schémy (A2) dostaneme $\vdash (A \to (A_i \to B)) \to (A \to A_i) \to (A \to B)$. Dvojnásobným použitím pravidla modus ponens nakoniec dostávame $T \vdash A \to B$. ♣

2.6 Postove vety

Lema 1:

1. $\vdash \neg A \to (A \to B)$
2. $\vdash \neg\neg A \to A$
3. $\vdash A \to \neg\neg A$
4. $\vdash (A \to B) \to (\neg B \to \neg A)$
5. $\vdash A \to (\neg B \to \neg(A \to B))$
6. $\vdash (\neg A \to A) \to A$

Dôkaz: Prvé tvrdenie:

1. krok	$\vdash \neg A \to (\neg B \to \neg A)$	(A1)
2. krok	$\neg A \vdash (\neg B \to \neg A)$	(VD)
3. krok	$\vdash (\neg B \to \neg A) \to (A \to B)$	(A3)
4. krok	$\neg A \vdash (A \to B)$	(2, 3, MP)
5. krok	$\vdash \neg A \to (A \to B)$	(VD)

Aby som neporušil peknú tradíciu matfyzáckych skrípt prenechávam zvyšné dôkazy na usilovného čiateteľa.

Lema 2: (o neutrálnej formule) *Nech T je množina formúl výrokovej logiky; A, B sú formuly; nech $T, A \vdash B$ a $T, \neg A \vdash B$. Potom $T \vdash B$.*

Dôkaz:

1. krok	$T, \neg A \vdash B$	(predpoklad)
2. krok	$T \vdash \neg A \to B$	(VD)
3. krok	$T \vdash \neg B \to \neg\neg A$	(Lema 1(4.), MP)
4. krok	$T, \neg B \vdash \neg\neg A$	(VD)
5. krok	$T, \neg B \vdash A$	(Lema 1(2.), MP)
6. krok	$T, A \vdash B$	(predpoklad)
7. krok	$T \vdash A \to B$	(VD)
8. krok	$T, \neg B \vdash B$	(5, 7, MP)
9. krok	$T \vdash \neg B \to B$	(VD)
10. krok	$\vdash (\neg B \to B) \to B$	(Lema 1(6.))
11. krok	$T \vdash B$	(9, 10, MP)

Definícia: *Nech B je formula výrokovej logiky, nech v je ohodnotenie prvotných formúl. B^v označuje formulu B, ak $\overline{v}(B) = 1$ resp. formulu $\neg B$, ak $\overline{v}(B) = 0$.*

Lema 3: *Nech v je valuácia prvotných formúl. Nech $p_1, p_2, \ldots, p_n$ sú všetky prvotné formuly, ktoré sa vyskytujú vo formule A. Potom*

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

Dôkaz: matematickou indukciou vzhľadom na konštrukciu formuly A

1. báza indukcie: A je prvotná formula, teda $p^v \vdash p^v$
2. indukčný krok:

- formula A je tvaru $\neg B$ a $\overline{v}(B) = 0$:
  Teda $B^v = \neg B = A$, ďalej platí $A^v = (\neg B)^v$ a zároveň $\overline{v}(\neg B) = 1$, teda $A^v = A$. Z indukčného predpokladu $p_1^v, p_2^v, \ldots, p_n^v \vdash B^v$ môžme teda odvodiť $p_1^v, p_2^v, \ldots, p_n^v \vdash A^v$
- formula A je tvaru $\neg B$ a $\overline{v}(B) = 1$:
  Teda $B^v = B$, ďalej platí $A^v = (\neg B)^v$ a zároveň $\overline{v}(\neg B) = 0$, teda $A^v = \neg\neg B$. Z indukčného predpokladu $p_1^v, p_2^v, \ldots, p_n^v \vdash B^v$ s pomocou teorémy $\vdash B \to \neg\neg B$ môžme teda odvodiť $p_1^v, p_2^v, \ldots, p_n^v \vdash A^v$
- formula A je tvaru $C \to D$ a $\overline{v}(C) = \overline{v}(D) = 1$:
  Teda $C^v = C$, $D^v = D$, $A^v = C \to D$. Z indukčného predpokladu $p_1^v, p_2^v, \ldots, p_n^v \vdash D^v$ s pomocou teorémy $\vdash D \to (C \to D)$ môžme teda odvodiť $p_1^v, p_2^v, \ldots, p_n^v \vdash A^v$
- formula A je tvaru $C \to D$ a $\overline{v}(C) = 1 \wedge \overline{v}(D) = 0$:
  Teda $C^v = C$, $D^v = \neg D$, $A^v = \neg(C \to D)$. Z indukčného predpokladov $p_1^v, p_2^v, \ldots, p_n^v \vdash C^v$ a $p_1^v, p_2^v, \ldots, p_n^v \vdash D^v$ s pomocou teorémy $\vdash C \to (\neg D \to \neg(C \to D))$ môžme teda odvodiť $p_1^v, p_2^v, \ldots, p_n^v \vdash A^v$
- formula A je tvaru $C \to D$ a $\overline{v}(C) = 0$:
  Teda $C^v = \neg C$, $A^v = C \to D$. Opäť z indukčného predpokladu $p_1^v, p_2^v, \ldots, p_n^v \vdash C^v$ s pomocou teorémy $\vdash \neg C \to (C \to D)$ môžme teda odvodiť $p_1^v, p_2^v, \ldots, p_n^v \vdash A^v$

Veta: (slabá forma vety o úplnosti)

$$\vdash A \Leftrightarrow \models A$$

(: Pre výrokovú formulu A výrokovej logiky platí, že je dokázateľná práve vtedy, keď je tautológia :)

Dôkaz:

Implikáciu zľava doprava dokážeme tak, že ukážeme, že axiómy (A1), (A2) a (A3) sú tautológie (napr. tabuľkovou metódou alebo sporom) a ďalej že pravidlo modus ponens je korektné (t.j. aplikovaním na tautológie dostaneme opäť tautológiu).

Implikáciu sprava doľava dokážeme nasledovne:
Z lemy 3 vieme,že

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

Keďže A je tautológia, tak $A^v = A$, čiže

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

Uvažujme dve ohodnotenia v_1 a v_2 také, že

$$v_1(p_n) = 1, v_2(p_n) = 0 \; a \; v_1(p_i) = v_2(p_i) \; pre \; i < n$$

Dostávame

$$p_1^w, p_2^w, \ldots, p_{n-1}^w, p_n \vdash A \; a \; p_1^w, p_2^w, \ldots, p_{n-1}^w, \neg p_n \vdash A$$

Z toho na základe lemy 2 vieme, že

$$p_1^w, p_2^w, \ldots, p_{n-1}^w \vdash A$$

Viacnásobným aplikovaním tohto postupu sa dostaneme až k tvrdeniu $\vdash A$. ♣

Definícia: *Hovoríme, že formálny systém je sporný, ak každá jeho formula je dokázateľná. V opačnom prípade je formálny systém bezosporný.*

Definícia: *Ak T je množina formúl (nejakého formálneho systému) hovoríme, že T je sporná, ak každá formula je dokázateľná z predpokladov T. Inak hovoríme, že množina formúl T je bezosporná.*

Poznámka: Formálny systém je bezosporný, ak je bezosporná prázdna množina predpokladov.

Definícia: *Bezosporné formálne systémy nazývame konzistentné (sporné naopak inkonzistentné).*

Poznámka: Sémantický ekvivalent bezospornej množiny formúl T je jej splniteľnosť.

Dôsledok: *Množina formúl výrokovej logiky je bezosporná práve vtedy, keď je splniteľná.*

Dôkaz: Predpokladajme, že množina formúl T je splniteľná – ukážeme, že je bezosporná. Nech v je ohodnotenie prvotných formúl, ktoré je modelom T ($\forall A \in T\ \overline{v}(A) = 1$). Korektnosť pravidla modus ponens nám zaručuje, že neodvodíme žiadnu formulu B takú, že $\overline{v}(B) = 0$.

Obrátene: predpokladajme, že T je bezosporná – ukážeme, že má model (je splniteľná). Budeme postupovať sporom. Nech teda T nie je splniteľná. Potom podľa dôsledku vety o kompaknosti určite existuje konečná podmnožina $\{A_1, A_2, \ldots, A_n\} \subseteq T$, ktorá nie je splniteľná. Pre každé ohodnotenie v sa nájde formula A_i, že platí $\overline{v}(A_i) = 0$, čiže formula $X \equiv \neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n$ je tautológia. Ďalej platí $T \vdash A_i$ pre $i = \overline{1, n}$. Použitím vety $T \vdash A \wedge T \vdash B \Rightarrow T \vdash A \wedge B$ (ktorú neskôr dokážeme!) dostávame $T \vdash A_1 \wedge A_2 \wedge \ldots \wedge A_n$, teda $T \vdash \neg X$. Čiže je dokázateľná formula X aj jej negácia. Použitím tautológie $\vdash \neg B \to (B \to C)$, pričom za B dosadíme X dostávame $T \vdash C$, kde C je ľubovoľná formula. A to je spor s bezospornosťou. ♣

Veta: (silná forma vety o úplnosti) *Pre ľubovoľnú množinu formúl T a formulu A platí:*

$$T \vdash A \Leftrightarrow\ T \models A$$

Dôkaz: Implikáciu zľava doprava dokážeme rovnako ako pri slabej forme vety.
Obrátene nech $T \models A$, podľa dôsleku vety o kompaktnosti platí, že existuje konečná podmnožina $T_0 = \{A_1, A_2, \ldots, A_n\} \subseteq T$, že platí $T_0 \models A$.

$$T_0 \models A \iff \models A_1 \to (A_2 \to (A_3 \to \ldots (A_n \to A)\ldots)$$

$$\Updownarrow \text{ pomocou slabej formy vety o úplnosti}$$

$$\vdash A_1 \to (A_2 \to (A_3 \to \ldots (A_n \to A)\ldots)$$

$$\Updownarrow \text{ pomocou vety o dedukcii}$$

$$T_0 \vdash A \iff A_1, A_2, \ldots, A_n \vdash A$$

Z $T_0 \vdash A$ už triviálne vyplýva aj $T \vdash A$. ♣

2.7 Ďalšie vety

Lema 4:

1. $A \wedge B \vdash A$
2. $A \wedge B \vdash B$
3. $A, B \vdash A \wedge B$

Dôkaz: Prvé tvrdenie:

1. krok	$\vdash \neg A \to (A \to \neg B)$	(Lema 1(1.))
2. krok	$\vdash \neg A \to (A \to \neg B) \to \neg(A \to \neg B) \to \neg\neg A$	(Lema 1(4.))
3. krok	$\neg(A \to \neg B) \to \neg\neg A$	(1, 2, MP)
4. krok	$\neg\neg A \to A$	(Lema 1(2.))
5. krok	$\neg(A \to \neg B) \to A$	(3, 4, jednoduchý sylogizmus)
6. krok	$\neg(A \to \neg B) \vdash A$	(VD)
7. krok	$A \wedge B \vdash A$	$(A \wedge B \Leftrightarrow \neg(A \to \neg B))$

Dôkaz ďalších tvrdení už prenechávam usilovnému čitateľovi.

Poznámka: Pravidlo jednoduchého sylogizmu:

$$\frac{A, A \to B, B \to C}{C}$$

Poznámka: $A \leftrightarrow B$ je skrátený zápis pre $(A \to B) \wedge (B \to A)$.

Dôsledok:

1. $A \leftrightarrow B \vdash A \to B$
2. $A \leftrightarrow B \vdash B \to A$
3. $A \to B \wedge B \to A \vdash A \leftrightarrow B$
4. ak $\vdash A \leftrightarrow B$, potom $T \vdash A$ práve vtedy, keď $T \vdash B$

Dôsledok:

1. $\vdash (A \wedge B) \leftrightarrow (B \wedge A)$
2. $\vdash (A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C)$
3. $\vdash (A_1 \to (A_2 \to \ldots (A_n \to B)\ldots) \leftrightarrow (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \to B$

Veta: *Nech formula A' vznikne z formuly A nahradením niektorých podformúl $A_1, A_2, \ldots, A_n$ formulami $A'_1, A'_2, \ldots, A'_n$. Keď platí $\vdash A_i \leftrightarrow A'_i$ $i = \overline{1,n}$, potom $\vdash A \leftrightarrow A'$.*

Dôkaz: matematickou indukciou vzhľadom na konštrukciu formuly A

1. báza indukcie triviálne platí
2. indukčný krok:
   - nech $A \equiv \neg B$

1. krok	$\vdash B \leftrightarrow B'$	(indukčný predpoklad)
2. krok	$\vdash (B \to B') \to (\neg B' \to \neg B)$	(Lema 1(4.))
	$\vdash (B' \to B) \to (\neg B \to \neg B')$	(Lema 1(4.))
3. krok	$\vdash \neg B' \to \neg B$	(1, 2, MP)
	$\vdash \neg B \to \neg B'$	(1, 2, MP)
4. krok	$\vdash \neg B' \leftrightarrow \neg B$	(3)
5. krok	$\vdash A \leftrightarrow A'$	$(A \equiv \neg B)$

   - nech $A \equiv (B \to C)$

1. krok	$\vdash B \leftrightarrow B'$	(IP)
	$\vdash C \leftrightarrow C'$	(IP)
2. krok	$B', B' \to B, B \to C, C \to C' \vdash C'$	(sylogizmus)
3. krok	$B' \to B, B \to C, C \to C' \vdash B' \to C'$	(VD)
4. krok	$B' \to B, C \to C' \vdash (B \to C) \to (B' \to C')$	(VD)
5. krok	$\vdash (B \to C) \to (B' \to C')$	(1, 4, MP)
6. krok	symetricky dokážeme opačnú implikáciu	(—)
7. krok	$\vdash A \leftrightarrow A'$	(5, 6)

Lema 5: (De Morganove pravidlá)

1. $\vdash \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
2. $\vdash \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$

Dôkaz:

$$
\begin{array}{ll}
\vdash \neg(A \wedge B) & \leftrightarrow \neg\neg(A \to \neg B) \\
 & \leftrightarrow (\neg\neg A \to \neg B) \\
 & \leftrightarrow (\neg A \vee \neg B) \\
\vdash \neg(A \vee B) & \leftrightarrow (\neg A \wedge \neg B) \\
 & \leftrightarrow \neg(\neg A \to B) \\
 & \leftrightarrow \neg(\neg A \to \neg\neg B) \\
 & \leftrightarrow \neg A \wedge \neg B
\end{array}
$$

Dôsledok:

1. $\vdash A \to (A \vee B)$
   $\vdash B \to (A \vee B)$
2. $\vdash (A \vee B) \leftrightarrow (B \vee A)$
3. $\vdash (A \vee B) \vee C \leftrightarrow A \vee (B \vee C)$

Dôkaz: Prenechávam na čitateľa.

Veta: (o dôkaze rozborom prípadov) *Nech T je množina formúl výrokovej logiky a A, B, C sú formuly výrokovej logiky. Potom platí*

$$T, (A \vee B) \vdash C \;\Leftrightarrow\; T, A \vdash C \;\wedge\; T, B \vdash C$$

Dôkaz: Pri dôkaze implikácie zľava doprava stačí využiť predošlú vetu (resp. dôsledok). Obrátená implikácia:

1. krok	$T, A \vdash C \;\Rightarrow\; T \vdash A \to C$	(IP, VD)
	$T, B \vdash C \;\Rightarrow\; T \vdash B \to C$	(IP, VD)
2. krok	$T \vdash \neg C \to \neg A \;\Rightarrow\; T, \neg C \vdash \neg A$	(1, Lema 1(4.), VD)
	$T \vdash \neg C \to \neg B \;\Rightarrow\; T, \neg C \vdash \neg B$	(1, Lema 1(4.), VD)
3. krok	$T, \neg C \vdash \neg A \wedge \neg B$	(Lema 4(3.))
4. krok	$T \vdash \neg C \to (\neg A \wedge \neg B)$	(VD)
5. krok	$T \vdash \neg(\neg A \wedge \neg B) \to \neg\neg C$	(Lema 1(4.))
6. krok	$T \vdash \neg\neg A \vee \neg\neg B \to \neg\neg C$	(Lema 5(1.))
7. krok	$T \vdash A \vee B \to C$	(Lema 1(2.))
8. krok	$T, A \vee B \vdash C$	(VD)

Dôsledok: (distributivita konjunkcií a disjunkcií)

1. $\vdash (A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$
2. $\vdash (A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$

Dôkaz: Prenechávam na čitateľa (je trošku dlhší, ale aspoň získate prax).

2.8 Konjunktívny a disjunktívny normálny tvar

Definícia: *Prvotné formuly a ich negácie nazývame literály.*

Veta: *Každá formula A výrokovej logiky je ekvivalentná istej formule tvaru*

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n,$$

kde každá z formúl A_i $1 \leq i \leq n$ je disjunkciou literálov. Tento tvar nazývame konjunktívny normálny tvar.
Formula A je takiež ekvivalentná istej formule tvaru

$$B_1 \vee B_2 \vee \ldots \vee B_n,$$

kde každá z formúl B_i $1 \leq i \leq n$ je konjunkciou literálov. Tento tvar nazývame disjunktívny normálny tvar.

Dôkaz: matematickou indukciou vzhľadom na zložitosť formuly A

1. báza indukcie: ak A je prvotná formula, tak je automaticky v konjunktívnom aj disjunktívnom normálnom tvare
2. indukčný krok:

- nech $A \equiv \neg B$
  Podľa IP existujú pre B formuly B_k (*resp.* B_d) v KNF (resp. DNF). Keď tieto formuly znegujeme dostaneme formuly ekvivalentné s A v DNF (resp. KNF).
- nech $A \equiv (B \to C)$
  Platí $\vdash (B \to C) \leftrightarrow (\neg B \vee C)$. Ďalej podľa IP vieme, že $\vdash B \leftrightarrow B_d$ a $\vdash C \leftrightarrow C_k$. Dosadením $B := B_d,\ C := C_k$ do formuly $\neg B \vee C$ sa B_d po znegovaní zmení na B'_k a využitím distributivity konjunkcií a disjunkcií môžme formulu upraviť na KNF.
  Ak použijeme zvyšné dve tvrdenia IP a dosadíme $B := B_k,\ C := C_d$ po znegovaní dostaneme priamo formulu $B'_d \vee C_d$ v DNF. ♣

Veta: *Nech $A, A_1, A_2, \ldots A_n$ sú formuly a $p_1, p_2, \ldots, p_n$ sú navzájom rôzne prvotné formuly, ktoré sa vyskytujú v A. Nech formula A' vznikne z formuly A nahradením každého výskytu p_i formulou A_i $i = \overline{1,n}$. Potom $\vdash A \Rightarrow \vdash A'$.*

Dôkaz: Ak je A dokázateľná formula, tak z Postovej vety vyplýva, že je tautológia. A teda pre ľubovoľné ohodnotenie v prvotných formúl je $\overline{v}(A) = 1$. Ak budeme namiesto $v(p_i)$ vo formule A uvažovať $\overline{v}(A_i)$ vo formule A' nemôže sa nijako zmeniť pravdivostná hodnota, pretože štruktúra formuly zostala rovnaká a na ohodnotení prvkov tejto štruktúry nezáleží. Teda A' je tautológia a opätovným použitím Postovej vety dostávame, že A' je dokázateľná. ♣

3 Predikátová logika

3.1 Syntax predikátovej logiky

Vo výrokovej logike sme detailne skúmali vlastnosti logických spojok, teraz budeme pracovať s jazykom logiky prvého rádu, ktorý okrem spojok obsahuje ešte premenné, funkčné symboly a predikátové symboly.

Definícia: *Jazyk 1. rádu obsahuje:*

1. *neohraničene veľa symbolov pre premenné* $x_1, x_2, \ldots, y_1, y_2, \ldots$
2. *symboly pre logické spojky* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
3. *symboly pre kvantifikátory* $\forall, \exists$
4. *predikátové symboly* $P, Q, R, \ldots$ *ku každému symbolu je priradené prirodzené číslo väčšie alebo rovné* 1*, ktoré vyjadruje jeho -árnosť*
5. *funkčné symboly* $f, g, h, \ldots$ *ku každému symbolu je priradené prirodzené číslo väčšie alebo rovné* 0*, ktoré vyjadruje jeho -árnosť*
6. *pomocné symboly – zátvorky, čiarku, ...*
7. *Špeciálny predikát "=" - binárny predikát pre rovnosť*

Poznámka: Symboly pre premenné, spojky a kvantifikátory nazývame logické, ak ide o jazyk s rovnosťou, symbol predikátu rovnosti počítame taktiež k logickým symbolom. Symboly pre ostatné predikáty a symboly pre funkcie určujú špecifiká jazyka a odrážajú oblasť, ktorú jazyk môže popisovať, preto ich nazývame špeciálne. Jazyk prvého rádu je daný výpočtom špeciálnych symbolov.

Výrazy jazyka prvého rádu, ktoré majú matematický zmysel môžeme rozdeliť do dvoch hlavných skupín: termy a formuly.

Príklad: (jazykov 1. rádu)

1. Jazyk teórie ostrého usporiadania: je jazyk s rovnosťou (kvôli trichotómii), ktorý obsahuje jediný špeciálny symbol $''<''$ – binárny predikátový symbol
2. Jazyk teórie grúp: jazyk 1. rádu s rovnosťou, ktorý obsahuje dva špeciálne symboly: $''1''$ – nulárny funkčný symbol pre jednotkový prvok a $''+''$ – binárny funkčný symbol pre grupovú operáciu
3. Jazyk teórie telies: jazyk 1. rádu s rovnosťou, ktorý obsahuje dva binárne funkčné symboly: $''+''$ a $''\cdot''$ (sčítanie a násobenie) a dva nulárne funkčné symboly pre nulový a jednotkový prvok: $''0''$ a $''1''$
4. Jazyk teórie množín: jazyk 1. rádu s rovnosťou, ktorý obsahuje jediný špeciálny symbol $''\in''$ – binárny predikátový symbol označujúci patričnosť
5. Jazyk elementárnej aritmetiky: jazyk 1. rádu s rovnosťou, obsahujúci $''0''$ – nulárny funkčný symbol, S – unárny funkčný symbol pre nasledovníka, $''+''$ a $''\cdot''$ – binárne funkčné symboly pre sčítanie a násobenie

Definícia: (Term)

1. *Každá premenná a konštanta (nulárny funkčný symbol) je term.*
2. *Ak výrazy $t_1, t_2, \ldots, t_n$ sú termy a f je n-árny funkčný symbol, potom $f(t_1, t_2, \ldots, t_n)$ je term.*
3. *Každý term vznikne konečným počtom použití pravidiel (1) a (2).*

Príklad: V jazyku elementárnej aritmetiky sú nasledujúce výrazy termy: $0, S(x), S(S(0))$. U zaužívaných binárnych symbolov $+, \cdot$ (prípadne iných) píšeme $(x+y)$ namiesto $+(x, y)$ a $(x \cdot y)$ namiesto $\cdot(x, y)$. Preto taktiež $((x + y) \cdot 0)$, $((S(0) + (x \cdot y)) \cdot S(0))$ sú termy. Ak je f n-árny funkčný symbol, $f((x \cdot y), y_1, \ldots, y_{n-1})$ je taktiež term.

Z definície termu vidíme, že ide o výrazy, ktoré pomocou funkčných symbolov popisujú skladanie operácií. Termy jazyka elementárnej aritmetiky môžeme chápať ako symbolický zápis výsledkov naznačených operácií. Iný charakter majú formuly.

Definícia: (Formula)

1. *Nech P je n-árny predikátový symbol a nech $t_1, t_2, \ldots, t_n$ sú termy. Potom výraz $P(t_1, t_2, \ldots, t_n)$ je atomická formula.*
2. *Nech A, B sú formuly, potom $\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B$ sú formuly.*
3. *Ak x je premenná, A je formula, potom $(\forall x)\, A$, $(\exists x)\, A$ sú formuly*
4. *Každá formula vznikne konečným počtom použití pravidiel (1), (2) a (3).*

Definícia: (Podformula) *Nech A je formula. Jej podformulou sa nazýva:*

1. *len ona sama, ak A je atomická formula*
2. *ona sama a každá podformula formuly B, ak $A = (\neg B)$ alebo $A = (\forall x)B$, $A = (\exists x)B$*
3. *ona sama a každá podformula formúl B a C, ak $A = (B \wedge C)$, $A = (B \vee C)$, $A = (B \rightarrow C)$ alebo $A = (B \leftrightarrow C)$*
4. *žiadne iné podformuly okrem týchto nepoznáme*

Poznámka: Podobne ako v prípade binárnych funkčných symbolov $+, \cdot$, atď. budeme písať $(x = y), (x < y)$ namiesto $= (x, y), < (x, y)$. V tomto prípade píšeme $x \neq y$ namiesto $\neg(x = y)$.

Príklad:

$$\begin{array}{ll} S(0) = (0.x) + S(0) & (1) \\ (\exists x)(y = x.z) & (2) \\ (\forall x)(x \neq 0 \rightarrow (\exists y)(x = S(y))) & (3) \end{array}$$

sú formuly jazyka aritmetiky. Formula (1) je atomická, formuly (2) a (3) nie sú atomické. Formula (3) vznikla z atomických formúl $(x = 0), (x = S(x))$ použitím zodpovedajúcich pravidiel:

$$\begin{array}{ll} \neg(x = 0) & (2) \\ (\exists y)(x = S(y)) & (3) \\ (\neg(x = 0) \rightarrow (\exists y)(x = S(y))) & (2) \\ (\forall x)(x \neq 0 \rightarrow (\exists y)(x = S(y))) & (3) \end{array}$$

Práve sme sa presvedčili, že formula $(\forall x)(x \neq 0 \rightarrow (\exists y)(x = S(y)))$ vznikla predpísaným spôsobom. Formuly, ktoré sme v priebehu konštrukcie zostrojili (vrátane nej samej) sa nazývajú jej podformuly.

Z predchádzajúcich definícií je zrejmé, že termy a formuly sú isté konečné postupnosti symbolov daného jazyka zostavené podľa pevných syntaktických pravidiel. Ľubovoľnú konečnú postupnosť symbolov budeme v krátkosti nazývať slovo alebo výraz. Ak je nejaký symbol s napísaný na i-tom mieste v slove S, hovoríme, že s sa vyskytuje v slove S na i-tom mieste. V takom prípade i-ty symbol v slove S nazývame výskyt symbolu s v slove S. Napríklad symbol (sa v vyskytuje vo formule (1) vo vyššie uvedenom príklade na druhom, šiestom a trinástom mieste, symbol x sa vyskytuje v tej istej formule na desiatom mieste (počítame zľava doprava).

Spojovanie slov, ktorému sa taktiež hovorí zreťazenie (konkatenácia) je najjednoduchšia operácia, ktorú je možné so slovami prevádzať. Poslúži nám k presnejšiemu popisu ďalších syntaktických pojmov, ktoré budeme zavádzať.

Ak sú A, B slová, potom výrazom AB označíme slovo, ktoré vznikne zo slov A, B tak, že najprv napíšeme slovo A a za posledný symbol slova A (bez medzery) pripojíme slovo B.

Napríklad slovo 112 vznikne spojením slov 1, 12 alebo taktiež zo slov 11, 2. Slovo, ktoré vznikne spojením slov $A_1, A_2, \ldots, A_n$ v uvedenom poradí budeme označovať $A_1 A_2 \ldots A_n$.

Hovoríme, že slovo C je podslovom slova A, ak slovo A má tvar BCD pre nejaké slová B, D.

Príklad: Nech t je term $f(x, g(x, y))$. Potom slová $g(x, y)$ a $g(x, y))$ sú podslová slova t. Prvé z nich je taktiež termom, druhé termom nie je.

Podobne slovo $(\forall x)$ je podslovom formuly $(\forall x)(x \neq 0 \rightarrow (\exists y)(x = S(y)))$, ale samé nie je formulou.

Definícia: Nech t je term a A je formula.

1. *Hovoríme, že term s je podtermom termu t, ak s je podslovom slova t.*

2. *Hovoríme, že formula B je podformulou formuly A, ak B je podslovom slova A.*

3. *Hovoríme, že daný výskyt premennej x vo formule A je viazaný, ak je súčasťou nejakej jej podformuly tvaru $(\forall x)B$ alebo $(\exists x)B$. Ak nie je daný výskyt premennej x viazaný, hovoríme, že je voľný.*

4. *Hovoríme, že premenná x je voľná vo formule A, ak tam má voľný výskyt. Hovoríme, že premenná x je viazaná vo formule A, ak tam má viazaný výskyt. (Toto je trošku voľný spôsob definície, pripúšta totiž obidva interpretácie – riešenie spočíva v tom, že viazané premenné možno premenovať.)*

5. *Hovoríme, že formula A je otvorená, ak neobsahuje žiadnu viazanú premennú. Hovoríme, že formula A je uzavretá, ak neobsahuje žiadnu voľnú premennú. V oboch prípadoch A nazývame formulou s čistými premennými.*

Poznámka 1: Je zrejmé, že otvorená formula vznikne zo svojich atomických podformúl len pomocou logických spojok, neobsahuje teda žiadne kvantifikátory. Uzavretá formula naopak viaže každú premennú niektorým kvantifikátorom.

Poznámka 2: Je treba si uvedomiť, že jedna a tá istá premenná môže byť v danej formule súčasne voľná i viazaná, napríklad $(x = z) \rightarrow (\exists x)(x = z)$, kde premenná x má voľný i viazaný výskyt. Táto situácia je umožnená voľnosťou v definícii formuly, v matematickej praxi sa také formuly väčšinou neuvádzajú. Ako uvidíme neskôr, viazané premenné je možné zameniť a tak sa podobnej situácii môžeme vždy vyhnúť. V takomto prípade ako sme uviedli v definícii, formuly u ktorých každá premenná je buď voľná (a nie je viazaná) alebo len viazaná (a nie voľná) sa niekedy nazývajú formuly s čistými premennými.

3.2 Sémantika predikátovej logiky

Teraz už máme k dispozícii základné fakty a pojmy o syntaxi predikátovej logiky, zaviedli sme pojem termu, formuly a viazanosti, ktorú môže mať premenná vo formule. Môžeme skúmať otázku štruktúr, ktoré realizujú symboly jazyka predikátovej logiky a najmä to, ktoré formuly sú pravdivé v danej realizácii. Ak chceme dať symbolom jazyka nejakú matematickú interpretáciu, je treba začať najprv od premenných, musíme vymedziť obor, ktorý bude určovať možné "hodnoty" premenných. Taký obor bude neprázdna množina $M \neq \emptyset$, jej prvky budeme nazývať indivíduá. Ak je vymedzené minimum indivíduí, potom je prirodzené sa pýtať ako sú realizované operácie, ktoré sú naznačené v jazyku L funkčnými symbolmi. Napríklad sa môžeme pýtať, ktoré indivíduum bude odpovedať súčtu alebo inej operácii z daných indivíduí univerza. Funkčný symbol f (n-árny) z jazyka L bude realizovaný zobrazením $f_M : M^n \rightarrow M$ tak, že rovnosť $f_M(i_1, i_2, \ldots, i_n) = j$ pre $i_1, i_2, \ldots, i_n, j \in M$ znamená, že indivíduum j bude výsledkom operácie f prevedenej na indivíduách $i_1, i_2, \ldots, i_n$. Nakoniec zostávajú predikátové symboly. Ak máme napríklad realizovať binárny predikátový symbol $<$, ktorý "porovnáva" indivíduá, použijeme binárnu reláciu $<_M \subseteq M^2$. Podobne n-árne relácie $P_M \subseteq M^n$ budú realizácie n-árnych predikátových symbolov P. Pretože na tej istej množine M je možné predikát P resp. funkciu f realizovať viacerými rôznymi reláciami resp. operáciami je teda správnejšie písať $P_{\mathcal{M}}$ a $f_{\mathcal{M}}$ namiesto P_M a f_M, kde $\mathcal{M}$ bude označovať realizáciu. Zvláštnu pozíciu tu má symbol $=$, ktorý počítame k symbolom logickým a ktorý by mal byť realizovaný tak, aby odpovedal našim predstavám o rovnosti. Preto ho nerealizujeme inak, než ako identitu indivíduí. V definícii pravdivosti sa to odráža zvláštnou klauzulou, ktorá definuje splňovanie atomických formúl s rovnosťou. Ostatné logické symboly ako spojky a kvantifikátory nemá zmysel realizovať. Popísaný súbor, ktorý obsahuje univerzum M, funkcie a relácie na tomto univerze sa nazýva relačná štruktúra.

Definícia: *Nech L je jazyk 1. rádu. Relačná štruktúra $\mathcal{M}$, ktorá obsahuje:*

1. *neprázdnu množinu M (univerzum), ktorej prvky sa nazývajú indivíduá*
2. *zobrazenia $f_M : M^n \rightarrow M$ pre každý n-árny funkčný symbol f jazyka L*
3. *n-árnu reláciu $P_M \subseteq M^n$ pre každý n-árny predikátový symbol $p \in L$ okrem symbolu pre rovnosť.*

sa nazýva realizácia jazyka L.

Poznámka: Predikát rovnosti chápeme ako rovnosť indivíduí.

Príklad:

1. Štruktúra $< N, N \times N >$, kde N je množina prirodzených čísel je realizácia jazyka teórie usporiadania.

2. Štruktúra $< \{e\}, e, \cdot e >$, kde $\cdot e$ je binárne zobrazenie $\{e\}^2 \to \{e\}$ definované jediným možným spôsobom je realizácia jazyka teórie grúp.

3. $\mathcal{N}=< N^+, 0, S, \oplus, \odot >$, kde $N^+ = \{1, 2, \ldots, n, \ldots\}$, S je funkcia, ktorá číslu n priradí nasledujúce prirozené číslo a $\oplus, \odot$ sú obvyklé operácie súčtu a súčinu; je realizáciou jazyka elementárnej aritmetiky. Ak S nahradíme nejakým číslom, napríklad jednotkou, vznikne štruktúra, ktorá je realizáciou jazyka teórie telies (to však neznamená, že je telesom).

Definícia: *Zobrazenie e, ktoré každej premennej x priradí nejaké indivíduum z univerza $\mathcal{M}$ nazývame ohodnotenie premenných. Ak t je term, potom zápis $t[e]$ označuje realizáciu termu t pri ohodnotení e v relačnej štruktúre $\mathcal{M}$.*

Lema: *Nech $x_1, x_2, \ldots x_n$ sú všetky premenné, ktoré sa vyskytujú v terme t. Ak e a e' sú dve ohodnotenia premenných také, že platí $e(x_i) = e'(x_i)$ pre $i = \overline{1,n}$, potom $t[e] = t[e']$.*

Dôkaz: matematickou indukciou vzhľadom na t

1. $t \equiv x$
   $e(x) = e'(x) \;\Rightarrow\; t[e] = t'[e]$

2. $t \equiv f(t_1, t_2, \ldots, t_n)$; $t_1, t_2, \ldots, t_n$ sú termy
   $t[e] = f(t_1[e], t_2[e], \ldots, t_n[e])$
   $t[e'] = f(t_1[e'], t_2[e'], \ldots, t_n[e'])$
   Z indukčného predpokladu vyplýva, že $t[e] = t'[e]$.

Teraz už môžeme definovať, kedy je nejaká formula pravdivá pri danom ohodnotení, to znamená pri pevne danom význame voľných premenných. Ak je tento pojem zavedený, môžeme už prirodzeným postupom definovať splňovanie danej formuly v štruktúre.

Definícia: (Tarského definícia pravdivosti formuly) *Nech $\mathcal{M}$ je realizácia jazyka L, e je ohodnotenie premenných formuly A. Indukciou podľa zložitosti formuly A budeme definovať pravdivosť formuly A v relačnej štruktúre $\mathcal{M}$ pri ohodnotení e. Označujeme $\mathcal{M} \models A[e]$.*

1. *ak A je atomická formula tvaru $P(t_1, t_2, \ldots, t_n)$, kde P je n-árny predikátový symbol rôzny od "=" a $t_1, t_2, \ldots, t_n$ sú termy. Potom $\mathcal{M} \models A[e]$, ak $(t_1[e], t_2[e], \ldots, t_n[e]) \in P_M \subseteq M^n$*

2. *ak A je atomická formula tvaru $t_1 = t_2$, potom $\mathcal{M} \models A[e]$, ak $t_1[e] = t_2[e]$ (t.j. ak oba termy sú realizované tým istým indivíduom)*

3. *ak A je tvaru $\neg B$, potom $\mathcal{M} \models A[e]$, keď $\mathcal{M} \not\models B[e]$*

4. *ak A je tvaru $B \to C$, potom $\mathcal{M} \models A[e]$, keď $\mathcal{M} \not\models B[e]$ alebo $\mathcal{M} \models C[e]$*

5. *ak A je tvaru $(\forall x)B$, potom $\mathcal{M} \models A[e]$, ak pre ľubovoľné indivíduum $m \in M$ platí $\mathcal{M} \models B[e(x/m)]$*

6. *ak A je tvaru $(\exists x)B$, potom $\mathcal{M} \models A[e]$, ak $\mathcal{M} \models B[e(x/m)]$ pre nejaké indivíduum $m \in M$*

Hovoríme, že formula A je splnená v $\mathcal{M}$ a píšeme $\mathcal{M} \models A$, ak je pravdivá pre ľubovoľné ohodnotenie e.

Poznámka: Bod č. 6 sme definovali 'zbytočne', keďže platí $(\exists x)B \leftrightarrow \neg[(\forall x)\neg B]$. Z rovnakého dôvodu sme nedefinovali pravdivosť pre spojky $\wedge, \vee, \leftrightarrow$, keďže spojky $\neg, \rightarrow$ tvoria úplný systém.

Lema: *Nech $x_1, x_2, \ldots, x_n$ sú všetky voľné premenné formuly A. Ohodnotenia e, e' také, že $e(x_i) = e'(x_i)$ pre $i = \overline{1,n}$. Potom $\mathcal{M} \models A[e] \Leftrightarrow \mathcal{M} \models A[e']$.*

Dôkaz: Prenechávam na čitateľa. (Návod: použite matematickú indukciu na zložitosť formuly A. V báze indukcie rozoberte prípad, keď A je atomická formula, v indukčnom kroku prípady, keď $A \equiv \neg B$, $A \equiv B \rightarrow C$ a $A \equiv (\forall x)B$.)

Poznámka: (k Tarského definícii pravdivosti) Ak je A tvaru $(\forall x)B$, jej pravdivosť ($\mathcal{M} \models A[e]$) nezávisí od ohodnotenia x. Podobne aj pre existenčný kvantifikátor. Teda, ak zisťujeme, či $\mathcal{M} \models A$, stačí zistiť, či $\mathcal{M} \models A[e]$ platí aspoň pre jedno ohodnotenie e.

Poznámka: Ak uzavretá formula A je splnená v $\mathcal{M}$, tak hovoríme, že je pravdivá v $\mathcal{M}$.

Definícia: *Nech $x_1, x_2, \ldots x_n$ sú všetky voľné premenné vo formule A. Potom formulu $A' = (\forall x_1)(\forall x_2)\ldots(\forall x_n)A$ nazývame uzáver formule A.*

Lema: *Formula A je splnená v relačnej štruktúre $\mathcal{M}$ práve vtedy, keď A' (jej uzáver) je pravdivý v $\mathcal{M}$.*

Dôkaz: Prenechávam na čitateľa.

3.3 Substitúcia termov za premenné

V matematickej praxi je bežné dosadzovať za premenné termy a tým získavať špeciálne prípady termov alebo formúl. Z praktických dôvodov musíme najprv definovať substitúciu do termov.

Označenie: *$t_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ – term, ktorý vznikne tak, že každý výskyt x_i nahradíme t_i (naraz!!) pre $i \leq n$.*

Poznámka: Indukciou na zložitosť termu t môžme dokázať, že $t_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ je opäť term.

Teraz môžeme prejsť k formulám. Ak A je formula, t term, potom výraz, potom výraz, ktorý vznikne z formuly A nahradením každého voľného výskytu premennej x termom t označíme $A_x[t]$.

Označenie: $A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ – *formula, ktorá vznikne tak, že každý výskyt* x_i *nahradíme* t_i *(naraz!!) pre* $i \leq n$.

Poznámka: Indukciou na zložitosť formuly A môžme dokázať, že $A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$ je opäť formula.

Zamyslime sa nad zmyslom substitúcií. Ak je napríklad formula A tvaru $x + x = z.x$, potom pre $t = \sin z$ je $A_x[t]$ formula $\sin z + \sin z = z.\sin z$, ktorá je špeciálnym prípadom (inštanciou) formuly A. Našim úmyslom je, aby inštancia $A_x[t]$ "hovorila" o t "to isté", čo formula A "hovorí" o x, za ktoré bolo substituované. Ak budeme postupovať pri substituovaní bez akýchkoľvek obmedzení, môžeme veľmi rýchlo prísť o náš zámer.

Príklad: Uvažujme formulu A na jazyku elementárnej aritmetiky, nech A je tvaru $(\exists y)(x = y + y)$ a term t v tvare $y + 1$. Po substitúcii termu t za x do A dostávame formulu A' tvaru $(\exists y)(y + 1 = y + y)$.

Ak sme formulu A jednoducho interpretovali ako tvrdenie "x je párne" sme teraz na rozpakoch ako interpretovať formulu A'. Len jedno je zrejmé, že A' nemožno chápať ako "y+1 je párne", pretože premenná y je vo formule A viazaná. V tom je totižto hlavná chyba uvedenej substitúcie. Term, ktorý bol substituovaný za voľný výskyt premennej x vo formule A, obsahuje premennú, ktorá sa po substitúcii termu do A stala viazanou. Preto pri substitúcii termov do formúl sa tejto situácii vyhneme; výsledok našej úvahy zhrnieme v nasledujúcej definícii.

Definícia: *Hovoríme, že term t je substituovateľný za x do formuly A, ak pre každú premennú y obsiahnutú v t, žiadna podformula tvaru* $(\forall y)B$, $(\exists y)B$ *formuly A neobsahuje (z hľadiska formuly A) žiaden voľný výskyt premennej x. V ďalšom budeme označenie* $A_x[t]$ *používať len vtedy, ak je term t substituovateľný za x do formuly A.*

Ihneď ľahko rozpoznáme dva prípady, keď substituovateľnosť termu t do formuly A za premennú x je bez akýchkoľvek problémov.

Poznámka 1: Ak formula A je otvorená, tak potom za ľubovoľnú premennú x, ktorá sa vyskytuje v A je substituovateľný ľubovoľný term t.

Poznámka 2: Ak ľubovoľná premenná y vyskytujúca sa v terme t vystupuje vo formule A voľne (nie je viazaná v A), tak potom t je substituovateľný za ľubovoľnú voľnú premennú.

Tieto oba jednoduché prípady substituovateľnosti nevyčerpávajú celú šírku možností.

Príklad: Ak je z premenná, potom term tvaru z je substituovateľný za x do formuly $(x = 0) \rightarrow \neg(\exists z)(z \neq 0)$

Substitúciu termov za premenné budeme používať aj pre viacej premenných súčasne; ak je term t_1 substituovateľný za premennú x_1 do formuly A pre $i = 1, 2, \ldots, n$ tak výrazom $A_{x_1,x_2,\ldots,x_n}[t_1, \ldots, t_n]$ budeme označovať formulu, ktorá vznikne z formuly A nahradením každého voľného výskytu premennej x_i termom t_i pre $i = 1, 2, \ldots, n$. Výslednú formulu nazývame inštancia formuly A.

Nasledujúci jednoduchý fakt je užitočný pri skúmaní pravdivosti inštancií formuly.

Lema: *Nech $\mathcal{M}$ je realizácia jazyka L; A je formula; $t_1, t_2, \ldots, t_n$ sú termy jazyka L a e je ohodnotenie také, že $t_i[e] = m_i$ (m_i sú indivíduá) $i = \overline{1,n}$. Potom:*

1. $t_{x_1,\ldots,x_n}[t_1,\ldots,t_n][e]$ *je indivíduum* $t(e(x_1/m_1,\ldots,x_n/m_n))$
2. $\mathcal{M} \models A_{x_1,\ldots,x_n}[t_1,\ldots,t_n] \Leftrightarrow \mathcal{M} \models A[e(x_1/m_1,\ldots,x_n/m_n)]$

Dôkaz: Prvé tvrdenie:

1. t' nech označuje term $t_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$
   a) $t \equiv x \quad x \notin \{x_1,\ldots,x_n\} \quad \Rightarrow \quad t' = t[e]$
   b) $t \equiv x \quad x \in \{x_1,\ldots,x_n\} \quad \Rightarrow \quad t' = t_i[e]$
2. $t \equiv f(s_1,\ldots,s_n)$
   Z ind. predpokladu: $s_i[t_1,\ldots,t_n][e] = s_i[e(x_1/m_1,\ldots,x_n/m_n)]$ $i = \overline{1,n}$.
   Teda $t'[e] = f_M(s_1[e(x_1/m_1,\ldots,x_n/m_n)],\ldots,s_n[e(x_1/m_1,\ldots,x_n/m_n)])$

Druhé tvrdenie: matematickou indukciou vzhľadom na zložitosť formuly A

1. Nech A je atomická formula $P(s_1, s_2, \ldots, s_n)$, s_i sú termy.
   Označme $A' \equiv A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$.
   $\mathcal{M} \models A'[e] \Leftrightarrow (s_1[t_1,\ldots,t_n][e],\ldots,s_n[t_1,\ldots,t_n][e]) \in P_M \Leftrightarrow$
   $\Leftrightarrow (s_1[e(x_1/m_1,\ldots,x_n/m_n)],\ldots,s_n[e(x_1/m_1,\ldots,x_n/m_n)]) \in P_M \Leftrightarrow$
   $\Leftrightarrow \mathcal{M} \models A[e(x_1/m_1,\ldots,x_n/m_n)]$

   Nech A je atomická formula tvaru $t = s$.
   Označme $A' \equiv t_{x_1,\ldots,x_n}[t_1,\ldots,t_n] = s_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$.
   $\mathcal{M} \models A'[e] \Leftrightarrow t_{x_1,\ldots,x_n}[t_1,\ldots,t_n][e] = s_{x_1,\ldots,x_n}[t_1,\ldots,t_n][e] \Leftrightarrow$
   $\Leftrightarrow t[e(x_1/m_1,\ldots,x_n/m_n)] = s[e(x_1/m_1,\ldots,x_n/m_n)] \Leftrightarrow$
   $\Leftrightarrow \mathcal{M} \models A[e(x_1/m_1,\ldots,x_n/m_n)]$
2. Prípady, keď $A = \neg B$ alebo $A = B \to C$ prenechávam na čitateľa. Rozoberieme však prípad, keď $A = (\forall x)B$.
   - Nech z je niektorá z premenných $x_1, x_2, \ldots, x_n$. BUNV predpokladajme, že $z \equiv x_1$.
     $\mathcal{M} \models A'[e] \Leftrightarrow \forall k \in M : \mathcal{M} \models B_{x_2,\ldots,x_n}[t_2,\ldots,t_n][e(x_1/k)] \Leftrightarrow$
     $\Leftrightarrow \forall k \in M : \mathcal{M} \models B[e(x_1/k, x_2/m_2,\ldots,x_n/m_n)] \Leftrightarrow$
     $\Leftrightarrow \mathcal{M} \models A[e(x_2/m_2,\ldots,x_n/m_n)] \Leftrightarrow \mathcal{M} \models A[e(x_1/k,\ldots,x_n/m_n)]$
     Posledná ekvivalencia vyplýva z toho, že pravdivosť A v $\mathcal{M}$ od ohodnotenia e nezávisí. Stačí teda dosadiť $k := m_1$.
   - Nech z je rôzna od $x_1, x_2, \ldots, x_n$
     — postup je zjednodušením predchádzajúceho prípadu ♣

3.4 Axiómy predikátovej logiky

Vyslovíme teraz axiómy a odvodzovacie pravidlá predikátovej logiky, dosť z nich už poznáme; sú to axiómy, ktoré určujú vlastnosti logických spojok. Ukážeme, že spolu s nimi prechádza vo predikátovej logiky celá výroková logika pri vhodnej voľbe množiny

prvotných formúl. Podobne ako vo výrokovej logike budeme niektoré logické symboly chápať ako základné a iné ako odvodené. Z logických spojok budú základné spojky $\neg$ pre negáciu a pre implikáciu $\rightarrow$, ostatné spojky budú definované zo základných pomocou skratiek rovnakým spôsobom ako vo výrokovej logike. Z oboch kvantifikátorov chápeme symbol pre vľeobecný (veľký) kvantifikátor $\forall$ ako základný a symbol $\exists$ pre existenčný (malý) kvantifikátor ako odvodený. Zavedieme to nasledujúcim spôsobom.

Dohoda: Ak A je formula, x premenná, potom výraz $(\exists x)A$ je skrátený zápis za formulu $\neg(\forall x)\neg A$.

Je zrejmé, že týmto spôsobom možno každú formulu jazyka L vyjadriť len pomocou všeobecného kvantifikátora. Hlavným zmyslom našej dohody je redukovať počet axióm tým, že vlastnosti existenčného kvantifikátora budú odvodené z axióm pre všeobecný kvantifikátor. Axiómy, ktoré určujú vlastnosti logického symbolu pre rovnosť zavedieme neskôr.

Najprv vyslovíme axiómy pre logické spojky.

Definícia: Nech L je jazyk prvého rádu a nech A, B, C sú formuly jazyka L, potom každá formula tvaru

$$\begin{array}{ll} (A \rightarrow (B \rightarrow A)) & \text{(A1)} \\ (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) & \text{(A2)} \\ ((\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)) & \text{(A3)} \end{array}$$

je axióma predikátovej logiky.

Odvodzovacie pravidlo: "modus ponens"

$$\frac{A,\ A \rightarrow B}{B}$$

Uvedené axiómy odpovedajú schéme axióm výrokovej logiky. Ak vezmeme za množinu P prvotných formúl všetky formuly jazyka L, ktoré vo výrokovej logike nemôžeme ďalej rozkladať, to znamená, že P bude tvorená všetkými atomickými formulami a všetkými formulami tvaru $(\forall x)B$ a $(\exists x)B$ pre nejakú premennú x a ľubovoľnú formulu B, potom každá formula jazyka L vznikne z prvotných formúl pomocou logických spojok. Všetky uvedené axiómy preto súhlasia s axiómami výrokovej logiky nad P. Pravidlo odvodzovania vezmeme pravidlo modus ponens.

Vzťah medzi výrokovou logikou a predikátovou logikou je zhrnutý v nasledujúcej vete.

Veta: *Nech A je formula jazyka L predikátovej logiky, nech P je množina všetkých atomických formúl jazyka L a všetkých formúl tvaru $(\exists x)B$ a $(\forall x)B$, kde x je nejaká premenná jazyka L a B formula jazyka L. Ak A je tautológia vo výrokovej logike nad P, potom A je teorémou predikátovej logiky.*

Dôkaz: Podľa definície množiny P každá formula jazyka L nad P vznikne z formúl množiny P len použitím výrokových spojok. Axiómy výrokovej logiky nad P preto súhlasia s odpovedajúcimi axiómami predikátovej logiky a pravidlo modus ponens patrí k obom formálnym systémom. Ak je A tautológia, podľa Postovej vety je odvoditeľná vo výrokovej logike nad P a jej dôkaz (odvodenie) je taktiež odvodením v predikátovej

logike.

Poznámka: V ďalšom budeme bežne používať známe dôkazové postupy výrokovej logiky. Aby sme zdôraznili výrokový charakter nejakého dôkazu, napríklad formuly B z predpokladov $A_1, A_2, \ldots, A_n$, budeme hovoriť, že B je tautologickým dôsledkom formúl $A_1, A_2, \ldots, A_n$. Pri prenášaní výrokových dôkazov si všimnime ešte jednu vec. Výrokové dôkazy častokrát používajú vetu o dedukcii výrokovej logiky. Tento obrat sa prenáša len pokiaľ znak dokázateľnosti má rovnaký význam ako vo výrokovej logike, teda dokázateľnosť z "výrokových axióm" pomocou jediného pravidla modus ponens. Predikátová logika má taktiež svoju vetu o dedukcii, ale so silnejšími požiadavkami na predpoklady. K tomu sa vrátime neskôr. Ďalšie axiómy určujú vlastnosti všeobecného kvantifikátora. Vyjadríme ich v dvoch schémach.

Definícia: Schéma špecifikácie: Ak A je formula, x je premenná a t je term (substituovateľný za premennú x do formuly A), potom formula

$$(\forall x)A \to A_x[t] \quad \text{(A4)}$$

je axióma predikátovej logiky.

Táto axióma má názorný zmysel: Ak A platí pre "ľubovoľné" x, potom platí aj pre každý špeciálny prípad $A_x[t]$.

Druhá schéma, ktorú vyslovíme má skôr technický ráz a jej zmysel vynikne pri štúdiu tzv. prenexných operácií.

Ak A, B sú formuly a x je premenná, ktorá nemá voľný výskyt v A, potom formula

$$(\forall x)(A \to B) \to (A \to (\forall x)B) \quad \text{(A5)}$$

je axióma predikátovej logiky.

Predikátová logika má dve odvodzovacie pravidlá; modus ponens a pravidlo (generalizácie) zovšeobecňovania, ktoré znie: Pre ľubovoľnú premennú x z formuly A odvoď formulu $(\forall x)A$.

$$\frac{A,\ x}{(\forall x)A}$$

Zmysel pravidla zovšeobecnenia je viac menej názorný a určuje úlohu voľných premenných v teorémach; ak formula A je dokázateľná a má voľnú premennú x, potom je dokázateľná (odvoditeľná) aj formula "pre každé x platí A".

Uvedené axiómy a odvodzovacie pravidlá určujú syntax predikátovej logiky bez rovnosti. Predikátová logika s rovnosťou vznikne z popísaného formálneho systému už iba rozšírením jazyka o predikátový symbol rovnosti a pridaním axióm pre tento predikát. Žiadne ďalšie odvodzovacie pravidlá sa nepridávajú. V ďalšom texte bude symbol $\vdash$ označovať dokázateľnosť (odvoditeľnosť) z axióm predikátovej logiky a prípadne ďalších formúl pomocou oboch odvodzovacích pravidiel.

Teraz odvodíme základné vety o vlastnostiach kvantifikátorov. Postup, ktorým to prevádzame je typický pre podobné odvodzovanie aj v iných formálnych systémoch: najprv odvodzujeme "pomocné" odvodzovacie pravidlá, ktoré rozširujú paletu dôkazových obratov a súbežne s tým sa odvodzujú rôzne analógie určitých axióm motivovaných buď "symetriou" alebo istou "dualitou" (napríklad medzi všeobecným a existenčným kvantifikátorom).

Lema 1: *Ak* $\vdash A \to B$ *a premenná x nemá voľný výskyt v A, potom* $\vdash A \to (\forall x)B$.

Dôkaz: Ak je $\vdash A \to B$, potom použitím pravidla zovšeobecnenia platí, že $\vdash (\forall x)(A \to B)$. Pritom $\vdash (\forall x)(A \to B) \to (A \to (\forall x)B)$ je axióma (A5) predikátovej logiky. Formula $A \to (\forall x)B$ sa odvodí z predchádzajúcich dvoch formúl pravidlom modus ponens.

1. krok	$\vdash (\forall x)(A \to B)$	(predpoklad, GEN)
2. krok	$\vdash (\forall x)(A \to B) \to (A \to (\forall x)B)$	(A5)
3. krok	$\vdash A \to (\forall x)B$	(1, 2, MP)

Pomocné odvodzovacie pravidlo, ktoré sme práve dokázali, budeme vďalšom bežne používať.

Lema 2: *Pre ľubovoľné formuly A, B a term t platí:*

1. $\vdash A_x[t] \to (\exists x)A$
2. *ak* $\vdash A \to B$ *a premenná x nemá voľný výskyt v B, potom* $\vdash (\exists x)A \to B$

Dôkaz: Tvrdenie (1) je duálna forma axiómy špecifikácie a (2) je duálna forma pravidla zavedenia všeobecného kvantifikátora. Toto pomocné pravidlo budeme nazývať pravidlo zavedenia existenčného kvantifikátora.

1. krok	$\vdash (\forall x)\neg A \to \neg A_x[t]$	(A4)
2. krok	$\vdash \neg\neg(\forall x)\neg A \to (\forall x)\neg A$	
3. krok	$\vdash \neg(\exists x)A \to (\forall x)\neg A$	$((\exists x)A \equiv \neg[(\forall x)\neg A])$
4. krok	$\vdash \neg(\exists x)A \to \neg A_x[t]$	(1, 3, sylogizmus)
5. krok	$\vdash A_x[t] \to (\exists x)A$	

1. krok	$\vdash (A \to B) \to (\neg B \to \neg A)$	
2. krok	$\vdash (\forall x)(\neg B \to \neg A)$	(1, predpoklad, MP, GEN)
3. krok	$\vdash (\forall x)(\neg B \to \neg A) \to (\neg B \to (\forall x)\neg A)$	(A5)
4. krok	$\vdash \neg B \to (\forall x)\neg A$	(2, 3, MP)
5. krok	$\vdash \neg(\forall x)\neg A \to \neg\neg B$	
6. krok	$\vdash (\exists x)A \to B$	

Lema 3: *Nech A' je inštancia formuly A (t.j. A' je tvaru* $A_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$*). Potom ak* $\vdash A$*, tak* $\vdash A'$.

Dôkaz: indukciou vhľadom na n – počet substituovaných termov

1. báza indukcie:

1. krok	$\vdash A \Rightarrow \vdash (\forall x_1)A$	(predpoklad, GEN)
2. krok	$\vdash (\forall x_1)A \to A_{x_1}[t_1]$	(A4)
3. krok	$\vdash A_{x_1}[t_1]$	(1, 2, MP)

2. indukčný krok: Nech $z_1, \ldots, z_n$ sú premenné, ktoré sa nevyskytujú v A ani v ter-

moch $t_1, \ldots, t_n$. Potom môžme uplatniť postup z bázy indukcie nasledovne:

$$\begin{array}{l}
\vdash A \\
\vdash A_{x_1}[z_1] \\
\vdash A_{x_1,x_2}[z_1, z_2] \\
\vdash A_{x_1,\ldots,x_n}[z_1, \ldots, z_n] \equiv B \\
\vdash B \\
\vdash B_{z_1}[t_1] \\
\vdash B_{z_1,z_2}[t_1, t_2] \\
\vdash B_{z_1,\ldots,z_n}[t_1, \ldots, t_n] \equiv A'
\end{array}$$

Príklad: Prečo sme museli indukčný krok v dôkaze predchádzajúcej vety tak skomplikovať? Uvažujme nasledujúcu formulu: $A \equiv x < y$.

- Spravme substitúciu $A_{x,y}[y, x]$, pričom všetky premenné nahradíme naraz! Dostávame $A_{x,y}[y, x] \equiv y < x$.
- Spravme substitúciu $A_{x,y}[y, x]$, pričom najprv nahradíme x, potom y! Dostávame $A_{x,y}[y, x] \equiv x < x$.

Keďže sme potrebovali práve postupnú substitúciu museli sme si pomôcť pomocnými premennými.

Poznámka: Z lemy vyplýva, že ľubovoľné voľné premenné možno premenovať.

Dôsledok: *Nech $x_1, \ldots, x_n$ sú všetky voľné premenné vyskytujúce sa vo formule A. Nech $z_1, \ldots, z_n$ sú navzájom rôzne premenné také, že z_i je substituovateľná za x_i $i = \overline{1,n}$ vo formule A. Ak A' je inštancia tvaru $A_{x_1,\ldots,x_n}[z_1, \ldots, z_n]$, potom ak $\vdash A$, tak $\vdash A'$.*

Dôkaz: Vyplýva z lemy 3.

Lema 4: *Pre ľubovoľnú formulu A, premenné $x_1, \ldots, x_n$ a termy $t_1, \ldots, t_n$ platí:*

1. $\vdash (\forall x_1)(\forall x_2) \ldots (\forall x_n)A \rightarrow A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$
2. $\vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \rightarrow (\exists x_1)(\exists x_2) \ldots (\exists x_n)A$

Dôkaz:

1. Uvažujme špeciálny tvar axiómy špecifikácie: $\vdash (\forall x)A \rightarrow A$. Z neho a z pravidla jednoduchého sylogizmu môžme odvodiť $\vdash (\forall x_1) \ldots (\forall x_n)A \rightarrow A$. Formula $\vdash (\forall x_1)(\forall x_2) \ldots (\forall x_n)A \rightarrow A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ je iba inštanciou tejto formuly, takže na základe lemy 3 je dokázateľná.
2. Analogický postup s využitím špeciálneho tvaru formuly z lemy 2:
   $\vdash A \rightarrow (\exists x_1)(\exists x_2) \ldots (\exists x_n)A$.

Poznámka: Z formúl v predchádzajúcom dôkaze môžme pomocou pravidiel zavedenia všeobecného (Lema 1) a existenčného (Lema 2(2.)) kvantifikátora dokázať tvrdenia:

$$\vdash (\forall x_1) \ldots (\forall x_n)A \leftrightarrow (\forall x_{\pi(1)}) \ldots (\forall x_{\pi(n)})A$$

$$\vdash (\exists x_1)\dots(\exists x_n)A \leftrightarrow (\exists x_{\pi(1)})\dots(\exists x_{\pi(n)})A$$

kde π je ľubovoľná permutácia množiny $\{1, 2, \dots, n\}$.

Definícia: *Nech $x_1, \dots, x_n$ sú všetky premenné s voľným výskytom vo formule A v nejakom usporiadaní. Potom formulu $(\forall x_1)(\forall x_2)\dots(\forall x_n)A$ nazveme uzáver formuly A.*

Veta (o uzávere): *Nech A' je uzáver A. Potom $\vdash A \Leftrightarrow \vdash A'$.*

Dôkaz: Prvú implikáciu môžme dokázať pomocou pravidla zovšeobecnenia. Druhú implikáciu pomocou lemy 4(jej prvej časti).

Poznámka: Veta o uzávere charakterizuje vlastnosti voľných premenných v dokázateľných formulách.

Lema 5 (o distribúcii kvantifikátorov): *Ak je $\vdash A \to B$ potom $\vdash (\forall x)A \to (\forall x)B$ a $\vdash (\exists x)A \to (\exists x)B$.*

Dôkaz: Pre všeobecný kvantifikátor použijeme najprv axiómu špecifikácie a nasledovne pravidlo zavedenia všeobecného kvantifikátora. Pre existenčný kvantifikátor použijeme lemu 2 (najprv prvú a následne jej druhú časť).

Veta: (o ekvivalencii) *Nech formula A' vznikne z formuly A nahradením všetkých výskytov podformúl $B_1, \dots B_n$ v uvedenom poradí formulami $B'_1, \dots, B'_n$. Ak platí $\vdash B_i \leftrightarrow B'_i$ pre $i = \overline{1,n}$ potom $\vdash A \leftrightarrow A'$.*

Dôkaz: Veta je obdobou tvrdenia vo výrokovej logike, ktorú sme už dokázali. Ešte si rozoberieme prípad, keď $A \equiv (\forall x)B$. Vtedy stačí použiť indukčný predpoklad a uplatniť na ňho vetu o distribúcii kvantifikátorov.

Definícia: *Hovoríme, že formula A' je variantom formuly A, ak A' vznikne z A postupným nahradením podformúl tvaru $(Qx)B$ formulami $(Qy)B_x[y]$, kde y nie je voľná vo formule B a $Q \in \{\forall, \exists\}$.*

Veta: (o variantoch) *Nech A' je variant formuly A. Potom $\vdash A \leftrightarrow A'$.*

Dôkaz: Stačí dokázať, že ak nahrádzame v A formulu typu $(Qx)B$ formulou $(Qy)B_x[y]$, získame ekvivalentné formuly. Potom už len aplikujeme vetu o ekvivalencii.

1. $Q \equiv \forall$:

1. krok	$\vdash (\forall x)B \to B_x[y]$	(A4)
2. krok	$\vdash (\forall x)B \to (\forall y)B_x[y]$	(GEN)

1. krok	označme $B' \equiv B_x[y]$	
2. krok	$\vdash (\forall y)B' \to B'_y[x]$	(A4)
3. krok	$\vdash (\forall y)B' \to (\forall x)B'_y[x]$	(Lema 1)
4. krok	$\vdash (\forall y)B' \to (\forall x)B$	

2. $Q \equiv \exists$: analogicky

3.5 Veta o dedukcii

Definícia: *Nech A je niektorá formula z množiny T a nech $A_1, \dots A_n$ je ľubovoľné odvodenie B z predpokladov (hypotéz) T. Hovoríme, že formula A_i je v tomto odvodení závislá od A, ak platí:*

1. *formula A_i je A a objavila sa v odvodení ako prvok T*
2. *A_i je formula, ktorú sme dostali podľa pravidla zovšeobecnenia z A_j $(j < i)$ a formula A_j závisí od A*
3. *formula A_i vznikla odvodením z formúl A_j, A_k $j, k < i$ pomocou pravidla MP a aspoň jedna z formúl A_j, A_k závisí od A*
4. *A_i je jedna zo schém axióm predikátovej logiky a obsahuje aspoň jednu podformulu, ktorá závisí od A*

Veta: (o dedukcii) *Nech T je množina formúl a A, B sú formuly predikátovej logiky.*

1. *Ak $T \vdash A \to B$, potom $T, A \vdash B$*
2. *Ak $T, A \vdash B$ a existuje také odvodenie B z $\{T, A\}$, že sa v ňom pri aplikácii pravidla zovšeobecnenia na formuly, ktoré v tomto odvodení závisia od A veľkým kvantifikátorom neviaže žiadna premenná voľná v A, potom $T \vdash A \to B$.*

Dôkaz: Prvé tvrdenie sa dokazuje rovnako ako vo výrokovej logike. Druhé tvrdenie dokážeme indukciou na dĺžku odvodenia B z $\{T, A\}$.

1. báza indukcie: ako vo výrokovej logike (3 prípady)
2. indukčný krok: ako vo výrokovej logike (4 prípady), avšak pribudne ďalší prípad — ak sme formulu $B(A_n)$ získali použitím pravidla zovšeobecnenia.
   - Nech A_i nezávisí od A

1. krok	$T \vdash A_i$	
2. krok	$T \vdash (\forall x)(A_i)$	(GEN)
3. krok	$\vdash (\forall x)A_i \to (A \to (\forall x)A_i)$	(A1)
4. krok	$T \vdash A \to B$	$(B \equiv (\forall x)A_i)$

   - Nech A neobsahuje x voľne

1. krok	$T \vdash A \to A_i$	(IP)
2. krok	$T \vdash (\forall x)(A \to A_i)$	(GEN)
3. krok	$\vdash (\forall x)(A \to A_i) \to (A \to (\forall x)A_i)$	(A5)
4. krok	$T \vdash A \to (\forall x)A_i$	(2, 3, MP)

Dôsledok 1: *Z dôkazu je vidieť, že stačí, ak vieme, že v odvodení formuly B z predpokladov $\{T, A\}$ nebolo použité pravidlo zovšeobecnenia na žiadnu premennú, ktorá je voľná v A, potom $T \vdash A \to B$.*

Dôsledok 2: *Ak $T, A \vdash B$ a A je uzavretá, potom $T \vdash A \to B$.*

Dôsledok 3: *Ak $T, A \vdash B$ a existuje také odvodenie B z predpokladov $\{T, A\}$, že neaplikujeme pravidlo zovšeobecnenia, potom $T \vdash A \to B$.*

Veta: (o konštantách) *Nech T je množina formúl jazyka L a nech A je formula jazyka L. Nech jazyk L' vznikne z L rozšírením o nové konštanty (symboly pre konštanty). Nech $c_1, \ldots, c_m$ sú nové konštanty, potom $T \vdash A[c_1, \ldots, c_m] \Leftrightarrow T \vdash A$.*

Dôkaz: Jedna implikácia vyplýva priamo z lemy 3. Druhú implikáciu dokážeme nasledovne: Nech $A'_1, \ldots, A'_n$ je odvodenie formuly $A[c_1, \ldots, c_m]$ z T. Nech $y_2, \ldots, y_m$ sú premenné, ktoré sa nevyskytujú v A ani v žiadnej formule dôkazu $A'_1, \ldots, A'_n$. Nech A_i vznikne z A'_i tak, že konštanty c_j nahradíme premennými y_j pre $j = \overline{1, m}$. Tým dostaneme dôkaz formuly $A[y_1, \ldots, y_m]$ z predpokladov T. Keďže A je iba inštanciou tejto formuly, tak platí $T \vdash A$.

Poznámka: Uvažujme, že A nie je uzavretá (obsahuje voľné premenné $y_1, \ldots, y_m$). Chceme dokázať $T \vdash A \to B$. Rozšírme teda L o nové konštanty $c_1, \ldots, c_m$. Podľa vety o konštantách a vety o dedukcii platí:

$$T \vdash A \to B \Leftrightarrow T \vdash A[c_1 \ldots c_m] \to B[c_1 \ldots c_m] \Leftrightarrow T, A[c_1 \ldots c_m] \vdash B[c_1 \ldots c_m]$$

Veta: (zovšeobecnenie vety o dedukcii) *Ak A je formula a T, S sú množiny formúl, potom $T \cup S \vdash A$ práve vtedy, keď existuje prirodzené číslo n a formuly $B_1, \ldots, B_n$ také, z ktorých každá je uzáverom nejakej formuly z S, pričom platí:*

$$T \vdash B_1 \to (B_2 \to (\ldots \to (B_n \to A) \ldots)$$

Dôkaz: Ak formuly $B_1, B_2, \ldots, B_n$ spĺňajú podmienky vety, potom $S \vdash B_i$ pre $i = 1, 2, \ldots, n$ a podľa vety o uzávere výsledok dostávame niekoľkonásobným použitím pravidla modus ponens.

Ak je A dokázateľná z predpokladov T, S a nech $A_1, A_2, \ldots, A_n$ sú všetky formuly z S použité v dôkaze formuly A ako predpoklady. Ak B_i je uzáverom formuly A_i pre $i = 1, 2, \ldots, n$, potom $T, B_1, B_2, \ldots, B_n \vdash A$, pretože každá z formúl A_i je dokázateľná z B_i podľa vety o uzávere. Nakoniec $T \vdash B_1 \to (B_2 \to \ldots (B_n \to A) \ldots)$ dostávame z predchádzajúceho tvrdenia podľa vety odedukcii.

Poznámka: Predchádzajúca veta ukazuje, že dokázateľnosť formuly z nejakej množiny predpokladov je ekvivalentná dokázateľnosti inej formuly z redukovanej množiny predpokladov. Je zrejmé, že rovnakým spôsobom by bolo možné eliminovať i množinu T a redukovať tak dokázateľnosť formuly A na dokázateľnosť inej formuly len v predikátovej logike. Tento výsledok, ktorý ukazuje významné postavenie predikátovej logiky medzi teóriami, nemá priamy praktický význam, pretože nedáva návod ako zostrojiť formulu $T \vdash B_1 \to (B_2 \to \ldots (B_n \to A) \ldots)$

Na záver odvodíme ešte jeden dôsledok vety o dedukcii. Pripomíname, že množina formúl T jazyka L je sporná, ak ľubovoľná formula jazyka L je odvoditeľná z T. Z teorémy $\vdash \neg A \to (A \to B)$ je zrejmé, že T je sporná práve vtedy, keď z T je odvoditeľná nejaká formula A a jej negácia $\neg A$.

Dôsledok: (o dôkaze sporom) *Nech A' je uzáver formuly A, nech T je množina*

formúl. Tvrdíme, že $T \vdash A \Leftrightarrow T \cup \{\neg A'\}$ *je sporná.*

Dôkaz: Nech $T \vdash A$. Potom podľa vety o uzávere $T \vdash A'$. Teória $T \cup \{\neg A'\}$ je sporná, pretože z $\vdash \neg A \rightarrow (A \rightarrow B)$ by sme vedeli dokázať ľubovoľnú formulu. Obrátene nech $T \cup \{\neg A'\}$ je sporná. Potom z nej možno dokázať ľubovoľné tvrdenie, teda aj $T \cup \{\neg A'\} \vdash A'$. Z vety o dedukcii vyplýva $T \vdash \neg A' \rightarrow A'$. Použitím tautológie $\vdash (\neg A' \rightarrow A') \rightarrow A'$ dostávame pomocou pravidla MP tvrdenie $T \vdash A'$. Z vety o uzávere napokon vyplýva $T \vdash A$.

Predchádzajúce tvrdenie ukazuje, že dôkaz nejakej formuly môžeme rovnocenne nahradiť dôkazom spornosti nejakej množiny formúl. Taký postup sa nazýva nepriamym dôkazom a je obvyklý v matematickej praxi. Používa sa aj v niekoľkých metódach dokazovania viet pomocou počítačov.

3.6 Prenexné tvary formúl

Vo výrokovej logike sme ukázali, že ku každej formule môžeme zostrojiť ekvivalentnú formulu v jednom z dvoch syntaktických tvarov: konjunktívnom alebo disjunktívnom. V oboch tvaroch sa používajú len spojky, ktoré vyjadrujú negáciu, konjunkciu a disjunkciu, naviac len v určitom poradí. V rovnakom duchuje aj definícia prenexného tvaru formúl predikátovej logiky, ktorá požaduje, aby sa kvantifikátory pri výstavbe formuly uplatnili až nakoniec.

Prv než vyslovíme definíciu pripomíname, že formuly, ktoré neobsahujú žiadnu viazanú premennú nazývame otvorené. To znamená, že otvorené sú práve tie formuly, ktoré vznikajú z atomických podformúl len pomocou logických spojok.

Definícia: *Hovoríme, že formula A je v prenexnom tvare, ak má tvar:*

$$(Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) B,$$

kde $n \geq 0$ a pre každé $i = \overline{1,n}$ je $Q_i \in \{\forall, \exists\}$, B je otvorená formula a $x_1, \ldots, x_n$ sú navzájom rôzne premenné. B sa nazýva otvorené jadro formuly A a postupnosť kvantifikátorov, ktoré jej predchádzajú je prefix.

Príklad: Formula $(\forall x)(\forall y)(\exists z)(x = y + z)$ je v prenexnom tvare. Otvorené jadro formuly z vyššie uvedenej definície predstavuje jej najväčšiu otvorenú podformulu a prefix obsahuje všetky jej kvantifikátory. V prípade $n = 0$ prefix odpadá a prenexný tvar je totožný s B. Požiadavka, aby všetky premenné v prefixe boli rôzne navzájom má obmedziť zbytočné kvantifikácie.

Ukážeme, že každú formulu predikátovej logiky je možné transformovať doprenexného tvaru.

Veta: *Ku každej formule A predikátovej logiky môžme zostrojiť formulu A' v prenexnom tvare takú, že* $\vdash A \leftrightarrow A'$.

Dôkaz: Uvedieme neskôr.

Poznámka: Formulu A' získame z A pomocou prenexných operácií ("vyťahovanie kvantifikátorov pred zátvorku").

Označenie: Ak Q označuje všeobecný kvantifikátor, tak $\overline{Q}$ označuje existenčný a naopak.

Prenexné operácie:

1. podformulu B nahraď nejakým jej variantom B' (premenovanie premenných)
2. podformulu $\neg(Qx)B$ nahraď formulou $(\overline{Q}x)\neg B$
3. ak premenná x nie je voľná vo formule B, podformulu $B \to (Qx)C$ nahraď formulou $(Qx)(B \to C)$
4. ak premenná x nie je voľná vo formule C, podformulu $(Qx)B \to C$ nahraď formulou $(\overline{Q}x)(B \to C)$
5. ak symbol $\diamond$ zastupuje symbol $\wedge$ alebo $\vee$ a premenná x nie je voľná vo formule B, tak podformulu $B \diamond (Qx)C$ nahraď formulou $(Qx)(B \diamond C)$

Jadrom dôkazu vyššie uvedenej vety je nasledujúce tvrdenie.

Lema: *Pre ľubovoľné formuly B, C a každú premennú x platí:*

1. $\vdash (\overline{Q}x)\neg B \leftrightarrow \neg(Qx)B$
2. $\vdash (Qx)(B \to C) \leftrightarrow (B \to (Qx)C)$, ak x nie je voľná v B
3. $\vdash ((\overline{Q}x)(B \to C) \leftrightarrow ((Qx)B \to C)$, ak x nie je voľná v C
4. $\vdash (Qx)(B \diamond C) \leftrightarrow ((Qx)B \diamond C)$, ak x nie je voľná v C $(\diamond \in \{\wedge, \vee\})$

Prenexné operácie teda nahrádzajú podformuly ekvivalentnými formulami. Tvrdenie (4) dáva ekvivalenciu pre konjunkciu a disjunkciu, ak si uvedomíme, že obidve spojky sú "komutatívne". Ďalej poznamenávame, že nahradenie podformuly nejakým jej variantom je ekvivalentná operácia.

Dôkaz: Ak v tvrdení (1) zastupuje symbol Q kvantifikátor, potom $\vdash \neg(\forall x)B \leftrightarrow \neg(\forall x)\neg\neg B$, pretože formuly B a $\neg\neg B$ sú ekvivalentné. Pritom formulu na pravej strane ekvivalencie je možné vyjadriť skratkou $(\exists x)\neg B$. Prípad, keď Q zastupuje existenčný kvantifikátor je analogický: $\vdash \neg(\exists x)B \leftrightarrow \neg(\exists x)\neg\neg B \Leftrightarrow (\forall x)\neg B$.

Teraz dokážeme tvrdenie (2), najprv predpokladajme, že symbol Q zastupuje všeobecný kvantifikátor. Pokiaľ premenná x nie je voľná vo formule B , implikácia $\vdash (\forall x)(B \to C) \to (B \to (\forall x)C)$ je axióma. Aby sme dokázali obrátenú implikáciu, treba si uvedomiť, že formula $B \to C$ vznikne "zložením" implikácií $B \to (\forall x)C$ a $(\forall x)C \to C$ pomocou pravidla zámeny predpokladov. Ak na túto "zloženú" formulu použijeme jednoduchý sylogizmus a pravidlo modus ponens, tak dostávame, že $\vdash ((\forall x)C \to C) \to ((B \to (\forall x)C) \to (B \to C))$ je teoréma. Použitím pravidla modus ponens dostávame $\vdash (B \to (\forall x)C) \to (B \to C)$ a odtiaľ pravidlom zavedenia všeobecného kvantifikátora dostávame $\vdash (B \to (\forall x)C) \to (\forall x)(B \to C)$, čo je obrátená implikácia a s uvedenou axiómou nám dávajú tvrdenie (2) pre prípad, keď Q je všeobecný kvantifikátor.

Zostáva nám prípad, že Q je existenčný kvantifikátor. Vieme, že $\vdash C \to (\exists x)C$ – duálny tvar axiómy špecifikácie. Tak ako v predchádzajúcom prípade analogicky získavame formulu $B \to (\exists x)C$ "zložením" formúl $B \to C$ a $C \to (\exists x)C$, ďalej použitím sylogizmu dostávame $\vdash (C \to (\exists x)C \to ((B \to C) \to (B \to (\exists x)C))$ a použitím modus ponens dostávame $\vdash (B \to C) \to (B \to (\exists x)C)$ a napokon $\vdash (\exists x)(B \to C) \to (B \to (\exists x)C)$ môžeme odvodiť pravidlom zavedenia existenčného kvantifikátora, pretože $B \to (\exists x)C$ neobsahuje voľne premennú x.

K dôkazu obrátenej implikácie využijeme fakt, že pre ľubovoľné formuly D, E, F je formula $\vdash (\neg D \to F) \to ((E \to F) \to ((D \to E) \to F))$ tautológia. Ľahko sa o tom možno presvedčiť na základe nasledujúcich úvah: z predpokladov

$$\neg D \to F, E \to F, D \to E, D \vdash F$$

ďalej z predpokladov

$$\neg D \to F, E \to F, D \to E, \neg D \vdash F$$

na základe lemy o neutrálnej formule

$$\neg D \to F, E \to F, D \to E \vdash F$$

a použitím vety o dedukcii trikrát dostávame uvažované tvrdenie.

Ďalej odvodíme

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

distribúciou kvantifikátora $\exists$ a axiómy (A1). Vieme, že platí

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

a

$$\vdash \neg B \to (B \to C).$$

Zložením týchto dvoch implikácii dostávame

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

ako tautologický dôsledok. Ak nahradíme $B, (\exists x)C, (\exists x)(B \to C)$ v uvedenom poradí za D, E, F do vyššie uvedenej teorémy, tak použitím pravidla modus ponens dostávame obrátenú implikáciu

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

Dôkaz 4. ekvivalencie pre prípad, že Q zastupuje kvantifikátor $\forall$ je nasledujúci: máme teda dokázať, že

$$\vdash (\exists x)(B \to C) \leftrightarrow ((\forall x)B \to C).$$

Platí

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

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

$$\vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to (\exists x)\neg B).$$

Ďalej podľa 3. ekvivalencie platí

$$\vdash (\exists x)(\neg C \to \neg B) \leftrightarrow (\neg C \to (\exists x)\neg B)$$

ďalej platí

$$\vdash (\exists x)(B \to C) \leftrightarrow (\neg C \to (\exists x)\neg B)$$

a teda

$$\vdash (\exists x)(B \to C) \leftrightarrow ((\forall x)\neg\neg B \to \neg\neg C).$$

Prípad, keď Q je $\exists$ je analogický.

Posledné tvrdenie lemy sa dokáže tak, že rozpíšeme spojku $\diamond$ pomocou negácie a implikácie a použijeme prenexné operácie 2 až 4.

Dôkaz: (sľúbený dôkaz vety) Matematickou indukciou na zložitosť formuly A:

1. báza indukcie: A je atomická formula a teda $A \equiv A'$
2. indukčný krok: rozoberieme 3 prípady
   - $A = \neg B$
     Na B sa vzťahuje indukčný predpoklad. Uplatnením prenexnej operácie (2) dostaneme formulu A v prenexnom tvare.
   - $A = B \to C$
     Na B a C sa vzťahuje indukčný predpoklad. Formulu $B' \to C'$ najprv upravíme pomocou operácie (1) tak, aby mali rôzne premenné a potom pomocou operácií (3) a (4) tak, aby sme dostali formulu v prenexnom tvare.
   - $A = (\forall x)B$
     Podľa IP vytvoríme B'. Ak x nie je v prefixe B', tak $A' \equiv (\forall x)B'$, ináč $A' \equiv B'$.

Definícia: *Nech prefix uzavretej formuly A má tvar* $(\exists x_1)\ldots(\exists x_k)(\forall x_{k+1})\ldots(\forall x_m)$*, kde* $k+1 \geq 1$*. Potom hovoríme, že formula A je vyjadrená v Skolemovom tvare.*

Definícia: *Hodnosťou formuly A vyjadrenej v prenexnom tvare nazývame počet všeobecných kvantifikátorov, ktoré v prefixe predchádzajú poslednému existenčnému kvantifikátoru (počítame zľava).*

Veta: *Ku každej formule A predikátovej logiky možno zostrojiť formulu A' vyjadrenú v Skolemovom tvare tak, že* $\vdash A \Leftrightarrow \vdash A'$*.*

Dôkaz: Môžeme predpokladať, že formula A je uzavretá, pretože $\vdash A$ práve vtedy, keď jej uzáver je teorémou. Ak berieme do úvahy predchádzajúcu vetu , môžeme predpokladať, že A je vyjadrená v prenexnom tvare. Hodnosťou takej formuly nazývame počet veľkých kvantifikátorov, ktoré v prefixe predchádzajú poslednému existenčnému kvantifikátoru, počítame zľava doprava. Ak hodnosť formuly A je rovná nule, potom je formula vyjadrená v Skolemovom tvare. Takýmto spôsobom báza indukcie (pri dôkaze vety pomocou matematickej indukcie vzhľadom na hodnosť formuly) zrejme platí.

Induktívny krok: Predpokladajme, že vieme zostrojiť Skolemovu formu pre formuly hodnosti neprevyšujúcej $m-1$. Ukážeme ako možno zostrojiť Skolemovu formu pre

formuly hodnosti rovnej m. Uvažujme ľubovoľnú formulu A hodnosti m. Nech má nasledujúci tvar:

$$A = (\exists x_1) \dots (\exists x_n)(\forall y)B(x_1, \dots, x_n, y),$$

kde vo formule B sú voľnými premennými iba $x_1, \dots, x_n, y$. Pretože hodnosť formuly A je rovná m, tak vo formule B poslednému existenčnému kvantifikátoru predchádza rovno $m-1$ veľkých kvantifikátorov. Vezmime ľubovoľný (n+1)-árny predikátový symbol $P^{(n+1)}$, ktorý sa nevyskytuje vo formule A a uvažujme formulu A^*:

$$A^* = (\exists x_1) \dots (\exists x_n)[(\forall y)(B(x_1, \dots, x_n, y) \to P^{(n+1)}(x_1, \dots, x_n, y)) \to (\forall y)P^{(n+1)}(x_1, \dots, x_n, y)].$$

Dokážeme, že $\vdash A$ práve vtedy, keď $\vdash A^*$.

Nech je $\vdash A$. Pretože

$$\vdash (B \to P^{(n+1)}) \to (B \to P^{(n+1)})$$

a vezmeme do úvahy tautológiu

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

dostávame

$$\vdash [(B \to P^{(n+1)}) \to (B \to P^{(n+1)}) \to (B \to ((B \to P^{(n+1)}) \to P^{(n+1)}))],$$

použitím pravidla modus ponens dostávame:

$$\vdash (B \to ((B \to P^{(n+1)}) \to P^{(n+1)})).$$

Ak budeme aplikovať pravidlo zovšeobecnenia (vzhľadom na y) a teorému

$$\vdash (\forall x)(A \to B) \to ((\forall x)A \; to (\forall x)B)$$

dvakrát, dostávame:

$$\vdash ((\forall y)B \to ((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})).$$

Potom použijeme n-krát pravidlo zovšeobecnenia a n-krát teorému

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

dostávame:

$$\vdash (\exists x_1) \dots (\exists x_n)(\forall y)B \to (\exists x_1) \dots (\exists x_n)((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})$$

ak vezmeme do úvahy, že

$$A = (\exists x_1) \dots (\exists x_n)(\forall y)B,$$

tak potom dostávame, že $\vdash A^*$.

Predpokladajme teraz, že $\vdash A^*$, ak zameníme predikátový symbol $P^{(n+1)}$ formulou B (v niektorých axiomatických systémoch používajú pravidlo zámeny formuly namiesto predikátového symbolu ako jedno z odvodzovacích pravidiel), dostávame teorému:

$$\vdash (\exists x_1) \dots (\exists x_n)((\forall y)(B \to B) \to (\forall y)B),$$

ak uvažujeme teorému

$$\vdash (\exists x)(A \to B) \to ((\forall x)A \to (\exists x)B)$$

a použijeme ju n-krát, tak dostávame:

$$\vdash (\exists x_1)\dots(\exists x_n)((\forall y)(B \to B) \to (\forall y)B) \to (\forall x_1)\dots(\forall x_n)(\forall y)(B \to B) \to (\exists x_1)\dots(\exists x_n)(\forall y)B,$$

ak použijeme dvakrát pravidlo modus ponens, tak dostávame $\vdash (\exists x_1)\dots(\exists x_n)(\forall y)B$, teda, že $\vdash A$.

Vyššie sme teda dokázali, že $\vdash A \Leftrightarrow \vdash A^*$. Pre dokončenie dôkazu vety vyjadrime v špeciálnom tvare formulu A^*. Nech teda $B = (Q_1 z_1)\dots(Q_l z_l)C$, kde C je formula bez kvantifikátorov. Dostávame

$$A^* \leftrightarrow (\exists x_1)\dots(\exists x_n)((\forall y)[(Q_1 z_1)\dots(Q_l z_l)C \to P^{(n+1)}] \to (\forall y)P^{(n+1)})$$

$$\leftrightarrow (\exists x_1)\dots(\exists x_n)((\forall y)(\hat{Q}_1 z_1)\dots(\hat{Q}_l z_l)[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}).$$

Použili sme l-krát tvrdenia $\vdash (\forall x)(A \to B) \leftrightarrow ((\exists x)A \to B)$ a $(\exists x)(A \to B) \leftrightarrow ((\forall x)A \to B)$. Ďalej dostávame, že

$$A^* \leftrightarrow (\exists x_1)\dots(\exists x_n)((\exists y)(\hat{Q}_1 z_1)\dots(\hat{Q}_l z_l)[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}).$$

Použili sme 1-krát $(\exists x)(A \to B) \leftrightarrow (\forall x)A \to B$, ďalej

$$A^* \leftrightarrow (\exists x_1)\dots(\exists x_n)(\exists y)(Q_1 z_1)\dots(Q_l z_l)([C \to P^{(n+1)}] \to (\forall u)P^{(n+1)})$$

l-krát sme použili $\vdash (\forall x)(A \to B) \leftrightarrow (\exists)A \to B$ a $\vdash (\exists x)(A \to B) \leftrightarrow (\forall x)A \to B$. Nakoniec použitím tvrdenia $\vdash (\forall x)(A \to B) \leftrightarrow (A \to (\forall x)B)$ dostávame, že

$$A^* \leftrightarrow (\exists x_1)\dots(\exists x_n)(Q_1 z_1)\dots(Q_l z_l)([C \to P^{(n+1)}] \to P^{(n+1)}).$$

Poznamenávame, že v prefixe $(Q_1 z_1)\dots(Q_l z_l)$ poslednému existenčnému kvantifikátoru predchádza rovno $m-1$ všeobecných kvantifikátorov. Takýmto spôsobom sme dokázali platnosť indukčného kroku. Veta je dokázaná. Na záver uvádzame, že tvrdenia, na platnosť ktorých sa vo vete odvolávame, vyplývajú z platnosti prenexných operácií, sú to ich špeciálne prípady. Ďalej poznamenávame, že $C : C(x_1, \dots, x_n, y, z_1, \dots, z_l)$; $P : P^{(n+1)}(x_1, \dots, x_n, y)$ alebo $P^{(n+1)}(x_1, \dots, x_n, u)$.

3.7 Predikátová logika s rovnosťou

Pri definícii splňovania sme zdôraznili zvláštne postavenie predikátu rovnosti v sémantike jazyka s rovnosťou. Axiómy rovnosti, ktoré syntakticky popisujú vlastnosti predikátu rovnosti vyjadrujú prirodzené požiadavky, ktoré matematika kladie na rovnosť: aby každé indivíduum bolo rovné samo sebe, teda aby rovnosť bola reflexívna a aby sebe rovné indivíduá mali rovnaké vlastnosti voči každému predikátu jazyka a dávali rovnaké výsledky pri použití ľubovoľnej operácie.

V ďalšom budeme predpokladať, že jazyk, s ktorým pracujeme obsahuje predikátový symbol "=" pre rovnosť. Syntaktické vlastnosti tohoto predikátu sú vyjadrené v troch nasledujúcich schémach axióm.

Definícia: *Označme nasledujúce axiómy (R1), (R2) a (R3):*

1. *Ak x je premenná, potom formula $x = x$ je axióma.*

2. *Ak $x_1, \ldots, x_k; y_1, \ldots, y_k$ sú premenné, a ak f je k-árny funkčný symbol, potom formula $(x_1 = y_2 \to (x_2 = y_2 \to \ldots \to (x_k = y_k \to f(x_1, \ldots, x_k) = f(y_1, \ldots, y_k)\ldots)$ je axióma.*

3. *Ak $x_1, \ldots, x_k; y_1, \ldots, y_k$ sú premenné, a ak P je k-árny predikátový symbol, potom formula $(x_1 = y_2 \to (x_2 = y_2 \to \ldots \to (x_k = y_k \to (P(x_1, \ldots, x_k) \to P(y_1, \ldots, y_k))\ldots)$ je axióma.*

Axióma (R1) poskytuje reflexívnosť rovnosti, budeme ju nazývať axióma identity. Symetriu a tranzitívnosť je možné odvodiť z axiómy (R3) pre predikát rovnosti.

Lema: (symetria a tranzitívnosť)

1. $x = y \to y = x$

2. $x = y \to y = z \to x = z$

Dôkaz:

$\vdash x = y \to x = x \to x = x \to y = x$	(R3)
$\vdash x = x \to x = x \to x = y \to y = x$	(VD)
$\vdash x = y \to y = x$	(R1, MP, MP)

$\vdash y = x \to z = z \to y = z \to x = z$	(R3)
$\vdash z = z \to y = x \to y = z \to x = z$	(VD)
$\vdash y = x \to y = z \to x = z$	(R1, MP)
$\vdash x = y \to y = z \to x = z$	(symetria)

Veta: *Nech $t_1, \ldots, t_n, s_1, \ldots, s_n$ sú termy také, že platí $\vdash t_i = s_i$ pre $i = \overline{1,n}$. Potom*

1. *Ak t je term a s je term, ktorý vznikne z t zámenou niektorých výskytov t_i zodpovedajúcimi termami s_i, potom $\vdash t = s$.*

2. *Nech formula A' vznikne z formuly A zámenou niektorých výskytov termov t_i zodpovedajúcimi termami s_i okrem prípadu, keď v t_i je premenná x, ktorá je súčasťou kvantifikácie $(\forall x)$ alebo $(\exists x)$. Potom $\vdash A \leftrightarrow A'$.*

Dôkaz: Prvé tvrdenie dokážeme indukciou na zložitosť termu t. V báze indukcie uvažujeme dva prípady. Ak t je premenná, tak tvrdenie vyplýva z axiómy (R1), ak t je niektorý z t_i, tak tvrdenie je vlastne jeden z predpokladov. V indukčnom kroku uvažujme t v tvare $t = f(u_1, \ldots, u_k)$, kde f je k-árny funkčný symbol a $u_1, \ldots, u_k$ sú termy, na ktoré sa vzťahuje indukčný ppredpoklad. Substitúciou nahrádzame tieto termy novými, pričom platí $\vdash u_j = u'_j$. Uvažujme formulu:

$$\vdash u_1 = u'_1 \to u_2 = u'_2 \to \ldots \to u_k = u'_k \to f(u_1, \ldots, u_k) = f(u'_1, \ldots, u'_k),$$

ktorá je inštanciou axiómy (R2) — k-násobným použitím pravidla MP dostaneme požadované tvrdenie.

Druhé tvrdenie: Keďže žiadne premenné, ktoré sú súčasťou kvantifikácie sa nenahrádzajú stačí uvažovať nahrádzanie iba v atomických podformulách. Dôkaz rozdelíme na 2 časti. Najprv uvažujme podformuly tvaru $P(u_1, \ldots, u_k)$. Inštancovaním axiómy (R3)

a k-násobným použitím pravidla MP dostaneme jednu implikáciu požadovanej ekvivalencie. S využitím vlastnosti symetrie sa rovnakým postupom dopracujeme aj k druhej implikácii. Nakoniec uvažujme podformuly tvaru $u_1 = u_2$. Vieme, že platí $\vdash u_1 = u_1'$ aj $\vdash u_2 = u_2'$. Pomocou vlastnosti tranzitívnosti dokážeme obe implikácie dokazovanej ekvivalencie. ♣

Veta: *Ak sú* $t, t_1, \ldots, t_n, s_1, \ldots, s_n$ *termy a ak* A *je formula, potom platí*

1. $\vdash t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to t[t_1 \ldots t_n] = t[s_1 \ldots s_n]$
2. $\vdash t_1 = s_1 \to t_2 = s_2 \to \ldots \to t_n = s_n \to (A(t_1 \ldots t_n) \leftrightarrow A(s_1 \ldots s_n))$

Ak naviac premenná x *nie je obsiahnutá v terme* t*, potom*

1. $\vdash A_x[t] \leftrightarrow (\forall x)(x = t \to A)$
2. $\vdash A_x[t] \leftrightarrow (\exists x)(x = t \wedge A)$

Dôkaz: Pokiaľ termy $t_1, \ldots, t_n, s_1, \ldots, s_n$ neobsahujú premenné, tak prvá časť vety vyplýva priamo z predchádzajúcej vety a vety o dedukcii. Ak tieto termy obsahujú premenné, nahradíme ich rôznymi konštantami, použijeme vetu o konštantách, vetu o dedukcii a predchádzajúcu vetu.
Teraz dokážeme druhú časť vety. Najprv uvažujme prvé tvrdenie.

$$\begin{array}{ll}
\vdash (\forall x)(x = t \to A) \to (t = t \to A_x[t]) & \text{(A4)} \\
\vdash (t = t) \to ((\forall x)(x = t \to A) \to A_x[t]) & \text{(VD)} \\
\vdash (\forall x)(x = t \to A) \to A_x[t] & \text{(R1, MP)}
\end{array}$$

$$\begin{array}{ll}
\vdash x = t \to (A \leftrightarrow A_x[t]) & \text{(predošlá veta)} \\
\vdash x = t \to (A_x[t] \to A) & \\
\vdash A_x[t] \to (x = t \to A) & \text{(VD)} \\
\vdash A_x[t] \to (\forall x)(x = t \to A) & \text{(GEN)}
\end{array}$$

Druhé tvrdenie dokážeme pomocou prvého nasledovne:

$$\begin{array}{l}
\vdash (\forall x)(x = t \to \neg A) \leftrightarrow \neg A_x[t] \\
\vdash \neg(\forall x)(x = t \to \neg A) \leftrightarrow \neg\neg A_x[t] \\
\vdash (\exists x)(x = t \to \neg A) \leftrightarrow A_x[t] \\
\vdash (\exists x)\neg(\neg(x = t) \vee \neg A) \leftrightarrow A_x[t] \\
\vdash (\exists x)((x = t) \wedge A) \leftrightarrow A_x[t]
\end{array}$$