Katedra informatiky fakulty Matematiky fyziky a informatiky
Univerzity Komenského

Kompendium matematickej logiky: teoretické základy pre databázy a sémantiku logických a ekvacionálnych programov

Ján Šturc

Bratislava, zima 2004

1 Úvod

Matematická informatika (*Computer science*) prekonala za krátky čas svojej existencie prudký vývin. V každej etape rozvoja sa opierala o inú matematickú disciplínu. Na počiatku (*v I. etape*) základne problémy boli problémy návrhu a prekladu programovacích jazykov. Základnou teoretickou disciplínou bola teória jazykov a automatov. Z matematického hľadiska ide o rozpracovanie a zjemnenie teórie algoritmov a prepisovacích systémov.
Ďalší vývin (*II. etapa*) zdôraznil význam analýzy programov z hľadiska ich výpočtovej zložitosti. Do tejto etapy môžme zaradiť aj časove o niečo posunuté problémy analýzy VLSI obvodov. Matematickým základom pre riešenie problémov druhej etapy bola a je kombinatorika a teória grafov.
V súčasnosti (*III. etapa*) za hlavné disciplíny môžme považovať rôzne metódy formálnych špecifikácii úloh a automatickej syntézy algoritmov. Sú to databázové a logické programovanie a „hra na sémantiku programov". Teoretickým základom pre tieto disciplíny je matematická logika, algebra a teória modelov.
Časové delenie asi nie je celkom výstižné, pretože všetky tri etapy sa vyvíjali paralelne. Časove sa rozdelil len dôraz na disciplíny v jednotlivých etapách.
Na nešťastie, informatika sa nevyvíja ako jedna z aplikácii matematiky, ale ako samostatná vedná disciplína. Znamená to, že matematické poznatky nie sú jednoducho aplikované, ale často znovu objavované v špecializovaných a modifikovaných podobách prispôsobených konkrétnej aplikácii. Navyše matematikov a logikov často zaujímali problémy, ktoré pre svoju nekonštruktívnu povahu presahujú možnosti aplikácii v informatike. Znamenaná to, že v súčasnosti máme k dispozícii niekoľko mierne sa odlišujúcich formalizmov a špecialistovi v jednej oblasti (napr. sémantike) je nepohodlné čítať práce z inej oblasti založené na spoločnej teórii (napr. logické programovanie).
Cieľom tejto práce je poskytnúť unifikovaný matematický základ pre disciplíny založené na predikátovom kalkule I. rádu a jeho modeloch. Snažíme sa pritom vychádzať skôr z formalizmu a označení používaných v matematických prácach než z formalizmov zavedených v jednotlivých disciplínach informatiky. Ako základ berieme predikátový kalkul I. rádu s rovnosťou ako logickým symbolom. V matematike aj v niektorých disciplinách matematiky sa uvažuje aj slabšia verzia predikátového kalkulu bez rovnosti. Rovnosť sa v takomto prípade dá zaviesť ako mimologický symbol, ale pojem konečnej axiomatizovateľnosti sa pri tom mení. Máme zato, že brať rovnosť ako logický symbol je prirodzenejšie hlavne v prípadoch, keď sa v ďalšom mienime obmedziť na konečne axiomatizovateľne teórie.
Často sa uvažujú rôzne modifikácie ako mnohosortový (*many sorted*) predikátový kalkul a predikátový kalkul s usporiadanými sortami (*order sorted*), pokiaľ neuvažujeme štruktúry obsahujúce len prázdne a jednoprvkové sorty sú takéto variácie nepodstatné. Taktiež sa niekedy uvažujú čiste algebraické jazyky (bez relačných symbolov), alebo čiste relačné jazyky (bez funkčných symbolov). Znovu tieto obmedzenia sú nepodstatné, ak máme v jazyku k dispozícii aspoň dve rôzne konštanty. Jednoducho povedané, pre väčsinu praktických aplikácii nie je potrebné rozlišovať medzi jednotlivými variantami predikátového kalkulu.

2 Logický jazyk

Jazykom budeme nazývať jazyk predikátového počtu I. rádu s rovnosťou. Ako každý jazyk je i logický jazyk popísaný gramatikou. Popíšeme si najskôr abecedu[1]:

Definícia 2.1

a: Terminálne symboly:

(i) *logické symboly:* $\forall, \exists, \neg, \wedge, \vee, \Rightarrow, \equiv, \ldots$ $a = b$ *(rovnosť).*

(ii) *spočitateľná množina premenných* $x_0, x_1, x_2, \ldots$.

(iii) *spočitateľná množina funkčných symbolov* F. *Pre funkčné symboly je definovaná funkcia* Σ_F *(signatúra),* $\Sigma_F : F \to nat$ *priraďujúca každému funkčnému symbolu* $f \in F$ *prirodzené číslo* $\Sigma_F(f)$, *ktoré nazývame aritou funkčného symbolu. Funkčné symboly arity* 0 *nazývame konštanty.*

(iv) *konečná množina predikátových symbolov* R. *Pre predikátové symboly je tiež definovaná arita – funkcia* $\Sigma_R : R \to nat^+$ *(do kladných prirodzených čísiel).*

b: Neterminálne symboly:

formula, atomická formula rovnosti, atomická formula nerovnosti, kvantifikátor, binárna logická spojka, term.

c: Počiatočný symbol je *formula.*

d: Pravidlá gramatiky:

(i) *Premenná alebo konštanta je term.*

(ii) *Ak* $t_1, t_2, \ldots t_n$ *sú termy a* f *je* n*-árny funkčný symbol, kde* $n > 1$. *Potom* $ft_1t_2 \ldots t_n$ *je term.*

(iii) *Ak* t_1 *a* t_2 *sú termy, potom* $= t_1t_2$ *je atomická formula rovnosti.*

(iv) *Ak* $t_1t_2, \ldots t_n$ *sú termy* r *je* n*-árny predikátový symbol, potom* $rt_1t_2 \ldots t_n$ *je atomická formula nerovnosti.*

(v) *Ak* φ *je formula, potom aj* $\neg\varphi$ *formula.*

(vi) *Binárna logická spojka je* $\wedge, \vee, \Rightarrow, \equiv$

(vi) *Ak* φ_1 *a* φ_2 *sú formuly a* $\oplus$ *je binárna logická spojka, potom aj* $\oplus\varphi_1\varphi_2$ *je formula.*

(vii) *Ak* x *je premenná, potom* $\forall x$ *a* $\exists x$ *sú kvantifikátory.*

(viii) *Ak* Q *je kvantifikátor a* φ *je formula, potom aj* $Q\varphi$ *je formula.*

[1]Abeceda logickéh jazyka sa uvažuje ako nekonenečná spočitateľná. Aby logický jazyk bol bezkontextovým jazykom nesmeli by sme považovať premenné a funkčné symboly za symboly abecedy, ale museli by sme generovať z elementárnych znakov (písmen a číslíc).

Ak v tejto definícii jazyka prvého rádu pridáme k pravidlám v bode *(vii)*, že aj $\forall f$ a $\exists f$, kde f je funkčný symbol a $\forall r$ a $\exists r$, kde r je relačný symbol sú kvantifikátory, definujeme *jazyk II. rádu.*
Z hľadiska syntaxe sa môžeme na logický jazyk pozerať ako na akýkoľvek programovací jazyk. V podstate sa dá popísať bezkontextovou gramatikou. Jediné kontextové podmienky sa týkajú arity. Túto podmienku však poznáme veľmi dobre (správny počet argumentov funkcie), prakticky sa rieši na základe tabuľky symbolov pomocou deklarácií, formálne sa dá popísať atribútovými gramatikami.

Veta 2.1 *Logický jazyk je jednoznačný.*

Dôkaz indukciou cez štruktúru formúl.

V ďalšom budeme označovať $Term_{\mathfrak{L}}$ množinu všetkých termov a $Form_{\mathfrak{L}}$ množinu všetkých formúl jazyka $\mathfrak{L}$. V prípade, že jazyk je z kontextu zrejmý, alebo nedôležitý, budeme index $\mathfrak{L}$ vynechávať.
Z formálneho hľadiska by mohla rušiť nekonečná abeceda, dá sa to však jednoducho riešiť zavedením identifikátorov premenných, funkčných symbolov a predikátových symbolov. Príslušnosť k druhu sa môže riešiť implicitne podľa prvého písmena (napr. x – premenná, f – funkčný symbol, r – predikátový symbol, a – konštanta), alebo pomocou deklarácií.
Logici často minimalizujú množinu logických symbolov (napr. na $\exists, \wedge, \neg, =$) a ostatné logické symboly chápu ako skratky za ekvivalentné formuly. Tento prístup zjednodušuje dôkazy indukciou cez štruktúru formúl.
Z hľadiska čitateľnosti je zasa výhodné používať notáciu so zátvorkami $ft_1 \dots t_n = f(t_1, t_2, \dots t_n)$ a infixová notácia po operátory a rovnosti $t_1 = t_2$ namiesto $= t_1 t_2$, resp. $a \vee b$ namiesto $\vee ab$. Budeme preto logický jazyk používať značne volne s bežnými konvenciami o zátvorkách a priorite operátorov. Gramatika tohto jazyka je síce trochu zložitejšia, ale veta 2.1 zostáva v platnosti pre všetky používané modifikácie logického jazyka.
Dôležitým pojmom v ďalšom je pojem volnej premennej. Označíme $FV(\varphi)$ množinu všetkých voľných premenných formule φ. Voľné premenné sú definované nasledujúcimi pravidlami:

(i) V atomickej formule (rovnosti alebo nerovnosti) sú všetky vyskytujúce sa premenenné voľné.

(ii) $FV(\neg\varphi) = FV(\varphi)$.

(iii) Pre každú binárnu logickú spojku $\oplus$ platí: $FV(\varphi \oplus \psi) = FV(\varphi) \cup FV(\psi)$.

(iv) Pre kvantifikátor Qx platí: $FV(Qx\varphi) = FV(\varphi) - \{x\}$.

Poznámka 1 *Viazanie premennej kvantifikátorom sa vzťahuje len na podstrom prislúchajúci uzlu kvantifikátoru. Ak sa vyskytuje vo formule tá istá premenná aj v iných častiach formuly, je voľná alebo viazaná podľa toho, či jej dominuje kvantifikátor*[2] *ju obsahujúci.*

[2]Ak by sme chceli použiť analogiu s programovacími jazykami, potom volné premenné sú globálne a viazané lokálne v podstrome prislúchajúcom kvantifikátoru.

Terminológia:
Formuly neobsahujúce voľné premenné nazývame uzavreté formuly alebo výroky (sentence). Atomické formuly nerovnosti budeme nazývať fakty. Hovoríme o jednoduchých faktoch (neobsahujú premenné), existenčných (uzavretých existenčným kvantifikátorom) a všeobecných (uzavretých univerzálnym kvantifikátorom) faktoch. Množinu formúl nazývame teóriou.

3 Interpretácie a modely

Definícia 3.1 *(Interpretácia, štruktúra pre jazyk $\mathfrak{L}$)*
Interpretáciou jazyka $\mathfrak{L}$ I. rádu rozumieme dvojicu $\mathfrak{I} = < D, \Phi >$, kde D je neprázdna množina, ktorá sa nazýva obor interpretácie a Φ je zobrazenie, ktoré n-árnemu funkčnému symbolu $f \in F$ priraďuje n-árnu funkciu $f : D^n \to D$ a každému n-árnemu relačnému (predikátovému) symbolu $r \in R$ reláciu $R \subseteq D^n$. Algebraickú štruktúru $\mathfrak{M} = < D, \mathfrak{F}, \mathfrak{R} >$, kde $\mathfrak{F} = \Phi(F)$ a $\mathfrak{R} = \Phi(R)$ nazývame štruktúrou[3]

Poznámka 2 *Pokiaľ to bude možné, budeme kvôli jednoduchosti niektoré jemnosti jazyka ignorovať. Budeme hovoriť o relácii r o funkcii f. Prísni formalisti to môžu považovať za skratky dlhších formulácií, relácia priradená predikátovému symbolu r, funkcia priradená funkčnému symbolu f. Celkom presne, relácia je trojica $< \mathfrak{D}, \mathfrak{C}, \mathfrak{R} >$, kde $\mathfrak{D}$ je množina oborov, $\mathfrak{C}$ množina kooborov a konečne $\mathfrak{R}$ je zmienená podmnožina kartézského súčinu oborov a kooborov, nazývaná aj graf relácie R. Matematicky presný pojem určuje: odkiaľ kam relácia zobrazuje, aj možné hodnoty*[4]*. Je zrejmé, že pri mnohých úvahách zanedbanie niektorých aspektov pojmu relácia nevadí, inokedy je však potrebná presnosť.*

Pojem interpretácie zaviedli logici (A. Tarski) na to, aby mohli definovať sémantiku logického jazyka.

Definícia 3.2 *(Pravdivosť formuly v interpretácii).*

(i) Uzavreté atomické formuly rovnosti $t_1 = t_2$ sú pravdivé v interpretácii $\mathfrak{M}$, ak po dosadení funkcie za funkčné symboly a vyhodnotení dostaneme v interpretácii $\mathfrak{M}$ identitu.

(ii) Uzavretá atomická formula nerovnosti $r(t_0, \dots t_n)$ je pravdivá, ak $t_0 = a_0, \dots, t_n = a_n$, $< a_0, \dots a_n > \in \ D^{n+1}$ $a < a_0, \dots, a_n > \in r$.

(iii) Pre atomické formuly s volnými premennými je pravdivosť formuly φ relativizovaná vzhľadom na nejakú substitúciu[5] *σ za premenné ($\sigma : Var \to D$). Formula $\varphi(x_1, \dots x_n)$ s volnými premennými $\{x_1, x_2, \dots x_n\}$ je pravdivá v interpretácii $\mathfrak{M}$ pri ohodnotení premenných σ ak $\varphi(\sigma(x_1), \dots \sigma(x_n))$ je pravdivá v interpretácii $\mathfrak{M}$.*

[3] Často aj táto štruktúra sa nazýva interpretáciou pre jazyk $\mathfrak{L}$. Či interpretácia je zobrazenie alebo výsledok zobrazenia rozumieme z kontextu.

[4] Podľa definície $\mathfrak{C}$ a $\mathfrak{D}$ môže byť relácia s tým istým grafom totálna alebo čiastočná, či spojitá alebo nespojitá.

[5] Túto substitúciu nazývame ohodnotením premenných.

(iv) Pravdivosť zložených formúl je definovaná indukciou cez štruktúru formúl $\neg\varphi$ je pravdivá ak nie je pravdivá φ; $\varphi_1 \vee \varphi_2$ je pravdivá ak je pravdivá aspoň jedna z formúl $\varphi_i (i \in \{1,2\})$; $\varphi_1 \wedge \varphi_2$ je pravdivá ak sú pravdivé obe formuly φ_1 aj φ_2; $\varphi_1 \Rightarrow \varphi_2$ je pravdivá, ak je nepravdivá φ_1 alebo ak je pravdivá φ_2 atď. Ak formuly obsahujú volné premenné znova je ich pravdivosť relativizovaná ohodnotením premenných.

(v) Formula $\exists x\varphi(x)$ je pravdivá pri danom ohodnotení ostatných premenných okrem x ak existuje také ohodnotenie premennej $s(x) = a$, že $\varphi(a)$ je pravdivá.

(vi) Formula $\forall x\varphi(x)$ je pravdivá, ak pri každom ohodnotení a premennej x je formula $\varphi(a)$ pravdivá v interpretácii $\mathfrak{M}$.

Poznámka 3 *Často hovoríme, že v interpretácii $\mathfrak{M}$ platí φ namiesto formula φ je pravdivá v interpretácii $\mathfrak{M}$. Zapisujeme $\mathfrak{M} \models \varphi$. Interpretáciu $\mathfrak{M}$ takú, že $\mathfrak{M} \models \varphi$ nazývame modelom formuly φ.*

Pojem modelu zovšeobecňujeme aj na teórie (množiny formúl). Hovoríme, že interpretácia $\mathfrak{M}$ je modelom teórie T, píšeme $\mathfrak{M} \models T$, ak pre každú formulu $\varphi \in T$ platí: $\mathfrak{M} \models \varphi$.
Môžeme si všimnúť, že nie každá formula musí mať model napr. $\varphi \wedge \neg\varphi$ pre ľubovoľnú formulu φ nemá model, lebo $\neg\varphi$ je splnené práve vtedy, keď nie je splnené φ. Na druhej strane niektoré formuly sú splnené v každej interpretácii napr. $\varphi \vee \neg\varphi$. Formuly, ktoré sú splnené v každej interpretácii nazývame tautológiami.

Definícia 3.3 *(dôsledok)*
Hovoríme, že formula φ je dôsledok teórie T, píšeme $T \models \varphi$, ak každý model T je aj modelom φ.

Nech T je teória. Označíme $\overline{T} = \{\varphi : T \models \varphi\}$. $\overline{T}$ je množina všetkých dôsledkov teórie T. Podobne, označíme $Mod(T)$ triedu všetkých modelov teórie T.
Trieda všetkých modelov nám takto definuje sémantiku teórie v jazykoch prvého rádu. Nevýhodou takejto definície je však skutočnosť, že keď chceme zistiť, či $T \models \varphi$ musíme overiť, či pre každý model $\mathfrak{M} \in Mod(T)$ je $\mathfrak{M} \models \varphi$.

4 Príklady teórii a modelov

Algebry len s unárnymi a nulárnymi operáciami asi nie sú z praktického hľadiska príliš zaujímavé, lebo neumožňujú vzájomné skladanie operácií.
Algebry len s unárnymi a nulárnymi operáciami sú z praktického hľadiska málo zaujímavé. Je to vyšetrovanie vlastností nejakej množiny funkcií.
Algebra $< G, \cdot >$ s jednou binárnou operáciou a prázdnou množinou axióm sa nazýva grupoid. Ak v ňom platí asociatívny zákon $\forall(a,b,c)\{a \cdot (b \cdot c) = (a \cdot b) \cdot c\}$ hovoríme o pologrupe.
Algebru $< G, \cdot, \lambda >$ typu $< 2, 0; >$ s axiomami: $\forall(a,b,c)\{a \cdot (b \cdot c) = (a \cdot b) \cdot c\}$ a $\forall(x)\{(x \cdot \lambda = x) \wedge (\lambda \cdot x = x)\}$ nazývame monoid. Konštanta (prvok G) určený nulárnou operáciou λ sa nazýva jednotkou. Algebraici často definujú monoid ako pologrupu, v ktorej platí: $\exists(e \in G)\forall(x \in G)\{(x \cdot e = x) \wedge (e \cdot x = x)\}$. Takéto

alternatívy v definíciach sú možné, pretože algebra nerozlišuje medzi izomorfnými štruktúrami.
Grupa je algebra $< G, \cdot, ^{-1}, 1 >$ typu $< 2, 1, 0; >$ s axiómami:
$\forall(a,b,c)\{a \cdot (b \cdot c) = (a \cdot b) \cdot c\}$, $\forall(x)\{(x \cdot x^{-1} = 1) \wedge (x^{-1} \cdot x = 1)\}$ a $\forall(x)\{x \cdot 1 = x\}$.
Takto definovanú grupu nazývame multiplikatívnou. Keď hovoríme o aditívnej grupe používame notáciu $< G, +, {}_u-, 0 >$, kde ${}_u-$ označuje unárne mínus.
Grupu v ktorej platí komutatívny zákon nazývame komutatívnou alebo Abelovou. Pre Abelove grupy používame obvykle aditívnu notáciu $< G, +, {}_u-, 0 >$ a charakterizujeme ich axiómami: $\forall(a,b,c)\{a + (b + c) = (a + b) + c\}$,
$\forall(a,b)\{a + b = b + a\}$, $\forall(x)\{x + {}_u - x = 0\}$ a $\forall(x)\{x + 0 = x\}$.

Okruh je algebra $< K, +, \cdot, {}_u-, 0 >$ typu $< 2, 2, 1, 0; >$ s axiómami:

1. $< K, +, {}_u-, 0 >$ je Abelova grupa,
2. $< K, \cdot >$ je pologrupa
3. a platia distributívne zákony: $x \cdot (y + z) = x \cdot y + x \cdot z$ a
   $(x + y) \cdot z = x \cdot z + y \cdot z$

CPO
Úplné zväzy
Boolové algebry
Cylindrické algebry
Relačná algebra

5 Formálne systémy

Definícia 5.1 *(formálny systém)*
Formálnym alebo deduktívnym systémom rozumieme trojicu $< \mathfrak{L}, \mathfrak{A}, \mathfrak{R} >$, *kde* $\mathfrak{L}$ *je jazyk* $\mathfrak{A}$ *je (rekurzívna) množina formúl prvky, ktorej nazývame axiomy a* $\mathfrak{R}$ *je množina (prepisovacích) pravidiel (rules of inference).*

Definícia 5.2 *(odvodenie, dôkaz)*
Nech $\mathfrak{S} =< \mathfrak{L}, \mathfrak{A}, \mathfrak{R} >$ *je formálny systém a* T *je teória v jazyku* $\mathfrak{L}$. *Hovoríme, že formula* φ *sa dá odvodiť z teórie* T, *píšeme* $T \vdash_{\mathfrak{S}} \varphi$, *ak existuje konečná postupnosť formúl* $\varphi_0, \varphi_1, \ldots, \varphi_n = \varphi$ *taká, že* $\varphi_i \in T \cup \mathfrak{A}$, *alebo* φ_i *sa dá odvodiť z* $\{\varphi_j : j < i\}$ *použitím nejakého pravidla z* $\mathfrak{R}$. *Postupnosť* $\varphi_0, \varphi_1, \ldots, \varphi_n$ *nazývame odvodením alebo dôkazom formuly* φ.

Ak je z kontextu jasný použitý formálny systém $\mathfrak{S}$ budeme v znaku odvodenia $\vdash$ vynechávať index $\mathfrak{S}$. Označíme $T^{*\mathfrak{S}} = \{\varphi : T \vdash \varphi\}$. Teóriu $T^{*\mathfrak{S}}$ nazývame deduktívnym uzáverom teórie T (vzhľadom na formálny systém $\mathfrak{S}$).
Pre predikátovú logiku I. rádu sa spravidla používajú dva formálne systémy Hilbertov, ktorý zdôrazňuje axiómy a Gentzenov, ktorý zdôrazňuje pravidlá. Uvedieme si axiómy a pravidlá odvodenia pre oba systémy.

5.1 A. Hilbertov systém $\mathfrak{H}$

Axiomy:

(1) Všetky tautologie

(2) Axiomy rovnosti

(i) $u = u$ (pre každú premennú alebo konštantu)

(ii) $u = v \Rightarrow\ v = u$ (symetria rovnosti)

(iii) $(u = v \wedge v = w) \Rightarrow\ u = w$ (tranzitívnosť rovnosti)

(iv) $(u_1 = v_1 \wedge \ldots \wedge u_n = v_n) \Rightarrow\ (R(u_1, \ldots, u_n) \Rightarrow\ R(v_1, \ldots, v_n))$
$(u_1 = v_1 \wedge \ldots \wedge u_n = v_n) \Rightarrow\ (f(u_1, \ldots u_n) = f(v_1, \ldots, v_n))$
(substitúcia rovného rovným)

(3) Všetky formuly tvaru:

(i) $(\forall v \varphi(v)) \Rightarrow\ \varphi(t)$

(ii) $\varphi(t) \Rightarrow\ \exists v \varphi(v)$,
kde t je ľubovolný výraz.

Pravidlá:

(1) $\dfrac{\varphi \Rightarrow \psi,\ \varphi}{\psi}$ (Modus ponens.)

Čítame: Z $\varphi\ \Rightarrow\ \psi$ a φ vyvoď ψ.

(2) Pravidlá zovšeobecnenia: Ak v nie je volná premenná vo φ, potom:

(i) $\dfrac{\varphi \Rightarrow\ \psi(v)}{\forall y \psi(y)}$.

(ii) $\dfrac{\psi(v) \Rightarrow\ \varphi}{\exists y \psi(y) \Rightarrow\ \varphi}$.

Hibertov systém je názorný, ľahko sa mu dá porozumieť, ale ťažko sa používa. Dôkazy, ak sú dosť dlhé, môžu byť značné „nelokálne a neštrukturované".

5.2 B. Gentzenov systém $\mathfrak{G}$

Základným pojmom pre Gentzenov systém je pojem sekventu. Sekventom nazývame dvojicu konečných množín formúl $< \Gamma, \Delta >$, ktorú zapisujeme $\Gamma \vdash \Delta$. Čítame z Γ vyplýva Δ, presnejšie z konjunkcie formúl v Γ vyplýva disjunkcia formúl v Δ.

Axiomy:

Všetky sekventy tvaru: (i) $\Gamma, \varphi\ \vdash\ \Delta, \varphi$
(ii) $\Gamma\ \vdash\ \Delta, (t = t)$ pre ľubovolný term t.

Pravidlá:

1. Pravidlá pre propozicionálne spojky

$$(\wedge\vdash)\quad \frac{\Gamma,\varphi,\psi\vdash\Delta}{\Gamma,(\varphi\wedge\psi)\vdash\Delta} \qquad (\vdash\wedge)\quad \frac{\Gamma\vdash\Delta,\varphi\quad\Gamma\vdash\Delta,\psi}{\Gamma\vdash\Delta,(\varphi\wedge\psi)}$$

$$(\vee\vdash)\quad \frac{\Gamma,\varphi\vdash\Delta\quad\Gamma,\psi\vdash\Delta}{\Gamma,(\varphi\vee\psi)\vdash\Delta} \qquad (\vdash\vee)\quad \frac{\Gamma\vdash\Delta,\varphi,\psi}{\Gamma\vdash\Delta,(\varphi\vee\psi)}$$

$$(\neg\vdash)\quad \frac{\Gamma\vdash\Delta,\varphi}{\Gamma,\neg\varphi\vdash\Delta} \qquad (\vdash\neg)\quad \frac{\Gamma,\varphi\vdash\Delta}{\Gamma\vdash\Delta,\neg\varphi}$$

$$(\Rightarrow\vdash)\quad \frac{\Gamma\vdash\Delta\,\varphi\quad\Gamma,\varphi\vdash\Delta}{\Gamma,(\varphi\Rightarrow\psi)\vdash\Delta} \qquad (\vdash\Rightarrow)\quad \frac{\Gamma,\varphi\vdash\Delta,\psi}{\Gamma\vdash\Delta,(\varphi\Rightarrow\psi)}$$

2. Pravidlo pre rovnosť. Ak E je formula $t_1 = t_2$ alebo $t_2 = t_1$, potom:

$$(E)\quad \frac{\Gamma,\varphi(t_1)\vdash\Delta,\psi(t_1)}{\Gamma,E,\varphi(t_2)\vdash\Delta,\psi(t_2)}$$

3. Pravidlá pre kvantifikátory:

$$(\forall\vdash)\quad \frac{\Gamma,\varphi(t)\vdash\Delta}{\Gamma,\forall v\varphi(v)\vdash\Delta} \qquad (\vdash\exists)\quad \frac{\Gamma\vdash\Delta,\varphi(t)}{\Gamma,\exists v\varphi(v)\vdash\Delta}$$

Nasledujúce dve pravidlá platia, ak v nie je volná premenná v $\Delta\ \vee\ \Gamma$:

$$(\vdash\forall)\quad \frac{\Gamma\vdash\Delta,\varphi(v)}{\Gamma\vdash\Delta,\forall y\varphi(y)} \qquad (\exists\vdash)\quad \frac{\Gamma,\varphi(v)\vdash\Delta}{\Gamma,\exists y\varphi(y)\vdash\Delta}$$

Často sa uvažuje Gentzenov systém $\mathfrak{G}^+$, ktorý sa od systému $\mathfrak{G}$ odlišuje tým, že obsahuje navyše pravidlo, ktoré je analógom „modus ponens" a nazýva sa cut.

$$\text{cut:}\ \frac{\Gamma,\varphi\vdash\Delta\quad\Gamma\vdash\Delta,\varphi}{\Gamma\vdash\Delta}$$

Veta 5.1

$$T^{*\mathfrak{H}} = T^{*\mathfrak{G}} = T^{*\mathfrak{G}^+} = \overline{T}$$

Dôkaz. Veta 5.1 zhrňuje Gentzenovú Hauptsatz o eliminácii cutov a Gödelovú vetu o úplnosti predikátového počtu (viď napr. Bairwise [1] kap. AI.). Gödelová veta nám hovorí, že formálne systémy $\mathfrak{G}, \mathfrak{G}^+$ a $\mathfrak{H}$ sú konzistentné a úplné vzhľadom na definíciu sémantiky formúl jazyka I. rádu prostredníctvom ich pravdivosti vo všetkých modeloch.

Dôsledok 5.2 *Ak T je rekuzívna teória (množina formúl), potom $\overline{T}$ je rekurzívne spočitateľná.*

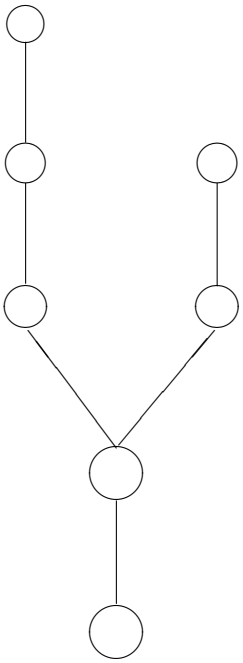
Dôkazy v Gentzenových systémoch majú stromovú štruktúru. Listy stromu sú axiómy alebo formuly teórie T.

Každý uzol má najviac dvoch synov a koreň stromu je dokazovaná formula. Navyše s každým uzlom je spojené práve jedno pravidlo, ktorého predpoklady sú v synoch a záver v menovanom uzle. Overovanie dôkazu sa tak stáva lokálnou mechanickou záležitosťou.

Príklad 4.1.
Ako príklad si uvedieme dôkaz tautológie výrokového počtu:
$(p \wedge \neg q \vee r) \rightarrow (p \vee r)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{p, \neg q \vdash p, r}{p \wedge \neg q \vdash p, r}\,(\wedge\vdash)}{p \wedge \neg q \vdash p \vee r}\,(\vdash\vee) \qquad \dfrac{r \vdash r, p}{r \vdash r \vee p}\,(\text{axiom})\ (\vdash\vee)}{p \wedge \neg q \vee \vdash r \vee p}\,(\vee\vdash)}{p \wedge \neg q \vee r \Rightarrow r \vee p}\,(\vdash\Rightarrow)$$

Strom dôkazu má štruktúru:



V informatike je však obvyklejšie kresliť stromy koreňom hore a tomu je prispôsobená aj terminológia. Takže uvedený dôkaz je typu zdola – nahor (forward chaining). Pre automatické dokazovanie je v dôkazoch zdola – nahor priveľa nedetermizmu — celý dôkaz je potrebné nejak uhádnuť a potom sa len overuje. Používa sa preto opačná metóda zhora – nadol (backward chaining), kde stačí v každom kroku uhádnuť „iba" použité pravidlo. Hľadanie takéhoto dôkazu je menej nedeterministické a v konečných systémoch (v systémoch s konečným množstvom axióm a pravidiel sa dá realizovať prehľadávaním s návratom (backtrack). Pozorný pozorovateľ si môže všimnúť, že dôkaz sa dá urobiť takým spôsobom, že sa dokazujú iba podformuly formuly, ktorú treba dokázať.

6 Význačné teórie a význačné modely

V tomto odstavci si uvedieme niekoľko v logike všeobecne známych skutočností, ktoré však budú mať význam v ďalšom keď sa na teórie budeme pozerať ako na programy a na dôkazy ako na výpočty.

Definícia 6.1 *(Bezosporná teória)*
Hovoríme, že teória T je bezosporná[6] *(consistent) vzhľadom k formálnemu systému $\mathfrak{S} =< \mathfrak{L}, \mathfrak{A}, \mathfrak{R} >$, ak $T^{*\mathfrak{S}} \subset Form_S$. Teóriu T bezospornú vzhľadom k niektorému zo systémov $\mathfrak{G}^+, \mathfrak{H}, \mathfrak{G}$ budeme nazývať jednoducho bezospornou.*

Veta 6.1 *Nasledujúce tvrdenia sú ekvivalentné:*

(i) T *je bezosporná*

(ii) T *má (neprázdny) model*

(iii) Neexistuje formula φ *taká, že* $T \vdash \varphi$ *a súčasne* $T \vdash \neg\varphi$.

Definícia 6.2 *(formula konzistentná s teóriou)*
Budeme hovoriť, že formula φ je konzistentná s teóriou T ak $\neg\varphi \notin T^*$ (alebo ekvivalentné $T \nvdash \neg\varphi$).

Na druhej strane, sa ľahko presvedčíme, že pre množinu $\mathbf{Th}(\mathfrak{M})$ formúl pravdivých v modeli $\mathfrak{M}$ platí, že buď $\varphi \in \mathbf{Th}(\mathfrak{M})$ alebo $\neg\varphi \in \mathbf{Th}(\mathfrak{M})$. Týmto je motivovaná nasledujúca definícia.

Definícia 6.3 *(úplná teória)*
Hovoríme, že teória T je úplná vzhľadom k formálnemu systému $\mathfrak{S} =< \mathfrak{L}, \mathfrak{A}, \mathfrak{R} >$, ak pre každú formulu $\varphi \in \mathbf{Form}_{\mathfrak{L}}$ platí, buď $\varphi \in T^{*\mathfrak{S}}$ alebo $\neg\varphi \in T^{*\mathfrak{S}}$. Teóriu nazývame jednoducho úplnou ak je úplná vzhľadom k nejakému systému logiky I. rádu ($\mathfrak{H}$, $\mathfrak{G}^+$, $\mathfrak{G}$).

Pojem úplnej teórie sme zaviedli syntakticky. Jeho sémantickú charakterizáciu udáva nasledujúca lema.

Lema 6.2 *Pre bezospornú (neprotirečivú) teóriu T sú nasledujúce tvrdenia ekvivalentné:*

(i) T *je úplná teória.*

(ii) Každé dva modely teórie T *sú elementárne ekvivalentné.*

(iii) Pre každý model $\mathfrak{M}$ *teórie* T *je* $T = \mathbf{Th}(\mathfrak{M})$.

Úplné teórie sú teórie charakterizujúce množiny všetkých platiacich formúl v nejakej konkrétnej štruktúre $\mathfrak{M}$.

[6] Často sa hovorí aj neprotirečivá.

Definícia 6.4 *Teóriu T_2 nazývame rozšírením (extension) teórie T_1, ak $\mathfrak{L}_{T_1} \subseteq \mathfrak{L}_{T_2}$ a $T_1 \subseteq T_2$. Ak navyše teórie T_1 a T_2 sú teórie toho istého jazyka $\mathfrak{L}$, hovoríme o elementárnom rozšírení.*

Veta 6.3 *(Lindenbaum)*
Ak T je bezosporná teória, potom existuje úplná teória T', ktorá je elemntárnym rozšírením teórie T.

Definícia 6.5 *(rekurzívne axiomatizovateľná, rozhodnuteľná teória)*
Hovoríme, že teória T je rekurzívne axiomatizovateľná, ak existuje rekurzívna teória T' taká, že $T' = T$.
Hovoríme, že teória T je rozhodnuteľná, ak T je rekurzívna.

Budeme uvažovať konkrétnu teóriu *PA* (Peano's arithmetic). Jazyk tejto teórie obsahuje konštantu 0 unárny funkčný symbol s (succesor) a dva binárne funkčné symboly + (add), . (multiply), ktoré v súlade so zvyklosťami budeme používať ako infixové.
PA pozostáva z nasledujúcich formúl (axióm):

(i) $\forall x \forall y(s(x) = s(y)) \Rightarrow x = y$

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

(iii) $\forall x(x + 0 = x)$

(iv) $\forall x V y(x + s(y)) = s(x + y))$

(v) $\forall x(x.0 = 0)$

(vi) $\forall x \forall y(x.s(y) = x.y + y)$

(vii) Všetkých uzavretých formúl tvaru:
$\forall z_1, \ldots \forall z_n \forall x((F(0, z_1, \ldots, z_n) \wedge \forall y((F(y, z_1, \ldots z_n) \Rightarrow F(s(y), z_1, \ldots, z_n))) \Rightarrow F(x, z_1, \ldots, z_n))$, kde F je ľubovoľná formula taká, že $FV(F) \subseteq \{x, z_1, \ldots, z_n\}$.

Definícia 6.6 *Teóriu T takú, že $PA \subseteq T$, nazývame ω-bezospornou (ω-consistent), ak pre každú formulu $F(x)$, $\neg F(n)$ pre všetky $n = 0, 1, 2, \ldots$ implikuje $T \nvdash \exists x F(x)$.*

Z ω-bezospornosti vyplýva bezospornosť, opak neplatí.
Nasledujúce dve vety, patriace dnes už k matematickému folklóru, dokázané Gödelom [1930] hovoria, že väčšina zaujímavých teórií je neúplná.

Veta 6.4 *(Prvá veta o neúplnosti)*
Nech T je rekurzívne axiomatizovateľná teória a nech $PA \subseteq T$. Potom existuje formula φ, ktorá tvrdí vlastnú nedokázateľnosť a platí:

(i) Ak T je bezosporná, potom $T \nvdash \varphi$.

(ii) Ak T je ω-bezosporná, potom $T \nvdash \neg\varphi$.

Veta 6.5 *(Druhá veta o neúplnosti)*
Nech T je bezosporná teória a nech $PA \subseteq T$. Potom $T \nvdash Con_T$, kde Con_T je výrok tvrdiaci, že T je bezosporná (Pre PA je to $\neg(\vdash\ 0 = 1$)).

Dôkazy týchto viet sa zakladajú na Gödelovom číslovaní formúl, dôkazov a diagonalizačnom argumente.
Interpretácie jazyka I. rádu a modely teórií prvého rádu sú algebraické štruktúry. Pozostávajú z nosiča (carrier), čo je obor interpretácií, operácií či funkcií a relácií. Môžeme teda hovoriť o homomorfizme a izomorfizme interpretácii či modelov.

Definícia 6.7 *(Homomorfizmus, izomorfizmus, automorfizmus)*
Nech $\mathfrak{A} = (A, F, R)$ a $\mathfrak{B} = (B, G, S)$ sú dve štruktúry zobrazenie $h : \mathfrak{A} \to \mathfrak{B}$ nazývame homomorfizmom z $\mathfrak{A}$ do $\mathfrak{B}$ ak pre každký funkčný symbol $f \subseteq F$ a každý prvok $a \in A^n$, kde n je arita f resp. r, platí $h(f(a)) \equiv h(f)(h(a))$ a pre každý relačný symbol $r \in R$ platí $r(a) \to h(r)(h(a))$. Ak je h navyše jednoznačné zobrazenie hovoríme o izomorfizme. Izomorfizmus $i : \mathfrak{A} \to \mathfrak{A}$ nazývame automorfizmus. Skutočnosť, že $\mathfrak{A}$ je izomorfné $\mathfrak{B}$, zapisujeme $\mathfrak{A} \cong \mathfrak{B}$.

V logike sa často musíme zaoberať modelmi jednej teórie.

Definícia 6.8 *(Elementárne ekvivalentné štruktúry, podštruktúra, elementárne vnorenie)*
Hovoríme, že štruktúry $\mathfrak{A}$ a $\mathfrak{B}$ sú elementárne ekvivalentné, píšeme $\mathfrak{A} \equiv \mathfrak{B}$, ak $\mathbf{Th}(\mathfrak{A}) \equiv \mathbf{Th}(\mathfrak{B})$.
Hovoríme, že štruktúra $\mathfrak{A} = (A, F, R)$ je podštruktúra štruktúry $\mathfrak{B} = (B, G, S)$, ak $A \subseteq B$ a každému $g \in G$ zodpovedá nejaké $f \in F$ také, že $g = g|A$ (g zúžené na A) a každé $s \in S$ nejaké $r = s|A$ a navyše pre každú formulu φ a každé ohodnotenie premenných t v $\mathfrak{A}$ platí: $\mathfrak{A} \models \varphi[t]$ práve vtedy, ak $\mathfrak{B} \models \varphi[t]$. Fakt $\mathfrak{A}$ je podštruktúrou $\mathfrak{B}$ zapisujeme $\mathfrak{A} < \mathfrak{B}$.
Ak $\mathfrak{A} < \mathfrak{B}$ a $f : \mathfrak{A} \to \mathfrak{B}$ je injektívne zobrazenie také, že $\mathfrak{A} \models \varphi[t]$ práve vtedy, ak $\mathfrak{B} \models \varphi[f(t)]$. Potom zobrazenie f nazývame vložením $\mathfrak{A}$ do $\mathfrak{B}$, píšeme $f : \mathfrak{A} \to_< \mathfrak{B}$.

Lema 6.6 $f : \mathfrak{A} \cong \mathfrak{B} \Rightarrow\ f : \mathfrak{A} \to_< \mathfrak{B} \Rightarrow\ \mathfrak{A} \equiv \mathfrak{B}$.

Veta 6.7 *(Grätzer)*
Nech $\mathfrak{A}$ je nekonečná štruktúra spočítateľnej signatúry ($|F| + |R| \leq \aleph_0$). Potom $\mathfrak{A}$ obsahuje spočítateľnú elementárne ekvivalentnú podštruktúru $\mathfrak{B}$. ($\mathfrak{B} < \mathfrak{A}$ a $\mathfrak{A} \equiv \mathfrak{B}$).

Význam vety 6.7 spočíva v tom, že hoci logická sémantika jazykov I. rádu je definovaná cez triedu všetkých modelov, pre jej skúmanie sa nám stačí obmedziť na spočítateľné modely. Neznamená to, že treba odmietať modely väčšej kardinality tam, kde naša matematická intuícia lepšie pracuje s týmito modelmi, ale znamená to, že pri skúmaní pravdivosti formúl sa môžeme bez veľkých modelov celkom dobre zaobísť.

Definícia 6.9 *(definovateľnosť)*
Nech $\mathfrak{A} = (A, F, R)$ interpretácia jazyka $\mathfrak{L}$ hovoríme, že prvok $a \in A$

(i) je definovateľný v $\mathfrak{A}$, ak existuje formula φ s jednou volnou premennou taká, že $\mathfrak{A} \models \varphi(a)$ a ak $A \models \varphi(a)$ a $\mathfrak{A} \models \varphi(b)$ pre nejaké $b \in A$. Potom $\mathfrak{A} \models a = b$.

(ii) je definovateľný v teórii T, ak existuje formula φ s jednou volnou premennou taká, že $T \vdash \varphi(a)$ a $T \vdash \forall x V y \varphi(x) \wedge \varphi(y) \vdash x = y$.

(iii) n-árna relácia $M \subseteq A^n$ je definovateľná, ak existuje formula $\varphi(x_1, \ldots, x_n)$ s množinou voľných premenných $\{x_1, \ldots, x_n\}$ taká, že:
$$M = \{< a_1, \ldots, a_n >: \mathfrak{A} \models \varphi(a_1, \ldots, a_n)\}.$$

(iv) n-árna funkcia $f(x_1, \ldots, x_n)$ je definovateľná, ak existuje formula $\varphi(x_1, \ldots, x_n, y)$ s voľnými premennými $x_1, \ldots, x_n, y$; a graf funkcie f je definovateľný funkciou φ ako množina t.j. $f(a_1, \ldots, a_n) = a$ práve vtedy, ak $\mathfrak{A} \models \varphi(a_1, \ldots, a_n, a)$ a $\mathfrak{A} \models \forall x_1 \ldots \forall x_n \forall y_1 \forall y_2 \varphi(x_1, \ldots, x_n, y_1) \wedge \varphi(x_1, \ldots, x_n, y_2) \Rightarrow y_1 = y_2$.

Definícia 6.10 *(Kánonická interpretácia, kánonický model)*
Štruktúru $\mathfrak{A} = (A, F, R)$ nazývame kánonickou, ak každý prvok $a \in A$ je definovateľný nejakou konjunktívnou formulou. Konjunktívnou formulou rozumieme formulu, ktorá je alebo atomická alebo konjunkcia atomických formúl alebo konjunkciou atomických formúl predchádzanú nejakou množinou existenčných kvantifikátorov.

Kánonické modely sú modely, ktoré sa dajú syntakticky konštruovať z termov jazyka. Obvykle $x = t$ je atomická formula, ktorá definuje prvok $a \in A$ zodpovedajúci term t vo volnej term - algebre. Táto konštrukcia je v algebraických štruktúrach úspešná. Zložitejšie definície potrebujeme, ak naše štruktúry nemajú dostatok termov.

Príklad. 5.1
Uvažujme jazyk $\mathfrak{L}_1$ s konštantou 0 a unárnou funkciou s. Termy v tomto jazyku sú: $0, s(0), s(s(0)), \ldots, s(s(\ldots s(0)\ldots), \ldots$.
Uvažujme jazyk $\mathfrak{L}_2$ s konštantou 0 a binárnym relačným symbolom *succ*. V tomto jazyku existuje jediný term 0. Ak však pridáme axióm $\forall x \forall y \forall z succ(x, y) \wedge succ(x, z) \Rightarrow y = z$, sa v oboch jazykoch dá vyjadriť to isté, ale prvky nosiča štruktúry sa nedajú vyjadriť ako termy. Treba ich postupne definovať formulami:
$0, succ(0, x), \exists x_1 succ(0, x_1) \wedge succ(x_1, x)$,
$\exists x_1 \exists x_2 succ(0, x_1) \wedge succ(x_1, x_2) \wedge succ(x_2, x), \ldots$.
Nasledujúca veta je našou modifikáciou známej Herbrandovej vety.

Veta 6.8 *Ku každej štruktúre a pre spočitateľný jazyk $\mathfrak{L}$ existuje elementárna ekvivalentná kánonická štruktúra.*

Dôkaz. Podľa vety 6.5 ku každej štruktúre $\mathfrak{A}$ existuje spočitateľná štruktúra $\mathfrak{B} < \mathfrak{A}$. Vezme teóriu $\mathbf{Th}(B)$. Konjunktívne formuly si usporiadame podľa štruktúry. Ak $\mathbf{Th}(B)$ sa dá odvodiť nejaká konjunktívna formula $\exists x \varphi(x)$ podľa vety 5.1 musí byť φ splnená pre nejaké termy $t_1, t_2, \ldots, t_k$. Ak $\mathfrak{B} \models \exists x \varphi(x, y)$ a nevieme nájsť term t. $\mathfrak{B} \models \exists x \varphi(x, t)$ vezmeme formulu $\exists x \varphi(x, y)$, ako definíciu ďalšieho prvku nosiča. Pretože formuly sú usporiadané nemôže sa stať, že nejaká ďalšia definícia splní túto definíciu druhý krát (subformula property).
Vo výskume logiky ako programovacieho a špecifikačného jazyka hrajú významnú úlohu niektoré „konkrétne" malé modely. Väčšinou tieto modely skúmame vzhľadom na nejakú triedu modelov obvykle na triedu $\mathbf{Mod}(T)$ všetkých modelov teórie T.

Definícia 6.11 *(Iniciálny model)*
Nech $\mathfrak{K}$ je trieda štruktúr jazyka $\mathfrak{L}$. Štruktúru $\mathfrak{A}$ nazývame iniciálnou v triede $\mathfrak{K}$, ak pre každú štruktúru $\mathfrak{B} \in \mathfrak{K}$ existuje práve jeden homomorfizmus $h_{\mathfrak{B}} : \mathfrak{A} \to \mathfrak{B}$.

Všeobecným pozorovaním je nasleldujúca lema.

Lema 6.9 *(Makowsky 1987) Ak existuje netriviálny automorfizmus $f : \mathfrak{A} \to \mathfrak{A}$, potom $\mathfrak{A}$ nemôže byť iniciálna štruktúra.*

Veta 6.10 *(Makowsky 1987)*
Nech T je teória v jazyku I. rádu a nech $\mathfrak{A}$ je iniciálny model v $\mathbf{Mod}(T)$. Potom $\mathfrak{A}$ je kánonický model.

Definícia 6.12 *(Prvomodel (prime model))*
Nech $\mathfrak{K}$ je trieda modelov. $\mathfrak{A} \in \mathfrak{K}$ sa nazýva prvomodel pre $\mathfrak{K}$, ak pre každé $\mathfrak{B} \in \mathfrak{K}$ existuje vloženie $f : \mathfrak{A} \to_< \mathfrak{B}$.

7 Konštrukcia modelov

Skolem Henkinová metóda
Forcing
Tarského veta o pevnom bode
Ekvacionálne teórie: Variety a quasivariety.

Referencie

[1] J. Bairwise: Handbook of mathematical logic. North-Holland, 1977

[2] S. Burris and H. P. Sankappanavar: A course in universal algebra, Springer-Verlag, 1981 *(Milenium edition http://www.thoralf.uwaterloo.ca/htdocs/UALG/univ-algebra.pdf)*

[3] Ю. Л. Ершов: Теория нумерации. Наука 1997

[4] G. Grätzer: Universal algebra. Second edition. Springer-Verlag, 1979

[5] J. W. Lloyd: Foundation of logic programming. Springer-Verlag, 1984

[6] D. W. Loveland: Automated theorem proving: A logical basis. North-Holland, 1978

[7] Мальцев: Алгебраические структури. Москва 1966

[8] J. A. Makowsky: Why Horn formulas matter in computer science: Initial structures and generic examples. *JCSS 34 (1987),* 266 - 292

[9] J. D. Monk: Mathematical logic. Springer-Verlag 1976

[10] P. Padawitz: Computing in Horn clause theories. Springer-Verlag, 1988

[11] F. P. Preparata, R. T. Yeh: Úvod do teórie diskrétnych matematických štruktúr. Alfa Bratislava, 1982

[12] M. Schmidt-Schauß: Computational aspects of an order-sorted logic with term declarations. LNCS 395, Springer-Verlag, 1989

[13] J. R. Shoenfield: Mathematical logic. Addison-Wesley, 1967