3.4. Formální prostředky automatizace dokazování teorémů

Uvedenou problematikou se budeme zabývat pouze v rámci jazyka a kalkulu predikátové logiky prvého řádu. Cílem této podkapitoly je zejména procvičit obraty formalizace indukované používáním Robinsonova resolučního principu a vytvořit tak základní podmínky pro pochopení a snadné zvládnutí jazyků typu Prolog.

Nejprve sjednotíme názvosloví, které budeme používat v rámci této podkapitoly :

<u>Abecedu jazyka predikátů</u> tvoří : předmětové konstanty (a,b,...) , predikátové konstanty (P,Q,...) , funkční konstanty (f,g,...) , předmětové proměnné (x,y,...) a znaky pro logické operace a vztahy (konjunkce "∧" nebo "ET", disjunkce " ∨ " nebo "VEL" , negace "¬ " , implikace " => " , existenční kvantifikátor "∃ " , univerzální kvantifikátor " ∀ ", oddělovače "(",",", ")" a vztah odvoditelnosti (dokázatelnosti) "⊢ "). ∎

<u>Formační gramatika jazyka predikátů nad abecedou A</u> :

<u>Def.3.4.1.</u>: Termem v jazyce predikátů rozumíme :

1. Předmětové proměnné a předmětové konstanty.
2. Výrazy typu $f(t_1,\dots,t_n)$, kde f je funkční konstanta a $t_1,\dots,t_n$ jsou termy.

(Jiné termy než 1. a 2. neexistují.) ∎

<u>Def.3.4.2.</u>: Atomickou formulí jazyka predikátů rozumíme výraz $P(t_1,\dots t_n)$, kde P je predikátová konstanta a $t_1,\dots,t_n$ jsou termy.
<u>Formulí</u> jazyka predikátů pak rozumíme :

1. Atomickou formuli .
2. Výrazy : $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$, kde A,B jsou formule.
3. Výrazy : $\exists x\, A$, $\forall x\, A$,kde x je předmětová proměnná a A je formule.

(Jiné formule než 1.,2.,3. - nejsou.) ∎

Další pojmy důležité v technice resolučního dokazování uvedeme již volně :

Atomické formule a jejich negace nazýváme souhrně <u>literály</u> .
Disjunkci literálů nazýváme <u>složkou</u> . <u>Prenexní forma formule</u> obsahuje všechny kvantifikátory před zbývající částí formule. Zvláštním typem prenexní verze formule je <u>Skolemova normální forma</u> , která je konjunkcí složek bez existencionálních kvantifikátorů. Zvláštním druhem složky je tzv. <u>Hornova klausule</u>. Obsahuje nejvýše jediný pozitivní literál.

<u>Příklad 24.3.</u>:

Přepis do tvaru Hornovy klausule : $A_1,\dots,A_n$, B - literály,

$$((A_1 \text{ ET } A_2 \dots \text{ ET } A_n) \Rightarrow B) \Leftrightarrow (B \text{ VEL } \neg A_1 \text{ VEL } \neg A_2 \dots \text{ VEL } \neg A_n).$$

<u>Odstraňování existenčních kvantifikátorů</u> zaváděním Skolemových funkcí :

$$a)\ \exists x\ P(x) \rightsquigarrow P(a) \quad , \tag{18.3}$$

$$b)\ \exists x \forall y\ P(x,y) \rightsquigarrow \forall y\ P(a,y) \quad , \tag{19.3}$$

$$c)\ \forall y \exists x\ P(x,y) \rightsquigarrow \forall y\ P(f(y),y) \quad , \tag{20.3}$$

kde x,y jsou předmětové proměnné , a je předmětová konstanta , f je funkční konstanta a P je predikátová konstanta .∎

<u>Příklad 25.3.</u>:

Odstraňte existenční kvantifikátory z následujících formulí a převeďte je do Skolemovy normální formy s Hornovými klausulemi :

$$(\exists x \forall y\ (P(x,y) \Rightarrow Q(x))\ \mathrm{ET}\ (\forall x \exists y\ (R(x) \Rightarrow S(x,y))\ \mathrm{ET}\ Q_1(a)\ \mathrm{ET} (\exists x \exists y\ D(x,y)) \ .$$

$$(\forall y\ (Q(b)\ \mathrm{VEL}\ \neg P(b,y))\ \mathrm{ET}\ (\forall x\ (S(x,f(x))\ \mathrm{VEL}\ \neg R(x))\ \mathrm{ET}\ Q_1(a)\ \mathrm{ET}\ D(c,d) \ ,$$

$$\forall x \forall y\ ((Q(b)\ \mathrm{VEL}\ \neg P(b,y))\mathrm{ET}(S(x,f(x))\ \mathrm{VEL}\ \neg R(x))\mathrm{ET}(Q_1(a))\mathrm{ET}(D(c,d))) \ .$$

<u>Substituce do literálů</u> :

Za proměnné v literálech je povoleno substituovat termy.Ale nikoli libovolně.Skolemovské úpravy (např. ty,které jsme použili v příkladu 25.3.) vyčerpávají pouze část možností při substitucích. Povšimneme si zatím pouze toho,co je nutné dodržet (co je výhodné budeme studovat dále). Důležité je určit,které individuální předmětové konstanty je možno dosazovat v systémech klausulí za které proměnné a dále pak omezit rozsah množiny termů pro substituce.

Pro prvou otázku připomeneme znalosti z používání sémantických rozkladových tabulek :

- za univerzálně kvantifikovanou proměnnou je možno substituovat libovolný term ,
- za různé existenčně kvantifikované proměnné v systému složek (literálů) dosazujeme obecně různé individuální předmětové konstanty nebo je při skolemovských úpravách nahrazujeme v literálech termy s odlišnými funkčními konstantami ,
- v posloupnosti substitucí prováděných na systému složek (literálů) respektujeme toto pravidlo : za existenčně kvantifikovanou proměnnou je nutno dosadit předmětovou konstantu,která se ještě v předchozích literálech nevyskytla,nebo ji nahradit termem s funkční konstantou,která se ještě v předchozích literálech nevyskytla .

Tyto uvedené předpisy jsou zcela jistě jazykově velmi složité a není možno je efektivně lépe precizovat.Dříve,než postoupíme dále , vysvětlíme jejich význam a platnost příkladem.

Příklad 26.3.:

Rozbor substitucí v příkladu 25.3.: předložený výraz je konjunkce formulí. Je tedy "jakoby" libovolné,kterou substituci začneme provádět nejprve. Ovšem vzhledem k tomu,že odlišnost dosazovaných termů závisí také na "již použitých" termech (pokud jde o konstanty) ,nutno chápat předloženou formuli tak,že už (možná) nějaká substituce provedena byla (a my to nevíme).To je důvod,proč si povšimneme formule $Q_1(a)$.Protože jiná formule tohoto typu již v předložené konjunkci formulí není,můžeme začít provádět substituce nadále libovolně - např. zleva doprava.Při prvé skolemovské úpravě je tedy nutno použít při dosazení za proměnnou x jinou konstantu než a ! (Doufáme,že nikoho nenapadne trvat na neurčitosti ve třetím uvedeném předpisu a " v literálu P(x,y) dosazovat za x jinou konstantu,než v literálu Q(x)."Nelze.Patří k témuž oboru kvantifikace.) Důležité je ještě zdůraznit,že i v témže literálu je nutno pro odlišné proměnné použít odlišné konstanty.Proto - D(c,d).

Je nesporné,že substitucemi do literálů získáváme opět literály.Pro odlišení vztahu literálů k proběhnuvším substitucím se někdy používá pojem instance.

Instancí literálu rozumíme literál vzniklý substitucí.
Základní instancí literálu je pak literál,který již neobsahuje proměnné.

Příklad 27.3.:

Instancí literálu S(x,y) je literál S(x,f(x)). Základní instancí literálu D(x,y) je literál D(c,d).

Uvažujeme nyní situaci,kdy množina složek je po skolemovských úpravách a systém formulí je ve Skolemově normální formě.Předpokládejme,že některé literály obsahují proměnné.Obecně lze nyní vytvářet libovolně složité termy a dosazovat je do literálů, aniž bychom porušili uvedené předpisy substitucí.Pokud ovšem systém literálů obsahuje alespoň jedinou funkční konstantu,je z definice termu zřejmé,že množina možných substituent je spočetně nekonečná. V tomto okamžiku je již vhodné gramatické aspekty výstavby jazykových útvarů predikátové logiky prvého řádu opustit a věnovat se jejich uplatnění v kalkulu predikátové logiky 1.řádu (odkud také přijdou efektivní hlediska omezení využití obecně nekonečné množiny termů).

Cílem aplikace kalkulu predikátů 1.řádu je zprostředkovávat přenos hodnot pravdivosti na systémech formulí.Toho se dosahuje pomocí nejrůznějších systémů odvozovacích pravidel.Vzhledem k nárokům na počítačovou realizaci procesů dokazování bylo výhodné redukovat množinu odvozovacích pravidel na jediné.To umožňuje Robinsonův resoluční princip,za předpokladu, že množina formulí k důkazu jejich konsistentnosti je určitým způsobem předzpracována.Jedním z vhodných způsobů předzpracování je převedení systému formulí do Skolemovy normální formy.Robinsonův resoluční princip pak spočívá v opakovaném provádění dvou následujících kroků až do zpracování "celé" Skolemovy normální formy:

1.Minimální substituce , 2. Aplikace pravidla: $(A \vee B) ET (\neg A \vee C) \Rightarrow (B \vee C)$,

(21.3)

Minimální substituce je vztažena vždy k některým dvěma složkám.Cílem je nalezení takových termů,které po substituci za příslušné proměnné umožní uplatnit na tyto složky uvedené pravidlo.Je zřejmé,že po uplatnění pravidla získáme novou složku , které již neobsahuje literály A , $\neg A$. Tato nová složka se nazývá <u>resolventa</u> , ($r(s_1,s_2)$).
Důkaz konsistentnosti množiny formulí se pomocí Robinsonova resolučního principu převádí na postupné uplatňování kroků 1. a 2 . až do situace,kdy se podaří separovat prázdnou resolventu, tj.

$$r(s_1,s_2) = (A \wedge \neg A) \Rightarrow \emptyset \,, \tag{22.3}$$

na množině výchozích složek Γ_s.(Množina výchozích složek vzniká z množiny formulí (axiómů) rozšířených o negaci formule,kterou máme dokázat, po převedení do Skolemovy normální formy.Důkaz konsistentnosti množiny axiómů s dokazovanou formulí se převádí na důkaz nesplnitelnosti množiny výchozích složek.)

<u>Postup dokazování pomocí Robinsonova resolučního principu</u>

Je dána množina formulí axiómů Γ (Γ konsistentní) a formule A , pro kterou se hledá důkaz $\Gamma \vdash A$.(Γ ani A neobsahují volné proměnné.)

1. Sestrojíme množinu $(\Gamma \cup \{\neg A\}) = \Gamma_A$.
2. Každou formuli typu $B \Rightarrow C$ v Γ_A nahradíme formulí typu $\neg B \vee C$.
3. Každou formuli upravíme tak,aby negace se vztahovaly jen na atomické formule (formujeme literály).
4. Přejmenujeme proměnné (pokud je nutno) tak,aby žádné dvě uzavřené formule neobsahovaly stejné proměnné .
5. Odstraníme existenční kvantifikátory z formulí pomocí skolemovských úprav při respektování předpisů o korektních substitucích do literálů.
6. Všechny formule z Γ_A převedeme do Skolemovy normální formy s předponou,ve které jsou všechny v Γ_A univerzálně kvantifikované proměnné (a $\forall$- kvantifikátory). Tyto předpony je nyní možno vypustit a jednotlivé složky vázané konjunkcemi zapsat do sloupce pod sebe.Tímto jsme získali vhodný tvar výchozí množiny složek Γ_s.
7. Na množině Γ_s hledáme minimální substituce do proměnných a uplatňujeme resoluční pravidlo.Vzniklé resolventy připojujeme do Γ_s k dalšímu zpracování jako rovnocenné složky.Tento postup se opakuje až do separace prázdné resolventy. ∎

<u>Příklad 28.3.</u>:

Je dána množina $\Gamma = \{ (\forall x \forall y\ (P(x,y) \vee (\exists x \exists y\ P(x,y))))$,

$((\exists y \forall x\ R(y,x)) \vee (\forall x \forall y\ \neg Q(h(x,y)))) \}$ a

formule $A = \exists x\ (\neg R(x,a) \Rightarrow (\neg Q(h(x,a))))$.
Dokažte , že $\Gamma \vdash A$.

Postupujeme podle kroků 1. - 7.:

1\. - 4.: $\Gamma_A = \{ (\forall x \forall y\ (P(x,y) \vee (\exists x \exists y\ P(x,y)))) ,$
$((\exists z \forall u\ R(z,u)) \vee (\forall u \forall z\ (\neg Q(h(u,z))))) ,$
$(\forall s\ (\neg R(s,a) \wedge Q(h(s,a)))) \} .$

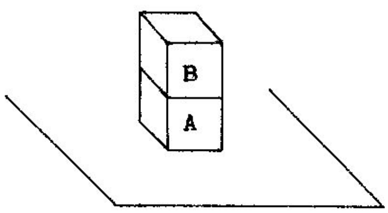
5\.: $\Gamma_A = \{ (\forall x \forall y\ (P(x,y) \vee P(f(y),g(x)))) ,$
$(\forall u \forall z\ (R(b,u) \vee (\neg Q(h(u,z))))) ,$
$(\forall s\ (\neg R(s,a) \wedge Q(h(s,a)))) \} .$

6\.: Γ_s : s_1: $P(x,y) \vee P(f(y),g(x))$,
s_2: $R(b,u) \vee (\neg Q(h(u,z)))$,
s_3: $\neg R(s,a)$,
s_4: $Q(h(s,a))$.

7\.: Substituce do složky s_2 : $u = s$, $z = a$.
$r(s_2,s_4) = (R(b,u) \vee (\neg Q(h(s,a)))) \wedge (Q(h(s,a)) \vee \emptyset) \Rightarrow R(b,u) = s_5$,
$\Gamma_s = \Gamma_s \cup s_5$.
Substituce do složky s_3 : $s = b$, do složky s_5 : $u = a$.
$r(s_3,s_5) = \neg R(b,a) \wedge R(b,a) \Rightarrow \emptyset$.
Platí $\Gamma \vdash A$. Důkaz je skončen .∎

Příklad 29.3.:

Uvažujme situaci na obr. 12.3. Inteligentní robot analyzuje scénu. Ukažme, jak lze automatického dokazování použít k prověření odpovědi " B je nad stolem " na otázku typu " Kde je B ? ".



=> NA(A,B) !
NA(Stůl,A) !
NAD(Stůl,B) ?

Obr.12.3.

K popisu scény byly využity predikáty :

NA(x,y) ... "na x je y" (y leží na x) ,
NAD(x,y) .. "nad x je y" .

K atomickým formulím NA(A,B) , NA(Stůl,A) , které obsahují jen konstanty a popisují bezprostředně analyzovaný fragment realizy, přistupují následující dva axiomy univerzálně platné pro libovolnou situaci "hranatého světa" :

$$AX1: \forall x \forall y \ (NA(x,y) \Rightarrow NAD(x,y)) \ ,$$

$$AX2: \forall x \forall y \forall z((NAD(x,y) \wedge NAD(y,z)) \Rightarrow NAD(x,z)) \ .$$

Sestrojme množinu Γ_A :

$$\Gamma_A = \{ NA(A,B) \ , NA(Stůl,A) \ , \forall x \forall y \ (Na(x,y) \Rightarrow Nad(x,y)) \ ,$$
$$\forall x \forall y \forall z \ ((NAD(x,y) \wedge NAD(y,z)) \Rightarrow NAD(x,z)) \ , \neg NAD(Stůl,B) \} \ .$$

V daném případě lze snadno provést kroky 2.- 6. a získat množinu Γ_s :

$$\Gamma_s : s_1 : \ NA(A,B) \ ,$$
$$s_2 : \ NA(Stůl,A) \ ,$$
$$s_3 : \ \neg NA(u,v) \vee NAD(u,v) \ ,$$
$$s_4 : \ \neg NAD(x,y) \vee (\neg NAD(y,z)) \vee NAD(x,z) \ ,$$
$$s_5 : \ \neg NAD(Stůl,B) \ .$$

V kroku 7. provedeme postupně následující substituce a resoluce :

- do složky s_4 : x = Stůl , $z = B$,

$$s_6 : r(s_4,s_5) = \neg NAD(Stůl,y) \vee (\neg NAD(y,B))$$

- do složky s_6 : $y = u$, do složky s_3 : $v = B$:

$$s_7 : r(s_3,s_6) = \neg NA(u,B) \vee (\neg NAD(Stůl,u)) \ ,$$

- do složky s_7 : $u = A$:

$$s_8 : r(s_1,s_7) = \neg NAD(Stůl,A) \ ,$$

- do složky s_3 : u = Stůl , $v = A$:

$$s_9 : r(s_3,s_8) = \neg NA(Stůl,A) \ ,$$

- pomocí s_2 a s_9 získáme prázdnou resolventu :

$$s_{10} : r(s_2,s_9) = NA(Stůl,A) \wedge (\neg NA(Stůl,A)) = \emptyset \ .$$

Odpověď potvrzena. Platí : NAD(Stůl,B) - "B je nad stolem". ∎

<u>Příklad 30.3.</u>:

Prověřme konsistentnost zápisů z výstupní kontroly výrobků :

Z1: Žádný výrobek série A nebyl reklamován.

Z2: Žádný při dalším zpracování vyřazený výrobek nebyl ze série A.

Z3: Všechny kontrolované výrobky byly ze série A.

Z4: Neexistuje výrobek,který by byl po kontrole reklamován nebo při dalším zpracování vyřazen.

Situaci přepíšeme do formulí pomocí predikátových konstant : $SEQ_A(x)$ ... být výrobkem ze série A , RM(x) ... být reklamovaným výrobkem , LIQU(x) ... být vyřazeným výrobkem.

$$Z1 : \neg \exists x(SEQ_A(x) \wedge RM(x)) \ ,$$

$$Z2 : \neg \exists x(SEQ_A(x) \wedge LIQU(x)) \ ,$$

$$Z3 : \ \forall x \ SEQ_A(x) \ ,$$

$$Z4 : \neg \exists x(RM(x) \vee LIQU(x)) \ .$$

Prověřme vyplývání : $\{ Z1 \text{ ET } Z2 \text{ ET } Z3 \} \vdash Z4$

V krocích 1.,3.,4. sestrojíme upravenou množinu Γ_{Z4} :

$$\Gamma_{Z4} = \{ \forall x \ (\neg SEQ_A(x) \vee (\neg RM(x)) \ , \forall u \ (\neg SEQ_A(u) \vee (\neg LIQU(u))), \forall v \ SEQ_A(v) \ , \exists z \ (RM(z) \vee LIQU(z)) \}.$$

V krocích 5. a 6. sestrojíme sestrojíme množinu Γ_s :

$$\Gamma_s : s_1 : \neg SEQ_A(x) \vee (\neg RM(x)) \ ,$$

$$s_2 : \neg SEQ_A(u) \vee (\neg LIQU(u)) \ ,$$

$$s_3 : \ SEQ_A(v) \ ,$$

$$s_4 : \ RM(a) \vee LIQU(a) \ .$$

V kroku 7. provedeme následující substituce a resoluce :

- Substituce do složky s_1 : $x = v$,

$$s_5 = r(s_1, s_3) = \neg RM(v) \ ,$$

- substituce do složky s_5 : $v = a$,

$$s_6 = r(s_4, s_5) = LIQU(a) \ ,$$

- substituce do složky s_2 : $u = a$,

$$s_7 = r(s_2, s_6) = \neg SEQ_A(a) \ ,$$

- substituce do složky s_3 : $v = a$,

$$s_8 = r(s_3, s_7) = SEQ_A(a) \wedge (\neg SEQ_A(a)) \Rightarrow \emptyset \ .$$

Zápisy Z1,Z2,Z3,Z4 jsou vzájemně konsistentní.■

<u>Kontrolní otázky a úlohy</u> :

1. Uveďte některé přednosti (a také nevýhody) použití Robinsonova resolučního principu proti možnostem syntaktických inferenčních systémů a proti metodě důkazu pomocí sémantických rozkladových tabulek.

2. Ukažte , že známé pravidlo " modus tolens " je speciálním případem resoluce.

3. Navrhněte jednoduchý algoritmus řízení postupu resolučního důkazu tak, aby vstup lidského operátora se omezoval pokud možno jen na zadání úlohy .

4. Promyslete,jak se projeví v důkazu resoluční metodou důsledek nerozhodnutelnosti predikátového kalkulu prvého řádu.

5. Následující formule převeďte do Skolemovy normální formy s Hornovými klausulemi.Nalezněte některou správnou interpretaci k výchozí formuli a srovnejte s interpretací získané Skolemovy normální formy:

   a) $\forall x \forall y \exists z \; (((x > y) \wedge (y > z)) \Rightarrow (x > z))$,

   b) $\forall x \neg((P(x) \Rightarrow (Q(x) \Rightarrow N(x))) \Rightarrow ((P(x) \Rightarrow Q(x)) \Rightarrow (P(x) \Rightarrow N(x))))$,

   c) $\exists x \exists y \; (P(x,y) \Leftrightarrow \forall z (P(y,z) \Rightarrow P(y,x)))$

   d) $\forall x \forall y ((NAD(x,y) \wedge (\neg NA(x,y))) \Rightarrow (\exists z \; (NAD(x,z) \wedge NAD(z,y))))$.

6. Uvažujete o počtu operací,které je třeba vykonat k realizaci postupu důkazu resoluční metodou.Naznačte,jak analyticky odvodit,zda počet operací narůstá exponenciálně nebo polynomiálně.

7. Rozhodněte resoluční metodou o následujících axiomech :

$$\forall x \; (\neg Equal(x,x+1))$$
$$Equal(2,3) \; .$$

8. Ověřte,zda následující formule jsou tautologiemi :

   a) $\exists x \; (P(x) \wedge Q(x)) \Rightarrow ((\exists x \; P(x)) \wedge (\exists x \; Q(x)))$,

   b) $\forall x \; (\neg P(x,x) \wedge (\forall z \exists y \; (P(z,y) \Rightarrow P(z,x))))$.

9. Je dána množina formulí Γ :

   $\Gamma = \{\forall x \; (R(x) \Rightarrow Q(x)), \forall x \; (S(x) \Rightarrow (\neg Q(x))), \exists x \; (S(x) \wedge P(x))\}$ a

   formule $A = \exists x \; (P(x) \wedge (\neg R(x)))$. Dokažte $\Gamma \vdash A$.

10. Je dána množina výroků :

   - Jestliže je kurs dobrý, pak stojí za to jej absolvovat.
   - Buďto je klasifikace mírná,nebo nestojí za to ten kurs absolvovat.
   - Jenže klasifikace není mírná .

   Závěr : Tento kurs není dobrý .

   Dokažte resolučním principem,zda závěr vyplývá z předchozích premis.