УДК 510.662

Афонін А. О.

ПРО МАШИННО-ОРІЄНТОВАНІ ЧИСЛЕННЯ СЕКВЕНЦІАЛЬНОГО ТИПУ ДЛЯ КЛАСИЧНОЇ ЛОГІКИ ПЕРШОГО ПОРЯДКУ

Стаття присвячена розробці підходу до побудови машинно-орієнтованих числень секвенціального типу, які не потребують проведення попередньої сколемізації. Особливості цього підходу продемонстровано за допомогою побудови спеціального числення такого типу, яке досліджується на коректність і повноту. Використовуючи це числення, описано засоби повних розширень SLD-резолюції, як для множин диз'юнктів довільного вигляду, так і для множин звичайних формул мови логіки предикатів першого порядку.

Вступ

Дослідження в аспекті"створення засобів логічної обробки математичних знань, призначених для зфективного розв'язання природничих і технічних задач за допомогИю ЕОМ, були започатковані ще в першій половині 1960-х років. З часом актуальність таких досліджень тільки зростає. Поява обчислювальних машин високої швидкодії, інформаційної ємності і гнучкості дала змогу побудувати перші системи автоматизації міркувань. На час виникнення таких систем їх дослідження були досить умоглядні, але наразі розширені можливості ЕОМ привертають до систем автоматизації міркувань пильну увагу як з теоретичного погляду, так і з погляду їх практичного використання. Зокрема, прикладом практичного застосування систем автоматизації міркувань є перевірка коректності протоколів (криптографічних, комунікаційних і т. п.). До інших можливих застосувань належать: перевірка коректності математичних текстів, дистанційне навчання математичним дисциплінам, вилучення знань з математичних праць, створення баз формалізованих знань.

На сучасному етапі використовується низка машинних методів пошуку логічного виведення в логіці першого порядку: методи резолюційного типу, машинно-орієнтовані секвенціальні числення, які часто набувають вигляду табличних методів, різноманітні модифікації методу елімінації моделей, різновиди зворотного методу та інші [1]. Розробники цих методів найперше мають за мету досягнення максимальної ефективності пошуку виведень. Однак, як засвідчив багаторічний досвід з автоматизації міркувань, навіть максимально висока ефективність якогось методу (хоча б на певному класі завдань) не дає змоги досягти людських можливостей за креативністю – дотепер немає методів, що дають можливість автоматично довести досить складне твердження. Це викликано тим, що під час пошуку виведення генерується настільки швидко зростаючий пошуковий простір, що знайдення хоч якогось доведення складного твердження не забезпечується ресурсами навіть сучасних комп'ютерів. Тому варто розглядати підхід до автоматизації міркувань, який веде до розуміння людиною процесу пошуку доведення і, як наслідок, до дружнього інтерфейсу з користувачем. За такої орієнтації розвитку машинних методів пошуку логічного виведення найбільш придатним є секвенціальний формалізм (у різних своїх модифікаціях). Це викликано такими причинами: 1) вдається зберегти структуру вихідного завдання; 2) процес пошуку має деревоподібну структуру й може використовувати різні переборні стратегії, як-от: «спочатку вглиб, а потім вшир», «спочатку вшир, а потім вглиб», а також різні їхні комбінації; 3) не є складним вбудовування евристичних і природних прийомів доказу; 4) процес розв'язку рівнянь (рівностей) може бути відділений від логічних кроків; 5) легко вбудовуються інтерактивні режими пошуку за участю людини.

Саме виходячи із цих позитивних особливостей секвенціального формалізму, пошук логічного виведення був узятий за основу у розробці машинно-орієнтованих числень, що досліджуються у цій роботі.

Окремої згадки заслуговує секвенціальний підхід до побудови дедуктивних методів систем логічного програмування, якими зазвичай стають різні модифікації так званої SLD-резолюції, що є повним методом тільки для множин хорнових диз'юнктів. У зв'язку з цим постає запитання: якими логічними засобами можна розширити SLD-резолюцію так, щоб отримати повний метод для множин довільних диз'юнктів? Тим більше, що ряд результатів [2–4] засвідчує, що

можна отримати повні в спільному випадку розширення вхідної резолюції, і вони мають вигляд лінійного пошуку спростування (див., наприклад, [4]). Підхід, запропонований у роботі, дає певну відповідь і на це запитання.

1. Основні поняття

Основним об'єктом у численні, яке будується нижче, є *a*-секвенція.

A-секвенцію можна розглядати як спеціальне узагальнення звичайного поняття секвенції. Ми розглядаємо секвенції, сукцедент яких складається лише з одного об'єкта (що має назву *цілі*).

Будемо вважати, що класичне числення предикатів першого порядку представлено у вигляді секвенційного числення *G*, описаного в [5].

Ми використаємо поняття підстановки та результату застосування підстановки до виразу в змісті роботи [6].

Підстановочна компонента – це вираз виду t/x, де x – змінна, а t – терм підстановки.

Нехай L – літера, позначимо як $\sim L$ її заперечення. Використаємо вираз $L(t_1,...,t_n)$ для позначення того, що t_1, ..., t_n є список всіх термів (можливо, з повтореннями), що займають аргументні місця в літері L, у тому порядку, у якому вони зустрічаються в ній.

Позначимо $F|_y^x$ результат заміни у формулі F змінної x на змінну y.

Крім звичайних змінних, будемо використовувати дві зліченні множини спеціальних змінних: невідомі й фіксовані змінні («фіктивні змінні») і «параметри» у термінології [7].

Упорядкована трійка $<w, F, E>$ називається *ансамблем*, якщо w є послідовність (слово, що складається з невідомих і фіксованих змінних), то F – формула першого порядку, E – множина пар термів t_1 і t_2 рівностей вигляду $t_1 = t_2$.

Вираз виду $[B], <w_1, P_1, E_1>,...,<w_n, P_n, E_n> \rightarrow <w_1, G, E>$, де $<w_1, P_1, E_1>$, ..., $<w_n, P_n, E_n>$, $<w_1, G, E>$, – ансамблі і $[B]$ – список ансамблів, можливо, порожній, назвемо *a-секвенцією*.

Ансамблі в антецеденті *a*-секвенції називаються *припущеннями*, а ансамбль в сукцеденті – *ціллю* даної *a*-секвенції.

Сукупність припущень розглядається як множина; таким чином, порядок припущень не істотний.

Нехай W – множина послідовностей невідомих і фіксованих змінних, s – підстановка.

Покладемо $A(W,s) = \{<z, t, w>$: z – змінна s, t – терм s, а змінна z розташована в w ліворуч від деякої фіксованої змінної з $t\}$.

Підстановка s називається *допустимою для* W [див.: 8], якщо (1) всі змінні s є невідомими змінними, (2) в $A(W,s)$ не існує (різних) елементів $<z_1, t_1, w_1>$, ..., $<z_m, t_m, w_m>$, таких, що $t_2/z_1 \in s$, ..., $t_1/z_m \in s$ $(m > 0)$.

2. Машинно-орієнтоване секвенціальне числення *aS*

На базі *a*-секвенцій нижче будується числення секвенціального типу, яке називається численням *a*-секвенцій та позначається ***aS.***

Вихідна a-секвенція в численні ***aS*** задається так:

Припустимо, деякий цілісний математичний текст *Txt*, записаний мовою класичної логіки першого порядку, містить сукупність визначень, припущень і допоміжних тверджень P_1, ..., P_q, а T позначає теорему, яку треба довести в контексті *Txt*. Цю задачу можна сформулювати як встановлення вивідності секвенції виду $P_1, ..., P_q \rightarrow F$ в числення G [5]. Тоді будемо вважати вираз $<,P_1,>,...,<,P_q,>,<,\neg F,> \rightarrow <,F,>$ *вихідною a-секвенцією* в численні ***aS*** (відносно тексту *Txt*). (Ми не виключаємо випадок, коли $p = 0$ та/або $q = 0$.)

Шукаючи висновок у численні ***aS***, будуємо дерево пошуку виведення. На початку воно складається з вихідної a-секвенції. У процесі пошуку усіма вузлами дерева пошуку виведення є секвенції вигляду, $M \rightarrow F$ (M позначає множину припущень, а формула F – ціль).

Нехай літера K може бути отримана з літери $L(t_1,...,t_n)$ шляхом заміни термів $t_1,...,t_n$ деякими термами $t'_1,...,t'_n$. Тоді будемо говорити, що L *збігається* з K з точністю до рівностей $t_1 = t'_1$, ..., $t_n = t'_n$ та писати $L \approx K \bmod \Sigma(L, K)$, де $\Sigma(L, K) = \{t_1 = t'_1, ..., t_n = t'_n\}$.

Введемо поняття позитивного та негативного входження літери L у формулу F (позначуваного відповідно $F\lfloor L^+ \rfloor$ або $F\lfloor L^- \rfloor$) з точністю до рівностей:

(I) якщо L і E – літери і $L \approx K \bmod \Sigma(L, K)$, то $K\lfloor L^+ \rfloor$;

(II.1) якщо має місце $F\lfloor L^+ \rfloor$ $(F\lfloor L^- \rfloor)$ з точністю до рівностей $\Sigma(L, K) = \{t_1 = t'_1, ..., t_n = t'_n\}$ і F_1 є формула, то L має позитивне (негативне) входження (з точністю до рівностей $\Sigma(L, K)$) до формул: $F_1 \wedge F$, $F_1 \vee F$, $F_1 \supset F$, $\forall xF$ і $\exists xF$;

(II.2) якщо має місце $F\lfloor L^+ \rfloor$ $(F\lfloor L^- \rfloor)$ з точністю до рівностей $\Sigma(L, K) = \{t_1 = t'_1, ..., t_n = t'_n\}$ і F_1 є формула, то L має негативне (позитивне) входження (з точністю до рівностей $\Sigma(L, K)$) в формули $F \supset F_1$ і $\neg F$.

2.1. Правила виведення числення *aS*

Нижче ми використаємо $F^{\neg}$ для позначення результату однократного пронесення зовнішнього знака «¬» у формулу F відповідно до таких тотожностей: $\neg(F_1 \vee F_2) \equiv \neg F_1 \wedge \neg F_2$; $\neg(F_1 \wedge F_2) \equiv \equiv \neg F_1 \vee \neg F_2$; $\neg(F_1 \supset F_2) \equiv F_1 \wedge \neg F_2$; $\neg\neg F_1 \equiv F_1$; $\neg\forall x F_1(x) \equiv \exists x \neg F_1(x)$; $\neg \exists x F_1(x) \equiv \forall x \neg F_1(x)$.

Правила виведення числення, що розглядаються, розподілено на кілька груп.

2.1.1. Правила розщеплення цілі

Правила розщеплення цілі використовуються для елімінації головної логічної зв'язки з формули, що перебуває в тілі оброблюваної *a*-секвенції. Застосування кожного з правил приводить до породження нової *a*-секвенції з єдиною ціллю.

Елімінація пропозиціональних зв'язок виконується так само, як і в класичній логіці першого порядку, і може бути виражена в термінах похідних правил стандартного числення генценівського типу [9].

Істотна відмінність від традиційних засобів пошуку висновку генценівського типу спостерігається під час обробки кванторів. Ця відмінність відображує спеціальні засоби обробки квантотів за допомогою поняття допустимої підстановки, що вивчалися в [8], при яких змінні кванторів, котрі елімінуються, заміщаються (залежно від виду і позиції квантора, що елімінується) невідомими або фіксованими змінними.

Пропозиційні правила

$$\frac{[B],\ M \to \langle w, F \supset G, E\rangle}{[B], M, \to \langle w, G, E\rangle};\quad \frac{[B],\ M \to \langle w, F \supset G, E\rangle}{[B],\ M, \to \langle w, F^{\neg}, E\rangle};$$

$$\frac{[B],\ M \to \langle w, F \vee G,\ E\rangle}{[B], M \to \langle w, G, E\rangle};\quad \frac{[B],\ M \to \langle w, F \vee G,\ E\rangle}{[B], M \to \langle w, F,\ E\rangle};$$

$$\frac{[B], M \to \langle w, F \wedge G,\ E\rangle}{[B], M \to \langle w, F, E\rangle\ [B], M \to \langle w, G, E\rangle};$$

$$\frac{[B], M \to \langle w, \neg F, E\rangle}{[B], M \to \langle w, F^{\neg}, E\rangle};$$

$$\frac{[B], M \to \langle w, L, E\rangle}{[B, \langle w', L', E'\rangle], M \to \langle w,\ L, E\rangle};$$

де F, G – формули, L – тільки літера і L' – новий варіант літери L, і перейменування змінних, що перетворює L в L', переводить w у w' та E в E'.

Кванторні правила

$$\frac{[B], M \to \langle w, \forall x F,\ E\rangle}{[B], M \to \langle w\, x^{+}, F|^{x}_{x+}, E\rangle};\quad \frac{[B],\ M \to \langle w, \exists y F,\ E\rangle}{[B], M \to \langle w\, y^{-}\, F|^{y^{-}}_{y}, E\rangle},$$

де x^+ – нова фіксована змінна, y^- – нова невідома змінна і $F|^{x}_{x+}$, $(F|^{y}_{y})$ – результат заміни в F всіх змінних x (y) змінними x^+ (y^-).

2.1.2. Правила допоміжної цілі

Правила допоміжної цілі можна інтерпретувати в термінах числень генценівського типу як елімінацію головних логічних зв'язок з формул, котрі входять у припущення. Скрізь нижче K і L позначають літери, що задовольняють умову: $L \approx K \bmod \Sigma(L, K)$.

Пропозиційні правила

$$\frac{[B],\ M, \langle w', F\lfloor K^{-}\rfloor \supset G, E'\rangle \to \langle w, L,\ E\rangle}{[B], M, \langle w', (F\lfloor K^{-}\rfloor)^{\neg}, E'\rangle \to \langle w, L,\ E\rangle};$$
$$[B,\ \langle w, L,\ E\rangle],\ M \to \langle w', G, E'\rangle$$

$$\frac{[B],\ M,\ \langle w', F \supset G\lfloor K^{+}\rfloor, E'\rangle \to \langle w, L, E\rangle}{[B],\ M, \langle w', (G\lfloor K^{+}\rfloor), E'\rangle \to \langle w, L,\ E\rangle};$$
$$[B,\ \langle w, L, E\rangle],\ M \to \langle w', F\lfloor K^{+}\rfloor, E'\rangle$$

$$\frac{[B],\ M,\ \langle w', F\lfloor\ K^{+}\rfloor \vee G, E'\rangle \to \langle w, L, E\rangle}{[B], M, \langle w', (F\lfloor\ K^{+}\rfloor)^{\neg}, E'\rangle \to \langle w, L, E\rangle};$$
$$[B,\ \langle w, L, E\rangle], M \to \langle w', G^{\neg}, E'\rangle$$

$$\frac{[B],\ M,\ \langle w', F \vee G\lfloor\ K^{+}\rfloor, E'\rangle \to \langle w, L, E\rangle}{[B], M, \langle w', F, E'\rangle \to \langle w, L, E\rangle};$$
$$[B,\ \langle w, L, E\rangle], M \to \langle w',\ (G\lfloor\ K^{+}\rfloor)^{\neg}, E'\rangle$$

$$\frac{\rfloor,\ M,\ \langle w', F \wedge G\lfloor\ K^{+}\rfloor, E'\rangle \to \langle w, L, E\rangle}{[B],\ M, \langle w', F, E'\rangle, \langle w',\ (G\lfloor\ K^{+}\rfloor)^{\neg}, E'\rangle \to \langle w, L, E\rangle};$$

$$\frac{[B],\ M,\ \langle w', F\lfloor\ K^{+}\rfloor \wedge G, E'\rangle \to \langle w, L, E\rangle}{[B],\ M, \langle w', (F\lfloor\ K^{+}\rfloor)^{\neg}, E'\rangle, \langle w', G, E'\rangle \to \langle w, L, E\rangle};$$

$$\frac{[B],\ M,\ \langle w', \neg(F[K^{-}]), E'\rangle \to \langle w, L, E\rangle}{[B], M, \langle w', (F[K^{-}])^{\neg}, E'\rangle \to \langle w, L, E\rangle}.$$

Кванторні правила

$$\frac{[B], M, \langle w', \exists x\, F[K^{-}], E'\rangle \to \langle w, L, E\rangle}{M, \langle w' x^{+}, F|^{x}_{x+}, E'\rangle \to \langle w, L, E\rangle};$$

$$\frac{[B], M, \langle w', \forall y F, E'\rangle \to \langle w, L, E\rangle}{M, \langle w' y^{-}, F|^{y^{-}}_{y}, E'\rangle \to \to \langle w, L, E\rangle},$$

де x^+ – нова фіксована змінна, y^- – нова невідома змінна, а $w'x^+$ ($w'y^-$) – результат приписування x^+ (y^-) у послідовності w'.

2.1.3. Термінальні правила

($\#_1$)-правило:

$$\frac{[B], M, \langle w, K(t_1,\ldots,t_n), E\rangle \to \langle w', L(t'_1,\ldots,t'_n), E'\rangle}{[B], M, \langle w, K(t_1,\ldots,t_n), E\rangle \to \langle w, \#, E''\rangle};$$

($\#_2$)-правило:

$$\frac{[B, \langle w, K(t_1,\ldots,t_n), E\rangle, B'], M, \to \langle w', L(t'_1,\ldots,t'_n), E'\rangle,}{[B, \langle w, K(t_1,\ldots,t_n), E\rangle, B'], M \to \langle w', \#, E''\rangle}$$

де $L \approx K \bmod \Sigma(L, K)$, $E'' = E \cup E'_{-} \cup \{t_1 = t'_1, \ldots, t_n = t'_n\}$.

2.1.4. Аксіоми

$[B], M, K \to \langle w, \#, E''\rangle$, де # означає порожню формулу.

2.1.5. Дерево виведення

Зазначимо, що спосіб завдання вихідної *a*-секвенції *S* для числення ***aS*** був описаний вище.

Застосовуючи правила висновку «зверху вниз» до вихідної *a*-секвенції, а потім до її «нащадків» і т. д., ми одержуємо в підсумку *дерево пошуку виведення*. Дерево пошуку виведення *Tr* називається *деревом доведення* для вхідної a-секвенції тоді й тільки тоді, коли (1) усякий лист дерева *Tr* – аксіома; (2) існує уніфікатор *s* [6] всіх рівностей з *Tr*; (3) уніфікатор *s* допустимий (у сенсі даної роботи) для множини всіх послідовностей фіксованих і невідомих змінних, що знаходяться в листах дерева *Tr*.

Зауважимо, що перевірка можливості перетворення поточного дерева пошуку виведення в дерево доведення може бути виконана на будь-якому етапі. Для виконання перевірки можуть бути використані довільні засоби побудови найбільш загального уніфікатора [6].

3. Коректність і повнота числення *aS*

Відносно числення ***aS*** мають місто наступні результати.

ПРОПОЗИЦІЯ 1 (коректність і повнота числення ***aS***). Нехай $P_1,...,P_n$ утворюють сумісну множину формул, і F є деяка формула. Секвенція $P_1, ..., P_q \to F$ виводиться в генценівському численні *LK* [9] тоді і тільки тоді, коли в численні ***aS*** існує дерево доведення відносно вихідної *a*-секвенції [9], $<,P_1,>,...,<,P_q,>,<,F^{\neg},> \to <,F,>$.

Ескіз доведення. Техніку доведення коректності і повноти числення GD_2 [10] можна поширити на загальний випадок, зважаючи на властивості припустимих підстановок, які зазначені в [8] Q.E.D.

НАСЛІДОК 1. Формула F є загальнозначущою тоді і тільки тоді, коли у численні ***aS*** існує дерево доведення відносно ініціальної a-секвенції [9], $<,F^{\neg},> \to <,F,>$ у численні ***aS***.

Доведення. Формула F є загальнозначущою тоді і тільки тоді, коли в численні *LK* виводиться секвенція $\to F$. Далі достатньо застосувати пропозицію 1. Q.E.D.

Вище зазначено, що математичні тексти можуть бути трансльовані в об'єкти класичної логіки першого порядку. Це дає змогу говорити про формули, які відповідають таким одиницям математичного тексту, як теорема, визначення, допоміжне твердження, а також працювати із цілісним текстом як множиною формул першого порядку.

Таким чином, такі вирази, як «несуперечність тексту», «дана теорема є логічним наслідком даного тексту», «загально значність» розуміються однозначно й не потребують спеціального визначення.

НАСЛІДОК 2. Теорема T є логічний наслідок несуперечливого математичного тексту *Txt* (що не містить в собі *T*) тоді й тільки тоді, коли в ***aS*** може бути побудоване дерево доведення з вихідною секвенцією відносно *T* і *Txt*.

Зазначимо також, що досить багатий набір правил числення ***aS*** дає змогу будувати різноманітні стратегії пошуку доведень, які можуть модулювати звичайні математичні прийоми, але нижче нас цікавитимуть деякі його спеціальні стратегії, що формулюються для певних класів диз'юнктів.

4. Літеральна модифікація числення *aS*

Нижче показано, що певне звуження числення ***aS*** на випадок так званих літеральних *a*-секвенцій дає змогу побудувати такі розширення *SLD*-резолюції, які породжують повні методи для множин диз'юнктів довільної структури.

Розглянемо випадок секвенції вигляду $K_{1,1} \vee ... \vee K_{1,r1},..., K_{1,r1} \vee ... \vee K_{n,mn} \to L_1 \wedge ... \wedge L_k$, де $K_{1,1}, ..., K_{n,mn}, L_1, ..., L_k$ – літери. Оскільки кожна формула першого порядку певними перетвореннями, які зберігають логічну еквівалентність, може бути спочатку зведена до сколемівської функціональної форми, а після опускання кванторів – до кон'юнктивної (диз'юнктивної) нормальної форми, то на підставі результатів з [9] легко показати, що встановлення вивідності будь-якої секвенції довільного вигляду еквівалентне встановленню вивідності схожої секвенції вказаного вигляду. У цьому зв'язку відзначимо, що якщо $G \in L_1 \wedge ... \wedge L_k$, то $G^{\neg} \in \sim L_1 \vee ... \vee \sim L_k$, то $G^{\neg} \in \sim L_1 \vee ... \vee \sim L_k$.

Враховуючи вищесказане, числення ***aS*** може бути трансформоване у числення ***lS*** «літеральних» *a*-секвенцій, яке має такі правила (вважаємо, що диз'юнкція і кон'юнкція мають довільні скінченні арности (≥ 1)):

Правило розщеплення цілі. Це правило узагальнює правило «розщеплення кон'юнкції» в правилах допоміжної цілі числення ***aS***:

$$\frac{[B], M \to <w, L_1 \wedge ... \wedge L_k, E>}{[B], M \to <w, L_1 \; ... \; M \to <w, L_k, E>};$$

$$\frac{[B], M \to <w, L, E>}{[B, <w', L', E'>], M \to <w, L, E>}$$

де $L_1, ..., L_k$, і L' – новий варіант літери L, і перейменування змінних, що перетворює L в L', переводить w в w' та E в E'.

Правило розщеплення посилки. Це правило може бути застосоване, коли мета розглянутої секвенції є літерою:

$$\frac{[B], M, <w, A_1 \vee ... \vee A_n \vee K \vee B_1 \vee ... \vee B_j, E'> \to <w, L, E>}{[B], M' \to <w', \sim A'_1, E'> \; ... \; M' \to <w', \sim A'_n, E'> M' \to <w', \sim B'_1, E'> \; ... \; M' \to <w', \sim B'_j, E'>},$$

де $A_1,..., A_n, B_1,..., B_r, L$ і K є літери; $L \approx K$ mod $\Sigma(L, K)$; $M' = M \cup \{ <w, A_1 \vee ... \vee A_n \vee K \vee B_1 \vee ... \vee B_r, E'>\}$; $A'_1, \ldots, A'_n, B'_1,..., B'_r$ – нові варіанти літер $A_1,..., A_n, B_1,..., B_r$, і відповідне перейменування переводить w в w' та E в E'.

Числення ***lS*** *також має правила* ($\#_1$) і ($\#_2$) числення ***aS***.

ПРОПОЗИЦІЯ 2 (коректність і повнота числення ***lS***). Нехай $P_1, ..., P_n$ утворюють сумісну множину диз'юнктів. Кон'юнкція літер G є логічний наслідок диз'юнктів $P_1, ..., P_n$ тоді і тільки тоді, коли в численні ***aS*** існує дерево доведення відносно вихідної a-секвенції $[10],<,P_1,>,...,<,P_q,>,<,G^\neg,>\rightarrow<,G,>$.

Схема доведення. Відповідно до пропозиції 1, існує дерево доказу Tr щодо a-секвенції $P_1,..., P_n, G^\neg \rightarrow G$ в численні ***aS***. Очевидно, що Tr містить вживання лише таких правил виводу числення ***lS***, які мають відповідні аналоги в численні ***aS***. Q. E. D.

Зауваження. Звертаємо увагу на те, що через відсутність кванторів у початковій a-секвенції (і як результат, кванторних правил), будь-яка a-секвенція в численні числення ***lS*** має вигляд $<,K_{1,1} \vee ... \vee K_{1,r1},E_1>,..., <,K_{1,r1} \vee ... \vee K_{n,mn}, E_n>\rightarrow <,L_1 \wedge ... \wedge L_k,E'>$, тобто перші компоненти ансамблів будь-яких a-секвенцій числення ***lS*** є порожньою послідовністю.

Особливістю числення ***lS*** є те, що антецеденти a-секвенцій, що виводяться, збігаються з антецедентом відповідної вихідної a-секвенції. Це дає змогу розглядати антецедент цієї вихідної a-секвенції як множину вхідних диз'юнктів і перетворювати кожне дерево доведення Tr числення ***lS*** в дерево $\gamma(Tr)$, листя якого збігаються з листям дерева Tr і позначені літерами цілей відповідних a-секвенцій (і лише ними). Ми називатимемо таке дерево $\gamma(Tr)$ деревом цілей, відповідним дереву Tr. Таким чином, є простий спосіб переходу від числення ***lS*** до *SLD*-резолюції.

Повнота *SLD*-резолюції для множини хорнових диз'юнктів є відомим результатом логічного програмування. Наступна пропозиція містить його.

НАСЛІДОК 3 (коректність і повнота *SLD*-резолюції). Нехай $P_1,..., P_n$ є позитивними хорновими диз'юнктами, і G є кон'юнкцією атомарних формул. Кон'юнкція G є логічним наслідком сумісної множини диз'юнктів $P_1,..., P_q$ в тому і лише тому випадку, коли в численні ***lS*** існує дерево доведення відносно a-секвенції $<,P_1,>,...,<,P_q,>,<,G^\neg,>\rightarrow<,G,>$ (тобто без застосування $\#_2$-правила).

Доведення. Відповідно до пропозиції 2, в численні ***lS*** існує дерево доведення Tr відносно вихідної секвенції $[9],<,P_1,>,...,<,P_q,>,<,G^\neg,>\rightarrow<,G,>$. Очевидно, що Tr не містить секвенцій, які виводяться за $\#_2$-правилом. Отже, Tr побудовано в численні ***lS*** без деякого використання ансамблю $<,G^\neg,>$ і компоненти $[B]$ довільної a-секвенції з Tr, тобто $\gamma(Tr)$ може розглядатися як дерево, генероване за методом *SLD*-резолюції [3], коли одночасний найбільш загальний уніфікатор (якщо він існує) породжується кожного разу при застосуванні будь-якого правила числення ***lS***. Q. E. D.

З цього наслідку та пропозицій 1 і 2 випливає істинність наступного твердження.

НАСЛІДОК 4 (про повні розширення *SLD*-резолюції). Числення ***lS*** може розглядатися як повне розширення *SLD*-резолюції на випадок довільних диз'юнктів, а числення ***aS*** – як її розширення на випадок довільних формул мови логіки предикатів першого порядку.

Висновки

Підхід, розвинений в роботі, демонструє таке. По-перше, він дає змогу будувати машинно-орієнтовані числення секвенціального типу, достатньо ефективні у разі встановлення вивідності без виконання попередньої сколемізації. По-друге, він дає засоби повних розширень *SLD*-резолюції як для множин диз'юнктів довільного вигляду, так і для множин будь-яких формул мови логіки предикатів першого порядку. Ця його властивість дає змогу запропонувати методи модифікації програмних засобів інтелектуальних систем (наприклад, систем логічного програмування, експертних систем, дедуктивних баз даних і т. д.) з метою отримання повних, в загальному випадку, розширень їх дедуктивного апарату, що використовує *SLD*-резолюцію як базову техніку пошуку логічного висновку.

1. Handbook of Automated Reasoning / Edited by A. Robinson and A.Voronkov. – Elsevier Science Publishers, 2001. – Vol. 1. – 1020 p.
2. Stickel M. A. Prolog Technology Theorem Prover / M. A. Stickel. – New Generation Comp. – 1984. – Vol. 4. – P. 371–383.
3. Lloyd J. V. Foundations of Logic Programming / J. V. Lloyd. – Berlin : Springer, 1987. – 476 p.
4. Apt K. R. Contributions into the Theory of Logic Programming / K. R. Apt, M. H. van Emden // JASM. – 1982. – Vol. 3. – № 29. – P. 841–862.
5. Gallier J. Logic for computer science: foundations of Automatic Theorem Proving / J. Gallier. – New York : Harper and Row, Inc., 1986.
6. Robinson J. A machine-oriented logic based on resolution principle / J. Robinson // Journal of the ACM. – 1965. – Vol. 12. – № 1. – P. 23–41.
7. Kanger S. Simplified proof method for elementary logic / S. Kanger – Comp. Program. and Form. Sys. : Stud. in Logic. – Amsterdam : North-Holl., Publ. Co., 1963. – P. 87–93.
8. Lyaletski A. Gentzen calculi and admissible substitutions / A. Lyaletski. – Actes Preliminaieres, du Symposium Franco-

Sovietique «Informatika-91». – Grenoble, France. – 16–19 October, 1991. – P. 99–111.
9. Gentzen G. Untersuchungen uber das Logische Schliessen / G. Gentzen. – Math. Z. – 1934. – Vol. 39. – P. 176–210.
10. Lyaletski A. Goal-driven inference search in classical propositional logic / A. Lyaletski, A. Paskevich. – Proc. International Workshop STRATEGIES'2001, Siena, Italy. – 2001. – P. 65–74.
11. Минц Г. Е. Теорема Эбрана / Г. Е. Минц // Математическая теория логического вывода. – М. : Наука, 1967. – С. 311–350.

A. Afonin

ON COMPUTER-ORIENTED SEQUENT-TYPE CALCULI FOR FIRST-ORDER CLASSICAL LOGIC

The paper is devoted to an approach to the construction of computer-oriented sequent-type calculi that is not required fulfilling the preliminary skolemization operation. Its peculiarity is demonstrated with the help of the construction of a special calculus being investigated on the soundness and completeness. Using the calculus, methods for complete extensions of the SLD-resolution both for sets of arbitrary clauses and for sets of usual formulas of the 1st order language are described.

УДК 518.74

Коляденко А. А.

ВИКОРИСТАННЯ ЗАСОБІВ АВТОМАТИЧНОГО ДОВЕДЕННЯ ТЕОРЕМ ДЛЯ ДОСЛІДЖЕННЯ МОДЕЛЕЙ КОНТРОЛЮ ДОСТУПУ НА БАЗІ РОЛЕЙ ТА ГЕНЕРАЦІЇ АВТОРИЗАЦІЙНИХ ТВЕРДЖЕНЬ

Розглянуто проблематику застосування засобів автоматичного доведення теорем для дослідження моделей контролю доступу на базі ролей. Запропоновано шляхи представлення моделей стандарту ANSI-INCITS 359-2004 Role Based Access Control як теорій першого порядку, дослідження їх властивостей та генерації авторизаційних рішень за допомогою ПЗ EProver.

1. Вступ

Одним з найпопулярніших підходів в цій галузі є контроль доступу на базі ролей (Role Based Access Control, або RBAC). Головна риса RBAC зводиться до того, що користувач не отримує прямого доступу до ресурсів інформаційної системи. Натомість такий доступ реалізується опосередковано через поняття ролі. За такого підходу для надання доступу користувачеві до певного ресурсу інформаційної системи встановлюється відповідність користувача деякій ролі, яка, своєю чергою, отримує доступ безпосередньо до ресурсу. На думку автора, такий шлях має дві переваги:

- система контролю доступу стає більш гнучкою (користувач може бути від'єднаним або приєднаним до ролі без зміни її властивостей або під час зміни властивостей ролі. Ця зміна автоматично впливає на всіх користувачів, що є чи будуть приєднаними до ролі) порівняно, наприклад, з традиційними Access Control Lists та Discretionary Access Control [5];
- поняття ролей дає змогу вдало відображати структуру організації, яка експлуатує цільову інформаційну систему, на об'єкти механізмів контролю доступу (наприклад, посаду account manager можна авторизувати роллю RBAC Account Manager).

Завдяки цим перевагам контроль доступу на основі ролей реалізовано в багатьох провідних проектах програмного забезпечення (операційні