ЛОГИКО-МАТЕМАТИЧЕСКИЕ ОСНОВЫ ПРОБЛЕМЫ МОЗ
(Вычислительные системы)
1985 год Выпуск 107

УДК 510.662

ОДИН МЕТОД ПОИСКА ДОКАЗАТЕЛЬСТВА

А.А. Воронков

Введение

В последнее время в области автоматического доказательства теорем в классическом исчислении предикатов все большее значение приобретают системы поиска доказательств, отличные от метода резолюций [1]. Большинство таких систем основано на процедуре Правица [2], иначе называемой методом матричных редукций [3-5]. В [6] приведены количественные оценки, показывающие, что на формулах исчисления высказываний метод Правица ведет себя не менее эффективно, чем метод резолюций и некоторые его разновидности. Однако при реализации метода Правица в исчислении предикатов появляются некоторые недостатки. Отметим главные из них. Во-первых, области действия кванторов в этом методе или вся доказываемая формула, или ее большие части, т.е. переменные являются "глобальными". Из-за глобальности переменных при поиске доказательства приходится, как правило, осуществлять большое число удваиваний кванторов. Во-вторых, в методе отсутствуют хорошие механизмы возврата при выборе неправильного направления поиска. Вследствие этого алгоритм вынужден проделывать одну и ту же работу по несколько раз.

Эти и некоторые другие недостатки доставляют много неудобств при использовании процедуры Правица как метода поиска доказательства в исчислении предикатов. В данной работе мы опишем один алгоритм поиска доказательства, базирующийся на идеях, сходных с идеями метода Правица, и в то же время свободный от указанных недостатков: алгоритм DS.

Поиск вывода алгоритмом DS ведется "сверху-вниз", т.е. от аксиом к цели. Приведения доказываемой формулы к дизъюнктивной или конъюнктивной нормальной форме не требуется. Используется известная процедура унификации [I]. Ввиду направления поиска вывода алгоритм DS мы иногда будем называть прямым методом доказательства теорем. Локальность переменных в прямом методе достигается за счет того, что при поиске вывода части полученных подстановок постепенно отбрасываются и не участвуют в дальнейших унификациях. Из-за этого отпадает необходимость в удваивании некоторых кванторов. За счет введения порядка $\leq$ на доказываемой формуле, алгоритму DS надо искать не все выводы, а только согласованные с этим порядком.

Интересной особенностью метода является запись подстановок отдельно от секвенций. Аналогичный подход к отделению подстановок продемонстрирован в [5,7].

В §I даются основные определения и описывается формальная система D, на которой основан алгоритм. В §2 рассматривается модификация D_A этой системы, направленная на поиск вывода формулы A без удваиваний кванторов и определяется алгоритм DS. В §3 вводятся две важные тактики поиска доказательства - тактика избегания конъюнктов и тактика поглощения, позволяющие существенно сократить пространство поиска. Приводятся некоторые оценки длины секвенций, возникающих при поиске вывода.

§I. Основные понятия. Система D

Перед тем, как перейти к описанию системы D, дадим несколько определений. Будем считать, что у нас имеется набор предикатных символов A, B, C,... .

Понятия <u>переменной</u>, <u>терма</u> и <u>подстановки</u> термов вместо переменных определяются стандартным способом. n-ки переменных мы будем обозначать $\bar{x},\bar{y},\bar{z},\ldots$; n-ки термов - $\bar{r},\bar{s},\bar{t},\ldots$, а подстановки - $[\bar{x} \leftarrow \bar{t}]$.

<u>Элементарная формула</u> - это выражение вида $A^i(\bar{t})$ или $\neg A^i(t)$, где A - предикатный символ, i - индекс.

<u>Формулы</u> строятся по индукции.

I. Элементарная формула есть формула.

2. Если $A_1,\ldots,A_n$ - формулы, то $A_1\vee\ldots\vee A_n$ и $A_1\wedge\ldots\wedge A_n$ - также формулы.

3. Если A - формула, то $\exists\bar{x}A$ - также формула.

В дальнейшем мы будем считать дизъюнкцию и конъюнкцию коммутативными, таким образом, например, формулы $A\vee B$ и $B\vee A$ не раз -

личаются. Индексы в элементарные подформулы добавлены для того, чтобы отличать разные вхождения этих подформул.

Формула A <u>правильно построена,</u> если выполняются следующие условия:

I) все связанные переменные в A различны;

2) любые два разных вхождения одного и того же предикатного символа в A имеют разные индексы;

3) в A нет подформул вида $\exists\bar{x}\,(A_1 \vee \ldots \vee A_n)$, т.е. кванторы могут стоять только перед конъюнкциями или перед элементарными формулами.

Начиная с этого места, мы будем иметь дело только с правильно построенными формулами.

<u>Секвенция</u> - конечное множество $\{B_1, \ldots, B_n\}$ формул. Для удобства в обозначениях мы будем записывать формулы секвенции через запятую: $B_1, \ldots, B_n$.

<u>Ослабление</u> формулы A есть формула, полученная из A с помощью конечной последовательности замен подформул C вида $\exists\bar{x}\,B$ на $C \vee C_1$, где C_1 получается из C переименованием связанных переменных и заменой индексов у элементарных подформул на новые.

<u>Аксиомы системы D</u>:

$$\exists\bar{x}\,A^i \vee \varphi_1,\ \exists\bar{y}\,\neg A^j \vee \varphi_2,$$

где $\bar{x}$ $\bar{y}$ - n-ки переменных, возможно пустые, i,j - индексы, φ_1, φ_2 - формулы, возможно пустые ($\exists\bar{x}\,A$ для "пустого" $\bar{x}$ означает просто A, а $A \vee \varphi$ для "пустой" формулы φ означает A), и существуют n-ки термов $\bar{r}$ $\bar{s}$, такие, что $A^i[\bar{x} \leftarrow \bar{r}]$ совпадает с $A^j[\bar{y} \leftarrow \bar{s}]$.

<u>Правила вывода D:</u>

$$(\wedge) \qquad \frac{\Gamma_1,\ A_1[\bar{x} \leftarrow \bar{t}] \ \ldots\ \Gamma_m, A_m[\bar{x} \leftarrow \bar{t}]}{\Gamma_1, \ldots, \Gamma_m,\ \exists\bar{x}(A_1 \wedge \ldots \wedge A_m) \vee \varphi},$$

где $\bar{x}$ - n-ка переменных, возможно пустая φ - формула, возможно пустая, $\Gamma_1, \ldots, \Gamma_m$ - секвенции, $m \geq 2$;

$$(*) \qquad \frac{\Gamma, A^*}{\Gamma, A},$$

где A^* - ослабление формулы A.

Вывод формулы в системе D мы будем называть просто D-выводом.

Формула A <u>доказуема</u> в классическом исчислении предикатов, если таковой является формула, полученная из A вычеркиванием индексов. Формула A без кванторов <u>тождественно истинна</u>, если таковой является формула, полученная из A вычеркиванием индексов.

Для того чтобы доказать полноту системы D, введем новую <u>систему D'</u>. Последняя отличается от D тем, что ее аксиомы имеют вид Γ_1, Γ_2, где Γ_1 – аксиома системы D, Γ_2 – произвольная секвенция. Правила вывода D' те же, что у D.

<u>Скелет</u> формулы A есть формула, полученная из A вычеркиванием всех термов. Например, скелет формулы $\exists x(A^1(x,y,z) \wedge \exists u B^1(u,f(u)))$ есть $\exists x(A^1 \wedge \exists u B^1)$. Пусть Γ – секвенция вида $A_1, \dots, A_n$. <u>Порядком на Γ</u> мы назовем любой линейный порядок $\le$, заданный на множестве скелетов всех подформул формул $A_1, \dots, A_n$, имеющих вид $\exists \bar{x}(B_1 \wedge \dots \wedge B_m)$, где $\bar{x}$ – возможно пустая, такой, что для любых скелетов подформул C_1 C_2 указанного вида, если C_1 – подформула C_2, то $C_1 \le C_2$.

Пусть $\le$ – порядок на Γ, Π – D (D')-вывод секвенции Γ, в котором не применяется правило (*). Мы будем говорить, что Π <u>согласован с порядком $\le$</u>, если в Π нет ветвей вида

$$\cfrac{\Gamma_1, A_1[\bar{x} \leftarrow \bar{t}] \; \dots \; \Gamma_n, A_n[\bar{x} \leftarrow \bar{t}]}{\Gamma_1, \dots, \Gamma_n, \exists \bar{x}(A_1 \wedge \dots \wedge A_n) \vee \varphi_1}$$

$$\vdots$$

$$\cfrac{\Sigma_1, B_1[\bar{y} \leftarrow \bar{s}] \; \dots \; \Sigma_m, B_m[\bar{y} \leftarrow \bar{s}]}{\Sigma_1, \dots, \Sigma_m, \exists \bar{y}(B_1 \wedge \dots \wedge B_m) \vee \varphi_2}$$

таких, что $\exists \bar{y}(B_1 \wedge \dots \wedge B_m) \le \exists \bar{x}(A_1 \wedge \dots \wedge A_n)$.

ЛЕММА I. Пусть Π' – вывод секвенции Γ' в D' без применений правила (*), $\le$ – порядок на Γ'. Тогда существует подмножество Γ секвенции Γ' и вывод Π секвенции Γ в D без применений правила (*), такой, что любая секвенция Σ, входящая в Π, является подмножеством некоторой секвенции Σ', входящей в Π'. Если, кроме того, Π' согласован с порядком $\le$, то и Π согласован с порядком $\le$.

ДОКАЗАТЕЛЬСТВО ведется индукцией по длине вывода Π'. Если Γ' – аксиома, то утверждение леммы следует прямо из определения аксиом D' и D.

Пусть Π' имеет вид

$$\dfrac{\begin{matrix}\vdots\,\Pi'_1 & & \vdots\,\Pi'_n\\ \Gamma_1,\ A_1[\bar{x}\leftarrow\bar{t}] & \ldots & \Gamma_n,\ A_n[\bar{x}\leftarrow\bar{t}]\end{matrix}}{\Gamma_1,\ldots,\Gamma_n,\ \exists\bar{x}(A_1\wedge\ldots\wedge A_n)\vee\varphi}\ .$$

Применяя индукционное предположение к $\Pi'_1,\ldots,\Pi'_n$, получаем D-выводы $\Pi_1,\ldots,\Pi_n$ секвенций $\Sigma_1\subseteq\Gamma_1,\ A_1\ldots\ \Sigma_n\subseteq\Gamma_n,\ A_n$. Если существует Σ_i, $1\le i\le n$, содержащаяся в Γ_i, то в качестве Π можно взять

$$\begin{matrix}\vdots\,\Pi_i\\ \Sigma_i\end{matrix}\ .$$

Если же каждая Σ_i имеет вид $\Delta_i,\ A_i[\bar{x}\leftarrow\bar{t}]$, где $\Delta_i\subseteq\Gamma_i$, то в качестве Π можно взять

$$\dfrac{\begin{matrix}\vdots\,\Pi_1 & & \vdots\,\Pi_n\\ \Delta_1,\ A_1[\bar{x}\leftarrow\bar{t}] & \ldots & \Delta_n,\ A_n[\bar{x}\leftarrow\bar{t}]\end{matrix}}{\Delta_1,\ldots,\Delta_n,\exists\bar{x}(A_1\wedge\ldots\wedge A_n)\vee\varphi}\ .$$

Утверждение о согласованности Π с $\le$ проверяется непосредственно. Таким образом, лемма полностью доказана.

ТЕОРЕМА I. (Полнота системы D.) Пусть формула A доказуема в классическом исчислении предикатов. Тогда существует ослабление A^* формулы A, такое, что для любого порядка $\le$ на A^* существует согласованный с $\le$ вывод Π без применений правила (*) формулы A^* в D.

ДОКАЗАТЕЛЬСТВО. По теореме Эрбрана [8] существует ослабление A^* формулы A, такое, что формула B, полученная из A^* вычеркиванием кванторов и применением некоторой подстановки $[\bar{x}\leftarrow\bar{t}]$, тождественно истинна. Порядок $\leq$ на A^* индуцирует некоторый порядок на B, который мы обозначим тоже $\leq$. Вначале построим по индукции D'-вывод Π' формулы B, согласованный с $\leq$. На каждом шаге построения мы будем достраивать полученное к этому шагу дерево, пока требуемый вывод не будет построен. Для того чтобы гарантировать согласованность с порядком $\leq$, мы будем на каждом шаге подчеркивать некоторые подформулы, и на последующих шагах эти подформулы уже не использовать.

Шаг I. Поставим в корень дерева Π' секвенцию, состоящую из одной формулы B.

Шаг $(n+1)$. Если во всех листьях дерева Π' стоят аксиомы системы D', то построение закончено. В противном случае выберем стоящую в каком-либо листе Π' секвенцию Γ, не являющуюся аксиомой. Пусть $A_1 \wedge \ldots \wedge A_n$ – наибольшая относительно $\leq$ подформула из Γ, которая не была подчеркнута на предыдущих шагах. Тогда Γ имеет вид $\Sigma, (A_1 \wedge \ldots \wedge A_n) \vee \varphi$. Достроим Π' следующим образом:

$$\frac{\Sigma, (A_1\wedge\ldots\wedge A_n)\vee\varphi,\ A_1 \ldots \Sigma, (A_1\wedge\ldots\wedge A_n)\vee\varphi,\ A_n}{\Sigma,(A_1\wedge\ldots\wedge A_n)\vee\varphi}$$

и подчеркнем во всех вновь полученных секвенциях $\Sigma,(A_1\wedge\ldots\wedge A_n)\vee\varphi$, A_i подформулу $A_1\wedge\ldots\wedge A_n$ и все формулы, которые были подчеркнуты в Γ.

Так как подчеркнутая в одном месте подформула ниже уже не используется, то, во-первых, Π' будет согласован с $\leq$, а во-вторых, шагов будет сделано конечное число. Докажем, что после завершения всех шагов в листьях Π' будут стоять только аксиомы. В самом деле, пусть Γ стоит в листе Π' и Γ не аксиома. Положим $S \rightleftharpoons \{ E \mid E$ – элементарная и существует $C \in \Gamma$, такая, что C имеет вид $E \vee \varphi \}$. Индукцией по построению Π' можно доказать, что если все формулы из S сделать ложными (а это сделать можно, так как Γ не аксиома), то и вся формула B станет ложной. Таким образом, получено противоречие с тождественной истинностью B.

Из вывода Π', добавив в соответствующих местах кванторы, получаем D'-вывод Π_1' формулы A^*. Так как Π' согласован с индуцированным порядком, то Π_1' согласован с $\leq$. Применяя лемму I к выводу Π_1', секвенции $\{A^*\}$ и порядку $\leq$, получаем требуемый вывод Π. Теорема доказана.

§2. Система D_A. Алгоритм DS

Теперь, пользуясь результатом теоремы I, мы можем построить процедуру поиска выводимости формулы в классическом исчислении предикатов, основанную на поиске в системе D "сверху-вниз", т.е. от аксиом к цели.

Прежде всего, заметим, что любая формула B исчисления предикатов с помощью приведения к негативной нормальной форме [9], сколемизации [4] и добавления индексов к элементарным подформулам приводится к правильно построенной формуле A системы D, такой, что доказуемость B в классическом исчислении предикатов эквивалентно доказуемости A. При этом длина формулы A (число вхождений предикатных символов) равна длине B.

Пусть A – правильно построенная формула системы D. Посмотрим, какой вид может иметь D-вывод формулы A.

Во-первых, вывод в системе D обладает свойством подформульности. Следовательно, при поиске вывода нам достаточно искать вывод только на подформулах A. Во-вторых, в выводе могут участвовать не все подформулы формулы A, а только подформулы B специального вида, а именно, такие, что в A нет подформул вида $B \vee C$. Множество всех подформул такого вида мы обозначим M_A. Так как все формулы M_A являются подформулами формулы A, то любая формула $B \in M_A$ однозначно определяется своим скелетом и подстановкой термов вместо свободных переменных формулы B.

Дадим несколько определений. Подстановка θ_0 называется примером подстановки θ_1, если существует подстановка θ, такая, что $\theta_0 = \theta_1 \theta$. Если θ_0 – пример θ_1, то мы будем говорить, что θ_1 – более общая подстановка, чем θ_0. Если для всех $1 \le i \le n$ подстановка θ является примером θ_i, то θ называется унификатором подстановок $\theta_1, \ldots, \theta_n$. θ называется наиболее общим унификатором подстановок $\theta_1, \ldots, \theta_n$, если θ – унификатор $\theta_1, \ldots, \theta_n$ и любой другой унификатор $\theta_1, \ldots, \theta_n$ является примером θ. θ называется унификатором термов $\bar{r}$ и $\bar{s}$, если $\bar{r}\theta = \bar{s}\theta$. Через $\theta_{\bar{x}}$ мы обозначим подстановку, полученную из подстановки θ вычеркиванием ее части вида $[\bar{x} \leftarrow \bar{t}]$.

Опишем теперь модификацию D_A системы D, которая ориентирована на вывод данной замкнутой формулы A в D без правила (*).

Секвенция D_A: Пара $\Gamma;\ \theta$, где Γ – множество, состоящее из скелетов формул некоторого $\Gamma' \subseteq M_A$, θ – подстановка вида $[\bar{x} \leftarrow \bar{t}]$, где $\bar{x}$ – множество свободных переменных Γ'.

Аксиомы D_A:

$$\exists \bar{x}\, A^i \vee \varphi_1,\ \exists \bar{y}\, \neg A^j \vee \varphi_2;\ \theta_{\bar{x},\bar{y}},$$

где для некоторых $\bar{r},\bar{s}$ $A^i(\bar{r})$ и $\neg A^j(\bar{s})$ – элементарные подформулы A и θ – наиболее общий унификатор термов $\bar{r}$ и $\bar{s}$.

Правила вывода D_A:

$$(**)\qquad \frac{\Gamma_1,\ A_1;\ \theta_1\ \ldots \Gamma_n,\ A_n;\ \theta_n}{\Gamma_1,\ldots,\Gamma_n,\ \exists \bar{x}(A_1 \wedge \ldots \wedge A_n) \vee \varphi;\ \theta_{\bar{x}}},$$

где θ – наиболее общий унификатор $\theta_1,\ldots,\theta_n$ и в $\Gamma_1 \cup \ldots \cup \Gamma_n$ нет подформул формул $A_1,\ldots,A_n$.

ТЕОРЕМА 2. (Полнота и корректность D_A.) Пусть B – замкнутая формула. B доказуема в классическом исчислении предикатов тогда и только тогда, когда некоторое ослабление A формулы B доказуемо в D_A. Более того, если B доказуема, то существует ее ослабление A, такое, что для любого порядка $\leq$ на A существует D_A-вывод формулы A, согласованный с порядком $\leq$.

ДОКАЗАТЕЛЬСТВО. В одну сторону условие теоремы проверяется тривиально: по D_A-выводу A легко построить D-вывод A, и, следовательно, D-вывод B.

Пусть теперь B доказуема. Возьмем в качестве A формулу A^* из условия теоремы I. Для нее существует D-вывод, согласованный с порядком $\leq$. Запишем в этом D-выводе вместо секвенций их скелеты и подстановки. При этом еще не получается D_A-вывод, так как подстановки θ_i, записанные рядом с секвенциями, не являются наиболее общими. Заменив эти подстановки θ_i на наиболее общие θ'_i, получаем D_A-вывод формулы A. Корректность наших построений вытекает из следующих легко доказываемых свойств подстановок:

I) если существует унификатор θ термов $\bar{r}$ и $\bar{s}$, то существует и наиболее общий унификатор θ' этих термов;

2) если для всех $1 \leq i \leq n$ θ_i – пример θ'_i, θ – унификатор $\theta_1,\ldots,\theta_n$ и θ' – наиболее общий унификатор $\theta'_1,\ldots,\theta'_n$, то θ – пример θ';

3) если θ - пример θ', то $\theta_{\bar{x}}$ - пример $\theta'_{\bar{x}}$.

Пользуясь результатом теоремы 2, мы теперь можем описать <u>алгоритм DS</u> установления выводимости в классическом исчислении предикатов.

Шаг I. Доказываемая формула B приводится к правильно построенной формуле A системы D.

Шаг 2. По формуле A строится множество M_A и выбирается порядок $\leq$ на A.

Шаг 3. Положим $P \rightleftharpoons \{\Gamma | \Gamma$ - аксиома $D_A\}$.

Шаг 4. Если в P есть секвенция $\{A\}$, то доказательство найдено и алгоритм заканчивает работу. Если $P=\emptyset$, то формула A заменяется на некоторое ее ослабление и мы возвращаемся к шагу 2.

Шаг 5. В A выбирается наименьшая относительно $\leq$ подформула C вида $\exists\bar{x}(A_1 \wedge \ldots \wedge A_n)$ из тех, которые до этого на шаге 5 не выбирались. Пусть $P_i = \{\Gamma | \Gamma \in P$ и $A_i \in \Gamma\}$, $1 \leq i \leq n$. Секвенции из P_i имеют вид $\Sigma_i, A_i;\ \theta_i$. Для всех секвенций $\Sigma_1, A_1;\ \theta_1 \in P_1, \ldots, \Sigma_n, A_n;\ \theta_n \in P_n$ проделаем следующую процедуру: если существует наиболее общий унификатор θ подстановок $\theta_1, \ldots, \theta_n$, то добавляем в P секвенцию $\Sigma_1, \ldots, \Sigma_n, \exists\bar{x}(A_1 \wedge \ldots \wedge A_n) \vee \varphi;\ \theta_{\bar{x}}$. После того, как мы проделаем это со всеми $\Gamma_1 \in P_1, \ldots, \Gamma_n \in P_n$, выбросим из P $P_1, \ldots, P_n$ (никакой согласованный с $\leq$ вывод не может дальше использовать эти секвенции). Возвращаемся к шагу 4.

На этом описание алгоритма заканчивается.

ТЕОРЕМА 3. (Полнота алгоритма DS.) *Имеют место следующие утверждения:*

1) если существует вывод формулы A в D_A, согласованный с порядком $\leq$ на A, то этот вывод будет найден алгоритмом DS;

2) при фиксированном ослаблении A алгоритм DS всегда делает конечное число шагов.

ДОКАЗАТЕЛЬСТВО. Первое утверждение прямо следует из того, что алгоритм DS ищет все выводы A, согласованные с порядком $\leq$. Второе очевидно, так как после выполнения шага 5 секвенции из P уже не могут содержать формул $A_1, \ldots, A_n$, и любая формула из P, отлична от A, будет выброшена из P на некотором шаге.

Чтобы пояснить изложенный материал, приведем пример D_A-вывода. Пусть доказываемая формула B имеет вид

$$\neg\exists x\,\forall y(F(y,x)\leftrightarrow\neg\exists z\,(F(y,z)\wedge F(z,y)))$$

(пример взят из [10]). Строим по В формулу А системы D:

$$A \rightleftharpoons \exists y(F^1(y,a)\wedge\exists z(F^2(y,z)\wedge F^3(z,y)))\vee$$
$$\vee\exists u(\neg F^4(u,a)\wedge(\neg F^5(u,f(u))\vee\neg F^6(f(u),u))).$$

Формулы из M_A имеют вид

$A_1 = F^1(y,a)$,
$A_2 = F^2(y,z)$,
$A_3 = F^3(z,y)$,
$A_4 = \neg F^4(u,a)$,
$A_5 = \neg F^5(u,f(u))\vee\neg F^6(f(u),u)$,
$A_6 = \exists z(A_2\wedge A_3)$,
$A_7 = \exists y(A_1\wedge A_6)\vee\exists u(A_4\wedge A_5)$.

В качестве $\leq$ выбираем $A_2\wedge A_3\leq A_1\wedge A_6\leq A_4\wedge A_5$. Для удобства D_A-вывод мы запишем в линейной форме:

$A_1, A_4;[y\leftarrow x_0,\ u\leftarrow x_0]$ (аксиома), (1)
$A_1, A_5;[u\leftarrow a,\ y\leftarrow f(a)]$ (аксиома), (2)
$A_3, A_4;[y\leftarrow a,\ z\leftarrow x_1,\ u\leftarrow x_1]$ (аксиома), (3)
$A_3, A_5;[z\leftarrow x_2,\ u\leftarrow x_2,\ y\leftarrow f(x_2)]$ (аксиома), (4)
$A_2, A_4;[z\leftarrow a,\ y\leftarrow x_3,\ u\leftarrow x_3]$ (аксиома), (5)
$A_2, A_5;[z\leftarrow x_4,\ u\leftarrow x_4,\ y\leftarrow f(x_4)]$ (аксиома), (6)
$A_6, A_4;[u\leftarrow a,\ y\leftarrow a]$ (из (3),(5)), (7)
$A_6, A_5;[u\leftarrow x_5,\ y\leftarrow f(x_5)]$ (из (4),(6)), (8)
$A_7, A_4;[u\leftarrow a]$ (из (I),(7)), (9)
$A_7, A_5;[u\leftarrow a]$ (из (2),(8)), (10)
A_7; (из (9),(I0)). (11)

§3. Понятия конъюнкта и поглощения

В этом параграфе будут даны два важных понятия: конъюнкта и поглощения, которые позволяют улучшить алгоритм DS. На протяжении всего параграфа мы будем считать, что у нас имеются фиксированная замкнутая формула А и порядок $\leq$ на A. Все рассматриваемые формулы будут элементами множества M_A. Выводом в системе $D_{\langle A,\leq\rangle}$ мы будем называть любой D_A-вывод, согласованный с $\leq$.

Пара формул B,C называется <u>конъюнктом</u>, если существует формула $\exists\bar{x}(A_1, \ldots ,A_n) \vee \varphi \in M_A$, такая, что $n \geq 2$, B – подформула A_1 и C – подформула A_n.

ТЕОРЕМА 4. *Пусть Π – вывод формулы A в $D_{\langle A,\leq\rangle}$ и Γ – секвенция из Π. Тогда любая пара формул $B,C \in \Gamma$ не является конъюнктом.*

ДОКАЗАТЕЛЬСТВО. Пусть Γ – секвенция из Π, $B,C \in \Gamma$. Предположим, что существуют $A_1, A_n \in M_A$, такие, что B – подформула A_1, C – подформула A_n и $\exists\bar{x}\,(A_1 \wedge \ldots \wedge A_n) \vee \varphi \in M_A$. Проследив всех потомков секвенции Γ в Π, получаем, что в Π есть ветвь вида

$$
\begin{array}{c}
\Gamma \\
\vdots \\
\dfrac{\Gamma_1, A_1 \quad \ldots \quad \Gamma_n, A_n}{\Gamma_1, \ldots, \Gamma_n, \exists\bar{x}(A_1 \wedge \ldots \wedge A_n) \vee \varphi} \\
\vdots \\
\dfrac{\Sigma_1, A_1 \quad \ldots \quad \Sigma_n, A_n}{\Sigma_1, \ldots, \Sigma_n, \exists\bar{x}(A_1 \wedge \ldots \wedge A_n) \vee \varphi}
\end{array}
$$

или наоборот, поменяв местами A_1 и A_n. Но так как для любого порядка $\leq$ выполняется $\exists\bar{x}(A_1 \wedge \ldots \wedge A_n) \leq \exists\bar{x}(A_1 \wedge \ldots \wedge A_n)$, то Π не согласован с $\leq$. Получили противоречие.

СЛЕДСТВИЕ. (Тактика избегания конъюнктов.) *Алгоритм DS сохраняет полноту, если при поиске вывода*

1) не включать на шаге 3 в список аксиом секвенции вида $\exists\bar{x}\,A^i \vee \varphi_1, \exists\bar{y}\,A^j \vee \varphi_2; \theta$, если пара $\exists\bar{x}\,A^i \vee \varphi_1$, $\exists\bar{y}\,A^j \vee \varphi_2$ – конъюнкт;

2) не применять на шаге 5 правило

$$\frac{\Gamma_1, A_1;\ \theta_1\ \dots\ \Gamma_n, A_n;\ \theta_n}{\Gamma_1,\dots,\Gamma_n,\ \exists\bar{x}\,(A_1\wedge\dots\wedge A_n)\vee\varphi;\theta_{\bar{x}}},$$

если в $\Gamma_1\cup\dots\cup\Gamma_n$ есть пара формул, являющаяся конъюнктом.

Мы будем говорить, что секвенция $\Gamma_1;\theta_1$ <u>поглощает</u> секвенцию $\Gamma_2;\ \theta_2$, если выполняются следующие условия:

I) для любой $B\in\Gamma_1$ существует $C\in\Gamma_2$, такая, что C – подформула B,

2) θ_2 – пример θ_1.

Секвенция Γ <u>выводима из секвенций $\Gamma_1,\dots,\Gamma_n$</u>, если существует $D_{\langle A,\le\rangle}$-вывод секвенции Γ, все верхние секвенции которого принадлежат множеству $\{\Gamma_1,\dots,\Gamma_n\}$.

ТЕОРЕМА 5. Пусть $\Gamma;\ \theta$ выводима из $\Gamma_1;\ \theta_1,\dots,\Gamma_n;\ \theta_n$, и $\Sigma_1;\sigma_1,\dots,\Sigma_m;\sigma_m$ – список секвенций, такой, что для любого $1\le i\le n$ существует $1\le j\le m$, такой, что $\Sigma_j;\ \sigma_j$ поглощает $\Gamma_i;\theta_i$. Тогда существует секвенция $\Sigma;\ \sigma$, такая, что $\Sigma;\sigma$ выводима из $\Sigma_1;\sigma_1\dots\Sigma_m;\sigma_m$ и $\Sigma;\sigma$ поглощает $\Gamma;\theta$.

ДОКАЗАТЕЛЬСТВО ведется индукцией по выводу Π. Для верхних секвенций вывода условие теоремы прямо вытекает из определения выводимости. Пусть, далее, в выводе Π встретилось применение правила

$$\frac{\Delta_1, A_1;\delta_1\ \dots\ \Delta_k, A_k;\delta_k}{\Delta_1,\dots,\Delta_k,\ \exists\bar{x}(A_1\wedge\dots\wedge A_k)\vee\varphi;\ \delta_{\bar{x}}}.$$

По индукционному предположению существуют секвенции $\Lambda_i;\ \lambda_i$, $1\le i\le k$, которые выводимы из $\Sigma_1;\sigma_1\ \dots\ \Sigma_m,\sigma_m$ и поглощают Δ_i, $A_i;\ \delta_i$. Если для некоторого i $A_i\notin\Lambda_i$, то, ввиду ограничения на правило (**), в λ_i нет частей вида $[\bar{x}\leftarrow\bar{t}]$ и, следовательно, $\delta_{\bar{x}}$ есть пример λ_i и $\Lambda_i;\ \lambda_i$ поглощает $\Delta_1,\dots,\Delta_k$, $\exists\bar{x}(A_1\wedge\dots\wedge A_k)\vee\varphi;\ \delta_{\bar{x}}$. Если же для всех $1\le i\le k$ $A_i\in\Lambda_i$, то Λ_i имеют вид $\Lambda_i', A_i;\ \lambda_i$. В этом случае мы можем применить правило

$$\frac{A_1', A_1; \lambda_1 \ \ldots \ A_k', A_k; \lambda_k}{A_1, \ldots, A_k, \exists \bar{x}(A_1 \wedge \ldots \wedge A_k) \vee \varphi; \lambda_{\bar{x}}}.$$

Нижняя секвенция этого применения правила удовлетворяет условиям теоремы.

СЛЕДСТВИЕ I. Пусть П - вывода A в $D_{\langle A, \leq \rangle}$ из $\Gamma; \theta, \Gamma_1; \theta_1 \ \ldots \ \Gamma_n; \theta_n$ и $\Gamma_1; \theta_1$ поглощает $\Gamma; \theta$. Тогда существует $D_{\langle A, \leq \rangle}$ - вывод $П_1$ формулы A из $\Gamma_1; \theta_1 \ \ldots \ \Gamma_n; \theta_n$, причем $П_1$ не длинней, чем П (под длиной вывода мы понимаем количество применений правила (**)).

СЛЕДСТВИЕ 2. (Тактика поглощения.) Алгоритм DS сохраняет полноту и корректность, если при поиске вывода

I) выбрасывать из списка P секвенции, которые поглощаются другими секвенциями из этого списка;

2) заменять в списке P секвенции $\Gamma, A_1, A_2; \theta$, где A_1 - подформула A_2 $\Gamma, A_1; \theta$.

ДОКАЗАТЕЛЬСТВО. Первое утверждение прямо следует из теоремы 5. Второе - секвенции $\Gamma, A_1, A_2; \theta$ и $\Gamma, A_1; \theta$ поглощают друг друга.

Пусть $M \subseteq M_A$ - множество формул. Назовем M <u>максимальным</u> множеством, если выполняются следующие условия:

I) для любых двух формул $A_1, A_2 \in M$, или пара A_1, A_2 - конъюнкт, или A_1 - подформула A_2, или A_2 - подформула A_1;

2) M нельзя расширить так, чтобы сохранялось первое.

ТЕОРЕМА 6. При использовании тактик избегания конъюнктов и поглощения число формул в любой секвенции из P не больше, чем число максимальных множеств.

Замена подформулы B вида $\exists \bar{x}\, C$ на $\exists \bar{x}\, C \vee \exists \bar{y}\, C_1$ в определении ослабления соответствует правилу удвоения квантора в методах автоматического доказательства теорем, основанных на процедуре Правица. Хорошо известно [4], что эти методы сохраняют полноту, если разрешить удваивать только самые внешние кванторы. То же самое можно доказать и в отношении алгоритма DS. Если в алгоритме

DS разрешить удваивать только самые внешние кванторы, то можно получить интересный результат о длине секвенции при поиске вывода на одном классе формул.

Пусть $\mathfrak{A}$ - класс формул B, таких, что у B нет подформул вида $\exists \bar{x}(A_1 \wedge \ldots \wedge A_n) \vee \exists \bar{y}(B_1 \wedge \ldots \wedge B_m)$ . . Класс $\mathfrak{A}$ можно охарактеризовать иначе следующим образом: формула B принадлежит $\mathfrak{A}$ тогда и только тогда, когда все множество M_B является максимальным.

СЛЕДСТВИЕ. Пусть B - формула класса $\mathfrak{A}$. Пусть при поиске вывода формулы B алгоритмом DS разрешается удваивать только самые внешние кванторы. Тогда при использовании тактик поглощения и избегания конъюнктов число формул в любой секвенции Г из P не превосходит числа удваиваний кванторов.

Отметим, что класс $\mathfrak{A}$ достаточно широк. Например, все формулы в конъюнктивной нормальной форме принадлежат классу $\mathfrak{A}$.

Заключение

Отметим в заключение особенности прямого метода, которые позволяют надеяться, что он будет достаточно эффективной процедурой доказательства.

1. Одним из достоинств метода является локальность переменных, достигающаяся благодаря постепенному выбрасыванию частей подстановок. Из-за этого происходит существенно меньше, чем в процедуре Правица, удваиваний кванторов.

2. В методе не используется дизъюнктивная или конъюнктивная нормальная форма, а приведение к правильно построенной формуле системы D не увеличивает длины доказываемой формулы.

3. Найденное алгоритмом доказательство легко перестраивается в вывод в известных системах, например в системе Генцена LK [11].

4. Краткость секвенций: как правило, секвенции из списка P по сложности можно сравнить с единичными дизъюнктами метода резолюций.

Отметим, что на некоторых классах формул прямой метод может вести себя как известные методы автоматического доказательства теорем, например, как позитивная единичная резолюция на множестве хорновых дизъюнктов [I2] или как разновидность обратного метода [I3] на формулах в конъюнктивной нормальной форме.

Автор благодарен Д.И.Свириденко за постоянную поддержку при проведении данной работы и В.Ю.Сазонову за множество полезных замечаний по форме и содержанию статьи.

Литература

I. РОБИНСОН Дж.А. Машинно-ориентированная логика, основанная на принципе резолюции. -Кибернетический сборник (новая серия), I970, вып. 7, с. I94-2I8.

2. PRAWITZ D. Proof procedure with matrix reduction.- In: Symp.on Automatic Demonstration.-Springer,1970,p.207-214.

3. BIEBEL W. Automated theorem proving.- Wiesbaden: Vieweg Verlag,1982.

4. ANDREWS P.B. Theorem proving via general matings.- JACM, 1981,v.28,N 2,p.193-214.

5. CAFERRA R. Proof by matrix reduction as plan+validation.- In: 6th Conf.on Automated Deduction.-Springer,1982,p.309-325.

6. BIBEL W. A comparative study of several proof procedures. - Artificial Intelligence Journal,1982,v.18,N 3,p.269-293.

7. PLAISTED D.A. Theorem proving with abstraction.- Artificial Intelligence Journal,1981,v.16,N 1,p.47-108.

8. МИНЦ Г.Е. Теорема Эрбрана. -В кн.: Математическая теория логического вывода. М., Наука, I967, с. 3II-350.

9. КЕЙСЛЕР Г., ЧЭН Ч.Ч. Теория моделей. -М.: Мир, I977.

I0. LOVELAND D.W. Mechanical Theorem proving by Model Elimination.- JACM,1968,v.15,N 2,p.236-251.

II. ГЕНЦЕН Г. Исследования логических выводов. -В кн.: Математическая теория логического вывода. М., Наука, I967, с.9-74.

I2. HANSHEN L., WOS L. Unit refutation and Horn sets. - JACM, 1974,v.21, N 4,p.590-605.

I3. МАСЛОВ С.Ю. Обратный метод установления выводимости для логических исчислений. -В кн.: Труды МИАН им. В.А.Стеклова, I968, вып. 98, с. 26-87.

Поступила в ред.-изд.отд.
II февраля I985 года