ЯЗЫКИ СПЕЦИФИКАЦИЙ И ЛОГИЧЕСКОЕ ПРОГРАММИРОВАНИЕ
(Вычислительные системы)
1988 год Выпуск 124

УДК 519.68

ПРЕДСТАВИМЫЕ ПРЕОБРАЗОВАНИЯ ФОРМУЛ

А.В. Манцивода

Настоящая работа посвящена некоторым вопросам автоматического доказательства теорем. Эта область прикладной логики привлекает внимание большого числа специалистов как у нас в стране, так и за рубежом [2,3]. Был получен целый ряд важных результатов [4,8, 9,13,14]. Заслуженным вниманием пользуются конструктивные аспекты математической логики и автоматического доказательства теорем в их приложении к программированию [6,7].

В данной работе рассматриваются некоторые "внутренние" проблемы одного метода автоматического доказательства теорем. В ней формулируется определение представимых преобразований формул, являющихся естественным обобщением метода инвариантных преобразований, предложенного в [4], рассматриваются условия корректности правил вывода, основанных на представимых преобразованиях.

В [4,5,10-12 и др.] исследовались вопросы корректности различных классов преобразований метода, изложенного в [4]. В §2, на основании результатов §1, дается полное описание условий корректности для всех преобразований данного метода.

Опишем основные понятия и обозначения, используемые в работе. Зафиксируем некоторую сигнатуру σ. Пусть L – множество всех формул первого порядка данной сигнатуры. Через буквы A,B,C,... будем обозначать формулы языка L; с помощью W, быть может, с индексами, – переменные для формул, т.е. те переменные, вместо которых можно подставлять формулы из L.

Зафиксируем кортеж $\bar{x} = \langle e_1,\dots,e_n,y_1,\dots,y_n\rangle$, где e_i и y_i, $i=\overline{1,n}$, – переменные, а также кванторный комплекс $Q\bar{x} \equiv \exists e_1 \forall y_1 \dots \exists e_n \forall y_n$. Этими обозначениями мы будем пользоваться до конца работы. Будем говорить, что формула $P\bar{u}F(\bar{u})$ из L, где $P\bar{u}$ – кван-

торная приставка, принадлежит классу T_Q, если $\bar{x} \subseteq \bar{u}$ и все переменные из $\bar{x}$ связаны с $P\bar{u}$ теми же кванторами и в той же последовательности, что и в $Q\bar{x}$.

В дальнейшем дизъюнктивную нормальную форму формулы A будем обозначать через [A].

Остальные определения и понятия можно найти в книгах по математической логике, например, в [I].

§I. Представимые преобразования

В параграфе дается определение представимых преобразований и формулируются условия их корректности. Сначала дадим несколько вспомогательных определений.

ОПРЕДЕЛЕНИЕ I. Назовем схемой выражение вида

$$\Phi = \bigvee_{i=1}^{m} (W_i \,\&\, A_i(\bar{x})) \vee C(\bar{x}) \quad , \qquad (1)$$

где $A_i(\bar{x}), C(\bar{x})$ принадлежат L, W_i – переменные для формул.

Очевидно, схема Φ выделяет в L некоторое подмножество, а именно, подмножество формул, получающихся из Φ подстановкой вместо W_i некоторых формул языка L.

ОПРЕДЕЛЕНИЕ 2. Конкретизацией схемы Φ вида (I) будет формула языка L, имеющая вид

$$F = P\bar{u}\Big(\bigvee_{i=1}^{m} (H_i(\bar{u}) \,\&\, A_i(\bar{x})) \vee C(\bar{x})\Big),$$

где $H_i(\bar{u})$, $1 \le i \le m$, принадлежат L, а $P\bar{u}$ – некоторая кванторная приставка.

Конкретизацию F схемы Φ назовем T_Q-конкретизацией, если $F \in T_Q$.

Следующие два определения вводят вспомогательные преобразования формул, используемые для определения представимых преобразований.

ОПРЕДЕЛЕНИЕ 3. Отображение φ: L → L назовем примитивным преобразованием формул, если существуют две схемы Φ и Φ' такие, что φ переводит любую конкретизацию

$$F = P\bar{u}\Big(\bigvee_{i=1}^{m} (H_i(\bar{u}) \,\&\, A_i(\bar{x})) \vee C(\bar{x})\Big)$$

схемы Φ вида (I) в соответствующую ей конкретизацию

$$F' = P\vec{u}\left(\bigvee_{i=1}^{m}(H_i(\vec{u}) \,\&\, B_i(\vec{x})) \vee D(\vec{x})\right)$$

схемы

$$\Phi' = \bigvee_{i=1}^{m}(W_i \,\&\, B_i(\vec{x})) \vee D(\vec{x}) \ .$$

Для F , не являющихся конкретизациями Φ ,полагаем $\varphi(F) = F$.

Заметим, что примитивное преобразование полностью определяется своими начальной и конечной схемами Φ и Φ' соответственно.

Примитивные преобразования можно рассматривать как некие "переписывающие правила", определенные на классах логических формул, причем применимость данного преобразования φ к данной формуле F определяется "унифицируемостью" F и начальной схемы Φ .

Пример примитивного преобразования:

$$\Phi = W \,\&\, (A \subseteq B),$$

$$\Phi' = W \,\&\, \forall z(z \in A \to z \in B).$$

ОПРЕДЕЛЕНИЕ 4. Преобразование $\varphi: L \to L$ назовем полупримитивным, если существуют такие примитивные преобразования $\varphi_1, \ldots, \varphi_n$ с общей начальной схемой Φ , что для любой F, на которой φ определено, существует H-конкретизация Φ такая, что $F \equiv H$ и $\varphi(F) \equiv \varphi_1(H) \,\&\, \ldots \,\&\, \varphi_m(H)$, и, кроме того, любая F из области определения φ эквивалентна некоторой конкретизации схемы Φ.

Полупримитивные преобразования ответственны за ветвление доказательства. Заметим также, что эквивалентность в данном опре - делении носит весьма неконструктивный характер и может в конкретных определениях преобразований трактоваться по-разному,например, как графическое равенство. Другой вариант такой трактовки будет рассмотрен в §2.

Перейдем непосредственно к представимым преобразованиям.

ОПРЕДЕЛЕНИЕ 5. Отображение $\varphi: L \to L$ назовем представимым преобразованием формул, если существует набор $\varphi_1, \ldots, \varphi_n$ полупримитивных преобразований такой, что $\varphi(F) = H$ тогда и только тогда, когда $\varphi_i(F) = H$ для некоторого i, $1 \le i \le m$.

Как видно из определения, представимые преобразования допускают несколько "точек входа". Определение 5 весьма недетерминированно, в частности, не требует однозначности.

Легко заметить, что далеко не все представимые преобразования являются корректными с логической точки зрения. Однако для каждой фиксированной области математики мы можем выделить те или иные классы преобразований, корректные в данной области.

Можно рассматривать разнообразные, как синтаксические, так и семантические варианты понятия корректности. В нашей работе мы будем пользоваться семантическим ее определением. Такой подход, в частности, позволяет нам "настраивать" условия корректности правил вывода на данную область математики или другую формализованную предметную область. Под корректностью (инвариантностью) мы здесь будем понимать следующее.

ОПРЕДЕЛЕНИЕ 6. Отображение $\varphi: L \to L$ назовем инвариантным преобразованием формул относительно класса моделей K для кванторного комплекса $Q\bar{x}$, если для любой $F \in T_Q$ из области определения φ выполняется $K \models F \equiv \varphi(F)$.

Несмотря на достаточную общность представимых преобразований, оказалось, что свойства их корректности могут быть описаны средствами того же языка, т.е. справедлива

ТЕОРЕМА I. Для любого представимого преобразования φ и произвольного кванторного комплекса $Q\bar{x}$ можно указать формулу G_φ языка L такую, что для любого класса K преобразование φ корректно относительно K для $Q\bar{x}$ тогда и только тогда, когда $K \models G_\varphi$.

Перед тем, как непосредственно перейти к доказательству теоремы, сформулируем несколько полезных лемм. Для этого введем одно вспомогательное определение: под корректностью (в узком смысле), в отличие от инвариантности, будем понимать следующее. Преобразование φ корректно относительно K для $Q\bar{x}$ тогда и только тогда, когда для любой $F \in T_Q$ из области определения φ верно $K \models \varphi(F) \to F$.

ЛЕММА I. Для любого примитивного преобразования φ и кванторного комплекса $Q\bar{x}$ можно построить $G \in L$ такую, что для любого K преобразование φ корректно относительно K для $Q\bar{x}$ тогда и только тогда, когда $K \models G$.

ДОКАЗАТЕЛЬСТВО. Следует найти для преобразования φ такую G из L, что для любого $\mathbb{K}$ выполнено $\mathbb{K} \models G$ тогда и только тогда, когда для произвольной конкретизации $F \in T_Q$ схемы Φ и соответствующей ей конкретизации $\varphi(F)$ схемы Φ' выполняется $\mathbb{K} \models \varphi(F) \to F$.

Через $H_i(\bar{e},\bar{z})$, $i = \overline{1,n}$, где $\bar{e} = \langle e_1,\dots,e_n\rangle$, $\bar{z} = \langle z_1,\dots,z_n\rangle$, обозначим формулу со свободными переменными $e_1,\dots,e_i$, $z_1,\dots,z_i$, имеющую вид: $\forall e_{i+1} \exists z_{i+1} \dots \forall e_n \exists z_n \neg C(\bar{e},\bar{z})$, где $C(\bar{e},\bar{z})$ отличается от $C(\bar{x})$ тем, что каждая переменная y_j заменена в ней на z_j. Выберем в качестве G формулу $G_1 \vee G_2$, где

$$G_1 = R\Big(\bigvee_{i=1}^{m}((A_i(\bar{x}) \to (\&_{j=1}^{n} H_j(\bar{e},\bar{z}) \,\&\, \bar{y} \neq \bar{z})) \,\&\, A_i(\bar{x})) \vee C(\bar{x})\Big),$$

$$G_2 = \bar{R}\Big(\&_{i=1}^{m}((A_i(\bar{x}) \,\&\, ((\&_{j=1}^{n} H_j(\bar{e},\bar{z})) \to \bar{y} = \bar{z})) \vee \neg B_i(\bar{x})) \,\&\, \neg D(\bar{x})\Big),$$

R – кванторная приставка вида $\exists e_1 \exists z_1 \forall y_1 \dots \exists e_n \exists z_n \forall y_n$, $\bar{R}$ – кванторная приставка, "обратная" к R, т.е. имеющая вид $\forall e_1 \forall z_1 \exists y_1 \dots \forall e_n \forall z_n \exists y_n$. Вообще, $\overline{P\bar{x}}, \overline{Q\bar{x}}, \dots$ будут везде в дальнейшем обозначать кванторные приставки, обратные к $P\bar{x}, Q\bar{x}, \dots$ Докажем, что эта формула и будет искомой.

Необходимость. Предположим, что G ложна на $\mathbb{K}$. Тогда существует такая модель $\mathcal{M} \in \mathbb{K}$, что $\mathcal{M} = \neg G_1 \,\&\, \neg G_2$. Легко убедиться, что G_1 является T_Q-конкретизацией схемы. Кроме того,

$$\varphi(G_1) = R\Big(\bigvee_{i=1}^{m}((A_i(\bar{x}) \to (\&_{j=1}^{n} H_j(\bar{e},\bar{z}) \,\&\, \bar{y} \neq \bar{z})) \,\&\, B_i(\bar{x})) \vee D(\bar{x})\Big).$$

Очевидно, что $\varphi(G_1) \equiv \neg G_2$, откуда следует, что $\mathcal{M} \models \varphi(G_1)$. Значит, $\mathcal{M} \models \varphi(G_1) \,\&\, \neg G_1$, $\mathbb{K} \not\models \varphi(G_1) \to G_1$, и преобразование φ некорректно.

Достаточность. Пусть теперь $\mathbb{K} \models G$. Предположим, что φ некорректно.

В этом случае существуют модель $\mathcal{M} \in \mathbb{K}$ и T_Q-конкретизация $F = P\bar{u}\Big(\bigvee_{i=1}^{m}(E_i(\bar{v},\bar{w},\bar{e},\bar{y}) \,\&\, A_i(\bar{e},\bar{y})) \vee C(\bar{e},\bar{y})\Big)$ начальной схемы Φ такие, что $\mathcal{M} \models \neg F \,\&\, \varphi(F)$, где

$$\varphi(F) = P\bar{u}\Big(\bigvee_{i=1}^{m}(E_i(\bar{v},\bar{w},\bar{e},\bar{y}) \,\&\, B_j(\bar{e},\bar{y})) \vee D(\bar{e},\bar{y})\Big).$$

Здесь кортежи $\bar{v}$ и $\bar{w}$ состоят из тех переменных кортежа $\bar{u}$, которые не входят в $\bar{e}$ и $\bar{y}$ и связаны в $P\bar{u}$ кванторами существования и всеобщности соответственно.

Сначала рассмотрим случай, когда $\mathcal{M} \models G_1$.

Предварительно заметим, что если формула $Q\bar{x}C(\bar{x})$ истинна на $\mathcal{M}$, то преобразование φ корректно на $\mathcal{M}$. Это легко следует из того, что даже в том случае, когда все W_i будут превращены в тождественно ложные формулы (наихудший вариант), получившаяся конкретизация все равно останется истинной. Докажем теперь, что из G_1 всегда следует $Q\bar{x}C(\bar{x})$. Доказательство проведем так: покажем, что $\overline{Q\bar{x}}\,\neg C(\bar{x}) \to \neg G_1$, откуда уже будет очевидным образом следовать импликация $G_1 \to Q\bar{x}C(\bar{x})$.

Итак, пусть выполняется $\overline{Q\bar{x}}\,\neg C(\bar{x})$. Нам достаточно указать скулемовские функции формулы

$$\neg G_1 = \bar{R}\Big(\&_{i=1}^{m}\big((A_i(\bar{x}) \,\&\, (\&_{j=1}^{n} H_j(\bar{e},\bar{z}) \to \bar{y} = \bar{z}) \vee \neg A_i(\bar{x})\big) \,\&\, \neg C(\bar{x})\Big)$$

для переменных кортежа $\bar{y}$. Именно они связаны в кванторной приставке $\bar{R}$ кванторами существования. Несложно проверить, что мы можем выбрать для y_k в формуле $\neg G_1$ следующую скулемовскую функцию:

$$g_k(e_1,\ldots,e_k,z_1,\ldots,z_k) = \begin{cases} z_k, & \text{если } H_k(\bar{e},\bar{z}), \\ f_k(e_1,\ldots,e_k), & \text{если } \neg H_k(\bar{e},\bar{z}), \end{cases}$$

где $f_k(e_1,\ldots,e_k)$ – некоторая скулемовская функция для y_k в формуле $\overline{Q\bar{x}}\,\neg C(\bar{x})$, очевидно, такая существует. Отсюда следует, что если $\mathcal{M} \models G_1$, то $\mathcal{M} \models Q\bar{x}\,C(\bar{x})$, а значит, любая конкретизация схемы Φ не может быть ложной на $\mathcal{M}$ и, следовательно, $\mathcal{M} \models \varphi(F) \to F$, что противоречит выбору F и $\mathcal{M}$.

Пусть $\mathcal{M} \models G_2$. Запишем формулу $\neg F$, заменив все вхождения y_i, $i = \overline{1,n}$, на переменные z_i:

$$\neg F' = \bar{P}\bar{u}'\Big(\&_{i=1}^{m}(\neg E_i(\bar{v},\bar{w},\bar{e},\bar{z}) \vee \neg A_i(\bar{e},\bar{z})) \,\&\, \neg C(\bar{e},\bar{z})\Big),$$

где $\bar{u}'$ получается из $\bar{u}$ заменой всех y_i на z_i. Очевидным образом $\mathcal{M} \models \neg F'$.

Выберем наборы элементов $\tilde{\bar{v}},\tilde{\bar{w}},\tilde{\bar{e}},\tilde{\bar{y}},\tilde{\bar{z}} \in |\mathcal{M}|$ так. Пусть для всех i, $i < k$, элементы, соответствующие переменным u_i и u'_i, уже выбраны. Тогда элементы, соответствующие u_k и u'_k, выберем так:

1. $u_k = u'_k = v_j$ для некоторого j. Тогда если $f_{j1}(u_1, \ldots, u_{k-1})$ - скулемовская функция v_j в формуле $\varphi(F)$, то $\tilde{v}_j = \tilde{u}_k = \tilde{u}'_k = f_{j1}(\tilde{u}_1, \ldots, \tilde{u}_{k-1})$.

2. $u_k = u'_k = w_j$ для некоторого j. Тогда если $f_{j2}(u'_1, \ldots, u'_{k-1})$ - скулемовская функция w_j в формуле $\neg F'$, то $\tilde{w}_j = \tilde{u}_k = \tilde{u}'_k = f_{j2}(\tilde{u}'_1, \ldots, \tilde{u}'_{k-1})$.

3. $u_k = u'_k = e_j$ для некоторого j. Тогда если $f_{j3}(u_1, \ldots, u_{k-1})$ - скулемовская функция e_j в формуле $\varphi(F)$, то $\tilde{e}_j = \tilde{u}_k = \tilde{u}'_k = f_{j3}(\tilde{u}_1, \ldots, \tilde{u}_{k-1})$.

4. $u_k = y_k$, а $u'_k = z_j$ для некоторого j. Тогда если $f_{j4}(u'_1, \ldots, u'_{k-1})$ - скулемовская функция $\neg F$ для z_j, то $\tilde{z}_j = \tilde{u}'_k = f_{j4}(\tilde{u}'_1, \ldots, \tilde{u}'_k)$. Выбрав $\tilde{z}_j$, найдем $\tilde{y}_j$: если $f_{j5}(e_1, \ldots, e_j, z_1, \ldots, z_j)$ - скулемовская функция y_j в формуле G_2, то $\tilde{y}_j = \tilde{u}_k = f_{j5}(\tilde{e}_1, \ldots, \tilde{e}_j, \tilde{z}_1, \ldots, \tilde{z}_j)$.

Пусть искомые наборы получены. Из способа их выбора ясно, что на $\mathcal{M}$ должны выполняться следующие три формулы:

$$\&_{i=1}^{m} (\neg E_i(\tilde{\bar{v}},\tilde{\bar{w}},\tilde{\bar{e}},\tilde{\bar{z}}) \vee \neg A_i(\tilde{\bar{e}},\tilde{\bar{z}})) \;\&\; \neg C(\tilde{\bar{e}},\tilde{\bar{z}}),$$

$$\vee_{i=1}^{m} (E_i(\tilde{\bar{v}},\tilde{\bar{w}},\tilde{\bar{e}},\tilde{\bar{y}}) \;\&\; B_i(\tilde{\bar{e}},\tilde{\bar{y}})) \vee D(\tilde{\bar{e}},\tilde{\bar{y}}),$$

$$\&_{i=1}^{m} (A_i(\tilde{\bar{e}},\tilde{\bar{y}}) \;\&\; (\&_{j=1}^{n} H_j(\tilde{\bar{e}},\tilde{\bar{z}}) \to \tilde{\bar{y}} = \tilde{\bar{z}}) \vee \neg B_i(\tilde{\bar{e}},\tilde{\bar{y}})) \;\&\; \neg D(\tilde{\bar{e}},\tilde{\bar{y}}).$$

Рутинной проверкой устанавливается, что эта система противоречива. Из этого следует, что противоречивой является и система G_2, $\neg F'$, $\varphi(F)$: если G_2 и $\varphi(F)$ истинны на $\mathcal{M}$, то на $\mathcal{M}$ необходимо истинна и F, что доказывает корректность преобразования φ в случае $\mathcal{M} \models G_2$. Окончательно получаем: если $K \models G$, то φ корректно относительно K для $Q\bar{x}$. Лемма доказана.

Заметим, что примитивные преобразования абсолютно симметричны: каждому такому преобразованию с начальной схемой Φ и конец -

ной Φ' соответствует обратное ему с начальной схемой Φ' и конечной Φ. Отсюда, в частности, следует, что для примитивных преобразований теорема I выполняется: формулой G_φ из ее условия будет $\bar{G}_\varphi \& \bar{G}_{\varphi'}$, где $\bar{G}_\varphi$ - формула из леммы I для примитивного преобразования φ, формула $\bar{G}_{\varphi'}$ - для обратного ему преобразования φ'.

Зафиксируем теперь некоторое представимое преобразование, обозначив его через φ. Пусть оно определено с помощью полупримитивных преобразований $\varphi_1, \ldots, \varphi_k$, которые, в свою очередь, зависят от примитивных преобразований $\varphi_1^1, \ldots, \varphi_1^{m_1}; \ldots; \varphi_k^1, \ldots, \varphi_k^{m_k}$ соответственно. Пользуясь леммой I, мы можем найти формулы, описывающие условия корректности данных примитивных преобразований относительно класса моделей $\mathbf{K}$ для кванторного комплекса $Q\bar{x}$. Обозначим их через $G_1^1, \ldots, G_1^{m_1}; \ldots; G_k^1, \ldots, G_k^{m_k}$.

ЛЕММА 2. Представимое преобразование φ корректно относительно класса моделей $\mathbf{K}$ для кванторного комплекса $Q\bar{x}$ тогда и только тогда, когда на $\mathbf{K}$ истинна формула $G_1 = \&_{i=1}^{k} (\vee_{j=1}^{m} G_i^j)$.

ДОКАЗАТЕЛЬСТВО. Необходимость. Предположим, что $\mathbf{K} \not\models G_1$. Следовательно, существует такая модель $\mathcal{M}$, что $\mathcal{M} \not\models G_1$. Это значит, что мы можем указать полупримитивное преобразование φ_p со свойством $\mathcal{M} \not\models \vee_{j=1}^{m_p} G_p^j$. Отсюда следует, что на $\mathcal{M}$ истинна $\&_{j=1}^{m_p} \neg G_p^j$. Из леммы I ясно, что для любого примитивного преобразования φ_p^j выражение G_p^j имеет вид $G_{p1}^j \vee G_{p2}^j$. Так как начальная схема всех φ_p^j по определению полупримитивного преобразования одинакова, то для всех j, $j=\overline{1,m_p}$, G_{p1}^j будет одна и та же. Поскольку G_{p1}^j находится в области определения всех φ_p^j, то, по свойствам полупримитивного преобразования, существует F, $F \equiv G_{p1}^j$, которая находится в области определения φ_p. Применив φ_p к F, мы получим формулу H, $H \equiv \varphi_p^1(G_{p1}^j) \& \ldots \& \varphi_p^{m_p}(G_{p1}^j)$. Чтобы преобразование было корректным, нам требуется, чтобы на $\mathcal{M}$ была истинна имплика-

ция $\varphi_p^1(G_{p1}^j) \& \ldots \& \varphi_p^{m_p}(G_{p1}^j) \to G_{p1}^j$. Но так как $\mathcal{M} \models \&_{j=1}^{m_p} \neg G_p^j$, то

все φ_p^j некорректны на $\mathcal{M}$, и поэтому $\mathcal{M} \models \varphi_p^1(G_{p1}^j) \& \ldots \& \varphi_p^{m_p}(G_{p1}^j)$ и $\mathcal{M} \not\models G_{p1}^j$. Отсюда следует, что φ_p, а значит, и φ на K некорректны.

Достаточность. Предположим, что $K \models G_1$, формула F находится в области определения φ и $\varphi(F) = H$. По определению представимых преобразований существует полупримитивное преобразование φ_p, такое, что $\varphi_p(F) = H$. Так как $K \models \&_{i=1}^{n} (\vee_{j=1}^{m_i} G_i^j)$, то $K \models \vee_{j=1}^{m_p} G_p^j$. Отсюда следует, что для любой модели $\mathcal{M}$ среди примитивных преобразований $\varphi_p^1, \ldots, \varphi_p^{m_p}$ есть преобразование с некоторым номером r, которое является корректным относительно $\mathcal{M}$ для $Q\bar{x}$. Обозначим через $\bar{F}$ конкретизацию начальной схемы преобразования φ_p, эквивалентную F. По определению, в этом случае $H \equiv \varphi_p^1(\bar{F}) \& \ldots \& \varphi_p^r(\bar{F}) \& \ldots \& \varphi_p^{m_p}(\bar{F})$. Чтобы φ было корректно на формуле F в модели $\mathcal{M}$, требуется, чтобы на $\mathcal{M}$ выполнялась импликация $\varphi_p^1(\bar{F}) \& \ldots \& \varphi_p^{m_p}(\bar{F}) \to \bar{F}$. Но это очевидным образом следует из того, что примитивное преобразование φ_p^r корректно на $\mathcal{M}$, а значит, верно $\mathcal{M} \models \varphi_p^r(\bar{F}) \to \bar{F}$. Из произвольности выбора модели $\mathcal{M}$ следует, что φ является корректным на K. Лемма доказана.

Перейдем к доказательству теоремы I. Нам осталось показать, что существует формула G_2 такая, что $K \models G_2$ тогда и только тогда, когда для любой F из области определения представимого преобразования φ выполняется $K \models F \to \varphi(F)$.

Как отмечалось выше, это условие вытекает из примитивных преобразований из леммы 2 в связи с их симметричностью. Пусть формула, описывающая условие корректности для примитивного преобразования, обратного φ_i^j, будет обозначена через $G_i'^j$.

Выберем в качестве формулы G_2 формулу вида $\&_{i=1}^{K} \&_{j=1}^{m_i} G_i'^j$. Докажем, что она удовлетворяет нужным нам требованиям.

Предположим сначала, что $K \models G_2$. Пусть F находится в области определения φ и существует модель $\mathcal{M}$ из K, такая что $\mathcal{M} \models F \& \neg\varphi(F)$.

По определению представимого преобразования существует полупримитивное преобразование φ_i такое, что F эквивалентно некото-

рой конкретизации H начальной схемы φ_i и, кроме того, $\varphi(F) \equiv \equiv \varphi_i^1(H) \& \ldots \& \varphi_i^{m_i}(H)$. Так как G_2 истинна на K, то, по ее свойствам, на K истинны все импликации $H \to \varphi_i^j(H)$, $j = \overline{1,m_i}$, а так как $\mathcal{M} \models F$, то $\mathcal{M} \models \varphi_i^1(H) \& \ldots \& \varphi_i^{m_i}(H)$ и, следовательно, $\mathcal{M} \models \varphi(F)$, что противоречит выбору $\mathcal{M}$.

Предположим теперь, что существует $\mathcal{M}$ из K такая, что $\mathcal{M} \not\models G_2$. Следовательно, найдутся такие i и j, что $\mathcal{M} \not\models G_i^j$. По лемме I, G_i^j имеет вид $G_{i1}^j \vee G_{i2}^j$, причем G_{i1}^j является конкретизацией начальной схемы преобразования φ_i^j, обратного φ_i^j. Следовательно, поскольку $\mathcal{M} \not\models G_i^j$ и φ_i^j симметрично, то $\mathcal{M} \not\models \varphi_i^j(G_{i1}^j) \to \to \varphi_i^j(\varphi_i^j(G_{i1}^j))$. Кроме того, существует формула H из области определения представимого преобразования φ такая, что $H \equiv \varphi_i^j(G_{i1}^j)$ и $\varphi(H) \equiv \varphi_i^1(\varphi_i^j(G_{i1}^j)) \& \ldots \& \varphi_i^{m_i}(\varphi_i^j(G_{i1}^j))$. Очевидно, что $\mathcal{M} \models H$ и $\mathcal{M} \models \varphi(H)$. Нам осталось заметить, что G_φ из условия теоремы имеет вид $G_1 \& G_2$, где G_1 – формула из леммы 2. Теорема доказана.

§2. Инвариантные преобразования формул

В [4] введены преобразования формул, являющиеся одной из основных составляющих метода инвариантных преобразований. Данный метод имеет интересные приложения в автоматическом доказательстве теорем и синтезе программ. Отличительной чертой метода является тот факт, что не все преобразования формул являются корректными с логической точки зрения: пользуясь ими без разбора, мы можем вполне успешно доказать и ложные формулы.

Как избежать некорректности? Здесь возможен следующий выход: выделить такие преобразования, с помощью которых мы могли бы доказать только те формулы, которые на данном классе моделей были бы истинными. Для этого, естественно, требуется найти критерии выбора таких преобразований формул.

Как уже было отмечено в начале работы, условия корректности для многих частных классов преобразований описаны в [4,5,I0-I2 и др.]. В этом параграфе будет установлено, что все три основных типа преобразований: ζ-, ρ- и η-преобразований – с точки зрения классической логики являются представимыми, и поэтому условия их

корректности легко получаются как следствие теоремы I. Кроме того, из этой же теоремы непосредственно вытекает, что если класс моделей имеет сигнатуру σ, то эти условия могут быть описаны некоторой формулой той же сигнатуры.

Для строгой формулировки определений преобразований метода потребуется еще одно ключевое понятие метода - строгая вложимость. Последняя представляет собой некоторую "конструктивную" имплика - цию в том смысле, что если формула B строго вложима в A, сим - волически $A \rhd B$, то $A \to B$ выводима в интуиционистской логике. Более того, проверка строгой вложимости представляет собой разрешимую проблему. Естественно, далеко не каждая интуиционистски доказуемая импликация может быть успешно проверена с помощью стро - гой вложимости. Ее формальное определение весьма громоздко, поэтому мы ограничимся только этими замечаниями, дополнительно приведя в качестве примера всего три из десяти пунктов индуктивного определения строгой вложимости [5]:

I. Если A и B атомны, то $A \rhd B$ тогда и только тогда, когда $A = B$.

2. Если $B = B_1 \vee \ldots \vee B_n$, то $B \rhd A$ тогда и только тогда, когда $B_1 \rhd A, \ldots, B_n \rhd A$.

3. Если $A = \neg A_1$ и $B = \neg B_1$, то $B \rhd A$ тогда и только тогда, когда $A_1 \rhd B_1$.

Несложно убедиться, что строгая вложимость имеет весьма естественную природу.

Перейдем теперь непосредственно к преобразованиям формул. Первый вид преобразований, так называемые ζ-преобразования формул, служит инструментом для "накопления" информации в посылке доказательств. В частности, если мы доказываем утверждение

$$\Phi = \begin{cases} \text{дано: } A, B, \ldots, \\ \text{доказать: } C, D, \ldots \end{cases}$$

и есть аксиома данной области математики вида $A \to E$, то мы переходим к доказательству

$$\Phi' = \begin{cases} \text{дано: } A, B, \ldots, E, \\ \text{доказать: } C, D, \ldots \end{cases}$$

В некотором смысле такое преобразование является аналогом правила модус поненс: если мы считаем, что выполняется A и знаем, что $A \to E$, то мы можем считать, что выполняется E. Конечно, реальное определение ζ-преобразования выглядит значительно сложнее, чем в нашем простом примере.

ОПРЕДЕЛЕНИЕ 7. Формуле

$$A = R\bar{x}(B_1(\bar{x}) \;\&\; B_2(\bar{x}) \to C(\bar{x}))$$

поставим в соответствие преобразование ζ_A такое, что если

$$F = P\bar{u}(H_1(\bar{u}) \;\&\; (H_2(\bar{u}) \vee H_3(\bar{u})) \to G(\bar{u})) \;,$$

причем $H_1(\bar{u}) \rhd B_1(\bar{x})$ и $H_2(\bar{u}) \rhd B_2(\bar{x})$, то

$$\zeta_A(F) = P\bar{u}(H_1(\bar{u}) \;\&\; (H_2(\bar{u}) \;\&\; C(\bar{x}) \vee H_3(\bar{u})) \to G(\bar{u})) \;.$$

В противном случае $\zeta_A(F) = F$.

Второй важный класс преобразований - ρ-преобразования - является аналогом выделения лемм в содержательной математике. Например, если

$$\Phi = \begin{cases} \text{дано: } A, B, \ldots, \\ \text{доказать: } C, D, \ldots \end{cases}$$

и известно, что $(A_1 \to C_1) \to (A \to C)$ является аксиомой данной области математики, то для доказательства Φ нам достаточно доказать

$$\Phi' = \begin{cases} \text{дано: } A, B, \ldots, A_1, \\ \text{доказать: } C_1, \end{cases} \qquad \Phi'' = \begin{cases} \text{дано: } A, B, \ldots, \\ \text{доказать: } D, \ldots, \end{cases}$$

где Φ' и есть лемма, в которой сформулирована подцель: доказательство утверждения C. Строгое определение ρ-преобразования следующее.

ОПРЕДЕЛЕНИЕ 8. Формуле

$$A = \bar{x}((D(\bar{x}) \to E(\bar{x})) \to (B(\bar{x}) \to C(\bar{x})))$$

поставим в соответствие ρ_A-преобразование такое, что если

$$F = P\bar{u}(H(\bar{u}) \to C(\bar{x}) \;\&\; G(\bar{u})) \;,$$

причем $H(\bar{u}) \rhd B(\bar{x})$, то

$$\rho_A(F) = P\bar{u}(H(\bar{u}) \to G(\bar{u})) \;\&\; P\bar{u}(H(\bar{u}) \;\&\; D(\bar{x}) \to E(\bar{x})) \;.$$

В противном случае $\rho_A(F) = F$.

Последний класс преобразований формул, которые мы рассмотрим, есть η-преобразования. Вообще, η-преобразования есть частный случай ρ-преобразований, но настолько важный, что они были выделены в специальный класс хотя бы потому, что все определения понятий, используемых в доказательстве, вводятся через η-преобразования формул.

В [4] было введено следующее определение η-преобразований.

ОПРЕДЕЛЕНИЕ 9. Формуле

$$\forall \bar{x}((B(\bar{x}) \to C(\bar{x})) \equiv D(\bar{x}))$$

поставим в соответствие преобразование $\eta_A: L \to L$ такое, что если

$$F = P\bar{u}(H(\bar{u}) \to D(\bar{x}) \,\&\, G(\bar{u})),$$

причем $H(\bar{u}) \rhd B(\bar{x})$, то

$$\eta_A(F) = P\bar{u}(H(\bar{u}) \to C(\bar{x}) \,\&\, G(\bar{u})).$$

В противном случае $\eta_A(F) = F$.

Для частного случая η_A-преобразований, когда условие $H(\bar{u}) \rhd B(\bar{x})$ заменено на конъюнктивное вхождение, был получен следующий результат [4]: если $K \models A$, то η_A-преобразование, соответствующее A, является инвариантным.

Надо сказать, что определение 9 не совсем полно отражает специфику применения содержательных аналогов η-преобразований, т.е. применения определения некоторого понятия в процессе доказательства. В качестве примера рассмотрим определение открытого множества топологического пространства:

$$\forall M(\forall x(x \in M \to \text{вн}(x,M)) \equiv \text{откр}(M)),$$

где откр(M) означает "M открытое", а предикат вн(x,M) - "x есть внутренняя точка M".

В формуле F есть "внутренняя" кванторная приставка $\forall \bar{x}$, которой нет в формуле A из определения 9 и которая, следовательно, не учитывается в теореме 5. А так как такие кванторные приставки присутствуют в определениях многих очень важных математических понятий: функции, группы и др., то ясна необходимость введения нового более общего определения η-преобразования.

ОПРЕДЕЛЕНИЕ 10. Формуле

$$A = \forall \bar{x}(S\bar{y}(B(\bar{x},\bar{y}) \to C(\bar{x},\bar{y})) \equiv T\bar{z}D(\bar{x},\bar{z})),$$

где $S\bar{y}$, $T\bar{z}$, $\forall \bar{x}$ - кванторные приставки, поставим в соответствие преобразование $\bar{\eta}_A$ такое, что если

$$F = P\bar{u}(H(\bar{u}) \to D(\bar{x},\bar{z}) \,\&\, E(\bar{u})),$$

где $H(\bar{u}) \rhd B(\bar{x},\bar{y})$, переменные кортежей $\bar{y}$ и $\bar{z}$ связаны в $P\bar{u}$ теми же кванторами и в той же последовательности, что и в $S\bar{y}$, и в $T\bar{z}$ соответственно, то

$$\bar{\eta}_A(F) = P\bar{u}(H(\bar{u}) \to C(\bar{x},\bar{y}) \,\&\, E(\bar{u})).$$

В противном случае $\bar{\eta}_A(F) = F$.

Сформулируем основную теорему данного параграфа.

ТЕОРЕМА 2. Все преобразования формул метода инвариантных преобразований являются представимыми.

В связи с недостатком места, доказательство теоремы мы опускаем. Отметим только, что оно существенно опирается на свойства строгой вложимости [I5].

СЛЕДСТВИЕ. Для любого преобразования формул φ метода инвариантных преобразований существует формула G_φ той же сигнатуры такая, что φ инвариантно относительно класса моделей $\mathbf{K}$ для кванторного комплекса $\mathfrak{Q}$ тогда и только тогда, когда $\mathbf{K} = G_\varphi$.

Это утверждение легко следует из теорем I и 2.

В заключение отметим, что из результатов работы следует, что нам требуется наложить достаточно сильные условия на преобразование, чтобы оно оказалось корректным. В [I0,II] показано, что несколько ограничив свободу применения преобразований, т.е. сузив область применения, мы можем значительно улучшить ситуацию, например, любое η-преобразование становится корректным.

Литература

I. ЕРШОВ Ю.Л., ПАЛЮТИН Е.А. Математическая логика.-М.:Наука, I979. - 320 с.

2. ВОРОНКОВ А.А., ДЕГТЯРЕВ А.И. Автоматическое доказательство теорем. I //Кибернетика. - I986. - №3. - С.27-33.

3. ДЕГТЯРЕВ А.И., ВОРОНКОВ А.А. Методы управления равенством в машинном доказательстве теорем //Кибернетика. - I986. -№3.-С.34-4I.

4. МАРТЬЯНОВ В.И. Методы задания и частичного построения теории на ЭВМ //Кибернетика. - I982. -№6. -С. I02-II0.

5. МАРТЬЯНОВ В.И. Об инвариантных преобразованиях формул //Мат. заметки. - I984. -Т.36, №6. - С. 57I-58I.

6. ГОНЧАРОВ С.С., СВИРИДЕНКО Д.И. Σ-программирование //Логико-математические основы проблемы МОЗ. - Новосибирск, I985.-Вып. I07: Вычислительные системы. - С.3-29.

7. БОРЩЕВ В.Б. Пролог - основные идеи и конструкции //Прикладная информатика. - I986. -№2. -С. 49-76.

8. РОБИНСОН Дж. Машинно-ориентированная логика, основанная на принципе резолюции //Кибернетич.сб., нов.серия.-М., I970.-Вып. 7. -С. I94-2I8.

9. BLEDSOE W.W. Non-resolution theorem proving// Artif.Intelligence.- 1977.- V.1. - P.1-35.

10. МАНЦИВОДА А.В. Об одном классе преобразований формул /Ред. журн. "Сиб. мат.журн.". - Новосибирск, 1985.-15 с. -Деп. в ВИНИТИ № 5878-85.

11. МАНЦИВОДА А.В. О преобразованиях, соответствующих определениям //Всесоюз. конференция по проблемам теоретической кибернетики, Иркутск, сентябрь, 1985: Тез.докл.-Т.1. - Иркутск,1985. - С. 104-105.

12. НАНСАЛМАА Н. О $\tilde{\zeta}$-преобразованиях формул //Там же.-С.146-147.

13. ПОПОВ С.В. Диаграммы выводов в секвенциальных исчислениях //Проблемы кибернетики. - М., 1984. - Вып. 41. -С. 49-100.

14. ДЕГТЯРЕВ А.И., ЛЯЛЕЦКИЙ А.В. Логический вывод в системе автоматизации доказательств //Математические основы систем искусственного интеллекта. - Киев, 1981. - С.3-11.

15. МАНЦИВОДА А.В. О строгой вложимости //4 Всесоюз. конференция по применению методов математической логики, Таллин,май,1986 : Тез.докл. - Таллин, 1986. - Т.1. - С. 104-105.

Поступила в ред.-изд.отд.
18 апреля 1987 года