П Р И К Л А Д Н А Я   Л О Г И К А
(Вычислительные системы)

1986 год   Выпуск 116

УДК 519.714.7

ОБ ИНВАРИАНТНЫХ ПРЕОБРАЗОВАНИЯХ ФОРМУЛ

А.В.Манцивода, В.И.Мартьянов

Рассматриваемый в работах [1,2] подход к автоматизации доказательства теорем основывается на представлении элементарных шагов содержательных доказательств преобразованиями формул узкого исчисления предикатов. Эти преобразования по синтаксическим свойствам распадаются на несколько классов. В настоящей работе доказываются теоремы инвариантности (корректности) для преобразований, являющихся аналогом правила заключения (modus ponens) для содержательных доказательств.

Специфику применения правила заключения в содержательных доказательствах можно проиллюстрировать на следующем простом примере. Пусть доказывается утверждение

$$F = \begin{cases} \text{дано: } B, D, \ldots \\ \text{доказать: } E, \ldots \end{cases}$$

Формула $A = B \to C$ – аксиома данной области математики. Тогда правило заключения применяется к формуле A и формуле B из "дано", после чего переходим к доказательству утверждения

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

Если представить теперь утверждения F формулой узкого исчисления предикатов, то "дано" будет посылкой импликации, "доказать" – следствием, а использование аксиомы A будет проводиться применением правила заключения к посылке импликации формулы. Такая схема применения дает модификацию правила заключения, которую в настоящей работе будем называть ζ-преобразованием формул.

В дальнейшем буквами $A, B, C, \ldots$ мы будем обозначать формулы узкого исчисления предикатов, с помощью $P, Q, P\bar{x}, Q\bar{x}, \ldots$ – квантор –

ные приставки формул; $\bar{P}\bar{x}, \bar{Q}, \ldots$ будут означать кванторные приставки, "обратные" к $P\bar{x}, Q, \ldots$, т.е. если $P\bar{x} = \exists\bar{x}_1 \exists\bar{x}_2 \ldots \forall\bar{x}_n$, то $\bar{P}\bar{x} \lneq \exists\bar{x}_1 \forall\bar{x}_2 \ldots \exists\bar{x}_n$.

Пусть $\mathcal{K}$ – некоторый класс моделей сигнатуры σ, L – множество всех формул узкого исчисления предикатов сигнатуры σ. Отображение $\varphi: L \to L$ называется инвариантным преобразованием формул языка L относительно класса моделей $\mathcal{K}$, если для любой формулы F языка L выполняется $\mathcal{K} \models (F \leftrightarrow \varphi(F))$.

Формуле

$$A = Q\bar{x}\,(B(\bar{x}) \to C(\bar{x})) \qquad (1)$$

поставим в соответствие преобразование ζ_A такое, что если

$$F = P\bar{z}(D(\bar{z})\ \&\ B(\bar{x}) \to E(\bar{z})), \qquad (2)$$

где все переменные из кортежа $\bar{x}$ содержатся среди переменных кортежа $\bar{z}$, причем последовательность вхождений переменных $\bar{x}$ в кванторной приставке $Q\bar{x}$ та же, что и в $P\bar{z}$, то

$$\zeta_A(F) = P\bar{z}(D(\bar{z})\ \&\ B(\bar{x})\ \&\ C(\bar{x}) \to E(\bar{z})).$$

Это определение несколько упрощено по сравнению с данным в [I,2]. Такое упрощенное определение вполне достаточно для наших целей.

Заметим, что очевидным необходимым условием инвариантности ζ-преобразования является истинность на $\mathcal{K}$ формулы (I), так как она используется здесь в качестве аксиомы.

Будем говорить, что x – существенная $\exists$-переменная формулы $A = P_1 \exists x\, P_2(B(x,\bar{y}) \to C(x,\bar{y}))$, если x входит явно в посылку формулы A и, кроме того, формула A истинна на классе моделей $\mathcal{K}$, а формула $A' = P_1 \forall x\, P_2(B(x,\bar{y}) \to C(x,\bar{y}))$ ложна на $\mathcal{K}$.

ТЕОРЕМА I [2]. Преобразование ζ_A инвариантно тогда и только тогда, когда формула A истинна на классе моделей $\mathcal{K}$ и не содержит существенных $\exists$-переменных.

В качестве одного из следствий теоремы I отметим, что можно, не нарушая инвариантности ζ-преобразования, заменить все кванторы при несущественных $\exists$-переменных на кванторы всеобщности.

Большое число конкретных ζ-преобразований приведено в работах [3-5].

Важное уточнение ζ-преобразования получается в том случае, если потребовать, чтобы переменные из $\bar{x}$, связанные в кванторной приставке $Q\bar{x}$ формулы (I) $\exists$-кванторами (см.определение ζ-преобразования), были также связаны в кванторной приставке $P\bar{z}$ формулы (2) кванторами существования. Такое преобразование будем обозначать $\bar{\zeta}_A$: $L \to L$. Для ζ-преобразований теорема I дает только достаточные условия инвариантности, так как, например, формула $\exists x \forall y (x \nmid y \to y \neq y)$ с существенной $\exists$-переменной x определяет инвариантное $\bar{\zeta}$-преобразование на модели $\langle \mathbb{Z}; | \rangle$, где $\mathbb{Z}$ - целые числа, $|$ - отношение делимости.

ЗАМЕЧАНИЕ. Преобразование типа $\bar{\zeta}$ названо здесь важным уточнением ζ-преобразований, так как применение правила заключения в содержательных доказательствах для аксиом, содержащих существенные $\exists$-переменные, происходит именно по схеме $\bar{\zeta}$-преобразований. Примером этого может служить применение в качестве $\bar{\zeta}$-преобразования определения непрерывности функции $f(x)$ в точке x_0, которому соответствует формула

$$A(f, x_0) = \forall \varepsilon \exists \delta \forall x (|x - x_0| < \delta \to | f(x) - f(x_0) | < \varepsilon)$$

(предполагаем, что ε и δ принимают только положительные значения).

ТЕОРЕМА 2. Преобразование $\bar{\zeta}_A$, соответствующее формуле $A = \forall \bar{x} \exists e \forall \bar{y} (B(\bar{x}, e, \bar{y}) \to C(\bar{x}, e, \bar{y}))$, инвариантно относительно класса моделей $\mathcal{K}$ тогда и только тогда, когда на $\mathcal{K}$ истинна формула $A' = \forall \bar{x} \forall e \forall \bar{y} \; ((\forall d \exists \bar{z} \; B(\bar{x}, d, \bar{z})) \;\&\; B(\bar{x}, e, \bar{y}) \to C(\bar{x}, e, \bar{y}))$.

ДОКАЗАТЕЛЬСТВО. Необходимость. Пусть условие теоремы не выполняется. Тогда класс $\mathcal{K}$ содержит модель $\mathfrak{M}$ такую, что $\mathfrak{M} \nvDash A'$. Это значит, что в модели $\mathfrak{M}$ существует набор элементов $\tilde{\bar{x}}$, на котором выполняется формула $\forall d \exists \bar{z} \; B(\bar{x}, d, \bar{z})$, и существуют такие $\tilde{e}$ и $\tilde{\bar{y}}$, что на $\tilde{\bar{x}}, \tilde{e}, \tilde{\bar{y}}$ выполняется формула $G(\bar{x}, e, \bar{y}) = B(\bar{x}, e, \bar{y}) \;\&\; \neg C(\bar{x}, e, \bar{y})$. Тогда формула $F = \forall \bar{x} \exists e \forall \bar{y} \forall d \forall \bar{z} \exists \bar{u} \; (G(\bar{x}, d, \bar{z}) \;\&\; B(\bar{x}, e, \bar{y}) \to G(\bar{x}, e, \bar{u}) \;\&\; C(\bar{x}, e, \bar{y}))$ будет ложна на $\mathfrak{M}$. Если мы применим к этой формуле $\bar{\zeta}_A$-преобразование, то легко убедиться, что $\bar{\zeta}_A(F)$ будет истинной на $\mathcal{K}$, а, значит, $\bar{\zeta}_A$-преобразование неинвариантно.

Достаточность. Пусть $\mathcal{K} \vDash A'$. Применим $\bar{\zeta}_A$-преобразование к формуле $F = Q_1 \bar{z}_1 \exists e Q_2 \bar{z}_2 (D(\bar{z}_1, e, \bar{z}_2) \;\&\; B(\bar{x}, e, \bar{y}) \to E(\bar{z}_1, e, \bar{z}_2))$, где все переменные кортежей $\bar x$ и $\bar y$ содержатся среди переменных $\bar z_1$ и $\bar z_2$ соответственно. Тогда $F' = \bar\zeta_A(F) = Q_1\bar z_1 \exists e Q_2\bar z_2(D(\bar z_1, e, \bar z_2) \& B(\bar x, e, \bar y) \& C(\bar x, e, \bar y) \to E(\bar z_1, e, \bar z_2))$. Предположим, что F ложна (достаточно рассмотреть этот случай, так как сохранение истинности при $\bar\zeta$-преобразовании очевидно). Тогда истинна $\neg F = \bar Q_1\bar z_1 \forall e \bar Q_2\bar z_2(D(\bar z_1, e, \bar z_2) \& B(\bar x, e, \bar y) \& \neg E(\bar z_1, e, \bar z_2))$. Истинность на $\mathcal{K}$ формулы $\neg F$ влечет за собой истинность

$$\bar Q_1\bar z_1 \forall e\, \bar Q_2\bar z_2 B(\bar x, e, \bar y).$$

Но так как $\mathcal{K} \models A'$, то в любой модели $\mathfrak{M} \in \mathcal{K}$ на любом наборе элементов $\tilde{x}$, на котором выполняется $\forall e \exists \bar y B(\bar x, e, \bar y)$, выполняется и формула $\forall e \forall \bar y (B(\bar x, e, \bar y) \to C(\bar x, e, \bar y))$. Следовательно, $\neg(\zeta_A(F))$, полученная из $\neg F$ добавлением подформулы $C(\bar x, e, \bar y)$ в качестве конъюнктивного члена, будет также истинна на $\mathcal{K}$, а, значит, $\mathcal{K} \not\models \bar\zeta_A(F)$. Это доказывает инвариантность $\bar\zeta_A$-преобразования.

Из теоремы 2 видно, насколько сильные условия надо наложить на $\bar\zeta_A$-преобразование для достижения его инвариантности. Более того, оказалось, что многие понятия содержательной математики, используемые в этом методе автоматического доказательства теорем как $\bar\zeta$-преобразования, не являются инвариантными. Примером этого может служить, в частности, уже упоминавшееся выше определение непрерывности функции в точке. Это легко проверить, используя теорему 2. Весьма часто от инвариантности удается избавиться за счет наложения некоторых ограничений на применимость $\bar\zeta$-преобразования, а именно добавим в определение $\bar\zeta$-преобразования следующее условие: вхождение в формулу (2) переменных из кортежа $\bar x$, являющихся существенными $\exists$-переменными формулы (I), должно быть ограничено подформулой $B(\bar x)$. Если же это условие не выполнено, то формула (2) остается неизменной. Такую модификацию $\bar\zeta$-преобразования назовем $\bar\zeta^*$-преобразованием. Для $\bar\zeta^*$-преобразований получены следующие необходимые и достаточные условия инвариантности.

ТЕОРЕМА 3. Преобразование ζ^*_A, соответствующее формуле $A = \forall\bar x \exists e \forall\bar y(B(\bar x, e, \bar y) \to C(\bar x, e, \bar y))$, инвариантно относительно класса моделей $\mathcal{K}$ тогда и только тогда, когда на $\mathcal{K}$ истин-

на формула $A' = \forall\bar{x}\forall d\,\exists e\forall\bar{y}\,(B(\bar{x},e,\bar{y}) \to B(\bar{x},d,\bar{y})\ \&$
$\&\ C(\bar{x},d,\bar{y}))$.

ДОКАЗАТЕЛЬСТВО. Необходимость. Пусть $\mathcal{K} \nvDash A'$. Так как формула $\zeta^*_A(A')$ тождественно истинна (это становится очевидным при замене e на d), то преобразование ζ^*_A не инвариантно.

Достаточность. Пусть условия теоремы выполнены. Применим ζ^*_A-преобразование к формуле

$$F = Q_1\bar{z}_1\,\exists e Q_2\bar{z}_2\,(D(\bar{z}_1\bar{z}_2)\ \&\ B(\bar{x},e,\bar{y}) \to E(\bar{z}_1,\bar{z}_2)).$$

Тогда

$$F' = \zeta^*_A(F) = Q\bar{z}(D(\bar{z})\ \&\ B(\bar{x},e,\bar{y})\ \&\ C(\bar{x},e,\bar{y}) \to E(\bar{z})).$$

Пусть $\mathcal{K} \models F'$. Покажем, что в этом случае $\mathcal{K} \models F$.

Действительно, пусть $\varphi(\bar{x}, d)$ и $\psi(\bar{z}_1,\bar{x})$ – скулемовские функции переменной соответственно для формул A' и F'. Тогда функция $\varphi(\bar{x},\psi(\bar{z}_1, \bar{x}))$ будет скулемовской для формулы F.

Заметим, что здесь пропущены некоторые технические детали, связанные с тем, что некоторые переменные из $\bar{x}$ связаны в $Q_1\bar{z}_1$ кванторами существования, кроме того, в кортеже $\bar{z}_1$ могут быть "лишние" переменные, входящие в кванторный комплекс $Q_1\bar{z}_1$.

Из теоремы 3, в частности, следует, что определение непрерывности функции в точке, упоминавшееся выше как порождающее неинвариантное ζ-преобразование, соответствует ζ^*-преобразованию, являющемуся инвариантным.

Аналогично предыдущей теореме доказывается следующий критерий инвариантности произвольного ζ^*-преобразования.

ТЕОРЕМА 4. Преобразование ζ^*_A, соответствующее формуле

$$A = \forall\bar{x}_1\,\exists\bar{e}_1\ldots\forall\bar{x}_n\,\exists\bar{e}_n(B(\bar{x},\bar{e}) \to C(\bar{x},\bar{e})),$$

инвариантно относительно класса моделей $\mathcal{K}$ тогда и только тогда, когда на $\mathcal{K}$ истинна формула

$$A' = \forall\bar{x}_1\forall\bar{d}_1\,\exists\bar{e}_1\ldots\forall\bar{x}_n\forall\bar{d}_n\,\exists\bar{e}_n(B(\bar{x},\bar{e}) \to B(\bar{x},\bar{d})\ \&\ C(\bar{x},\bar{d})).$$

Л и т е р а т у р а

1. МАРТЬЯНОВ В.И. Доказательство теорем на ЭВМ. - В кн.: Алгоритмические вопросы алгебраических систем и ЭВМ. Иркутск, 1979, с.111-127.

2. МАРТЬЯНОВ В.И. Методы задания и частичного построения теории на ЭВМ. -Кибернетика, 1982, №6, с.102-110.

3. ЖЕРЛОВ А.К., МАРТЬЯНОВ В.И. Автоматизация вывода теорем теории групп. -В кн.: Алгоритмические вопросы алгебраических систем и ЭВМ. Иркутск, 1979, с.36-64.

4. КЛЕЙМЕНОВ В.Ф. Автоматизация вывода теорем теории категорий. -Там же, с. 65-83.

5. НИКОЛАЕНКО А.Б. Автоматизация вывода теорем аксиоматической теории множеств. -Там же, с.177-190.

Поступила в ред.-изд.отд.
10 мая 1984 года