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

УДК 681.142.2:518.5

ДОКАЗАТЕЛЬСТВО ЗАВЕРШАЕМОСТИ ПРОГРАММ СРЕДСТВАМИ ДИНАМИЧЕСКОЙ ЛОГИКИ

Н.В.Шилов

I. Синтаксис и семантика динамической логики

Пусть $V = \{x, y, \ldots\}$ - алфавит переменных, $F = \{f, g, \ldots\}$ - алфавит символов функций, $P = \{p, q, \ldots\}$ - алфавит символов предикатов. В дальнейшем функциональные и предикатные символы мы часто будем называть просто функциями и предикатами. Мы предполагаем, что каждая функция и предикат имеют определенную местность. Язык динамической логики состоит из формул и программ, но прежде всего необходимо определить понятия терма, равенства, атомной формулы, оператора присваивания.

Термы строятся обычным образом из переменных и функций: всякая переменная есть терм, и если f - функция, n - ее местность, а $t_1, \ldots, t_n$ - термы, то $f(t_1, \ldots, t_n)$ - терм. Равенством называется выражение вида $t = t'$, где t и t' - произвольные термы. Атомной формулой называется выражение вида $p(t_1, \ldots, t_n)$, где p - произвольный предикат, n - его местность, а $t_1, \ldots, t_n$ - произвольные термы. Оператором присваивания называется выражение вида $x := t$, где x - произвольная переменная, а t - произвольный терм. В таком случае считаем, что:

I) всякое равенство является формулой;

2) всякая атомная формула является формулой;

3) если X и Y - формулы, то $(\neg X)$, $(X \wedge Y)$, $(X \vee Y)$ - формулы;

4) если X - формула, а x - переменная, то $(\exists x \cdot X)$ и $(\forall x \cdot X)$ - формулы;

5) если X - формула, а α - программа, то $(\langle\alpha\rangle X)$ и $([\alpha]X)$ - формулы;

6) всякий оператор присваивания является программой;

7) если X - формула, то $X?$ - программа;

8) если α, β - программы, то (α^*), $(\alpha;\beta)$ и $(\alpha \cup \beta)$ - программы.

Программа вида $X?$, где X - произвольная формула, называется тестом.

Интерпретация I - это пара $(D_I, (\ )_I)$, где D_I - непустое множество (область интерпретации), а $(\ )_I$ - означивание функций и предикатов: означивание $(\ )_I$ ставит в соответствие каждой функции f всюду определенную на D_I операцию $f_I = (f)_I : D_I^m \to D_I$, где m - местность f, а каждому предикату p - множество $p_I = (p)_I \subseteq D_I^n$, где n - местность p. Состояние в интерпретации I - это произвольное отображение s, которое ставит в соответствие каждой переменной x значение $s(x) \in D_I$. Таким образом, множество всех состояний в интерпретации I - это множество D_I^V. Пусть $s \in D_I^V$ - произвольное состояние; исходя из значений переменных в состоянии s значение $s(t) \in D_I$ произвольного терма t в s мы можем определить следующим образом: если t - некоторая переменная, то $s(t)$ уже определено, а если t - терм $f(t_1, \ldots, t_n)$, то $s(t) = f_I(s(t_1), \ldots, s(t_n))$.

Пусть I - произвольная интерпретация. Каждая формула X определяет на D_I^V унарное отношение $\models_I X$ - "X выполнена в состоянии", а каждая программа α - бинарное отношение $\langle \alpha \rangle_I$ - "начав вычисления во входном состоянии, программа α останавливается в выходном состоянии". Пусть s, s' и s'' - произвольные состояния из D_I^V. Если формула X выполнена в состоянии s, то принято писать $s \models_I X$. Если программа α перерабатывает входное состояние s' в выходное состояние s'', то принято писать $s' \langle \alpha \rangle_I s''$. В таком случае имеем:

1. $s \models_I (t = t') \Leftrightarrow s(t) = s(t')$;

2. $s \models_I p(t_1, \ldots, t_n) \Leftrightarrow (s(t_1), \ldots, s(t_n)) \in p_I$;

3. а) $s \models_I (\neg X) \Leftrightarrow$ неверно $s \models_I X$;

   б) $s \models_I (X \wedge Y) \Rightarrow s \models_I X$ и $s \models_I Y$;

   в) $s \models_I (X \vee Y) \Rightarrow s \models_I X$ или $s \models_I Y$;

4. а) $s \models_I (\exists x X) \Leftrightarrow$ существует такое состояние $s''' \in D_I^V$, что для любой переменной y, отличной от x, $s'''(y) = s(y)$ и $s''' \models_I X$;

б) $s \models_I (\forall x \cdot X) \Leftrightarrow$ для любого состояния $s''' \in D_I^V$, такого, что для любой переменной y, отличной от x, $s'''(y) = s(y)$, верно $s''' \models_I X$;

5. а) $s \models_I (\langle \alpha \rangle X) \Leftrightarrow$ существует такое состояние $s''' \in D_I^V$, что $s \langle \alpha \rangle_I s''' \models_I X$;

б) $s \models_I ([\alpha] X) \Leftrightarrow$ для любого состояния $s''' \in D_I^V$, если $s \langle \alpha \rangle_I s'''$, то $s''' \models_I X$;

6. $s' \langle x := t \rangle_I s'' \Leftrightarrow s''(x) = s'(t)$ и для любой переменной y, отличной от x, верно $s''(y) = s'(y)$;

7. $s' \langle X? \rangle_I s'' \Leftrightarrow s'' = s' \models_I X$;

8. а) $s' \langle (\alpha^*) \rangle_I s'' \Leftrightarrow$ существует такая последовательность состояний $s_0 \ldots s_k \in D_I^V$, $k \geq 0$, что $s_0 = s'$, $s_k = s''$, и для любого i, $0 \leq i < k$, имеем $s_i \langle \alpha \rangle_I s_{i+1}$;

б) $s' \langle (\alpha ; \beta) \rangle_I s''' \Leftrightarrow$ существует такое состояние $s''' \in D_I^V$, что $s' \langle \alpha \rangle_I s''' \langle \beta \rangle_I s''$;

в) $s' \langle (\alpha \cup \beta) \rangle_I s'' \Leftrightarrow s' \langle \alpha \rangle_I s''$ или $s' \langle \beta \rangle_I s''$.

Если неверно $s \models_I X$, то принято писать $s \not\models_I X$. Формула X называется истинной в интерпретации I ($\models_I X$), если она выполнена в каждом состоянии этой интерпретации. Формула X называется истинной ($\models X$), если она истинна в каждой интерпретации.

Как обычно, язык, на множестве формул которого определено отношение истинности, принято называть логикой. Таким образом, отношение $\models$ "превращает" язык динамической логики в соответствующую логику. В дальнейшем мы определим ряд других логик, языки которых будут фрагментами языка динамической логики, а истинность зададим также посредством $\models$; в таких случаях мы не будем указывать каждый раз, что истинность задана посредством $\models$.

В рамках динамической логики удобно использовать ряд сокращений: $X \supset Y$ – сокращение для формулы $((\neg X) \vee Y)$; $X \equiv Y$ – для формулы $((X \supset Y) \wedge (Y \supset X))$; если $\bar{x}$ – конечная последовательность переменных $x_1 \ldots x_k$, $k \geq 0$, а Q – квантор $\exists$ или $\forall$, то $(Q\bar{x} \cdot X)$ – это или сама формула X при $k = 0$, или сокращение для формулы $(Qx_1 \ldots (Qx_k X))$ при $k > 0$; аналогично, если f и p – k-местные функция и предикат, то $f(\bar{x})$ и $p(\bar{x})$ – сокращения для $f(x_1, \ldots, x_k)$ и $p(x_1, \ldots, x_k)$.

2. Постановка задачи

Известно [I], что динамическая логика обладает высокой степенью неразрешимости: множество истинных формул динамической логики является Π_1^1-полным; в частности это означает, что ни множество истинных формул динамической логики, ни множество формул динамической логики, выполнимых в некотором состоянии некоторой интерпретации, не являются даже рекурсивно-перечислимыми. Естественно, возникает задача описания нетривиальной подлогики динамической логики, множество истинных формул которой является рекурсивно-перечислимым. Какие результаты в этом направлении уже получены? Во-первых, так как исчисление предикатов - это фрагмент динамической логики без программ, то первым результатом можно считать теорему Гёделя о полноте, хотя, разумеется, динамическая логика возникла значительно позже исчисления предикатов; из теоремы Гёделя о полноте следует рекурсивная перечислимость множества истинных формул исчисления предикатов. Мы примем этот факт за основу исследования. Второй важный результат - это разрешимость детерминированной пропозициональной динамической логики с экспоненциальной верхней и нижней оценками сложности [2]. Не вдаваясь в детали, скажем только, что детерминированная пропозициональная динамическая логика - это фрагмент динамической логики, в рамках которого алфавит переменных V состоит из одной переменной (например, x), используются только одноместные функции и предикаты и не используются кванторы. Отметим также, что в настоящее время получено много интересных результатов о разрешимости различных пропозициональных вариантов динамической логики. В-третьих, важным результатом в этом направлении является рекурсивная перечислимость истинных условий завершаемости [3]. Остановимся на нем подробнее.

Условием завершаемости (termination assertion) [3] называется выражение вида $X \supset \langle\alpha\rangle Y$, где X и Y - произвольные формулы исчисления предикатов, а α - программа, в которой в качестве тестов используются формулы исчисления предикатов. В [3] описана аксиоматическая система, состоящая из рекурсивного множества аксиом и двух конечных правил вывода, которая является полной аксиоматизацией множества истинных условий завершаемости. Отсюда, в частности, следует рекурсивная перечислимость множества истинных условий завершаемости. Доказательство теоремы полноты в [3] основано на теореме компактности.

Четвертым важным результатом является теорема полноты для ◇ ДЛ*), полученная в [4]. Напомним, что ◇ДЛ - это фрагмент динамической логики, в рамках которого операция отрицания ˥ применяется только к формулам исчисления предикатов и не используются скобки [ ] (см. [4]). Полная аксиоматическая система для ◇ДЛ состоит из рекурсивно-перечислимого множества аксиом (множества истинных формул исчисления предикатов) и конечного множества конечных правил вывода [4]. Отсюда, в частности, следует рекурсивная перечислимость множества истинных формул ◇ДЛ. Отметим, что всякое условие завершаемости является формулой ◇ДЛ, поэтому работа [4] - это обобщение [3]. Однако в отличие от [3] доказательство теоремы полноты в [4] основано на вложении динамической логики в инфинитарную логику $L_{\omega_1\omega}$ (см. [5]). Существенной особенностью работ [3,4] является то, что для проверки истинности (т.е. выводимости в упомянутых работах аксиоматических систем) не существует какой-либо стратегии построения дерева вывода. Соответственно при практическом использовании аксиоматических систем из [3,4] возникает проблема сокращения пространства вывода.

В настоящей работе описана полная аксиоматизация ◇ДЛ, состоящая из рекурсивно-перечислимого множества аксиом и конечного множества конечных правил вывода, принципиально отличающаяся от системы из [4]. Особенностью описанной в работе аксиоматической системы является то, что существует стратегия применения правил вывода, которая позволяет за полиномиальное время по произвольной формуле ◇ДЛ построить дедуктивно равную формулу исчисления предикатов. Таким образом, проблема истинности ◇ДЛ сводится к проблеме истинности исчисления предикатов, а проблема поиска вывода ◇ДЛ - к проблеме поиска вывода в исчислении предикатов.

3. Аксиоматизация ◇ДЛ

Прежде чем перейти к описанию аксиом и правил вывода ◇ДЛ, опишем ряд технических понятий. Пусть X и Y - пара формул ◇ДЛ. Формула Y называется подформулой X, если слово Y является подсловом X; положительными вхождениями подформулы Y в X называются те вхождения слова Y в X, которые не находятся в области действия ни одного знака теста ? и отрицания ˥ (здесь мы рассматри-

---

*) ДЛ - динамическая логика.

ваем формулы $\Diamond$ДЛ как слова в алфавите переменных, функций, предикатов и знаков $\rceil$, $\wedge$, $\vee$, $\exists$, $\forall$, $\langle\ \rangle$, $*$, ;, $\cup$, ?, :=, =).

Введем еще одно обозначение. Пусть e, e' и e" - произвольные выражения (формулы, программы, термы и т.д.). Тогда e(e'/e") - выражение, которое получается из e, e' и e" по следующему правилу: если e, e' и e" - формулы $\Diamond$ДЛ, то e(e'/e") получается из e в результате замены всех положительных вхождений e" на e'; если же e, или e', или e" не являются формулой $\Diamond$ДЛ, то e(e'/e") получается из e в результате замены всех вхождений e" на e'.

УТВЕРЖДЕНИЕ I. Пусть X, Q и Q' - произвольные формулы $\Diamond$ДЛ, $\bar{x} = x_1 \ldots x_k$, $k \geq 0$, - все переменные, которые встречаются в Q и Q'. Тогда $\forall \bar{x}(Q \supset Q') \supset (X \supset X(Q'/Q))$ - истинная формула.

ДОКАЗАТЕЛЬСТВО можно провести индукцией по структуре формулы X над Q. База индукции здесь соответствует случаю, когда X - сама формула Q. Доказательство в целом тривиально, поэтому разберем только шаг индукции в случае, когда X - формула $(\langle \alpha \rangle Y)$. Тогда предположение индукции состоит в том, что для Y утверждение уже доказано. Заметим, что $X(Q'/Q)$ - это формула $(\langle \alpha \rangle Y(Q'/Q))$. Пусть I - произвольная интерпретация, а $s \in D_I^V$ - произвольное состояние. Предположим, что $s \not\models_I \forall \bar{x}(Q \supset Q') \supset (X \supset X(Q'/Q))$. Тогда $\models_I Q \supset Q'$ и $s \not\models_I X \supset X(Q'/Q)$, а также $s \models_I X$ и $s \not\models_I X(Q'/Q)$. Следовательно, существует такое состояние $s' \in D_I^V$, что $s \langle \alpha \rangle_I s' \models_I Y$. Но по предположению индукции $\models_I \forall \bar{x}(Q \supset Q') \supset (Y \supset Y(Q'/Q))$. Поскольку $\models_I Q \supset Q'$, то $s' \models_I Y \supset Y(Q'/Q)$. Следовательно, $s' \models_I Y(Q'/Q)$. Так как $s \langle \alpha \rangle_I s'$, то, стало быть, $s \models_I \langle \alpha \rangle Y \supset \langle \alpha \rangle Y(Q'/Q)$. Значит, $s \models_I X \supset X(Q'/Q)$. Следовательно, $s \models_I \forall \bar{x}(Q \supset Q') \supset (X \supset X(Q'/Q))$, и сделанное выше предположение неверно. Значит, формула $\forall \bar{x}(Q \supset Q') \supset (X \supset X(Q'/Q))$ истинна.

Теперь все готово для аксиоматизации $\Diamond$ДЛ. В качестве аксиом мы примем множество истинных формул исчисления предикатов. Каждое правило вывода имеет вид Y/X, где X и Y - формулы $\Diamond$ДЛ. Всего правил вывода 6.

Правило "/" . Пусть X - произвольная формула $\Diamond$ДЛ, Q - ее подформула, $x = x_1 \ldots x_k$, $k \geq 0$, - все переменные, которые встречаются в Q , q - новый, не встречающийся в X k-местный предикат. Тогда правило "/" имеет следующий вид:

$$\frac{\exists \bar{x}(Q \wedge \neg q(x)) \vee X(q(x)/Q)}{X}.$$

УТВЕРЖДЕНИЕ 2. Если Y/X - частный случай правила "/", то формула Y истинна тогда и только тогда, когда истинна формула X .

ДОКАЗАТЕЛЬСТВО. Так как Y/X - частный случай правила "/", то формула Y имеет вид $\exists \bar{x}(Q \wedge \neg q(\bar{x})) \vee X(q(x)/Q)$. Сначала докажем, что из истинности формулы X следует истинность формулы Y . Действительно, согласно утверждению I, формула $\forall \bar{x}(Q \supset q(\bar{x})) \supset (X \supset X(q(\bar{x})/Q))$ истинна. Следовательно, если X - истинная формула, то истинна формула $\forall \bar{x}(Q \supset q(\bar{x})) \supset X(q(\bar{x})/Q)$. Но эта формула эквивалентна формуле Y . Таким образом, из истинности формулы X следует истинность формулы Y .

Докажем обратную импликацию. Для этого предположим противное, т.е. что формула Y истинна, но существуют интерпретация I и состояние $s \in D_I^V$ такие, что $s \not\models_I X$. Определим интерпретацию J следующим образом. Пусть $D_J = D_I$; для любой функции f пусть $f_J = f_I$; для любого предиката p , отличного от q , пусть $p_J = p_I$; пусть $q_J = \{(d_1, \ldots, d_k) \mid$ существует такое состояние $s' \in D_I^V$, что $s'(x_1) = d_1, \ldots, s'(x_k) = d_k$ и $s' \models_I Q \}$. Тогда для любой формулы Z , в которой не встречается предикат q ,для произвольного состояния $s' \in D_I^V$ имеем $s' \models_J Z \Rightarrow s' \models_I Z$. Следовательно, $\models_J (Q \equiv q(\bar{x}))$ и $s \not\models_J X$. Стало быть, $s' \not\models_J X(q(\bar{x})/Q)$. Значит, $s \not\models_J \forall \bar{x}(Q \supset q(\bar{x})) \supset X(q(\bar{x})/Q)$. Но последняя формула эквивалентна формуле Y . Значит,мы пришли к противоречию с истинностью Y .Следовательно,предположение о том, что $s \not\models_I X$, ложно. Таким образом, из истинности Y следует истинность формулы X .

Правило " * ". Пусть X - произвольная формула $\Diamond$ДЛ, $(\langle \alpha^* \rangle Q)$ - ее подформула, $\bar{x} = x_1 \ldots x_k$, $k \geq 0$, - все переменные, которые встречаются в $(\langle \alpha^* \rangle Q)$, q - новый k-местный предикат.Тогда правило " * " имеет следующий вид:

$$\frac{\exists\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \wedge \urcorner q(\bar{x})) \vee X(q(\bar{x})/\langle\alpha^*\rangle Q)}{X}.$$

УТВЕРЖДЕНИЕ 3. Если Y/X - частный случай правила "$*$", то формула Y истинна тогда и только тогда, когда истинна формула X.

ДОКАЗАТЕЛЬСТВО. Так как Y/X - частный случай правила "$*$", то формула Y имеет вид $\exists\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \wedge \urcorner q(\bar{x})) \vee X(q(\bar{x})/\langle\alpha^*\rangle Q)$.

Сначала докажем, что из истинности формулы X следует истинность формулы Y. Действительно, как легко видеть, формула $\forall\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \supset q(\bar{x})) \supset \forall\bar{x} (\langle\alpha^*\rangle Q \supset q(\bar{x}))$ является истинной. Согласно утверждению I, формула $\forall\bar{x}(\langle\alpha^*\rangle Q \supset q(\bar{x})) \supset (X \supset X(q(\bar{x})/\langle\alpha^*\rangle Q))$ также является истинной. Следовательно, формула $\forall\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \supset q(\bar{x})) \supset (X \supset X(q(\bar{x})/\langle\alpha^*\rangle Q))$ является истинной. В таком случае если X - истинная формула, то истинна формула $\forall\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \supset q(\bar{x})) \supset X(q(\bar{x})/\langle\alpha^*\rangle Q)$. Но эта формула эквивалентна формуле Y. Таким образом, из истинности формулы X следует истинность формулы Y.

Докажем обратную импликацию. Для этого предположим противное, т.е. что формула Y истинна, но существуют интерпретация I и состояние $s \in D_I^V$ такие, что $s \not\models_I X$. Определим интерпретацию J следующим образом. Пусть $D_J = D_I$; для любой функции f пусть $f_J = f_I$; для любого предиката p, отличного от q, пусть $p_J = p_I$; пусть $q_J = \{(d_1,\ldots,d_k) \mid$ существует такое состояние $s' \in D_I^V$, что $s'(x_1) = d_1, \ldots, s'(x_k) = d_k$ и $s' \models \langle\alpha^*\rangle Q\}$. Тогда для любой формулы Z, в которой не встречается предикат q, произвольного состояния $s' \in D_I^V$ имеем: $s' \models_J Z \Leftrightarrow s' \models_I Z$. Следовательно, $\models_J (q(\bar{x}) \equiv \langle\alpha^*\rangle Q)$ и $s \not\models_J X$. Значит, $s \not\models_J X(q(\bar{x})/\langle\alpha^*\rangle Q)$ и, стало быть, $s \not\models_J \forall\bar{x}((Q \vee \langle\alpha\rangle q(\bar{x})) \supset q(\bar{x})) \supset X(q(\bar{x})/\langle\alpha^*\rangle Q)$. Но последняя формула эквивалентна формуле Y. Следовательно, мы пришли к противоречию с истинностью Y. Значит, предположение о том, что $s \not\models_I X$, ложно. Таким образом, из истинности Y следует истинность формулы X.

Правило ";". Пусть X - произвольная формула ОДЛ, $(\langle\alpha;\beta\rangle Q)$ - ее подформула. Тогда правило ";" имеет следующий вид:

$$\frac{X(\langle\alpha\rangle\langle\beta\rangle Q/\langle\alpha;\beta\rangle Q)}{X}.$$

Правило " $\cup$". Пусть X - произвольная формула $\Diamond$ДЛ, $(\langle \alpha \cup \beta \rangle Q)$ - ее подформула. Тогда правило " $\cup$ " имеет следующий вид:

$$\frac{X((\langle \alpha \rangle Q \vee \langle \beta \rangle Q)/\langle \alpha \cup \beta \rangle Q)}{X} .$$

Правило "?". Пусть X - произвольная формула $\Diamond$ДЛ, $(\langle R? \rangle Q)$ - ее подформула. Тогда правило "?" имеет вид:

$$\frac{X((R \wedge Q)/\langle R? \rangle Q)}{X} .$$

Правило ":=". Пусть X - произвольная формула $\Diamond$ДЛ, $(\langle x := t \rangle Q)$ - ее подформула, в которой Q - формула исчисления предикатов, не имеющая связанных вхождений переменной x. Тогда правило ":=" имеет следующий вид:

$$\frac{X(Q(t/x)/\langle x := t \rangle Q)}{X} .$$

УТВЕРЖДЕНИЕ 4. Если Y/X - частный случай одного из правил ";", "$\cup$", "?" или ":=", то формула Y истинна тогда и только тогда, когда истинна формула X.

ДОКАЗАТЕЛЬСТВО во всех четырех случаях непосредственно следует из истинности следующих формул:

1. $\langle \alpha ; \beta \rangle Q \equiv \langle \alpha \rangle \langle \beta \rangle Q$;
2. $\langle \alpha \cup \beta \rangle Q \equiv \langle \alpha \rangle Q \vee \langle \beta \rangle Q$;
3. $\langle R? \rangle Q \equiv R \wedge Q$;
4. $\langle x := t \rangle Q \equiv Q(t/x)$.

Здесь (в 1-3) Q и R - произвольные формулы динамической логики, а Q из 4 - произвольная формула исчисления предикатов, в которой переменная x имеет только свободные вхождения.

Из утверждений 2-4 следует

УТВЕРЖДЕНИЕ 5. Правила вывода "/", "$*$", ";", "$\cup$", "?" и ":=" являются допустимыми правилами для $\Diamond$ДЛ.

4. Теорема полноты для $\Diamond$ДЛ

Сначала докажем следующее

УТВЕРЖДЕНИЕ 6. По произвольной формуле $\Diamond$ДЛ за кубическое время можно построить формулу исчисления предикатов, истинную тогда и только тогда, когда истинна исходная формула.

ДОКАЗАТЕЛЬСТВО. Ниже описан алгоритм построения по произвольной формуле $\Diamond$ДЛ формулы исчисления предикатов, каждый шаг которого состоит в применении к формуле, полученной на предыдущем шаге, одного из правил "/", "*", ";", "$\cup$", "?", ":=" "в обратном порядке": под обратным порядком применения правила $rule \in \{/, *, ;, \cup, ?, :=\}$ к формуле X мы понимаем построение такой формулы Y, что Y/X - частный случай правила rule ; в таком случае мы будем писать Y:= rule(X) . Следовательно (согласно утверждениям 2-4), после того, как мы опишем алгоритм в этих терминах, для завершения доказательства достаточно определить его верхнюю оценку сложности.

Итак, пусть Z_1 - произвольная формула $\Diamond$ДЛ, i - специальная переменная (счетчик), начальное значение которой равно единице (счетчик введен для удобства описания алгоритма). Тогда описание алгоритма перевода $\Diamond$ДЛ в исчисление предикатов состоит из пяти пунктов:

I. Если Z_i - формула исчисления предикатов, то перейти к выполнению п.5, иначе - перейти к п.2.

2. Пусть L - самая левая подформула Z_i, которая имеет вид $(\langle\gamma\rangle Q)$, где Q - формула исчисления предикатов; перейти к выполнению п.3.

3. Если Q - атомная формула, то перейти к выполнению п. 4, иначе - $Z_i := /(Z_i)$, перейти к выполнению п.2.

4. Возможны следующие варианты:

а) γ - это (α^*) ;

б) γ - это $(\alpha;\beta)$;

в) γ - это $(\alpha\cup\beta)$;

г) γ - это R?;

д) γ - это x:= t .

В каждом из этих случаев выполнить соответствующий пункт из следующих ниже:

а) $Z_{i+1} := *(Z_i)$;

б) $Z_{i+1} := ;(Z_i)$;

в) $Z_{i+1} := \cup(Z_i)$;

г) $Z_{i+1} := ?(Z_i)$;

д) $Z_{i+1} := :=(Z_i)$.

Выполнить $i = i+1$ и перейти к выполнению п.I.

5. Конец.

Пусть m - число различных переменных в Z_1, а n - число знаков $\bullet$, ;, $\cup$, ? и := в Z_1. Пусть $k \geq 1$ - последнее текущее значение счетчика i (значение i во время выполнения п.5). Для любого i, $1 \leq i \leq k$, пусть $|Z_i|$ - длина формулы Z_i (общее число символов в слове Z_i), m_i - число различных переменных в Z_i, а n_i - число знаков $\bullet$, ;, $\cup$, ? и := в Z_i. Тогда из описания п.4 следует, что для любого i, $1 \leq i < k$, $m_{i+1} = m_i$ и $n_{i+1} = n_i - 1$. Следовательно, число повторений в цикле пп. I-4 равно n, причем общее число переменных остается постоянным и равно m. В то же время для любого i, $1 \leq i < k$, имеем: $|Z_{i+1}| \leq |Z_i| + const + 2m$, причем формулу Z_{i+1} можно построить по Z_i за время $const \cdot |Z_i|$. Следовательно, $|Z_k| \leq |Z_1| + (const + 2m) \cdot n \leq const \cdot |Z_1|^2$, а построить Z_k можно за время $const \cdot |Z_1|^3$.

ТЕОРЕМА. Аксиоматическая система, состоящая из правил вывода "/", "$\bullet$", ";", "$\cup$", "?" и ":=", в которой в качестве аксиом приняты истинные формулы исчисления предикатов, является полной аксиоматизацией $\Diamond$ДЛ.

Доказательство следует из формулировки и доказательства утверждения 6.

5. Анализ полученных результатов

Как уже было сказано в разделе 2, описанная в теореме полная аксиоматизация $\Diamond$ДЛ принципиально отличается от описанной в [4] аксиоматизации $\Diamond$ДЛ, а именно: из доказанного утверждения 6 мы получаем стратегию поиска вывода (алгоритм перевода $\Diamond$ДЛ в исчисление предикатов). Но в то же время, хотя для доказательства теоремы полноты нам не пришлось прибегать к инфинитарной логике $L_{\omega_1 \omega}$, однако (в отличие от [4]) использование правил вывода "/" и "$\bullet$" приводит к появлению новых предикатов. Отсюда на практике использование описанного в доказательстве утверждения 6 алгоритма перевода формулы $\Diamond$ДЛ в дедуктивно равную формулу исчисления предикатов для доказательства истинности исходной формулы $\Diamond$ДЛ сопряжено с проблемой создания универсального (а не проблемно-ориентированного) программного модуля для доказательства формул исчисления предикатов. Использование же аксиоматической системы, описанной в [4], позволяет иметь дело с проблемно-ориентированным (не универсальным) модулем поиска доказательства формул исчисления предикатов, однако, как уже было сказано, в этом случае возникает проблема выбора стратегии доказательства. В заключение этого краткого анализа полученных результатов отметим, что предполагается их реализация в рамках системы верификации "Спектр", создаваемой в ВЦ СО АН СССР.

Литература

1. HAREL D. First-order Dynamic Logic.-Berlin,1979.- 160 p.

2. VALIEV M.K. Decision complexity of variants of propositional dynamic logic// Lecture Notes on Computer Science.-1980.-Vol. 88.- P.656-664.

3. MEYER A.R., HALPERN J.Y. Axiomatic definitions of programming languages: a theoretical assesment// J.Assoc.Comput.Mach. - 1982.- Vol.29.- P.555-576.

4. SCHMITT P.H. Diamond Formulas: a Fragment of Dynamic Logic with Recursively Enumerable Validity Problem// Information and Control.-1984.-Vol.61,N 2.-P.147-158.

5. КЕЙСЛЕР Дж. Х. Основы теории моделей //Справочная книга по математической логике. - 1982. Т.2, гл.2. -С. 55-108.

Поступила в ред.-изд.отд.
18 мая 1988 года