УДК 681.3.057.51-7.311.17

ВНУТРЕННЯЯ МОДЕЛЬ МАТЕМАТИЧЕСКОЙ ПРАКТИКИ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО КОНСТРУИРОВАНИЯ ДОКАЗАТЕЛЬСТВ ТЕОРЕМ. Ч. 3. Модель доказательства[1]

Т. Л. Гаврилова, А. С. Клещев

Институт автоматики и процессов управления ДВО РАН, г. Владивосток

Статья завершает цикл из трех работ, посвященных модели математической практики для систем автоматизированного доказательства теорем. Сформулированы правила рассуждения, используемые при конструировании доказательств. Определена модель полного доказательства. Приведены примеры формулировок математических утверждений на языке ММД (модели математического диалекта) и модель правильного полного доказательства одного из них.

ВВЕДЕНИЕ

В доказательствах, которые строят математики, центральную роль играют утверждения, имеющие форму импликации, — пропозициональные тавтологии, лежащие в основе логических рассуждений, математические утверждения (аксиомы и теоремы), лежащие в основе математических рассуждений, и метаматематические утверждения, позволяющие использовать в рассуждениях свойства логических и нелогических кванторов, а также логические и нелогические принципы. Правило вывода, связанное с использованием утверждений, имеющих форму импликации, известно как Modus ponens. Это правило вывода позволяет сводить доказательство утверждения, совпадающего с заключением импликации, к доказательству утверждений, совпадающих с ее посылками (декомпозиция), либо выводить утверждение, совпадающее с заключением импликации, из утверждений, совпадающих с ее посылками (вывод). Совпадение обеспечивается процедурой унификации (конкретизации). Сама же импликация доказывается на основе теоремы дедукции. Кроме того, в процессе доказательства выдвигаются и используются различные предположения. В моделях математической логики, в том числе используемых в системах интерактивного доказательства теорем, эти свойства математических доказательств представлены в крайне усеченных вариантах, что существенно затрудняет управление построением доказательств. Настоящая статья завершает цикл работ, начатый в работах [1, 2].

1. ПРАВИЛА РАССУЖДЕНИЯ

Два правила рассуждения (декомпозиция и вывод) определяют все возможные шаги, из которых могут конструироваться полные доказательства. Эти правила рассуждения формулируются на математическом диалекте. Каждое правило рассуждения позволяет получить непустую совокупность предложений.

Будем говорить, что *математическое утверждение справедливо,* если оно входит в математические знания или является конкретизацией метаматематического утверждения, входящего в математические знания. Будем говорить, что *предложение справедливо,* если оно либо получено в результате доказательства без выдвижения предположений, либо является конкретизацией пропозициональной тавтологии, либо является конкретизацией справедливого математического утверждения, сделанной без предположений (в последнем случае предварительно должны быть доказаны все утверждения о допустимости синтаксической подстановки, связанные с этой конкретизацией).

Будем говорить, что *предложение справедливо при совокупности предположений,* если оно либо получено в ре-

[1] Работа выполнена при финансовом содействии программы № 16 Президиума РАН, проект «Теоретические основы интеллектуальных систем, основанных на онтологиях, для интеллектуальной поддержки научных исследований» и программы № 16 ОЭММПУ РАН проект «Синтез интеллектуальных систем управления базами знаний и базами данных».

зультате доказательства с использованием этой совокупности предположений, либо является конкретизацией справедливого математического утверждения, с которой связана эта совокупность предположений.

Внутренняя модель математической практики содержит два правила рассуждения.

Декомпозиция. Если справедливо (при совокупности предположений) предложение f_1 & ... & $f_k \Rightarrow f$ и требуется доказать предложение f, то для этого достаточно доказать (при тех же предположениях) предложения f_1, ..., f_k.

Вывод. Если справедливо (при совокупности предположений) предложение f_1 & ... & $f_k \Rightarrow f$ и справедливы (при некоторых совокупностях предположений) предложения f_1, ..., f_k, то справедливо (при объединении всех этих предположений) предложение f.

2. МОДЕЛЬ ПОЛНОГО ДОКАЗАТЕЛЬСТВА

2.1. Вспомогательные понятия

С каждым предложением f, входящим в полное доказательство, свяжем множество (возможно, пустое) $t^+(f) = t_1^+(f) \cup t_2^+(f)$ предположений, при которых предложение f истинно, причем $t_1^+(f)$ есть множество предположений о свойствах произвольных объектов, а $t_2^+(f)$ — множество предположений о справедливости предложений, при которых истинно f. Если «$a \in t$» — предположение о свойствах произвольного объекта, то «$a \in t$» $\in t_1^+$(«$a \in t$»); если же f — предположение о справедливости предложения, то $t_2^+(f) = \{f\}$. Кроме того, с каждым предложением f, требующим доказательства, свяжем множество (возможно, пустое) $t^-(f) = t_1^-(f) \cup t_2^-(f)$ предположений, при которых предложение f должно быть доказано, причем $t_1^-(f)$ есть множество предположений о свойствах произвольных объектов, а $t_2^-(f)$ — множество предположений об истинности предложений, при которых f должно быть доказано. Если $t^+(f) = \varnothing$, то f справедливо безусловно; если $t^-(f) = \varnothing$, то f должно быть доказано без всяких предположений.

2.2. Определение модели полного доказательства

Модель полного доказательства математического утверждения $(v_1: t_1) \ldots (v_m: t_m)f$ есть доказательство предложений $t_1' \neq \varnothing$, ..., $t_m' \neq \varnothing$ и предложения f', являющегося конкретизацией формулы f, сделанной при полном наборе предположений P, связанных с этой конкретизацией; здесь t_1', ..., t_m' — результаты применения подстановки, при которой сделана эта конкретизация, к термам t_1, ..., t_m. Для $i = 1, \ldots, m$ имеет место $t^-(t_i' \neq \varnothing) = P$; кроме того, $t^-(f') = P$.

Модель полного доказательства предложения f_1 & ... & $f_k \Rightarrow f$ (имеющего форму импликации) есть доказательство предложения f в предположении, что справедливы предложения f_1 ,..., f_k. При этом $t^-(f) = t^-(f_1$ & ... & $f_k \Rightarrow f) \cup \{f_1$,..., $f_k\}$.

Модель полного доказательства предложения f, не имеющего форму импликации, может быть либо его декомпозицией, либо его выводом, либо пустым доказательством.

Декомпозиция предложения f есть результат применения правила декомпозиции к предложению f. Она характеризуется множеством компонент декомпозиции, каждая из которых состоит из предложения и его доказательства. Смысл декомпозиции состоит в том, что для доказательства предложения f достаточно доказать предложения всех компонент декомпозиции (задача поиска доказательства предложения сводится к множеству подзадач поиска доказательств предложений для всех компонент декомпозиции). Пусть в результате применения правила декомпозиции выдвигается множество предположений P (если предположения не выдвигаются, $P = \varnothing$). Если доказывается предложение f, и f_1, ..., f_m — предложения компонент декомпозиции, то для $i = 1, \ldots, m$ имеет место $t^-(f_i) = P \cup t^-(f)$.

Вывод предложения f характеризуется процессом вывода, на каждом шаге которого применяется правило вывода. Начальным состоянием процесса вывода является множество предложений $t^-(f)$. Если на текущем шаге в состоянии процесса вывода содержится предложение f, то процесс вывода завершается (если предложение f содержится в начальном состоянии, то процесс вывода является пустым). Если при этом $t^+(f) \subseteq t^-(f)$, где $t^+(f)$ получено в результате процесса вывода, то процесс вывода завершается нормально, и предложение f считается доказанным. Заметим, что если в том же самом или в другом доказательстве было получено такое $t^+(f)$, что выполнено $t^+(f) \subseteq t^-(f)$, то доказательством предложения f может служить ссылка на процесс вывода в том же самом или в другом доказательстве, где было получено это $t^+(f)$. Применение правила вывода на очередном шаге процесса вывода состоит в следующем. Если значения посылок правила вывода — предложения f_1, ..., f_m — справедливы (входят в текущее состояние процесса вывода или получаются в результате конкретизации), то состояние процесса вывода на следующем шаге получается из состояния на текущем шаге добавлением предложения f — результата применения правила вывода. Пусть в результате применения правила вывода выдвигается множество предположений P (если предположения не выдвигаются, $P = \varnothing$). Тогда $t^+(f) = P \cup t^+(f_1) \cup \ldots \cup t^+(f_m)$.

Модель доказательства справедливого предложения — пустое доказательство.

2.3. Примеры

Примеры определений терминов. Далее приводится запись на языке ММД нескольких определений из теории пределов последовательностей.

1. *Последовательности* $\equiv I[1, \infty) \to R$.

2. *Предел* ≡ (λ(*x*: последовательности)(*a*: *R*)(∀(ε: *R*(0, ∞))(∃(*N*: *I*[1, ∞)(∀(*n*: *I*[*N*, ∞))|*x*(*n*) − *a*| < ε))).

3. *Бесконечно малые величины* ≡ {(*x*: *последовательности*) *предел*(*x*, 0)}.

Примеры определений новых способов записи. Далее приводится запись на языке ММД нескольких определений новых способов записи.

4. (*v*: *R*)*R*(*v*, ∞) ≡ {(*w*: *R*)*w* > *v*}.

5. (*v*: *R*)|*v*| ≡ /(*v* ⩾ 0 ⇒ *v*)(*v* < 0 ⇒ −*v*)/.

6. (*v*: *R*) − *v* ≡ 0 − *v*.

7. (v_1: *I*)*I*[v_1, ∞) ≡ {(v_2: *I*)v_2 ⩾ v_1}.

8. (v_1: *I*)(v_2: *I*[v_1, ∞))*I*[v_1, v_2] ≡ {(v_3: *I*)v_3 ⩾ v_1 & v_3 ⩽ v_2}.

Примеры пропозициональных тавтологий. Доказательство равносильного утверждения:

9. (v_1: *L*)(v_2: *L*)(v_1 ⇒ v_2) & (v_2 ⇒ v_1) ⇒ (v_1 ⇔ v_2).

Доказательство от противного:

10. (*v*: *L*)(¬ *v* ⇒ ложь) ⇒ *v*.

Доказательство противоречия:

11. (*v*: *L*)*v* & ¬ *v* ⇒ ложь.

Примеры математических утверждений. Далее приводится примеры записи на языке ММД математических утверждений.

Теорема о единственности предела числовой последовательности:

12. (*x*: *последовательности*) (a_1: *R*)(a_2: *R*) *предел* (*x*, a_1) & *предел*(*x*, a_2) ⇒ a_1 = a_2.

Теорема о сумме членов конечного отрезка натурального ряда:

13. (*n*: *I*[0, ∞))(Σ(*i*: *I*[0, *n*])*i*) = *n* ∗ (*n* + 1)/2.

Правило приведения к общему знаменателю дроби и числа:

14. (*x*: *R*)(*y*: *R*\{0})(*z*: *R*)*x*/*y* + *z* = (*x* + *y* ∗ *z*)/*y*.

Правило выноса общего множителя за скобки:

15. (*x*: *R*)(*y*: *R*)(*z*: *R*)*x* * *y* + *z* * *y* = (*x* + *z*) * *y*.

Свойство коммутативности умножения:

16. (*x*: *R*)(*y*: *R*)*x* * *y* = *y* * *x*.

Примеры метаматематических утверждений. Далее приводятся примеры записи на метаязыке некоторых метаматематических утверждений.

Одна из форм принципа полной математической индукции:

17. (v_1: *I*[0, ∞)(v_2: *I*[0, v_1[)*f*⊢0⊣ & (*f*⊢v_2⊣ ⇒ *f*⊢v_2 + + 1⊣) ⇒ *f*⊢v_1⊣.

Свойство квантора Σ — сумма с одним слагаемым:

18. (*v*: *I*)(Σ(*v*: *I*[*v*, *v*])*t*⊢*v*⊣) = *t*-*v*⊣.

Свойство квантора Σ — добавление слагаемого в сумму:

19. (v_1: *I*)(v_2: *I*[v_1, ∞))(Σ(*v*: *I*[v_1, v_2 + 1])*t*⊢*v*⊣) = (Σ(*v*: *I*[v_1, v_2])*t*⊢*v*⊣) + *t*⊢v_2 + 1⊣.

Принцип замены равных термов (замена в формуле вхождения терма равным ему):

20. *f*⊢t_1⊣ & t_1 = t_2 ⇒ *f*⊢t_2⊣.

Пример формального доказательства. Доказывается теорема о сумме членов начального отрезка натурального ряда (см. пример 13).

Модель доказательства теоремы представлена в виде последовательности шагов, каждый из которых характеризуется правилом рассуждения, примененным на этом шаге, значениями посылок, возможно, способом конкретизации при их получении, значением заключения правила, а также, возможно, выдвинутыми предположениями.

Формулировка теоремы на языке ММД:

$$(n\colon I[0, \infty))(\Sigma(i\colon I[0, n])i) = n * (n + 1)/2.$$

Модель доказательства теоремы, по определению, есть доказательство предложений

$$I[0, \infty) \neq \varnothing \qquad (1)$$

и

$$(\Sigma(i\colon I[0, a])i) = a*(a + 1)/2 \qquad (2)$$

в предположении, что

$$a \in I[0, \infty).$$

Шаги доказательства:

1) *модель доказательства предложения* (1) здесь не приводится;

2) *модель доказательства предложения* (2):

из принципа полной математической индукции в примере 17 посредством конкретизации получается аксиома:

$$\begin{gathered}(v_1\colon I[0, \infty))(v_2\colon I[0, 1])(\Sigma(i\colon I[0, 0])i) = \\ = 0 \ \&\ ((\Sigma(i\colon I[0, v_2])i) = v_2 * (v_2 + 1)/2 \Rightarrow \\ \Rightarrow (\Sigma\ (i\colon I[0, v_2 + 1])i) = (v_2 + 1) * (v_2 + 2)/2) \Rightarrow \\ \Rightarrow (\Sigma(i\colon I[0, v])i) = v_1 * (v_1 + 1)/2; \end{gathered} \qquad (3)$$

из нее в предположении, что $b \in I[0, \infty]$, посредством конкретизации получается предложение

$$\begin{gathered}(\Sigma(i\colon I[0, 0])i) = 0 \ \&\ ((\Sigma(i\colon I[0, b])i) = b * (b + 1)/2 \Rightarrow \\ \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = (b + 1) * (b + 2)/2) \Rightarrow \\ \Rightarrow (\Sigma(i\colon I[0, a])i) = a * (a + 1)/2; \end{gathered} \qquad (4)$$

применяя предложение (4) для декомпозиции (2), получаем компоненты декомпозиции — предложения:

$$(\Sigma(i\colon I[0, 0])i) = 0 \qquad (5)$$

и

$$\begin{gathered}(\Sigma(i\colon I[0, b])i) = b * (b + 1)/2 \Rightarrow \\ \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = (b + 1) * (b + 2)/2; \end{gathered} \qquad (6)$$

3) *модель доказательства предложения* (5):

из свойства квантора **Σ** (сумма с одним слагаемым) в примере 18 посредством конкретизации получается аксиома:

$$(v\colon I)(\Sigma(i\colon I[v, v])i) = v;$$

из нее посредством конкретизации получается предложение (5) (пустое доказательство);

4) *модель доказательства предложения* (6), имеющего форму импликации, по определению, есть доказательство предложения

$$(\Sigma(i\colon I[0, b + 1])i) = (b + 1) * (b + 2)/2 \qquad (7)$$

в предположении, что

$$(\Sigma(i\colon I[0, b])i) = b * (b + 1)/2; \qquad (8)$$

5) *модель доказательства предложения* (7) есть вывод этого предложения.

Шаг 1 вывода предположения (7): из принципа замены равных термов в примере 20 посредством конкретизации получается предложение (аксиома):

$$(\Sigma(i\colon I[0, b + 1])i) = \\ = (\Sigma(i\colon I[0, b])i) + b + 1 \ \& \ (\Sigma(i\colon I[0, b])i) = \\ = b * (b + 1)/2 \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = \\ = b * (b + 1)/2 + b + 1; \qquad (9)$$

из свойства квантора Σ (добавление слагаемого в сумму) в примере 19 посредством конкретизации получается аксиома:

$$(v_1\colon I)(v_2\colon I[v_1, \infty))(\Sigma(i\colon I[v_1, v_2 + 1])i) = \\ = (\Sigma(i\colon I[v_1, v_2])i) + v_2 + 1;$$

из нее посредством конкретизации получается предложение

$$(\Sigma(i\colon I[0, b + 1])i) = (\Sigma(i\colon I[0, b])i) + b + 1;$$

из него и предположения (8) с учетом аксиомы (9) выводится предложение

$$(\Sigma(i\colon I[0, b + 1])i) = b * (b + 1)/2 + b + 1. \qquad (10)$$

Шаг 2 вывода предположения (7): из принципа замены равных термов в примере 20 посредством конкретизации получается предложение (аксиома)

$$(\Sigma(i\colon I[0, b + 1])i) = \\ = b * (b + 1)/2 + b + 1 \ \& \ b * (b + 1)/2 + b + 1 = \\ = (b * (b + 1) + 2 * (b + 1))/2 \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = \\ = (b * (b + 1) + 2 * (b + 1))/2; \qquad (11)$$

из математического утверждения в примере 14 посредством конкретизации получается предложение

$$b * (b + 1)/2 + b + 1 = (b * (b + 1) + 2 * (b + 1))/2; \qquad (12)$$

предварительно должно быть доказано, что $b*(b + 1) \in R$, $2 \in R\backslash\{0\}$, $b + 1 \in R$ (эти доказательства здесь не приводятся); из предложений (10) и (12) с учетом аксиомы (11) выводится предложение

$$(\Sigma(i\colon I[0, b + 1])i) = (b * (b + 1) + 2 * (b + 1))/2. \qquad (13)$$

Шаг 3 вывода предложения (7): из принципа замены равных термов в примере 20 посредством конкретизации получается предложение (аксиома)

$$(\Sigma(i\colon I[0, b + 1])i) = \\ = (b * (b + 1) + 2 * (b + 1))/2 \ \& \ b * (b + 1) + 2 * (b + 1) = \\ = (b + 2) * (b + 1) \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = \\ = (b + 2) * (b + 1)/2; \qquad (14)$$

из математического утверждения в примере 15 посредством конкретизации получается предложение

$$b * (b + 1) + 2 * (b + 1) = (b + 2) * (b + 1); \qquad (15)$$

из предложений (13) и (15) с учетом аксиомы (14) выводится предложение

$$(\Sigma(i\colon I[0, b + 1])i) = (b + 2) * (b + 1)/2. \qquad (16)$$

Шаг 4 вывода предложения (7): из принципа замены равных термов в примере 20 посредством конкретизации получается предложение (аксиома)

$$(\Sigma(i\colon I[0, b + 1])i) = \\ = (b + 2) * (b + 1)/2 \ \& \ (b + 2) * (b + 1) = \\ = (b + 1) * (b + 2) \Rightarrow (\Sigma(i\colon I[0, b + 1])i) = \\ = (b + 1) * (b + 2)/2; \qquad (17)$$

из математического утверждения в примере 16 посредством конкретизации получается предложение

$$(b + 2) * (b + 1) = (b + 1) * (b + 2); \qquad (18)$$

из предложений (16) и (18) с учетом аксиомы (17) выводится предложение (7).

ЗАКЛЮЧЕНИЕ

В цикле из трех статей [1, 2 и настоящая статья] предложена формальная система с расширяемым логико-математическим языком высокого порядка. Наряду с этим языком в формальной системе присутствуют язык пропозициональных утверждений для представления правил логических рассуждений и метаязык для представления свойств логических и нелогических кванторов, а также логических и нелогических принципов. Основным правилом вывода в формальной системе является Modus ponens. Так как набор метаматематических аксиом не фиксирован и может расширяться, традиционное понятие полноты исчисления оказывается неприменимым к этой формальной системе (что имеет место и для математической практики). Понятно, что отсутствие большинства ограничений, характерных для моделей математической логики, используемых в компьютерных системах доказательства теорем, еще не является гарантией того, что доказательства, представленные в предложенной формальной системе будут сопоставимы по сложности с математическими доказательствами. Поэтому одно из направлений дальнейших исследований заключается в экспериментальном изучении математических доказательств средствами этой формальной системы с целью выявления в них конструкций еще более высокого уровня.

ЛИТЕРАТУРА

1. *Гаврилова Т. Л., Клещев А. С.* Внутренняя модель математической практики для систем автоматизированного конструирования доказательств теорем. Ч. 1. Общее описание модели // Проблемы управления. — 2006. № 4. — С. 32—35.
2. *Гаврилова Т. Л., Клещев А. С.* Внутренняя модель математической практики для систем автоматизированного конструирования доказательств теорем. Ч. 2. Модель математического диалекта // Там же. — № 5.— С. 68—73.

☎ *(4232) 31-40-01, 31-04-24*

E-mail: gavrilov@iacp.dvo.ru ; kleschev@iacp.dvo.ru ❑