УДК 681.3.057.51-7.311.17

МОДЕЛЬ АНАЛОГИИ МЕЖДУ МАТЕМАТИЧЕСКИМИ ДОКАЗАТЕЛЬСТВАМИ[1]

А. С. Клещев

Институт автоматики и процессов управления ДВО РАН, г. Владивосток

На основе расширяемой модели математической практики построена модель аналогии между доказательствами. Исходное доказательство обобщается путем замены некоторых его частей глобальными синтаксическими переменными; целевое доказательство получается из обобщения как результат применения к нему синтаксической подстановки вместо глобальных синтаксических переменных. Задачи обнаружения аналогии, построения целевого доказательства по аналогии, генерации лемм, необходимых для построения целевого доказательства по аналогии, а также генерации теорем, аналогичных исходной, состоят в поиске такой синтаксической подстановки.

ВВЕДЕНИЕ

Считается, что в своей деятельности математики почти всегда пользуются аналогией: они интуитивно обнаруживают сходство между математическими структурами на различных уровнях абстракции и опираются на него при решении новых проблем, в частности, при построении доказательств. Рассматривая те или иные свойства аналогии как существенные, авторы приходили к различным моделям аналогии между доказательствами.

В работе [1] аналогия рассматривалась как отношение между двумя теоремами, при котором имеется соответствие между множествами входящих в них символов. Модель такой аналогии строилась в виде графа соответствия между множествами символов этих теорем.

В более поздних работах аналогия рассматривалась как отношение эквивалентности: исходная теорема и ее доказательство обобщались до некоторого класса эквивалентности (два доказательства считаются аналогичными, если они входят в один и тот же класс эквивалентности). В работе [2] были введены «абстракции теорем» — операции над множеством клауз и мульти-клауз, которые сохраняют корректность при каждом применении бинарной резолюции. В работе [3] использовалась парадигма «предложения как типы», в соответствии с которой доказательства представлялись как термы. Доказательство исходной теоремы преобразуется в терм, из которого может быть получено доказательство аналогичного предложения с использованием сопоставления с образцом второго порядка, содержащим переменные функциональные символы. В работе [4] основная идея состояла в том, чтобы трансформировать доказательство исходной теоремы в более общее множество доказательств. Для этого было введено понятие «наиболее общая теорема». Ее доказательство преобразуется в терм второго порядка, к которому применяется множество правил обобщения, причем функциональные и предикатные символы, входящие в исходное доказательство, используются как переменные второго порядка. В качестве альтернативной модели множества аналогичных доказательств в работе [5] использовался план доказательства, состоящий из методов, которые являются спецификациями тактик (два доказательства, построенные по одному плану, аналогичны).

С моделированием аналогии между доказательствами теорем связаны различные задачи: автоматическое обнаружение аналогии; автоматическое построение доказательства новой теоремы с помощью доказательства старой; автоматическая генерация таких лемм, что их справедливость необходима для построения доказательства новой теоремы с помощью доказательства старой; автоматическая генерация новых теорем вместе с их доказательствами, аналогичных старым теоремам. В литературе, посвященной моделированию аналогии между доказательствами, рассматривались лишь первые три задачи.

Таким образом, к настоящему времени достигнуты определенные успехи в моделировании аналогии между математическими доказательствами и в решении некоторых задач, связанных с аналогией. Однако в основе этих моделей лежит слишком грубая модель математической практики (исчисление предикатов или его модификации), что делает слишком грубой и саму модель аналогии: в одних моделях аналогичными считаются доказательства, которые отличаются друг от друга лишь используемой терминологией; в других — которые могут быть получены с помощью одних и тех же процедур, декларативное представление которых не всегда является полным; не все задачи, связанные с аналогией, могут быть удовлетворительно решены с помощью этих моделей.

[1] Работа выполнена при финансовой поддержке РФФИ, проект 06-07-89071-а «Исследование возможностей коллективного управления в семантическом вебе информационными ресурсами различных уровней общности», и ДВО РАН в рамках Программы №15 ОЭММПУ РАН, проект «Синтез интеллектуальных систем управления базами знаний и базами данных».

В работе [6] предложена расширяемая модель математической практики (РММП), в которой семантика языка для представления математических знаний определяется содержанием базы знаний, а не исчислением. В настоящей работе на основе этой модели определяется модель аналогии между доказательствами, позволяющая поставить и решить все упомянутые выше задачи, связанные с аналогией.

1. МОДЕЛЬ АНАЛОГИИ МЕЖДУ ДОКАЗАТЕЛЬСТВАМИ

В настоящей работе, как и в ряде работ, упомянутых во Введении, аналогия рассматривается как отношение эквивалентности, а ее модель строится как обобщение доказательства исходной теоремы, т. е. как класс эквивалентности, содержащий исходное доказательство. Для построения модели аналогии вводится новый класс синтаксических переменных.

Синтаксические переменные уже использовались в РММП; их вхождение является отличительным признаком метаматематических аксиом. Областью действия каждой такой синтаксической переменной является метаматематическая аксиома, в которую эта переменная входит. Будем называть такие синтаксические переменные локальными. Локальная синтаксическая переменная заменяется подходящим значением из синтаксической подстановки при выполнении конкретизации метаматематической аксиомы на шаге доказательства. В отличие от локальных, областью действия вводимых здесь глобальных синтаксических переменных является все доказательство. Глобальные синтаксические переменные имеют те же типы, что и локальные, и такие же обозначения, с той лишь разницей, что тип глобальной переменной обозначается соответствующей прописной буквой. Таким образом, будем говорить о глобальных синтаксических переменных типа $\boldsymbol{F}$ (формулы), $\boldsymbol{T}$ (термы) и др. Глобальные синтаксические переменные, также как и локальные, могут быть модифицированы.

Назовем метарассуждением последовательность шагов (имеющую форму доказательства), в которую входит хотя бы одна глобальная синтаксическая переменная. Будем называть метадоказательством такое метарассуждение, для которого существует допустимая синтаксическая подстановка вместо глобальных синтаксических переменных, такая, что результат ее применения к метарассуждению является доказательством некоторой теоремы. Последнее означает, что все шаги полученного доказательства являются правильными применениями правил рассуждения, все утверждения, входящие в полученное доказательство, корректны, а все утверждения, относящиеся к базе знаний, в ней содержатся.

Заголовок метадоказательства будем называть метатеоремой. Математическое утверждение, получаемое из метатеоремы с помощью синтаксической подстановки, будет теоремой лишь в том случае, если расширение этой синтаксической подстановки позволяет получить доказательство этой теоремы из метадоказательства этой метатеоремы. Метадоказательство назовем обобщением исходного доказательства, если это доказательство может быть получено из этого метадоказательства при некоторой синтаксической подстановке. Два доказательства будем считать аналогичными, если они могут быть получены из одного и того же метадоказательства при разных синтаксических подстановках. Модель аналогии сохраняет взаимно-однозначное соответствие между шагами аналогичных доказательств, а также логические и нелогические рассуждения на соответствующих шагах этих доказательств.

Пример 1. Теорема:

последовательности $\neq \varnothing$. (1.1)

Доказательство (содержащее шаги декомпозиции и конкретизации).

Декомпозиция. Используем метаматематическую аксиому $\boldsymbol{t_1} = \boldsymbol{t_2}$ & $\boldsymbol{f}\vdash\boldsymbol{t_2}\dashv \Rightarrow \boldsymbol{f}\vdash\boldsymbol{t_1}\dashv$. Из определения: последовательности $\equiv I[1, \infty) \to R$ следует, что для доказательства (1.1) достаточно доказать

$$I[1, \infty) \to R \neq \varnothing. \quad (1.2)$$

Декомпозиция. Используем аксиому $(v_1 : S)(v_2 : S)v_1 \neq \neq \varnothing$ & $v_2 \neq \varnothing \Rightarrow v_1 \to v_2 \neq \varnothing$. Для доказательства (1.2) достаточно доказать

$$I[1, \infty) \in S, \quad (1.3)$$

$$R \in S, \quad (1.4)$$

$$I[1, \infty) \neq \varnothing, \quad (1.5)$$

$$R \neq \varnothing. \quad (1.6)$$

Декомпозиция. Используем аксиому $(v : I)I[v, \infty) \in S$. Для доказательства утверждения (1.3) достаточно доказать

$$1 \in I. \quad (1.7)$$

Конкретизация. Утверждение (1.7) следует из метаматематической аксиомы $\boldsymbol{i} \in I$.

Конкретизация. Утверждение (1.4) совпадает с аксиомой.

Конкретизация. Утверждение (1.5) следует из аксиомы $(v : I)I[v, \infty) \neq \varnothing$ и (1.7).

Конкретизация. Утверждение (1.6) совпадает с математической аксиомой.

Пример 2. Обобщение примера 1. Метатеорема:

$$\boldsymbol{F_1}\vdash\boldsymbol{T_1}\dashv. \quad (2.1)$$

Метадоказательство.

Декомпозиция. Используем метаматематическую аксиому $\boldsymbol{t_1} = \boldsymbol{t_2}$ & $\boldsymbol{f}\vdash\boldsymbol{t_2}\dashv \Rightarrow \boldsymbol{f}\vdash\boldsymbol{t_1}\dashv$. Из утверждения базы знаний $\boldsymbol{T_1} = \boldsymbol{T_2}\vdash\boldsymbol{T_5}\vdash\boldsymbol{I}\dashv$, $\boldsymbol{T_6}\dashv$ следует, что для доказательства (2.1) достаточно доказать

$$\boldsymbol{F_1}\vdash\boldsymbol{T_2}\vdash\boldsymbol{T_5}\vdash\boldsymbol{I}\dashv,\ \boldsymbol{T_6}\dashv\dashv. \quad (2.2).$$

Декомпозиция. Используем утверждение базы знаний $(v_1 : \boldsymbol{T_3})(v_2 : \boldsymbol{T_4})\boldsymbol{F_2}\vdash v_1\dashv$ & $\boldsymbol{F_3}\vdash v_2\dashv \Rightarrow \boldsymbol{F_1}\vdash\boldsymbol{T_2}\vdash v_1$, $v_2\dashv\dashv$. Для доказательства (2.2) достаточно доказать

$$\boldsymbol{T_5}\vdash\boldsymbol{I}\dashv \in \boldsymbol{T_3}, \quad (2.3)$$

$$\boldsymbol{T_6} \in \boldsymbol{T_4}, \quad (2.4)$$

$$\boldsymbol{F_2}\vdash\boldsymbol{T_5}\vdash\boldsymbol{I}\dashv\dashv, \quad (2.5)$$

$$\boldsymbol{F_3}\vdash\boldsymbol{T_6}\dashv. \quad (2.6)$$

Декомпозиция. Используем утверждение базы знаний $(v : I)\boldsymbol{T_5}\vdash v\dashv \in \boldsymbol{T_3}$. Для доказательства утверждения (2.3) достаточно доказать $\boldsymbol{I} \in I$. (2.7)

Конкретизация. Утверждение (2.7) следует из метаматематической аксиомы $\boldsymbol{i} \in I$.

Конкретизация. Утверждение (2.4) совпадает с утверждением базы знаний.

Конкретизация. Утверждение (2.5) следует из утверждения базы знаний $(v : I)\boldsymbol{F_2}\vdash\boldsymbol{T_5}\vdash v\dashv\dashv$ и (2.7).

Конкретизация. Утверждение (2.6) совпадает с утверждением базы знаний.

Доказательство примера 1 получается из метадоказательства примера 2 при следующей синтаксической подстановке: $\boldsymbol{I}$: 1, $\boldsymbol{T_1}$: последовательности, $\boldsymbol{T_2}$: $\tau_1 \to \tau_2$, $\boldsymbol{T_3}$: S, $\boldsymbol{T_4}$: S, $\boldsymbol{T_5}$: $I[\tau, \infty)$, $\boldsymbol{T_6}$: R, $\boldsymbol{F_1}$: $\tau \neq \varnothing$, $\boldsymbol{F_2}$: $\tau \neq \varnothing$, $\boldsymbol{F_3}$: $\tau \neq \varnothing$, где τ (с индексом или без него) обозначают места вставки элементов модификатора в формулу или терм.

Пример 3. Теорема:

$$(x\text{: последовательности})(a\text{: } R)(p\text{: } R)\ \text{предел}\ (x, a)\ \&\ a > p \Rightarrow (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))\ x(n) > p)). \quad (3.1)$$

(Теорема о единственности предела еще не доказана, поэтому «предел» определен как двухместный предикат.)

Доказательство (содержащее шаги вывода и применение специальных правил). Пусть

$$x^* \in \text{последовательности}, \quad (3.2)$$

$$a^* \in R, \quad (3.3)$$

$$p^* \in R. \quad (3.4)$$

Для доказательства утверждения (3.1) достаточно доказать:

$$\text{предел}\ (x^*, a^*)\ \&\ a^* > p^* \Rightarrow (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))\ x^*(n) > p^*)). \quad (3.5)$$

Пусть

$$\text{предел}\ (x^*, a^*), \quad (3.6),$$

$$a^* > p^*. \quad (3.7)$$

Для доказательства утверждения (3.5) достаточно доказать

$$(\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))\ x^*(n) > p^*)). \quad (3.8)$$

Вывод. Используем **лемму 1:**

$$(x\text{: последовательности})(a\text{: } R)(\varepsilon\text{: } R(0, \infty))\text{предел}(x, a) \Rightarrow (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x(n) - a| < \varepsilon)).$$

Пусть

$$\varepsilon^* \in R(0, \infty). \quad (3.9)$$

Из выражений (3.2), (3.3), (3.9) и (3.6) следует

$$(\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x^*(n) - a^*| < \varepsilon^*)). \quad (3.10)$$

Вывод. Используем **лемму 2:**

$$(x\text{: последовательности})(a\text{: } R)(p\text{: } R)(\varepsilon\text{: } R(0, \infty))a > p\ \&\ (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x(n) - a| < \varepsilon)) \Rightarrow (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x(n) - a| < a - p)).$$

Из выражений (3.2), (3.3), (3.4), (3.9), (3.7) и (3.10) следует

$$(\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x^*(n) - a^*| < a^* - p^*)). \quad (3.11)$$

Вывод. Используем **лемму 3:**

$$(x\text{: последовательности})(a\text{: } R)(p\text{: } R)(v_3\text{: } \{(v_1\text{: } I[1, \infty))(\forall(v_2\text{: } I[v_1, \infty))|x(v_2) - a| < a - p)\})(v_4\text{: } I[v_3, \infty))a > p\ \&\ (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))|x(n) - a| < a - p)) \Rightarrow |x(v_4) - a| < a - p.$$

Пусть

$$N^* \in \{(v_1\text{: } I[1, \infty))(\forall(v_2\text{: } I[v_1, \infty))|x^*(v_2) - a^*| < a^* - p^*)\}, \quad (3.12)$$

$$n^* \in I[N^*, \infty). \quad (3.13)$$

Из выражений (3.2), (3.3), (3.4), (3.12), (3.13), (3.7) и (3.11) следует

$$|x^*(n^*) - a^*| < a^* - p^*. \quad (3.14)$$

Вывод. Используем **лемму 4:**

$$(x\text{: последовательности})(a\text{: } R)(p\text{: } R)(N\text{: } \{(v_1\text{: } I[1, \infty))(\forall(v_2\text{: } I[v_1, \infty))|x(v_2) - a| < a - p)\})(n\text{: } I[N, \infty))a > p\ \&\ |x(n) - a| < a - p \Rightarrow x(n) > p.$$

Из выражений (3.2), (3.3), (3.4), (3.12), (3.13), (3.7) и (3.14) следует

$$x^*(n^*) > p^*. \quad (3.15)$$

Вывод. Используем **лемму 5:**

$$(x\text{: последовательности})(a\text{: } R)(p\text{: } R)(v_3\text{: } \{(v_1\text{: } I[1, \infty))(\forall(v_2\text{: } I[v_1, \infty))\ |x(v_2) - a| < a - p)\})(v_4\text{: } I[v_3, \infty))a > p\ \&\ x(v_4) > p \Rightarrow (\exists(N\text{: } I[1, \infty))(\forall(n\text{: } I[N, \infty))x(n) > p)).$$

Из выражений (3.2), (3.3), (3.4), (3.12), (3.13), (3.7) и (3.15) следует (3.8).

Пример 4. Обобщение примера 3. Метатеорема:

$$(x\text{: } \boldsymbol{T_1})(a\text{: } \boldsymbol{T_2})(p\text{: } \boldsymbol{T_3})\boldsymbol{F_1}\vdash x,\ a\dashv\ \&\ \boldsymbol{F_2}\vdash a,\ p\dashv \Rightarrow \boldsymbol{F_3}\vdash x,\ p\dashv. \quad (4.1)$$

Метадоказательство.

Пусть $\boldsymbol{A_1} \in \boldsymbol{T_1}$, (4.2)

$\boldsymbol{A_2} \in \boldsymbol{T_2}$, (4.3)

$\boldsymbol{A_3} \in \boldsymbol{T_3}$, (4.4)

Для доказательства утверждения (4.1) достаточно доказать

$$\boldsymbol{F_1}\vdash\boldsymbol{A_1},\ \boldsymbol{A_2}\dashv\ \&\ \boldsymbol{F_2}\vdash\boldsymbol{A_2},\ \boldsymbol{A_3}\dashv \Rightarrow \boldsymbol{F_3}\vdash\boldsymbol{A_1},\ \boldsymbol{A_3}\dashv. \quad (4.5)$$

Пусть

$$\boldsymbol{F_1}\vdash\boldsymbol{A_1},\ \boldsymbol{A_2}\dashv, \quad (4.6)$$

$$\boldsymbol{F_2}\vdash\boldsymbol{A_2},\ \boldsymbol{A_3}\dashv. \quad (4.7)$$

Для доказательства утверждения (4.5) достаточно доказать

$$\boldsymbol{F_3}\vdash\boldsymbol{A_1},\ \boldsymbol{A_3}\dashv. \quad (4.8)$$

Вывод. Используем утверждение базы знаний $(x\text{: } \boldsymbol{T_1})(a\text{: } \boldsymbol{T_2})(\varepsilon\text{: } \boldsymbol{T_4})\boldsymbol{F_1}\vdash x,\ a\dashv \Rightarrow \boldsymbol{F_4}\vdash x,\ a,\ \varepsilon\dashv$. Пусть

$$\boldsymbol{A_4} \in \boldsymbol{T_4}. \quad (4.9)$$

Из выражений (4.2), (4.3), (4.9) и (4.6) следует

$$\boldsymbol{F_4}\vdash\boldsymbol{A_1},\ \boldsymbol{A_2},\ \boldsymbol{A_4}\dashv. \quad (4.10)$$

Вывод. Используем утверждение базы знаний $(x\text{: } \boldsymbol{T_1})(a\text{: } \boldsymbol{T_2})(p\text{: } \boldsymbol{T_3})(\varepsilon\text{: } \boldsymbol{T_4})\boldsymbol{F_2}\vdash a,\ p\dashv\ \&\ \boldsymbol{F_4}\vdash x,\ a,\ \varepsilon\dashv \Rightarrow \boldsymbol{F_5}\vdash x,\ a,\ p\dashv$. Из выражений (4.2), (4.3), (4.4), (4.9), (4.7) и (4.10) следует

$$\boldsymbol{F_5}\vdash\boldsymbol{A_1},\ \boldsymbol{A_2},\ \boldsymbol{A_3}\dashv. \quad (4.11)$$

Вывод. Используем утверждение базы знаний $(x\text{: } \boldsymbol{T_1})(a\text{: } \boldsymbol{T_2})(p\text{: } \boldsymbol{T_3})(v_3\text{: } \boldsymbol{T_5}\vdash x,\ a,\ p\dashv)(v_4\text{: } \boldsymbol{T_6}\vdash v_3\dashv)\boldsymbol{F_2}\vdash a,\ p\dashv\ \&\ \boldsymbol{F_5}\vdash x,\ a,\ p\dashv \Rightarrow \boldsymbol{F_6}\vdash x,\ v_4,\ a,\ p\dashv$.

Пусть

$$\boldsymbol{A_5} \in \boldsymbol{T_5}\vdash\boldsymbol{A_1},\ \boldsymbol{A_2},\ \boldsymbol{A_3}\dashv, \quad (4.12),$$

$$\boldsymbol{A_6} \in \boldsymbol{T_6}\vdash\boldsymbol{A_5}\dashv. \quad (4.13).$$

Из выражений (4.2), (4.3), (4.4), (4.12), (4.13), (4.7) и (4.11) следует

$$\boldsymbol{F_6}\vdash\boldsymbol{A_1},\ \boldsymbol{A_6},\ \boldsymbol{A_2},\ \boldsymbol{A_3}\dashv. \quad (4.14)$$

Вывод. Используем утверждение базы знаний $(x\colon \boldsymbol{T}_1)(a\colon \boldsymbol{T}_2)(p\colon \boldsymbol{T}_3)(N\colon \boldsymbol{T}_5\vdash x, a, p\dashv)(n\colon \boldsymbol{T}_6\vdash N\dashv)\boldsymbol{F}_2\vdash a, p\dashv$ & $\boldsymbol{F}_6\vdash x, n, a, p\dashv \Rightarrow \boldsymbol{F}_7\vdash x, n, p\dashv$. Из выражений (4.2), (4.3), (4.4), (4.12), (4.13), (4.7) и (4.14) следует

$$\boldsymbol{F}_7\vdash \boldsymbol{A}_1, \boldsymbol{A}_6, \boldsymbol{A}_3\dashv. \qquad (4.15)$$

Вывод. Используем утверждение базы знаний $(x\colon \boldsymbol{T}_1)(a\colon \boldsymbol{T}_2)(p\colon \boldsymbol{T}_3)(v_3\colon \boldsymbol{T}_5\vdash x, a, p\dashv)(v_4\colon \boldsymbol{T}_6\vdash v_3\dashv)\boldsymbol{F}_2\vdash a, p\dashv$ & $\boldsymbol{F}_7\vdash x, v_4, p\dashv \Rightarrow \boldsymbol{F}_3\vdash x, p\dashv$.

Из выражений (4.2), (4.3), (4.4), (4.12), (4.13), (4.7) и (4.15) следует (4.8).

Доказательство примера 3 получается из метадоказательства примера 4 при следующей синтаксической подстановке: $\boldsymbol{T}_1$: последовательности, $\boldsymbol{T}_2$: R, $\boldsymbol{T}_3$: R, $\boldsymbol{T}_4$: $R(0, \infty)$, $\boldsymbol{T}_5$: $\{(v_1\colon I[1, \infty))(\forall(v_2\colon I[v_1, \infty))|\boldsymbol{\tau}_1(v_2) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_2 - \boldsymbol{\tau}_3)\}$, $\boldsymbol{T}_6$: $I[\boldsymbol{\tau}, \infty)$, $\boldsymbol{F}_1$: предел $(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$, $\boldsymbol{F}_2$: $\boldsymbol{\tau}_1 > \boldsymbol{\tau}_2$, $\boldsymbol{F}_3$: $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))\boldsymbol{\tau}_1(n) > \boldsymbol{\tau}_2))$, $\boldsymbol{F}_4$: $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))|\boldsymbol{\tau}_1(n) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_3))$, $\boldsymbol{F}_5$: $(\exists(N\colon I[1, \infty)) \times (\forall(n\colon I[N, \infty))\ |\boldsymbol{\tau}_1(n) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_2 - \boldsymbol{\tau}_3))$, $\boldsymbol{F}_6$: $|\boldsymbol{\tau}_1(\boldsymbol{\tau}_2) - \boldsymbol{\tau}_3| < \boldsymbol{\tau}_3 - \boldsymbol{\tau}_4$, $\boldsymbol{F}_7$: $\boldsymbol{\tau}_1(\boldsymbol{\tau}_2) > \boldsymbol{\tau}_3$.

2. ОБОБЩЕНИЕ ДОКАЗАТЕЛЬСТВ

Обобщение доказательства состоит в замене глобальными синтаксическими переменными (возможно модифицированными) тех его частей, которые участвуют в применении правил рассуждения на каждом шаге доказательства. Те части доказательства, которые являются унифицируемыми, должны оставаться унифицируемыми и после обобщения.

Пропозициональные тавтологии и метаматематические аксиомы, входящие в доказательство, переходят в метадоказательство без изменений (они представляют правила логического и нелогического рассуждения, сохраняемые аналогией). В математических утверждениях базы знаний, применяемых в доказательстве на шагах декомпозиции и вывода и имеющих вид $(v_1\colon t_1)...(v_m\colon t_m)$ f_1 &...& $f_n \Rightarrow f$, при переходе к метадоказательству термы t_1, ..., t_m обозначаются глобальными синтаксическими переменными типа $\boldsymbol{T}$, а формулы f_1, ..., f_m и f — глобальными синтаксическими переменными типа $\boldsymbol{F}$, причем если эти термы или формулы содержат вхождения свободных переменных, то обозначающие их глобальные синтаксические переменные являются модифицированными, а в качестве элементов модификаторов выступают эти свободные переменные. В математических утверждениях базы знаний, применяемых в доказательстве на шагах конкретизации и в промежуточных выводах и имеющих вид $(v_1\colon t_1)...(v_m\colon t_m)f$, при переходе к метадоказательству термы t_1, ..., t_m обозначаются глобальными синтаксическими переменными типа $\boldsymbol{T}$, а формула f — глобальной синтаксической переменной типа $\boldsymbol{F}$. Модификация этих глобальных синтаксических переменных выполняется, как и выше. Если математическое определение унифицируется с равенством, то обе его части обозначаются разными глобальными синтаксическими переменными типа $\boldsymbol{T}$.

3. ОБНАРУЖЕНИЕ АНАЛОГИИ И ПОСТРОЕНИЕ ДОКАЗАТЕЛЬСТВА ЦЕЛЕВОЙ ТЕОРЕМЫ

Метатеорема и ее метадоказательство, полученные обобщением доказательства некоторой исходной теоремы, добавляются в базу знаний подобно тому, как это делается в работе [4]. Обнаружение аналогии для новой целевой теоремы состоит из двух этапов.

На первом из них осуществляется поиск такой метатеоремы в базе знаний, для которой удается построить синтаксическую подстановку вместо глобальных синтаксических переменных, входящих в эту метатеорему, результат применения которой к метатеореме дает целевую теорему.

На втором этапе для каждой найденной метатеоремы делается попытка построить доказательство целевой теоремы с помощью метадоказательства. Часть глобальных синтаксических переменных метадоказательства уже получили значения в результате выполнения первого этапа. Значения остальных ищутся в ходе сопоставления обобщенных математических утверждений из метадоказательства, относящихся к базе знаний, с математическими утверждениями, хранящимися в базе знаний. Если в результате этого процесса значения всех глобальных синтаксических переменных метадоказательства будут найдены, доказательство целевой теоремы будет построено.

Пример 5. Использование метадоказательства примера 4 для построения по аналогии доказательства целевой теоремы: $(x\colon$ последовательности$)(a\colon R)(p\colon R)$ предел (x, a) & $a < p \Rightarrow (\exists(N\colon I[1, \infty))\ (\forall(n\colon I[N, \infty))\ x(n) < p))$. Сопоставление целевой теоремы с метатеоремой примера 4 позволяет определить значения следующих глобальных синтаксических переменных: $\boldsymbol{T}_1$: последовательности, $\boldsymbol{T}_2$: R, $\boldsymbol{T}_3$: R, $\boldsymbol{F}_1$: предел $(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$, $\boldsymbol{F}_2$: $\boldsymbol{\tau}_1 < \boldsymbol{\tau}_2$, $\boldsymbol{F}_3$: $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))\boldsymbol{\tau}_1(n) < \boldsymbol{\tau}_2))$.

Сопоставление **леммы 1** с обобщенным утверждением, применяемым на первом шаге вывода в метадоказательстве, позволяет определить значения следующих глобальных синтаксических переменных: $\boldsymbol{T}_4$: $R(0, \infty)$, $\boldsymbol{F}_4$: $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))|\boldsymbol{\tau}_1(n) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_3))$.

Сопоставление **леммы 6** $(x\colon$ последовательности$)$ $(a\colon R)(p\colon R)(\varepsilon\colon R(0, \infty))$ $a < p$ & $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))|x(n) - a| < \varepsilon)) \Rightarrow (\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))\ |x(n) - a| < p - a))$ с обобщенным утверждением, применяемым на втором шаге вывода в метадоказательстве, позволяет определить значение глобальной синтаксической переменной $\boldsymbol{F}_5$: $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))|\boldsymbol{\tau}_1(n) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_3 - \boldsymbol{\tau}_2))$.

Сопоставление **леммы 7** $(x\colon$ последовательности$)$ $(a\colon R)(p\colon R)(v_3\colon \{(v_1\colon I[1, \infty))(\forall(v_2\colon I[v_1, \infty))|x(v_2) - a| < p - a)\})(v_4\colon I[v_3, \infty))a < p$ & $(\exists(N\colon I[1, \infty))(\forall(n\colon I[N, \infty))|x(n) - a| < p - a)) \Rightarrow |x(v_4) - a| < p - a$ с обобщенным утверждением, применяемым на третьем шаге вывода в метадоказательстве, позволяет определить значения следующих глобальных синтаксических переменных: $\boldsymbol{T}_5$: $\{(v_1\colon I[1, \infty))(\forall(v_2\colon I[v_1, \infty))\ |\boldsymbol{\tau}_1(v_2) - \boldsymbol{\tau}_2| < \boldsymbol{\tau}_3 - \boldsymbol{\tau}_2)\}$, $\boldsymbol{T}_6$: $I[\boldsymbol{\tau}, \infty)$, $\boldsymbol{F}_6$: $|\boldsymbol{\tau}_1(\boldsymbol{\tau}_2) - \boldsymbol{\tau}_3| < \boldsymbol{\tau}_4 - \boldsymbol{\tau}_3$.

Сопоставление **леммы 8** $(x\colon$ последовательности$)$ $(a\colon R)(p\colon R)(N\colon \{(v_1\colon I[1, \infty))(\forall(v_2\colon I[v_1, \infty))\ |x(v_2) - a| < p - a)\})(n\colon I[N, \infty))\ a < p$ & $|x(n) - a| < p - a \Rightarrow x(n) < p$

с обобщенным утверждением, применяемым на четвертом шаге вывода в метадоказательстве, позволяет определить значение глобальной синтаксической переменной $\boldsymbol{F_7}$: $\boldsymbol{\tau_1(\tau_2) < \tau_3}$.

Сопоставление **леммы 9** (x: последовательности) (a: R)(p: R)(v_3: {(v_1: $I[1, \infty)$)($\forall$(v_2: $I[v_1, \infty)$) $|x(v_2) - a| < p - a$)})(v_4: $I[v_3, \infty)$) $a < p$ & $x(v_4) < p \Rightarrow$ ($\exists$(N: $I[1, \infty) \times$ ($\forall$(n: $I[N, \infty)$) $x(n) < p$)) с обобщенным утверждением, применяемым на пятом шаге вывода в метадоказательстве, позволяет завершить построение доказательства. Легко видеть, что леммы 6—9 могут быть доказаны по аналогии с леммами 2—5.

Формирование такой совокупности лемм, что доказательство теоремы состоит из шагов, на каждом из которых используется одна из них для декомпозиции или вывода, позволяет перенести смысловые части доказательства теоремы в доказательства соответствующих лемм (как в примере 5). При обобщении такого доказательства используемые леммы обобщаются «внешним» образом: сохраняется такая форма этих лемм, которая необходима для аналогии при их применении. «Внутреннее» обобщение этих лемм, получаемое на основе обобщения их доказательств, может существенно отличаться от внешнего. В этом случае аналогия между доказательствами двух теорем не требует аналогии между доказательствами соответствующих лемм; требуется лишь, чтобы форма этих лемм соответствовала внешнему обобщению. Поэтому предложенная модель аналогии является более общей, чем в работе [5].

4. ГЕНЕРАЦИЯ ЛЕММ С ИСПОЛЬЗОВАНИЕМ АНАЛОГИИ

Рассмотрим, сначала, использование полной аналогии для решения этой задачи. Если при построении доказательства целевой теоремы на основе метадоказательства для некоторого обобщенного утверждения, относящегося к базе знаний, не удается найти его конкретизацию в базе знаний, то может быть сгенерирована лемма (гипотеза), доказательство которой позволит продолжить построение доказательства целевой теоремы по аналогии. Если все глобальные синтаксические переменные, входящие в это обобщенное утверждение, уже получили значения до генерации этой леммы, то может быть сгенерирована ее точная формулировка. Если же некоторые глобальные синтаксические переменные к этому моменту еще не получили значений, то может быть сгенерирован лишь образец леммы, содержащий эти синтаксические переменные. По этому образцу пользователь, строящий доказательство целевой теоремы, должен уточнить формулировку леммы, задав значения этих синтаксических переменных. В примере 5, если лемма 6 отсутствует в базе знаний, может быть сгенерирован ее образец (x: последовательности)(a: R)(p: R)(ε: $R(0, \infty)$) $a < p$ & ($\exists$(N: $I[1, \infty)$)($\forall$(n: $I[N, \infty)$)$|x(n) - a| < \varepsilon$)) $\Rightarrow \boldsymbol{F_5}\vdash x, a, p\vdash$. Если же в базе знаний отсутствует лемма 9, то ее формулировка (а не образец) может быть сгенерирована автоматически.

Теперь рассмотрим использование частичной аналогии для генерации лемм. Предположим, что для какого-либо утверждения компонента декомпозиции некоторого шага доказательства не удалось построить его доказательства с использованием метадоказательства (в примере 1 не удалось построить доказательство утверждения (1.5) с использованием метадоказательства примера 2). Тогда из обобщенного утверждения этого компонента декомпозиции метадоказательства (обобщенного утверждения (2.5) примера 2) может быть сгенерирована лемма (или ее образец), доказательство которой может не зависеть от исходного метадоказательства. Остальная же часть доказательства целевой теоремы (за исключением доказательства сгенерированной леммы) может строиться на основе этого метадоказательства. Частичная аналогия для генерации лемм в случае вывода может использоваться способом, похожим на предложенный в работе [4].

5. ГЕНЕРАЦИЯ АНАЛОГИЧНЫХ ТЕОРЕМ И ИХ ДОКАЗАТЕЛЬСТВ

Если для заданного метадоказательства удается найти такую синтаксическую подстановку вместо глобальных синтаксических переменных, результат применения которой к этому метадоказательству является доказательством, то результат применения этой подстановки к метатеореме является теоремой. Легко видеть, что для заданных целевого доказательства и состояния базы знаний по обобщению этого доказательства за конечное число шагов могут быть найдены все теоремы (вместе с их доказательствами), аналогичные целевой, или установлено, что таких теорем нет. Теорема примера 5 может быть сгенерирована по метадоказательству примера 4 и состоянию базы знаний, содержащему леммы 1 и 6—9.

ЗАКЛЮЧЕНИЕ

Аналогия является одним из способов сокращения перебора при построении доказательств. Чем богаче модель математической практики, тем глубже может быть аналогия. В предложенной модели аналогии обобщение доказательств соответствует индуктивной части аналогии. Построение доказательства по аналогии и генерация аналогичных теорем соответствует ее дедуктивной части. Наконец, генерация лемм, поддерживающих построение доказательства по аналогии, соответствует ее абдуктивной части.

ЛИТЕРАТУРА

1. *Owen S.* Analogy for automated reasoning. — N.-Y. : Academic Press, 1990. — 770 p.
2. *Plaisted D. A.* Theorem proving with abstraction // AI. — 1981. — Vol. 16. — P. 47—108.
3. *Boy de la Tour Th., Kreitz Ch.* Building proofs by analogy via the Curry-Howard isomorphism // Proc. of LPAR. — 1992. — P. 202—213.
4. *Défourneaux G., Bourely C., Peltier N.* Semantic generalizations for proving and disproving conjectures by analogy // J. of Automated Reasoning. — 1998. — Vol. 20, N 1 & 2. — P. 27—45.
5. *Melis E.* A model of analogy-driven proof-plan construction // Proc. of IJCAI. — 1995. — P. 182—189.
6. *Гаврилова Т. Л., Клещев А. С.* Внутренняя модель математической практики для систем автоматизированного конструирования доказательств теорем // Проблемы управления. — 2006. — № 4. — Ч. 1. — С. 32—35; № 5. — Ч. 2. — С. 68—73; № 6. — Ч. 3. — С. 68—71.

☎ *(4232) 31-04-24;*

e-mail: kleschev@iacp.dvo.ru

Статья представлена к публикации членом редколлегии О. П. Кузнецовым. ❑