УДК 681.3.057.51-7.311.17

ОПЕРАЦИОННАЯ МОДЕЛЬ ИНТУИТИВНЫХ ДОКАЗАТЕЛЬСТВ

А.С. Клещев

Предложена операционная модель интуитивного доказательства, представляющая собой последовательность команд, операндами которых служат формализованные математические утверждения. Множество команд является расширяемым. Операционная семантика команд определяется средствами макроязыка с использованием фиксированного множества базисных операций. Остаточная модель (макрорасширение) операционной модели интуитивного доказательства, формируемая макрогенератором макроязыка, представляет собой программу для виртуальной машины, успешное выполнение которой подтверждает правильность интуитивного доказательства.

Ключевые слова: интуитивное доказательство, формализация, операционная модель, макроязык, интерактивная система, автоматическое доказательство теорем, проверка правильности.

ВВЕДЕНИЕ

В 1994 г. был опубликован QED-манифест [1] анонимных авторов, в котором выдвинуты цели формализации большей части математики, в том числе и математических доказательств, и проверки правильности этих доказательств. В зарубежной и отечественной литературе (см., например, работы [2, 3]) можно найти публикации, в которых ставятся цели, близкие к выдвинутым в манифесте. В 2007 г. был опубликован пересмотренный манифест [4], в котором хотя и подтверждались цели исходного манифеста, но констатировалось, что за время, прошедшее с момента его опубликования, не произошло существенного продвижения в достижении этих целей. Там же были названы две основные причины такого положения: слишком мало ученых занимаются этой сложной и трудоемкой проблематикой; формализованная математика совершенно непохожа на реальную, из-за чего уже полученные результаты оказываются невостребованными в математических исследованиях.

В настоящее время единственным критерием правильности математического доказательства служит отсутствие в нем кем-либо обнаруженных ошибок. Поскольку такое положение устраивает большинство участников математических исследований и потребителей их результатов, то можно предположить, что достижение целей QED-манифеста возможно лишь при радикальном решении проблемы, а именно, когда разница между реальной и формализованной математикой будет полностью устранена благодаря созданию такой формализованной математики, которая не будет отличаться от реальной. Это означает, что гипотетическая QED-система должна иметь на входе тексты обычных интуитивных доказательств, представленные средствами подготовки математических публикаций, и автоматически переводить эти математические тексты на язык некоторой формальной модели. Прежде чем заниматься лингвистическими вопросами трансляции математических текстов, должна быть предложена формальная модель, удовлетворяющая двум требованиям: семантика ее языка должна быть как можно ближе к семантике математического диалекта, чтобы автоматический перевод математических текстов был реализуем; она должна допускать автоматическую проверку правильности формальных доказательств. Как известно, математический диалект не только не является фиксированным, явно описанным языком, но и продолжает развиваться. Поэтому, нет никакой надежды построить такую фиксированную формальную модель (с фиксированными языком представления математических утверждений, логическим исчислением и моделью доказательства), которую можно было бы положить в основу QED-системы (т. е. которая продолжала бы удовлетворять обоим требованиям, несмотря на дальнейшее развитие математического диалекта,

методов математических рассуждений и техники доказательства). Тем не менее, все известные автору работы, связанные с проблематикой проверки правильности интуитивных математических доказательств, посвящены построению или исследованию именно фиксированных логических моделей.

В цикле работ, опубликованных в настоящем журнале, автор предложил использовать для целей проверки правильности математических доказательств расширяемые формальные модели. Использование расширяемых моделей базируется на концепции управления интеллектуальными системами [5]. Основанная на расширяемой модели QED-система должна быть дополнена программными средствами управления ею (интерактивными, автоматическими и автоматизированными), чтобы лица, управляющие системой с помощью этих средств, имели возможность расширять лежащие в ее основе логические и лингвистические модели, расширяя тем самым корпус математических текстов, допускающих автоматическую обработку.

В работах [6, 7] предложен расширяемый формальный язык представления математических утверждений, задаваемый контекстно-зависимой грамматикой, как средство представления семантики (полуформального) языка математических утверждений. В статье [8] введена расширяемая модель исчисления высокого порядка над этим языком, задаваемая метаязыком, как средство представления семантики математических рассуждений. В работе [9] предложена простая, но достаточно общая формально-логическая модель интуитивного (неполного) доказательства, основанная, в первом приближении, на двух допущениях: формируемые в процессе построения полного доказательства вспомогательные утверждения о принадлежности значения терма в унификаторе к области определения соответствующей предметной переменной должны доказываться автоматически; при доказательстве любой цели может быть выбрана альтернатива «доказательство очевидно», и в этом случае эта цель также должна доказываться автоматически. Проверка правильности неполного формального доказательства сталкивается с проблемой необходимости доказательства громадного числа тривиальных лемм. Решению этой проблемы с помощью технологии «облачных вычислений» (cloud computing) и модели аналогии между доказательствами, базирующейся на ранее построенных расширяемых моделях, посвящены работы [9—11].

Однако формально-логическая модель интуитивного доказательства содержит элементы, которые необходимы для проверки правильности формальных доказательств, но в неформальных интуитивных доказательствах не встречаются, а именно, применяемые на каждом шаге правила вывода и значения их посылок. Автоматическое извлечение этих элементов из текста интуитивного доказательства проблематично, поскольку эта информация в тексте доказательства, обычно, лишь подразумевается. Требуется иная, более близкая к семантике интуитивных доказательств формальная модель интуитивного доказательства, которая, также, должна быть расширяемой. Цель настоящей работы заключается в построении такой модели, согласованной с предыдущими. Эти и предыдущие результаты могут быть использованы не только в проекте QED-системы, но и в новых проектах управляемых интерактивных систем доказательства теорем [12], представляющих собой приближения к этому проекту.

1. КОНЦЕПЦИЯ ОПЕРАЦИОННОЙ МОДЕЛИ ИНТУИТИВНОГО ДОКАЗАТЕЛЬСТВА

Интуитивное доказательство начинается с формулировки теоремы и содержит явную или неявную информацию о переменных, используемых в формулировке теоремы и доказательстве, о способе доказательства и о его узловых шагах. Простейший способ доказательства — это последовательность шагов. Другие способы доказательства связаны с заменой исходной цели на одну или несколько новых, каждая из которых имеет свое интуитивное доказательство.

Метафорой для операционной модели интуитивного доказательства служит точка зрения на интуитивное доказательство как на последовательность предписаний для читателя, которые он должен выполнить, чтобы понять это доказательство и убедиться в его правильности. Операционная модель интуитивного доказательства представляет собой последовательность команд, операндами которых служат формализованные математические утверждения. При преобразовании интуитивного доказательства в его операционную модель «вручную» математик должен: явно описать все переменные, используемые в формулировке теоремы и доказательстве; формализовать теорему (исходную цель); указать способ, которым доказывается очередная цель; если выбранный способ доказательства — это последовательность его шагов, то разбить это доказательство на шаги, заменить каждый шаг последовательностью из одной или нескольких подходящих операций и формализовать математические выражения этого шага, представив их в качестве операндов этих операций; если выбранный способ доказательства связан с заменой очередной цели на одну или несколько новых, то для каждой новой цели построить операционную модель ее интуитивного доказательства. Интерактивная система доказательства теорем, основанная на операционной модели доказательств, должна поддерживать ввод операционной модели интуитив-

ного доказательства, выполнять содержащиеся в ней команды и контролировать правильность операционной модели.

Пример 1. Интуитивное доказательство [13] и его операционная модель.

Теорема. Если x_n стремится к пределу a, и $a > p$, то и все значения x_n, начиная с некоторого, будут больше p.

Описания переменных: последовательность x; вещественные a, p, ε; натуральное N; целое $[N, \infty)$ *n.*

Формализация теоремы: $\lim x = a \;\&\; a > p \Rightarrow \exists\, N\colon \forall\, n\colon x(n) > p$.

Способ доказательства: *доказательство импликации* (утверждения $\lim x = a$ и $a > p$ включаются в список справедливых утверждений, исходная цель заменяется новой целью $\exists\, N\colon \forall\, n\colon x(n) > p$, которую интерактивная система доказательства теорем должна показать пользователю).

Способ доказательства цели $\exists\, N\colon \forall\, n\colon x(n) > p$: *последовательность шагов*.

Шаг 1. Пусть x_n имеет предел a (в операционной модели этого доказательства этот шаг может быть опущен, поскольку это предположение уже было выдвинуто после выбора способа доказательства исходной цели).

Шаг 2. При любом $p < a$ легко подобрать $\varepsilon > 0$ так, чтобы было $a - \varepsilon > p$; для этого достаточно взять $\varepsilon < a - p$.

Команда: *доказать* $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$ (утверждение доказывается подсистемой автоматического поиска полных формальных доказательств; эта подсистема при поиске доказательства сначала использует утверждения из списка справедливых утверждений, а затем утверждения из базы знаний; далее утверждение этого шага включается в список справедливых утверждений).

Команда: *доказать* $a - \varepsilon > p$.

Шаг 3. Но по определению предела найдется такой номер N, что для $n > N$ будет выполняться неравенство $x_n > a - \varepsilon$.

Команда: *доказать* $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$, *используя определение «предел»* (определение «предел» включается в список справедливых утверждений, после чего утверждение $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$ доказывается подсистемой автоматического поиска полных формальных доказательств, а затем включается в список справедливых утверждений).

Шаг 4. А следовательно — и подавно неравенство $x_n > p$.

Команда: *доказать* $x(n) > p$.

Конец последовательности (проверяется, есть ли цель, доказательством которой является последовательность, в списке справедливых утверждений; если ее там нет, как в данном случае, то эта цель доказывается подсистемой автоматического поиска полных формальных доказательств). ♦

Очевидно, что невозможно зафиксировать полный список команд операционной модели интуитивных доказательств. Он определяется не только всеми существующими интуитивными доказательствами, но и теми, которые будут созданы в будущем. Поэтому множество команд операционной модели должно быть расширяемым. Один из способов достижения этой цели заключается в определении операционной семантики команд через совокупность более простых операций.

2. ОПЕРАЦИОННАЯ СЕМАНТИКА КОМАНД

Будем считать, что перед началом исполнения операционной модели каждого простого интуитивного доказательства формируется два пустых списка — целей и справедливых утверждений. Операция *«формализация теоремы»* записывает формулировку теоремы в список целей. Операция *«заменить на»* заменяет первый элемент списка целей на последовательность своих операндов. Операция *«записать ... в ...»* записывает свой первый операнд в список, указанный как второй операнд. Операция *«удалить»* удаляет первый элемент списка целей. Операция *«вспомогательное утверждение»* строит с помощью подсистемы поиска полных формальных доказательств доказательство для своего операнда, используя список справедливых утверждений (в первую очередь) и базу знаний. Операция *«описания переменных»* формирует информационную структуру, содержащую описания переменных. Эта информационная структура используется подсистемой поиска полных формальных доказательств.

Операционная семантика команд операционной модели определяется с помощью макроопределений. Операционная модель интуитивного доказательства может рассматриваться как последовательность макрокоманд, выполнение которых приводит к остаточной модели интуитивного доказательства. Остаточная модель начинается командами *«описания переменных»* и *«формализация теоремы»*, за которыми следуют команды *«заменить на»*, *«записать... в ...»*, *«удалить»* и *«вспомогательное утверждение»*. Приведем макроопределения команд, использованных в примере 1.

Доказательство импликации: если текущая цель $\equiv \boldsymbol{f}_1 \;\&\; \ldots \;\&\; \boldsymbol{f}_n \Rightarrow \boldsymbol{f}$ *то записать* $\boldsymbol{f}_1$ *в список справедливых утверждений; ...; записать* $\boldsymbol{f}_n$ *в список справедливых утверждений; заменить на* $\boldsymbol{f}$, *иначе ошибка.* (Если текущая цель не имеет формы импликации, то такой способ доказательства неприменим).

Последовательность шагов: (пустое макроопределение).

Доказать $\boldsymbol{f}$: *вспомогательное утверждение* $\boldsymbol{f}$; *записать* $\boldsymbol{f}$ *в список справедливых утверждений.*

Доказать $\boldsymbol{f}$, *используя* $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$: *записать* $\boldsymbol{f}_1$ *в список справедливых утверждений; ...; записать* $\boldsymbol{f}_n$ *в список справедливых утверждений; вспомогательное утверждение* $\boldsymbol{f}$.

Конец последовательности: если текущая цель ь список справедливых утверждений, то вспомогательное утверждение текущая цель; записать текущая цель в список справедливых утверждений; удалить.

Пример 2. Остаточная модель интуитивного доказательства примера 1.

Описания переменных: последовательность x; вещественные a, p, ε; натуральное N; целое $[N, \infty)$ n.

Формализация теоремы: $\lim x = a \;\&\; a > p \Rightarrow \exists\, N\colon \forall\, n\colon x(n) > p$.

Записать $\lim x = a$ *в список справедливых утверждений.*

Записать $a > p$ *в список справедливых утверждений.*

Заменить на $\exists\, N\colon \forall\, n\colon x(n) > p$.

Вспомогательное утверждение $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$.

Записать $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$ *в список справедливых утверждений.*

Вспомогательное утверждение $a - \varepsilon > p$.

Записать $a - \varepsilon > p$ *в список справедливых утверждений.*

Записать определение «предел» в список справедливых утверждений.

Вспомогательное утверждение $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$.

Записать $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$ *в список справедливых утверждений.*

Вспомогательное утверждение $x(n) > p$.

Записать $x(n) > p$ *в список справедливых утверждений.*

Вспомогательное утверждение $\exists\, N\colon \forall\, n\colon x(n) > p$.

Удалить. ♦

3. КОНТРОЛЬ ПРАВИЛЬНОСТИ ИНТУИТИВНЫХ ДОКАЗАТЕЛЬСТВ

Как уже отмечалось, для каждого вспомогательного утверждения подсистема поиска полных формальных доказательств должна найти доказательство, используя связанное с этим элементом состояние списка справедливых утверждений (в первую очередь) и базу знаний. При этом поиск доказательства может осуществляться на основе методов, предложенных в работе [9]. Интуитивное доказательство считается правильным, если после построения его операционной модели для каждого вспомогательного утверждения удается найти его полное формальное доказательство. В этом случае интуитивное доказательство можно рассматривать как изложение идеи доказательства, а исполнение его операционной модели — как доведение этой идеи до построения полного формального доказательства. Если идея доказательства изложена достаточно подробно, доказательство каждого вспомогательного утверждения будет сравнительно коротким, а шансы построить его с помощью подсистемы поиска полных формальных доказательств достаточно велики. Если же идея доказательства изложена менее подробно, то, как говорят математики, в этом случае требуется более высокая математическая культура, которая может проявляться в том, что более длинные доказательства будут строиться сначала интерактивно, а затем по аналогии, когда база метадоказательств станет достаточно обширной [11].

Пример 3. Задачи подсистемы поиска полных формальных доказательств примера 2.

Доказательство $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$ при условии, что справедливы выражения $\lim x = a$ и $a > p$.

Доказательство $a - \varepsilon > p$ при условии, что справедливы выражения $\lim x = a$, $a > p$ и $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$.

Доказательство $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$ при условии, что справедливы выражения $\lim x = a$, $a > p$, $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$, $a - \varepsilon > p$ и определение «предел».

Доказательство $x(n) > p$ при условии, что справедливы выражения $\lim x = a$, $a > p$, $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$, $a - \varepsilon > p$, определение «предел» и $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$.

Доказательство $\exists\, N\colon \forall\, n\colon x(n) > p$ при условии, что справедливы выражения $\underline{\lim} x = a$, $a > p$, $p < a \Rightarrow \exists\, \varepsilon\colon \varepsilon > 0 \;\&\; \varepsilon < a - p$, $a - \varepsilon > p$, определение «предел» и $\exists\, N\colon \forall\, n\colon x(n) > a - \varepsilon$ и $x(n) > p$. ♦

4. БОЛЕЕ СЛОЖНЫЕ КОМАНДЫ

Приведем несколько примеров макроопределений более сложных команд и примеры интуитивных доказательств, в операционные модели которых эти команды входят.

От противного f*: если* f*, то вспомогательное утверждение* $\neg$ *текущая цель* $\Leftrightarrow f$*; записать* f *в список справедливых утверждений, иначе записать* $\neg$ *текущая цель в список справедливых утверждений все; заменить на противоречие.* (Если у команды есть аргумент, то формируется вспомогательное утверждение, а аргумент становится предположением, иначе предположением становится отрицание текущей цели. Текущая цель заменяется на противоречие.)

Будем считать $f|\text{-}v_1, \ldots, v_n\text{-}|$*: если* $\forall\ v_1'\colon \ldots\ v_n'\colon \exists\ v_1\colon \ldots\ v_n\colon t|\text{-}v_1', \ldots, v_n'| = t|\text{-}v_1, \ldots, v_n| \;\&\; f|\text{-}v_1, \ldots, v_n| \in$ *база знаний, то записать* $f|\text{-}v_1, \ldots, v_n|$ *в список справедливых утверждений, иначе ошибка.* (Если в базе знаний имеется утверждение указанного вида, аргумент команды является справедливым, иначе доказательство таким способом невозможно).

Подставить t_2 *в* $f|\text{-}t_1|$ *вместо* t_1*: если* $f|\text{-}t_1| \in$ *список справедливых утверждений* $\cup$ *база знаний и* $t_1 = t_2 \in$ *список справедливых утверждений* $\cup$ *база знаний, то записать* $f|\text{-}t_2|$ *в список справедливых утверждений, иначе ошибка.*

$f_1, \ldots, f_n$ *равносильны* $f_1', \ldots, f_n'$ *: вспомогательное утверждение* $f_1 \Leftrightarrow f_1'$ *; …; вспомогательное утверждение* $f_n \Leftrightarrow f_n'$ *; если* $f_1 \in$ *список справедливых утверждений* $\cup$ *база знаний и … и* $f_n \in$ *список справедливых утверждений* $\cup$ *база знаний, то записать* f_1' *в список справедливых утверждений; …; записать* f_n' *в список справедливых утверждений.*

f *равносильно* $f_1, \ldots, f_n$*: вспомогательное утверждение* $f \Leftrightarrow f_1$*; …; вспомогательное утверждение* $f_{n-1} \Leftrightarrow f_n$*; если*

$f \in$ список справедливых утверждений $\cup$ база знаний, то записать f_n в список справедливых утверждений.

Доказательство существования и единственности: если текущая цель $\equiv \forall\ v_1: \ldots v_m: \exists!\ w_1: \ldots w_n: f\vdash v_1, \ldots, v_m, w_1, \ldots w_n\dashv$, *то заменить на* $\forall\ v_1: \ldots v_m: \exists\ w_1: \ldots w_n: f\vdash v_1, \ldots, v_m, w_1, \ldots, w_n\dashv \forall\ v_1: \ldots v_m: w_1: \ldots w_n: w_1': \ldots w_n': f\vdash v_1, \ldots, v_m, w_1, \ldots, w_n\dashv\ \&\ f\vdash v_1, \ldots, v_m, w_1', \ldots, w_n'\dashv \Rightarrow w_1 = w_1'\ \&\ldots\&\ w_n = w_n'$, *иначе ошибка.*

Пусть $f_1, \ldots, f_n$: записать f_1 в список справедливых утверждений; ...; записать f_n в список справедливых утверждений.

Получим $t_1 = t_2 = \ldots = t_n$: вспомогательное утверждение $t_1 = t_2$; ...; вспомогательное утверждение $t_{n-1} = t_n$; записать $t_1 = t_n$ в список справедливых утверждений.

Прибавим t к обеим частям равенства $t_1 = t_2$: если $t_1 = t_2 \in$ список справедливых утверждений $\cup$ база знаний, то записать $t_1 + t = t_2 + t$ в список справедливых утверждений, иначе ошибка.

Достаточно доказать f: вспомогательное утверждение $f \Rightarrow$ текущая цель; заменить на f.

Новая цель f: записать f в список целей. ♦

Пример 4. Интуитивное доказательство [13] и его операционная модель.

Теорема. Нет такой рациональной дроби p/q (где p и q — натуральные числа), квадрат которой был бы равен 2.

Описания переменных: натуральные p, q, r;

Формализация теоремы: $\neg\ \exists\ p: q: (p/q)\uparrow 2 = 2$.

Для доказательства допустим противное: пусть существует такая дробь p/q, что $(p/q)\uparrow 2 = 2$.

От противного $\exists\ p: q: (p/q)\uparrow 2 = 2$.

Последовательность шагов.

Шаг 1. Мы вправе считать эту дробь несократимой, т. е. p и q лишенными общих множителей.

Будем считать несократимая дробь (p, q). *Доказать взаимно простые* (p, q).

Шаг 2. Так как $p^2 = 2 * q^2$, то p есть число четное: $p = 2 * r$ (r — целое) и, следовательно, q — нечетное.

Доказать $p\uparrow 2 = 2 * (q\uparrow 2)$. *Доказать четное число* (p). *Доказать* $\exists\ r: p = 2 * r$. *Доказать нечетное число* (q).

Шаг 3. Подставляя вместо p его выражение, найдем: $q^2 = 2 * r^2$, откуда следует, что q — число четное.

Подставить $2 * r$ *в* $p\uparrow 2 = 2 * (q\uparrow 2)$ *вместо* p. *Доказать* $q\uparrow 2 = 2 * r\uparrow 2$. *Доказать четное число* (q).

Шаг 4. Полученное противоречие доказывает наше утверждение.

Доказать противоречие.

Конец последовательности. ♦

Пример 5. Интуитивное доказательство [13] и его операционная модель.

Теорема. Для любых рациональных чисел a, b и c из $a < b$ и $b < c$ следует, что $a < c$.

Описания переменных: рациональное a, b, c.

Формализация теоремы: $a < b\ \&\ b < c \Rightarrow a < c$.

Доказательство импликации.

Последовательность шагов.

Шаг 1. Действительно, неравенства $a < b$ и $b < c$ равносильны по условию неравенствам $b > a$ и $c > b$; отсюда следует $c > a$ или, что тоже самое, $a < c$.

$a < b$, $b < c$ равносильны $b > a$, $c > b$. Доказать $c > a$. Доказать $a < c$.

Конец последовательности. ♦

Пример 6. Интуитивное доказательство [13] и его операционная модель.

Теорема. Для любых рациональных чисел a и b существует и единственна их разность.

Описания переменных: рациональные a, b, c, c'.

Формализация теоремы: $\exists!\ c: c = a - b$.

Доказательство существования и единственности.

Последовательность шагов.

Шаг 1.1. Положив $c = a + (-b)$, получим: $c + b = [a + (-b)] + b = a + [(-b) + b] = a + [b + (-b)] = a + 0 = a$, так что это число c удовлетворяет определению разности.

Пусть $c = a + (-b)$. Получим $c + b = (a + (-b)) + b = a + ((-b) + b) = a + (b + (-b)) = a + 0 = a$. Доказать $c = a - b$.

Конец последовательности.

Последовательность шагов.

Шаг 2.1. Пусть, обратно c' есть разность чисел a и b, так что $c' + b = a$.

Пусть $c' = a - b$. Доказать $c' + b = a$.

Шаг 2.2. Прибавив к обеим частям этого равенства по $(-b)$ и преобразуя левую часть: $(c' + b) + (-b) = c' + (b + (-b)) = c' + 0 = c'$, заключим, что $c' = a + (-b) = c$.

Прибавим $-b$ к обеим частям равенства $c' + b = a$. Получим $(c' + b) + (-b) = c' + (b + (-b)) = c' + 0 = c'$. Получим $c' = a + (-b) = c$.

Конец последовательности. ♦

Пример 7. Интуитивное доказательство [13] и его операционная модель.

Теорема. Для любых рациональных чисел a и b имеет место $-(a + b) = (-a) + (-b)$.

Описания переменных: рациональные a, b.

Формализация теоремы: $-(a + b) = (-a) + (-b)$.

Последовательность шагов.

Шаг 1. Для этого достаточно доказать, что $(a + b) + ((-a) + (-b)) = 0$.

Достаточно доказать $(a + b) + ((-a) + (-b)) = 0$.

Конец последовательности. ♦

Пример 8. Интуитивное доказательство [13] и его операционная модель.

Теорема. В множестве всех рациональных чисел a, для которых $a^2 < 2$, нет наибольшего числа.

Описания переменных: рациональные a, b; натуральное n; $A = \{a: a > 0\ \&\ a\uparrow 2 < 2\} \cup \{a: a \leqslant 0\}$.

Формализация теоремы: $\neg\ \exists\ b: (b \in A\ \&\ \forall\ a: a \in A \Rightarrow b \geq a)$.

Последовательность шагов.

Шаг 1. Пусть a — любое положительное число класса A, тогда $a^2 < 2$.

Пусть $a \in A$, $a > 0$. Доказать $a\uparrow 2 < 2$.

Шаг 2. Покажем, что можно подобрать такое целое положительное n, что $(a + 1/n)^2 < 2$, так что и число $a + 1/n$ будет принадлежать классу A.

Доказать $\forall\ n: (a + 1/n)\uparrow 2 < 2 \Rightarrow a + 1/n \in A$. Новая цель $\exists\ n: (a + 1/n)\uparrow 2 < 2$.

Последовательность шагов.

Шаг 2.1. Это неравенство равносильно неравенствам $a^2 + (2*a)/n + 1/n^2 < 2$, $(2*a)/n + 1 / n^2 < 2 - a^2$.

$(a + 1/n)\uparrow 2 < 2$ *равносильно* $a\uparrow 2 + (2 * a)/n + 1/n\uparrow 2 < 2$, $(2*a)/n + 1/n\uparrow 2 < 2 - a\uparrow 2$. *Заменить на* $(2 * a)/n + 1/n\uparrow 2 < 2 - a\uparrow 2$.

Последовательность шагов.

Шаг 2.1.1. Последнее неравенство и подавно будет выполнено, если n удовлетворит неравенству $(2*a + 1)/n < 2 - a^2$, для чего достаточно взять $n > (2*a + 1)/(2 - a^2)$, а это всегда возможно.

Доказать $(2*a + 1)/n < 2 - a\uparrow 2 \Rightarrow (2*a)/n + 1/n\uparrow 2 < 2 - a\uparrow 2$. *Доказать* $n > (2*a + 1)/(2 - a\uparrow 2) \Rightarrow (2*a + 1)/n < 2 - a\uparrow 2$. *Доказать* $\exists\, n$: $n > (2*a + 1)/(2 - a\uparrow 2)$.

Конец последовательности.

Конец последовательности.

Шаг 3. Итак, каково бы ни было положительное число a из класса A, в этом же классе A найдется большее его число; так как для чисел $a \leqslant 0$ это утверждение непосредственно очевидно, то никакое число класса A не является в нем наибольшим.

Доказать $\forall\, a$: $a \in A \,\&\, a > 0 \Rightarrow \exists\, b$: $b \in A \,\&\, b > a$. *Доказать* $\forall\, a$: $a \in A \,\&\, a \leqslant 0 \Rightarrow \exists\, b$: $b \in A \,\&\, b > a$. *Доказать* $\forall\, a$: $a \in A \Rightarrow \exists\, b$: $b \in A \,\&\, a < b$.

Конец последовательности. ♦

ЗАКЛЮЧЕНИЕ

В работе введена операционная модель интуитивного доказательства, представляющая собой последовательность команд, операндами которых служат формализованные математические утверждения. Множество команд является расширяемым. Операционная семантика команд определяется средствами макроязыка с использованием фиксированного множества базисных операций. Остаточная модель (макрорасширение) операционной модели интуитивного доказательства, формируемая автоматически макрогенератором макроязыка, представляет собой программу для виртуальной машины, успешное выполнение которой подтверждает правильность интуитивного доказательства. Базисными являются операции виртуальной машины для работы со списками целей и доказанных утверждений, а также обращение к подсистеме автоматического доказательства теорем.

Переход от интуитивного доказательства к его операционной модели существенно проще, чем переход к его формально-логической модели, но требует от математика понимания логики доказательства. Если в интуитивном доказательстве те действия, которые должен выполнить читатель этого доказательства, чтобы его понять, описаны неявно, то в операционной модели эти действия описываются явно. Ввод операционных моделей интуитивных доказательств и их последующая обработка может выполняться интерактивной системой доказательства теорем с соответствующим интерфейсом и набором подсистем.

Другим направлением использования операционных моделей интуитивных доказательств может быть автоматический анализ интуитивных доказательств (математических текстов) и их преобразование в операционные модели. Близость семантики интуитивных доказательств и их операционных моделей, расширяемость операционных моделей, а также жесткость и сравнительная бедность языка представления интуитивных доказательств позволяют надеяться на успешное решение и этой проблемы в будущем. В этом случае интуитивные доказательства, представленные средствами подготовки математических публикаций, могут быть входом QED-системы, которая автоматически проверяет их правильность.

ЛИТЕРАТУРА

1. *The QED* Manifesto // Automated Deduction. — 1994. — Vol. 814 — P. 238—251. — URL: http://www.cs.ru.nl/~freek/qed/qed.ps.gzi (дата обращения 28.06.2010).
2. *Muzalewski Ml.* An Outline of PC Mizar. — Brussels: Fondation Philippe le Hodey, 1993. — URL: http://www.cs.ru.nl/~freek/mizar/mizarmanual.ps.gzi (дата обращения 28.06.2010).
3. *Вершинин К.П.*, *Лялецкий А.В.*, *Паскевич А.Ю.* Применение Системы Автоматизированной Дедукции для верификации математических текстов. — URL: http://tertium.org/papers/ii-03.ru.pdf (дата обращения 28.06.2010).
4. *Freek W.* The QED Manifesto Revisited // Studies in Logic, Grammar and Rhetoric. — 2007. — Vol. 10. — P. 121—133. — URL: http://mizar.org/trybulec65/8.pdf (дата обращения 28.06.2010).
5. *Грибова В.В.*, *Клещев А.С. Шалфеева Е.А.* Управление интеллектуальными системами. // Изв. РАН. Теории и системы управления. — 2010. — № 6. — С. 122—137.
6. *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.
7. *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.
8. *Гаврилова Т.Л.*, *Клещев А.С.* Внутренняя модель математической практики для систем автоматизированного конструирования доказательств теорем. Ч. 3. Модель доказательства // Там же. — № 6. — С. 69—71.
9. *Клещев А.С.* Концепция банка математических знаний для научных исследований. Ч. 2. Интерактивное формирование интуитивных доказательств // Там же. — 2008. — № 5. — С. 26—30.
10. *Клещев А.С.* Концепция банка математических знаний для научных исследований. Ч. 1. Метафора // Там же. — 2008. — № 4. — С. 2—6.
11. *Клещев А.С.* Модель аналогии между математическими доказательствами // Там же. — 2007. — № 1. — С. 20—24.
12. *Asperti A.* A Survey on Interactive Theorem Proving. 2009. — URL: http://www.cs.unibo.it/~asperti/SLIDES/itp.pdf (дата обращения 28.06.2010).
13. *Фихтенгольц Г.М.* Курс дифференциального и интегрального исчисления. Т. 1. — М.: Наука, 1969. — 608 с.

Статья представлена к публикации членом редколлегии академиком РАН С.Н. Васильевым.

Клещев Александр Сергеевич — д-р физ.-мат. наук, гл. науч. сотрудник, Институт автоматики и процессов управления ДВО РАН, г. Владивосток, ☎ (4232) 31-04-24, ✉ kleschev@iacp.dvo.ru.