УДК 681.3.057.51-7.311.17

ВНУТРЕННЯЯ МОДЕЛЬ МАТЕМАТИЧЕСКОЙ ПРАКТИКИ ДЛЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО КОНСТРУИРОВАНИЯ ДОКАЗАТЕЛЬСТВ ТЕОРЕМ[1]

Ч. 1. Общее описание модели

Т. Л. Гаврилова, А. С. Клещев

Для разработки автоматизированных систем конструирования правильных доказательств математических утверждений на основе математических знаний предложена модель математической практики, более адекватная, чем модели математической логики. Модель математической практики представлена в виде комбинации двух моделей: внутренней модели — формальной системы, и внешней модели, в рамках которой математик управляет процессом конструирования интуитивных доказательств. Сформулированы требования к внешней и внутренней моделям математической практики. Дано общее описание внутренней модели.

ВВЕДЕНИЕ

Проблема автоматизации процесса конструирования правильных доказательств математических теорем является актуальной и для математического образования (обучения студентов доказательству теорем), и для математической практики (доказательства теорем профессиональными математиками). В работе [1] показано, что наиболее перспективны не автоматические, а автоматизированные (человеко-машинные) системы конструирования доказательств. Однако до сих пор и те, и другие системы основывались на моделях математической логики, предназначенных для исследования проблем метаматематики [2—5]. Именно поэтому эти системы служат целям обучения скорее математической логике, чем доказательству математических теорем. Такие модели неадекватно представляют математическую практику и потому неудобны для математиков и студентов, работающих с системами автоматизированного конструирования доказательств (САКД). Дальнейшее развитие САКД может быть связано с разработкой более адекватной модели математической практики [1]. Такую модель можно представить в виде комбинации двух моделей: внутренней модели — формальной системы, в рамках которой САКД осуществляет конструирование полных доказательств по информации, получаемой от математика, и внешней модели, в рамках которой математик управляет процессом конструирования интуитивных доказательств. Внутренняя модель отвечает за правильность сконструированных доказательств, а внешняя имитирует привычную для математиков систему понятий и представлений математической практики. Одним из недостатков существующих САКД как раз и является отсутствие в них внешней модели и использование в этом качестве внутренней модели.

В настоящем цикле статей на основе требований к внешней и внутренней моделям математической практики предлагается внутренняя модель для САКД. Данная статья является первой из цикла. В ней определяются требования к внешней и внутренней моделям математической практики, и дается общее описание внутренней модели.

[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».

1. ВНЕШНЯЯ И ВНУТРЕННЯЯ МОДЕЛИ МАТЕМАТИЧЕСКОЙ ПРАКТИКИ

Каждая из моделей математической практики, и внешняя, и внутренняя, в свою очередь, состоит из четырех моделей: математического диалекта, знаний, способов рассуждения и доказательств. Далее приведены определения этих моделей и требования к ним.

Внешняя модель математического диалекта (ММД) — это язык, на котором САКД представляет математику математические знания. Этот язык должен быть достаточно богат, чтобы представленные на нем математические знания выглядели привычно и понятно для математика (не требовали изучения какого-либо неизвестного ему языка). Он должен быть расширяемым, как и математический диалект, а утверждения на нем должны интерпретироваться однозначно [1]. Кроме того, этот язык должен имитировать разделение математического диалекта на неформальную (естественно-языковую) и формальную части. *Внутренняя модель математического диалекта* — это формальный язык, на котором математические знания представляются в САКД. Он также должен быть расширяемым, утверждения на нем также должны однозначно интерпретироваться. Но в отличие от внешней модели, этот язык не должен имитировать разделение математического диалекта на неформальную и формальную части, а в его описании должны быть явно выделены формальный синтаксис, контекстные условия, логическая семантика и прагматика.

Внешняя модель математических знаний — это множество математических утверждений (аксиом, определений, теорем и лемм), представленных на языке внешней модели и доступных математику в процессе конструирования доказательств теорем с помощью САКД. *Внутренняя модель математических знаний* — это множество математических утверждений, представленных на языке внутренней модели и доступных САКД в процессе конструирования доказательств. Обе модели математических знаний должны допускать расширение новыми аксиомами, новыми определениями и вновь доказанными теоремами и леммами. Система автоматизированного конструирования доказательств должна поддерживать соответствие между внутренней и внешней моделями математических знаний.

Внешняя модель способов рассуждения — это множество описаний способов рассуждения, представленных на языке внешней модели и доступных математику в процессе конструирования доказательств теорем с помощью САКД. *Внутренняя модель способов рассуждения* — это множество описаний тех же способов рассуждения, но представленных на языке внутренней модели и доступных САКД в процессе конструирования доказательств. Обе модели способов рассуждения должны быть достаточно богатыми, чтобы охватить принятые в математике способы рассуждения, и допускать расширение описаниями новых способов рассуждения. Система должна поддерживать соответствие между внутренней и внешней моделями способов рассуждения.

Внешняя модель доказательства теоремы — это текст интуитивного доказательства этой теоремы [1], представленный на языке внешней модели. *Внутренняя модель доказательства теоремы* — это структура данных САКД, представляющая полное доказательство этой теоремы [1]. Правильность доказательства теоремы (в том числе и интуитивного) должна следовать из возможности конструирования ее полного доказательства. Система должна поддерживать соответствие между внутренней и внешней моделями доказательств.

2. ОБЩЕЕ ОПИСАНИЕ ВНУТРЕННЕЙ МОДЕЛИ МАТЕМАТИЧЕСКОЙ ПРАКТИКИ

Рассмотрим более подробно, каким образом построена внутренняя модель математической практики, удовлетворяющая сформулированным выше требованиям.

Расширяемость языка ММД обеспечивается расширяемостью его синтаксиса, контекстных условий и семантики.

Расширяемость синтаксиса достигается благодаря средствам САКД, позволяющим описать (конкретный или абстрактный) синтаксис каждой новой конструкции (терма или формулы) языка и добавить это описание к описанию синтаксиса языка ММД. Заметим, что с этой точки зрения описание синтаксиса термов и формул можно рассматривать как расширение пустых множеств термов и формул языка ММД. Если САКД предоставляет средства описания конкретного синтаксиса, то в ее состав должен входить синтаксически управляемый синтаксический анализатор, например, YACC [6]; если же в САКД имеются средства описания абстрактного синтаксиса, то в ее состав должен входить универсальный структурный редактор, (см., например, работу [7]). Рассмотрим случай, когда описывается только конкретный синтаксис языка ММД.

Расширяемость контекстных условий следует из их определения. Контекстные условия языка ММД делятся на два класса. Контекстные условия первого класса суть ограничения, которые могут быть проверены по тексту на языке ММД. Контекстные условия второго класса задаются указанием для каждой конструкции языка ММД способов построения предложений, из справедливости которых следует корректность этой конструкции. Проверка контекстных условий второго класса состоит в автоматическом (или автоматизированном) доказательстве этих предложений.

Внутренняя модель математических знаний состоит только из корректных конструкций. Как будет видно из дальнейшего изложения, она задает семантику языка ММД в том смысле, что она определяет множество тех предложений этого языка, про которые известно, что они истинны. Поэтому *расширяемость семантики* языка ММД обеспечивается расширяемостью внутренней модели математических знаний, которая достигается путем добавления новых истинных математических и метаматематических утверждений.

Язык ММД состоит из трех подъязыков: языка представления математических утверждений, языка представления пропозициональных утверждений и метаязыка. Математические знания представляются на первом из них. Пропозициональные утверждения не могут быть представлены на этом языке, поэтому для их представления вводится специальный язык. Математические принципы и утверждения о синтаксических преобразованиях математических формул (например, правила дифференцирования или взятия неопределенного интеграла) также не могут быть представлены на первом подъязыке, поэтому для их представления также вводится специальный язык (метаязык). Средства расширения имеет только язык представления математических утверждений. Метаязык, надстроенный над ним, расширяется автоматически при его расширении. Язык представления пропозициональных утверждений расширяемым не является.

Поскольку язык ММД является расширяемым, то можно говорить о версиях этого языка, причем в дальнейшем изложении считается, что каждая следующая версия языка является расширением предыдущей. Как обычно, *предложением* языка будем называть корректную формулу, не содержащую свободных вхождений переменных. *Экстенсионалом версии языка* ММД будем называть множество всех предложений, представимых в этой версии языка. Это множество для нетривиальных версий языка будет бесконечным. Очевидно, что при переходе к следующей версии языка его экстенсионал будет расширяться. Математика разбивает экстенсионал языка ММД на два подмножества: истинных и ложных предложений. Цель математической практики состоит в явном описании множества тех предложений, про которые известно, что они истинны. Это множество описывается с помощью внутренней модели математических знаний как множество, состоящее из ядра внутренней модели знаний и его оболочки. *Ядро внутренней модели знаний* определяется как совокупность математических определений, пропозициональных тавтологий, математических аксиом и метаматематических аксиом, представленных на языке ММД. Ядро является, очевидно, расширяемым, поэтому можно говорить о состояниях этого ядра. Каждое следующее состояние ядра является расширением предыдущего. *Оболочка ядра* определяется как множество математических и метаматематических теорем, доказанных на основе ядра. Оболочка расширяется путем включения в нее вновь сформулированных на языке ММД теорем, доказанных на основе ядра. Поскольку оболочка также является расширяемой, то можно говорить и о ее состояниях. Каждое следующее состояние оболочки является расширением предыдущего.

Экстенсионалом определения будем называть множество, состоящее из единственного предложения, имеющего форму равенства между определяемым термином и термом, задающим значение этого термина. *Экстенсионалом пропозициональной тавтологии* будем называть множество предложений (конкретизаций), полученных из этой тавтологии заменой вхождений всех пропозициональных переменных на произвольные предложения. *Экстенсионалом математического утверждения* (в частности, математической аксиомы) будем называть множество предложений (конкретизаций), полученных из этого утверждения заменой вхождений всех свободных переменных на произвольные, но «подходящие» термы без свободных переменных. *Экстенсионалом метаматематического утверждения* (в частности, метаматематической аксиомы) будем называть объединение экстенсионалов всех математических утверждений (конкретизаций), полученных из этого метаматематического утверждения заменой вхождений всех синтаксических переменных на произвольные, но «подходящие» термы без свободных переменных или предложения. *Экстенсионалом ядра* (*оболочки)* внутренней модели знаний будем называть объединение экстенсионалов всех элементов этого ядра (оболочки). Объединение экстенсионалов ядра и оболочки внутренней модели знаний и есть множество тех предложений, про которые известно, что они истинны.

Как было указано выше, оболочка расширяется путем включения в нее теорем, доказанных на основе ядра. *Доказательство математической теоремы* сводится к доказательству ее конкретизации при подходящем наборе предположений о значениях свободных переменных. *Доказательство предложения, имеющего форму импликации*, сводится к доказательству заключения этой импликации в предположении истинности ее условия. Основным способом *доказательства предложения, не имеющего формы импликации,* является использование правила вывода Modus ponens: выбирается некоторое предложение, имеющее форму импликации и принадлежащее объединению экстенсионалов ядра и оболочки; если Modus ponens используется для *декомпозиции*, т. е. требуется доказать предложение, совпадающее с заключением этой импликации, то это доказательство сводится к доказательству условий этой импликации; если же Modus ponens используется для *вывода*, т. е. истинны условия этой импликации (установлено, что они принадлежат объединению экстенсионалов ядра и оболочки), то заключение этой импликации считается доказанным. *Доказательство предложения пусто*, если это предложение входит в объединение экстенсионалов ядра и оболочки.

Способы рассуждений, которые используются при конструировании доказательств, делятся на *три класса*: с опорой на *пропозициональные тавтологии* (например, сведение доказательства равносильного утверждения к доказательству двух импликаций, доказательство от противного и т. п.); с опорой на *математические утверждения* (применение математических аксиом, теорем и лемм); с опорой на *математические принципы* (например, применение принципа полной математической индукции, принципа замены равных термов в формулах и т. п.). Все эти способы рассуждения представляются соответствующим образом во внутренней модели математических знаний: пропозициональными тавтологиями, математическими и метаматематическими утверждениями.

В процессе конструирования доказательства для каждого доказываемого предложения определяется множество *предположений*, при которых это предложение должно быть доказано. *Правильность полного доказательства предложения* обеспечивается проверкой условия, что при доказательстве этого предложения не было использовано предположений, не входящих в это множество.

Управление процессом конструирования доказательств в терминах внутренней модели сводится к выбору на каждом шаге процесса *цели* использования правила вывода Modus ponens (для декомпозиции или для вывода), к выбору в модели знаний *способа рассуждения* на этом шаге и к подбору *посылок* для применения правила вывода Modus ponens.

ЗАКЛЮЧЕНИЕ

Результаты работы состоят в следующем. Определены требования к внешней и внутренней моделям математической практики для САКД. Дано общее описание внутренней модели, введен ряд определений, которые будут использованы в последующих статьях этого цикла.

ЛИТЕРАТУРА

1. *Гаврилова Т. Л., Клещев А. С.* Анализ подходов к решению проблемы правильности математических знаний // Проблемы управления. — 2005. — № 3. — С. 13—19.
2. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. — М.: Наука, 1983. — 320 с.
3. *ETPS: A System* to Help Students Write Formal Proofs / B. Andrews Peter, M. Bishop, E. Brown Chad, et al. // Research Report No. 03-002, April 2003 (Departvent of Mathematical Sciences. Carnegie Mellon University).
4. *JProver*: Integrating Connectoin-Based Theorem Proving into Interactive Proof Assistants / Schmitt S., Lorigo L., Kreitz C. and Nogin A. // International Joint.
5. *Ulrich Endriss*. The Interactive Learning Environment WinKE for Teaching Deductive Reasoning // First International Congress on Tools for Teaching Logic. King's College. — London, September 6, 2000.
6. *Stepheh C. Johnson*. Yacc: Yet Another Compiler-Compiler <http://dinosaur.comilertools.net/yacc/>.
7. *Орлов В. А., Клещев А. С.* Многоцелевой банк знаний. Ч. 3. Концепция универсального Редактора ИРУО. — Владивосток: ИАПУ ДВО РАН, 2003. — 28 с. <www.iacp.dvo.ru/es/publ/186_3.rtf>.

☎*(4232) 31-40-01, 31-04-24*

e-mail: gavrilov@iacp.dvo.ru

kleschev@iacp.dvo.ru