УДК 681.3.057.51-7.311.17

КОНЦЕПЦИЯ БАНКА МАТЕМАТИЧЕСКИХ ЗНАНИЙ ДЛЯ НАУЧНЫХ ИССЛЕДОВАНИЙ. Ч. 1. Метафора[1]

А.С. Клещев

Институт автоматики и процессов управления ДВО РАН, г. Владивосток

На основе расширяемой внутренней модели математической практики и модели аналогии между доказательствами предложена концепция системы компьютерной поддержки научной деятельности в области математики и реализующих ее механизмов. Приведена метафора системы и структура внешней модели математической практики.

ВВЕДЕНИЕ

Доказательство теорем является творческой деятельностью. Несмотря на то, что ей пытаются учить детей еще в школе, она остается трудной и для профессиональных математиков. Научная значимость автоматизации этой деятельности обсуждалась в статье [1]. Основная в области теоретической математики, она занимает значительное место и в прикладной математике, а также в науках, связанных с активным использованием математических знаний, — в физике, технических науках и др. Наконец, и в программировании доказательство правильности алгоритмов и программ составляло мечту многих выдающихся ученых. Однако ни одна из существующих систем автоматического или интерактивного доказательства теорем не используется систематически в научной деятельности.

Цель настоящей статьи заключается в разработке концепции и реализующих ее механизмов для системы компьютерной поддержки научной деятельности в области математики. В первой части приводится метафора системы и структура внешней модели математической практики.

[1] Работа выполнена при финансовой поддержке РФФИ, проект 06-070-89071-а, и ДВО РАН в рамках Программы № 15 ОЭММПУ РАН, проект 06-I-П15-055.

1. СИСТЕМЫ ИНТЕРАКТИВНОГО ПОСТРОЕНИЯ ДОКАЗАТЕЛЬСТВ

Идея формализации математики имеет долгую традицию. Возможность чисто синтаксического построения математики и механической проверки правильности доказательств была показана в первой половине XX в. Во второй половине были разработаны компьютерные системы, с помощью которых были получены некоторые нетривиальные математические результаты. В течение последних десятилетий были созданы компьютерные системы и среды для проверки правильности и помощи в построении доказательств, такие как Coq [2], Isabelle [3] и HOL [4]. Эти средства обеспечивают высокую степень уверенности в правильности полученных с их помощью доказательств. Они нашли применение для верификации элементной базы и программного обеспечения компьютеров, но построение корпуса механически верифицированной математики пока остается недостижимой мечтой [5]. Другим приложением является обучение математике [6].

Большинство из этих систем однопользовательские, а некоторые — свободно распространяемые. Их установка на персональном компьютере довольно сложна, причем пользователь в результате получает «пустую» систему (без базы знаний). Исключение составляет система ActiveMath [6], где

Интернет используется как средство общения между преподавателями и студентами.

Работа с такой системой начинается с формирования некоторого проекта, связанного, например, с поиском доказательства некоторой теоремы или с формальной верификацией программы. Проект представляет собой одну или несколько теорий, образующих сеть (граф без циклов), в которой каждый потомок расширяет одну или несколько родительских теорий. Формированием теорий занимается «специалист по спецификациям». Лишь после того, как сформированы все необходимые теории, «специалист по доказательствам» может приступить к интерактивному построению доказательств теорем [7]. Если при построении очередного доказательства выясняется, что в сформированных теориях не хватает необходимых для этого знаний (аксиом, определений или теорем), пользователь вынужден приостанавливать построение доказательства и переходить в режим формирования теорий.

При формировании теорий «специалист по спецификациям» вынужден использовать язык с фиксированным синтаксисом, являющийся либо языком исчисления предикатов, либо его расширением, допускающим некоторые классы арифметических, теоретико-множественных и иных формул. «Специалист по доказательствам» вынужден строить полные доказательства в рамках фиксированного исчисления предикатов первого или более высокого порядка. Доказательство формируется как последовательность команд. На очередном шаге «специалист по доказательствам» анализирует состояние доказательства и формирует очередную команду. Система выполняет ее и представляет ему новое состояние. Состояние доказательства характеризуется несколькими открытыми (еще не доказанными) целями. Кроме того, оно может иметь и другие элементы, такие как локальные описания и предположения. Построение доказательства заканчивается, когда достигнуто состояние, в котором нет открытых целей [8, 9].

Опыт применения таких систем показал, что построение полных доказательств в рамках фиксированного исчисления слишком трудоемко. Математик обычно имеет долговременный план для сложных доказательств, который считается непредставимым на уровне исчисления (отдельных шагов вывода). Более того, в хорошо известной ему области он имеет множество стратегий, техник и приемов доказательства. Идея моделирования этих способностей на компьютере состоит в следующем. План есть представление доказательства на более высоком уровне абстракции, чем уровень логического исчисления. Он состоит из последовательности макрооператоров, таких как применение гомоморфизмов, применение лемм, некоторые упрощения, дифференцирование или интегрирование функций, вызов системы автоматического доказательства или компьютерной алгебры, специализированной процедуры и др. Каждый из этих макрооператоров может быть раскрыт в последовательность шагов вывода и называется тактикой. Методы доказательств получаются из тактик добавлением к ним предусловий и постусловий. Стратегии доказательств объединяют вместе взаимосвязанные методы и поисковые эвристики. В таких расширенных исчислениях построение доказательств заменяется построением планов доказательств (автоматическим или интерактивным). План есть последовательность методов. Доказательство является результатом выполнения плана. Для облегчения процесса построения доказательств или их планов некоторые системы содержат механизм предложения команд: пользователю выдается список команд, применимых в текущем состоянии доказательства или его плана, из которого он выбирает необходимую команду и уточняет ее аргументы [10, 11].

В процессе взаимодействия с системами интерактивного построения доказательств пользователь вынужден оперировать такими понятиями, как: проект, теория, иерархия теорий, потомок теории, предок теории; логический контекст, логический базис, внелогический контекст; аксиома, теорема; формула, терм, константа, тип, сорт; доказательство, цель, главная цель, шаг доказательства, команда построения доказательства, состояние доказательства, открытая цель, попытка доказательства. Интерфейс таких систем основан на двух альтернативных принципах — текстовом вводе информации, с последующим контролем ее синтаксической правильности, и совокупности выборов информации из списков. Обычно обе эти возможности присутствуют в интерфейсе в том или ином сочетании [9].

Рассмотрим, в какой мере системы, обладающие подобными свойствами, пригодны для использования в математических исследованиях.

Сложная установка однопользовательской системы на персональном компьютере не может быть приемлемой, поскольку ученый-математик не всегда обладает достаточной для этого компьютерной грамотностью. Интернет-системы в этом отношении явно предпочтительнее. Однако прямое взаимодействие пользователей между собой во время сеансов их работы вряд ли требуется.

«Пустые» системы вообще неприменимы для научных исследований. Средства поддержки научной деятельности могут использоваться лишь тогда, когда содержат значительную часть уже накопленных математических знаний. Принцип формирования отдельных «проектов», т. е. сетей баз знаний, специально организованных для целей доказательства отдельной теоремы или совокупности содержательно связанных теорем, также неприемлем. Исследователям нужна общая база математических знаний, к которой они смогут быстро при-

выкнуть, причем организованная таким образом, чтобы они могли достаточно легко ориентироваться в ней при поиске необходимой информации.

Разделение ролей «специалиста по спецификации» теорий и «специалиста по доказательству» теорем, а также строго последовательный порядок их работы противоречат математической практике, поскольку в работе исследователя эти два вида деятельности тесно переплетены и постоянно чередуются.

Хотя при написании формул математик вынужден соблюдать целый ряд правил синтаксиса, однако переход при их вводе с математического диалекта на его формальный аналог, который требует знания значительного числа дополнительных правил, также является неприемлемым. Столь же неприемлем фиксированный синтаксис такого языка, поскольку математический диалект постоянно развивается по мере развития математики. Полные доказательства не строятся в математической практике, несмотря на призывы ревнителей их достоверности. Поэтому необходимость построения полных доказательств отпугивает от таких систем большинство математиков. Наконец, неприемлема и фиксированная формальная система (исчисление), в рамках которой строятся доказательства, поскольку до сих пор неизвестны попытки практически приемлемой кодификации правил математического рассуждения. Построение доказательства в виде последовательности команд можно считать приемлемым, если набор возможных команд удовлетворителен для пользователей.

Возможность расширять исчисление, несомненно, прогрессивная идея. Однако такие расширения должны выполняться либо самими математиками в ходе построения доказательств, либо системой на основе анализа этих доказательств. Использование процедурного метаязыка (или макроязыка) для описания повторно используемых тактик, методов и стратегий исключает возможность участия большинства математиков в расширении исчисления. Выделение же работы по расширению исчисления в самостоятельную деятельность требует организации оперативного взаимодействия между ее исполнителями (программистами) и математиками, у которых возникает потребность в таких расширениях при построении доказательств. Самостоятельной проблемой выступает обеспечение правильности тактик, методов и стратегий, представленных в виде программ, относительно их спецификации (предусловий и постусловий) и содержательного описания (без которого их использование математиками оказывается невозможным). Это же, но в еще большей степени, относится и к повторно используемым планам доказательств. Важен механизм предложения команд при условии, что математик понимает, что ему предлагается.

Желательно, чтобы при взаимодействии с подобными системами пользователю приходилось оперировать как можно меньшим числом нематематических понятий, из которых большую часть желательно выдать за понятия, в терминах которых в математической литературе обычно описывается процесс построения доказательств. В процессе построения доказательства текстовый ввод информации с последующим синтаксическим контролем неприемлем по двум причинам: он требует знания математиками синтаксиса такого языка (а они не хотят учить новые формальные языки); в случае совершения синтаксических ошибок процесс их обнаружения и устранения может оказаться для математиков слишком сложным (из-за неточной диагностики и наведенных ошибок). Выбор информации из списков не обладает этими недостатками, но не всегда привычен.

Таким образом, на пути применения систем интерактивного построения доказательств для научных применений лежит еще много нерешенных проблем.

2. МЕТАФОРА БАНКА МАТЕМАТИЧЕСКИХ ЗНАНИЙ

В качестве метафоры для компьютерной поддержки математических исследований (назовем такую систему «Банк математических знаний» (БМЗ)) возьмем организацию математической практики. Чем ближе такой банк будет к этой метафоре, тем более востребованным он может оказаться.

Цель математических исследований состоит в расширении математических знаний, в том числе в формулировании новых аксиоматических систем, определений и математических утверждений (теорем, лемм и т. п.), а также их доказательстве. Доступные для выполнения этой деятельности и расширяемые в результате нее математические знания, помимо персональных знаний ее участников, практически недоступных для других, распределены между учебниками и справочниками (где их легче всего найти), монографиями (где их найти несколько труднее), а также научными статьями (где их найти труднее всего в силу обилия таких статей). В этой деятельности принимает участие большое число специалистов, которых можно условно разделить на потребителей знаний (преподавателей, студентов и прикладных специалистов), генераторов знаний или исследователей (тех, кто занимается получением новых математических знаний) и интеграторов знаний (тех, кто занимается систематизацией математических знаний). Источниками для потребителей знаний служат учебники, справочники, реже монографии, еще реже научные статьи. Результатом деятельности исследователей являются научные статьи, а результатом деятельности интеграторов — монографии, учебники и справочники. Если исследователь в статье использует (и вводит) лишь такое множес-

тво понятий, которое достаточно, чтобы представить формулировки и доказательства новых утверждений, то интегратор вынужден формировать более широкую систему понятий, в которой могут быть представлены все включенные в монографию, справочник или учебник утверждения и доказательства. Поэтому интегратор, используя свои и (или) чужие статьи, формирует более или менее значительный фрагмент математических знаний. Если в результате деятельности исследователей знания растут экстенсивно, то интеграторы превращают те или иные их части в системы (способствуют интенсивному накоплению знаний).

Банк математических знаний следует рассматривать как систему для накопления достоверных математических знаний. Реальное накопление знаний возможно лишь в том случае, если в этой работе может принять участие любой заинтересованный исследователь. Не менее важна и деятельность интеграторов, в задачу которых входит приведение разрозненных знаний, соответствующих интересам отдельных исследователей, в системы. Наконец, знания, накапливаемые в БМЗ, должны быть широко доступны, чтобы все заинтересованные потребители знаний могли не только ими пользоваться, но и страховать возможные ошибки исследователей и интеграторов. Интернет является той средой, которая может обеспечить широкое и удобное участие всех заинтересованных лиц в работе БМЗ. Принципы организации подобных систем рассматривались в статье [12].

Пользователей БМЗ можно разделить на четыре группы — гостей (потребителей знаний), исследователей (генераторов знаний), интеграторов знаний и администраторов. Гость может лишь просмотреть общую базу знаний БМЗ, а также сообщить администраторам о замеченных в ней недостатках. Математик может сделать заявку на участие в работе БМЗ в качестве исследователя, в ответ получить от администратора полномочие на развитие знаний БМЗ и использовать это полномочие, формируя свою персональную базу знаний (виртуальный аналог своего рабочего стола). Интеграторы знаний рассматривают результаты деятельности каждого исследователя по развитию знаний БМЗ, находящиеся в его персональной базе знаний. Они решают вопрос о включении каждого (возможно модифицированного ими) результата исследователя в общую базу знаний БМЗ. Системные процессы БМЗ поддерживают деятельность исследователей и интеграторов знаний, освобождая их от части рутинной работы.

3. СТРУКТУРА ВНЕШНЕЙ МОДЕЛИ МАТЕМАТИЧЕСКОЙ ПРАКТИКИ

В работе [13] были введены понятия внутренней и внешней моделей математической практики и предложена внутренняя модель для БМЗ. Далее вводится структура внешней модели для БМЗ и устанавливается соответствие между компонентами математической практики и ее внешней модели.

Математическому диалекту может быть поставлена в соответствие грамматика модели математического диалекта, представленная в виде расширенных форм Бекуса—Наура. Исследователи и интеграторы знаний должны иметь возможность включать в текущее состояние этой грамматики новые правила либо модифицировать существующие для расширения языка. Грамматика не охватывает язык пропозициональной логики, поскольку он является фиксированным (и может быть встроен в БМЗ жестко). Язык описания нелогических правил рассуждения (метаязык внутренней модели) является надстройкой над моделью математического диалекта, расширяется благодаря ей и определяется лишь набором типов синтаксических переменных. Каждый тип характеризуется нетерминальным символом грамматики модели математического диалекта, терминальные порождения которого образуют множество возможных значений синтаксических переменных этого типа. Исследователи и интеграторы знаний должны иметь возможность вводить новые типы синтаксических переменных.

Математическим знаниям соответствует общая база знаний, представляющая собой сеть разделов. Всей сетью разделов должен управлять (вводить новые разделы и назначать для них интеграторов знаний) глобальный администратор БМЗ. Информацией внутри каждого раздела должен управлять интегратор знаний этого раздела. Каждый раздел может иметь несколько предков и потомков. Раздел содержит онтологические знания (системы аксиом, определения терминов и новых формальных способов записи), теоремы и модели их интуитивных доказательств. В разделе-потомке справедливы онтологические знания всех его предков. Информации, содержащейся на рабочем столе исследователя и относящейся к его научной работе, соответствует его персональная база знаний. В ней он может вводить свои разделы, онтологические знания, теоремы и доказательства.

Онтологические знания и теоремы представляются средствами модели математического диалекта. Модель каждой теоремы, кроме формулировки, может иметь название (для облегчения ее поиска).

Интуитивным доказательствам соответствуют модели интуитивных доказательств. В теории доказательств обычно различают полное, формальное и интуитивное доказательства. Доказательство является полным, если оно правильно (т. е. правильные правила рассуждения и методы доказательства на каждом шаге правильно применяются к посылкам для вывода следствий), показывает, как доказываемое утверждение следует из посылок, и при этом не ссылается ни на какие недока-

занные утверждения, кроме онтологических знаний. Доказательство является формальным, если оно выполнено в рамках некоторой формальной системы. Последнее означает, что все математические утверждения, использованные в доказательстве, представлены на некотором формальном языке, а все использованные в нем правила рассуждения являются правилами вывода некоторой формальной системы, представленными на некотором формальном метаязыке. Понятно, что эти два определения являются конструктивными — полное или формальное доказательство можно разобрать на части (математические утверждения, правила рассуждения или вывода, методы доказательства), для каждой части можно установить ее правильность, а для всего доказательства — правильность и полноту его сборки из этих частей. Доказательство является интуитивным (ИД), если оно представлено в математической литературе. Очевидно, что это определение не является конструктивным; из него следует, что публикация доказательства в математической литературе, делает его интуитивным. Однако смысл этого определения в другом — все доказательства, имеющиеся в математической литературе, считаются интуитивными (если доказательство принимается математическим сообществом, то оно является интуитивным).

У системы, не поддерживающей построения ИД, нет шансов быть востребованной в науке. Это означает, что усилия, которые математик должен затратить на построение любого доказательства с ее помощью, не должны заметно превышать усилий на построение соответствующего ИД обычным способом. Одновременно, такая система должна гарантировать правильность ИД, построенных с ее помощью.

Отсюда возникают два вопроса: как устроено ИД, и как можно проверить (обеспечить) его правильность? Ответ на второй вопрос очевиден — ИД является правильным, если его можно расширить до полного и формального доказательства. На первый вопрос нельзя дать исчерпывающий ответ (для этого требуется провести анализ всех существующих в математической литературе доказательств), но можно попытаться к нему приблизиться. Модели ИД, способам их интерактивного формирования и обеспечения правильности посвящена вторая часть этой статьи.

Модели способов рассуждения могут быть представлены в специальной базе, разделенной на логический (пропозициональные тавтологии) и нелогический (метаматематические аксиомы) разделы. Модель способа рассуждения может иметь название (для облегчения его поиска).

Модели методов доказательства также могут быть представлены в специальной базе. Модель метода может иметь название (для облегчения его поиска).

ЗАКЛЮЧЕНИЕ

Предложена концепция Интернет-системы компьютерной поддержки научной деятельности в области математики. Основная цель такой системы — накопление математических знаний, обеспечение их достоверности, повышение их доступности и поддержка современного стиля работы математиков. Концепция допускает стихийность в работе исследователей в сочетании с централизованным управлением общими знаниями со стороны интеграторов знаний. Для этого вводится разделение базы знаний на общую и множество персональных. Работа исследователей в своих персональных базах прямо не влияет на содержимое общей базы, которая доступна всем пользователям. Интеграторы знаний формируют общую базу на основе персональных.

ЛИТЕРАТУРА

1. *Гаврилова Т.Л., Клещев А.С.* Анализ подходов к решению проблемы правильности математических знаний // Проблемы управления. — 2005. — № 3. — С. 13—19.
2. *The Coq* Proof Assistant User's Guide, version 6.1 / Cornes C., Courant J., Filliatre J.-C., et al. INRIA-Rocquencourt et CNRSENS. — Lyon, 1996.
3. *Paulson L.C.* Isabelle: A Generic Theorem Prover. LNCS 828. — Springer, 1994.
4. *Gordon M.J.C. and Melham T.F.* (editors). Introduction to HOL: A theorem proving environment for higher order logic. Cambridge University Press, 1993.
5. *Aspinall D.* Eclipse Proof General. 2004 ⟨http://proofgeneral.inf.ed.ac.uk/Kit/docs/EIG04.pdf⟩.
6. *Melis E., Meier A. and Pollet M.* Adaptive Access to a Proof Planner // Third International Conference on Mathematical Knowledge Management. — Springer-Verlag, 2004. — P. 251—264.
7. *Aitken S., Gray Ph.* On using GOMS to analyse definition-making in interactive proving. 1997. ⟨http://www.dcs.gla.ac.uk/~stuart/ITP/ITP.html⟩.
8. *Proof* General in Eclipse. System and Architecture Overview / D. Aspinall, et al. 2006. ⟨http://www.cs.mcgill.ca/%7Emartin/etx2006/papers/30.pdf⟩.
9. *Voelker N.* Thoughts on Requirements and Design Issues of User Interfaces for Proof Assistants. — 2003 ⟨http://www.informatik.uni-bremen.de/~cxl/uitp03/entcs/08-Voelker.pdf⟩.
10. *Melis E. and Siekmann J.H.* Concepts in Proof Planning // Intellectics and Computational Logic. Kluwer. — 2000. — P. 263—276.
11. *Meier A., Melis E., Pollet M.* Adaptable Mixed-Initiative Proof Planning for Educational Interaction. — 2003. ⟨http://www.informatik.uni-bremen.de/~cxl/uitp03/entcs/06-PolletMellisMeier.pdf⟩.
12. *Мультидисциплинарная* система управления информационными ресурсами различных уровней общности / И.Л. Артемьева, Т.Л. Гаврилова, В.В. Грибова и др. // Проблемы управления. — 2006. — № 4. — С. 64—68.
13. *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. ❑