УДК 165.17
DOI:
10.15372/PS20200105

А.В. Хлебалин

ИНТЕРАКТИВНОЕ ДОКАЗАТЕЛЬСТО: ВЕРИФИКАЦИЯ И ГЕНЕРИРОВАНИЕ НОВОГО МАТЕМАТИЧЕСКОГО ЗНАНИЯ*

В статье рассматриваются классические вопросы эпистемологии математики в связи с применением компьютерных систем в математическом исследовании. Показано, что зачастую проблемы эпистемологической характеристики математических результатов, полученных с помощью компьютера, связаны с непроясненностью содержания традиционных концепций эпистемологии математики, таких как доказательство, вычисление, истины и верификация. На примере характеристики логико-теоретических оснований интерактивных компьютерных систем, созданных на базе теории типов, демонстрируется их потенциал в области экспликации традиционных концепций эпистемологии математики.

Ключевые слова: компьютерное доказательство; автоматизированные системы верификации в математике; гомотопная теория типов; доказательство; вычисление

A.V. Khlebalin

INTERACTIVE PROOF: VERIFICATION AND GENERATION OF NEW MATHEMATICAL KNOWLEDGE

The article discusses the classical issues of the epistemology of mathematics in connection with the use of computer systems in mathematical research. It is shown that the problems of epistemological description of computer-assisted mathematical results are often due to the confusion over the content of traditional concepts of the epistemology of mathematics, such as proof, calculation, truths, and verification. The example of characteristics of the logical and theoretical foundations of interactive computer systems based on the theory of types demonstrates their potential in explicating the traditional concepts of the epistemology of mathematics.

Keywords: computer-assisted proof; automate verification systems in mathematics; homotopy type theory; proof; calculation

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 19-011-00301).

Применение компьютера в математической практике привело к постановке целого спектра проблем: от логико-эпистемологических до социально-психологических. Само использование компьютеров разделило математическое сообщество на апологетов применения компьютера в математической практике, таких, например, как В. Воеводский, и принципиальных противников, связывающих все возрастающее применение компьютеров в математике со «смертью математического доказательства», таких как, например, Дж. Хорган.

Доказательство теоремы о четырех красках послужило катализатором возникновения эпистемологических по своему содержанию споров о природе компьютерных доказательств и их статусе в целом. Т. Тимошко [6] первым формулирует вызовы, с которыми сталкивается математика в связи с применением компьютера.

1. С традиционной точки зрения доказательство теоремы о четырех красках нужно воспринимать как доказательство с пробелом из-за отсутствия доказательства одной ключевой леммы. Этот пробел в настоящее время считается заполненным посредством ее компьютерного доказательства.

2. Поскольку никто не может проверить предоставленные компьютером доказательства, принятие их означает, что математика становится, наподобие физики, эмпирической. Надежность подобных доказательств не определена и основана на комплексе эмпирических факторов, связанных с функционированием компьютеров.

3. Некоторые математические истины больше не являются априорными, а становятся зависимыми от чувственного опыта, опирающегося на результаты экспериментов.

В то же самое время появляется альтернативная точка зрения, сторонники которой считают беспокойство Т. Тимошко либо преувеличенным, либо вовсе необоснованным.

Так, П. Теллер [5] оспаривает все три приведенные выше положения на том основании, что в них очевидна путаница концепций доказательства и проверки правильности доказательства. По его мнению, концепция доказательства не изменилась с применением компьютеров; утрата в случае компьютерных доказательств обозримости, на его взгляд, свидетельствует только о расширении методов проверки доказательств. Но это изменение в методах проверки Теллер объявляет несущественным, потому что нет принципиальной разницы между проверкой доказательства компьютером и его проверкой математиком, так

как оба могут ошибаться, и в большом числе случаев компьютерная проверка по очевидным причинам предпочтительнее проверки, выполненной человеком.

М. Детлефсен и М. Лукер [1] придерживаются совершенно другой точки зрения, согласно которой проверку правильности доказательства, в частности когда речь идет о проверке правильности вычислений, от которых зависит доказательство, можно рассматривать в качестве части самого доказательства. Более того, такого типа проверки иногда опирались на эмпирические данные даже в случае традиционных, осуществляемых людьми доказательств математических теорем. Эти авторы согласны с Т. Тимошко в том, что доказательство теоремы о четырех красках включает эмпирический компонент, но использование таких доказательств не является чем-то новым, утверждают они, и, следовательно, использование компьютеров для проверки не влечет никаких фундаментальных изменений в математической практике.

Сложно отрицать, что в обсуждение проблем применения компьютера в математической практике включено большое количество вопросов, которые оказались слишком тесно переплетенными. Также не вызывает сомнения, что проблема не может иметь общего решения без подробного анализа составляющих ее частей. Простейшей экспозиции точек зрения апологетов и противников использования компьютеров в математической практике достаточно, для того чтобы стало явным то обстоятельство, что в обсуждении эпистемологических характеристик компьютерных результатов в математике переплетаются классические концепции, имеющие многообразные трактовки в философии математики, такие как концепция доказательства, истины, вычислимости. Ниже мы ограничимся обзором того, каким образом интерактивные системы математического доказательства, прежде всего логико-теоретические основания таких систем, позволяют уточнить и сделать более ясным содержание традиционных концепций эпистемологии математики.

Идея формализации математических рассуждений имеет длительную историю. Очевидное преимущество формального способа рассуждения состоит в том, что он максимально облегчает верификацию математического результата. Механизация математического рассуждения может рассматриваться как абсолютное воплощение формального рассуждения. В явном виде восходя к идее о «Mathesis Universalis», последние 150 лет идея механизации математических рассуждений переживает наиболее бурное развитие. XX век может рассматриваться в качестве этапа наибольшего расцвета и максимальной степени практической

реализации этой идеи. Непрекращающийся рост количества полностью автоматизированных и интерактивных компьютерных систем можно рассматривать как конкретные технические решения задач по реализации указанной идеи. Роль компьютера в получении математического результата может варьировать от проверки формализованного доказательства, созданного человеком, до случаев, когда прувер настолько автоматизирован, что получает результат, но тем не менее контролируется и в известной степени направляется человеком. Между этими крайними позициями располагается большое количество многообразных способов взаимодействия машины и человека. «В свете практических ограничений, сегодня кажется – нравится ли это кому-то или нет, – что интерактивное доказательство является единственным способом формализовать большинство нетривиальных теорем математики или способом проверки корректности компьютерных систем» [4, p. 223].

Теоретики 1950–1960 годов – М. Дэвис, Д. Гилмор, Д. Правиц, Х. Ван были заняты полностью автоматизированными системами доказательства. Очевидной целью создания таких систем стала бы проверка известных математических результатов, т.е. задачей являлось создание автоматизированных систем проверки ранее поученных результатов. Несмотря на то что математическое знание традиционно воспринимается как воплощенный образец строгости и обоснованности, широко известны примеры часто допускаемых ошибок в доказательствах. Наверное, наиболее известен случай с Д. Гильбертом, связанный с желанием коллег и учеников ученого издать к его юбилею избранные работы, при подготовке которых случайно была обнаружена ошибка в вычислениях. В связи с этим обстоятельством было решено тщательно проверить вычисления и доказательства в статьях, составляющих издание, и выявление ошибок и их исправление отложили выход книги на три года.

Верификация ранее полученных результатов казалась в 1950–1960-е ггоы подходящей задачей для вычислительных систем, достигших должной степени мощности. Например, Х. Ван так формулирует поставленные цели: «Первоначальной целью было взять математические руководства вроде работ Ландау о системах счисления, Харди и Райта о теории числа, Веблена и Янга о проективной геометрии, томов Бурбаки и создать машинную формализацию всех содержащихся в них доказательств» [7, p. 15].

Помимо полностью автоматизированной верификации математических результатов, в 1960-е годы возникает идея интерактивной вери-

фикации результатов. О преимуществах такого подхода заявляет, например, Дж. Маккарти: «Проверка математических доказательств является потенциально одним из самых интересных и полезных приложений автоматов. Компьютеры могут проверять не только доказательства новых математических теорем, но и доказательства того, что сложные инженерные системы и компьютерные программы соответствуют своим спецификациям. Доказательства, проверенные компьютером, могут оказаться проще, чем неформализованные доказательства, принятые у математиков. Это потому, что мы можем заставить компьютер проделать гораздо большую работу по проверке каждого шага, которую люди не желают делать. … Комбинирование техник проверки доказательств с эвристиками нахождения доказательства позволит математикам воспользоваться такими идеями для создания доказательств, которые пока довольно расплывчаты, но могут ускорить математические исследования» [4, p. 222].

Развитие обеих тенденций привело к возникновению целого направления – «экспериментальной математики», апологеты которой оценивают ее как своеобразную математическую «лабораторию», в которой анализируются примеры, тестируются новые идеи или происходят поиски новых структур. В качестве основных могут быть указаны следующие направления приложения компьютера в математике: «1) достижение понимания и прояснение интуиции; 2) обнаружение новых структур и отношений; 3) использование графических демонстраций для обнаружения лежащих в основании математических принципов; 4) проверка и особенно фальсификация предположений; 5) исследование предполагаемых результатов с целью определения необходимости их формального доказательства; 6) предложение подходов для формального доказательства; 7) замена пространных доказательств компьютерными вычислениями; 8) подтверждение аналитических результатов» [3, p. 157].

С точки зрения эпистемологии математики эти многообразные направления применения компьютера в математике могут быть обобщены до двух основных: верификации математического знания с помощью компьютера и использования компьютера для доказательства новых теорем. Такое противопоставление этих направлений во многом условное и востребовано скорее в философии математики, чем в процессе разработки самих интерактивных и автоматизированных компьютерных систем.

При использовании компьютерных программ для верификации математических результатов основной проблемой оказывается задача верификации самой используемой программы. Корректность программы может быть продемонстрирована двумя различными способами: индуктивным и дедуктивным. Хотя само это противопоставление в случае верификации компьютерной программы теоретически не прояснено, традиционно дедуктивная демонстрация корректности программы считается более надежной. Вместе с тем доказательство корректности программы, как правило, является невероятно сложным и объемным, потому что строится компьютером, а не человеком. Здесь мы сталкиваемся с проблемой соотнесения концепции доказательства и вывода. Концепция формального доказательства включает в себя идею рассмотрения всей структуры доказательства как цепочки выводов. Но действительно ли выводы интерпретированной формальной системы представляют собой доказательство, зависит от природы правил вывода. Может казаться достаточным факт, что используемые правила вывода гарантируют сохранение истинности, а формальная система, построенная на основе таких правил вывода, и предоставляет доказательство. Однако такое понимание игнорирует следующие обстоятельства. Прежде всего, правила вывода действительно могут сохранять истинность, но эпистемическая дистанция между предпосылками и заключением может быть столь большой, что полученное на основе этих правил доказательство будет полностью лишено какого-либо понимания. Далее, убедительность доказательства должна происходить из самого доказательства, если же она достигается на метауровне посредством демонстрации сохранения истинности правилами вывода формальной системы, мы имеем дело с переадресацией вопроса об убедительности на более высокий уровень.

Разработка точной эпистемической концепции доказательства требует выхода за пределы концепции формального вывода. Так, например, конструктивистская традиция включает в себя концепцию основания утверждения в связи с его значением. Эти идеи могут быть использованы для рекурсивного определения оснований суждений различной формы. Простейшим примером может служить система натурального вывода Г. Генцена, в которой правила введения логических констант «дают, так скажем, определения этих констант», т.е. определяют значение предложений, построенных с их помощью. В таком случае можно определить, что *g* является основанием утверждения истинности конъюнкции $A_1 \wedge A_2$ только в том случае, если *g* представляет

собой $<g_1, g_2>$, где g_1 и g_2 являются основанием утверждения истинности A_1 и A_2 соответственно.

Коль скоро мы определили, что́ конституирует основания для суждений различной формы, появляется возможность понимать вывод не как утверждение заключения на основе ранее принятых посылок, а скорее как трансформацию основания. В этом случае вывод определяется не только предпосылками и заключением, но и операциями по трансформации основания. Вывод, определяемый своими посылками, заключением и применимыми к основаниям операциями, будет определяться как валидный в том случае, если операции, применимые к основаниям посылок, позволяют получить основания для заключения. Доказательство, таким образом, понимается как построенное на основе успешного применения таких операций. В такой концепции доказательство определяется тем, что дает ответ на вопрос о том, каким образом доказательство утверждения может обеспечивать его истинность: доказательство утверждения A предоставляет окончательное основание для A в силу значения A и того, как определяются операции вывода, на основе которого строится доказательство.

Эта краткая характеристика связи доказательства и истинности вместе с тем сталкивает нас с проблемой связи концепций доказательства и вычисления. Соотношение этих концепций в высшей степени важно в контексте проблемы развития дедуктивного подхода к верификации программ. Х. Карри первым отметил изоморфизм между доказательствами в импликативном фрагменте минимальной пропозициональной логики и терминами в определенных (комбинаторная логика и лямбда-исчисление) вычислительных системах. У. Ховард расширяет его до изоморфизма между дедукцией в генценовской системе интуиционистской предикатной логики и расширенным лямбда-исчислением, что завершает формирование соответствия Карри – Ховарда. Это формальное соответствие имеет большое значение для обсуждения интересующих нас проблем, особенно в контексте связи вычислений и программ с учетом результата А.Н. Колмогорова о том, что пропозиции в интуиционистской системе могут интерпретироваться в качестве проблем, а интуиционистское доказательство – как метод, или программа, решения проблем. Эта интерпретация интуиционистских пропозиций систематически была разработана П. Мартин-Лефом в его теории типов, согласно которой выражение $a \in A$ может быть прочитано как утверждающее не то, что a является доказательством пропозиции A, а то, что a является объектом типа A и что a является программой (алгоритмом) разрешения A.

В теории типов Мартин-Лефа задача верификации корректности программы может быть представлена как аналогичная установлению истинности всех предложенных доказательств. То есть проблема верификации корректности программ сводится к механически разрешимой проблеме.

Первой интерактивной программой доказательства теорем, использующей изоморфизм Карри – Ховарда для кодирования доказательств, бала Automath. Эта программа положила начало традиции, продолжающейся до сих пор. Принято различать два варианта изоморфизма Карри – Ховарда: в одном из них формула представлена типом, тогда как во втором формулы не являются типами, но с каждой из них ассоциирован тип объектов доказательств (известны закрепленные за каждым из вариантов слоганы, демонстрирующие специфику каждого из вариантов изоморфизма; для первого из них – «формулы как типы», а для второго – «доказательства как объекты») [2]. Первый из вариантов изоморфизма реализован в таких системах, как Coq, Agda и NuPRL, второй – в самой системе Automath. В любом из вариантов изоморфизма реализуется идея, согласно которой тип «объектов доказательства», ассоциированный с формулой, оказывается непустым только в том случае, если формула истинна. Современным этапом развития теории типов является унивалентная теория типов, в которой первая расширяется интерпретацией равенства как гомотопного, что служит источником аксиомы унивалентности. Это позволяет «встроить» в теорию типов представление о независимости, что дало возможность рассматривать гомотопную теорию типов в качестве претендента на то, чтобы выступать новыми основаниями математики.

Развитие основанной на теории типов интерактивной системы Automath и других систем, а также разработка их логико-теоретических оснований в существенной степени позволяют прояснить содержание традиционных концепций эпистемологии математики, а логико-теоретические решения, реализованные в этих системах, позволяют эксплицировать во многом интуитивное содержание этих концепций вплоть до того, чтобы выступить источником возникновения теорий, претендующих на роль новых оснований математики, как в случае с гомотопной теорией типов.

Литература

1. *Detlefsen M., Luker M.* The four-color theorem and mathematical proof // The Journal of Philosophy. – 1980. – Vol. 77. – P. 803–820.

2. *Geuvers H., Barendsen E.* Some logical and syntactical observations concerning the first-order dependent type system lambda-P // Mathematical Structures in Computer Science. – 1999. – № 9 (4). – P. 335–359.

3. *Mathematics* by Experiment: Plausible Reasoning in the 21st Century / Ed. by J. Borwein, D. Bailey. – A. K. Peters/CRC Press. – 393 p.

4. *McCarthy J.* Computer programs for checking mathematical proofs // Proceedings of the Fifth Symposium in Pure Mathematics of the American Mathematical Society, 1961. – P. 219–227.

5. *Teller P.* Computer proof // The Journal of Philosophy. – 1980. – Vol. 77. – P. 797–803.

6. *Tymoczko T.* The four-color problem and its philosophical significance // The Journal of Philosophy. – 1979. – Vol. 76. – P. 57–83.

7. *Wang H.* Toward mechanical mathematics // IBM Journal of Research and Development. – 1960. – Vol. 4. – P. 2–22.

References

1. *Detlefsen, M. & M. Luker.* (1980). The four-color theorem and mathematical proof. The Journal of Philosophy, 77, 803–820.

2. *Geuvers, H. & E. Barendsen.* (1999). Some logical and syntactical observations concerning the first-order dependent type system lambda-P. Mathematical Structures in Computer Science, 9 (4), 335–359.

3. *Borwein, J. & D. Bailey* (Eds.). (2004). Mathematics by Experiment: Plausible Reasoning in the 21st Century. A.K. Peters, 302.

4. *McCarthy, J.* (1961). Computer programs for checking mathematical proofs. In: Proceedings of the Fifth Symposium in Pure Mathematics of the American Mathematical Society, 219–227.

5. *Teller, P.* (1980). Computer proof. The Journal of Philosophy, 77, 797–803.

6. *Tymoczko, T.* (1979). The four-color problem and its philosophical significance. The Journal of Philosophy, 76, 57–83.

7. *Wang, H.* (1960). Toward mechanical mathematics. IBM Journal of Research and Development, 4, 2–22.

Информация об авторе

Хлебалин Александр Валерьевич – кандидат философских наук, старший научный сотрудник Институт философии и права СО РАН (630090, Новосибирск, ул. Николаева, 8, e-mail: sasha_khl@mail.ru).

Information about the author

Khlebalin Aleksandr Valerievich – Candidate of Sciences (Philosophy), Researcher at the Institute of Philosophy and Law, Siberian Branch of the Russian Akademy of Sciences (8, Nikolaev st., Novosibirsk, 630090 Russia, e-mail: sasha_khl@mail.ru)

Дата поступления 13.01.2020