ФИЛОСОФИЯ

УДК 165.24+168.3:[51+004.9]

DOI: 10.17072/2078-7898/2021-1-5-19

ПРАКТИКА КОМПЬЮТЕРНЫХ ДОКАЗАТЕЛЬСТВ И ЧЕЛОВЕЧЕСКОЕ ПОНИМАНИЕ: ЭПИСТЕМОЛОГИЧЕСКАЯ ПРОБЛЕМАТИКА

Ламберов Лев Дмитриевич

Уральский федеральный университет им. первого Президента России Б.Н. Ельцина (Екатеринбург)

В последние десятилетия в математике особую остроту приобрели эпистемологические проблемы, связанные со слишком большой длиной доказательства важных математических результатов, а также с большим и постоянно возрастающим количеством публикаций по математике. Предполагается, что эти затруднения могут быть разрешены (хотя бы частично) путем обращения к компьютерным доказательствам. Однако и компьютерные доказательства оказываются проблематичными с эпистемологической точки зрения. И относительно доказательств в обычной (неформальной) математике, и относительно компьютерных доказательств в равной степени актуальна проблема их обозримости. Исходя из традиционного понимания доказательства оно обязательно должно быть обозримым, иначе оно не будет достигать своей основной цели — формирования убежденности в правильности доказываемого математического результата. Около 15 лет назад начал развиваться новый подход к основаниям математики, сочетающий в себе конструктивистские, структуралистские черты и ряд преимуществ классического подхода к математике. Этот подход выстраивается на основе гомотопической теории типов и носит название унивалентных оснований математики. Благодаря мощному понятию равенства этот подход позволяет значительно сократить длину формализованных доказательств, что намечает путь к разрешению возникших эпистемологических затруднений.

Ключевые слова: доказательство, понимание, обозримость, основания математики, практика.

COMPUTER PROOFS PRACTICE AND HUMAN UNDERSTANDING: EPISTEMOLOGICAL ISSUES

Lev D. Lamberov

Ural Federal University named after the first President of Russia B.N. Yeltsin (Ekaterinburg)

In recent decades, some epistemological issues have become especially acute in mathematics. These issues are associated with long proofs of various important mathematical results, as well as with a large and constantly increasing number of publications in mathematics. It is assumed that (at least partially) these difficulties can be resolved by referring to computer proofs. However, computer proofs also turn out to be problematic from an epistemological point of view. With regard to both proofs in ordinary (informal) mathematics and computer proofs, the problem of their surveyability appears to be fundamental. Based on the traditional concept of proof, it must be surveyable, otherwise it will not achieve its main goal — the formation of conviction in the correctness of the mathematical result being proved. About 15 years ago, a new approach to the foundations of mathematics began to develop, combining constructivist, structuralist features and a number of advantages of the classical approach to mathematics. This approach is built on the basis of homotopy type theory and is called the univalent foundations of mathematics. Due to its

powerful notion of equality, this approach can significantly reduce the length of formalized proofs, which outlines a way to resolve the epistemological difficulties that have arisen.
Keywords: proof, understanding, surveyability, foundations of mathematics, practice.

На протяжении истории математика довольно часто воспринималась как дисциплина, претендующая на абсолютное знание. Такое понимание предполагает, что математика «непогрешима», математические результаты не пересматриваются, а общая структура математического исследования и математического знания являются желаемой целью и ориентиром для остальных наук. В истории философии и математики такие идеи можно встретить и у древнегреческих авторов, и у философов Нового времени, и у ряда современных исследователей. Тем не менее математикой занимаются люди, а людям, как утверждает древняя мудрость, свойственно ошибаться. Следовательно, имеется определенный запрос на выработку таких методов математического исследования, которые бы соответствовали предполагаемой «непогрешимости» математики и гарантировали отсутствие ошибок. Кроме того, в настоящее время развитие математического знания дошло до такой стадии, когда в некоторых предметных областях доказательство даже ключевых теорем становится настолько большим, что проверка этих доказательств серьезно затрудняется. Для некоторых исследователей указанные обстоятельства служат основанием для обращения к компьютерным доказательствам.

Настоящая статья посвящена рассмотрению некоторых сложившихся практик работы с компьютерными доказательствами, а также вопросам соотношения компьютерных доказательств с человеческим пониманием. Рассматриваются эпистемологические затруднения, возникающие при использовании компьютерных доказательств, а также дается обзор современных подходов к основаниям математики. Предполагается, что новые подходы к основаниям математики позволяют изменить практику разработки компьютерных доказательств таким образом, что рассматриваемые эпистемологические затруднения (частично) разрешаются. В статье предлагаются вопросы, обсуждение которых позволит в дальнейшем определить, являются ли предполагаемые решения эпистемологических затруднений достаточными и могут ли они косвенно использоваться при сравнении различных конкурирующих подходов к основаниям математики.

Статья разделена на пять частей. В первой части указываются причины обращения к компьютерным доказательствам. Во второй части рассматриваются некоторые сложившиеся практики разработки и использования компьютерных доказательств. В третьей части дается обзор проекта QED, основной целью которого является переход к формализованной и компьютеризированной математике. Четвертая часть посвящена проблематике человеческого понимания в связи с компьютерными доказательствами, что позволяет наметить основные эпистемологические затруднения компьютерных доказательств. В пятой части дается обзор современных подходов к основаниям математики, которые, как это предполагается, (частично) разрешают эпистемологические затруднения. В пятой же части ставятся вопросы для дальнейшего исследования эпистемологии компьютерных доказательств и оснований математики.

I. Причины обращения к компьютерным доказательствам

Основной (своего рода, насущной) причиной обращения к компьютерным доказательствам является постоянно увеличивающаяся сложность математического знания. Компьютерные доказательства сами по себе представляли и представляют собой интересный предмет исследований, однако причина особого внимания к ним состоит в надежде на то, что компьютерные доказательства позволят упростить труд работающего математика. Причем необходимо отметить, что сложность математики понимается в данном случае сразу в нескольких аспектах[1].

Первый и наиболее важный аспект сложности математики заключается в размерах доказательств. Так, некоторые теоремы имеют настолько объемные доказательства, что их проверка существенно затруднена. Причем это касается в том числе и теорем, которые являют-

[1] По отдельности эти аспекты отмечаются, например, в статье В. А. Шапошникова [Шапошников В.А., 2018].

ся центральными для некоторых разделов математики. Чего стоит, например, препринт доказательства теоремы Ф. Олмгрена из геометрической теории измерений, занимающий 1728 машинопечатных страниц[2], или доказательство теоремы Робертсона–Сеймура из теории графов, опубликованной в виде серии из 20 статей общим объемом почти 600 страниц[3]. Таким образом, по меньшей мере некоторые результаты насколько велики, что временные затраты на проверку доказательств превосходят разумные (человеческие) пределы. Поскольку понимание доказательства дает понимание причин, *почему* математический результат имеет место, постольку слишком трудоемкое освоение доказательства не позволяет достичь более глубокого понимания самого математического результата. В качестве иллюстрации можно привести случай, описываемый Б. Дэйвисом [Davies B., 2005, p. 1353], когда один из его студентов поставил под сомнение использование в доказательстве одной из теорем обобщенного варианта теоремы Мерсера [Mercer J., 1909]. Дело в том, что хотя обобщенный вариант теоремы Мерсера использовался многими математиками, он не был явно приведен ни в одной публикации[4] (соответственно, и не имел опубликованного доказательства). В связи с этим Б. Дэйвис решил опубликовать обобщенный вариант теоремы Мерсера с доказательством. Хотя, как он сам признался, «для меня и для всякого, кто достаточно подробно изучил изначальное доказательство, было очевидно, что классическое ограничение интервала не является необходимым, однако потребовалось четыре страницы для описания и доказательства достаточно общей формы данного результата» [Davies B., 2005, p. 1353]. Очевидно, что отсутствие понимания изначального доказательства не позволило бы использовать обобщенный вариант теоремы в доказательстве многих других математических результатов, которые в этом случае просто оказались бы недоступными математическому сообществу.

Второй аспект сложности математики связан скорее не с внутренними особенностями современного математического знания, а с социологическими (или даже демографическими) факторами. Этот аспект касается совокупного объема публикуемых математических работ. К примеру, рейтинг математических журналов (область: математика; без предметной категории, с включением компьютерных наук) Scimago Journal and Country Rank за 2019 г. содержит 2024 журнала[5], а в arXiv, архив электронных публикаций и препринтов, за 2019 г. было добавлено 37 294 статьи по математике[6]. Это весьма и весьма приличный объем, который не позволяет отдельно взятому математику быть в курсе всех новых результатов (по меньшей мере, в математике в целом), не говоря уже о внимательном изучении соответствующих доказательств. Несомненно, такая ситуация приводит к усилению специализации среди математиков и дальнейшему дроблению математической науки на составные части, области исследований, а проверка результатов потенциально затрудняется (например, ввиду недостаточного числа квалифицированных специалистов и отсутствия у них времени).

Однако два указанных аспекта, поскольку они являются независимыми друг от друга, вполне могут совмещаться, и фактически в математике такое совмещение уже имеет место. Наиболее обсуждаемым примером такого совмещения является теорема о классификации простых конечных групп. Доказательство этой теоремы занимает десятки тысяч страниц и разделяется на большое количество промежуточных результатов, опубликованных в нескольких сотнях журнальных статей. Само по себе доказательство представляет собой своего рода «мозаику», собранную приблизительно сотней разных авторов. Впервые завершение доказательства было анонсировано в 1983 г. Д. Горенстейном, однако оно содержало некоторое ко-

[2] Автор работал над доказательством теоремы более 10 лет, с 1970-х до начала 1980-х гг., а до 2000 г. эта работа не была опубликована, хотя сама по себе эта теорема сегодня считается одной из фундаментальнейших [Almgren's Big Regularity Paper, 2000].

[3] Статьи публиковались с 1983 по 2004 г. в журнале «Journal of Combinatorial Theory» [Robertson N., Seymour P., 1983, 2004].

[4] Ср. с концепцией «личностного» знания М. Полани [Polanyi M., 1958].

[5] Scimago Journal and Country Rank. 2019. URL: https://www.scimagojr.com/journalrank.php?area=2600&year=2019 (accessed: 09.09.2020).

[6] Mathematics. Article statistics for 2019. URL: https://arxiv.org/year/math/19 (accessed: 09.09.2020).

личество пробелов, небольшие из которых были заполнены относительно быстро, однако наибольший пробел, заключающийся в классификации квазитонких групп, был заполнен лишь в 2004 г. после завершения совместной работы М. Ашбахера [Aschbacher M., 2004] и С. Смита (один только этот результат занимает 1221 страницу). Планировалось систематически представлять доказательство теоремы в виде многотомного книжного издания, однако публикацию планируется завершить лишь к 2023 г. при условии, что будут решены все оставшиеся проблемы [Solomon R., 2018]. Таким образом, в настоящее время полное доказательство не только не издано, но оно пока отсутствует в принципе, хотя сомнений у большинства математиков в том, что оно будет рано или поздно получено, нет. То есть этот результат получил статус теоремы еще до полного построения доказательства. Такая «незавершенность» доказательства объясняется следующей особенностью: нет какого-то серьезного ограничения на «открытие» новых простых конечных групп. Если новая (не учтенная до этого) простая конечная группа окажется достаточно «похожей» на уже известные и классифицированные, то это не должно вызвать серьезных затруднений. Однако обнаружение новой простой конечной группы, которая будет серьезно отличаться от уже известных, вновь приведет к ситуации, когда доказательство этой теоремы станет незавершенным. Надежды на правильность доказательства основываются на том, что обнаруженные до сих пор пробелы, заполнялись путем выполнения дополнительной математической работы. Однако не следует забывать, как выражается Б. Дэйвис, что «цепь настолько крепка, насколько слабо ее самое слабое звено, а тот факт, что всякое дефектное звено до настоящего времени заменялось на правильное, не гарантирует того, что так будет продолжаться и далее» [Davies B., 2005, p. 1354]. Даже если предполагать, что доказательство всегда можно будет дополнить для учета любой новой простой конечной группы, это не делает невозможной ситуацию, когда доказательство оказывается принципиально незавершаемым.

Один из авторов доказательства теоремы о классификации простых конечных групп утверждает, что «польза» этой теоремы основывается на двух важных фактах [Aschbacher M., 2005, p. 2403–2404]. Во-первых, это сводимость конечных групп к простым группам. Во-вторых, описание групп дополняется эффективной репрезентацией. Соответственно, из набора объектов со «слабой» структурой и высокой сложностью можно получить набор объектов с «сильной» структурой и более низкой сложностью (этот переход скрыт в доказательстве от тех, кто использует теорему), а «перевод» проблемы, не имеющей классической математической структуры (например, из области биологии или теории информации), в теорию групп позволяет благодаря обсуждаемой теореме достаточно быстро получить решение. В этой связи достаточно сложная математика становится близкой к таким наукам, в которых имеет место переизбыток информации (например, в смысле наблюдаемых данных). Другими словами, такая математика стремится к связному описанию и последовательному объяснению чрезмерно большого количества разнородной (возможно, слабо структурированной) информации, а соответствующее доказательство зачастую оказывается чрезмерно длинным и сложным. Поэтому узкие идеалы классической математической строгости и красоты могут быть расширены или пересмотрены в пользу идеалов приложимости математических результатов.

Таким образом, в настоящее время мы имеем дело со все возрастающей сложностью математики, которая выходит за пределы когнитивных способностей отдельно взятого человека. В связи с этим некоторые исследователи выражают надежду на (хотя бы частичное) разрешение проблемы сложности математики путем обращения к компьютерным доказательствам и тотальной формализации.

II. Компьютерное доказательство: история и сложившаяся практика

Использование людьми вспомогательных вычислительных средств имеет довольно давнюю историю, однако эти средства применялись в основном в приложениях математики, а не в доказательствах теорем[7] (т.е. не для получения нового математического знания). В силу принципов функционирования вычислительных ма-

[7] Обзор проблематики компьютерных доказательств см.: [Ламберов Л.Д., 2018а, 2019, 2020].

шин (вплоть до настоящего времени) только формализованные доказательства могут быть представлены в компьютерной форме. Таким образом, у истоков компьютерных доказательств стоят создатели современной математической логики. Хотя математическая логика, метод формализации применительно к математике и формализованные математические теории вообще развивались начиная со второй половины XIX в., возможность создания первых компьютерных доказательство появилась лишь в 1950-х гг. с созданием первых вычислительных машин общего назначения (по сути, цифровых компьютеров).

Одними из первых[8] компьютерных доказательств стали (1) доказательство М. Дэвисом [Davis M., 1983a] того, что сумма двух четных чисел является четным числом в арифметике Пресбургера на компьютере JOHNNIAC в 1954 г., (2) доказательства 38 теорем исчисления высказываний из второй главы *Principia Mathematica* Б. Рассела и А. Уайтхэда, выполненные «Машиной логической теории», программой, написанной А. Ньюэлом, Дж. Шоу и Г. Саймоном [Newel A. et al., 1983] в 1957 г.

В дальнейшем и приблизительно до 1970-х гг. в качестве основного метода, используемого в компьютерных доказательствах, выступал метод резолюций. Например, Л. Вос и Л. Геншен описывают ситуацию таким образом: «Между 1967-м и 1970-м гг. по автоматическому доказательству теорем появилось около девяноста статей и докладов, из которых более шестидесяти в том или ином аспекте касались [метода] резолюций» [Wos L., Henschen L., 1983, p. 4]. Исследователям казалось, что благодаря открытию Дж. Робинсоном алгоритма синтаксической унификации для метода резолюций практически все проблемы автоматических доказательств решены. Правда, следует отметить одну важную особенность систем компьютерных доказательств, выстраиваемых на основе этого метода, которая делает компьютерные доказательства проблематичными с эпистемологической точки зрения. Дело в том, что при использовании метода резолюций вычислительная машина работает по принципу своего рода «черного ящика», когда исследователь имеет лишь крайне ограниченные возможности влияния на построение доказательства и вынужден, по сути, лишь ждать завершения работы программы. Причем ресурсы компьютера вполне могут закончиться раньше того момента, когда будет найдено доказательство.

Одновременно велись работы по разработке различных семантик языков программирования, которые позволяли бы использовать математические методы для доказательства корректности программного обеспечения (т.е. соответствия написанного программистом кода заданной спецификации). В частности, эти исследования привели к созданию около 1980 г. системы компьютерных доказательств LCF [Milner R., 1979], основной особенностью которой стала возможность программирования тактик доказательств на специальном языке ML. Кроме того, следует упомянуть серьезный прогресс в формализации доказательств по индукции и разработке систем переписывания термов, выразившийся в создании Р. Бойером и Дж.С. Муром (в создание дальнейших улучшений значительный вклад внес также М. Кауфман) системы Nqthm [Boyer R.S. et al., 1995].

Однако наибольшее влияние на современные подходы к разработке систем компьютерных доказательств оказало развитие теории типов. Так, в 1968 г. Н. де Брёйн [De Bruijn N., 1983] создал систему *Automath*, способную выполнять проверку корректности математических доказательств потенциально любой формы. Добиться этого удалось благодаря использованию теории типов и лямбда-исчисления. Теория типов была впервые представлена Б. Расселом[9] в качестве решения проблемы парадоксов и использована им совместно с А. Уайтхэдом в *Principia Mathematica*, а лямбда-исчисление создано А. Чёрчем [Church A., 1932, 1940] для исследования понятия вычислимости. Типизированное лямбда-исчисление помимо прочего представляет собой вариант исчисления высших порядков, т.е. может выступать в качестве более простой альтернативы метаматематике в духе Б. Рассела и

[8] Обзор предыстории и ранней истории компьютерных доказательств см.: [Davis M., 1983b].

[9] «Приложение B: Доктрина типов» см.: [Russell B., 1903].

А. Уайтхэда. Кроме того, вычисление лямбда-терма может быть представлено в схожем с натуральным выводом виде, что в конечном счете позволило обнаружить взаимосвязь между (конструктивными) доказательствами, с одной стороны, и лямбда-термами — с другой. Указанная взаимосвязь носит название изоморфизма Карри–Говарда и ставит в соответствие высказывания (теоремы) и типы, а также доказательства высказываний (теорем) и термы, обладающие соответствующим типом.

Расцвет развития теории типов в области компьютерных наук приходится на последнюю четверть XX в. и настоящее время. В 1970-х гг. на основе лямбда-исчисления П. Мартин-Лёф [Martin-Löf P., 1984; Ламберов Л.Д., 2017] сформулировал интуиционистскую теорию типов, мощную систему для конструктивной аксиоматизации математических структур. Благодаря структурной связи между высказываниями и доказательствами, с одной стороны (со стороны логики), и типами и термами — с другой (со стороны типизированных вычислений), теоретико-типовой подход представляет собой вариант интерпретации логических понятий и позволяет анализировать статику и динамику доказательств (например, в соответствии с конструктивным подходом). В дальнейшем на основе интуиционистской теории типов П. Мартин-Лёфа были построены различные исчисления, которые, в свою очередь, реализованы в специальных интерактивных средствах доказательства теорем (например, исчисление построений реализовано в языке *Coq*).

Полностью автоматические доказательства редко используются для доказательства математических результатов, в основном они нужны для гарантии корректности программного обеспечения и не предусматривают, что кто-то будет их читать. Для математических результатов намного более актуальными являются доказательства с помощью интерактивных средств. Такие доказательства (или наброски, используемые системой для создания полных доказательств) прочитываются, по меньшей мере, в момент их написания. В области интерактивных средств для построения доказательств сложилось два основных подхода [Wiedijk F., 2008], определяемых «стилем» работы с доказательствами по аналогии со «стилями» программирования: (1) процедурный (*Coq, HOL Light, Isabelle*), (2) декларативный (*Isabelle, Mizar*). При декларативном подходе пользователь записывает само доказательство при использовании специального языка, однако из-за того, что приходится прописывать каждый шаг, доказательство оказывается похожим скорее на исходный код программы, чем на обычное математическое доказательство. При процедурном подходе пользователь «подсказывает» системе, как следует выполнять построение доказательства при помощи специального языка тактик, само же доказательство строится уже не пользователем, а системой.

Вокруг некоторых программных средств сложились довольно обширные сообщества. К примеру, у сообщества *Coq* имеется своя библиотека формализованных доказательств[10], у сообщества *Mizar* — свой журнал формализованной математики (Formalized Mathematics) и обширная библиотека формализованных доказательств[11], у сообщества Isabelle также имеется собственный журнал формализованной математики (The Archive of Formal Proofs), который одновременно служит и библиотекой формализованных доказательств. Для подачи статей в журналы формализованной математики требуется соблюсти специфические для каждой отдельной системы правила, однако никакого внешнего рецензирования не требуется, поскольку всю проверку доказательства осуществляет вычислительная машина, редактору же остается лишь проверить взаимное соответствие названия статьи, аннотации и формулировки основного результата.

III. Проект QED

Изложенное вполне согласуется с «Манифестом QED» [The QED Manifesto, 1994], анонимно опубликованным группой исследователей в 1994 г. Этот манифест[12] призывает к тотальной формализации и компьютеризации математики с целью решения (обсуждавшихся

[10] Coq Package Index. URL: https://coq.inria.fr/opam/www/ (accessed: 05.10.2020).

[11] Mizar Mathematical Library. URL: http://mizar.uwb.edu.pl/library/ (accessed: 05.10.2020).

[12] Подробное рассмотрение манифеста в контексте распределенной концепции знания и коммуникации в математическом сообществе см. в уже цитированной статье В.А. Шапошникова.

ранее в настоящей статье) проблем сложности, а также сохранения математической культуры и улучшения математического образования[13]. Считается, что одним из основных создателей манифеста выступил Р. Бойер, упоминавшийся ранее в контексте системы Nqthm.

Предполагалось, что проект QED должен быть построен на «корневой логике», т.е. при допущении максимального уровня абстрактности логического ядра, которое может быть легко «дополнено» для работы как с классическими, так и с конструктивистскими и другими «стилями» доказательств. Система QED должна быть международным общественным достоянием, а ее успех должен состоять не в достижении «недостижимого» совершенства, а в том, чтобы позволить исследователям строить доказательства более точным образом. В конце концов ошибки неизбежны и в математике, но следует стремиться к их обнаружению и исправлению. Следовательно, основание QED должно быть сравнительно небольшим (предлагается ограничиться двумя страницами математического текста) и оно должно поддерживать возможность независимой реализации программы проверки. Однако следует помнить, что нет такого логического метода, который бы гарантировал, что формула «выражает» в точности то, что хочет человек, ее написавший.

Следует признать, что, несмотря на свое бурное развитие, тотально формализованная математики так и не вышла за пределы достаточно узкого сообщества. Причины [Wiedijk F., 2007] этого связываются с отсутствием согласия между различными исследователями по вопросу выбора «корневой логики», а также существованием слишком большого числа конкурирующих систем, сообщества вокруг которых не стремятся к унификации и объединению усилий. По сути, на 2007 г. существовало три больших проекта: Mizar, семейство HOL и Coq. Каждый из этих проектов предполагает собственный подход как к выбору «корневой логики», так и к выбору «стиля» записи доказательств. Ожидаемо, что у каждого из этих трех больших проектов имеются как свои «сильные», так и «слабые» стороны, а также более предпочтительные области применения. Так, анализ более удобным образом формализуется с помощью HOL и Coq, для абстрактной алгебры больше подходят Mizar и Coq, для теории категорий — Coq, а для теории множеств — Mizar. К сожалению, ни один из указанных проектов не решил проблему интеграции работ множества людей в единое целое.

Помимо чисто технических трудностей проект перехода к тотально формализованной и компьютеризированной математике сталкивается с рядом социальных, политических и экономических проблем. В частности, формализованная математики в том виде, в каком она практикуется в рамках любого из указанных выше проектов, чрезвычайно сильно отличается от привычной неформальной математики, требует полной экспликации в формальном виде каждого доказательства. Последнее просто не соответствует обычной математической практике, предполагающей предъявление лишь *наброска* доказательства для закрепления результата. Практически любой математический результат зависит от множества других математических результатов, которые используются в его доказательстве в качестве лемм. Таким образом, полная экспликация доказательства в формальном виде потребует чрезмерных усилий при относительной бедности библиотек формальной математики (по сравнению с общей «библиотекой» неформального математического знания). В связи с этим проект QED предлагается [Weiss I., 2016] реформировать в сторону отказа от тотальной формализации в пользу ограниченной формализации, обеспечивающей нормальную коммуникацию математического знания.

Представляется, однако, что затруднения в реализации проекта QED могут быть обусловлены кризисом традиционного подхода к основаниям математики (поиски «корневой логики») и разрешение этого кризиса может привести к обновлению всего здания математической науки, а также к переопределению места логики в основаниях. Некоторые наиболее перспективные современные подходы к основаниям математики будут рассмотрены в последней части настоящей статьи.

[13] Это предложение вряд ли можно назвать новаторским. Например, Дж. Пеано и коллектив французских математиков, публиковавшихся под псевдонимом Н. Бурбаки, предлагали использовать и фактически использовали формальные методы в математическом образовании.

IV. Человеческое понимание компьютерных доказательств

Эпистемологические затруднения [Целищев В.В., 2006; Целищев В.В., Хлебалин А.В., 2020; Хлебалин А.В., 2020], связанные с компьютерными доказательствами и касающиеся проблем человеческого понимания, проистекают в первую очередь из-за невозможности (или крайней затруднительности) их обозреть. Традиционное понятие доказательства [Tymoczko T., 1979, p. 59] предполагает, что оно (1) является средством достижения убежденности, (2) является обозримой конструкцией и (3) может быть формализовано. Как было видно выше, проблема обозримости доказательств актуальна и для математических результатов, полученных «обычными» математиками, однако для компьютерных доказательств она еще острее. В силу того что вычислительные машины способны работать только с формализованными доказательствами, которые целиком и полностью записаны в явном виде без исключения некоторых (даже очевидных) шагов, эти доказательства оказываются чрезвычайно объемными. Более того, иногда компьютеры используются для решения сложных в комбинаторном отношении задач, составляющих части некоторого доказательства. Например, это имело место в известном доказательстве теоремы [Appel K., Haken W., 1977; Appel K. et al., 1977] о четырех красках, а также в недавнем доказательстве теоремы [Athreya J.S. et al., 2020] о существовании на додекаэдре всюду прямого замкнутого пути, начинающегося в одной вершине и не проходящего через остальные вершины. Доказательство обеих теорем предполагает конечный (но довольно большой и трудоемкий для человека в силу высокой комбинаторной сложности) перебор различных вариантов. Этот конечный перебор просто находится за пределами вычислительных способностей, ограниченных продолжительностью человеческой жизни.

Поскольку компьютерные доказательства оказываются необозримыми, постольку возникают сомнения в том, насколько обоснованно считать их математическими в традиционном понимании математики как чистой внеэмпирической науки. В этой связи Т. Тимошко [Tymoczko T., 1979] (последователь фаллибилистской философии математики И. Лакатоса) предлагает пересмотр статуса математики с соответствующим пересмотром понятий доказательства и теоремы в духе фаллибилизма и квазиэмпиризма. При таком подходе математика не отличается от любой другой эмпирической науки, а доказательства (в частности, необозримые компьютерные доказательства) оказываются разновидностью экспериментов. Иной вывод делает (вслед за Л. Витгенштейном) С. Шэнкер [Shanker S., 1987], согласно которому доказательства представляют собой грамматические конструкции, определяющие правила употребления математических символов. Соответственно, если правило не может быть «схвачено» (а оно не может быть «схвачено» в случае отсутствия обозримости), то мы не можем научиться употреблять соответствующие математические символы. Последнее служит свидетельством в пользу того, что у нас отсутствует понимание математики в целом либо некоторых ее разделов. Тем не менее невозможность обозреть некоторые доказательства может считаться проявлением исключительно человеческой ограниченности. При таком подходе, предлагаемом, например, П. Теллером [Teller P., 1980], обозримые доказательства являются частью человеческой математики, однако можно помыслить других живых существ, когнитивные способности которых превосходили бы человеческие, их математика будет содержать некоторые необозримые для людей доказательства.

Представляется, что в общем случае необозримость математического доказательства (как компьютерного, так и «традиционного» неформального) представляет собой важную эпистемологическую проблему. Без обозримости убежденность в правильности доказательства оказывается сходной с убежденностью в пророчествах марсианского математика Саймона[14], прозрениях Рамануджана[15] или ответах

[14] Вымышленный математик, который всегда верно отгадывает правильные ответы на математические вопросы, см.: [Tymoczko T., 1979].

[15] Математик-гений начала XX в., утверждавший, что математические истины ему нашептывает во время молитвы или сна богиня Намагири Тхайяр. По некоторым свидетельствам, Рамануджан испытывал определенные трудности с построением доказательств, однако впоследствии довольно большая часть его математических «озарений» была строго доказана другими математиками.

вычислительного «черного» ящика. Математик, доверяющий вычислительной машине, не имея возможности обозреть все произведенное ею доказательство (либо фрагмент доказательства, как в случае с теоремой о четырех красках), вынужден верить в надежность ее работы, в правильность и обоснованность используемого формализма и корректность его реализации в вычислительной машине. Такая вера может быть обоснована в духе релайабилизма, но требует обращения к сложным вариантам понятия надежности, учитывающего указанные выше нюансы. Однако, в силу того что вычислительная машина является физическим устройством, всегда можно допустить существование некоторых неучтенных факторов, влияющих на корректность ее работы, чего вполне достаточно для того, чтобы необозримые доказательства не могли быть классифицированы как чистые априорные доказательства «традиционной» математики.

Рассматривая понятие обозримости математического доказательства, можно вслед за О.Б. Бэсслером [Bassler O.B., 2006] выделить две важные разновидности обозримости: (1) глобальная обозримость, предполагающая общее понимание идеи доказательства и его структуры, и (2) локальная обозримость, касающаяся интуитивного постижения применения правила при переходе от одного элементарного шага доказательства к другому. В целом любое известное на настоящий момент математическое доказательство является глобально обозримым. У слишком длинных доказательств (и, в частности, компьютерных доказательств) отсутствует локальная обозримость. Другими словами, мы понимаем общую идею каждого доказательства, понимаем его структуру, но не способны проследить и понять *каждый* переход от одного элементарного шага к следующему за ним. Связано это с тем, что длинные доказательства содержат слишком больше количество элементарных шагов, чтобы можно было проследить каждый переход от одного шага к другому, а также (в частности, в случае компьютерных доказательств) с большим количеством правил, используемых для таких переходов. Если первая причина достаточно очевидна (выше упоминались доказательства длиной 1000 и более страниц), то вторую причину необходимо проиллюстрировать отдельно.

Доказательство теоремы о четырех красках предполагает выделение неизбежного набора конфигураций карты (страна с двумя соседями, страна с тремя соседями и т.д.) и доказательство редуцируемости любого набора к другому набору с меньшим числом стран, для раскрашивания которого требуется то же число цветов. По сути, компьютерная часть доказательства представляет собой перебор возможных наборов. То есть с помощью вычислительной машины формируются неизбежные наборы конфигураций, а далее демонстрируется их редуцируемость. В окончательном варианте доказательства рассматриваются 1482 конфигурации, для построения которых было использовано около 500 правил. Принципы построения неизбежных конфигураций в общем случае понятны, но обозримость самого процесса их получения, доверенного машине, вызывает определенные сомнения, и немалую роль в этом играет использование столь большого количества правил. Использование такого большого количества правил (трудно представить себе, как обычный математик способен «держать» все их в голове) может иметь две причины. Во-первых, могут использоваться допустимые [Rybakov V.V., 1997] правила (класс правил, относительно которых данное исчисление замкнуто), которые не меняют множества выводимых утверждений, но позволяют сокращать длину вывода. Другими словами, в принципе можно использовать небольшой базовый набор правил, чтобы получить те же теоремы, но доказательства в этом случае будут длиннее, а вычислительной машине потребуется бо́льшее время на их построение и/или проверку. Естественно, в каждом конкретном случае вопрос обозримости доказательства будет представлять собой вопрос выбора между (условно) коротким доказательством и большим набором правил, с одной стороны, и (условно) длинным доказательством и небольшим набором правил — с другой. В общем случае критерий разрешения этого вопроса так, чтобы доказательство обязательно оказывалось обозримым, в настоящее время отсутствует. Во-вторых, описываемая некоторой данной формализованной теорией предметная область может быть достаточно сложной, в связи с чем число примитивных понятий, характеризующих эту предметную область, может быть велико. Соответственно, по-

требуется по меньшей мере по одному правилу на каждое такое понятие. Таким образом, если отсутствуют технические средства, с помощью которых можно было бы для данной предметной области обеспечить достаточный уровень абстракции, то число правил в рамках соответствующей формализации будет большим.

Поскольку набор правил и наличие мощных средств абстрагирования во много зависит от используемой базовой формальной системы, постольку представляется, что выбор подходящего подхода к основаниями математики позволит (хотя бы частично) разрешить проблему обозримости. В конце предыдущей части указывалось, что трудности реализации проекта QED во многом связаны с кризисной ситуацией в основаниях математики. В этой связи целесообразно обратиться к современным и наиболее перспективным разработкам в этой области.

V. Обзор современного теоретико-типового подхода к основаниям математики

Современные варианты теории типов представляют собой достаточно выразительные формализмы, сочетающие в себе мощное понятие равенства и конструктивный подход, позволяющий легко использовать их при построении интерактивных средств для доказательства теорем. В частности, гомотопическая теория типов (далее — ГТТ) опирается на аксиому универсальности, предложенную В. Воеводским[16]. Из-за этой аксиомы ГТТ в некотором смысле получает неконструктивный характер, однако другие варианты теории типов (например, кубическая теория типов) позволяют вывести эквивалентное ее утверждение в качестве теоремы, что дает конструктивную интерпретацию аксиомы универсальности. Данная аксиома может быть прочитана следующим образом: равенство двух типов эквивалентно эквиваленции этих типов. Необходимо указать, что эквиваленция понимается здесь весьма и весьма широко: как логическая, категорическая, гомотопическая и т.д. Равенство в ГТТ соответствует объекту, представляющему собой путь в пространстве путей. В отличие от теории типов П. Мартин-Лёфа в ГТТ высказываниям соответствуют лишь типы с не более чем одним термом. Эти типы относятся к -1 уровню иерархии типов, который может пониматься как уровень «чисто логического». Термы, подпадающие под типы более высоких уровней, представляют собой *разные* доказательства (или «компоненты» истинностного значения), от которых можно абстрагироваться, сведя любой тип к типу-высказыванию (сведя его к -1 уровню). В этой связи получается, что математика не сводится к чистой логике, как это предполагалось сторонниками логицизма и неологицизма, однако логика все же определяет «логическую» структуру математического знания, которая сохраняется на любом уровне иерархии типов.

Неоспоримым преимуществом такого подхода к основаниям математики является более «естественное» (по сравнению с формализациями с помощью, например, теории множеств) представление математических понятий, а также экстенсиональность для высказываний, функций и типов. Последняя особенность представляет собой более строгий вариант принципа тождественности неразличимых Г.В. Лейбница. В некотором смысле можно говорить о неразличимости изоморфных объектов. Другими словами, в ГТТ и аналогичных формализмах можно обращаться с изоморфными объектами как с равными. Безусловно, с чисто теоретической точки зрения это не совсем верно, однако этот принцип довольно широко используется математиками на практике. Благодаря тому что в теории типов (и это сохраняется в ГТТ и родственных системах) определимыми являются только инвариантные свойства математических объектов, при формализации математических теорий можно легко избавиться от громоздких конструкций с классами эквивалентности для инвариантов, что значительно сокращает длину доказательств.

ГТТ как подход к основаниям математики предполагает возрождение интереса к структуралистскому подходу [Ламберов Л.Д., 2018b; Доманов О.А., 2017] и геометризму [Родин А.В., 2014] в духе Г.В. Лейбница. В рамках ГТТ логическая форма обладает геометрической природой (типы понимаются как топологические пространства, объекты — как точки в пространстве, доказательства равенства объектов — как доказательство существования пути из одной точки в другую и т.д.).

[16] Введение в ГТТ см.: [Homotopy Type Theory..., 2013].

Геометризм[17] оснований математики вкупе с выразительностью ГТТ как формальной теории способствуют большей «прозрачности» доказательств. Соответственно, помимо локальной и глобальной обозримости обоснованно выделить «мезоскопическую» [Rodin A., 2019; Родин А.В., 2014] обозримость. Таким образом, ГТТ и родственные системы при их сравнении с традиционной «чистой» логикой и теорией множеств представляют собой более мощный инструмент для анализа доказательств и позволяют получать более близкие к традиционным математическим рассуждениям и обычной математической интуиции [Целищев В.В., 2007] компьютерные доказательства.

Выражение признательности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-011-00301.

Acknowledgements

The research was carried out with the financial support of the RFBR, project No 19-011-00301.

Список литературы

Доманов О.А. Структурализм и конструктивизм в гуманитарных науках и математике // Сибирский философский журнал. 2017. Т. 15, № 3. С. 39–50. DOI: https://doi.org/10.25205/2541-7517-2017-15-3-39-50

Ламберов Л.Д. Основания математики: теория множеств vs. теория типов // Философия науки. 2017. № 1. С. 41–60. DOI: https://doi.org/10.15372/ps20170104

Ламберов Л.Д. Понятие доказательства в контексте теоретико-типового подхода, I: доказательство программ // Вестник Томского государственного университета. Философия. Социология. Политология. 2018. № 46. С. 49–57. DOI: https://doi.org/10.17223/1998863x/46/6

Ламберов Л.Д. Понятие доказательства в контексте теоретико-типового подхода, II: доказательства теорем // Вестник Томского государственного университета. Философия. Социология. Политология. 2019. № 49. С. 34–41. DOI: https://doi.org/10.17223/1998863x/49/4

Ламберов Л.Д. Понятие доказательства в контексте теоретико-типового подхода, III: доказательства как (некоторые) типы // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 57. С. 25–32. DOI: https://doi.org/10.17223/1998863X/57/3

Ламберов Л.Д. Унивалентность и понятие структуры в философии математики // Сибирский философский журнал. 2018. Т. 16, № 1. С. 20–32. DOI: https://doi.org/10.25205/2541-7517-2018-16-1-20-32

Родин А.В. Делать и показывать // Доказательство: очевидность, достоверность и убедительность в математике / под ред. В.А. Бажанова, А.Н. Кричевца, В.А. Шапошникова. М.: Либроком, 2014. С. 219–255.

Хлебалин А.В. Интерактивное доказательство: верификация и генерирование нового математического знания // Философия науки. 2020. № 1. С. 87–95. DOI: https://doi.org/10.15372/ps20200105

Целищев В.В. Интуиция, финитизм и рекурсивное мышление. Новосибирск: Параллель, 2007. 220 с.

Целищев В.В. Эпистемология математического доказательства. Новосибирск: Параллель, 2006. 212 с.

Целищев В.В., Хлебалин А.В. Формальные средства в математике и концепция понимания // Философия науки. 2020. № 2. С. 45–58. DOI: https://doi.org/10.15372/ps20200204

Шапошников В.А. Распределенное познание и математическая практика в цифровом обществе: от формализации доказательств к пересмотру оснований // Эпистемология и философия науки. 2018. Т. 55, № 4. С. 160–173. DOI: https://doi.org/10.5840/eps201855474

Almgren's Big Regularity Paper: Q-Valued Functions Minimizing Dirichlet's Integral and the Regularity of Area-Minimizing Rectifiable Currents up to Codimension 2 / ed. by V. Scheffer, J.E. Taylor. Singapore: World Scientific, 2000. 972 p. DOI: https://doi.org/10.1142/4253

Appel K., Haken W. Every Planar Map is Four Colorable. I. Discharging // Illinois Journal of Mathematics. 1977. Vol. 21, iss. 3. P. 429–490. DOI: https://doi.org/10.1215/ijm/1256049011

Appel K., Haken W., Koch J. Every Planar Map is Four Colorable. II. Reducibility // Illinois Journal of Mathematics. 1977. Vol. 21, iss. 3. P. 491–567. DOI: https://doi.org/10.1215/ijm/1256049012

Aschbacher M. Highly Complex Proofs and Implications of Such Proofs // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2005. Vol. 363, iss. 1835. P. 2401–2406. DOI: https://doi.org/10.1098/rsta.2005.1655

[17] Можно сказать, что логика «становится частным случаем геометрии» [Lawvere F.W., 1971, p. 329].

Aschbacher M. The Status of the Classification of the Finite Simple Groups // Notices of the American Mathematical Society. 2004. Vol. 51, no. 7. P. 736–740.

Athreya J.S., Aulicino D., Hooper W.P. Platonic Solids and High Genus Covers of Lattice Surfaces // Experimental Mathematics. 2020. URL: https://www.tandfonline.com/doi/full/10.1080/10586458.2020.1712564 (accessed: 07.10.2020). DOI: https://doi.org/10.1080/10586458.2020.1712564

Bassler O.B. The Surveyability of Mathematical Proof: A Historical Perspective // Synthese. 2006. Vol. 148, iss. 1. P. 99–133. DOI: https://doi.org/10.1007/s11229-004-6221-7

Boyer R.S., Kaufmann M., Moore J.S. The Boyer-Moore Theorem Prover and Its Interactive Enhancement // Computers & Mathematics with Applications. 1995. Vol. 29, iss. 2. P. 27–62. DOI: https://doi.org/10.1016/0898-1221(94)00215-7

Church A. A Formulation of the Simple Theory of Types // The Journal of Symbolic Logic. 1940. Vol. 5, iss. 2. P. 56–68. DOI: https://doi.org/10.2307/2266170

Church A. A Set of Postulates for the Foundation of Logic // Annals of Mathematics (2nd Series). 1932. Vol. 33, no. 2. P. 346–366. DOI: https://doi.org/10.2307/1968337

Davies B. Whither Mathematics? // Notices of the American Mathematical Society. 2005. Vol. 52, no. 11. P. 1350–1356.

Davis M. A Computer Program for Presburger's Algorithm // Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966 / ed. by J. Sielmann, G. Wrightson. Berlin; Heidelberg: Springer-Verlag, 1983. P. 41–48. DOI: https://doi.org/10.1007/978-3-642-81952-0_3

Davis M. The Prehistory and Early History of Automated Deduction // Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966 / ed. by J. Sielmann, G. Wrightson. Berlin; Heidelberg: Springer-Verlag, 1983. P. 1–28. DOI: https://doi.org/10.1007/978-3-642-81952-0_1

De Bruijn N. Automath, a Language for Mathematics // Automation of Reasoning. Vol. 2: Classical Papers on Computational Logic, 1967–1970 / ed. by J. Sielmann, G. Wrightson. Berlin; Heidelberg: Springer-Verlag, 1983. P. 159–200. DOI: https://doi.org/10.1007/978-3-642-81955-1_11

Homotopy Type Theory: Univalent Foundations of Mathematics. 2013. URL: https://homotopytypetheory.org/book/ (accessed: 01.11.2020).

Lawvere F.W. Quantifiers and sheaves // Actes du congres international des mathematiciens / ed. by M. Berger, J. Dieudonne et al. Nice: Gauthier-Villars, 1971. Vol. 1. P. 329–334.

Martin-Löf P. Intuitionistic Type Theory. Napoli: Bibliopolis, 1984. 100 p.

Mercer J. Functions of Positive and Negative Type and Their Connection with the Theory of Integral Equations // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 1909. Vol. 209, iss. 441–458. P. 415–446. DOI: https://doi.org/10.1098/rsta.1909.0016

Milner R. LCF: A Way of Doing Proofs with a Machine // Mathematical Foundations of Computer Science 1979. Lecture Notes in Computer Science. Berlin; Heidelberg: Springer, 1979. Vol. 74. P. 146–159. DOI: https://doi.org/10.1007/3-540-09526-8_11

Newel A., Shaw J.C., Simon H.A. Empirical Explorations with the Logic Theory Machine: A Case Study in Heuristics // Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966 // ed. by J. Sielmann, G. Wrightson. Berlin; Heidelberg: Springer-Verlag, 1983. P. 49–73. DOI: https://doi.org/10.1007/978-3-642-81952-0_4

Polanyi M. Personal Knowledge: Towards a Post-Critical Philosophy. Chicago, IL: University of Chicago Press, 1958. 428 p.

Robertson N., Seymour P. Graph Minors. I. Excluding a Forest // Journal of Combinatorial Theory. Series B. 1983. Vol. 35, iss. 1. P. 39–61. DOI: https://doi.org/10.1016/0095-8956(83)90079-5

Robertson N., Seymour P. Graph Minors. XX. Wagner's Conjecture // Journal of Combinatorial Theory. Series B. 2004. Vol. 92, iss. 2. P. 325–357. DOI: https://doi.org/10.1016/j.jctb.2004.08.001

Rodin A. Formal Proof-Verification and Mathematical Intuition: the Case of Univalent Foundations // 16th International Congress on Logic, Methodology and Philosophy of Science and Technology (Prague, August 5–10, 2019): Book of Abstracts. Prague, 2019. P. 418.

Russell B. The Principles of Mathematics. Cambridge, MA: Cambridge University Press, 1903. 534 p.

Shanker S. Wittgenstein and the Turning Point in the Philosophy of Mathematics. Albany: Croom Helm, 1987. 358 p.

Solomon R. The Classification of Finite Simple Groups: A Progress Report // Notices of the American Mathematical Society. 2018. Vol. 65, no. 6. P. 646–651. DOI: https://doi.org/10.1090/noti1689

Studies in Logic and the Foundations of Mathematics. Vol. 136: Admissibility of Logical Inference

Rules / ed. by V.V. Rybakov. Amsterdam: Elsevier Science B.V., 1997. 616 p. DOI: https://doi.org/10.1016/s0049-237x(97)x8001-2

Teller P. Computer Proof // The Journal of Philosophy. 1980. Vol. 77, iss. 12. P. 797–803. DOI: https://doi.org/10.2307/2025805

The QED Manifesto // Automated Deduction – CADE 12 / ed. by A. Bundy. Berlin, Heidelberg: Springer-Verlag, 1994. P. 238–251.

Tymoczko T. The Four-Color Theorem and Its Philosophical Significance // The Journal of Philosophy. 1979. Vol. 76, iss. 2. P. 57–83. DOI: https://doi.org/10.2307/2025976

Weiss I. The QED Manifesto after Two Decades – Version 2.0 // Journal of Software. 2016. Vol. 11, no. 8. P. 803–815. DOI: https://doi.org/10.17706/jsw.11.8.803-815

Wiedijk F. Formal Proof — Getting Started // Notices of the American Mathematical Society. 2008. Vol. 55, no. 11. P. 1408–1414.

Wiedijk F. The QED Manifesto Revisited // Studies in Logic, Grammar and Rhetoric. 2007. Vol. 10, iss. 23. P. 121–133.

Wos L., Henschen L. Automated Theorem Proving, 1965–1970 // Automation of Reasoning. Vol. 2: Classical Papers on Computational Logic, 1967–1970 / ed. by J. Sielmann, G. Wrightson. Berlin; Heidelberg: Springer-Verlag, 1983. P. 1–24. DOI: https://doi.org/10.1007/978-3-642-81955-1_1

Получена: 09.11.2020. Принята к публикации: 21.11.2020

References

Appel, K. and Haken, W. (1977). Every planar map is four colorable. I. Discharging. *Illinois Journal of Mathematics*. Vol. 21, iss. 3, pp. 429–490. DOI: https://doi.org/10.1215/ijm/1256049011

Appel, K., Haken, W. and Koch, J. (1977). Every planar map is four colorable. II. Reducibility. *Illinois Journal of Mathematics*. Vol. 21, iss. 3, pp. 491–567. DOI: https://doi.org/10.1215/ijm/1256049012

Aschbacher, M. (2004). The status of the classification of the finite simple groups. *Notices of the American Mathematical Society*. Vol. 51, no. 7, pp. 736–740.

Aschbacher, M. (2005). Highly complex proofs and implications of such proofs. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. Vol. 363, iss. 1835, pp. 2401–2406. DOI: https://doi.org/10.1098/rsta.2005.1655

Athreya, J.S., Aulicino, D. and Hooper, W.P. (2020). Platonic solids and high genus covers of lattice surfaces. *Experimental Mathematics*. Available at: https://www.tandfonline.com/doi/full/10.1080/10586458.2020.1712564 (accessed 07.10.2020). DOI: https://doi.org/10.1080/10586458.2020.1712564

Bassler, O.B. (2006). The surveyability of mathematical proof: a historical perspective. *Synthese*. Vol. 148, iss. 1, pp. 99–133. DOI: https://doi.org/10.1007/s11229-004-6221-7

Boyer, R.S., Kaufmann, M. and Moore, J.S. (1995). The Boyer-Moore theorem prover and its interactive enhancement. *Computers & Mathematics with Applications*. Vol. 29, iss. 2, pp. 27–62. DOI: https://doi.org/10.1016/0898-1221(94)00215-7

Bundy, A. (ed.) (1994). The QED Manifesto. *Automated Deduction – CADE 12*. Berlin, Heidelberg: Springer-Verlag Publ., pp. 238–251.

Church, A. (1932). A set of postulates for the foundation of logic. *Annals of Mathematics (Second Series)*. Vol. 33, no. 2, pp. 346–366. DOI: https://doi.org/10.2307/1968337

Church, A. (1940). A formulation of the simple theory of types. *The Journal of Symbolic Logic*. Vol. 5, iss. 2, pp. 56–68. DOI: https://doi.org/10.2307/2266170

Davies, B. (2005). Whither mathematics? *Notices of the American Mathematical Society*. Vol. 52, no. 11, pp. 1350–1356.

Davis, M. (1983). A computer program for presburger's algorithm. *Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966*, ed. by J. Sielmann, G. Wrightson. Berlin, Heidelberg: Springer-Verlag Publ., pp. 41–48. DOI: https://doi.org/10.1007/978-3-642-81952-0_3

Davis, M. (1983). The prehistory and early history of automated deduction. *Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966*, ed. by J. Sielmann, G. Wrightson. Berlin, Heidelberg: Springer-Verlag Publ., pp. 1–28. DOI: https://doi.org/10.1007/978-3-642-81952-0_1

De Bruijn, N. (1983). Automath, a language for mathematics. *Automation of Reasoning. Vol. 2: Classical Papers on Computational Logic, 1967–1970*, ed. by J. Sielmann, G.. Wrightson. Berlin, Heidelberg: Springer-Verlag Publ., pp. 159–200. DOI: https://doi.org/10.1007/978-3-642-81955-1_11

Domanov, O.A. (2017). [Structuralism and constructivism in human sciences and mathematics]. *Sibirskiy filosofskiy zhurnal* [Siberian Journal of Philosophy]. Vol. 15, no. 3, pp. 39–50. DOI: https://doi.org/10.25205/2541-7517-2017-15-3-39-50

Homotopy type theory: univalent foundations of mathematics (2013). Available at:

https://homotopytypetheory.org/book/ (accessed 01.11.2020).

Khlebalin, A.V. (2020). [Interactive proof: verification and generation of new mathematical knowledge]. *Filosofiya nauki* [Philosophy of Sciences]. No. 1, pp. 87–95. DOI: https://doi.org/10.15372/ps20200105

Lamberov, L.D. (2017). [Foundations of mathematics: set theory vs. type theory]. *Filosofiya nauki* [Philosophy of Sciences]. No. 1, pp. 41–60. DOI: https://doi.org/10.15372/ps20170104

Lamberov, L.D. (2018). [The concept of proof in the context of a type-theoretic approach, I: proof of computer program correctness]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya* [Tomsk State University Journal of Philosophy, Sociology and Political Science]. No. 46, pp. 49–57. DOI: https://doi.org/10.17223/1998863x/46/6

Lamberov, L.D. (2018). [Univalence and the concept of structure in the philosophy of mathematics]. *Sibirskii filosofskii zhurnal* [Siberian Journal of Philosophy]. Vol. 16, no. 1, pp. 20–32. DOI: https://doi.org/10.25205/2541-7517-2018-16-1-20-32

Lamberov, L.D. (2019). [The concept of proof in the context of type-theoretic approach, II: proofs of theorems]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya* [Tomsk State University Journal of Philosophy, Sociology and Political Science]. No. 49, pp. 34–41. DOI: https://doi.org/10.17223/1998863x/49/4

Lamberov, L.D. (2020). [The concept of proof in the context of type-theoretic approach, III: proofs as (some) types]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya* [Tomsk State University Journal of Philosophy, Sociology and Political Science]. No. 57, pp. 25–32. DOI: https://doi.org/10.17223/1998863X/57/3

Lawvere, F.W. (1971). Quantifiers and sheaves. *Actes du congres international des mathematiciens*, ed. by M. Berger, J. Dieudonne et al. [Proceedings of the International Congress of mathematicians, ed. by M. Berger, J. Dieudonne et al.]. Nice: Gauthier-Villars Publ., vol. 1, pp. 329–334.

Martin-Löf, P. (1984). *Intuitionistic type theory*. Napoli: Bibliopolis Publ., 100 p.

Mercer, J. (1909). Functions of positive and negative type and their connection with the theory of integral equations. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. Vol. 209, iss. 441–458, pp. 415–446. DOI: https://doi.org/10.1098/rsta.1909.0016

Milner, R. (1979). LCF: a way of doing proofs with a machine. *Mathematical Foundations of Computer Science 1979. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Publ., vol. 74, pp. 146–159. DOI: https://doi.org/10.1007/3-540-09526-8_11

Newel, A., Shaw, J.C. and Simon, H.A. (1983). Empirical explorations with the logic theory machine: a case study in heuristics. *Automation of Reasoning. Vol. 1: Classical Papers on Computational Logic, 1957–1966*, ed. by J. Sielmann, G. Wrightson. Berlin, Heidelberg: Springer-Verlag Publ., pp. 49–73. DOI: https://doi.org/10.1007/978-3-642-81952-0_4

Polanyi, M. (1958). *Personal knowledge: towards a post-critical philosophy*. Chicago, IL: University of Chicago Press, 428 p.

Robertson, N. and Seymour, P. (1983). Graph minors. I. Excluding a forest. *Journal of Combinatorial Theory. Series B*. Vol. 35, iss. 1, pp. 39–61. DOI: https://doi.org/10.1016/0095-8956(83)90079-5

Robertson, N. and Seymour, P. (2004). Graph minors. XX. Wagner's conjecture. *Journal of Combinatorial Theory. Series B*. Vol. 92, iss. 2, pp. 325–357. DOI: https://doi.org/10.1016/j.jctb.2004.08.001

Rodin, A.V. (2014). [To do and to show]. *Dokazatel'stvo: ochevidnost', dostovernost' i ubeditel'nost' v matematike, pod red. V.A. Bazhanova, A.N. Krichevts, V.A. Shaposhnikova* [Proof: evidence, certainty, conclusiveness in mathematics, ed. by. V.A. Bazhanov, A.N. Krichevts, V.A. Shaposhnikov]. Moscow: Librokom Publ., pp. 219–255.

Rodin, A. (2019). Formal proof-verification and mathematical intuition: the case of univalent foundations. *16th International Congress on Logic, Methodology and Philosophy of Science and Technology (Prague, August 5–10, 2019): Book of Abstracts*. Prague, p. 418.

Russell, B. (1903). *The principles of mathematics*. Cambridge, MA: Cambridge University Press, 534 p.

Rybakov, V.V. (ed.) (1997). *Studies* in Logic and the Foundations of Mathematics. Vol. 136: Admissibility of Logical Inference Rules. Amsterdam: Elsevier Science Publ., 616 p. DOI: https://doi.org/10.1016/s0049-237x(97)x8001-2

Shanker, S. (1987). *Wittgenstein and the turning point in the philosophy of mathematics*. Albany: Croom Helm Publ., 358 p.

Shaposhnikov, V.A. (2018). [Distributed cognition and mathematical practice in the digital society: from formalized proofs to revisited foundations]. *Epistemologiya i filosofiya nauki* [Epistemology and

Philosophy of Science]. Vol. 55, no. 4, pp. 160–173. DOI: https://doi.org/10.5840/eps201855474

Scheffer, V. and Taylor, J.E. (eds.) (2000). *Almgren's big regularity paper: q-valued functions minimizing dirichlet's integral and the regularity of area-minimizing rectifiable currents up to codimension*. Singapore: World Scientific Publ., 972 p. DOI: https://doi.org/10.1142/4253

Solomon, R. (2018). The classification of finite simple groups: a progress report. *Notices of the American Mathematical Society*. Vol. 65, no. 6, pp. 646–651. DOI: https://doi.org/10.1090/noti1689

Teller, P. (1980). Computer proof. *The Journal of Philosophy*. Vol. 77, iss. 12, pp. 797–803. DOI: https://doi.org/10.2307/2025805

Tselischev, V.V. (2006). *Epistemologiya matematicheskogo dokazatel'stva* [Epistemology of mathematical proof]. Novosibirsk: Parallel' Publ., 212 p.

Tselischev, V.V. (2007). *Intuitsiya, finitizm i rekursivnoe myshlenie* [Intuition, finitism, and human understanding]. Novosibirsk: Parallel' Publ., 220 p.

Tselischev, V.V. and Khlebalin, A.V. (2020). [Formalism in mathematics and conception of understanding]. *Filosofiya nauki* [Philosophy of Sciences]. No. 2, pp. 45–58. DOI: https://doi.org/10.15372/ps20200204

Tymoczko, T. (1979). The four-color theorem and its philosophical significance. *The Journal of Philosophy*. Vol. 76, iss. 2, pp. 57–83. DOI: https://doi.org/10.2307/2025976

Weiss, I. (2016). The QED manifesto after two decades – Version 2.0. *Journal of Software*. Vol. 11, no. 8, pp. 803–815. DOI: https://doi.org/10.17706/jsw.11.8.803-815

Wiedijk, F. (2007). The QED manifesto revisited. *Studies in Logic, Grammar and Rhetoric*. Vol. 10, iss. 23, pp. 121–133.

Wiedijk, F. (2008). Formal proof — getting started. *Notices of the American Mathematical Society*. Vol. 55, no. 11, pp. 1408–1414.

Wos, L. and Henschen, L. (1983). Automated theorem proving, 1965–1970. *Automation of Reasoning. Vol. 2: Classical Papers on Computational Logic, 1967–1970*, ed. by J. Sielmann, G. Wrightson. Berlin, Heidelberg: Springer-Verlag Publ., pp. 1–24. DOI: https://doi.org/10.1007/978-3-642-81955-1_1

Received: 09.11.2020. Accepted: 21.11.2020

Об авторе

Ламберов Лев Дмитриевич
кандидат философских наук, доцент,
доцент кафедры онтологии и теории познания

Уральский федеральный университет
им. первого Президента России Б.Н. Ельцина
620002, Екатеринбург, ул. Мира, 19;
e-mail: lev.lamberov@urfu.ru
ORCID: https://orcid.org/0000-0001-9228-4909
ResearcherID: Q-5183-2016

About the author

Lev D. Lamberov
Ph.D. in Philosophy, Docent,
Associate Professor of the Department
of Ontology and Theory of Knowledge

Ural Federal University named after
the first President of Russia B.N. Yeltsin,
19, Mira st., Ekaterinburg, 620002, Russia;
e-mail: lev.lamberov@urfu.ru
ORCID: https://orcid.org/0000-0001-9228-4909
ResearcherID: Q-5183-2016

Просьба ссылаться на эту статью в русскоязычных источниках следующим образом:
Ламберов Л.Д. Практика компьютерных доказательств и человеческое понимание: эпистемологическая проблематика // Вестник Пермского университета. Философия. Психология. Социология. 2021. Вып. 1. С. 5–19. DOI: 10.17072/2078-7898/2021-1-5-19

For citation:
Lamberov L.D. [Computer proofs practice and human understanding: epistemological issues]. *Vestnik Permskogo universiteta. Filosofia. Psihologia. Sociologia* [Perm University Herald. Philosophy. Psychology. Sociology], 2021, issue 1, pp. 5–19 (in Russian). DOI: 10.17072/2078-7898/2021-1-5-19