Андрей Родин

Компьютерные доказательства в современной математике и проблема верификации знаний.

Практика использования технических средств для счета и измерений - наряду с использованием для этих целей частей собственного тела - уходит своими корнями в эпоху Палеолита. Описанные в научной литературе археологические находки такого рода представляют собой кости животных с нанесенными на них зарубками; древнейшая из таких находок, математическая функция которой считается весьма вероятной, согласно данным радиоуглеродного анализа, имеет возраст 43 тысячи лет. В этом смысле можно сказать, что использование технических средств в математике имеет такую же продолжительную историю, как и сама математика. Если под математикой понимать теоретическую дисциплину, оставляя в стороне до-теоретические практики измерения и счета, то придется признать, что история вычислительной техники многократно превосходит по своей продолжительности историю теоретической математики, которая насчитывает не более 3000 лет.

Рис. 1

Несмотря на этот исторический контекст, так называемые “компьютерные доказательства” в математике на настоящий момент являются относительно новой идеей и практикой, которая пока далека о того, чтобы стать общепризнанной и общеупотребительной. На первый взгляд, идея использования вычислительных устройств для доказательства математических утверждений, кажется беспроблемной. Как, например, самостоятельно убедиться в том, что 123 x 456 = 56088? Для любого человека, который не владеет специальными навыками устного счета, самый доступный способ проверки этого равенства состоит в использовании электронного калькулятора. Допуская возможность ошибки, можно проверить этот результат несколько раз на разных калькуляторах. Нельзя исключить, что даже такая многократная проверка может

не показаться кому-то убедительной. Возможно, во всех используемых сегодня калькуляторах присутствует систематическая ошибка, которая до сих пор не была никем замечена. Возможно, что существует всемирный заговор производителей калькуляторов, который направлен на то, чтобы обмануть потребителей в чьих-либо интересах. Однако такого рода сомнения по крайней мере в практическом отношении не кажутся разумными. Но если это так, какие могут быть основания не доверять компьютерам при доказательстве более сложных математических утверждений?

Чтобы с этим разобраться, полезно снова обратиться к истории. Хотя возможность извлечь практическую пользу из занятий теоретической математикой была многим понятна еще в древние времена и является вполне очевидной сегодня, теоретическая и практическая математика всегда находились в сложных и неоднозначных отношениях. В “Началах” Евклида, составленных около 300-го года до новой эры, в систематической форме представлены достижения теоретической работы нескольких поколений греческих математиков. Однако в этом фундаментальном тексте вообще не представлены вычислительные методы, которые в то же самое время использовались для практических нужд, и о которых сегодня известно по другим источникам. Византийский писатель Стобей (5-й век новой эры) передает следующую легенду. Некто, раздумывая о том, стоит ли ему изучать геометрию, спросил у Евклида, какую из этого можно извлечь пользу. Евклид приказал своему помощнику дать этому посетителю немного денег и отправить его восвояси. Скорее всего эта легенда не имеет под собой никаких фактических исторических оснований. Однако она точно указывает на важную черту теоретической математики. Чтобы успешно изучать теоретическую математику, и тем более чтобы внести свой вклад в эту дисциплину, необходимы мотивации совсем другого рода такие как чистый интерес к решению математических проблем и открытию новых математических истин. Только это обеспечивает успех, который уже впоследствии в некоторых случаях сопровождается успешными практическими применения полученных теоретических знаний. Хотя этот порядок в конкретных исторических условиях может варьироваться, отвлечение (абстракция) от узкой поставленных практических задач является непременным условием успешной теоретической деятельности в математике.

Теоретическая математика на протяжении своего развития постоянно уточняла свои критерии доказательности; это направление исследований остается актуальным и сегодня. У Евклида и его прямых последователей доказательства математических теорем не имеют ничего общего с вычислениями. В трудах математиков исламского средневековья (VIII-XV века новой эры), в память о которых арабские слова “алгебра” и “алгоритм” сегодня используются во всех языках мира, связь между вычислениями и математическими доказательствами уже можно проследить. Используя алгебраические подходы, Рене Декарт в своей “Геометрии” 1637-го года показал, что с помощью символических вычислений можно решать многие геометрические задачи и доказывать соответствующие геометрические теоремы. Общую идею о том, что подходящим образом организованные символические вычисления могут быть использованы для доказательства математических теорем самого разного рода, в явном виде высказал в том же веке математик и философ Готфрид Вильгельм Лейбниц (1646-1716) (Рис. 2).

В первой половине 20-го века эти пионерские идеи Лейбница получили более точную математическую формулировку в трудах Черча, Тьюринга и других исследователей, которых сегодня считают отцами-основателями компьютерной науки и технологии. Хотя сегодня компьютеры используются в самых разных сферах экономики и человеческой жизни, их использование в математических доказательствах, как мы сейчас увидим, до сих пор остается скорее исключением, а не правилом.

Во избежание недоразумений нужно уточнить, что компьютеры используются в современной математике не только для доказательства теорем. Специально разработанные для математиков пакеты программного обеспечения такие как Mathematica и Maple позволяют автоматически решать дифференциальные и алгебраические уравнения, вычислять интегралы и пределы, визуализировать многие математические объекты и построения, и выполнять много других полезных для практической математической работы функций. Однако с традиционной точки зрения такие такого рода программные средства, как и простой калькулятор, могут играть в теоретической математике только вспомогательную роль. Измеряя стороны прямоугольных треугольников и проводя вычислительные манипуляции с результатами этих измерений можно прийти к гипотезе о том, что во всех случаях сумма квадратов

катетов равна квадрату гипотенузы. Но чтобы эта гипотеза стала доказанной геометрической теоремой, нужно отбросить измерительные и вычислительные приборы и провести абстрактное математическое доказательство. Только это позволит убедиться, что теорема Пифагора верна для всех прямоугольных треугольников, а не только для некоторых и не только для большинства таких треугольников, причем верна не только приблизительно, но и точно. Этот простой пример еще раз иллюстрирует истоки традиционного недоверия по отношению к использованию компьютера как инструмента доказательства в теоретической математике.

Поскольку равенство 123 x 456 = 56088 установленное с помощью карманного калькулятора (или любое другое подобное равенство) при желании можно назвать теоремой, а проведенное на калькуляторе вычисление - доказательством этой теоремы, невозможно установить, когда компьютерные доказательства впервые появились в математической практике. Обычно пальму первенства в этой сфере отдают опубликованному в 1976-м году Кеннетом Аппелем (Kenneth Appel) и Вольфгангом Хакеном (Wolfgang Haken) доказательству теоремы о 4-х красках (в дальнейшем Т4К), согласно которой всякую разделенную на односвязные области и расположенную на плоскости карту можно раскрасить 4-мя красками так, чтобы все области имеющие общий участок границы были раскрашены в разные цвета (Рис. 3). Такая догадка была впервые высказана в 1852-м году, и после этого более ста лет не поддавалась ни доказательству, ни опровержению. Аппелю и Хакену удалось свести доказательство Т4К к проверке 1834-х частных случаев, каждый из которых требовал значительных вычислительных усилий. В этой части доказательства Аппель и Хакен использовали компьютер и специально написанный для данной цели код низкого уровня. Таким образом, предложенное Аппелем и Хакеном в 1976-м году доказательство содержало как традиционную часть, в которой излагалась основная идея доказательства, так и вычислительную часть, в которой использовался электронный компьютер. Из-за значительного объема необходимых вычислений эта компьютерная часть не могла быть выполнена вручную отдельным математиком или коллективом математиков. Впоследствии другими исследователями были предложены усовершенствованные версии этого доказательства. Однако все известные на сегодняшний день варианты доказательства Аппеля и Хакена имеют те же самые общие характеристики.

Работа Аппеля и Хакена вызвала неоднозначную реакцию в математическом сообществе и спровоцировала содержательную философскую дискуссию, которая продолжается и сегодня. Томас Тимошко (Thomas Tymoczko) указал на то, что предложенное Аппелем и Хакеном доказательство Т4К не дает достаточного понимания того, *почему* утверждение Т4К истинно. С точки зрения Тимошко, компьютерное доказательство Т4К вполне аналогично физическому эксперименту; в случае математического доказательства роль экспериментальной установки играет компьютер. Хотя воспроизводимые физические эксперименты заслуживают доверия, и их результаты используются для проверки и обоснования физических теорий, экспериментальные свидетельства не имеют такой доказательной силы, которую обычно ожидают от математических доказательств, и могут быть в последствии опровергнуты новыми экспериментами. Тимошко считает, что вместе с широким внедрением компьютерных доказательств в математическую практику математика должна отказаться от своих традиционных претензий на абсолютную строгость и следовать примеру естественных наук. Однако утверждение Тимошко о том, что использование компьютеров в математических доказательствах существенно меняет характер математики, может быть использовано и для обоснования противоположной позиции, которая состоит в том, что использование компьютеров в математических доказательствах является неправомочным.

На мой взгляд, самый тонкий и корректный эпистемологический анализ компьютерных доказательств Т4К был предложен Брэдли Басслером (Bradley Bassler). В отличие от Тимошко и ряда его критиков Басслер не готов отказаться от нормативной идеи о том, что математические доказательства должны обеспечивать прояснение и понимание вопроса, а не только предоставлять свидетельство истинности доказываемого утверждения в виде какой-то непрозрачной формальной процедуры. При этом Басслер замечает, что предложенное Аппелем и Хакеном доказательство Т4К частично удовлетворяет этому эпистемологическому требованию, причем двояким образом. Во-первых, это доказательство содержит традиционную неформальную часть, которая объясняет организацию вычислений в компьютерной части этого доказательства и то, почему результат этих вычислений нужно считать свидетельством истинности Т4К. Во-

вторых, программный код, который использовали Аппель и Хакен, не является полностью непрозрачным: каждый фрагмент этого кода может быть прочитан и интерпретирован человеком. (Это следует хотя бы из того, что этот код писался вручную, а не был сгенерирован другими программными средствами.) Таким образом, мы имеем здесь, с одной стороны, неформальное представление и объяснение общей структуры аргумента, то есть то, что математики обычно называют наброском доказательства, и, с другой стороны, возможность прослеживать и интерпретировать все используемые в данном доказательстве вычислительные процедуры на микроскопическом уровне элементарных логических шагов. Однако при этом в компьютерном доказательстве Т4К полностью отсутствует промежуточный уровень репрезентации, который мог бы позволить понять, каким образом необозримо длинная (для человеческого восприятия и понимания) последовательность элементарных действий выполняемых с помощью электронного вычислительного устройства складывается в ту макроскопическую структуру, которая описана в общих чертах в неформальной (“традиционной”) части доказательства.

Оставляя в стороне академические философские дискуссии, уместно привести социологическое наблюдение сделанное Кеннетом Аппелем во время публичной лекции, в которой он рассказывал результаты широкой публике. Согласно Аппелю, его аудитория разделилась на две части по возрастному признаку: слушатели старше 40 не могли поверить в то, что компьютерное доказательство может быть корректным, а слушатели младше 40 не могли поверить в то, что произведенное вручную вычисление длиной более 1000 страниц может не содержать ошибок. Интересно заметить, что хотя рассказ Аппеля относится к 1977 году, сегодня мы наблюдаем подобную корреляцию между возрастом аудитории и ее доверием к компьютерам. Если прогресс компьютерной техники действительно мало влияет на описанную Аппелем социологическую ситуацию, она нуждается в каком-то другом объяснении. Возможно, дело тут в том, что молодые люди как правило более склонны доверять новым техническим решениям и меньше доверять историческому опыту старших поколений совершенно независимо от уровня технологического развития.

Другим широко обсуждаемым примером компьютерного доказательство является

опубликованное в 2017-м году формальное доказательство гипотезы Кеплера. Согласно этой гипотезе, которую Иоган Кеплер выдвинул в 1611 году в трактате “О шестиугольных снежинках”, стандартная упаковка шаров одинакового размера в виде “пирамидок” (Рис. 4) является оптимальной по плотности в том смысле, что она при естественных общих предположениях позволяет упаковать максимальное количество шаров на единицу объема. Доказательство это предположения без дополнительных условий оказалось более сложной задачей, чем первоначально ожидалось. В настоящее время эту гипотезу следует, по всей видимости, считать доказанной несмотря на то, что опубликованное в 2003 году Томасом Халесом (Thomas Hales) доказательство этой гипотезы по-прежнему вызывает сомнения у ряда математиков. Возможно, что именно по этой причине это утверждение продолжают называть гипотезой, а не теоремой. Как и доказательство Т4К, предложенное Халесом доказательство гипотезы Кеплера содержит компьютерную часть, которая остается эпистемически непрозрачной. В 2017-м году Халес опубликовал полностью формализованную версию своего доказательства, которое допускает полную компьютерную проверку. Эта публикация представляет самостоятельный интерес как пример полного перевода сложного математического рассуждения на компьютерный язык. Однако нельзя сказать, что она полностью развеяла все сомнения относительно предложенного доказательства гипотезы Кеплера (и относительно самой этой гипотезы). По всей видимости, многие математики просто не готовы принять идею о том, что математического рассуждение, которое не имеет достаточной объяснительной силы, может иметь при этом иметь доказательную силу достаточную для того, чтобы быть полноценным доказательством.

Обратная сторона медали состоит в том, что традиционные математические доказательства, которые не требуют использования технических инструментов помимо карандаша и бумаги, в некоторых случаях оказываются трудно проверямыми и в этом смысле крайне ненадежными. В 2012 году Синъити Мотидзуки (Shinichi Mochizuki) объявил о доказательстве им арифметической гипотезы, которую принято называть ABC-гипотезой, и опубликовал в виде нескольких препринтов оригинальную математическую теорию, в которой ABC-гипотеза является одним из следствий. На сегодняшний день статус этой теории, включая статус предложенного в рамках этой теории доказательства ABC-гипотезы, остается неопределенным: хотя работа

Мотидзуки привлекла внимание экспертов, математическое сообщество за прошедшие годы так и не пришло ни к какому определенному консенсусу по поводу того, следует ли считать теорию Мотидзуки корректной.

Известны также достаточно многочисленные случаи, когда в признанной экспертным сообществом математической работе впоследствии обнаруживаются ошибки, причем по крайней мере часть таких ошибок оказывается неисправимыми - в том смысле, что ранее “доказанное” математическое утверждение оказывается на самом деле ложным. Именно такой случай имел место в профессиональной биографии Владимира Воеводского, которому принадлежит оригинальный подход к созданию компьютерных доказательств в рамках новых оснований математики, которые Воеводский предложил называть “унивалентными” основаниями. Воеводский и другие энтузиасты компьютерных доказательств не без оснований считают, что несмотря на все те трудности, о которых мы упоминали выше, именно формальные компьютерные доказательства могут помочь установить в математике единый стандарт доказательности, который позволит эффективно находить ошибки в сложных доказательствах и надежно отличать корректные доказательства от некорректных. Этот проект не предполагает того, что математика в некотором смысле перестанет быть человеческим занятием и станет уделом автономного искусственного интеллекта (хотя возможности поиска доказательств с помощью технологий искусственного интеллекта также рассматривается). Скорее проверку корректности доказательства в этом контексте нужно понимать по аналогии с автоматической проверкой орфографии и грамматики электронного текста, а поиск доказательств - по аналогии с “подсказками”, которые дают уже прочно вошедшие в широкий обиход роботы-помощники. Все, что касается познавательной, прикладной и эстетической ценности данной математической теоремы или теории, остается в ведении человека. Человек освобождает свой интеллект от рутинных задач, включая логическую и вычислительную рутину, и благодаря этому получает возможность использовать свои интеллектуальные ресурсы для решения более творческих задач. По крайней мере именно такое использование компьютеров в математических доказательствах представляется мне разумным и продуктивным.

Существенное препятствие на пути реализации этого проекта состоит в том, что

формализация привычных математических рассуждений стандартными логическими средствами оказывается в большинстве случаев практически нереализуемой в условиях ограниченных вычислительных ресурсов. Использование более специфических методов формализации во многих случаях успешно решает проблему реализуемости, но создает описанную выше ситуацию, при которой формализованное доказательство и вычислительная реализация этого формального доказательства оказывается эпистемически непрозрачными. В этом случае человек не может интерпретировать формальное доказательство в виде содержательного рассуждения даже если он или она при этом полностью доверяет результатам соответствующего машинного вычисления. Предложенные Воеводским унивалентные основания математики решают проблему эпистемической прозрачности компьютерных доказательств по крайней мере в некоторых областях современной математики тесно связанных с теорией гомотопий. Суть этого решения состоит в том, что гомотопическая теория типов, которая является теоретической основой унивалентного подхода, позволяет интерпретировать значительные фрагменты кода в виде пространственных (а именно, гомотопических) конструкций, которые по крайней мере в случае низких размерностей являются хорошо интуитивно представимыми. В предложенных Басслером терминах можно сказать, что гомотопическая пространственная интуиция заполняет разрыв между макроскопическими и микросопическими аспектами формального доказательства, позволяя человеку понять и проследить, каким образом элементарные шаги доказательства складываются в единое целое. Такой подход делает программный код гораздо более похожим на полуформальную символическую нотацию, которой обычно пользуются математики. В качестве наглядной иллюстрации этого подхода на Рис. 5 представлено « накручивающее отображение » (winding map), которое играет важную роль при доказательстве ряда теорем алгебраической топологии, и которое с помощью гомотопической теории типов практически пошагово переводится в компьютерный код.

Дискуссия по поводу компьютерных доказательств в математике показывает, что среди математиков, философов и логиков на сегодняшний день не существует консенсуса о том, чем является и чем должно быть математическое доказательство. Существующие формальные модели доказательств, которые математические логики активно и плодотворно изучают в течении последних десятилетий, на дают на этот вопрос

однозначного ответа, поскольку изучение математических свойств этих моделей ничего не говорит о том, насколько они адекватно представляют те рассуждения и конструкции, которые называют доказательствами математики работающие за пределами той относительно узкой области исследований, которую принято называть математической логикой и основаниями математики. Существует значительный разрыв между стандартным понятием формального доказательства в математической логике и неформальным понятием о доказательстве, которое в различных вариантах используется в обычной математической практике. Преодоление этого разрыва на теоретическом уровне является важным необходимым условием для широкого использования компьютерных доказательств в практике теоретических и прикладных математических исследований.

В заключение я хотел бы заметить, что проблема компьютерных доказательств в математике не является изолированной: аналогичные проблемы возникают во многих областях искусственного интеллекта и его приложений, особенно в той его части, которую в компьютерной науке принято называть представлением знаний и рассуждений. Современные электронные коммуникации делают доступными для рядового пользователя огромные массивы информации самого разного рода; однако проверка (верификация) доступной информации, которая необходима для того, чтобы полученную информацию можно было считать знаниями, в настоящее время представляет собой сложную задачу, для которой не существует стандартных решений. Хотя в последние годы были развиты некоторые технологические подходы направленные на решение этой проблемы, такие как технология блок-чейна, до сих пор отсутствует общепризнанная теоретическая основа для решения проблемы верификации и обоснования знаний, которая имеет очевидное практическое значение. Можно надеятся, что как это раньше часто случалось в истории, математика снова сыграет роль исследовательской площадки, на которой отрабатываются новые идеи имеющие важные приложения далеко за пределами этой академической дисциплины.

Подписи к рисункам:

Рис. 1: кость волка с нанесенными насечками для счета, найденная на стоянке человека

эпохи Верхнего Палеолита в местечке Дольни Вестонице (Чехия); возраст находки - около 30 тысяч лет.

Рис. 2: титульная страница работы Лейбница 1666-го года « Искусство комбинаторики », которая послужила автору отправной точкой для развития его идей о возможной роли вычислений в логике и математике.

Рис. 3: карта субъектов Российской Федерации, раскрашенная в 4 цвета

Рис. 4: упаковка шаров максимальной плотности

Рис. 5: накручивающее отображение в алгебраической топологии