Модуль 6.4. Компьютерные доказательства

Заслуживают отдельного рассмотрения доказательства с помощью компьютера. Но прежде чем говорить о компьютерных доказательствах, рассмотрим некоторые вопросы применения компьютеров в математике.

История математики до компьютерной эры содержит много примеров трудоемких вычислений. Некоторые вычисления сводились к сложным и громоздким преобразованиям формул, другие вычисления использовали небольшие формулы, но требовали выполнения операций с большим количеством цифр в числах.

Великий Леонард Эйлер был непревзойдённым мастером формальных выкладок и преобразований, в его трудах многие математические формулы и символика получили современный вид (например, ему принадлежат обозначения для e и π). Наглядными примерами мастерства Эйлера служат его вычисление суммы обратных квадратов и получение необычайной формулы, связывающей суммы делителей натуральных чисел [1, с. 40–43, 112–122].

В XIX веке очень много вычислений было проделано в астрономии. Например, французский математик Урбен Леверье проводил громоздкие расчеты орбиты Нептуна, основанные на аналитических вычислениях возмущенной орбиты Урана (что и позволило открыть Нептун).

Впечатляющие вычисления с карандашом и бумагой проделал французский астроном Чарльз-Евгений Делоне для вычисления орбиты Луны. Он вывел около 40 000 формул. На их вывод потребовалось 10 лет и еще 10 лет ушло на проверку формул. Окончательная формула занимала 128 страниц его книги с результатами работы. Проверка его аналитических преобразований было проведена двумя американскими математиками с помощью компьютера в 70-е годы XX века. Компьютеру потребовалось двое суток работы.

Большие усилия тратили математики на определение числа π, вручную вычисляя большое количество цифр. Так, например, наилучший результат к концу XIX века был получен англичанином Вильямом Шенксом. Он потратил 15 лет для того, чтобы вычислить 707 цифр, хотя из-за ошибки только первые 527 были верными. Он использовал формулу Мэчина (Johm Machin, 1680–1751 гг.):

$$\frac{\pi}{4} = 4\operatorname{arctg}\frac{1}{5} - \operatorname{arctg}\frac{1}{239}.$$

Ошибку Шенкса обнаружил в 1944 году Фергюсон (D. E. Ferguson); он считал по формуле, подобной формуле Мэчина,

$$\frac{\pi}{4} = 3\operatorname{arctg}\frac{1}{4} + \operatorname{arctg}\frac{1}{20} + \operatorname{arctg}\frac{1}{1985}$$

на настольном механическом калькуляторе.

В начале 50-х годов стали появляться первые программы, производящие частично аналитические вычисления. В 1951 году с помощью компьютера EDSAC 1 было открыто наибольшее известное простое число $180(2^{127} - 1)^2 + 1$ с 79 десятичными цифрами. В 1952 году математики Эмиль Артин и Джон фон Нейман проделали большие вычисления, связанные с эллиптическими кривыми, на компьютере MANIAC. В 1953 году было показано, как алгоритмы в теории групп могут быть реализованы на компьютере.

В 60-х годах XX века стали создаваться первые системы компьютерной алгебры. Система компьютерной алгебры (computer algebra system) — программа для выполнения символьных (математических) вычислений. Основная определяющая функциональность таких систем — это операции с выражениями в символьной форме.

Первые системы были ограничены по своим возможностям и предназначались для какой-то отдельной области математики. Системы компьютерной алгебры общего назначения (универсальные) — это те, в которых реализованы основные математические алгоритмы и есть возможность пользователю самому создать новые алгоритмы на языке программирования системы.

В настоящее время применяется несколько систем компьютерной алгебры общего назначения. Отметим одну из них.

Mathematica — система компьютерной алгебры, используется во многих научных, инженерных, математических и вычислительных областях. Система была задумана Стивеном Вольфрамом (физик, математик и программист) и в дальнейшем разработана в компании Wolfram Research (Шампейн, штат Иллинойс, США). Начало разработки — 1986 г.; первая версия — 1988 г.; последняя 10-я версия — 2014 г. [2].

Применение Mathematica позволяет эффективно вычислять математические объекты, что проливает свет на используемые математические понятия. Причем использование Mathematica не требует глубоких знаний программирования. Только человек, по роду своей деятельности имеющий дело с математическими вычислениями, глубоко понимающий их специфику и потребности, мог создать подобный программный продукт.

Пример 1

В параграфе 6.1 главы 6, пример 4, мы рассматривали задачу об определении числа R_n областей, образуемых $n(n-1)/2$ хордами, которые соединяют n фиксированных точек на окружности, при предположении, что никакие три хорды не пересекаются внутри круга. Эмпирически были установлены значения R_n для $n = 1, 2, \ldots, 6$ — это числа 1, 2, 4, 8, 16, 31. Mathematica может определить закономерность этой последовательности:

```
FindSequenceFunction[{1, 2, 4, 8, 16, 31}, n]
```

$$\frac{1}{24}\cdot\left(24 - 18n + 23n^2 - 6n^3 + n^4\right).$$

В настоящее время развивается экспериментальная математика: открытие новых математических закономерностей путем компьютерной обработки большого числа примеров. Такой подход не столь убедителен, как короткое доказательство, но может быть убедительнее длинного, сложного доказательства и в некоторых случаях вполне приемлем. В прошлом данную концепцию отстаивали и Дьердь Пойа [1, 3], и Лакатос[1] [4], убежденные сторонники эвристических методов и квазиэмпирической природы математики.

[1] Имре Лакатос (1922–1974 гг.) — английский философ венгерского происхождения.

Экспериментальной математике посвящены книги [5, 6]. Методы экспериментальной математики в естественно-научных дисциплинах, в первую очередь в физике, применяются и обосновываются в книге «Новый вид науки» Стивена Вольфрама [7].

Компьютеры иногда позволяют получить неформальные аргументы в пользу того или иного предположения, а иногда, наоборот, опровергнуть казавшиеся правдоподобными гипотезы. Компьютерные вычисления также поставляют первичную информацию, позволяющую обнаруживать новые свойства изучаемых объектов и выдвинуть новые гипотезы.

Можно ли компьютер использовать более существенным образом, а именно полностью поручить ему весь процесс доказательства математического результата?

Аксиоматический метод открывает для этого некоторые возможности. Формальное доказательство, в конечном счете, есть последовательность формул, получаемых из аксиом по чисто синтаксическим правилам. Поэтому в принципе для этого можно использовать компьютер. Но большинство полезных математических теорий являются неразрешимыми, т. е. для таких теорий не существует алгоритма, который нашел бы доказательство для теоремы. Что компьютер может — это постепенно в результате процесса вычисления порождать всё новые утверждения, выводимые в данной формальной системе, и этот процесс потенциально никогда не заканчивается. Так как мы не можем заранее знать, встретится или нет в этом перечислении интересующий нас результат, мы не можем рассчитывать и на построение его формального доказательства за конечное время.

Тем не менее некоторые рутинные части повседневной работы математиков очень хотелось бы отдать компьютеру. Но вот то, как это сделать, представляет собой значительную техническую проблему, которая связана не только с развитием математики и исследованиями логических теорий, но также и с развитием определенных компьютерных технологий.

Приблизительно лет пятнадцать-двадцать назад развитие компьютерных технологий достигло такого уровня, когда стало возможно всерьез надеяться на создание систем, которые действительно могли бы помочь работе математика при построении и проверке математических доказательств, то есть фактически взять на себя часть его интеллектуальной работы. На данный момент эта область очень быстро развивается, и существует больше десятка различных систем, предназначенных для автоматического и полуавтоматического, то есть интерактивного, доказательства теорем. Для этих систем появилось специфическое название theorem prover (система поиска вывода, «прувер») [8].

Пруверы делятся на два класса: автоматические (automated theorem prover), которые ищут доказательства совершенно независимо от человека, и интерактивные (proof-assistant = interactive theorem prover), которые взаимодействуют с человеком; он помогает компьютеру находить эти доказательства. Интерактивные системы наиболее перспективны для формализации реальных математических доказательств. На основе этих систем были уже получены полностью формализованные доказательства целого ряда знаменитых математических результатов.

Пример 2

Теорема Жордана о кривой. Если J — простая замкнутая кривая в $\mathbf{R}^2$, то $\mathbf{R}^2 \setminus J$ имеет две компоненты («внутреннюю» и «внешнюю») с J в качестве общей границы [9].

В 2005 году были независимо созданы два формальных доказательства этой теоремы с помощью пруверов HOL Light и Mizar [10].

Пример 3

Теорема Гёделя о неполноте (см. главу 2, параграф 2.3). Формализованные доказательства этой теоремы были созданы в 1986 году с помощью системы Nqthm [11] и в 2003 году с помощью системы Coq [12].

Пример 4

Теорема о распределении простых чисел [13]. Было формализовано два известных доказательства этой теоремы: в 2005 г. с помощью прувера Isabelle и в 2009 г. с помощью прувера HOL Light [14].

В предыдущих примерах были получены компьютерные доказательства теорем, для которых были уже известны неформальные доказательства. Но компьютеры уже применяются и там, где без них не удается провести доказательства. Расскажем об первом крупном результате, для доказательства которого был применен компьютер.

Теорема о четырех красках

Что такое теорема о четырех красках? Она долгое время была недоказанной математической гипотезой и состояла в том, что каждую карту на плоскости можно раскрасить правильным образом в четыре цвета. «Правильным образом» — это означает, что разные страны на этой карте, если они имеют общий участок границы, должны быть покрашены в разные цвета. Если исключить некоторые патологические ситуации, то хорошие карты на плоскости в соответствии с этой теоремой о четырех красках всегда можно раскрасить в четыре цвета.

Впервые эту гипотезу высказал один любитель математики по фамилии Гутри (Francis Guthrie) в 1852 г. Первые доказательства были предложены Кемпе (Alfred Kempe) в 1879 г. и Томасом (Peter Thomas) в 1880 г. Через 10 лет были найдены ошибки в обоих доказательствах.

Эта известная математическая гипотеза оставалась недоказанной в течение более ста лет. Первое доказательство этой гипотезы было получено с помощью компьютеров американскими математиками Аппелем и Хакеном в 1976 г. [15].

Аппель и Хакен свели доказательство этого результата к перебору более 1476 различных графов и проверки для них некоторого условия на компьютере.

Само сведение к более тысячи случаев было далеко не тривиальным и в общем занимало 400 страниц, т. е. это был очень сложный математический результат, сопровождаемый еще сложным компьютерным перебором, потребовавшим 1000 часов машинного времени.

Как математическое сообщество отнеслось к такому доказательству? Согласно традиционным представлениям, прочно утвердившимся в XX веке, смысл опубликованного доказательства некоторой задачи заключается в том, чтобы каждый математик мог прочесть доказательство, оценить его обоснованность, если нужно — проверить доказательство, высказать свои сомнения и возражения, если они у него есть. Только после того как опубликованное доказательство прошло подобное испытание среди математического сообщества, оно считается окончательно признанным.

Не все математики признали теорему о четырех красках доказанной, как раз из-за использования компьютера. Возражения были следующего рода.

Как найти ошибку в доказательстве, проведенном компьютером? Как можно понять такое доказательство, оценить его смысл и те связи, которые оно выявляет между различными сторонами исследуемой математической модели? Разобраться в деталях чужой сложной программы практически невозможно. Компьютеру придется просто доверять.

Во-первых, компьютер мог дать сбой при вычислениях. Даже если результат проверен несколько раз, это лишь повышает вероятность правильности доказательства, но не сделает его абсолютно надежным.

Во-вторых, в процессоре и вспомогательных программах (компиляторе, библиотеках и т. п.) могут содержаться (и даже наверняка содержатся) ошибки и невозможно полностью исключить их влияние на правильность доказательства.

И, наконец, самое главное: программа, которая была написана для поиска или проверки доказательства, тоже может содержать ошибки. Строго математически убедиться в том, что она в полной мере соответствует спецификации, настолько же сложно, как и проверить вручную выполненное с ее помощью доказательство (а возможно, и сложнее).

И проблемы с этим доказательством действительно начались, но они оказались не в компьютерной части, а в человеческой. В доказательстве были найдены недочеты. В начале 1980-х годов Ульрих Шмидт исследовал доказательство Аппеля и Хакена и обнаружил пропуски в математической части доказательства.

В 1989 году Аппель и Хакен напечатали дополненное и исправленное доказательство теоремы [16]. Все обнаруженные Шмидтом пропуски вариантов были устранены, были исправлены и прочие ошибки, найденные другими математиками. К доказательству был приложен полный текст программы.

Вслед за этим известные специалисты по теории графов Робертсон, Сандерс, Сеймур и Томас, упростили доказательство Аппеля и Хакена и свели эту задачу к перебору 633 случаев, причем ими был найден более эффективный по времени

алгоритм проверки условия [17]. Тем не менее без помощи компьютера добиться решения этой проблемы не удавалось.

И по-прежнему, поскольку компьютер участвовал в этом процессе, у математиков не было доверия к полученному решению. После этого за дело взялись специалисты по формальной математике, потому что было понятно, что здесь как раз тот случай, когда построение полностью формализованного и проверенного (как говорят в таких случаях, «верифицированного») доказательства теоремы может спасти положение и убедить всех в ее корректности. А такую верификацию можно также было сделать только с помощью компьютера.

В 2004 году группа французских ученых под руководством Жоржа Гонтье полностью формализовала с помощью системы интерактивного поиска вывода Coq компьютерную часть на основе доказательства Робертсона и его соавторов. Работа включает как верификацию содержательного сведения, так и компьютерного перебора. Фактически была написана верифицированная в Coq программа перебора (и не нужно было вводить 633 случая от руки) [18].

Прежде чем обсудить надежность компьютерного доказательства, остановимся на надежности человеческого доказательства. Современная математика переживает кризис переусложненности: доказательства стали настолько длинными и сложными, что ни один ученый не взял бы на себя смелость однозначно подтвердить или оспорить их правильность. Например, доказательство двух гипотез Бернсайда из теории конечных групп занимает около пятисот страниц каждое. Понятно, что такой длины сложный текст, конечно, может содержать ошибки.

Человек может прочитать чужое доказательство и проверить, правильное оно или нет. Но если вы читаете чужое достаточно длинное доказательство и в нем есть ошибка, то есть все шансы, что вы ее не заметите. Почему? В первую очередь потому, что раз сам автор доказательства сделал эту ошибку — значит, она психологически обоснована. То есть он не просто так ее сделал, по случайности — это в принципе такое место, где типичный человек может сделать такую ошибку. Значит, и вы можете сделать ту же самую ошибку, читая это место и соответственно ее не заметив.

И вот с этой проблемой — найти ошибку в записанном людьми математическом тексте, — становится все труднее справиться, а иногда и вообще невозможно — это серьезная проблема современной математики.

Насколько надежны компьютерные доказательства? Л. Беклемишев[1] считает, что достаточно надежны. Приведем его аргументы.

1. Степень надежности зависит от прувера, его интерфейса и внутренней архитектуры. Абсолютной надежности (по целому ряду не зависящих друг от друга причин) не гарантирует ни один прувер. Несмотря на это, в целом компьютерные доказательства намного надёжнее всего остального.
2. Идеальное техническое решение основывается на принципе де Брейна (de Bruijn), который состоит в следующем.
    - В основе прувера лежит логическое ядро — формальная аксиоматическая система, в которой записываются логические выводы. Логиче-

[1] Лев Дмитриевич Беклемишев (р. 1967 г.) — российский математик, доктор физико-математических наук. Имеет работы в области математической логики.

ское ядро должно быть обозримым — достаточно малым и простым. Например, аксиоматика Пеано и Цермело—Френкеля удовлетворяет этому условию.

- Прувер — который в принципе может быть сколь угодно сложной системой, — в результате работы конструирует явный формальный вывод в языке своего ядра.
- Верификатор (независимо от прувера) проверяет корректность данного вывода на соответствие правилам ядра.
- Простота ядра гарантирует простоту верификатора. Более того, каждый желающий может сам написать свой собственный верификатор и убедиться в корректности каждого конкретного формального доказательства.

3. Надежность доказательства определяется только надежностью ядра и верификатора. Остальные части прувера не влияют на правильность доказательства. Такое построение системы дает лучшую гарантию надежности, чем любые другие методы, в том числе традиционное «ручное» доказательство теорем.

Для формального доказательства теоремы о четырех красках Ж. Гонтье с коллегами верифицировали как содержательную часть доказательства, сведение к перебору, так и формально доказали корректность алгоритма той программы, которая осуществляла перебор. В этом было принципиальное отличие их работы от предыдущих доказательств этой теоремы: компьютерное вычисление было снабжено компьютерным же доказательством его корректности. Конечно, это был успех, потому что формальные верифицированные математические доказательства имеют гораздо большую надежность, чем любое сколько-нибудь объемное доказательство, полученное человеком.

Таким образом, теорему о четырех красках, при всей ее громоздкости, можно считать на данный момент одним из наиболее тщательно проверенных и надежно установленных математических результатов [19].

Список литературы по модулю

[1] Пойа Д. Математика и правдоподобные рассуждения / Д. Пойа. — 3-е изд. — М. : Книжный дом «ЛИБРОКОМ», 2010. — Т. 1, 2. — 464 с.

[2] WolframMathematica [Электронный ресурс]. — URL : http://www.wolfram.com/mathematica/ (дата обращения: 08.05.2015).

[3] Пойа Д. Математическое открытие: Решение задач: основные понятия, изучение и преподавание / Д. Пойа. — 3-е изд. — М. : КомКнига, 2010. — 448 с.

[4] Лакатос И. Доказательства и опровержения: Как доказываются теоремы / И. Лакатос. — 2-е изд. — М. : Изд.-во ЛКИ, 2010. — 152 с.

[5] Bailey D. Mathematics by Experiment: Plausible Reasoning in the 21st Century / D. Bailey. — Wellesley, MA: A K Peters, 2003.

[6] Borwein J. Experimentation in Mathematics / J. Borwein, D. Bailey, R. Gkgensohn. — Wellesley, MA: A K Peters, 2003. — 358 p.

[7] Wolfram S. A New Kind of Science / S. Wolfram. — Champaign, Illinois: Wolfram Media, Inc., 2002. — 1197 p.

[8] Wiedijk F. (ed): The Seventeen Provers of the World // Lecture Notes in Artificial Intelligence. — 2006. — Vol. 3600.

[9] Спеньер Э. Алгебраическая топология / Э. Спеньер. — М. : Мир, 1971. — 680 с.

[10] Hales Thomas C. The Jordan curve theorem, formally and informally // The American Mathematical Mounthly. — 2007. — Vol. 114 (10). — P. 882–894.

[11] Shankar N. Metamathematics, Machines and Gödel's Proof // Cambridge tracts in theoretical computer science. — 1994. — Vol. 38.

[12] Попов Г. Ошибка в проекте. Ленинский тупик / Г. Попов. — М. : Издательский дом Международного университета в Москве, 2008. — 512 с.

[13] Дербишир Д. Простая одержимость. Бернхард Риман и величайшая нерешенная проблема в математике / Д. Дербишир. — М. : Астрель, 2010. — 464 с.

[14] Harrison J. Formalizing an analytic proof of the Prime Number Theorem // Journal of Automated Reasoning. — 2009. — Vol. 43. — P. 243–261.

[15] Appel K. The Solution of the Four-Color Map Problem / K. Appel, W. Haken // Sci. Amer. — 1977. — Vol. 237. — P. 108–121.

[16] Appel K. Every Planar Map is Four-Colorable // K. Appel, W. Haken // Amer. Math. Soc. — 1989.

[17] A New Proof of the Four Colour Theorem. Electron. Res. Announc / N. Robertson [and others] // Amer. Math. Soc. — 1996. — N 2. — P. 17–25.

[18] Gonthier G. Formal Proof — The Four-Color Theorem // Notices of the American Mathematical Society. — 2008. — Vol. 55 (11). — P. 1382–1393.

[19] Wilson R. Four Colors Suffice: How the Map Problem Was Solved / R. Wilson. — Princeton, NJ: PrincetonUniversityPress, 2004.