Матиясевич Юрий Владимирович

УДК 510.23 510.652

МАТЕМАТИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО: ВЧЕРА, СЕГОДНЯ, ЗАВТРА

Аннотация

Этот текст является слегка отредактированной стенограммой содоклада на совместном заседании Санкт-Петербургского Математического общества и Секции математики Дома учёных 23 марта 2010 года. Материалы заседания, включая видеозаписи, доступны в [1].

Ключевые слова: формальное доказательство, интерактивное доказательство, нулевое знание.

Евклид продемонстрировал, что огромное количество геометрических теорем может быть выведено из довольно небольшого количества аксиом. Правда, впоследствии выяснилось, что его аксиоматика не полна, и надо добавить в качестве аксиом ещё несколько «очевидных утверждений», например *аксиому Паша*, утверждающую, что если прямая лежит в плоскости треугольника и пересекает одну из его сторон, то она пересекает ещё и какую-то другую его сторону. Позднее полная система геометрических аксиом была построена Давидом Гильбертом (David Hilbert).

Процесс аксиоматизации был расширен на всю математику, были сформулированы аксиомы теории множеств, в частности, построена *аксиоматика Цермело-Френкеля*. По крайней мере, 99,999 % теорем, которые доказываются современными математиками, можно вывести по формальным правилам из аксиом этой системы. В некотором смысле, большинство математиков сегодня не открывают абсолютно ничего нового – всё уже заложено в аксиомах. Возникает вопрос: за что тогда математикам платят деньги?

Один ответ таков. Формально можно было бы поступать, как поступали, говорят, древние греки: нарисован чертёж, а в качестве доказательства написано «Смотри». Когда теорема сформулирована, дальше можно было бы просто написать, например: «Следует из аксиоматики Цермело-Френкеля». Дело, однако, в том, что вывод теоремы из аксиом может быть очень и очень длинным (в общем случае его длину нельзя оценить сверху никакой вычислимой функцией от длины формулировки теоремы).

Найти такой длинный вывод теоремы из аксиом в принципе можно путём исчерпывающего перебора: на первом шаге из аксиом выводятся их непосредственные следствия, на втором – следствия следствий и так далее, пока среди следствий не окажется интересующая нас теорема. Понятно, однако, что на таком пути нельзя найти доказательство сколько-нибудь интересной теоремы. Математики же неведомыми нам путями из очень тонких соображений выводят весьма нетривиальные следствия из вполне ограниченного количества «очевидных» аксиом.

Эта способность человеческого мозга очень удивительна по следующей причине. С одной стороны, математика, несомненно,

играет очень полезную роль в современном обществе, и квалифицированные математики для него очень важны. С другой стороны, с биологической точки зрения, человек изменился за последние, скажем, пять тысяч лет не сильно, и, значит, и тогда рождались люди, которые по своим природным данным могли бы стать замечательными математиками. В те времена, однако, такие выдающиеся способности не приносили индивиду заметных преимуществ, в отличие, скажем, от роста, силы или скорости бега, и потому не могли служить существенным фактором естественного отбора. Почему же тогда у человека появились способности к абстрактному математическому мышлению?

Я, однако, хочу обсуждать не вопрос, откуда берутся математические доказательства, а то, как их проверять, – ведь известно немало случаев опубликованных неверных доказательств, при этом ошибка обнаруживалась иногда через десятилетия.

Я хочу рассказать, в первую очередь, о деятельности по проверке математических теорем, которая ведётся давно, но, тем не менее, не очень известна большинству математиков. А именно, уже много лет разрабатываются системы, позволяющие проверять с помощью компьютеров достаточно сложные доказательства при условии, что они изложены абсолютно со всеми деталями. Подобных систем сейчас существует довольно много. Была попытка [2] объединить их в одну систему, но по разным причинам объединения не произошло. Есть разные коллективы, разные авторы, которые работают независимо, может быть, это и к лучшему.

Для сравнения различных систем используется, в частности, один «джентльменский набор» из 100 теорем [5], которые были отобраны в конце XX века как по их роли в математике, так и по красоте. Доказательства многих из этих 100 теорем уже проверены компьютерными системами, и зачастую не одной.

К проверенным относятся, в частности,

– *теорема Пифагора*,

– *первая теорема Гёделя* о неполноте всякой достаточно мощной, но непротиворечивой логической системы,

– теоремы о невозможности трисекции угла и удвоения куба,

– *основная теорема арифметики*, утверждающая, что каждое натуральное число представимо в виде произведения простых чисел, причём единственным, с точностью до порядка сомножителей, образом,

– *основная теорема алгебры*, утверждающая, что каждый отличный от константы многочлен от одной переменной имеет хотя бы один корень в поле комплексных чисел,

– теорема о бесконечности множества простых чисел и *закон распределения простых чисел*,

– *теорема о четырёх красках*,

– теоремы о расходимости гармонического ряда и ряда чисел, обратных к простым,

– теорема, утверждающая, что любое натуральное число является суммой квадратов четырёх натуральных чисел,

– *теорема Брауера* о неподвижной точке,

– *теоремы Силова*,

– доказанный П.Л. Чебышевым *постулат Бертрана*, утверждающий, что если $n \geq 2$, то найдётся простое число p такое, что $n < p < 2n$.

В то же время своей очереди ждут, в частности:

– теорема о неразрешимости в радикалах уравнений высших степеней,

– независимость евклидова постулата о параллельных прямых от других геометрических аксиом,

– независимость континуум-гипотезы от других аксиом теории множеств,

– *великая теорема Ферма*, которую доказал Эндрю Уайлс (Andrew Wiles),

– теоретико-вероятностные *центральная предельная теорема* и *закон больших чисел*,

– теорема о том, что существуют только пять правильных многогранников (*платоновых тел*),

– трансцендентность чисел e и π.

С текущим статусом теорем можно ознакомиться на сайте [6].

Отдельно я хочу остановиться на теореме о четырёх красках. Как известно, она первоначально была доказана с помощью компьютера, и по этой причине были сомнения – всё ли там верно. Доказательство, дан-

ное Кеннетом Аппелем (Kenneth Appel) и Вольфгангом Хакеном (Wolfgang Haken), состояло из двух частей. Первая из них [7] устанавливала, что для доказательства теоремы достаточно разобрать 1936 случаев, и эта часть работы была проделана вручную (авторы указали, что сочли это более простым, чем написание соответствующей программы). Вторая часть [8] доказательства, в работе над которой принял участие программист Джон Кох, состояла в том, что компьютер разобрал каждый из этих 1936 случаев.

Впоследствии Нейл Роберсон (Neil Robertson), Даниель Сандерс (Daniel P. Sanders), Пол Сеймур (Paul Seymour) и Робин Томас (Robin Thomas) [12] решили проверить доказательство Аппеля–Хаккена. Эти четыре автора честно сказали, что им оказалось проще написать свою программу, чем разбираться в программе Аппеля–Хакена–Коха. В итоге новые авторы сделали гораздо больше: они проверили на компьютере и первую, и вторую части доказательства. Кроме того, для второй части доказательства они написали программу, которая может распечатать доказательство каждого из случаев в виде, который мог бы проверить человек.

У них получилось 633 случая, а длина текста для одного случая – порядка 10 тысяч страниц.

Уменьшение количества случаев не было самоцелью, авторы могли бы получить и меньшее их количество. Вместо этого авторы предпочли избегать случаев, требующих сложного разбора. Это позволило им построить алгоритм квадратичной сложности для раскраски любой карты в четыре цвета (доказательство Аппеля–Хакена давало лишь алгоритм со сложностью $O(n^4)$).

Появление нового независимого компьютерного доказательства теоремы о четырёх красках придало дополнительную уверенность в её справедливости. Тем не менее, снова была использована сложная программа, при написании которой также могла быть допущена ошибка. В 2008 году появилось ещё одно компьютерное доказательство теоремы о четырёх красках. Отличие нового доказательства от двух предыдущих состояло в том, что его автор Жорж Гонтье (George Gonthier) использовал не специально написанную программу, а универсальную программу Coq [11], способную проверить, в принципе, доказательство произвольной теоремы, выводимой из используемой аксиоматики.

Как уже говорилось, для того чтобы компьютер мог проверить доказательство, оно должно быть изложено со всеми-всеми деталями, что неизбежно делает такие доказательства очень длинными. Где же в наше время можно публиковать столь подробные доказательства? Есть журнал, который называется «Formalized Mathematics» (рис. 1). Он перестал выходить в бумажном виде, но

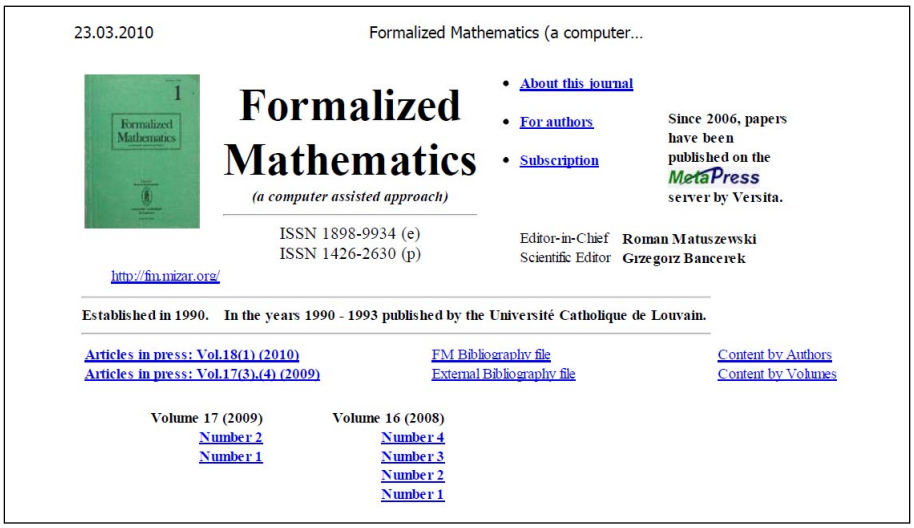

Рис. 1. Журнал Formalized Mathematics

FORMALIZED MATHEMATICS
Vol. 17, No. 2, Pages 73–77, 2009

Kolmogorov's Zero-One Law

Agnes Doll
Ludwig Maximilian University of Munich
Germany

Summary. This article presents the proof of Kolmogorov's zero-one law in probability theory. The independence of a family of σ-fields is defined and basic theorems on it are given.

MML identifier: KOLMOG01, version: 7.11.01 4.117.1046

The articles [8], [19], [2], [10], [12], [18], [20], [1], [15], [5], [21], [11], [3], [9], [7], [6], [17], [4], [16], [14], and [13] provide the terminology and notation for this paper.

For simplicity, we adopt the following convention: Ω, I are non empty sets, $\mathcal{F}$ is a σ-field of subsets of Ω, P is a probability on $\mathcal{F}$, D, E, F are families of subsets of Ω, A, B, s are non empty subsets of $\mathcal{F}$, b is an element of B, a is an element of $\mathcal{F}$, p, q, u, v are events of $\mathcal{F}$, n is an element of $\mathbb{N}$, and i is a set.

Next we state three propositions:

(1) For every function f and for every set X such that $X \subseteq \operatorname{dom} f$ holds if $X \neq \emptyset$, then $\operatorname{rng}(f \restriction X) \neq \emptyset$.

(2) For every real number r such that $r \cdot r = r$ holds $r = 0$ or $r = 1$.

(3) For every family X of subsets of Ω such that $X = \emptyset$ holds $\sigma(X) = \{\emptyset, \Omega\}$.

Let Ω be a non empty set, let $\mathcal{F}$ be a σ-field of subsets of Ω, let B be a subset of $\mathcal{F}$, and let P be a probability on $\mathcal{F}$. The functor $\operatorname{Indep}(B, P)$ yielding a subset of $\mathcal{F}$ is defined as follows:

(Def. 1) For every element a of $\mathcal{F}$ holds $a \in \operatorname{Indep}(B, P)$ iff for every element b of B holds $P(a \cap b) = P(a) \cdot P(b)$.

Next we state several propositions:

(4) Let f be a sequence of subsets of $\mathcal{F}$. Suppose for all n, b holds $P(f(n) \cap b) = P(f(n)) \cdot P(b)$ and f is disjoint valued. Then $P(b \cap \bigcup f) = P(b) \cdot P(\bigcup f)$.

Рис. 2. Страница журнала Formalized Mathematics

выходит в электронном виде и размещен в свободном доступе в Интернете [3]. Журнал издаётся в Польше, где группа авторов уже много лет разрабатывает систему для проверки доказательств «Mizar». Правила публикации в этом журнале очень простые: автор должен представить текст в специальном формате, и этот текст проверяет компьютер. Если компьютер признаёт, что всё верно, то доказательство сохраняется в базе знаний. Компьютер также генерирует краткий текст с определениями и формулировками лемм и теорем, который потом печатается в журнале.

На рис. 2 представлена первая страница статьи про «Закон 0-1 Колмогорова». В начале статьи идут ссылки на предыдущие публикации, из которых можно узнать необходимые определения и формулировки. Если какая-то требуемая лемма или теорема отсутствует в базе компьютера, то её надо сформулировать и доказать. Например, в этой статье пункт (2) гласит: «для каждого вещественного r, такого, что $r \times r = r$, или $r = 0$, или $r = 1$». Никто в обычной математической статье такого писать не будет, но в формальном доказательстве это необходимо.

Уже сегодня компьютеры могут проверять формализованные доказательства нетривиальных теорем.

ПРЕДСКАЗАНИЕ

Через 25 лет журналы (если они ещё будут существовать) не будут принимать к рассмотрению статьи, не сопровождаемые доказательствами, которые может проверить компьютер.

Нынешние молодые люди смогут через 25 лет проверить, сбудется ли моё предсказание или нет. Если оно окажется верным, то это радикально изменит ситуацию с фрематистами – они просто будут не в состоянии представить нужный формальный текст.

Что мешает внедрению в повседневную жизнь математиков доказательств, проверяемых компьютерами? Здесь много говорилось про аксиомы, теоремы, доказательства. Но прозвучало ещё одно важное слово: «метод». В математике разрабатывают методы. Разобраться, что такое метод, очень непросто. Если я доказал одну лемму, то про вторую могу просто сказать, что она доказывается аналогично. Однако пока что аналогия – вещь, очень трудная для компьютеров. Если будет разработана формальная техника доказательств по аналогии, то ситуация для построения формализованных доказательств изменится в лучшую сторону.

Другая трудность – необходимость создания большого задела из определений и теорем, хранящихся в базе знаний компьютера. Это весьма трудоемкая работа, но здесь имеется значительный прогресс. Иногда разработчикам удаётся получить грант на формализацию той или иной книги. Некоторые монографии написаны детально, например некоторые книги Эдмунда Ландау (Edmund Landau), и тогда это не очень трудная работа, формализация других книг бывает намного сложнее.

В развитие разговора про формальные доказательства я хочу рассказать некоторые другие вещи, которые непосредственно не затрагивают работу математиков, но тоже могут быть им интересны – про взгляд на доказательства в информатике.

Я начну со случая, который произошёл с одним моим коллегой ещё в советские времена. Он приходит в магазин и видит новую книгу, которая называется «Теория доказательств». Мой коллега в шоке. Почему? Он следит по каталогам, что выйдет нового, и даёт рекомендации по закупке книг в библиотеку, а тут вышла книга по его прямой специальности, но он об этой книге не знал. Напоминаю, что это было в советские времена, когда в магазинах не было свободного доступа к книгам, их отделял от покупателей прилавок. Мой коллега просит продавца показать ему книгу и видит, что у названия есть набранный более мелким шрифтом подзаголовок. Полное название:

ТЕОРИЯ ДОКАЗАТЕЛЬСТВ
в гражданских и уголовных процессах

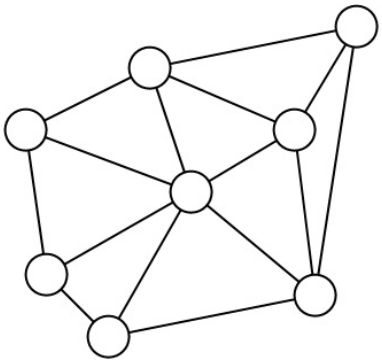

Рис. 3. Граф, вершины которого надо раскрасить

Это был учебник для студентов-юристов. Как видите, у них тоже есть доказательства. Чем же их доказательства отличаются от доказательств в математике?

Когда математик доказывает теорему, он первым делом доказывает её для кого? – для себя. Когда математик проверил доказательство, он может показать его другому математику, который, в свою очередь, может показать доказательство третьему, и так далее.

В информатике придумали так называемые *интерактивные доказательства*[1], которые скорее похожи на доказательства в юриспруденции. Там, чтобы доказывать судье, что обвиняемый невиновен, адвокату вовсе не обязательно верить, что его подзащитный действительно невиновен. Задача адвоката – убедить конкретного человека в невиновности другого человека. Это доказательство по принципу «Я *вам* докажу». И оказывается, что подобный принцип можно ввести и в информатике.

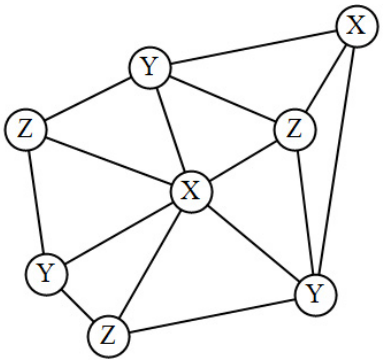

Рис. 4. Абстрактная раскраска графа

Сейчас я хочу продемонстрировать такое «убедительство».

Как вы понимаете, я не могу один провести интерактивное доказательство, поэтому у меня будет содокладчик из числа слушателей[2]. Я хочу доказать *ему* простую теорему: *вершины моего графа можно правильным образом раскрасить в три цвета*.

(*Докладчик кладёт на слайд-проектор изображение графа,* см. рис. 3).

Напомню, что раскраска называется правильной, если концы каждого ребра окрашены по-разному.

Конечно, я мог бы просто предъявить всем вам такую раскраску. Я действительно покажу её, но только залу, прошу содокладчика не смотреть на экран.

(*Содоклачик встаёт спиной к экрану*).

Вот требуемая правильная раскраска графа.

(*Докладчик меняет слайд,* см. рис. 4).

Здесь три цвета обозначены буквами X, Y, Z. Мы можем этим буквам поставить во взаимно-однозначное соответствие реальные цвета, скажем, красный, жёлтый и зелёный.

Существует 6 способов это сделать. Я бросаю кубик, выбираю случайным образом одно из 6 возможных соответствий:

X – красный,
Y – жёлтый,
Z – зелёный,

и получаю следующую раскраску (см. рис. 5).

Я, однако, не хочу показывать эту раскраску моему содокладчику.

(*Докладчик накрывает вершины монетами*, см. рис. 6).

Теперь я прошу содокладчика посмотреть на экран и прежде всего убедиться в том, что это тот самый граф, про который я

[1] По-английски «interactive proof»; я предлагал в качестве русского аналога использовать *убедительство*, но этот термин пока не прижился.

[2] Традиционно в английской литературе участники интерактивного доказательства называются «prover» и «verifier».

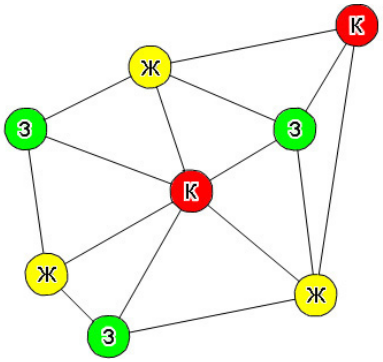

Рис. 5. Конкретная раскраска графа

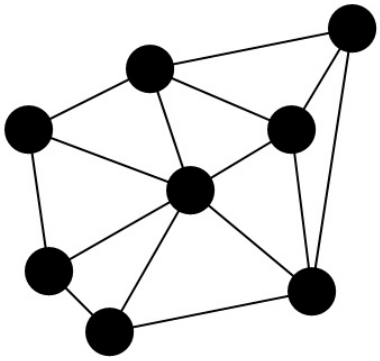

Рис. 6. Раскраска графа скрыта

утверждал, что он имеет правильную раскраску вершин в 3 цвета.

Содокладчик: «Да, это тот самый граф».

Я спрашиваю содокладчика: «Верите ли вы, что монетами закрыта правильная раскраска графа?»

Содокладчик: «Пока не очень».

Я предлагаю содокладчику: «Давайте я Вам покажу раскраску двух концов одного, какого-угодно, ребра, на Ваш выбор?»

Содокладчик указывает ребро, докладчик снимает монеты, покрывающие его концы, и все видят, что они действительно окрашены по-разному – в зелёный и красный цвета, см. рис. 7).

Я снова спрашиваю содокладчика: «Теперь-то Вы верите, что монетами закрыта правильная раскраска графа?»

Содокладчик: «Ешё нет. Я видел цвета концов только одного ребра, и хотел бы проверить и другие рёбра».

Я готов на это, но прошу содокладчика снова отвернуться от экрана, снова кидаю кубик, выбираю новое соответствие цветов буквам X, Y, Z:

X – жёлтый,

Y – зелёный,

Z – красный,

и получаю новую раскраску (см. рис. 8).

Докладчик снова накрывает вершины монетами, см. рис. 6.

Я опять предлагаю содокладчику проверить, что граф не изменился, и снова выбрать любое ребро.

Содокладчик указывает другое ребро, докладчик снимает монеты, покрывающие его концы, и все снова видят, что они действительно окрашены по-разному – в красный и жёлтый цвета (рис. 9).

Я снова спрашиваю содокладчика: «Ну а теперь-то Вы верите, что монетами закрыта правильная раскраска графа?»

Содокладчик: «Всё ещё нет. Я снова вижу цвета концов только одного ребра, и при этом я не могу быть уверен, что сейчас

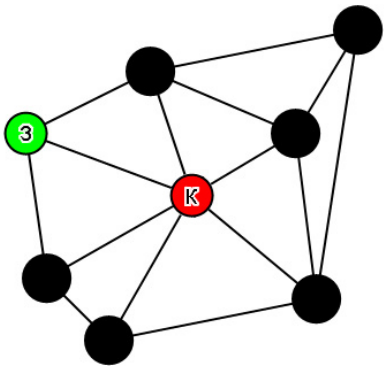

Рис. 7. Раскраска концов одного ребра

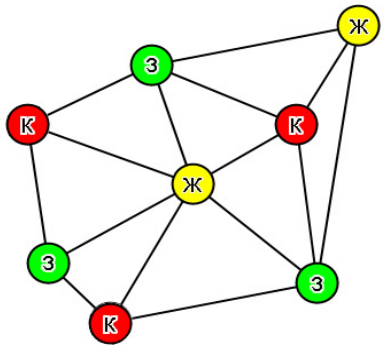

Рис. 8. Новая конкретная раскраска графа

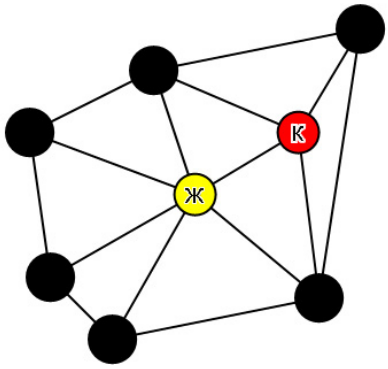

Рис. 9. Раскраска концов ещё одного ребра

концы того ребра, которое я выбирал ранее, по-прежнему раскрашены по-разному»

Я согласен повторить всю процедуру, включающую бросание кубика, ещё много раз. На первый взгляд кажется, что такое повторение бесполезно: в каждом раунде содокладчик видит раскраску концов только одного ребра и не может проверить, что правильность раскраски не нарушается где-либо в другом месте.

Действительно, на таком пути никогда не удастся получить доказательство, а вот «убедительство» получить можно.

Пусть в графе было n рёбер, и допустим, что он не имеет правильной раскраски. Тогда вероятность обнаружения этого за один раунд не меньше, чем $\frac{1}{n}$, если все рёбра выбираются с одинаковой вероятностью. Соответственно, вероятность обмана не больше, чем $1 - \frac{1}{n}$ в одном раунде, и не более, чем $\left(1-\frac{1}{n}\right)^m$, если было проведено m раундов. Например, если $m = 1000n$, то вероятность обмана будет не больше, чем $\left(1-\frac{1}{n}\right)^{1000n} \approx e^{-1000}$.

Таким образом, после $1000n$ циклов у содокладчика будет выбор между двумя альтернативами: или поверить в существование правильной раскраски, или признать, что он стал свидетелем события с ничтожно малой вероятностью.

Это был один из простейших примеров интерактивного доказательства.

В нём есть такой аспект, который называется *нулевое знание*. Я, вроде бы, убедил содокладчика, что у рассматриваемого графа имеется правильная раскраска. Но что конкретно он узнал от меня? Для некоторых, быть может, даже для всех рёбер он узнал, что есть раскраски, в которых концы этих рёбер окрашены в такие-то конкретные цвета. Однако существование таких раскрасок является следствием существования какой-то раскраски, ибо мы всегда можем применить перестановку цветов. Таким образом, я сообщил содокладчику ровно один бит информации – то, что граф имеет раскраску, но не сообщил больше ничего.

Это было интуитивное объяснение, почему в данном случае имело место нулевое знание. Для строгого обоснования надо дать определение этому понятию. Однако для начала спросим себя – зачем вообще был нужен диалог? Действительно, граф конечен, и мой соавтор мог бы сам установить, существует ли требуемая раскраска, например, путём полного перебора всех способов отобразить множество вершин в множество цветов. Для сколько-нибудь значительного количества вершин такой перебор невозможен на самых мощных современных компьютерах, и, к сожалению, в настоящее время неизвестно существенно более эффективных методов раскраски графов (эта проблема является NP-полной).

Формально доказательством можно считать любой объект, подтверждающий истинность теоремы, при условии, что проверить это можно быстро.

В информатике есть грубое, но удобное во многих случаях деление алгоритмов на быстрые и медленные – время работы первых ограничено полиномом от длины входных данных. В этом смысле фраза «Следует из аксиом», математически верная, не может рассматриваться как доказательство.

Строгое определение нулевого знания основано на сравнении времени работы *любого* алгоритма, использующего содержание диалога, со временем работы *некоторого* алгоритма, работающего без такой подсказ-

ки. В случае, когда время сокращается несущественно (полиномиально), и говорят про доказательство с нулевым знанием. В частности, можно доказать, что, каков бы ни был алгоритм, находящий раскраску графа, знающий и сам граф, и протокол диалога, произошедшего во время убедительства, имеется другой алгоритм, строящий раскраску любого графа, зная только его, и работающий лишь полиномиально медленнее.

Интерактивное доказательство с нулевым знанием – это действительно доказательство по принципу «Я *Вам* докажу». В самом деле, мой содокладчик, будучи сам убеждён в существовании раскраски, не имеет средств убедить кого-либо третьего. Это свойство таких доказательств находит применение в криптографии.

Почему я использовал для интерактивного доказательства слайд-проектор, а не компьютер?

Я мог бы показать то же самое, что вы видели на экране, используя компьютер и бимер, но это не было бы убедительством для моего содокладчика. Действительно, даже если граф не имеет правильной раскраски, легко написать программу, которая будет показывать разные цвета у концов любого конкретного ребра. Убедительная сила диалога была основана на том, что после того как я положил слайд на проектор, я не могу поменять раскраску вершин.

Сразу возникает вопрос: а можно ли провести «убедительство» по телефону или по Интернету? Оказалось, что это возможно.

Я привёл пример с раскраской, но сразу возникает вопрос, какие ещё теоремы можно так доказывать? Есть очень красивые примеры про изоморфизм графов и неизоморфизм графов. В конечном итоге было получено описание всего класса утверждений, допускающих интерактивные доказательства с нулевым знанием. В частности, в этот класс попадают все формализованные доказательства в любой логической системе. Тем самым, можно доказывать теоремы, не давая никакого знания о том, как теорема доказана, а только убеждая проверяющего, что теорема верна.

В заключение упомяну ещё один результат, полученный в информатике. Доказательство в любой формальной системе может быть преобразовано в другое доказательство того же утверждения с не более чем полиномиальным увеличением как его длины, так и времени проверки. При этом новое доказательство будет обладать ещё одним очень интересным свойством. Для него существует серия тестов, для выполнения каждого из которых достаточно знать лишь небольшое количество битов, специальным способом выбираемых из записи доказательства в виде строки из 0 и 1. Если все тесты проходят, то доказательство верно. Но если доказательство содержит ошибку, то это обнаружится не менее, чем половиной тестов. Таким образом, проделав, скажем, 1000 выбранных случайным образом тестов, мы будем стоять перед дилеммой: или поверить, что доказательство верно, или признать, что мы наблюдали событие, вероятность которого не более 2^{-1000} (обратите внимание, что эта оценка вероятности не зависит от длины доказательства, то есть вообще говоря его не нужно читать полностью). Такие доказательства были названы *голографическими*.

Традиционное доказательство в математике можно представить как груз, висящий на цепочке. Одно звено слабое – и всё доказательство рушится. В случае же голографических доказательств ошибка не может быть локализована в одном месте, она обязательно «размазана» по всему тексту.

ДИСКУССИЯ ПО ОКОНЧАНИИ ДОКЛАДА

Вопрос. Не перенесутся ли проблемы, свойственные обычным доказательствам, на доказательства, проверяемые с помощью новых методов? Правила формализации утверждений ведь пишутся в тех же условиях, в которых пишутся доказательства. Здесь тоже потребуется, например, начальная информация, неявные предположения, которым мы доверяем.

Докладчик. Например, я говорил о проверке проблемы четырёх красок на компью-

тере. Авторы честно написали, что проверили всё, кроме одной вещи: они не проверили правильность компилятора. Они написали программу на языке высокого уровня и поверили, что компилятор правильно перевёл. Некогда фирма Intel выпустила процессор, изредка делавший ошибку при делении. После её обнаружения некоторые авторы стали делать в своих статьях примечания: «Вычисления произведены с применением процессора Intel». Тем самым, авторы снимали с себя ответственность за правильность.

Да, есть вероятность, что у нас неправильный процессор или что программа проверки написана с ошибкой. В этом и состоит ценность универсальной программы – она написана на все случаи жизни, и если в ней есть ошибки, то они должны довольно скоро выявиться. Если программа много раз испытана на разных примерах, это даёт бóльшую убеждённость, что всё верно. Надежнее использовать одну многократно проверенную систему, чем программу, недавно написанную для решения одной конкретной задачи. А аксиоматика и правила вывода не меняются никогда.

Вопрос. Ещё про ошибки в процессоре – может быть, кто-то специально сделал «закладку», ошибочно вычисляющую то или иное число, например, произведение двух чисел? В нашем рассуждении важную роль играет вера – это слово однокоренное со словами «проверка», «уверенность».

Докладчик. Фирма Intel знала об ошибке, но скрывала от общественности, не желая портить свой имидж и веря в то, что ошибку никто никогда не найдёт. Действительно, вероятность ошибочного результата была очень мала, если полагать, что все аргументы операции равновероятны. Сотрудники Intel не учли однако, что в данном случае ошибки концентрировались вокруг очень специальных чисел – при делении на числа, которые чуть-чуть меньше, чем 5, 10, 15, 20 или 25. Но вероятность получения в ходе вычислений числа вида 4,999999, если истинное значение является целым числом 5, очень велика, и ошибка была обнаружена.

Если вы не верите в правильность процессора или компилятора, то можете заставить машину делать дополнительную работу по самопроверке. Например, если вам надо найти произведение целых чисел $a \times b$, то вы можете породить случайные целые числа $r_1, \ldots, r_n, s_1, \ldots, s_n$, вычислить

$$(a + r_1) \times (b + s_1) - a \times s_1 - b \times r_1 - r_1 \times s_1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(a + r_1) \times (b + s_n) - a \times s_n - b \times r_n - r_n \times s_n$$

и сравнить полученные числа друг с другом. Очень трудно представить ошибку в процессоре, которая всегда приводила бы к одинаковым числам, но иногда не равным истинному произведению $a \times b$.

В общем случае для увеличения надёжности можно как раз использовать голографические доказательства – маломощный, но надёжный компьютер может проверить вычисления суперкомпьютера, не будучи в состоянии выполнить их самостоятельно.

Вопрос. Сейчас надёжность вычислений на компьютере выше, чем надёжность вычислений вручную, где, например, скобочки не так расставлены. Ещё должно быть доверие к алгоритмам, которые используются. Многие знают, что существует несколько конкурирующих систем – Maple, Mathematica и другие, производящих вычисления высокого уровня, которые нельзя считать вычислениями в привычном смысле и которые скорее напоминают доказательство теоремы. И есть достаточно популярный алгоритм интегрирования функций. По функции он или сообщает, что она не интегрируема, или выдаёт результат интегрирования. Когда этот алгоритм появился, сравнивались возможности разных систем. И появлялись сообщения, например, о том, что одна среда интегрирует, а другая сообщает, что функция не интегрируема. То есть компьютерным вычислениям доверять можно, но хотя бы на теоретическом уровне мы должны оставить элемент веры. Так же как мы верим в непротиворечивость арифметики, чтобы обосновать непротиворечивость остальных систем аксиоматики.

Докладчик. Вопрос, который мы пока не обсуждали, – зачем нужны формализованные доказательства? В качестве одного из потенциальных приложений было предложено использовать их для проверки вычислений в системах типа Mathematica и Maple. Чтобы они не просто давали ответ, а давали ответ в форме, которую можно проверить любой системой.

Вопрос. Вы говорили о правилах принятия статей в польский журнал. Но когда мы говорим об оценке текста, то проверка часто проводится на примере американского языка, а он значительно отличается от британского. При этом в России учат как раз британский вариант. Как вы относитесь к компьютерной проверке текста, поскольку здесь возможно не вполне точное понимание?

Докладчик. По нынешним правилам автор должен представить статью на формальном языке, который не имеет прямого отношения к живым языкам. Это формализованный язык. А уже на его основе система генерирует английский текст по правилам: «рассмотрим» и т. д.

Вопрос. Чем будут заниматься математики, если будет принято решение о дополнении обычных доказательств формализованными?

Докладчик. Это непростой вопрос – чем будут заниматься математики. Есть такое мнение, что математика – это наука молодых людей, а люди старшего возраста могут создавать фундамент для будущих поколений, переводя доказательства на формальный уровень.

Из зала. Печальная старость.

Докладчик. Каждый делает, что может. Сейчас у польского журнала много авторов, люди этим занимаются и получают гранты под это дело. Вопрос на самом деле такой: процесс формализации довольно трудоёмкий, но по мере развития техники он должен становиться всё легче и легче.

Когда я был в Польше, я специально на три дня приехал в гости к разработчикам системы Mizar [4]. Они работают не в Варшаве, а в Белостоке. Меня, естественно, интересовало, как проверить на компьютере десятую проблему Гильберта. Но всё это слишком большая работа, и я проверил только две основные леммы. Для меня были созданы все условия. Три дня я сидел за компьютером, рядом со мной сидел основатель этой системы. У меня был формально написанный текст. За три дня мы преуспели. Но выяснилось, что некоторые очевидные вещи в системе ещё не реализованы, нужно было их доказывать. То есть пока это довольно трудоёмкий, скрупулёзный процесс. По мере создания базы будет всё легче и легче. Думаю, что это вопрос времени.

Вопрос. Насколько я понимаю, эта система – «чёрный ящик». Сама программа, насколько понимаю, сложная. Насколько мне известно, есть системы, которые можно расширять и которые дают не просто ответ, а длинный текст, который можно использовать. Я правильно понимаю, что программу формализации сложно дополнять новыми возможностями, и такое дополнение потребует перепроверки сложной программы? И внесение изменений чревато внесением ошибок в логике программы.

Докладчик. Что такое новые возможности, зачем они нужны? Как я сказал в самом начале своего выступления, 99,999 % новых теорем – это всего лишь следствия конечного набора аксиом теории множеств, и для вывода теорем достаточно использовать небольшое количество известных логических правил. Да, есть специалисты по математической логике, которые строят примеры утверждений, недоказуемых в той или иной формальной системе и придумывают новые аксиомы, позволяющие доказать такие утверждения в расширенной системе. Эта деятельность, однако, далека от того, чем занимаются «настоящие математики».

Ядро системы – аксиоматика, правила вывода, алгоритмы проверки правильности вывода – менять не нужно, они универсальны. Система расширяется за счёт введения новых определений и новых теорем, последние добавляются лишь после их формальной проверки. Меняться может интерфейс,

облегчающий человеку общение с системой. Например, желательно позволить человеку использовать слово «аналогично» и иметь препроцессор, который будет преобразовывать текст с этим словом в более длинный текст с подробным доказательством. Именно это доказательство будет проверять неизменное ядро системы.

Вопрос. Правильно ли было бы назвать Ваш доклад «Формальное доказательство: вчера, сегодня, завтра»? Проводите ли Вы связь между обычным доказательством и формализацией? Или это два разных способа доказательства? Какова роль интуиции в формализации доказательств?

Докладчик. Формальные доказательства нужны для нашей большей убеждённости в правильности. Вопрос о том, как работает интуиция в математике, я с самого начала оставил в стороне. Но когда математик убежден, что он нашел доказательство, то, на мой взгляд, он должен верить и в то, что мог бы изложить его со всеми требуемыми деталями.

Литература

1. Заседание Санкт-Петербургского Математического общества и Секции математики Дома учёных 23 марта 2010 года / http://www.mathnet.ru/php/seminars.phtml?option_lang=rus&presentid=2035, http://www.mathnet.ru/php/seminars.phtml?option_lang=rus&presentid=2036, http://www.mathnet.ru/php/seminars.phtml?option_lang=rus&presentid=2583 (дата обращения 20.12.2012).

2. QED manifesto / http://en.wikipedia.org/wiki/QED_manifesto, http://www.cs.ru.nl/~freek/qed/qed.ps.gz (первоначальный вариант), http://mizar.org/trybulec65/8.pdf (пересмотренная версия) (дата обращения 20.12.2012).

3. Formalized mathematics / http://mizar.org/fm (дата обращения 20.12.2012).

4. Mizar / http://mizar.org/ (дата обращения 20.12.2012).

5. Сто теорем / http://web.archive.org/web/20090330133636/http://personal.stevens.edu/~nkahl/Top100Theorems.html (дата обращения 20.12.2012).

6. Статус теорем / http://www.cs.ru.nl/~freek/100/ (дата обращения 20.12.2012).

7. *Appel Kenneth, Haken Wolfgang*. Every Planar Map is Four Colorable, Part I. Discharging // Illinois Journal of Mathematics, 21, 429–490 (1977).

8. *Appel Kenneth, Haken Wolfgang, Koch John*. Every Planar Map is Four Colorable, Part II. Reducibility // Illinois Journal of Mathematics, 21, 491–567 (1977).

9. *Appel Kenneth, Haken Wolfgang*. Every Planar Map is Four-Colorable, Providence, RI: American Mathematical Society, ISBN 0-8218-5103-9 (1989).

10. *Gonthier Georges*. Formal Proof–The Four-Color Theorem // Notices of the American Mathematical Society, 55 (11): 1382–1393 (2008) / http://www.ams.org/notices/200811/tx081101382p.pdf (дата обращения 20.12.2012).

11. Coq http://coq.inria.fr/ (дата обращения 20.12.2012).

12. *Robertson Neil, Sanders Daniel P., Seymour Paul, Thomas Robin.* The Four-Colour Theorem. J. Combin. Theory Ser. B 70 (1): 2–44, (1997), doi:10.1006/jctb.1997.1750.

Abstract

This publication is a slightly edited verbatim report of author's co-talk presented at joint meeting of St.Petersburg Mathematical Society and Mathematical section of the House of Scientists on March 23, 2010; related materials, including video recording, can be found on [1].

Keywords: formal proof, interactive proof, zero knowledge.

Матиясевич Юрий Владимирович,
академик РАН, советник РАН,
и.о. заведующего лабораторией
математической логики Санкт-
Петербургского отделения
Математического института РАН,
yumat@pdmi.ras.ru