Верификация длинных доказательств: мечты, планы и реальность

Г.Б. Шабат

15 апреля 2020

Научно-исследовательский семинар по математической логике, МГУ

План

0.0. Ошибка Воеводского (а)

Что привело Воеводского к убеждению в необходимости компьютерной проверки доказательств и затем к проблемам оснований математики?

Формальный ответ – обнаружении **ошибки** в доказательстве ключевой леммы в важной работе.

По [**Voevodsky2014**]:

The groundbreaking 1986 paper "Algebraic Cycles and Higher K-Theory" by Spencer Bloch was soon after publication found by Andrei Suslin to contain a mistake in the proof of Lemma 1.1. The proof could not be fixed, and almost all of the claims of the paper were left unsubstantiated. ...

The approach to motivic cohomology that I developed with Andrei Suslin and Eric Friedlander circumvented Bloch's lemma by relying instead on my paper "Cohomological Theory of Presheaves with Transfers," ... 1992–1993. In 1999–2000, ... I was giving a series of lectures, and Pierre Deligne ... was ... checking every step of my arguments. Only then did I discover that the proof of a key lemma in my paper contained a mistake and that the lemma, as stated, could not be salvaged. Fortunately, I was able to prove a weaker and more complicated lemma, which turned out to be sufficient for all applications. A corrected sequence of arguments was published in 2006.

This story got me scared. Starting from 1993, multiple groups of mathematicians studied my paper at seminars and used it in their work and none of them noticed the mistake. And it clearly was not an accident. A technical argument by a trusted author ... is hardly ever checked in detail.

0.0. Ошибка Воеводского (б)

О чём речь и при чём тут основания математики?

В 1992-1995 годах Воеводский занимался *мотивными когомологиями, реализуя мечту Гротендика.* Искалась ТЕОРИЯ.

Фрагмент неверной формулировка из [**Voevodsky2000**]:

Proposition 4.23. *Let W be a smooth ... and $W = U \bigcup V$ be an open covering of W. Then... the sequence ... is exact.*
Proof: It follows from Lemma 4.6 in exactly the same way as in the proof of Proposition 4.17.

Ошибка была обнаружена Воеводским (совместно с Делинем) в 1999-2000 при разборе деталей доказательства .

Исправлена в [**MaVoWe2006**].
Lemma 22.10. *Suppose that F is a homotopy invariant presheaf with transfers. Then for any open covering $S = U_0 \bigcup V$ there is an open $U \subset U_0$ such that $S = U \bigcup V$ and the sequence ... is exact.*
(corrects **4.23** in which the passage from U_0 to U was omitted).
This process uncovered a mistake in a key lemma [V00a, 4.23], which was corrected in [MVW, 22.10].

Итак, ошибка носила довольно технический характер и была исправлена. Однако Воеводский (как и многие комментаторы) сделал далеко идущие выводы:

The primary challenge that needed to be addressed was that the foundations of mathematics were unprepared for the requirements of the task.

0.1. Математика и искусственный интеллект

Гуманитарная трактовка **теоремы Гёделя о неполноте**:

(множество истинных положений
большинства формальных теорий неперечислимо $\Longrightarrow$)

класс устанавливаемых человеком истин строго шире класса теорем, доказуемых компьютером.

Операции, доступные человеку (при занятиях арифметикой) и недоступные компьютеру: *акты веры* в непротиворечивость, по Матиясевичу переводимые в (недоказуемые) утверждения о неразрешимости диофантовых уравнений.

Логические уточнения: [**Feferman1962**], [**HenkPakhomov2016**].

Вывод. *При доказательство теорем наиболее перспективно сотрудничество человека (творческие операции) и искусственного интеллекта (осуществление формальных доказательств).*
Proof assistance, о котором Воеводский мечтал и рассказывал в популярных лекциях, но до реализации которого не дошёл...

0.2. Личные точки зрения

Первого учителя Воеводского. К proof-checking и основаниям математики Володю влекла не столько личная история с ошибками, сколько стремление *дойти до самой сути*. Он внёс значительный вклад, но реализация его надежд займёт больше времени, чем он мечтал.

Математика. Проект интересен и перспективен, но требует важных уточнений. Подробности ниже.

Преподавателя. В сложившихся разделах преподаваемой математики проект реализуем, интересен и актуален. Подробности ниже.

1.0. Длинные доказательства. Обзор

Будут приведены примеры теорем, традиционное понимание доказательств которых затруднено или невозможно – известные доказательства слишком длинны или слишком сложны.

Природа затруднений может быть различна.

- Слишком длинны рассуждения;
- Теоремы выводятся из результатов, относящихся к другим (далёким) разделам математики;
- Теоремы являются частными случаями новых огромных теорий;
- ... .

1.1. Длинные рассуждения

Проблема Бернсайда: *Существуют ли бесконечные периодические группы?*
Первые публикации: С.И. Адян, П.С. Новиков.
Изв. АН СССР, 1968, 32:1, **212–244**; 32:2, **251–524**; 32:3, **709–731**
Впоследствии доказательства были существенно сокращены (а результаты усилены).

Проблема 4 красок. ...

Теорема Хиронаки о разрешении особенностей. Ann. Math(1964), **109–203.** Мойшезон...

Теорема Мамфорда-Харриса о пространствах модулей.
Invent. Math(1982), **23–86.** Шафаревич...

1.2. Следствия из других проблем

Великая теорема Ферма про $x^n + y^n = z^n$ следует из **теоремы Таниямы-Шимуры-Вейля**, для понимания которой надо знать, что такое *модулярная форма* и *кондуктор*.

Гипотеза Морделла $g_{\mathbf{X}} > 1 \Longrightarrow \#\mathbf{X}(\mathbb{Q}) < \infty$ следует из **гипотезы конечности Шафаревича**, для понимания которой надо знать, что такое *поляризация абелева многообразия*.

Гипотеза Пуанкаре $\pi_1\mathbf{X} = \{1\} \Longrightarrow \mathbf{X} \simeq \mathbf{S}^3$ следует из **гипотезы геометризации Терстона** и использует свойства *потока Риччи*.

1.3. Следствия из новых теорий

Гипотезы Вейля были выведены Делинем из намеченной Вейлем (1948) абсолютно оригинальной теории *когомологий алгебраических многообразий над конечными полями*, затем построенной Гротендиком. ТОПОЛОГИЧЕСКАЯ ИНТУИЦИЯ РАСПРОСТРАНЯЛАСЬ НА АЛГЕБРАИЧЕСКУЮ ГЕОМЕТРИЮ НАД КОНЕЧНЫМИ ПОЛЯМИ.

Гипотеза Милнора, доказанная Воеводским – продолжение этой истории. Была (частично) реализована мечта Гротендика о *мотивах алгебраических многообразий*, унифицирующих известные теории когомологий и устанавливающих их связь с K-теорией.

(Обе, очень абстрактные, теории получили разнообразные применения к "конкретной" математике).

1.4. Два заключительных замечания

(1) И в наше время существуют **непризнанные доказательства**. Пример: Mochizuki утверждает, что abc-гипотеза (*if a and b are composed from large powers of primes, then a+b is usually not divisible by large powers of primes*) вытекает из его Inter-universal Teichmuller Theory. Теория ОЧЕНЬ интересна, и Mochizuki пишет много длинных текстов, но их не понимают.

(2) Некоторые доказательства, бывшие когда-то длинными и трудными, стали короткими и прозрачными. Таковы

- основная теорема алгебры;
- лемма Жордана;
- формула Эйлера В-Р+Г=2-2g;
- ... .

Стремление прояснить тёмные доказательства сыграло важную роль в построении соответствующих понятийных аппаратов.

2.0.Унивалентные основания и Coq: идеи

Универсальность гомотопической интуиции. С распространением этой интуиции за пределы её естественного обитания Воеводский вошёл в математику мирового уровня (аналогичная *гомологическая* интуиция упоминалась выше в связи с программой Вейля). Не удивительно, что предложенная им гомотопическая теория типов (HoTT) быстро получила признание и вызвала интерес и готовность к сотрудничеству.

Гомотопический уровень
истинностных значение 0;
предложений ≤ 1;
множеств ≤ 2;
объектов категорий ≤ 3;
...

2.1. Аксиома универсальности

Формулировка:
отображение $(X = Y) \to (X \simeq Y)$ *является эквивалентностью.*

Одно из применений: возможность доказать

$$\mathbb{N} := \{x \in \mathbb{Z} \mid x \geq 0\},$$

затруднительная при обычном определении $\mathbb{Z} := \frac{\mathbb{N}\times\mathbb{N}}{\approx}$.

Аксиома универсальности же позволяет ввести требуемый (гомотопический) тип отождествления.

Daniel Grayson:
The formal mathematical language, together with the Univalence Axiom, fulfills the mathematicians' dream: a language for mathematics invariant under "equivalence" and thus freed from irrelevant details and able to merge the results of mathematicians taking different but equivalent approaches.

Доклад Делиня *What do we mean by "equal"* в Принстоне (2018) на конференции памяти Воеводского...

2.2. Работа Coq-сообщества

Прижизненная публикация: [**Voevodsky2014a**].

Текущее состояние: см, например
Freek Wiedijk's webpage on the "top 100" mathematical theorems
Несколько примеров с этого сайта:

Fundamental Theorem of Algebra;
The Denumerability of the Rational Numbers;
Godel's Incompleteness Theorem;
Law of Quadratic Reciprocity;
All Primes (= 1 mod 4) Equal the Sum of Two Squares;
Pascal's Hexagon Theorem.

Достижения:
- Запас Coq-теорем растёт(!);
- Сообщество Coq-энтузиастов расширяется;
- Информированность о Coq-деятельности (поддержка?) растёт.

Трудности:
- Овладение языком неспециалистами по-прежнему затруднительно;
- Coq-доказательства зависят от версий, а язык эволюционирует;
- Тексты доказательств ПЛОХО ЧИТАЮТСЯ (см. след. слайд).

2.3. Языковые проблемы

Разработчиками Coq и других подобных языков вряд ли учитывался **фактор адресата.**

Многочисленные пособия, хорошо и тщательно написанные, дружественны по отношению к математику, который хочет научиться **писать** на Coq. Но для приближения к мечтам Воеводского надо подумать и о тех, кто будет **читать** доказательства и – прежде всего – формулировки.

Современный читатель-математик избалован TeXовским качеством современных текстов и вряд ли удовлетворится худшим качеством. Но языковые проблемы глубже.

Почти не разработаны *естественно-подобные* языки, в которых грамматически правильно, **без обозначений**, можно точно сформулировать теорему (*квадрат гипотенузы...*). Попытка предпринята в [**KreydlinShabat2020**].

Вопрос о *переводимости* формулировок с естественно-подобных языков на более традиционные рассмотрен теми же авторами в ряде публикаций.

3.0 Идеальные доказательства

Компьютерная проверяемость + что-то ещё?

- Красота (можно объективно, с экспертными оценками);
- Естественность

(теорему о простых в арифметической прогрессии $\#\{7, 17, 37, 47, 67, \dots\} = \infty$ Дирихле вывел из $\lim_{s\to 1} \sum_{p\in\{7,17,37,47,67,\dots\}} \frac{1}{p^s} = \infty$."Элеменарное" доказательство Сельберга гораздо труднее понять);

- Перспективность

(снова теорема Дирихле: продумывание и обобщение его доказательства легло в основу нескольких теорий XX века);

- Понимаемость и проверяемость человеком (банальность);
- Переводимость на естественный язык (см. предыдущий слайд).

3.1. Сопоставление взглядов с Н. Вавиловым

Текст [**Vavilov2019**] написан интересно (оторваться невозможно!), талантливо, с замечательным знанием предмета и любовью к нему. Вот типичная цитата:

Here is what philosophers and popularisers declare:
- Proof is a formal text written according to rigorously defined rules. Essentially, a sequence of elementary steps each of them consisting of applying inference rules to axioms and previous steps.
- It is sometimes difficult to find a proof; this process may require intuition and inventiveness, but **checking a proof is an entirely mechanical process** that can be delegated to low-skilled personnel, and, ultimately, to a computer.
- Mathematics can be completely formalized, that is reduced to deriving consequences of explicitly given axioms according to explicitly listed inference rules.

...
- To understand and consciously use any mathematical result is possible only after its proof is fully understood. All results in all educational courses at any sufficiently advanced level should be accompanied by complete and detailed proofs.

I believe that such a simplistic propagandist picture is infinitely remote from reality.

Автор подробно и очень убедительно развенчивает перечисленные точки зрения наивных, далёких от математики людей. Возразить почти нечего, если бы не одно важное обстоятельство.

Доказательства эволюционируют! Выше приводились примеры, когда доказательства кардинально упрощались со временем; при этом и возражения о формализации и т.п. постепенно отпадают.

Мы не знаем, как будут выглядеть доказательства Воеводского и Перельмана через 100 лет. Но значительная часть математики уже сформировалась и заслуживает внимания; см. след. слайд.

3.2. Формализация преподаваемой математики

Краткие (апрельские) тезисы.

• Содержание большинства математических дисциплин, преподаваемых в школе и на младших курсах вузов, *может быть* изложено и строго, и понятно.

• Это может (и, видимо, должно) быть сделано на теоретико-множественной основе.

• Мечты Воеводского могут быть реализованы на этой (ему неинтересной) части математики.

• Такая реализация была бы полезна и как модель более обширных замыслов, и с педагогической тоски зрения.

Спасибо за внимание.

Литература


S. Feferman, *Transfinite recursive progressions of axiomatic theories*. Journal of Symbolic Logic, 27(3):259–316, 1962.


Paula Henk, Fedor Pakhomov, *Slow and Ordinary Provability for Peano Arithmetic*. arXiv:1602.01822v2.


Grigory Kreydlin, George Shabat, *Mathematical theorems in natural languages*. To appear in Nova Science Publishers, September 2020.


C. Mazza, V. Voevodsky, C. Weibel, *Lecture notes on motivic cohomology*. Clay Mathematics Monographs, vol. 2, American Mathematical Society, Providence, RI, 2006.


Nikolai Vavilov, *Reshaping the metaphor of proof*. Philosophical Transactions of the Royal Society A. Mathematical, Physical, and Engineering Sciences, 2019.


V. Voevodsky, *Cohomological theory of presheaves with transfers*. Cycles, transfers, and motivic homology theories: 87–137, 2000.


V. Voevodsky, *The origins and motivations of univalent foundations*. https://www.ias.edu/ideas/2014/voevodsky-origins.


V. Voevodsky, *An experimental library of formalized Mathematics* . arXiv:1401.0053v2 [math.HO]


Charles Weibel, *Vladimir Voevodsky. Memorial tribute* . Notices of the American Mathematical Society, volume 66 (2019), number 4.