Компьютерные доказательства и их понимание человеком: случай унивалентных оснований

А. В. Родин[1]

Компьютерное доказательство теоремы о четырех красках, которое было впервые опубликовано Аппелем, Хакеном и Кохом в 1977-м году, спровоцировало продолжающуюся по сегодняшний день философскую дискуссию об эпистемической ценности компьютерных доказательств. В настоящей работе мы показываем, опираясь на поход предложенный в 2006 году Баслером, как унивалентные основания математики (УО) решают некоторые эпистемологические проблемы, которые ранее обсуждались в литературе в связи с компьютерными доказательствами, и тем самым сглаживают различия между компьютерными и традиционными математическими доказательствами. Мы иллюстрируем наши аргументы примером формализованной и компьютеризированной версии доказательства из области алгебраической топологии.

Ключевые слова: унивалентные основания, компьютерные доказательства, пространственная интуиция

1. Введение

Компьютерное доказательство теоремы о четырех красках (Т4К) было впервые опубликовано Аппелем, Хакеном и Кохом в 1977-м году [1]. В 1979-м году Тимошко опубликовал провокационную статью [7], в которой он аргументировал, опираясь на пример доказательства Т4К, что использование компьютерных доказательств кардинально меняет природу математики и делает математику подобной экспериментальной физике. Это статья породила живую философскую дискуссию, которая продолжается по сегодняшний день [3],[2],[5]. В центре этой дискуссии находится вопрос об эпистемической прозрачности (surveyability) компьютерных доказательств. Как отмечает Тимошко и вслед за ним многие другие участники этой дискуссии, компьютерные доказательства в отличии от традиционных математических доказательств не обладают качеством эпистемической прозрачности: человек не в состоянии проследить за ра-

[1] *Родин Андрей Вячеславович* — доктор филос. наук, старший научный сотрудник ИФРАН и доцент СПбГУ, email: andrei@philomatica.org

Andrei Rodin, Sc.D., senior researcher in the Institute of Philosophy (Russian Academy of Sciences) and Associated Professor (Docent) in Saint-Petersburg State University.

ботой компьютера таким же образом, как он способен проследить за рассуждениями другого человека, и поэтому вынужден оценивать результаты компьютерных вычислений в готовом виде. В настоящей работе мы показываем, опираясь на поход предложенный в 2006 году Баслером, как унивалентные основания математики (УО) позволяют решить проблему прозрачности компьютерных доказательств и тем самым сгладить различия между компьютерными и традиционными математическими доказательствами. Мы иллюстрируем наши аргументы примером формализованной и компьютеризированной версии доказательства из области алгебраической топологии, который мы заимствуем из работы [4].

2. Локальная и глобальная прозрачность математических доказательств

Под *локальной* прозрачностью математического доказательства p Баслер понимает свойство (качество) этого доказательства, которое позволяет всякому человеку отслеживать каждый элементарный шаг p [2]. Баслер аргументирует, что локальная прозрачность сама по себе не делает данное доказательство эпистемически прозрачным, поскольку помимо локальной прозрачность для этого требуется *глобальная* прозрачность. Под глобальной прозрачностью Баслер понимает свойство (качество) доказательства p, которое позволяет человеку понять, что совокупность всех элементарных шагов p служит обоснованием заключения p при данных предпосылках. В исторической части своей статьи Баслер указывает на устойчивую философскую тенденцию игнорировать глобальный аспект эпистемической прозрачности, которая, по его мнению, восходит к философии Рене Декарта.

Применяя различие между локальной и глобальной прозрачностью доказательств вслед за Баслером к случаю компьютерного доказательства T4K, мы предлагаем следующее уточнение предложенного им анализа. Компьютерная часть этого доказательства локально прозрачна, поскольку соответствующий программный код написан человеком и может быть проверен и интерпретирован другим человеком. Содержащиеся в статье Аппеля, Хакена и Коха [1] неформальные аргументы, которые объясняют, *почему* положительный результат компьютерной проверки нужно считать завершением доказательства T4K, обеспечивают в большей или меньшей степени глобальную прозрачность данного доказательства. Причина того, что это доказательство тем не менее не кажется достаточно прозрачным, состоит, на наш взгляд, в том, что в нем отсутствует прозрачность промежуточного масштаба, которая позволила бы связать воедино элементарные шаги, реализованные с помощью выполняемой компьютерной программы, и общие соображения, представленные обычным образом с помощью неформальной или полу-формальной математической прозы.

3. Унивалентные основания и пространственная интуиция

Гомотопическая теория типов (ГТТ), которая представляет собой логический каркас УО , позволяет думать о формальных выводах в теории типов Мартина-Лефа (ТТМЛ) как о пространственных гомотопических построениях [8]. Когда выводы в ТТМЛ реализуются в виде исполнимого программного кода (например, на языке AGDA), те же самые пространственные интуиции оказываются применимыми к соответствующему коду. Гомотопическая интерпретация программного кода имеет интуитивный характер (при небольшом числе измерений), который позволяет уточнять формальную структуру соответствующих доказательства, не вникая при этом в мелкие технические детали. Интерпретированный таким образом программный код приобретает новое качество “мезоскопической” эпистемической прозрачности, играющее роль связующего звена между локальной прозрачностью, которая позволяет человеку интерпретировать и понимать небольшие фрагменты программного кода, и общим пониманием того, как данная программа работает и зачем она написана, то есть глобальной прозрачностью. Итак, ГТТ посредством УО обеспечивает представление математических рассуждений, которое

- является полностью формальным в том смысле, что оно использует логическое исчисление со строгим синтаксисом (ТТМЛ или ее аналоги);

- допускает компьютерную реализацию и компьютерную проверку рассуждений (с помощью помощников для доказательств таких как Coq, AGDA или Arend);

- поддерживает интуитивную интерпретацию формализованных рассуждений, которая связывает локальные и глобальные аспекты эпистемической прозрачности компьютерных доказательств подобно тому, как это происходит в случае традиционных геометрических построений циркулем и линейкой.

4. Пример: вычисление фундаментальной группы окружности

Простой, но не тривиальный пример математического доказательства представленный с помощью ГТТ/УО и реализованный на компьютере с помощью AGDA описан в статье Ликаты и Шульмана [4]. Речь идет о теореме алгебраической топологии, которая утверждает, что фундаментальная группа $\pi_1(S^1)$ (топологической) окружности S^1 изоморфна бесконечной циклической группе $\mathbb{Z}$, которая канонически представляется аддитивной группой целых чисел.

Пусть b это произвольная точка окружности S^1. Это суждение формально представляется в ТТМЛ следующей формулой:

$$b : S^1$$

Тогда петли, ассоциированные с выбранной базой, будут иметь простой вид

$$loop : b =_{S^1} b$$

Такая интуитивная геометрическая интерпретация формул распространяется на все последующие шаги построения фундаментальной группы и на последующее доказательство теоремы; та же интерпретация применима с незначительными модификациями к соответствующему программному коду на AGDA. Обычное содержательное доказательство данной теоремы оказывается сопряженным с формальным доказательством таким тесным образом, что обычного эпистемического разрыва между формальным и содержательным доказательством в данном случае не возникает. Компьютерный код (или псевдо-код) играет в таких случаях ту же роль, что и обычные для традиционной математической практики полуформальные символические обозначения. Но возникает важное преимущество, которое состоит в том, что компьютерный код в отличие от обычной математической символики делает возможной автоматическую формальную верификацию математических рассуждений.

5. Заключение

Подход к компьютерным доказательствам основанный на УО позволяет представлять математические рассуждения таким образом, что они оказываются более понятными для пользователей, чем компьютерные доказательства в стиле “черного ящика”, которые не обеспечивают достаточного эпистемического доступа к вычислениям. Важно иметь в виду, что успех компьютерного представления знаний и рассуждений с использованием УО сегодня критически зависит не только (и, на наш взгляд, даже не столько) от технических аспектов вычислительной реализации УО, сколько от успешности проекта УО как новых оснований математики в целом. Какие фрагменты современной математики допускают удобную интуитивно прозрачную переформулировку на языке УО, а какие, возможно, нет, на сегодняшний день остается открытым исследовательским вопросом.

Исследование выполнено при поддержке Российского фонда фундаментальных исследований, грант 19-011-00799

Список литературы

[1] K. Appel and W. Haken, "Every Planar Map is Four Colorable", *Illinois Journal of Mathematics*, **21**:3 (1977), 429–567.

[2] O. Bradley Bassler, "The Surveyability of Mathematical Proof: A Historical Perspective", *Synthese*, **148**:1 (2006), 99–133.

[3] M. Detlefsen and M. Luker, "The Four-Color Theorem and Mathematical Proof", *Journal of Philosophy*, **77**:12 (1980), 803-820.

[4] D.R. Licata and M. Shulman, *Calculating the Fundamental Group of the Circle in Homotopy Type Theory*, 2013, arXiv: 1301.3443.

[5] G. D. Secco and L.C. Pereira, "Proofs Versus Experiments: Wittgensteinian Themes Surrounding the Four-Color Theorem", *How Colours Matter to Philosophy*, ed. M. Silva, Springer, 2017, 289–307.

[6] P. Teller, "Computer Proof", *Journal of Philosophy*, **77**:12 (1980), 797–803.

[7] Th. Tymoczko, "The Four-Color Problem and Its Philosophical Significance", *Journal of Philosophy*, **76**:2 (1979), 57–83.

[8] Univalent Foundations Group, *Homotopy Type Theory: Univalent Foundations of Mathematics*, Institute for Advanced Study (Princeton), 2013, homotopytypetheory.org/book.

Computer-Assisted Proofs and Their Understanding by a Human: the case of Univalent Foundations

Rodin A.V.

The computer-assisted proof of Four Colour Map theorem published by Kenneth Appel, Wolfgang Haken and John Koch back in 1977 prompted a continued philosophical discussion on the epistemic value of computer-assisted mathematical proofs. We show, developing the approach proposed by O.B. Brassler in 2006, how the Univalent Foundations of Mathematics (UF) meets some earlier stressed epistemological concerns about computer-assisted proofs and thus offers a new possibility to fill the gap between computer-assisted and traditional mathematical proofs. We demonstrate the argument with a simple computer-assisted proof from Algebraic Topology.

Keywords: Univalent Foundations, Computer-Assisted Proof, Spatial Intuition

References

[1] K. Appel and W. Haken, "Every Planar Map is Four Colorable", *Illinois Journal of Mathematics*, **21**:3 (1977), 429–567.

[2] O. Bradley Bassler, "The Surveyability of Mathematical Proof: A Historical Perspective", *Synthese*, **148**:1 (2006), 99–133.

[3] M. Detlefsen and M. Luker, "The Four-Color Theorem and Mathematical Proof", *Journal of Philosophy*, **77**:12 (1980), 803-820.

[4] D.R. Licata and M. Shulman, *Calculating the Fundamental Group of the Circle in Homotopy Type Theory*, 2013, arXiv: 1301.3443.

[5] G. D. Secco and L.C. Pereira, "Proofs Versus Experiments: Wittgensteinian Themes Surrounding the Four-Color Theorem", *How Colours Matter to Philosophy*, ed. M. Silva, Springer, 2017, 289–307.

[6] P. Teller, "Computer Proof", *Journal of Philosophy*, **77**:12 (1980), 797–803.

[7] Th. Tymoczko, "The Four-Color Problem and Its Philosophical Significance", *Journal of Philosophy*, **76**:2 (1979), 57–83.

[8] Univalent Foundations Group, *Homotopy Type Theory: Univalent Foundations of Mathematics*, Institute for Advanced Study (Princeton), 2013, homotopytypetheory.org/book.