Унивалентные Основания Математики и компьютерная проверка доказательств

Памяти Владимира Воеводского (1966-2017)

16 октября 2017 г.

Володя

- Трижды исключен из школы;
- 1989: исключен из МГУ за неуспеваемость после 4-го курса;
- 1990: совместная статья с Михаилом Капрановым мотивированная “Эскизом Программы” Гротендика (1984) “∞-группоиды как модель для гомотопической категории”; опубликована в УМН (всего на конец 1990 года у В.В. уже опубликовано 7 статей в научных журналах.);
- 1990: благодаря помощи Михаила Капранова и Давида Каждана В.В. зачислен в аспирантуру Гарвардского университета без подачи заявления и прохождения формального отбора;
- 1992: защита диссертации (Ph.D.) в Гарварде раньше обычного срока и без посещения занятий;

Roggert Dijkgraaf quoting Albert Einstein

“Образование это единственное, что отвлекало меня от учебы.”

- 1995: доказательство гипотезы Милнора (первый препринт);
- 2003: Carlos Simpson (Лаборатория Дьедонне в университете Ниццы) публикует препринт, в котором утверждает, что он нашел контр-пример для основной теоремы Воеводского и Капранова. Воеводский уверен в своем доказательстве и игнорирует этот препринт. Статья Симпсона не публикуется: сообщество подозревает ошибку в контрпримере.
- 2002: Медаль Филдса за доказательство гипотезы Милнора и получение постоянной позиции в Institute of Advanced Studies, Princeton. Продолжение работы в мотивной теории гомотопий примерно до 2010 г.

- 2003: Лекция в Wuhan University (Китай): What is most important for mathematics in the near future?. :
  - Computerized version of Bourbaki;
  - Connecting pure and applied mathematics.
- 2003: Лекция в Bangalore (India): Mathematics and the Outside World;
- 2006: Инагурационная лекция в IAS: Foundations of Mathematics and Homotopy Theory;
- 2006: A Very Short Note on Homotopy λ-Calculus;
- 2010: Лекция на 80-летнем юбилее IAS: What if the current foundations of mathematics are inconsistent?;
- 2011 - 2013: Доклады о Унивалентных Основаниях в университетах Америки, Европы и Азии;
- 2013: Организация большой коллективной программы в IAS по гомотопической теории типов и Унивалентным основаниям. Результат: the HoTT Book. Впоследствии В.В. просит убрать свое имя из списка авторов.

- 2013: В.В. обнаруживает непоправимую ошибку в своей совместной статье с Капрановым 1990-го года: оказывается, что Симпсон в 1998 был прав!
- 2014: Бернайсовские лекции в ETH Zurich: Foundations of mathematics - their past, present and future.
- 2016: Приглашенная лекция на 7-м Европейском математическом конгрессе: UniMath - a library of mathematics formalized in the univalent style. Планируемая, но отмененная публикация в будущей коллективной монографии Reflections on the Foundations of Mathematics (Springer 2018).
- 2017: приглашенный доклад на Логическом Коллоквиуме с Стокгольме.

Зачем нужна компьютерная проверка доказательств?

Нынешняя ситуация, при которой корректность доказательств может быть в лучшем проверена несколькими экспертами, тогда как все остальное научное сообщество и широкая публика вынуждены опираться на *авторитет* этих экспертов , является нетерпимой. Сравни случаи недавно доказанных (?) теорем Пуанкаре, Ферма или открытую ABC-гипотезу. Такая экспертиза не может быть и действительно не является надежной (ср. случай Воеводского-Капранова-Симпсона).

При подобном положении вещей математика теряет свой *объективный характер* и вырождается в эзотерическую доктрину, которая конкурирует на медиарынке с множеством других подобных доктрин, включая религиозные доктрины.

Зачем нужна компьютерная проверка доказательств?

Хотя понятие авторитета играет в научном сообществе некоторую роль, научное знание не основано на мнении авторитетов (“идолы театра” у Бэкона), а включает другие процедуры обоснования, которые должны быть в какой-то форме доступны любому человеку и любому другому мыслящему существу.

Проблема объективного обоснования современного математического знания — имеет как прагматические и технические, так и эпистемологическое и социальное измерения.

Компьютерная проверка решает проблему в ее практическом аспекте, если

- Доказательства пишутся в виде компьютерного кода, причем содержание этого кода остается понятийно прозрачным для того, кто его пишет.
- Код эффективен с вычислительной точки зрения и может быть выполнен с использованием ресурсов существующих компьютеров за небольшое (по обычным человеческим меркам) время.
- Компьютерная технология является эпистемически прозрачной: пользователи понимают принципы работы компьютера и способны правильно оценивать вероятность ошибки.

Воеводский 2006 IAS Lecture

"Ideally, a paper submitted to a journal should contain text for human readers integrated with references to formalized proofs of all the results. Before being send to a referee the publisher runs all these proofs through a proof checker which verifies their validity. What remains for a referee is to check that the paper is interesting and that the formalizations of the statements correspond to their intended meaning."

История идеи:

- Декарт: символическая алгебра и аналитическая геометрия;
- Лейбниц: геометрическая характеристика;
- Гильберт : формальный аксиоматический метод как “инструмент необходимый для любого исследования”

Какие результаты на сегодняшний день:

Исключительно мета-математические включая, например, известные теоремы Геделя о семантической неполноте формальных теорий арифметики.

Эти результаты не имеют *никакой* прямой связи с задачей формализации математических рассуждения с целью их формальной формально проверки.

Почему формальная проверка доказательств еще не стала общей практикой:

НЕАДЕКВАТНАЯ ФОРМАЛИЗАЦИЯ МАТЕМАТИКИ

Проблемы теоретико-множественной формализации:

- Не инвариантна по отношению к изоморфизмам и эквивалентностям высших порядков (проблема Бенацераффа);
- Отождествление доказательства с формальным выводом при отсутствии формального различения между доказательными и бездоказательными дедукциями (Prawitz, Martin-Löf);
- Формальный вывод в ZFC *не* реализуется в форме алгоритмической (вычислительной) процедуры непосредственно.

Принцип изоморфизм-инвариантности :

Для любого утверждения P об объекте X и любого изоморфизма $X \cong X'$ существует утверждение P' об объекте X' такое что P' истинно тогда и только тогда, когда истинно утверждение P.

Нарушение изоморфизм-инвариантности при ZFC-кодировке:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

where

- $i \in \mathbb{N}$;
- $i \in \mathbb{Z}$

В ZFC целые числа кодируются *парами* натуральных чисел. Поэтому две версии формулы для суммы прогрессии (для натуральных и целых чисел) логически *не* эквивалентны.

Решение: комбинация след. элементов

- теория гомотопий;
- теория ∞-группоидов (Гротендик);
- конструктивная теория типов Мартина-Лефа (MLTT);
- реализующий MLTT прувер COQ (after Thierry Coquand).

+ Принцип Унивалентности.

MLTT: Syntax

- 4 basic forms of judgement:
  (i) $A : TYPE$;
  (ii) $A \equiv_{TYPE} B$;
  (iii) $a : A$;
  (iv) $a \equiv_A a'$
- Context : $\Gamma \vdash$ judgement (of one of the above forms)
- no axioms (!)
- rules for contextual judgements; Ex.: dependent product :
  If $\Gamma, x : X \vdash A(x) : TYPE$, then $\Gamma \vdash (\Pi x : X)A(x) : TYPE$

MLTT: Semantics of $t : T$ (Martin-Löf 1983)

- t is an element of set T
- t is a proof (construction) of proposition T ("propositions-as-types")
- t is a method of fulfilling (realizing) the intention (expectation) T
- t is a method of solving the problem (doing the task) T (BHK-style semantics)

Sets and Propositions Are the Same

If we take seriously the idea that a proposition is defined by lying down how its canonical proofs are formed [...] and accept that a set is defined by prescribing how its canonical elements are formed, then it is clear that it would only lead to an unnecessary duplication to keep the notions of proposition and set [...] apart. Instead we simply identify them, that is, treat them as one and the same notion. (Martin-Löf 1983)

MLTT: Definitional aka judgmental equality/identity

$x, y : A$ (in words: x, y are of type A)

$x \equiv_A y$ (in words: x is y by definition)

MLTT: Propositional equality/identity

$p : x =_A y$ (in words: x, y are (propositionally) equal as this is evidenced by proof p)

Definitional eq. entails Propositional eq.

$$\frac{x \equiv_A y}{p : x =_A y}$$

where $p \equiv_{x=_A y} \mathit{refl}_x$ is built canonically

Equality Reflection Rule (ER)

$$\frac{p : x =_A y}{x \equiv_A y}$$

ER is not a theorem in the (intensional) MLTT (Streicher 1993).

Extension and Intension in MLTT

- MLTT + ER is called *extensional* MLTT
- MLTT w/out ER is called *intensional*
  (notice that according to this definition intensionality is a negative property!)

Higher Identity Types

- $x', y' : x =_A y$
- $x'', y'' : x' =_{x =_A y} y'$
- $\ldots$

HoTT: the Idea

Types in MLTT are (informally!) modeled by spaces (up to homotopy equivalence) in Homotopy theory, or equivalently, by higher-dimensional groupoids in Category theory (in which case one thinks of n-groupoids as higher homotopy groupoids of an appropriate topological space).

Обратите внимание на *внелогическую* интерпретацию логического понятия тождества! В аксиоматических теориях в стиле Гильберта различение логических и внелогических символов жестко фиксировано заранее и интерпретации подлежат *только* внелогические символы: ср. понятие сигнатуры у Бурбаки!

Homotopical interpretation of Intensional MLTT

- $x, y : A$
  x, y are points in space A
- $x', y' : x =_A y$
  x', y' are paths between points x, y; $x =_A y$ is the space of all such paths
- $x'', y'' : x' =_{x=_A y} y'$
  x'', y'' are homotopies between paths x', y'; $x' =_{x=_A y} y'$ is the space of all such homotopies
- ...

Point

Definition

Space S is called contractible or space of h-level (-2) when there is point $p : S$ connected by a path with each point $x : A$ in such a way that all these paths are homotopic (i.e., there exists a homotopy between any two such paths).

Homotopy Levels

Definition

We say that S is a space of h-level $n+1$ if for all its points x, y path spaces $x =_S y$ are of h-level n.

Cummulative Hierarchy of Homotopy Types

- -2-type: single point pt;
- -1-type: the empty space $\emptyset$ and the point pt: truth-values aka (mere) propositions
- 0-type: sets: points in space with no (non-trivial) paths
- 1-type: flat groupoids: points and paths in space with no (non-trivial) homotopies
- 2-type: 2-groupoids: points and paths and homotopies of paths in space with no (non-trivial) 2-homotopies
- ...

Propositions-as-**Some**-Types !

Which types are propositions?

Def.: Type P is a *mere proposition* if $x, y : P$ implies $x = y$ (definitionally).

Truncation

Each type is transformed into a (mere) proposition when one ceases to distinguish between its terms, i.e., *truncates* its higher-order homotopical structure.

Interpretation: Truncation reduces the higher-order structure to a single element, which is **truth-value**: for any non-empty type this value is **true** and for an empty type it is **false**.
The reduced structure is the structure of **proofs** of the corresponding proposition.
To treat a type as a proposition is to ask whether or not this type is instantiated without asking for more.

- Thus in HoTT "merely logical" rules (i.e. rules for handling propositions) are instances of more general formal rules, which equally apply to non-propositional types.
- These general rules work as rules of building models of the given theory from certain basic elements which interpret primitive terms (= basic types) of this given theory.
- Thus HoTT qualify as *constructive* theory in the sense that besides of propositions it comprises non-propositional objects (on equal footing with propositions rather than "packed into" propositions as usual!) and formal rules for managing such objects (in particular, for constructing new objects from given ones). In fact, HoTT comprises rules with apply *both* to propositional and non-propositional types.

Univalence

$$(A =_{TYPE} B) \simeq (A \simeq B)$$

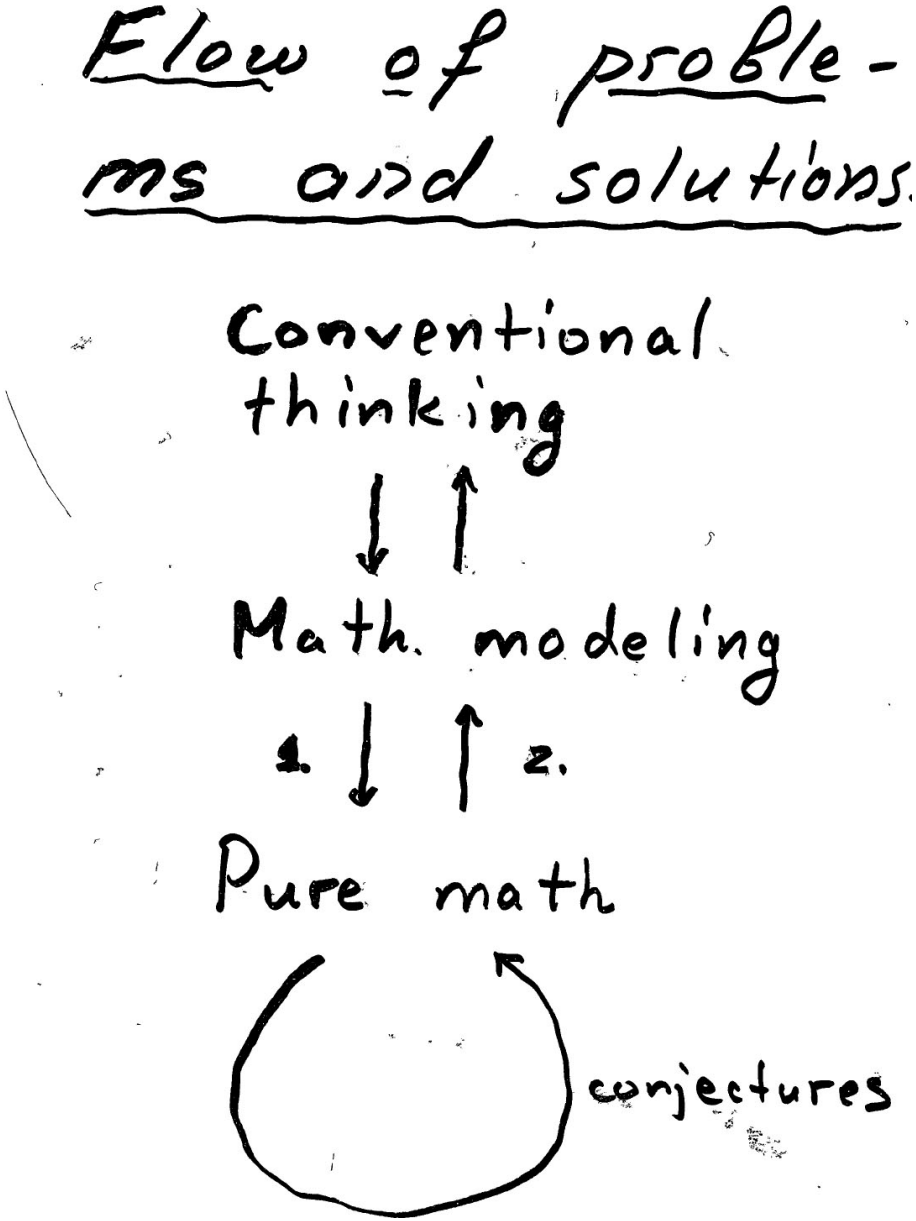
Словами: эквивалентность типов эквивалентна их равенству. Структурализм?

For PROPs: $(p = q) \leftrightarrow (p \leftrightarrow q)$ (propositional extensionality)

For SETs: Утверждения об изоморфных множествах логически эквивалентны (изморфизм-инвариантность)

Univalence implies *functional extensionality*: if for all $x \ \ X$ one has $fx =_Y gx$ then $f =_{X \to Y} g$ (the property holds at all h-levels).

Математика и внешний мир



UniMath Library

https://github.com/UniMath/UniMath