Proof-Verification & Mathematical Intuition

Lecture 2. From Bourbaki to Voevodsky

Andrei Rodin

Summer School ILLUMINATIONS - 2.0, Lukashino, Tyumen region, 30 July - 4 August 2019

1 August

Plan of 2 Lectures :

Plan of 2 Lectures :

1. From Euclid to Hilbert : Brief History of Aximatic Method

Plan of 2 Lectures :

1. From Euclid to Hilbert : Brief History of Aximatic Method
2. From Bourbaki to Voevodsky : Univalent Foundations of Mathematics.

Plan of Lecture 2

Bourbaki

- Architecture of Mathematics 1950
- Structuralism

Internal Logic

Univalent Foundations

- MLTT
- HoTT/UF

the *Elements* (1939 - ?) and its purpose

Systematic presentation of the conceptual core of contemporary mathematics modelled after Euclid, not just a demonstration of the *method* as in Hilbert 1899 book.

Architecture of Mathematics : Manifesto 1950

After more or less evident bankruptcy of the different systems [..] it looked, at the beginning of the present [20th] century as if the attempt had just about been abandoned to conceive of mathematics as a science characterized by a definitely specified purpose and method ; instead there was a tendency to look upon mathematics as a "collection of disciplines based on particular, exactly specified concepts", interrelated by "a thousand roads of communications" (Brunschvicg 1912). [...] Today, we believe however that the internal evolution of mathematical science has, in spite of appearance, brought about a closer unity among its different parts, so as to create something like a central nucleus that is more coherent than it has ever been. The essential aspect of this evolution has been the systematic study of the relation existing between different mathematical theories, and which has led to what is generally known as the "axiomatic method."

Architecture of Mathematics : Manifesto 1950 (cont'd)

What the axiomatic method sets as its essential aim, is exactly that which logical formalism by itself cannot supply, namely the profound intelligibility of mathematics. [..] Where the superficial observer sees only two, or several, quite distinct theories, lending one another "unexpected support" (Brunschvicg :1912) through the intervention of a mathematician of genius, the axiomatic method teaches us to look for the deep-lying reasons for such a discovery, to find the common ideas of these theories, buried under the accumulation of details properly belonging to each of them, to bring these ideas forward and to put them in their proper light.

Example : Group theory

Example : Group theory

- **G1** : $x \circ (y \circ z) = (x \circ y) \circ z$ (associativity of $\circ$)

Example : Group theory

- **G1** : $x \circ (y \circ z) = (x \circ y) \circ z$ (associativity of $\circ$)
- **G2** : there exists an item *1* (called *unit*) such that for all x $x \circ 1 = 1 \circ x = x$

Example : Group theory

- **G1** : $x \circ (y \circ z) = (x \circ y) \circ z$ (associativity of $\circ$)
- **G2** : there exists an item *1* (called *unit*) such that for all x $x \circ 1 = 1 \circ x = x$
- **G3** : for all x there exists x^{-1} (called *inverse* of x) such that $x \circ x^{-1} = x^{-1} \circ x = 1$

Example of proof in the Manifesto

Theorem : Unit in a group is unique.

Proof : Let e, e' be two units of the given group G. Then by **G2**

$$e \circ e' = e = e'$$

, which concludes the proof.

Semantic approach

"Set with a structure" : $< G, \circ >$

Assumes a background Set theory that provides for all intended interpretations of formal axioms and theorems.

Remark : Each algebraic group (identified either up to isomorphism or up to the set-theoretic identity) qualifies as a particular set-theoretic *model* of **G3**. Group theory as a mathematical discipline studies all groups and interesting relations between these groups (cf. Lagrange theorem).

Semantic approach (cont'd)

Thus the Group theory is a theory of set-theoretic (and perhaps some other) models of **G3** but not just an interpreted version of **G3**.

However since **G1-3** interprets into a (formal axiomatic) Set theory, the (informal) Group theory and the rest of Bourbaki's mathematics is *formalisable* (but not formalised !) in the Set theory.

Bourbaki's examples of proofs in the 1950 Manifesto are misguiding since they are not typical ; they are severely oversimplified ! **G1-3** is conventionally referred to and thought of as a *definition* of group concept, not as a foundation of Group theory ! The above theorem "follows from the definition", which is not a typical case. Recall Kant's argument pointing to the Angle Sum theorem !

Example : Kolmogorov & Fomin 1976

Example : Kolmogorov & Fomin 1976

- **enunciation :** Any closed subset of a compact space is compact

Example : Kolmogorov & Fomin 1976

- **enunciation :** Any closed subset of a compact space is compact
- **exposition :** Let F be a closed subset of compact space T

Example : Kolmogorov & Fomin 1976

- **enunciation :** Any closed subset of a compact space is compact
- **exposition :** Let F be a closed subset of compact space T
- **specification :** I say that F is a compact space

Example : Kolmogorov & Fomin 1976

- **enunciation :** Any closed subset of a compact space is compact
- **exposition :** Let F be a closed subset of compact space T
- **specification :** I say that F is a compact space
- **construction :** [Let] $\{F_\alpha\}$ [be] an arbitrary centered system of closed subsets of subspace $F \subset T$.

Example : Kolmogorov & Fomin 1976

- **proof :** [E]very F_α is also closed in T, and hence $\{F_\alpha\}$ is a centered system of closed sets in T. Therefore $\cap F_\alpha \neq \emptyset$. By Theorem 1 it follows that F is compact.

Example : Kolmogorov & Fomin 1976

- **proof :** [E]very F_α is also closed in T, and hence $\{F_\alpha\}$ is a centered system of closed sets in T. Therefore $\cap F_\alpha \neq \emptyset$. By Theorem 1 it follows that F is compact.
- **conclusion :** Thus any closed subset of a compact space is compact. (Which is) the very thing it was required to show.

Mathematical Structures according to the Manifesto

We take here a naive point of view and do not deal with the thorny questions, half philosophical, half mathematical, raised by the problem of the "nature" of the mathematical "beings" or "objects". Suffice it to say that the axiomatic studies of the nineteenth and twentieth centuries have gradually replaced the initial pluralism of the mental representation of these "beings" thought of at first as ideal "abstractions" of sense experiences and retaining all their heterogeneity by an unitary concept, gradually reducing all the mathematical notions, first to the concept of the natural number and then, in a second stage, to the notion of set.

Mathematical Structures according to the Manifesto

This latter concept, considered for a long time as "primitive" and "undefinable", has been the object of endless polemics, as a result of its extremely general character and on account of the very vague type of mental representation which it calls forth ; the difficulties did not disappear until the notion of set itself disappeared (and with it all the metaphysical pseudo-problems concerning mathematical "beings") in the light of the recent work on logical formalism. From this new point of view, *mathematical structures* [my emphasis - A.R.] become, properly speaking, the only "objects" of mathematics.

Mathematical Structuralism versus Set-theoretic Substantialism

Natural numbers after Zermelo and after von Neumann (Benacerraf problem)

Zermelo : $S(x) = x$:

$0 := \emptyset,\ 1 := \{\emptyset\},\ 2 = \{\{\emptyset\}\}, \ldots,$

von Neumann : $S(x) = x \cup \{x\}$:

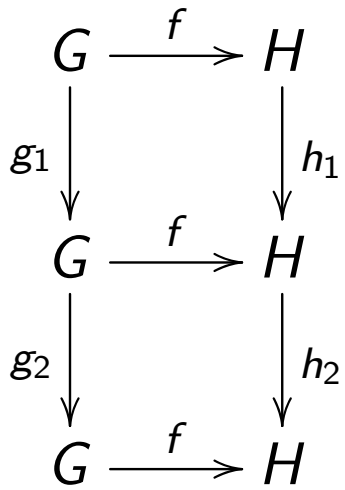
$0 := \emptyset,\ 1 := \{\emptyset\},\ 2 = \{\{\emptyset\}, \{\{\emptyset\}\}\}, \ldots$

Isomorphism of groups

Definition : Groups $< G, \oplus >, < H, \otimes >$ are said to be *isomorphic* when there is invertible map $f : \ G \xrightarrow{\sim} H$, i.e.,

- f maps elements of G to elements of H one-to-one ;
- $f(g_1 \oplus g_2) = f(g_{1)} \otimes f(g_2)$

Isomorphism of groups



Isomorphic groups are the same ! ?

Examples : **the** infinite cyclic group, **the** symmetric group S_2, **the** braid group B_2, etc.

Isomorphism invariance principle

For any statement P about object X and any isomorphism $\phi : X \xrightarrow{\sim} X'$ there is a statement P_ϕ about X' such that P holds if and only if P' holds ($P \leftrightarrow P'$).

Different ways of being equal

However : It is important to specify how two objects are identified !
(examples : S_2, S_3)

Lawvere 1970

The unity of opposites in the title [Quantifiers and Sheaves] is essentially that between logic and geometry, and there are compelling reasons for maintaining that geometry is the leading aspect. At the same time, in the present joint work with Myles Tierney there are important influences in the other direction : a Grothendieck "topology" appears most naturally as a modal operator, of the nature "it is locally the case that", the usual logical operators, such as $\forall$, $\exists$, $\rightarrow$ have natural analogues which apply to families of geometrical objects rather than to propositional functions, and an important technique is to lift constructions first understood for "the" category $\underline{S}$ of abstract sets to an arbitrary topos . We first sum up the principle contradictions of the Grothendieck-Giraud-Verdier theory of topos in terms of four or five adjoint functors [. . .] enabling one to claim that in a sense logic is a special case of geometry.

Voevodsky 2010 on proof-verification

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.

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 (Hilbert, Russell, ..)
- t is a proof (construction) of proposition T (Curry-Howard : "propositions-as-types")
- t is a method of fulfilling (realizing) the intention (expectation) T (Husserl)
- t is a method of solving the problem (doing the task) T (Euclid, 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).

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.

Why HoTT ? (1)

HoTT admits the constructive epistemically-laden proof-theoretic semantics intended by Martin-Löf's Type for MLTT (in a slightly modified form).

Why HoTT ? (2)

The cumulative *h*-hierarchy of types made explicit via the homotopical interpretation supports the distinction between propositional, set-level and higher-level types.

This distinctive feature of HoTT supports formal constructive representation of objects (of various levels) and propositions "about" these objects within the same framework. Each such object serves as a witness/truthmaker for proposition obtained via the propositional truncation of type where the given object belongs.

Why HoTT ? (3)

HoTT comprises a system of formal rules, which are interpreted as logical rules at the propositional *h*-level and as rules for object-construction at all higher levels.

This feature of HoTT supports representation various extra-logical procedures (such as material technological procedures) keeping track of the corresponding logical procedures at the propositional level of representation.

Why HoTT ? (4)

HoTT/MLTT is computationally implementable. Fragments of HoTT/MLTT have been implemented in proof-assistant Coq, program languages AGDA, LEAN and some other products.

Why HoTT ? (5)

HoTT-constructions admit intuitive spatial (homotopical) interpretations that may be used for facilitating human-computer interactions.

Univalence

Univalence Axiom : $(P = Q) \leftrightarrow (P \leftrightarrow Q)$

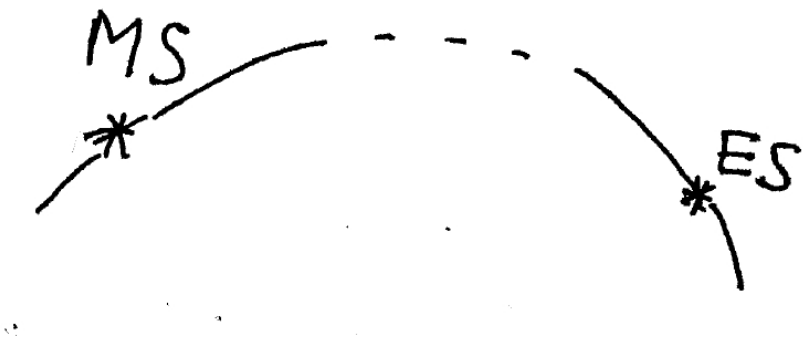
on the propositional level : propositional extensionality

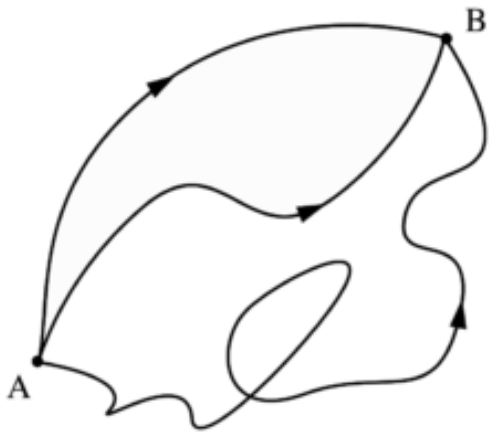
on the set level : realises the isomorphism invariance principle for Bourbaki-style structures BUT is not available in the Bourbaki-style set-theoretic universes !

on higher h-levels : ...

on the ∞-groupoid level : $\omega + 1 = \omega$

The Morning Star is The Evening Star





Conclusion

Symbolic intuition supports a fine-grained analysis of small fragments of mathematical reasoning but not a coarse-grain large-scale view of this reasoning. It is a conceptual mistake to think of this large-scale picture as a mere heuristic device. It has a properly epistemic role, namely, the justificatory role. In order to support the large-scale view other modes of mathematical intuition are needed.

Conclusion

Symbolic intuition supports a fine-grained analysis of small fragments of mathematical reasoning but not a coarse-grain large-scale view of this reasoning. It is a conceptual mistake to think of this large-scale picture as a mere heuristic device. It has a properly epistemic role, namely, the justificatory role. In order to support the large-scale view other modes of mathematical intuition are needed.

In UF the homotopical intuition intermediates between the fine-grained proof structure expressed symbolically as a program code (that allows for computer-assisted verification) and the coarse-grained representation of this reasoning in the user's brain. Shifting between local and global aspects of mathematical reasoning is crucial !

Thank you !