IA038 Types and Proofs

1. History of Math & Motivations

Jiří Zlatuška

February 21, 2023

Nature of Mathematical Objects

- Plato’s “Academy“: “*Let no one who is not a geometer enter*“ – Plato (427-348 BCE)
- Platonism:

1. There are mathematical objects
2. These are abstract objects existing outside of space and time
3. Math objects always existed & are entirely independent od people
4. Math objects do not interact with the physical world in any “causal” way – we cannot change them, and they cannot change us, yet
5. We are somehow able to gain knowledge of them

Prehistory of Formal Reasoning

- Aristotle (384-322 BCE) – Analytica Posteriora as a deductive science from basic truths or axioms
  * Deductive proofs as demonstration arguments in Euclid geometry
  * Logic in the form of syllogisms independent of mathematical/geometrical proofs

- Sufficient for more than two millenia

Logicism

- Gottfried Wilhelm Leibniz (1646-1716)

Mathematical facts as truths of reason

Hoped in "calculus ratiocinator" as a systematic calculational logic for representation of human reasoning (similar to the differential calculus for mathematical physics)

Introduced logical operations (but did not publish this)

- Immanuel Kant (1724-1804) – Critique of Pure Reason

Arithmetic and Geometry as synthetic a priori issues akin to Metaphysics

- Richard J. W. Dedekind (1831-1916) - culmination of arithmetization of Arithmetic and Geometry

Logicism

- Gottlob Frege (1848-1925)
- Begriffsschrift, 1879 (concept notation for pure thought / logic)
- Grundlagen der Arithmetic, 1884
  - ➢ Analyticity of arithmetic truths derived from their
  - ➢ 7+5=12 as analytical truth (contrary to Kant)
- Grundsetze der Arithmetic, Vol. 1, 1893
  - ➢ distinction between sense and reference
  - ➢ introduction of notation for concepts and semantics
  - ➢ symbolic language for expressing everything explicitly & finite set of rules
- Vol. 2 was at the publisher in 1903, when Russel wrote to Frege about the Russel Paradox ($A=\{B: B$ is a set & $B \notin B\}$, and both $A \in A$, and $A \notin A$)

❖ Problems with infinite sets in logicism, also Gödel‘s incompleteness

Formalization of logical inference

- Giuseppe Peano (1858-1932)

Around 1890 formalization of logical inference

Formal rules based on axioms and Modus Ponens (A=>B, A |- B)

- Bertrand Russel (1872-1970)

Principia Mathematica, 1910-13, with Whitehead: expressing axioms as basic truths, and deriving logical truths by Modus Ponens and universal generalization

David Hilbert (1862-1943)
Grundlagen der Geometrie,1899

Four foundational problems:

1. Formalization of mathematical theory
2. Proof of consistency of the the axioms
3. Independence and completeness of the axioms
4. The decision problem: is there a method answering any question in the theory?

David Hilbert

- By 1920's, "Hilbert style" axiomatic approach dominates
- Propositional logic proved complete and decidable
- Predicate logic presented in Hilbert style by Ackermann by 1920

Hilbert Program ~1920

- **Hilbert Program**: expressing higher mathematics in terms of elementary Arithmetics;
  formalizing all Mathematics in axiomatic form together with a proof of completeness
  (finitistic methods, purely intuitive basis of concrete signs)
- P. Bernays, W. Ackermann, J. von Neumann, J. Herbrand
- Ackermann and von Neumann – proof of consistency of number theory, Ackermann thought near completion for analysis
- Hilbert claimed in 1928 in Bologna that the work is essentially completed

Kurt Gödel: completeness of First-Order Predicate Logic

- Completeness of First-Order Predicate Logic stated by Hilbert and Ackermann in 1928
- Kurt Gödel tackled this in his doctoral thesis in 1929
- Thm: Every logical expression is either satisfiable or refutable, aka Every valid logical expression is provable

- Presented as his forthcoming PhD thesis in September 1930 in Königsberg

Kurt Gödel: incompleteness of formal systems

- Also in September 1930 in Königsberg, presented as an "aside" (not a talk on the conference programme)
- The First Incompleteness Thm showing existence of arithmetic formulas neither povable nor refutable in Peano arithmetic
- The Second Incompleteness Thm showing that consistency of arithmetic cannot be proved in Arithmetics itself, $Con(P) \equiv \neg Prov(\lceil 0 \rceil = \lceil 1 \rceil)$

- von Neumann interrupted his lectures on Hilbert proof theory in the Fall of 1930; seeing Hilbert program could not be achieved at all
  → Destruction of Hilbert Program (impossibility of proving consistence of a formal system inside of it)

Intuitionism (constructivism)

- L.E.J. Brower (1881-1966): mathematical knowledge comes from constructing mathematical objects within human intuition; belief that the law of wxcluded middle, or indirect existential proofs are dangerous to the coherence of Mathematics

  Around 1908 – clash with Hilbert, also in “The untrustworthiness of the principles of logic” challenged the belief that the rules of classical logic which came from Aristotle have absolute validity
- Arend Heyting (1898-1980) was his PhD student developing intuitionism further

Gödel and Gentzen

- Translation from Peano arithmetic to intuitionistic Heyting arithmetic by Gödel, in parallel with Gentzen, 1932-33

Gentzen

- Gentzen thesis (1934-35) on analysis of mathematical proofs
- Natural Deduction (intro & elim rules, esp. suitable for intuitionistic logic)

$$\frac{A \quad B}{A \,\&\, B}\ \&\mathrm{I}$$

$$\frac{A \,\&\, B}{A}\ \&\mathrm{E}_1 \qquad \frac{A \,\&\, B}{B}\ \&\mathrm{E}_2$$

$$\begin{array}{c}[A]\\ \vdots \\ \dfrac{B}{A \supset B}\ \supset\mathrm{I}\end{array}$$

$$\frac{A \supset B \quad A}{B}\ \supset\mathrm{E}$$

Gentzen

- Gentzen thesis (1934-35) on analysis of mathematical proofs
- “Sequenzenkalkul”, Sequent Calculus
- Normalization and cut-elimination

Conjunction

$$\frac{\Gamma \rightarrow \Delta, A \quad \Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \,\&\, B}\,\mathrm{R}\& \qquad \frac{A, \Gamma \rightarrow \Delta}{A \,\&\, B, \Gamma \rightarrow \Delta}\,\mathrm{L}\&_1 \qquad \frac{B, \Gamma \rightarrow \Delta}{A \,\&\, B, \Gamma \rightarrow \Delta}\,\mathrm{L}\&_2$$

Implication

$$\frac{A, \Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, A \supset B}\,\mathrm{R}{\supset} \qquad \frac{\Gamma \rightarrow \Theta, A \quad B, \Delta \rightarrow \Lambda}{A \supset B, \Gamma, \Delta \rightarrow \Theta, \Lambda}\,\mathrm{L}{\supset}$$

$$\frac{\Gamma \rightarrow A \quad A, \Delta \rightarrow C}{\Gamma, \Delta \rightarrow C}\,\mathrm{Cut}$$

Gödel and Gentzen

- Gentzen gave an alternative proof of the Incompleteness Thm (written 1939, published 1943) by showing a formula unprovable in Peano arithmetic (thus also showing consistency of Peano arithmetic)
- Gödel's proof of consistency using Dialectica interpretation

(Unclear mutual interaction in 1939.)

Computability and Undecidable problems

- Hilbert (1928): “Entscheidungsproblem”: Is there a general effective procedure deciding whether or not a given formula A of a calculus is provable?
- 1936: Alonzo Church proved on the basis of λ-calculus and Alan Turing on the basis of Turing machines several months later that

  the answer to the Entscheidungsproblem is negative

- Existence of *undecidable problems* in Informatics

Computability and Undecidable problems

- 1936: Alonzo Church proved on the basis of λ-calculus and Alan Turing on the basis of Turing machines several months later that

  the answer to the Entscheidungsproblem is negative

- Existence of *undecidable problems* in Informatics
- Church-Turing thesis (Kleene, 1952) – computable functions / computability

Alonzo Church (1903–1995) and his λ-calculus

- λ-abstraction: making bound variables in function definitions explicit
- λx(M) means definition of a function mapping an argument a into M[x/a] (“formal parameters” in programming languages)

- Operational semantics via rewriting: λx(M)N –> M[x/N]

- Fixed-point Theorem: For each F there is X s.t. FX= X
- There is a fixed-point combitator **Y** s.t. F(**Y**F) = **Y**F

- Proof: **Y** = λf(λx.f(xx))(λx.f(xx))

Church, Turing, and Gödel

- Church using λ-calculus as a formal tool tried to formalize mathematics
- Learning about Gödel's result, claimed that it does not apply to this system
- Kleene - recursive functions
- Rosser - reductions
- Church-Turing thesis (Kleene, 1952) for computable functions / computability:
  - Turing machines
  - λ-definability
  - Gödel's general recursive functions (Princeton, 1934)

Curry-Howard correspondence aka "formulae-as-types"

- Computational semantics for intuitionistic logic

$$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \supset B}\supset\mathrm{I}$$

$$\dfrac{x^A \qquad M^B}{(\lambda x.M)^{A \to B}}$$

$$\dfrac{A \supset B \quad A}{B}\supset\mathrm{E}$$

$$\dfrac{M^{A \to B} \qquad N^A}{(MN)^B}$$

Curry-Howard correspondence aka "formulae-as-types"

- Computational semantics for intuitionistic logic
- Computations = normalization

$$\dfrac{\dfrac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \supset B} \quad A}{B} \quad \to \quad \begin{matrix}A\\ \vdots \\ B\end{matrix}$$

$$\dfrac{\dfrac{x^A \qquad M^B}{(\lambda x.M)^{A \to B}} \quad N^A}{(MN)^B} \quad \to \quad M[x/N]$$

(λx.M)

Curry-Howard correspondence aka "formulae-as-types"

- Computational semantics for intuitionistic logic
- Computations = normalization
- Intuitionistic logic not tied to any philosophy of Mathematics, but corresponds to program execution
- Girard's Linear logic as a Sequent-Calculus-style system capable expressing parallel operations (via proof normalization)

Completing Gödel’s rupture in the structure of mathematics

- Gödel opened a crack in the foundations of Mathematics
- The complement of this rupture lays outside of combinatorial formulation; still within the real of Mathematics
- The “inside” of this crack opened up a new discipline, Informatics; may be thought of as a camouflage of formal logic (proof theory) into fairly applicable computational tool

Proof theory as a basis for constructivistic formulation

- Frege vs. Hilbert concerning Platonism vs. Formalism (Hilbert – Mathematics is invented and best viewed as formal symbolic games without intrinsic meaning)
- Hilbert vs. Brower concerning Formalism vs. Intuitionism
- Constructivism (Kronecker (1823-1891) with “God made the natural numbers, all else is the work of man“, and esp. Andrej Markov who claimed Mathematics should deal exclusively with constructive objects)
- Proof generation as object construction
- Proof simplification/normalization as a computational mechanism (even without underlying formula semantics)

Textbook for this course

Proofs and Types

Jean-Yves Girard, Yves Lafont and Paul Taylor

Cambridge University Press (Cambridge Tracts in Theoretical Computer Science, 7),
ISBN 0 521 37181 3; first published 1989, reprinted with corrections 1990

PDF available from http://www.paultaylor.eu/stable/Proofs+Types.html

Completion Requirements

- Essay on a topic using this concept, developing necessary mathematical details.
- Structure of the essay corresponding to an article introducing the topic, and developing details.
- This may either be something relevant to your work/interest, or e.g. taking some of the results concerning normalization within a suitable formal system, and completing proofs in sufficient mathematical detail.
- 3-5 thousand words (approx. 6-12 pages).