

Proof theory: Part I

Hilbert's Programme

Michael Rathjen

Fischbachau, August 5th - August 9th, 2005

Denn die Pioniere der Mathematik hatten sich von gewissen Grundlagen brauchbare Vorstellungen gemacht, aus denen sich Schlüsse, Rechnungsarten, Resultate ergaben, deren bemächtigten sich die Physiker, um neue Ergebnisse zu erhalten, und endlich kamen die Techniker, nahmen oft bloß die Resultate, setzten neue Rechnungen darauf und es entstanden Maschinen. Und plötzlich, nachdem alles in schönste Existenz gebracht war, kamen die Mathematiker - jene, die ganz innen herumgrübeln, - darauf, daß etwas in den Grundlagen der ganzen Sache absolut nicht in Ordnung zu bringen sei; tatsächlich, sie sahen zuunterst nach und fanden, daß das ganze Gebäude in der Luft stehe. Aber die Maschinen liefen! Man muß daraufhin annehmen, daß unser Dasein bleicher Spuk ist; wir leben es, aber eigentlich nur auf Grund eines Irrtums, ohne den es nicht entstanden wäre.

ROBERT MUSIL: *Der mathematische Mensch* (1913)

A central theme running through all the main areas of **Mathematical Logic** is the **classification of sets, functions** or **theories**, by means of **transfinite hierarchies** whose **ordinal** levels measure their **'rank'** or **'complexity'** in some sense appropriate to the underlying context. In **Proof Theory** this is manifest in the assignment of **'proof theoretic ordinals'** to theories, gauging their **'consistency strength'** and **'computational power'**.

Ordinal-theoretic proof theory came into existence in **1936**, springing forth from **Gentzen**'s head in the course of his consistency proof of arithmetic. To put it roughly, **ordinal analyses** attach ordinals in a given representation system to formal theories.

Proof theory, a major area of mathematical logic, has its roots in Hilbert's "Beweistheorie" - the aim of which was to lay to rest all worries¹ about the foundations of mathematics once and for all by securing mathematics via an absolute proof of consistency - technical results in proof theory are not different from those in any other branch of mathematics, inasmuch as they can be understood in a way that does not at all refer to any kind of (modified) Hilbert programme. In actuality, most proof theorists do not consider themselves pursuing consistency proofs.

¹As, in a rather amusing way, described by Musil in the above quote.

Plan:

- **Hilbert's Programme**
- **Sequent Calculi and Gentzen's Hauptsatz**
- **Infinitary Proof Theory I: Peano Arithmetic**
- **Infinitary Proof Theory II: Kripke-Platek Set Theory**
- **Proof-Theoretic Ordinals and Ordinal Analysis**
- **Applications of Ordinal Analysis**
 1. **Combinatorial Independence Results**
 2. **Classification of Provable Functions**
 3. **Equiconsistency Results**
- **Proof Theory of Stronger Theories: KPi and KPM**
- **Proof Theory of Much Stronger Theories**

Hilbert's Programme:

A Cure for the Foundational Crisis

The end of the nineteenth century and the first three decades of the twentieth was a period of great philosophical ferment amongst some of the most distinguished mathematicians of the day.

Mathematics was afflicted with problems ranging from paradoxes to antinomies. Moreover, new methods of proof introduced into mathematics precipitated an atmosphere of uncertainty regarding the foundations of mathematics.

Inconsistencies in Cantor's and Frege's set theories:

Russell's Paradox (1901): Unrestricted comprehension principle allows one to build sets by collecting all the sets having in common a property P to form a new set

$$R := \{x \mid P(x)\}.$$

Define $R := \{x \mid x \notin x\}$. Then : $R \in R \leftrightarrow R \notin R$.

Non-constructive proof methods

- **Indirect existence proofs** (Hilbert's Basis Theorem)
- **Zermelo's proof** that \mathbb{R} (the reals) can be well-ordered (1904)
- **Abstract notion of function** (In Euler's time functions were explicitly defined via an analytic expression)
- **Brouwer** (1908) rejects the law of excluded middle ($A \vee \neg A$ for arbitrary statements A)
- **H. Weyl**(1918) criticizes impredicative set formation principles as, e.g., *Every bounded non-empty set of reals has a least upper bound.*

Hilbert's Program (1922,1925)

While proofs are the essence of mathematics, they weren't the objects of mathematical investigations. In Hilbert's Proof Theory, **proofs** became mathematical objects sui generis.

- **(i) Codify the whole of mathematical reasoning in a formal theory T .**
- **(ii) Prove the consistency of T by finitistic means.**

The exact meaning of finitistic means was not delineated by Hilbert. Finitistic means form the basis of any scientific reasoning. They do not refer to the actual infinite and do not include any of the objectionable proof methods mentioned above.

Of course mathematics should be consistent, but why is (ii) sufficient for justifying non-constructive mathematics?

Here I have to say a few words about **Hilbert's ontology**:

Real objects: **Natural numbers,**
finite strings of symbols
(something a computer can handle?)

Ideal/abstract objects: **The other objects in mathematics:**
Hilbert spaces, ultrafilters, etc.

Real objects are the things mathematics is about. They do exist. On the other hand, **ideal/abstract objects** do not actually exist; they are just a *façon de parler*.

Method of ideal elements

Solve a mathematical problem concerning a specific structure (realm of objects) by **adjoining new ideal objects** to the structure.

Examples

Elementary Geometry → **points and lines at infinity**

→ **Projective Geometry**

Elementary Number Theory → **number ideals**

→ **Algebraic Number Theory**

Analysis → **ultrafilters**

→ **Set Theory**

Hilbert considered the **method of ideal elements** as vital for progress in mathematics. Different reading of Hilbert's program: **Elimination of ideal elements.**

Mathematical propositions



Real propositions

Ideal propositions

Real propositions are of one of the following forms:

$$\forall x_1 \cdots \forall x_r \quad f(x_1, \dots, x_r) = g(x_1, \dots, x_r);$$

$$\forall x_1 \cdots \forall x_r \quad f(x_1, \dots, x_r) \neq g(x_1, \dots, x_r);$$

$$\forall x_1 \cdots \forall x_r \quad f(x_1, \dots, x_r) \leq g(x_1, \dots, x_r)$$

for reasonably simple number-theoretic functions, where the quantifiers range over the natural numbers.

Examples

- Goldbach's conjecture (Every even number $n > 2$ can be expressed as the sum of two primes.)
- Fermat's conjecture (Wiles' theorem) :
"For all $a, b, c, n \in \mathbb{N}$ such that $a \cdot b \cdot c \neq 0$ and $n > 2$ we have $a^n + b^n \neq c^n$ "
- Riemann's conjecture
- the Four Colour Theorem

Hilbert's Conservation Programme

(Consequence of Hilbert's programme)

If a **real statement** φ is provable in **non-constructive mathematics**, then φ is provable by **finitistic means**.

Theorem

Let φ be a real statement. $F :=$ Finitistic reasoning.

$$T \vdash \varphi \implies F + \text{Con}_T \vdash \varphi.$$

The most important structure in mathematics is

$$\mathfrak{N} = (\mathbb{N}; 0^{\mathfrak{N}}, S^{\mathfrak{N}}, +^{\mathfrak{N}}, \cdot^{\mathfrak{N}}, <^{\mathfrak{N}}),$$

where $0^{\mathfrak{N}}$ denotes zero, $S^{\mathfrak{N}}$, $+^{\mathfrak{N}}$, $\cdot^{\mathfrak{N}}$ denote the successor, addition and multiplication function, respectively, and $<^{\mathfrak{N}}$ stands for the less-than relation on the natural numbers.

Many of the famous theorems and problems of mathematics (including the above examples) can be formalized as a sentence φ of the language of \mathfrak{N} and thus are equivalent to the question whether $\mathfrak{N} \models \varphi$.

Definition

A theory that aims at axiomatizing the structure \mathfrak{N} is **Peano arithmetic, PA**.

$$\text{Language of PA} := \begin{cases} \text{Predicate symbols} & : =, < \\ \text{Function symbols} & : +, \cdot, S \text{ (Successor)} \\ \text{Constant symbols} & : 0 \end{cases}$$

Axioms of PA

- (N1) $\forall x(Sx \neq 0)$
- (N2) $\forall xy[Sx = Sy \rightarrow x = y]$
- (N3) $\forall x[x + 0 = x]$
- (N4) $\forall xy[x + Sy = S(x + y)]$
- (N5) $\forall x[x \cdot 0 = 0]$
- (N6) $\forall xy[x \cdot Sy = (x \cdot y) + x]$
- (N7) $\forall x\neg(x < 0)$
- (N8) $\forall xy[x < Sy \leftrightarrow x < y \vee x = y]$
- (N9) $\forall xy[x < y \vee x = y \vee y < x]$
- (IND) $\varphi(0) \wedge \forall x[\varphi(x) \rightarrow \varphi(Sx)] \rightarrow \forall x\varphi(x)$
for all formulas φ .

First Incompleteness Theorem

Let T be a formal theory (with a decidable set of axioms) containing enough of **PA**. Then there is a **true** sentence φ (**real**) such that:

- (i) If T is consistent, then $T \not\vdash \varphi$.
- (ii) If T satisfies an extra condition called ω -consistency, then $T \not\vdash \neg\varphi$.

Second Incompleteness Theorem

Let T be a consistent formal theory containing arithmetic. Then

$$T \not\vdash \text{Con}_T$$

where Con_T is the sentence asserting the consistency of T .

The First Incompleteness Theorem shows that part (i) of Hilbert's program can only be partially realized. But this may be not so important. Maybe the mathematical statements we are really interested in do not fall under the First Incompleteness Theorem. However, the statement φ is real.

But the second Theorem clearly destroys the Consistency Program. Finitistic reasoning should be formalizable in **PA**. But if **PA** cannot prove it's own consistency, then the consistency of **PA** is not provable by finitistic means.

However, a **Modified Hilbert Program** has been very successful.
Replace “**Finitistic Reasoning**” by “**Constructive Reasoning**”.

Ordinary classical mathematics is consistent from a constructive point of view.

Gentzen's result

Gerhard Gentzen showed that transfinite induction up to the ordinal

$$\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\} = \text{least } \alpha. \omega^\alpha = \alpha$$

suffices to prove the **consistency** of **Peano Arithmetic, PA**. To appreciate Gentzen's result it is pivotal to note that he applied transfinite induction up to ε_0 solely to **primitive recursive predicates** and besides that his proof used only **finitistically justified means**.

Hence, a more precise rendering of Gentzen's result is

$$\mathbf{F} + \text{PR-TI}(\varepsilon_0) \vdash \text{Con}(\mathbf{PA}), \quad (1)$$

where \mathbf{F} signifies a theory that is acceptable in **finitism** (e.g. $\mathbf{F} = \mathbf{PRA} = \text{Primitive Recursive Arithmetic}$) and $\text{PR-TI}(\varepsilon_0)$ stands for transfinite induction up to ε_0 for primitive recursive predicates. Gentzen also showed that his result is best possible in that \mathbf{PA} proves transfinite induction up to α for arithmetic predicates for any $\alpha < \varepsilon_0$.

The compelling picture conjured up by the above is that the **non-finitist** part of **PA** is encapsulated in **PR-TI**(ε_0) and therefore “**measured**” by ε_0 , thereby tempting one to adopt the following definition of **proof-theoretic ordinal** of a theory T :

$$|T|_{Con} = \text{least } \alpha. \mathbf{PRA} + \mathbf{PR-TI}(\alpha) \vdash \text{Con}(T). \quad (2)$$