Obsevations, Truth and Logic

Jaap van Oosten

Department of Mathematics
Utrecht University

Axioma, Groningen
May 9, 2018

Art and Science have the same basic subject matter: *Observations*. Art (visual art): portrays visual perception experiences (perhaps from dreams, fleeting visions, views from afar). The human mind is all too willing to accept the artistic rendering as part of everyday reality.

Figure: Kazimir Malevich – *Eight Red Rectangles* (1915)

Science needs to develop a consistent picture of the world (often, a mathematical picture) which, as far as possible, agrees with the observations.
In both domains: we form a mental picture of the world, become emotionally attached to it, and call it *reality*.
"Realist art", "realistic arithmetic education"...

In mathematics, we also make observations (we see patterns, guess some generality), but our conjectures need *proofs*.
And: we form ourselves a picture of the mathematical universe. So we have:

Observations	Proofs
Interpretation	Foundational Theory

Proofs and picture of the mathematical universe: the subject matter of *Logic*

One of the most basic notions of mathematics: *infinity*. Ancient Greeks: for every number there is a greater prime number; the process of approximating $\sqrt{2}$ by fractions never ends.
The mathematician who pioneered the study of infinity: Georg Cantor (1845–1918).
As soon as there is an infinite set, there is an infinity of infinities: the set of real numbers is "more infinite" than the set of rational numbers; there are more subsets of the real line than there are real numbers, etcetera.

Figure: Georg Cantor

Cantor developed the notion of sets, ordinal and cardinal numbers, transfinite induction,. . .
He formulated the *Continuum Problem*: Is there a set of real numbers which is infinite, yet not in bijective correspondence with either the natural numbers or the real numbers?

Cantor's world of sets is seen by many as a good picture of the mathematical universe.
What about proofs? The mathematician who urged most strongly for a formal theory of proofs, was David Hilbert (1862–1943).

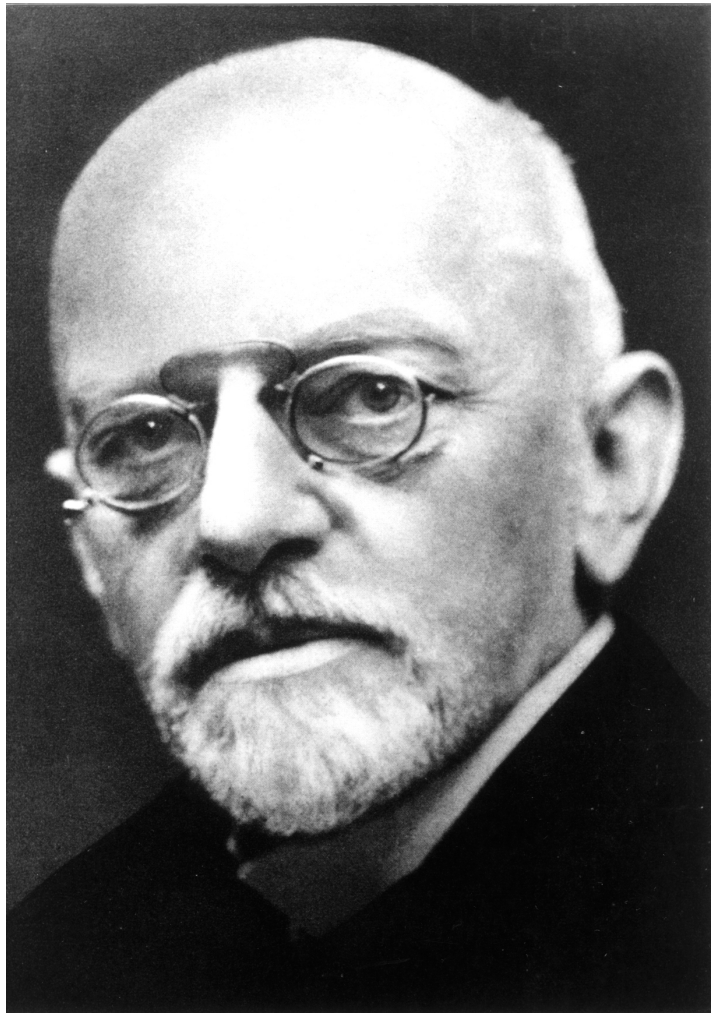


Figure: David Hilbert

Hilbert 1900:

1. Settle the Continuum Problem.
2. Prove that the axioms for the arithmetic of real numbers are free of contradiction.

10. Find an algorithm to decide whether a polynomial equation with integer coefficients has a solution in the integers.

Mathematics had become, during the 1800s, more and more an axiomatic science. Hilbert:

> *When we are engaged in investigating the foundations of a science, we must set up a system of axioms which contains an exact and complete description of the relations subsisting between the elementary ideas of that science.*

But then, we need to assure ourselves that our axiom systems are "free of contradiction"... What does that actually *mean*?

Hilbert 1926 (*On the Infinite*): There are two mathematical worlds:

- an *actual* world, directly accessible to inspection by the mind: the world of the integers and their elementary properties, and the geometry of euclidean space;
- and an *ideal* world, where lots of things live which have nicer properties than the actual things, and whose description is often more elegant.

Often, we arrive at knowledge about the actual world via a detour through the ideal world.

Examples of things from the ideal world:

- Imaginary numbers. Philosophers may doubt their existence but we enjoy the fact that every polynomial has a complete factorization, and the beauty of complex integration by which we also establish facts about the actual world (such as $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$).
- Infinitesimals. Weierstraß's theory of limits and convergence shows how these can be reduced to finite numbers.
- Fractional ideals of number rings. Many rings, like $\mathbb{Z}[\sqrt{-5}]$, lack the desirable property of unique prime factorization; but this is restored if one turns to factorization of fractional ideals; this was shown by Kummer.
- The world of infinite sets.

Hilbert was a great admirer of Cantor's work: he calls Cantor's theory of sets

> *the most admirable flower of the mathematical mind, and one of the highest achievements of purely intellectual human activity whatsoever.*

and:

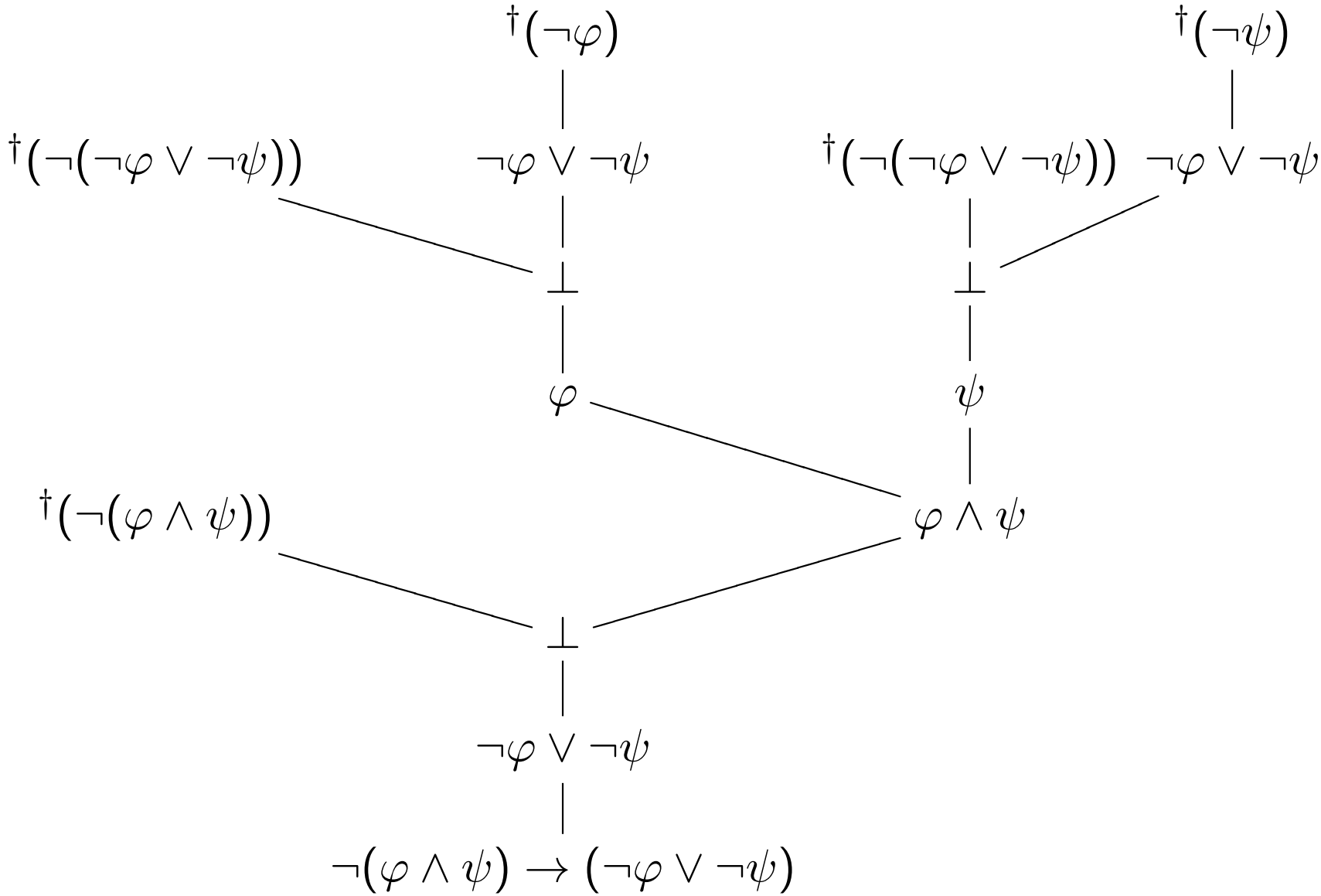
> *from the paradise Cantor has created for us, no one shall expel us.*

Infinite sets are hard to study, but *proofs* about infinite sets are finite things. What should a "theory of proofs" (*Beweistheorie*) achieve?
Hilbert formulated two versions of what later was termed "Hilbert's Programme":

- **Hilbert's Programme, weak form**: proof theory should establish that a detour through the ideal world can never lead to an absurd result.
- **Hilbert's Programme, strong form**: proof theory should establish that every detour through the ideal world can be *eliminated*, resulting in a (probably much longer and less elegant) proof which just mentions concrete things.

Example: Wiles' proof of Fermat's Last Theorem.

Example of a formal proof:



Algorithmic Computation

Another basic activity of mathematicians is: calculate according to an algorithm (long division, determining the gcd of two numbers, construct a perpendicular with ruler and compass,...).
Logic has provided a formal theory of algorithmic computability. The best articulated form was the theory in Alan Turing's paper *On Computable Numbers, with an Application to the Entscheidungsproblem*, 1936.

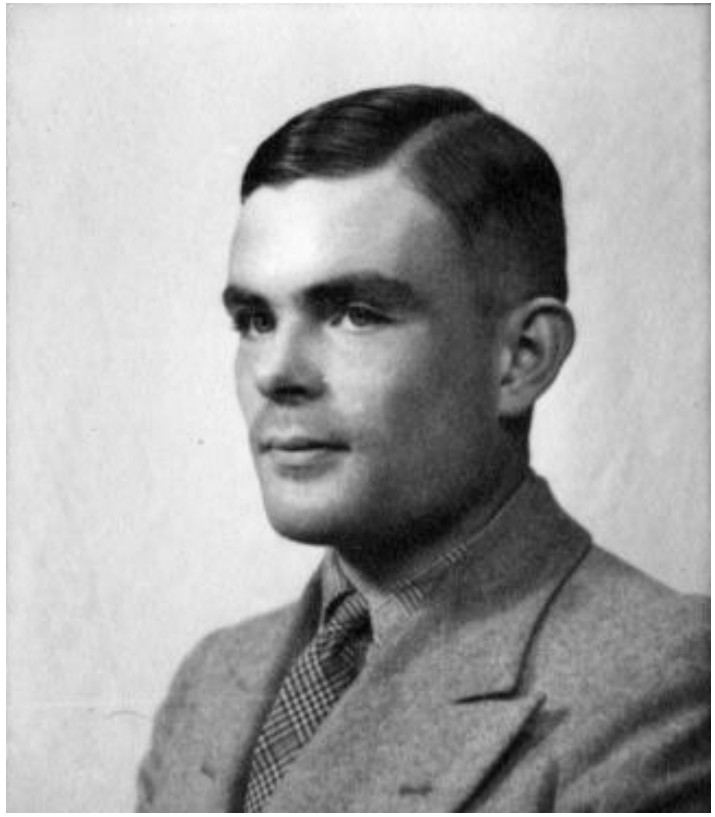


Figure: Alan Turing

Turing:

> *Computing is normally done by writing certain symbols on paper. We may suppose this paper is divided into squares like a child's arithmetic book.[. . .]*
> *I shall also assume that the number of symbols which may be printed is finite.[. . .]*
> *The behaviour of the computer at any moment is determined by the symbols which he is observing, and his "state of mind" at that moment.[. . .]*
> *We will also suppose that the number of states of mind which need to be taken into account is finite.[. . .]*

Turing's analysis of a human being who sets about doing a computation according to an algorithm, led to the definition of a "Turing machine", which consists of:

- a finite set SM of "states of mind";
- a finite set Sy of "symbols";
- a finite set A of "actions";
- a function $SM \times Sy \to A$, defining which action to take when reading a symbol in a particular state of mind.

Among the "states of mind" there is one special state, called the "halting state", after which no action is taken. When the machine reaches the halting state, then what is written on the tape is the "output" of the computation.

Turing's thesis: whatever can be calculated according to some algorithm whatsoever, can be calculated by a Turing machine. This thesis has stood the test of time.

A set A of (n-tuples of) natural numbers is *recursive* if its characteristic function is Turing machine computable.
A set R of (n-tuples of) natural numbers is *semi-recursive* if there is a recursive set A such that

$$R = \{\vec{x} \,|\, \text{for some } n,\ (\vec{x}, n) \in A\}$$

Every recursive set is semi-recursive, but not conversely. A counterexample: Turing's *Halting Set*, the set of tuples $(\vec{x}, n)$ such that the n-th Turing machine, acting on inputs $\vec{x}$, reaches the halting state.

A famous application of the formal theory of computation: Matiyasevich's Theorem

In 1970, the Russian Yuri Matiyasevich (he was 23 years old!) proved the following theorem:

Theorem Let R be a semi-recursive set of n-tuples of natural numbers. There is a polynomial P in $n + k$ variables $X_1, \ldots, X_n, Y_1, \ldots, Y_k$ such that for every n-tuple $\vec{x}$ of natural numbers the following statements are equivalent:

- $\vec{x} \in R$
- the polynomial in k variables $P(\vec{x}, Y_1, \ldots, Y_k)$ has a solution in the integers.

Recall Hilbert's 10th Problem from 1900:

10 Find an algorithm to decide whether a polynomial equation with integer coefficients has a solution in the integers.

Matiyasevich's theorem shows that such an algorithm cannot exist. One can ask: what if the ring of integers is replaced by other number rings? This is an area of continuing research.

Formal Proofs and Computations: working together

The most famous example of a "proof by computer" is the proof of the Four Colour Theorem: for any planar graph one can assign to each vertex one of four "colours" such that no two vertices which are linked (have an edge between them) get the same colour.
This was proved by Appel and Haken in 1976 with the help of enormous computer calculations; however, there were some errors.
Several mathematicians were not convinced.
What is the risk? Just as there is no test whether a Turing machine with given input will ever reach the halting state, there is no test whether a computer program, even if it appears to work, *performs the function it was designed for*.
But then, also extremely long "human" proofs arouse suspicion.
Chess players say: "long analysis, wrong analysis".
A typical mathematical paper is already a worthy assignment for a bachelor thesis.

Other examples of very long proofs:
Feit and Thompson (1963): every finite group of odd order is solvable.
Hales: proof of the Kepler Conjecture (no packing of congruent balls in 3-dimensional Euclidean space can have density greater than the so-called "cannonball arrangement".

Solution: Formal Proof Verification

Write out a *complete* formal proof of the theorem. This can now be done with the help of "proof assistants" (e.g., Coq). The computer can check the correctness of a formal proof.

Why is this any more trustworthy?

A proof system is usually *small*: fits on two A4 sheets. A program which checks that all proof rules have been applied correctly, can be so short that it is humanly verifiable.

Hales: *It has been necessary to [. . .] retool the foundations of mathematics for practical efficiency, while preserving its reliability and austere beauty*.

Other Foundations?

Is “Cantor’s Paradise” the only possible view on the mathematical universe?

A recent proposal (Voevodsky et al): Homotopy Type Theory.

Homotopy Type Theory forces us to think about “equality”.

Professor Whitehead writes in his last book that if we begin to ask ourselves the meaning of the simple word "equal" we find ourselves plunged into abstruse modern speculations concerning the character of the universe.
(E. Cunningham)

Homotopy Type theory sees the world organized in “path spaces”: the “equality” of two elements is testified by the existence of a path between them.

Appendix: Truth?

Reverting to the Cantor's Continuum Problem: is there a set of reals A which is infinite, yet not in bijection with either $\mathbb{N}$ or $\mathbb{R}$?

Cantor's speculation: *no*. This is the *Continuum Hypothesis*.

Gödel proved in 1938: the Continuum Hypothesis cannot be refuted.

Cohen proved in 1963: the Continuum Hypothesis cannot be proved.

Gödel asked: but is it *true*?