Finitism and Incompleteness

Ted Sider
Philosophy of Mathematics

1. Hilbert's program

1.1 The need for consistency proofs

In standard logic, any contradiction $P \wedge \sim P$ implies every statement Q:

1. $P \wedge \sim P$ (suppose)
2. P (from 1)
3. $P \vee Q$ (from 2)
4. $\sim P$ (from 1)
5. Q (from 3, 4)

So a deductivist wants consistent axiom systems—systems from which no contradiction can be proven. Hilbert eventually wanted *proofs* that axiom systems are consistent.

Consistency proofs would answer concerns that analysis and set theory, which traffic in infinity, are inconsistent.

> The idea behind the programme is to carefully and rigorously formalize each branch of mathematics, together with its logic, and then to study the formal systems to make sure they are coherent" (Shapiro, p. 159).

1.2 Consistency proofs using models

Poincaré's disk model shows a certain nonEuclidean set of axioms to be consistent. (If they proved a contradiction, then since proofs depend only on logical form, a contradiction would need to be true when 'point', 'line', and 'distance' mean what they do in the model.)

But this kind of proof assumes the consistency of the theory used to talk about the elements in the model—in this case, analysis—so it can't be used if that theory's consistency is at issue.

1.3 Finitism

To show that a modern, formalized mathematical theory is consistent, we need only show that no proof contains a contradiction—a line of the form "$P \wedge \sim P$". And proofs are finite objects, so Hilbert thought that an especially secure sort of mathematical reasoning, called *finitary reasoning*, could establish this.

Finitary reasoning deals with finite objects, whose properties our minds are capable of directly apprehending.

Examples:

Finitary: reasoning about particular natural numbers (which he regarded as terms: 1 is the stroke, "|", 2 is "||", 3 is "|||", etc.)

Finitary: "for all m and n, $m + n = n + m$"

Not Finitary: "There exist natural numbers a, b, c, and a natural number n that is greater than 2, such that $a^n + b^n = c^n$."

Finitary: "There exist natural numbers a, b, c, all less than $5,000,000$ and a natural number n that is greater than 2 but less than $5,000,000$, such that $a^n + b^n = c^n$."

Finitary: reasoning about particular proofs, such as "this particular sequence of formulas is a legal proof"

Not finitary: "there exists a proof of Fermat's last theorem"

Finitary: "there exists some proof with less then one million characters of Fermat's last theorem".

1.4 An example consistency proof

Let's prove that no contradiction can be proven in the following system of propositional logic. It has these axioms:

$$A \to (B \to A) \tag{PL1}$$
$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \tag{PL2}$$
$$(\sim B \to \sim A) \to ((\sim B \to A) \to B) \tag{PL3}$$

and one rule of inference, modus ponens: $\dfrac{A \qquad A \to B}{B}$

Step 1: define a contradiction as a sentence of the form $\sim(A \to A)$.

Step 2: define a *truth-value-assignment* as a way of associating exactly one of the numbers 1 and 0 to each sentence letter in a given proof.

Step 3: give these rules for determining the truth values of complex formulas:

- $\sim A$ is 1 if A is 0, and 0 if A is 1
- $A \to B$ is 1 if A is 0 or B is 1, and 0 if A is 1 and B is 0

Step 4: show that all axioms are 1 in every truth-value assignment. E.g.:

1. Suppose for reductio that some formula of the form $A \to (B \to A)$ is 0 under some truth value assignment.
2. Then A is 1 in that assignment and $B \to A$ is 0
3. But if $B \to A$ is 0, A must be 0, which contradicts the fact that it is 1

Step 5: show that if the premises of modus ponens are both 1, then so is its conclusion:

1. Suppose $A \to B$ is 1. Then either A is 0 or B is 1.
2. Suppose also that A is 1 as well. Thus A is not 0. But then given the previous step, B is 1.

Step 6: conclude from steps 4 and 5 that every line in every proof is 1 in any truth-value assignment

Step 7: conclude from step 6 that $\sim(A \to A)$ can never be 1. (Otherwise $A \to A$ would be 0, and so A would be 1 and 0.) So it can never occur in any proof.

2. Incompleteness

First incompleteness theorem Any "minimally strong" axiomatic system is incomplete: for some sentence, neither it nor its negation can be proven

Second incompleteness theorem No "slightly more than minimally strong" axiomatic system can prove its own consistency

2.1 Gödel numbering

Gödel numbering/coding: assigning a unique number to each string of symbols in a certain language.

Language of arithmetic: the language with the symbols 0, $'$ (for successor), $+$, and $\times$. Some formulas:

$$\forall n\, 0 \neq n'$$
$$0 + 0'' = 0''' \times 0''''$$
$$\forall x \forall y\; x + y = y + x$$

Each of these formulas would have some code. E.g., maybe 5, 47, and 7,000,000.

Also *sequences* of strings of symbols get codes. E.g., maybe the first of these has the code 67 and the second has the code 4,865,215:

1. $0 + 0'' = 0''' \times 0''''$
2. $0 + 0 = 0$
3. $\forall x \exists y\; x = y$

1. $\forall n\, 0 \neq n'$
2. $0 \neq 0'''$

2.2 Representing metalogic in arithmetic

Given any coding, any property of strings has a corresponding property of numbers. E.g., maybe the strings with the property *being a formulas containing at least one quantifier* just happen to be all and only the strings whose code is an even number. Then *evenness* is the corresponding arithmetic property.

Similarly, the property of *being a sequence of formulas that counts as a legal proof from the Peano axioms* has a mathematical counterpart: the property of numbers that are the codes of sequences of formulas that are legal proofs from the Peano axioms.

2.3 Formalizing metalogic in the language of arithmetic

For any property of strings and its arithmetic counterpart, we might produce a formula in the language of arithmetic that "formalizes" the arithmetic counterpart. E.g., if evenness is the arithmetic counterpart of being a formula with at least one quantifier; then the corresponding formula in the language of arithmetic would be:

$$\exists y\ x = y \times y$$

This lets the language of arithmetic "talk about itself"! For this sentence:

$$\exists x \exists y\ x = y \times y$$

in a sense "says" that some formula in the language of arithmetic contains a quantifier.

Another example. Let T be some axiomatic system for arithmetic. Suppose some formula T-Proof(x) formalizes the arithmetic property of *being a number that is the code of a sequence of formulas that counts as a legal proof in* T; and suppose that some formula Contains-contradiction(x) formalizes the arithmetic property of *being the code of a sequence of formulas that contains some contradiction*. Then this sentence "says" that T is consistent:

$$\sim\exists x(\text{T-Proof}(x) \wedge \text{Contains-contradiction}(x))$$

2.4 First incompleteness theorem

Let T be some "minimally strong" formal system, in that:

- The language of T includes the language of arithmetic
- The axioms of T are "effectively decidable"
- A certain minimal amount of arithmetic can be proven from the axioms of T.

For any formula, A, let $\ulcorner A \urcorner$ be the term that consists of "0" followed by n successor signs:

$$\overbrace{0''\ldots'}^{n \text{ of these}}$$

Gödel came up with a formula Provable(x) which "says in T" that x is provable in T, meaning that:

(P) if A is provable in T then Provable($\ulcorner A \urcorner$) is provable in T

Then Gödel showed how to construct a sentence, G, that "says" *of itself* that it is not provable, in that this is provable in T:

$$G \leftrightarrow \sim\text{Provable}(\ulcorner G \urcorner) \qquad (*)$$

Part of the proof that if T is consistent, neither G nor its negation is provable in T:

> Suppose that T is consistent and that G *is* provable. Then by (P), Provable($\ulcorner G \urcorner$) is provable. But also, since (*) is provable, $\sim$Provable($\ulcorner G \urcorner$) is also provable, which contradicts the fact that T is consistent. Therefore G is not provable.

2.5 Second incompleteness theorem

In the previous section we showed this conditional statement to be true:

> If T is consistent then G is not provable

Gödel showed that if T is slightly more than minimally strong, in that certain proofs by induction can be given in T, then the argument of the previous section can be *formalized in* T, in that the following sentence is provable in T:

$$\text{CON} \rightarrow \sim\text{Provable}(\ulcorner G \urcorner) \qquad (**)$$

where CON is the sentence $\sim\exists x(\text{Proof}(x) \wedge \text{Contains-contradiction}(x))$—a sentence that formalizes in T the claim that T is consistent. We can now argue as follows:

i) Suppose for reductio that CON is provable.

ii) Then since (**) is provable, so is $\sim$Provable($\ulcorner G \urcorner$)

iii) Then, since (*) is provable, so is G

iv) But we earlier showed that G is *not* provable. Therefore, CON is not provable. That is, T cannot "prove its own consistency"

This is fatal to Hilbert's program. His finitary methods of proof can all be formalized in a "slightly more than minimally strong" theory, T. So if his methods succeeded in proving the consistency of T, one could prove the

consistency of T within T. Since that's impossible, it follows that Hilbert's methods cannot prove the consistency of T. And so they certainly can't prove the consistency of arithmetic (since a proof of the consistency of arithmetic would ipso facto be a proof of T, which is a part of arithmetic), let alone stronger theories like analysis and set theory.