Lecture 17
Discussion of Incompleteness

Michael Beeson

Discussion of incompleteness

- Hilbert believed that every mathematical problem has a solution, and that we can find the solution to any given problem, if we are smart and industrious enough.
- Gödel's incompleteness theorems cast doubt on this proposition.
- In this section we will focus on the first half-century of attempts to wiggle out of this predicament.

What about making the theory stronger?

- Gödel's original result was for Russell and Whitehead's theory, as set forth in *Principia Mathematica*, which was then the gold standard for formalization.
- But it soon became apparent that the incompleteness phenomenon depends only on the recursive axiomatizability and consistency of the theory.
- Well, we certainly don't want to give up consistency, and mathematics without a listable set of axioms would hardly be mathematics as we know it.

A hierarchy of stronger and stronger theories

Nevertheless, we can try to create a stronger-and-stronger sequence of theories, possibly exhausting all true sentences in the limit, but axiomatizable at each stage. Here is one way we could try this. Suppose we have a way of strengthening a theory. We already have two good ways to strengthen a theory T:

- Add Con_T to T
- Add the reflection principle $\mathrm{Pr}_T(\overline{\ulcorner A \urcorner}) \supset A$ to T

Let T^* denote T strengthened in one of these (or some other) way. Then we can form a progression of theories by

$$T_0 = \mathbf{PA}$$

$$T_{n+1} = T_n^*$$

Question: Is there a true formula A that is not provable in any T_n? Yes, there is, because the union of the T_n is recursively axiomatizable.

Ordinals

In set theory one considers "infinite numbers" known as ordinals. These numbers are usually denoted by Greek letters (except for the ordinary integers, which count as ordinals too). They are linearly ordered. The rules defining them are

- 0 is an ordinal
- If α is an ordinal then α', often written $\alpha + 1$, is an ordinal.
- $\beta < \alpha'$ if and only if $\beta < \alpha$ or $\beta = \alpha$.
- If α_n is an increasing sequence of ordinals then there is an ordinal λ which is greater than all α_n, but less than any other ordinal greater than all α_n. λ is a "limit ordinal", i.e. not the successor of any ordinal.

Here are some examples:

- The limit of the sequence $1, 2, 3, \ldots$ is called ω.
- After that we have $\omega + 1, \omega + 2, \ldots, \omega + \omega = \omega \cdot 2$.
- $\omega + \omega + \omega \ldots = \omega \cdot \omega = \omega^2$.
- $\omega^2, \omega^3, \ldots, \omega^\omega, \ldots$.

There are more ordinals than names so there is no end of this game. The name of the game is "ordinal notations."

Transfinite Progressions

But the idea occurred to Turing to extend the progression of theories based on extensions by consistency or reflection principles into the transfinite.

$$T_{\alpha+1} = T_{\alpha}^{*}$$

and for λ a limit ordinal,

$$T_{\lambda} = \bigcup_{\alpha<\lambda} T_{\alpha}$$

Turing studied these transfinite progressions. Later Tarski's student Feferman (one of my teachers) wrote his thesis and an early paper about these progressions. There are two results:

(1) for a suitably chosen progression, we can get all true sentences of the form $\forall x\, A$ with A bounded;

(2) but we still don't get all true formulas.

Second-order arithmetic

- Another possibility is to start axiomatizing more of mathematics than number theory.
- We will now describe a theory that is important in logic, namely $\mathbf{Z_2}$, which is sometimes called “analysis”.
- $\mathbf{Z_2}$ has a two-sorted language, with one sort of variables for numbers, and the other sort for sets of numbers (in the “intended interpration”).
- There is one predicate $n \in X$ that links the two sorts of variables.
- Customarily one uses lower-case letters to range over variables of the first sort, and upper-case letters to range over variables of the second sort.
- Both second-order arithmetic and analysis contain the axioms of $\mathbf{PA}$.
- A sentence of this language is called “arithmetical” if it does not contain any set quantifiers, i.e. no quantifiers over variables of the second sort. It may contain free set variables.

The axioms of $\mathbf{Z_2}$

- The axioms of $\mathbf{PA}$
- The schema of mathematical induction, extended to all formulas of the language of $\mathbf{Z_2}$
- The *comprehension axioms* (one for each formula $A(n)$ that does not contain X)

$$\exists X \forall n \, (n \in X \equiv A(n))$$

Intuitively $X = \{n : A(n)\}$.

Analysis

- The reason that $\mathbf{Z_2}$ is called “analysis” is that the theory of the real numbers, and piecewise continuous functions of the real numbers, can be formalized in $\mathbf{Z_2}$, using pairs or triples of integers to describe rational numbers, and sets or sequences of rational numbers to define real numbers. Continuous functions can be described by their values on the rationals.
- Since $\mathbf{Z_2}$ is a recursively axiomatizable theory, the incompleteness theorems apply to it.
- Logicians have nevertheless had a lot of fun analyzing the various subtheories of $\mathbf{Z_2}$ and comparing their strengths, both to each other and to various mathematical theorems. For example, we could restrict induction and comprehension to only arithmetical formulas; and there are dozens of other interesting systems. See Simpson’s book *Reverse Mathematics*.

Real-closed fields

- Gödel threw us rudely out the gates of Hilbert's paradise, and after a while, the new realization of our situation began to sink in.
- Tarski brought a ray of sunshine, by discovering a theory weak enough that Gödel's theorem does not apply, yet strong enough to formalize high-school algebra and Euclidean geometry.
- Tarski was able to prove that, in contrast to $\mathbf{PA}$, this theory is decidable and complete!
- So incompleteness applies to number theory, but not to algebra and geometry, at least, ordinary Euclidean geometry and high-school algebra.

Ordered fields

We describe a theory known as "ordered fields."

- One important model is the real numbers $\langle \mathbb{R}, +, \cdot, \mathcal{P}, 0, 1 \rangle$, where $\mathcal{P}(x)$ holds if and only if $0 < x$.
- The language of this theory has constants 0 and 1, binary function symbols $+$ and $\cdot$, a unary relation symbol $P(x)$ (for "positive").
- The axioms say that the sum and product of positive elements is positive, and that $+$ and $\cdot$ satisfy the field axioms, i.e. both are commutative and associative, the distributive law holds, there are additive inverses and nonzero elements have multiplicative inverses.
- Technically $x < y$ is defined as $\exists z \, (P(z) \wedge x + z = y)$.

Tarski's theory RCF of real closed fields

The axioms of RCF are the axioms of ordered fields, plus the axiom that positive elements have square roots:

$$P(x) \supset \exists y\,(x = y \cdot y)$$

and the axiom schema that every non-constant polynomial of odd degree has a root:

$$\exists x\,(a_0 + a_1 \cdot x + \ldots a_n x^n = 0) \vee (a_1 = 0 \wedge \ldots a_n = 0)$$

where x^n, for a fixed integer n, abbreviates the left-associated product of x, taken n times.

- Tarski proved that RCF is complete and decidable.
- He also gave a first-order theory of Euclidean geometry and showed that its models are all of the form F^2, planes over a real-closed field F.

Expressive power of RCF

- It is possible to express some interesting and complicated problems in the language of RCF, so there may have been a flicker of hope to use Tarski's decision procedure to solve such problems.
- For example, problems about sphere-packing. Is the usual way of packing oranges really the densest?
- All geometry problems, e.g., the medians of any triangle meet in a point.
- There are unsolved problems that can be expressed in this language.

Computational intractability of RCF

- Tarski's procedure was worse than double-exponential in the size of the formula to be decided.
- Later it was shown that any decision procedure has to be at least as slow as double exponential in the number of variables.
- Such procedures have been discovered and implemented, but four or five variables is about the practical limit, and no interesting problems have been solved this way.
- See Section 10 of The mechanization of mathematics, in Teuscher, C. (ed.) Alan Turing: Life and Legacy of a Great Thinker, pp. 77-134. Springer-Verlag, Berlin Heidelberg New York, 2003. for further discussion and examples. If you're reading this online, the blue title is a link.

Set Theory

- Zermelo-Frankel set theory is also a first-order theory, and hence it is subject to the incompleteness theorems.
- Somewhat in the spirit of the transfinite progressions of theories mentioned above, set theory has explored the possibility of adding new axioms to increase the strength of the theory. We have inaccessible cardinals and measurable cardinals and other "large cardinal axioms". These fade into the infinite distance like railroad tracks. Even if one believes them, the augmented theories still are subject to the incompleteness theorems.
- One cannot, however, entirely dismiss these axioms as having no concrete content, because, according to the incompleteness theorems, every time we assume a stronger large cardinal axiom, we prove more *arithmetical* theorems.
- For example, if we assume Z_2 we can prove Con_{PA}, and if we assume a measurable cardinal, we can prove Con_{ZF}, and these consistency statements are fundamentally statements about the integers and addition and multiplication.

Independence of AC and CH: work of Paul Cohen

- If we cannot escape the facts exposed by the incompleteness theorems, we can try to minimize their significance.
- The propositions shown to be unprovable by the proof of the incompleteness theorem are said to be “artificial” assertions such as “would never arise in the course of normal mathematics.” It was therefore alleged that incompleteness was irrelevant to mathematics as practiced by mathematicians.
- This claim was put to death by Paul Cohen, who showed in 1963 that the axiom of choice is unprovable in ZF, and the continuum hypothesis is unprovable in **ZFC**. (Gödel had shown in the forties that both AC and CH are consistent with ZF.)
- Since these questions had arisen at the dawn of set theory and been the focus of much mathematical effort, it was no longer possible to maintain that independence results were irrelevant to mathematics.

No escape from Cohen's results by large cardinal axioms

- Moreover, Cohen's method extends to all known large cardinal axioms, leaving us in complete ignorance about the truth of AC and CH, assuming that we still believe that they have a definite truth value, which we just don't know.
- Others have decided that our notion of "set" is simply not clear enough to settle these issues, so perhaps AC and CH do not have definite truth values. On this view, we understand sets well enough to work with real numbers, but not well enough to work with the complicated sets involved in large cardinal theory, etc.
- This view is perhaps bolstered by the fact that before Russell's paradox, we thought that our intuition gave us evidence for the unrestricted comprehension axiom

  $$\exists x \forall y \, (y \in x \equiv \phi(y))$$

  whenever ϕ does not contain x. But Russell showed that axiom is inconsistent.

A personal story

In about 1969, while I was a graduate student, Ken Kunen went on the lecture circuit championing a new and powerful axiom of infinity, which said "there is a non-trivial elementary embedding of the universe into itself."

He and others derived more and more consequences from this new axiom–until one day they derived the strongest possible consequence, $0 = 1$.

So much for the "intuition" that said such an embedding should exist.

Hilbert's Tenth problem

- A Diophantine equation is an equation between polynomials (in several variables) with integer coefficients, which is to be solved in integers.
- Hilbert's tenth problem asks whether there is an algorithm to determine whether a given Diophantine equation has a solution or not.

Diophantine predicates

Definition

A Diophantine predicate (on the integers) is one defined by a formula of the form

$$P(z) \leftrightarrow \exists \mathbf{x}\, A(z, x) \qquad \text{where } A \text{ is quantifier-free.}$$

Such a formula is called a Diophantine formula.

Contrast that with the definition of a Σ_1^0 predicate, which has the same form except that A only has to be a bounded formula, not a quantifier-free formula. Thus every Diophantine predicate is Σ_1^0, but the converse was for decades an open question.

If every Σ_1^0 predicate were Diophantine, then solving the halting problem can be reduced to solving a Diophantine equation, so Hilbert's Tenth would be solved in the negative.

Solution of Hilbert's Tenth

It is now known that every Σ^0_1 predicate is indeed Diophantine. Here is how that happened:

- First, in a series of papers, Davis, Putnam, and Julia Robinson showed that every Σ^0_1 predicate is "exponential Diophantine", which is like Diophantine except a symbol for exponentiation is allowed.
- Then Matiyesevich gave a Diophantine definition of the exponential function, using something in number theory called Pell's equation.
- The theorem is now called the DPRM theorem:

Theorem (DPRM)

Every Σ^0_1 predicate is Diophantine

Implications of DPRM for incompleteness

- Even after Cohen's work, it was still possible to maintain that the incompleteness theorems are irrelevant at least as far as number theory goes.
- Indeed, the diagonal method produces "artifical" examples that would not come up in number theory.
- It is pretty hard to claim that Diophantine equations are irrelevant to mathematics.
- Therefore the unsolvability of Hilbert's Tenth is a nail in the coffin of Hilbert's idea that we should be able to solve any problem.

Implications of DPRM for incompleteness

- Nevertheless, it is true that the universal Diophantine equation has more variables, or higher degree, or both, than equations that have been considered by number theorists.
- That is not surprising, given that number theorists have yet not discovered decision procedures that even cover the class of equations of the form $x^3 + y^3 + z^3 = c$. They have enough to work on without considering more complicated equations.
- Perhaps it is like saying that it is irrelevant if you are in prison, if you do not have the strength to walk to the perimeter wall anyway. But that is not an encouraging line of thought!

Further implications of DPRM

- The proof of DPRM can be formalized in $\mathbf{PA}$.
- Therefore every Σ^0_1 formula is provably equivalent to a Diophantine formula.
- Con_{PA} is equivalent to the negation of a Σ^0_1 formula.
- So there is a polynomial $f(\mathbf{x})$ of several variables $\mathbf{x}$ that has a solution in integers if and only if $\mathbf{PA} \vdash 0 = 1$.
- The arithmetical relations specified in the polynomial encode the rules of proof of $\mathbf{PA}$!

Unprovable theorems about Diophantine equations

- From the formalized version of DPRM, we see that there are many true but unprovable formulas of the form $\forall \mathbf{x}\, f(\mathbf{x}) \neq 0$.
- Here, as above, we abuse notation, in that f is allowed to have positive or negative coefficients. To be more precise, we should write $f(\mathbf{x}) \neq g(\mathbf{x})$, and it requires an exercise to show that only one such equation is necessary.
- There is a Diophantine equation whose non-solvability expresses the consistency of $\mathbf{PA}$.
- There is another Diophantine equation whose non-solvability expresses the consistency of $\mathbf{Z_2}$, and yet another for **ZFC**.
- Nevertheless, mathematicians in the last stages of denial can still maintain that such Diophantine equations are rare and would never come up naturally. (But wasn't it a fairly natural way that they did come up?)

Dependence of the incompleteness theorems on the axiomatization of T

Here we point out an obvious, but philosophically interesting, consequence of the incompleteness theorems.

Theorem

There is a formula A of one free variable m such that, for any consistent recursively enumerable theory T, Con_T is expressed by $A[m := \bar{e}]$, where e is an index of a Turing machine that enumerates the axioms of T.

Proof The function $\mathrm{Prf}_T(k, x)$ can be written as a Σ^0_1 formula with a free variable m as in the theorem, since the formula that expresses "y is the Gödel number of a axiom of T" has the form

$$\exists x, k \, (\mathbf{T}(m, x, k) \wedge U(k) = y).$$

Then we can take

$$A(m) := \neg \exists k \, \mathrm{Prf}_T(k, \overline{\ulcorner 0 = 1 \urcorner}).$$

That completes the proof.

A two-player game

- Player I proposes axioms T for mathematics.
- Player II responds, "OK, if T is consistent then here is a true theorem it does not prove."
- Player I then has to give new axioms (extending T) that do prove this new theorem.
- The point of the theorem is the Player II's job is trivial: he or she just keeps producing the same formula, changing *only one number* in it.
- Player I's job, on the other hand, is very difficult, and after a while he or she will be stymied, unable to come up with a really original response.
- Player I can stall, by just returning at each stage the new "axiom" from Player II's move, but this strategy will only earn ridicule.

A more mathematical-sounding two-player game

Using the DPRM theorem, we can make those results sound less "logical" and more "mathematical."

Theorem

There is a fixed polynomial equation $f(e, \mathbf{x}) = g(e, \mathbf{x})$ in several variables $\mathbf{x}$, such that for any consistent recursively enumerable theory T, there is an e such that

$$\forall \mathbf{x}\, (F(\bar{e}, \mathbf{x}) \neq G(\bar{e}, \mathbf{x}))$$

is true, but not provable in T.

Proof of the theorem

As in the proof of the previous theorem, the formula $\mathrm{Prf}_T(k, x)$ can be written as a Σ^0_1 formula with free variable m for the index of a function enumerating the axioms of T. By the (formalized) DPRM theorem, every Σ^0_1 formula is provably equivalent to a Diophantine formula. Hence there are polynomials F and G such that

$$\mathrm{Prf}_T(k, \overline{\ulcorner 0 = 1 \urcorner}) \equiv \exists \mathbf{y}\,(F(m, k, \mathbf{y}) = g(m, k, \mathbf{y})).$$

Now let $\mathbf{x}$ be the list of variables $k, \mathbf{y}$, and let e be the index of a Turing machine that enumerates the axioms of T. Then

$$T \vdash \mathrm{Con}_T \equiv \forall \mathbf{x}, (F(\bar{e}, \mathbf{x}) \neq G(\bar{e}, x)).$$

That completes the proof of the theorem.

Revised two-player game

- Player I proposes axioms T for mathematics.
- Player II produces a Diophantine equation such that, if T is consistent, the equation has no solution, but that is not provable in T.
- Moreover, Player II does not think long for each move, as all he or she needs to do is change one number (albeit possibly in several places) in the equation.
- Player I will surely give up after a few turns, or be reduced to a ridiculous stalling strategy.

The Finite Ramsey Theorem

Another line of work after the incompleteness theorems has been to find explicit problems in combinatorics that "might have come up naturally", and prove that they are true but unprovable in various theories. The first such result was due to Paris-Harrington. They considered the "finite Ramsey theorem", which had come up naturally in combinatorics.

Theorem (Finite Ramsey Theorem)

For any positive integers n, k, m we can find N with the following property: if we color each of the n-element subsets of $S = \{1, 2, 3, \ldots, N\}$ with one of k colors, then we can find a subset Y of S with at least m elements, such that all n-element subsets of Y have the same color.

The Finite Ramsey Theorem can be stated and proved in $\mathbf{PA}$. (Finite subsets can be coded as integers, and the proof goes by induction.)

Paris-Harrington

- Paris and Harrington modified the theorem to the "extended finite Ramsey theorem" by adding the further condition, "and the number of elements of Y is at least the smallest element of Y."
- Here is the theorem, with the added condition in red:

Theorem (Extended Finite Ramsey Theorem)

For any positive integers n, k, m we can find N with the following property: if we color each of the n-element subsets of $S = \{1, 2, 3, \ldots, N\}$ with one of k colors, then we can find a subset Y of S with at least m elements, such that all n-element subsets of Y have the same color, and the number of elements of Y is at least the smallest element of Y.

Extended Ramsey is not provable in $\mathbf{PA}$

- These theorems are related to the function that gets the smallest possible N from n, k, and m; that function grows a lot faster with the extra condition.
- Paris and Harrington showed that in fact, it grows faster than any function that is provably total in $\mathbf{PA}$.
- It follows that the extended Ramsey theorem is not provable in $\mathbf{PA}$.
- So here is a theorem that "could have come up naturally", even if it actually did not.

Summary of today's discussion of incompleteness

- You can't escape the fact: axiomatic systems are inadequate to establish mathematical truth beyond a limited domain.
- You can't escape by adding more axioms; not even a transfinite progression of stronger and stronger theories helps.
- Famous and important problems in set theory have been shown unprovable in all known systems, so specific problems stare us in the face as more or less absolutely unsolvable, in spite of the fact that theoretically Gödel's theorem only applies to a fixed formal system.
- The realm of unsolvability certainly extends into the theory of Diophantine equations, by the DPRM theorem. However, as yet no specific previously-considered Diophantine equation has been shown to be unsolvable by a proof that can't be formalized in $\mathbf{PA}$.
- Combinatorics is not safe either.
- Finally, Chaitin's theory of algorithmic randomness has shown that, beyond a "set of measure zero", mathematical truth necessarily looks to us humans like the toss of a die.