Hilbert's problems, Gödel, and the limits of computation

Logan Axon

Gonzaga University

April 6, 2011

Hilbert at the ICM

At the 1900 International Congress of Mathematicians in Paris, David Hilbert gave a lecture on "Mathematical Problems". He presented 10 problems during his talk and included 13 more in a published text of the speech.

Some of the problems

1. "Cantor's problem of the cardinal number of the continuum": resolve the continuum hypothesis (Hilbert also suggests determining if the real numbers can be well-ordered).
4. "Problem of the straight line as the shortest distance between two points": "the construction and systematic treatment" of nearly–Euclidean geometries.
6. "Mathematical treatment of the axioms of physics".
8. "Problems of prime numbers": prove the Riemann Hypothesis, resolve Goldbach's conjecture, generalize to ideal primes of other fields, etc. Complete text of the address at `http://aleph0.clarku.edu/~djoyce/hilbert/problems.html`.

Resolutions

1. "Cantor's problem of the cardinal number of the continuum". Gödel (1940) showed that it is possible to satisfy all the axioms of set theory and have $\mathfrak{c}$ be the smallest uncountable cardinal. Cohen (1963/4)showed that it is possible to satisfy the axioms and have $\mathfrak{c}$ **not** be the the smallest uncountable cardinal.
4. "Problem of the straight line as the shortest distance between two points": never really took off?
6. "Mathematical treatment of the axioms of physics": amounts to finding a Theory of Everything–Physicists are still working on this one.
8. "Problems of prime numbers": prove the Riemann Hypothesis, et cetera: still very much unresolved and very much of interest. Now a Millennium Prize Problem: a solution is worth $1,000,000.

Hilbert's problems and computation

Focus on two problems:

2 "The compatibility of arithmetical axioms": prove that the axioms of arithmetic are consistent.

10 "Determination of the solvability of a Diophantine equation": "devise a process" for determining "in a finite number of operations" if a polynomial (in any number of variables) with integer coefficients has integer roots.

The "process according to which it can be determined by a finite number of operations" in question 10 is an algorithm. The connection of question 2 to computation is less clear.

Consistency

Hilbert's second problem

Prove that the axioms of arithmetic are consistent.

Definition

A set of axioms is consistent if there is no statement p such that both p and $\neg p$ can be proved.

Proposition (basic fact of logic)

For all statements p and q $(p \,\&\, \neg p) \implies q$.

Corollary

A set of axioms is consistent if and only if there is some statement p such that p cannot be proved.

Gödel's theorems

Theorem (Gödel)

In any consistent mathematical system sufficient for defining ordinary arithmetic, the following hold:

1. *There is a mathematical statement p such that neither p nor its negation $\neg p$ can be proved (p is undecidable);*
2. *The statement "this system is consistent" is undecidable.*

The second incompleteness theorem proves that Hilbert's second problem cannot be solved within ordinary mathematics. The first incompleteness theorem shows that there will always be assertions that we can neither prove nor disprove from our axioms (addresses Hilbert's Entscheidungsproblem).

What is a proof?

A formal system (for mathematics) has a language of "primitive" symbols which can be put together to make formulas and equations, some of which are axioms:

$$\forall a\ \forall b\ (a + b = b + a)$$
$$\forall a\ \exists b\ (a + b = 0)$$
$$\forall a\ (a + 0 = a)$$
$$\forall a\ \forall b\ \forall c\ [a \cdot (b + c) = a \cdot b + a \cdot c]$$
$$\vdots$$

A proof starts with axioms and consists of applying a few logical rules, most importantly *modus ponens*:

$$[(p \implies q)\ \&\ p] \implies q.$$

Gödel numbers

In practice proofs use all kinds of definitions, abbreviations, and shortcuts. but every proof can be written as a *finite sequence of symbols*.

Idea (Gödel)

We can encode every mathematical statement, including proofs, as natural numbers. Moreover, we can think of statements about numbers as being statements about the mathematical statements represented by those numbers.

This way of thinking is sometimes referred to as *metamathematics*.

Gödel numbers

Gödel actually gave an explicit code.

0	S	$=$	$\neg$	$\vee$	$\&$	$\Longrightarrow$	$\equiv$	$\forall$	$\exists$	$\in$	(	)
1	2	3	4	5	6	7	8	9	10	11	12	13

The integers greater than 13 and congruent to 0 mod 3 are variables for propositions, the integers greater than 13 and congruent to 1 mod 3 are variables for numbers, and the integers greater than 13 and congruent to 2 mod 3 are variables for functions.

A mathematical statement corresponds to a sequence of integers $k_1, k_2, \ldots, k_n$ which we then associate to a single number

$$2^{k_1} 3^{k_2} 5^{k_3} \ldots p_n^{k_n}$$

where p_n is the n^{th} prime.

Example of a Gödel number

S is the successor function: $S(a) = a + 1$. A simple true statement is $\forall a\ \neg(S(a) = a)$.

Statement: $\forall a\ \neg(S(a) = a)$

Sequence: $9, 16, 4, 12, 2, 12, 16, 13, 3, 16, 13$

Gödel number: $2^9 \cdot 3^{16} \cdot 5^4 \cdot 7^{12} \cdot 11^2 \cdot 13^{12} \cdot 17^{16} \cdot 19^{13} \cdot 23^3 \cdot 29^{16} \cdot 31^{13}$

Wolfram α reports that this number has 122 digits, starting with 81772105 . . . .

Proof of the first incompleteness theorem

Definition

- Let $R_n(x)$ be the n^{th}mathematical formula with one free variable.
- Let $Bew(x)$ be the statement, "the number x represents a *provable* mathematical statement (when decoded)".

Proposition

The expression $Bew(x)$ is a mathematical formula with one free variable.

$Bew(x)$ is equivalent to the statement "$\exists y$ such that y codes for a proof of x". Gödel proved that the statement "y codes for a proof of x" can be expressed using just arithmetic. He produced an explicit formula for this (by recursive construction).

Proof of the first incompleteness theorem

If mathematical statements can be self-referential, then we should be able to come up with something like the classic "this statement is false" or the set $\{S : S \notin S\}$.

Consider the mathematical formula

$$\neg Bew\left(R_x(x)\right).$$

This is a mathematical formula with one free variable and so there is some $q \in \mathbb{N}$ such that

$$R_q(x) \equiv \neg Bew\left(R_x(x)\right).$$

$R_q(q) \equiv \neg Bew\left(R_q(q)\right)$ so $R_q(q)$ asserts that $R_q(q)$ cannot be proved.

Proof of the first incompleteness theorem

Proposition

If the theory is consistent, then neither $R_q(q)$ nor $\neg R_q(q)$ can be proved (the statement $R_q(q)$ is undecidable).

Proof.

If $R_q(q)$ can be proved, then $Bew\left(R_q(q)\right)$ is true. But $R_q(q) \equiv \neg Bew\left(R_q(q)\right)$ and so $\neg Bew\left(R_q(q)\right)$ must be true (if we can prove it, then it must be true). Thus $Bew\left(R_q(q)\right)$ and $\neg Bew\left(R_q(q)\right)$ must both be true. This is a contradiction.

If $\neg R_q(q)$ can be proved then we again reach a contradiction.

□

Conclusion: if arithmetic is consistent, then there is an undecidable statement.

Proof of the second incompleteness theorem

Let *Con* be the statement that the theory is consistent.

$$Con \equiv \forall x \neg [Bew(x) \ \& \ Bew(\neg x)]$$

The first theorem showed that if the theory is consistent, then $R_q(q)$ is unprovable. But we can also see that $R_q(q)$ must actually be true, since it asserts its own unprovability. Therefore we have proved that

$$Con \implies R_q(q).$$

If we can prove *Con*, then using modus ponens we can also prove $R_q(q)$. This would contradict the first theorem. Therefore *Con* cannot be provable.
We assumed that the theory was actually consistent, and so $\neg Con$ must not be provable.

What does it mean?

Theorem (Gödel)

In any consistent mathematical system sufficient for defining ordinary arithmetic, the following hold:

1. *There is a mathematical statement p such that neither p nor its negation $\neg p$ can be proved (p is undecidable);*
2. *The statement "this system is consistent" is undecidable.*

"This theorem established a fundamental distinction between what is *true* about the natural numbers and what is *provable*..." (Floyd and Kanamori in the Notices).

The tenth problem

Hilbert's tenth problem

"Determination of the solvability of a Diophantine equation": "devise a process" for determining "in a finite number of operations" if a polynomial (in any number of variables) with integer coefficients has integer roots.

Modern formulation: write a computer program to determine if an arbitrary polynomial with integer coefficients has integer roots.

Examples of Diophantine equations:

1. $ax^2 + bx + c = 0$
2. $x^2 + 1 = 0$
3. $x^2 + y^2 = z^2$
4. $x^2 - ay^2 = \pm 1$ (Pell's equation)

Diophantine sets

Let $P(a, x_1, x_2, \ldots, x_n)$ be a polynomial with variables a and $x_1, x_2, \ldots, x_n$. Fix an integer a. We are interested in determining if there exist integers $b_1, b_2, \ldots, b_n$ so that

$$P(a, b_1, b_2, \ldots, b_n) = 0.$$

The existence of such an integer root will depend on the choice of a.

Example

The polynomial $x^2 + a$ has an integer root only when a is a square.

Definition

A subset $S \subseteq \mathbb{Z}$ is *Diophantine* if there is a polynomial $P(a, x_1, x_2, \ldots, x_n)$ such that

$$S = \{a \in \mathbb{Z} : P(a, x_1, x_2, \ldots, x_n) \text{ has an integer root}\}.$$

The MRDP theorem

Theorem (Matiyasevich, Robinson, Davis, Putnam)

A set is Diophantine if and only if it is computably enumerable.

Definition

A set is *computably enumerable* if there is a computer program that enumerates the elements of the set (in no particular order). A set is *computable* if there is a computer program that can determine if any given number is in the set.

Proposition

A set is computable if and only if both the set and its complement are computably enumerable.

Consequences

Examples of computable sets:

1. $\{a \in \mathbb{Z} : a \text{ is even}\}$.
2. $\{a \in \mathbb{N} : a \text{ is prime}\}$.
3. $\{a \in \mathbb{N} : a \text{ is the Gödel number of a valid proof}\}$.

By the MRDP theorem each of the above sets is Diophantine. In particular, there is a polynomial $P(a, x_1, x_2, \ldots, x_n)$ such that $P(a, x_1, x_2, \ldots, x_n)$ has an integer solution if and only if a is prime. An example (using 26 variables): `http://mathworld.wolfram.com/PrimeDiophantineEquations.html`.

Resolution of the tenth problem

Computably enumerable and computable are not the same.

Theorem

There is a set K which is computably enumerable but not computable.

Resolution of the tenth problem

By the MRDP theorem K is Diophantine. Hence there is a polynomial $P(a, x_1, x_2, \ldots, x_n)$ that has a root if and only if $a \in K$. If we had an algorithm that could determine whether or not $P(a, x_1, x_2, \ldots, x_n)$ has a root for any given a, then we could easily modify this into an algorithm to determine membership in K. Therefore no such algorithm exists.

Remark

The tenth and second problems are actually related.

Corollary

There is a polynomial $P(a, x_1, x_2, \ldots, x_n)$ *and a number* a_0 *such that the statement*

$$\forall x_1, x_2, \ldots, x_n \in \mathbb{Z}\ P(a_0, x_1, x_2, \ldots, x_n) \neq 0$$

cannot be proved even though it is true.