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

Logan Axon

Gonzaga University

April 5, 2024

Hilbert at the ICM

At the 1900 International Congress of Mathematicians in Paris, David Hilbert gave a lecture on "Mathematical Problems" that he thought would be important for the next century of mathematics. Ten problems during his talk and included 13 more published.

Hilbert's problems and computation

We focus on Hilbert's problem #2 (and mention another #10):

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.

Problem 10 asks for an algorithm; generalize the quadratic formula to work for polynomials of any degree or with more variables.

Hilbert's problems and computation

We focus on Hilbert's problem #2 (and mention another #10):

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.

Problem 10 asks for an algorithm; generalize the quadratic formula to work for polynomials of any degree or with more variables.

Problem 2 is also connected to computation, but in less obvious ways.

Consistent axioms

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: $(p \mathbin{\&} \neg p) \implies q$.

Consistent axioms

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: $(p \,\&\, \neg p) \implies q$.

Theorem

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

If the system is consistent, then we can't prove $0 = 1$. And if we can't prove $0 = 1$, the system is consistent.

Poll

Do you think arithmetic is consistent?

Poll

Do you think arithmetic is consistent?

In math we only **know** something is true once we have a proof. So we always look for proofs of the things we think are true. If we think it's true that arithmetic is consistent, then we want to prove it.

Gödel's incompleteness theorems

Theorem (Gödel, $\sim$ 1930)

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" cannot be proved or disproved (this is one of the undecidable statements).*

Part 2 proves that Hilbert's second problem cannot be solved within ordinary mathematics.
Part 1 says that there will always be assertions that we can neither prove nor disprove from our axioms, provided they're consistent (which addresses Hilbert's Entscheidungsproblem).

Gödel numbers

Idea (Gödel)

- Every mathematical statement (including proofs) can be encoded as a natural number.
- Statements about numbers may also be interpreted as statements about the mathematical statements encoded as the numbers.

Point 2 is the origin of **metamathematics**.

Gödel numbers

Gödel 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: $S(a) = a + 1$.
"No number is equal to its successor" 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: $2^9 \cdot 3^{16} \cdot 5^4 \cdot 7^{12} \cdot 11^2 \cdot 13^{12} \cdot 17^{16} \cdot 19^{13} \cdot 23^3 \cdot 29^{16} \cdot 31^{13}$

This number has 122 digits:
81772105583868532612128696004641827651917484637956352845 . . .

Proof of the first incompleteness theorem

Theorem (Gödel)

There is an undecidable mathematical statement.

Definition

- Let $R_n(x)$ be the n^{th}mathematical formula with one free variable. E.g. $\neg(S(x) = x)$ might be $R_{3710181\ldots}$.
- Let $Bew(x)$ be the statement, "the number x represents a provable mathematical statement (when decoded)".

Proposition (Gödel)

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

Gödel worked out a specific mathematical formula for $Bew(x)$: essentially programmed it into a (theoretical) computer that runs on arithmetic.

Proof of the first incompleteness theorem

We should now be able to come up with a paradoxical statement like "this statement is false."

Begin with "the x^{th} statement with input x cannot be proved":

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

Proof of the first incompleteness theorem

We should now be able to come up with a paradoxical statement like "this statement is false."

Begin with "the x^{th} statement with input x cannot be proved":

$$\neg Bew\,(R_x(x))$$

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

$$R_q(x) \equiv \neg Bew\,(R_x(x))$$

Proof of the first incompleteness theorem

We should now be able to come up with a paradoxical statement like "this statement is false."

Begin with "the x^{th} statement with input x cannot be proved":

$$\neg Bew\,(R_x(x))$$

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

$$R_q(x) \equiv \neg Bew\,(R_x(x))$$

Now take the "diagonal" that asserts its own unprovability:

$$R_q(q) \equiv \neg Bew\,(R_q(q))$$

Proof of the first incompleteness theorem

Proposition

If arithmetic is consistent, then neither $R_q(q)$ nor $\neg R_q(q)$ can be proved.

Proof.

If $R_q(q)$ can be proved, then $Bew\,(R_q(q))$ is true (definition of $Bew(x)$). But $R_q(q) \equiv \neg Bew\,(R_q(q))$. Hence a proof of $R_q(q)$ is a proof of $\neg Bew\,(R_q(q))$. Thus $Bew\,(R_q(q))$ and $\neg Bew\,(R_q(q))$ must both be true. Thus arithmetic must not be consistent.

If $\neg R_q(q)$ can be proved then we similarly conclude that arithmetic isn't consistent.

$\square$

Conclusion: **undecidable statements exist** (if arithmetic is consistent)

Proof of the second incompleteness theorem

Let *Con* be the statement that the mathematical system is consistent.

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

The first theorem showed that if arithmetic is consistent, then $R_q(q)$ is unprovable. $R_q(q)$ asserts its own unprovability and thus must actually be true. Therefore *Con* implies $R_q(q)$.

If we can prove *Con*, then this is a proof of $R_q(q)$. This would contradict the first theorem. Therefore *Con* cannot be proved (if the system is consistent).

If the system consistent, then $\neg Con$ cannot be proved (because it isn't true).

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" cannot be proved or disproved (it's 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).

H10

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 $x_1, x_2, \ldots, x_n$. We wish to determine 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

$$S = \{a \in \mathbb{Z} : P(a, x_1, x_2, \ldots, x_n) = 0 \text{ has an integer solution}\}.$$

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 (with 26 variables):
`http://mathworld.wolfram.com/PrimeDiophantineEquations.html`

Computably enumerable sets

Theorem

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

Proof.

Let B be the set of provable statements: $B = \{x \in \mathbb{N} : Bew(x)\}$.
Suppose that B is computable. Check to see if Con is in B.

- If Con is in B, then the system is consistent and Con cannot be proved. Contradiction.
- If Con is not in B, then there is some statement that cannot be proved (namely Con). Thus the system must be consistent. This is a proof of Con. Contradiction.

Therefore B is not computable. □

Algorithm for B

A pseudo-python script for enumerating B:

```
n = 1
  while TRUE:
    for x in range(0,n):
      for i in range(0,n):
        if i is a proof of x:
          return x
    n = n + 1
```

Thus B is computably enumerable.

Another important non-computable but computably enumerable set is the **halting set:** K.

Resolution of the tenth problem

Resolution of the tenth problem

B is computably enumerable, but not computable. By the MRDP theorem B is Diophantine. Hence there is a polynomial $P(a, x_1, x_2, \ldots, x_n)$ that has a root if and only if $a \in B$.

If there were 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 B. Since B is not computable, no such algorithm exists.

Conclusion: Hilbert's tenth problem is impossible.

Remark

The tenth and second problems are related in another way.

Corollary

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

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

(translation: "$P(a_0, x_1, x_2, \ldots, x_n) = 0$ *has no integer solutions")*

cannot be proved even though it is true.