Gödel's Incompleteness Theorem

Phil Hazelden

2012-02-08

Overview

- Godel's theorem says, roughly, that there are true statements about the natural numbers which cannot be proved.
- We prove this theorem by constructing such a statement.
- Roughly speaking, "this statement is unprovable".
  - If false, it can be proved to be true.
  - Therefore true, therefore unprovable.
- How is this not a proof?
- How is this statement about the natural numbers?

The "MIU" game

- Played with strings containing the symbols `M`, `I`, `U`.
- Some strings are theorems. Which?
- Derivations: making new theorems from old.
  - $\mathtt{M}x\mathtt{I} \to \mathtt{M}x\mathtt{IU}$
  - $\mathtt{M}x \to \mathtt{M}xx$
  - $\mathtt{M}x\mathtt{III}y \to \mathtt{M}x\mathtt{U}y$
  - $\mathtt{M}x\mathtt{UU}y \to \mathtt{M}xy$
- We start with a list of initial theorems ("axioms")
  - The only axiom is `MI`.

An example derivation

- MI — axiom
- MII — $\mathtt{M}x \to \mathtt{M}xx$
- MIIII — $\mathtt{M}x \to \mathtt{M}xx$
- MUI — $\mathtt{M}x\mathtt{III}y \to \mathtt{M}x\mathtt{U}y$
- MUIU — $\mathtt{M}x\mathtt{I} \to \mathtt{M}x\mathtt{IU}$
- MUIUUIU — $\mathtt{M}x \to \mathtt{M}xx$
- MUIIU — $\mathtt{M}x\mathtt{UU}y \to \mathtt{M}xy$

What about nontheorems?

- Is `MU` a theorem?
- If it is, we can prove it by producing a derivation.
  - We could search derivations methodically, and eventually find MU.
- If not, how can we prove that?
  - If we search for it, we'll never find it. But we'll never see that we'll never find it.
  - Answer: count the number of `I`s in a theorem, modulo 3.
  - This is not generalisable.

The "Number theory" (NT) Game

- A more complicated game that mathematicians like to play.
- Symbols: 0-9, +, ×, =, ∧, ∨, ¬, ⇒, (,), a, b, c, ′, ∀, ∃
- Some derivation rules:
  - $w(x \wedge y)z \to w\neg(\neg x \vee \neg y)z$ — de Morgan's law
  - $(x = y) \to (x + 1 = y + 1)$ — Successorship
  - $x,\ y \to (x \wedge y)$ — Joining
  - $x\{0\},\ \forall a(x\{a\} \Rightarrow x\{a+1\}) \to \forall a(x\{a\})$ — Induction
- Axioms:
  - $\forall a \neg(a + 1 = 0)$
  - $\forall a(a + 0 = a)$
  - $\forall a \forall b(a + (b + 1) = (a + b) + 1)$
  - $\forall a(a \times 0 = 0)$
  - $\forall a \forall b(a \times (b + 1) = (a \times b) + a)$

Is number theory complete?

- A well-formed statement in the numer theory game is either:
  - True or false;
  - A theorem or nontheorem.
  - If a nontheorem, its negation might be a theorem.
- We hope:
  - A statement is a theorem iff it is true;
  - x is a theorem iff $\neg x$ is a nontheorem.
  - These are (kind of) equivalent.
- But incompleteness ruins this hope.

Gödel numbering (MIU)

- Turn MIU-strings into numbers.
- M $\rightarrow$ 1, I $\rightarrow$ 2, U $\rightarrow$ 3
- New rules, where $x«^n$ means $x \cdot 10^n$:
  - $1«^{n+1} + x«^1 + 2 \rightarrow 1«^{n+2} + x«^2 + 23$ where $x < 1«^n$
  - $1«^n + x \rightarrow 1«^{2n} + x«^n + x$, where $x < 1«^n$
  - $1«^{m+n+3} + x«^{m+3} + 222«^m + y \rightarrow$
    $1«^{m+n+1} + x«^{m+1} + 3«^m + y$, where $x < 1«^n$ and $y < 1«^m$
  - $1«^{m+n+2} + x«^{m+2} + 33«^m + y \rightarrow 1«^{m+n} + x«^m + y$, where $x < 1«^n$ and $y < 1«^m$
  - 12 is an axiom
- So now we have derivations like:
  - 12 $\rightarrow$ 122 $\rightarrow$ 12222 $\rightarrow$ 132 $\rightarrow$ 1323 $\rightarrow$ 1323323 $\rightarrow$ 13223

Gödel numbering (number theory)

- Can do the same thing to the number theory game, it's just a lot more complicated.
- For example, De Morgan's law: $w(x \wedge y)z \to w\neg(\neg x \vee \neg y)z$.

$$w\text{«}^{l+m+n+3} + (\,\text{«}^{l+m+n+2} + x\text{«}^{m+n+2} + \wedge\text{«}^{m+n+1} + y\text{«}^{n+1} +)\text{«}^{n} + z$$

$$\to$$

$$w\text{«}^{l+m+n+6} + \neg\,(\,\neg\text{«}^{l+m+n+3} + x\text{«}^{m+n+3} + \vee\neg\text{«}^{m+n+1} + y\text{«}^{n+1} +)\text{«}^{n} + z$$

where $z < 1\text{«}^{n}$, $y < 1\text{«}^{m}$, $x < 1\text{«}^{l}$.

What good is this?

- Given an MIU-string x, can we construct an "equivalent" NT-string y?
  - If so, we can use number theory to talk about the MIU game.
  - And if so, maybe we can do the same thing to an NT-string?
  - Then we can make NT-theorems talk about NT-theorems.
  - Eventually, we need a theorem to talk about itself. So this is a good first step.
- "Equivalent" means y is an NT-theorem iff x is an MIU-theorem.
  - We want to be able to do this even if we don't know whether x is an MIU-theorem.
- It turns out we can.
- Won't prove this, but will try to convince.
  - Given a number x, we construct an NT-statement which is a theorem iff x is the Gödel number of a well-formed MIU-statement.
  - To be precise, iff x contains only the decimal digits 1, 2, 3.

Useful tricks

- Check that a finite set of things each has some property.
- Finite sequences are countable.
  - Can represent a sequence by a number, and use another number to extract elements from it.
- Instead of finding a number that satisfies P, just need to ask "does x satisfy P?" Then use $\exists$.

MIU-FORMED

- LOG$\{a, b\} \to 1 \ll^{b} > a \wedge 1 \ll^{b-1} \leq a$
- GOOD$\{a\} \to a = 1 \vee a = 2 \vee a = 3$
- NTH$\{a, b, c\}$ tests whether the b'th digit of a is c.
- MIU-FORMED$\{a\} \to$

$$\exists b(\text{LOG}\{a, b\} \wedge \\ \exists(\text{sequence } x_1 \text{ to } x_b)\forall c(c < b \Rightarrow \text{NTH}\{a, c, x_c\} \wedge \text{GOOD}\{x_c\}))$$

NT-THEOREM

- If an NT-statement can be Gödel-numberised, so can an NT-derivation.
- So given the number of a derivation, and the number of a statement, we can ask
  "Does this derivation prove this statement?"
- This can be expressed as an NT-statement, NT-DERIVES$\{a, b\}$.
- So we can construct:
  NT-THEOREM$\{a\} \rightarrow \exists b($NT-DERIVES$\{b, a\})$.
- Note that constructing a statement is much easier than determining its truth.

Self-reference

- Liar paradox: "This statement is true."
- Not much better: P - "Q is true." Q - "P is false."
- Quine:
  "yields falsehood when preceeded by its quotation." yields falsehood when preceeded by its quotation.
  - This turns out to be the key.

Quining

- If an NT-statement has free variables, we can substitute any number we like into them.
- In particular, we can substitute the Gödel number of the original statement.
- Construct a formula QUINE$\{a, b\}$ which tests whether b is "a quined".
    - Essentially, QUINE$\{a, b\} \rightarrow b = a\{a\}$

"This statement is unprovable"

- Let $U\{a\} \to \neg\exists b(\text{QUINE}\{a, b\} \wedge \text{NT-THEOREM}\{b\})$
- Let G be the quinification of U.
- In other words, find G such that QUINE$\{U, G\}$ is true.
- $U\{a\}$ says "a quined is not a theorem." Equivalently, "is not provable."
- So G $(= U\{U\})$ says "U quined is not provable."
- But G *is* U quined.
- Thus, G says "G is not provable."

Aftermath

- If G is false, we can find a proof of G, and number theory is inconsistent.
- If G is true, it can't be proved, so number theory is incomplete.
- Since $\neg G$ says "G is provable", $\neg G$ asserts its own negation.
- So neither G nor $\neg G$ is a theorem.