Gödel's Incompleteness Theorems

FORMAL METHODS SEMINAR – 25 NOVEMBER, 2020

EKANSHDEEP GUPTA

Early 20th Century Mathematics

- Foundational crisis of mathematics.
- Ripe with paradoxes:
  - Set of all sets that do not contain itself. Does this set contain itself?
  - Russel's Paradox
  - Axiom of Choice
  - Skolem's Paradox
- Two schools of thought:
  - Hilbert's Programme – Establish solid foundations with finite, complete axioms.
  - Intuintionism – Led by L. E. J Brouwer

Hilbert's Programme

- A formulation of all mathematics in a precise formal language and manipulated according to well defined rules.
- Completeness: all true mathematical statements can be proved.
- Consistency: no contradiction can be obtained in the formalism of mathematics.
- Decidability: algorithm for deciding the truth or falsity of any mathematical statement.

In other words, a fairy tale!

Peano's Arithmetic: $(\mathbb{N}, +, *, S, 0)$

[Giuseppe Peano, 1889]

First order logic:

- Symbols: 0
- Unary functions: S
- Binary functions: +, *

Axioms:

$$\big(S(m) = S(n)\big) \rightarrow (m = n)$$
$$\neg\,(S(a) = 0)$$

Addition:

$$a + 0 = a$$
$$a + S(b) = S(a + b)$$

Multiplication

$$a * 0 = 0$$
$$a * S(b) = a + a * b$$

Induction Schema:

For any formula $\psi(x, y_1, y_2, \ldots, y_k)$:

$$\forall \bar{y}\, \Big(\psi(0, \bar{y}) \wedge \Big(\forall x \, \big(\psi(x, \bar{y}) \rightarrow \psi(S(x), \bar{y})\big)\Big)\Big) \rightarrow (\forall z\, \psi(z, \bar{y}))$$

Examples

- 4 = S(S(S(S(0))))
- Not all numbers are perfect squares:
$$\exists x\ (\forall y \neg (y * y\ = x))$$
- Every number other than 0 is the successor of some number:
$$\forall x\ (\neg(x = 0) \rightarrow \exists y\ S(y) = x)$$
- prime(x)
$$\forall y\ \forall z\ (y\ * z = x) \rightarrow (y = 1 \vee y = x)$$
- power_of_two(x)
$$\forall y\ \forall z\ (y * z = x) \wedge prime(y) \rightarrow y = S(S(0))$$

Sidenote

Löwenheim–Skolem theorem: If a theory has a countable model, it has a model of *every* cardinality.

So non-standard models exist!

Replace first order induction schema:

For any formula $\psi(x, y_1, y_2, \dots, y_k)$:

$$\forall \bar{y}\ (\psi(0, \bar{y})\ \wedge\ \left(\forall x\ \left(\psi(x, \bar{y}) \rightarrow \psi(S(x), \bar{y})\right)\right)) \rightarrow (\forall z\ \psi(z, \bar{y}))$$

With second order axiom of induction:

$$\forall X\ (0 \in X\ \wedge\ \left(\forall y\ (y \in X \rightarrow S(y) \in X)\right)) \rightarrow (\forall z\ z \in X)$$

Gödel's Incompleteness Theorem

[Kurt Gödel, 1931]

- Any consistent formal system *F*
- within which a certain amount of elementary arithmetic can be carried out
- is incomplete
- i.e., there are statements of the language of *F* which can neither be proved nor disproved in *F*

Undecidability of Halting Problem

[Alan Turing, 1936]

- Given a Turing machine (read: a C++ program), there can be no algorithm to decide whether it will ever terminate or keep looping forever.

Proof:

- Suppose $halts(\{N\}, inp)$ correctly determines if N halts on inp or not.
- Construct $M(\{N\})$ = if $halts(N, \{N\})$ then $loop\_forever()$ else $halt()$
- Then, $M(\{M\})$ will do what?

Contradiction!

Proof Overview

1. Construct a way to talk about formulae from inside the logic.
   - For instance, FO doesn't allow us to write
     $\exists\ formula_1, formula_2 : formula_1 \ \wedge\ formula_2 \rightarrow (\forall x\ \exists y\ x < y)$
   - In FO, we can only quantify over elements of the universe.
   - But Gödel crafted self-reference!
2. Use self reference to construct a sentence which says, "I cannot be proved".
3. Win.

Gödel Numbering

Represent formulae and sequences of formulae by numbers, uniquely.

Number	Symbol	Meaning
666	0	zero
123	S	successor function
111	=	equality relation
212	<	less than relation
112	+	addition operator
236	×	multiplication operator
362	(	left parenthesis
323	)	right parenthesis

Number	Symbol	Meaning
262	x	a variable name
163	*	star (used to make more variables)
333	∃	existential quantifier
626	∀	universal quantifier
161	∧	logical and
616	∨	logical or
223	¬	logical not

$$G(x \land \neg x) = \underbrace{262}_{x}\,0\,\underbrace{161}_{\land}\,0\,\underbrace{223}_{\neg}\,0\,\underbrace{262}_{x} \rightarrow 262{,}016{,}102{,}230{,}262$$

Gödel Numbering

- Use 0 to separate symbols.

$$G(x \wedge \neg x) = \underbrace{262}_{x}\,0\,\underbrace{161}_{\wedge}\,0\,\underbrace{223}_{\neg}\,0\,\underbrace{262}_{x} \rightarrow 262{,}016{,}102{,}230{,}262$$

- Use 00 to separate different formulae in a sequence

$$G((x \wedge \neg x),(x \vee x *)) = \underbrace{262}_{x}\,0\,\underbrace{161}_{\wedge}\,0\,\underbrace{223}_{\neg}\,0\,\underbrace{262}_{x}\ \ 00\,\underbrace{262}_{x}\,0\,\underbrace{161}_{\vee}\,0\,\underbrace{262}_{x}\,0\,\underbrace{163}_{*}$$

$$\rightarrow 26{,}201{,}610{,}223{,}026{,}200{,}262{,}016{,}102{,}620{,}163 \approx 2.62 * 10^{31}$$

- Injective!

Gödel Numbering

- $well\_formed(x)$ = formula encoded by x is well-formed.
- $proof(x, y)$ = sequence of formulae encoded by y forms a proof of the formula encoded by x.
- $provable(x) \equiv \exists y\, proof(x, y)$

Sequences in PA

- Chinese Remainder Theorem: Given $n_1, n_2, \ldots, n_k$ relatively prime, and $m_1, \ldots, m_k$, there exists x such that for all $i, x \equiv m_i \ (mod\ n_i)$

- Encode sequence $(m_1, \ldots, m_k)$. Let n be big enough.
- Then $n+1, 2n+1, 3n+1, \ldots, kn+1$ are coprime. Set $n_i = n.i + 1$
- Let x satisfy $x \equiv m_i \ (mod\ n_i)$

- So, (x, n) encodes $(m_1, \ldots, m_k)$.

- Define $\beta(x, n, k) = remainder(x, n.k + 1)$. Then $\beta(x, n, i) = m_i$

Primitive Recursion!

Primitive Recursion

Suppose want $factorial(d, m) \coloneqq (m = d!)$

Encode by the sequence $(1!,\ 2!,\ 3!,\ 4!,\ \ldots\ ,\ d!)$

Check following:

- First term is 1.
- $(k+1)$th term is $(k+1) * k$th term.
- Last term is m.

$$factorial(d, m) \equiv \exists x\, \exists n\, \beta(x, n, 1) = 1 \wedge \beta(x, n, d) = m \wedge \\ \forall k\; k < d \rightarrow \beta(x, n, k+1) = (k+1).\, \beta(x, n, k)$$

Switching from predicates to functions:

$$function(a, b) = \alpha(a, b)\ where\ \beta(a, b)$$

is equivalent to

$$\exists c\ predicate(a, b, c) = \beta(a, b) \wedge c = \alpha(a, b)$$

Some useful formulae

- $pow(a,b) := (a^b) \equiv \beta(x,n,b+1)\ where\ \exists x\, \exists n\ \beta(x,n,1) = 1\ \forall k\ k < b \rightarrow \beta(x,n,k+1) = b.\beta(x,n,k)$

- $append(a,b)$ ≔ the seq of formulae a appended with the formula b, where a : a seq of formulae, b : a formula

$$append(a,b) \equiv a \ * pow(10,x) * 100 + b\ where$$
$$\exists x\ \ pow(10,x-1) < b \leq pow(10,x)$$

- $find(a,b)$ ≔ Holds if a : a seq of formulae, b : a formula contained in the sequence.

$$find(a,b) \equiv \exists x\, \exists y : a = append(append(x,b),y)$$

Gödel Numbering

For $proof(x, y)$:

- Given formula $F(x)$, number m, can define $substitute(n_1, m, n_2)$ where $n_1 = G(F(x))$, and $n_2 = \mathrm{G}(\mathrm{F}(\mathrm{m}))$

- For deduction rules, example Modus Ponens:

$$\frac{P\ ; \quad P \to Q}{Q}$$

Encode relation

MP$(m, n) \coloneqq G^{-1}(m)$ is a seq of formulae containing $P, P \to Q$ and $G^{-1}(n)$ is the seq of formulae $G^{-1}(m)$ appended with Q

$$MP(m, n) \equiv \exists p\ \exists q\ \exists r\ well\_formed(p) \wedge well\_formed(q) \wedge substitute_2(G(x \to y), p, q, r) \wedge find(p, m) \wedge find(r, m) \wedge n = append(m, q)$$

Gödel Numbering

For $proof(x, y)$:

- Suppose we have such relations $R_1, R_2, \dots, R_d$ for all the axioms + deduction rules.
- Check if $proof(x, y)$ holds as follows:
  - There exists some sequence $(m_1, \dots, m_k)$ such that for all i:
    $$R_1(m_i, m_{i+1}) \lor \dots \lor R_d(m_i, m_{i+1})$$
  - Check if $y = m_k$

Gödel Sentence

"this statement is false"

$not\_provable(x) = \neg provable(x)$

Let N be the Gödel number of $not\_provable(x)$.

Consider statement $p = not\_provable(N)$

Then p literally says: "this statement is not provable".

Gödel's 2nd Incompleteness Theorem

- No proof system can prove its own consistency.

- Can encode $Cons(PA)$ = “no proof exists for 0=1” in PA using Gödel Numbering. This statement is not provable.

Proof by contradiction:

- Suppose $Cons(PA)$ is provable.
- If PA is consistent, then p cannot be proved.
- Formalize the entire discussion in PA to prove in PA that p cannot be proved.
- But that is a proof of p! Contradiction!

- Sidenote: $Cons(PA)$ can be proved in ZFC, but $Cons(ZFC)$ can't.

Gödel's Completeness Theorem

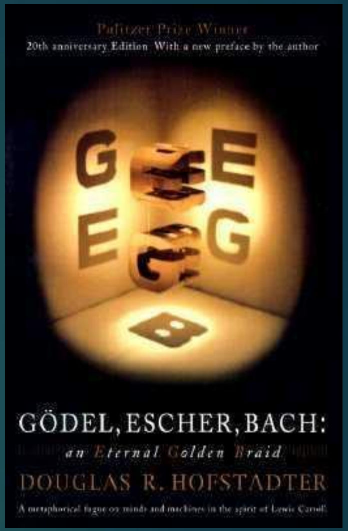
- First order logic is complete.
- If a formula is a syntactic consequence of our axioms, then it can be proved in the system.

Apparent contradiction!

Semantic consequence vs syntactic consequence.

References

- Gödel, Escher, Bach: an Eternal Golden Braid by Douglas R. Hofstadter
- Wikipedia: https://w.wiki/nRE
- Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/goedel-incompleteness/
- Kurt Gödel, *On Formally Undecidable Propositions of Principia Mathematica and Related Systems I*, 1931
- My friend’s YouTube video: https://youtu.be/EL4njRlv8pI



Thank you!