Theory of Computation:
Godel's Incompleteness Theorem

Language of Number Theory

This is an example of First Order Logic that expresses properties of the natural numbers $\mathbb{N}$:

- Variables: $x, y, z, \ldots$ ranging over $\mathbb{N}$.
- Operator symbols: $+, .$
- Constant 0 is additive identity and 1 is multiplicative identity.

Language of Number Theory

- Relation symbol: $=$ (Others like $<, >, \geq, \leq$ are definable from this)
- Quantifiers: $\forall, \exists$
- Propositional operations: $\vee, \wedge, \neg, \rightarrow, \iff$.
- Parentheses.

Important formulas

- $x \leq y := \exists z\ (x + z = y)$
- $x < y := \exists z\ (x + z = y \wedge \neg(z = 0))$
- $INTDIV(x, y, q, r) := (x = qy + r) \wedge (r < y)$ - q is the quotient and r the remainder when x is divided by y.
- $DIV(y, x) := \exists q\ INTDIV(x, y, q, 0)$ - x is divisible by y
- $EVEN(x) := DIV(2, x)$, $ODD(x) := \neg EVEN(x)$
- $PRIME(x) := (x \geq 2) \wedge \exists y\ (DIV(y, x) \rightarrow (y = 1 \vee y = x))$.

Sentences

- If there are no free (unquantified) variables in a formula, it is called a sentence.
- Example: $\forall x \exists y \ y = x + 1$ - Every number has a successor
- Not an example: $\forall x \ x + z \geq z$ as z is not quantified.
- Sentences have a well-defined truth value under its natural interpretation in $\mathbb{N}$:
  $\forall x \exists y \ y = x + 1$ - True.
  $\forall x \exists y \ x = y + 1$ - False because this says that every number has a predecessor when 0 does not.
- First Order Number Theory: The set of true sentences, denoted by $\mathrm{Th}(\mathbb{N})$.
- Decision Problem for Number Theory: Given a sentence, is it true?

Proof Systems: Peano Arithmetic

Any proof system (Eg. Peano Arithmetic or PA) consists of :
(1) a set of *axioms* which are some basic assumptions asserted to be true,
(2) and a set of *rules of inference*, which are applied in a mechanical way to derive further true sentences (theorems) from the axioms

PA

- Axioms of first order logic for manipulating:
  propositional formulas, such as $(\phi \wedge \psi \rightarrow \phi)$
  quantifiers, such as $(\forall x \phi(x)) \rightarrow \phi(100)$
  equality, such as $\forall x \forall y \forall z((x = y) \wedge (y = z) \rightarrow x = z)$

PA

Number Theoretic Axioms:

- $\forall x \neg(0 = x + 1)$ - 0 cannot be a successor
- $\forall x \forall y(x + 1 = y + 1 \rightarrow x = y)$ - one-to-one mapping of successors
- $\forall x x + 0 = x$ - 0 is the additive identity
- $\forall x \forall y x + (y + 1) = (x + y) + 1$ - $+$ is associative
- $\forall x x.0 = 0$ - 0 is the multiplicative annihilator
- $\forall x \forall y x.(y + 1) = (x.y) + x$ - $.$ distributes over $+$
- $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x + 1))) \rightarrow \forall x \phi(x)$ - induction axiom for a formula ϕ on a single free variable x

Rules of Inference

- Modus Ponens: $\phi, \phi \rightarrow \psi \Rightarrow \psi$
- Generalization: $\phi \Rightarrow \forall x\ \phi$

Proofs in a Proof System

- Proof for ϕ_n: Sequence $\phi_0, \phi_1 \ldots, \phi_n$ of formulas such that each ϕ_i is either an axiom or inferred from formulas appearing earlier in the sequence.
- Theorem: a sentence that has a proof in the system.

Soundness and Completeness

Proof Systems are:

- *Sound* if all theorems are true. So a false sentence cannot be proved to be true.
  This holds for any reasonable proof system. In PA, this can be shown by induction on the steps of inference to obtain the proof.
- *Complete* if all true sentences are theorems of the system.
  Then the set of theorems would coincide with $\mathrm{Th}(\mathbb{N})$.

Godel's Incompleteness Theorem

Theorem: For any reasonable proof system, including PA, a sentence ϕ can be constructed that implies the following sentence:
ϕ is true $\iff$ ϕ is not provable.
In other words, no reasonable proof system for number theory can be complete.

Godel's Incompleteness Theorem

Some points about the proof:

- The proof is constructive. The sentence ϕ constructed heavily uses self-referencing.
- The idea is to construct ϕ such that it asserts the truth of (ϕ is true $\iff$ ϕ is not provable). What are the consequences of the truth of (ϕ is true $\iff$ ϕ is not provable)?
- Since any reasonable proof system is sound, for any sentence ψ,
  ψ is provable $\Rightarrow$ ψ is true.
- Now suppose ϕ is false
  $\Rightarrow$ ϕ is provable
  $\Rightarrow$ ϕ is true, which is a contradiction.
  Thus ϕ must be true. This implies that ϕ is not provable and the proof system is not complete!

Simpler version

If we look at PA alone, it is possible to show that:
(i) The set of theorems is r.e
(ii) The set $\mathrm{Th}(\mathbb{N})$ of true sentences is not.
Thus, PA cannot be complete

Set of Theorems

- We can design a Turing machine that enumerates all theorems by enumerating all the axioms on PA, and systematically applying the rules of inference in all possible ways, and printing every sentence that is derived.
- Thus, the set of theorems for PA is r.e.

$\mathrm{Th}(\mathbb{N})$

- We can give a Turing reduction from $\neg HP$ to $\mathrm{Th}(\mathbb{N})$.
- Proof sketch: for an instance $M\#x$ of $\neg HP$, $\mathrm{VALCOMPS}(M, x)$ can be encoded as a number theoretic formula $\gamma_{M,x}(y)$, where y represents the valid computations history.
  The reduction involves the construction of this formula $\gamma_{M,x}(y)$ corresponding to $\mathrm{VALCOMPS}(M, x)$ such that $M\#x \in \neg HP \iff \neg\exists y \gamma_{M,x}(y) \in \mathrm{Th}(\mathbb{N})$.
- As $\neg HP$ is not r.e, the set $\mathrm{Th}(\mathbb{N})$ of true sentences is also not r.e.

Practice Problem

Prove that there exists a total computable function $f : \mathbb{N} \to \mathbb{N}$ that is not provably total in Peano arithmetic.
(Please try it yourself. Solution in next slide.)

Solution

- Function f is total if and only if $\forall x \exists y \; f(x) = y$.
- By soundness of PA, if f is provably total, then f is total.
- Assume that all total functions are provably total. Then there is a TM M enumerating all functions f with proofs for $\forall x \exists y \; f(x) = y$. Let $f^{(1)}, f^{(2)}, \ldots$ be the enumeration.
- Define a function $g : \mathbb{N} \to \mathbb{N}$ as follows: $g(z) = f^{(z)}(z) + 1$ for all z.

Solution contd.

- Since $f^{(z)}$ is total, so is g.
- Our assumption now implies that there is some $u \in \mathbb{N}$ such that $g = f^{(u)}$.
- But $g(u) = f^{(u)}(u) + 1 \neq f^{(u)}(u)$ $(\rightarrow\leftarrow)$.
- Therefore, there must exist some total function that is not provably total.