Lecture 12: Undecidability

Instructor: Ketan Mulmuley
Scriber: Yuan Li

February 17, 2015

1 Hilbert's Question

German mathematician David Hilbert proposed the following question as one of the main goals in his program:

Can truth be decided?

In order to formalize this question, we need to answer

- What is truth?
- What does it mean to be decided?

The first question (about truth) is answered in logic, which is usually different from the answer given by your grandmother. The second question (about decidability) is answered in Theory of Computation. At the time of Hilbert, there is no notion of "algorithm" or "Turing machine", he uses the phrase "mechanical procedure" to actually mean algorithm.

2 What is Truth

In order to formalize "truth", we need to choose a model including axioms and rules of inference from which all mathematical truths could in principle be proven. There are (at least) two options: set theory or number theory.

For example, based on set theory, we can define

$$\begin{aligned} 0 &:= \{\} \\ 1 &:= \{0\} = \{\{\}\} \\ 2 &:= \{0,1\} = \{\{\},\{\{\}\}\} \\ n &:= \{0,1,2,\ldots,n-2,n-1\}. \end{aligned}$$

Alfred Whitehead and Bertrand Russell have written a book called Principia Mathematica, which attempted to give a set of axioms and inference rules based on set theory and symbolic logic.

For different models, there are corresponding operators. For example, $+$, $-$, $*$, $<$, $>$, $=$, ... for number theory, and $\cup$, $\cap$, $=$, ... for set theory.

From now on, let us fix the model to be number theory, which we have learned in kindergartens.

Let the domain be $(\mathbb{N}, 0, \text{succ}, <, +, *)$, where $\mathbb{N}$ is the set of natural numbers, succ is the successor function. And we use Peano axioms and first-order logic, which uses quantifiers $\forall$, $\exists$.

For example, followings are two sentences in number theory.

$$(\forall x, y)(x^{y+1} = x^y x) \tag{1}$$

$$(\forall x, y)(x^{y+1} = x^y + x) \tag{2}$$

The first one is true, and the second is false.

We can (but we will not) formally define, given a well-formed sentence without free variables, it is either true or false over $\mathbb{N}$. Truth in number theory is a well-formed sentence without free variables that is true. For example, (1) is truth, but (2) is not.

3 Decidability of Truth

Question 3.1 (Hilbert's question)**.** *Is there an algorithm (mechanical procedure) to decide if a given sentence in number theory is true or false?*

Hilbert thought the answer should be YES. If it is the case, then mathematicians will be jobless. If you want to prove Fermat's Last Theorem, you can plug

$$(\forall n > 2)(\forall x, y, z > 0)(x^n + y^n \neq z^n)$$

into the algorithm, and let it run for a while, and finally it will produce a proof.

Gödel finally proves that the answer is NO, in a stronger sense, that truth is not even *definable* (we will not go there). The sentence which is not decidable is essentially the following

P: I am not provable.

We claim P is true. Assume for contradiction P is false, then P has no proof, which implies P is true. On the other hand, P can not have a proof, otherwise, it would be false. The main difficulty is to *encode* P as a sentence in number theory. However, the sentence itself is not very interesting.

Theorem 3.2 (Gödel)**.** *Number theory is undecidable, that is, there is no algorithm to decide if a given sentence in number theory is true or false.*

By the way, in the days of Gödel, there is no formal definition of algorithm. In the next class, we will come to the formal definition of algorithm and Church-Turing thesis: any function computable in *nature* is computable on Turing machine (or lambda calculus).

4 Some Undecidable Problems

Compared to the sentence "I am not provable", there is a more natural undecidable problem, called Diophantine problem.

Problem 4.1. *Given a polynomial $p(x_1, \ldots, x_n)$ (possibly nonhomogeneous) with integer coefficients, decide if there exists a nonnegative integer solution to the equation $p(x_1, \ldots, x_n) = 0$.*

The question is: whether Diophantine problem is decidable or not. The answer is NO.

For equations over reals (moreover, first-order logic sentence over reals), it is decidable (Tarski).

For equations over rational numbers, the question is open. If the answer is yes, then the proof will subsume Fermat's Last Theorem.

Problem 4.2 (Halting Problem)**.** *Given a program P (e.g. Turing machine), and input w, does P halt on w?*

Theorem 4.3. *Halting problem is undecidable.*

Given two CFLs G_1 and G_2, $L(G_1) \cap L(G_2) = \emptyset$ is undecidable; $L(G_1) = L(G_2)$ is undecidable; $L(G_1) = \Sigma^*$ is undecidable; $L(G_1) = \emptyset$ is decidable.

Problem 4.4 (Word problem in group)**.** *Given a representation of a group in terms of finitely many relations and generators, and given a word w in generators, decide if $w = 1$.*

The above word problem is also undecidable. For example, symmetric group S_n can be represented in terms of the following relations

$$\begin{aligned} s_i^2 &= 1 \\ s_i s_j &= s_j s_i \text{ if } j - i > 1 \\ s_{i+1} s_i s_{i+1} &= s_i s_{i+1} s_i, \end{aligned}$$

where s_i corresponds to the swap between i and $i + 1$.