CS 2742 (Logic in Computer Science) – Fall 2008
Lecture 31

Antonina Kolokolova

December 4, 2009

10 Gödel's incompleteness theorem

Proven by Gödel in 1931, said for any sufficiently powerful system of formalizing arithmetic there is a formula not provable in this arithmetic: this is the formula stating the the system does not prove a contradiction, a $0 = 1$.

Proving that some formalization of mathematics is not self-contradictory and can prove everything was part of Hilbert's program. Around 1900, Hilbert presented the list of 23 problems in mathematics that needed to be solved. The second problem asked for a proof that arithmetic (theory of natural numbers) is consistent. Several of the problems there can be stated in a form of "prove ¡something¿" or "find a method for solving ¡something¿", which later was proven to be unprovable or unsolvable. For example, the first problem was "prove or disprove Continuum Hypothesis". Many are resolved, some proven unsolvable, some, such as the Riemann Hypothesis and Goldbach conjecture that every even integer can be written as a sum of two primes are still open. A modern-day variant of Hilbert's list is a list of 7 major problems in mathematic was given by Clay Institute "Millenium prize problems" – they promised a million dollars per problem for solutions. One of these problems, the Poincare Conjecture, was since resolved (by Grigory Perelman); the rest remain open.

10.1 Basic definitions of logical theories

A theory, formally, is a set of logical statements. But more often when we talk about a theory we mean a set of axioms (may be infinite, but that can be easily described) and all statements that logically follow from these axioms. Axioms are logical statements that are assumed, and different theories can take different assumptions: it can be that two theories contradict each other on some assumption. A different way to compare theories is to look at all the possible "worlds", called *models*, in which axioms of theories are satisfied.

For example, Euclidean geometry can be viewed as everything that follows from 5 postulates of Euclid. A model for such a geometry can be flat world (planar geometry). If the 5th postulate of Euclid is replaced with another, contradictory, statement (e.g., "all parallel lines intersect") then a different theory of geometry is obtained (Riemann's geometry, which holds on the surface of a sphere).

Zermelo-Fraenkel set theory is a another example of a theory: there, the axioms describe basic properties of sets. Although ZFC can prove much of mathematics, there are worlds (models) of ZFC in which the Continuum Hypothesis ("is there a set A such that $|\mathbb{N}| < |A| < |\mathbb{R}|$") is true, and another model in which it is false.

Which leads us to a definition of completeness: a theory is incomplete if there is something that cannot be proven or disproven from the axioms of this theory. Eucledian geometry without the parallel postulate cannot prove or disprove this postulate; ZFC cannot prove or disprove the Continuum hypothesis, so they are incomplete.

An example of a "complete" (but not too useful) theory is a theory which has contradictory axioms, so it proves falsiness. Since $F \to \phi$ for any ϕ, from a false statement one can prove anything. Such theories, that can prove falsiness, are called *inconsistent*: the "good" theories, that don't contain a contradiction, are *consistent*.

Gödel's incompleteness theorems state, loosely, that a powerful enough theory of arithmetic cannot both be consistent and complete (and, moreover, cannot prove its own consistency unless it is inconsistent).

One theory that reasons about natural numbers and satisfies the conditions of Gödel's incompleteness theorems is Peano Arithmetic. It contains axioms defining basic properties of numbers (such as $\forall x\ x+1>0$) and an induction axiom scheme. Induction scheme consists of infinitely many axioms of the form $(\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x+1))) \rightarrow \forall x \phi(x)$, one for each possible formula ϕ. You can see that although there are infinitely many axioms, the theory can still be easily (efficiently) described.

As you know, numbers can be defined from sets and their properties proven from properties of sets. So Peano Arithmetic is weaker than than ZFC (consistency of PA can be proven in ZFC).

10.2 Proving Gödel's incompleteness theorem

Example of a theory of arithmetic: Peano Arithmetic. This was the kind of theory for which Hilbert wanted to prove the consistency.

- Equality is transitive.
- Natural numbers are recursively defined starting from 0 and adding 1 at each step of the recursion. Here, instead of "+1" sometimes people use the "successor" operation: $S(x) = x + 1$.
- For any x, $x + 1 > 0$ (can also be written as $S(x) > 0$).
- Induction works: if $\phi(0)$ holds and $\forall i$, $\phi(i) \rightarrow \phi(i+1)$ then $\forall n, \phi(n)$.
- Addition and multiplication satisfy algebraic axioms: $a+b=b+a$ and so on. Addition is defined using successor as $a + S(b) = S(a + b)$.
- $a \leq b$ is a total order.

A *model* of a theory is a set and interpretations of functions that satisfy the axioms. For example, Euclidean geometry without the parallel lines axiom has different models. E.g., a Mobius strip is not a model of Euclidean geometry, but it is a model of geometry without the fifth postulate.Riemann and Lobachevsky geometries.

A standard model of Peano arithmetic is natural numbers with the usual $=, +, *$ and so on on them.

Theorem 1 (Gödel's incompletenes theorems)**.** *1) Any effectively generated theory which can express elementary arithmetic cannot be both consistent and complete.*

2) Any such theory cannot prove the statement stating its own consistency (unless it is inconsistent and so can prove everything).

Idea of the proof of the first incompleteness theorem: construct a sentence G: "I am not provable". How do you say "I am" in arithmetic? The idea that the formulas can be enumerated (do a countability argument here). This technique is called arithmetization. Here, we end up saying "ϕ is a formula number n", where ϕ says "formula number n is not provable".

Gödel's numbers: a formula is a sequence of symbols $x_1x_2, x_3...x_n$ (for example, view each symbol as a byte). Then $G(x_1 \dots x_n) = 2^{x_1} \cdot 3^{x_2} \cdot p_n^{x_n}$ where p_n is the n^{th} prime number. Gödel uses this idea both to encode a formula as a number and a sequence of formulas (i.e., a proof) as a number.

Since a relation between formulas and proofs becomes a relation between two numbers, can define a formula $Bew(y) = \exists x(y$ is a Gödel number of a proof of the formula encoded by $y)$. The name Bew comes from German "Beweisbar" which translates as "provable".Now look at $\neg Bew(x)$. Then the statement $p \iff \neg Bew(p)$ says, more or less, "p is a Gödel number of an unprovable formula", and thus p says "my Gödel number is that of an unprovable formula".

For the intuition here, think of the two barbers who shave each other.