CS 2742 (Logic in Computer Science) – Fall 2011
Lecture 16

Antonina Kolokolova

October 28, 2011

6 A formal mathematical theory

In logic, the word *theory* has a very precise meaning: it is a set of formulas closed under consequence: that is, if formula A is a logical consequence of a formula B and B is in a theory, then A has to be there as well. However, this definition is not very easy to work with: for example, a theory of all formulas true about natural numbers with $+$ and $\cdot$ is an example of a theory, but how would we even know if a certain formula is true or false? We will see later that in this particular case, sometimes we can prove that we can not even tell if a given formula is true or false!

So another way to define a theory is *axiomatic*. In this case, a small set of formulas, usually easy to describe, is designated as *axioms*, and the theory in the previous sense consists of the set of axioms together with all other formulas, called *theorems*, which follow from them. For example, Euclid's 5 postulates are axioms of the theory of Euclid's geometry. Changing the parallel postulate (e.g., saying that more than one line can be drawn through a point not on a line that is parallel to a given line) would result in a different axiomatic system with different theorems.

So geometry on a plane is Eucledian, and geometry on a sphere is non-Eucledian, but what exactly do we mean saying that a set of axioms corresponds to a certain "situation in the real world"? What would be those "real worlds"?

Consider formulas talking about some predicates on the elements (e.g., divisibility and equality of natural numbers). We will use the term *structure* to denote a set of elements (universe) together with interpretations of predicates on that universe (call them "relations"). For example, a set can be $\mathbb{N}$, natural numbers, and predicates $x = y$, $x < y$, $x|y$, $+(x, y, z)$ and $\times(x, y, z)$ where $+$ and $\times$ are true on the triples such that sum (product) of x and y is equal to z. Now, a structure is a *model* for a given formula if this formula becomes true on this structure. Often we omit stating the predicates when they can be inferred from the context, and just talk about the universe. For example, we can say that $\mathbb{R}$ is a model for a formula stating that for every two numbers there is one in between them, but natural numbers $\mathbb{N}$ is not a model of this formula.

Finally, let's state two more definitions talking about the properties of the theories. A set of axioms is *consistent* if it does not imply a contradiction. This is a *syntactic* notion: we don't care about the models, just care whether with the rules of inference (like modus ponens) both A and $\neg A$ are derivable for some formula. If for a certain formula B both the theory together with B and the theory together with $\neg B$ are consistent, then we say that B is *independent* of that theory.

Two corresponding *semantic* notions relate theories to their models. A theory as a set of axioms and rules of inference allowing to derive theorems from these axioms is *sound* if everything that is derivable from the axioms is true in every model of the theory. Notice that a theory is consistent if and only if it has a model: the first is a *syntactic* notion of "being good", and the second is a *semantic* notion. A theory is *complete* if everything that is true in every model of the theory is actually derivable from the axioms.

6.1 Set theory as foundation for all mathematics

Set theory seems to be quite simple and generic, but exactly because it is so generic it is used, together with logic, as a foundation for all of mathematics. That is, the axioms that underlie the modern mathematics (in the same way as Euclid's postulates underlie geometry) are formulated in terms of first-order logic statements about sets. This axiomatization is called Zermelo-Fraenkel set theory (denoted ZFC).

You can ask why sets and not numbers. The reason is that numbers can be easily represented using set notation.

- When there are no elements, the only set we can construct is the empty set $\emptyset$. Let's call it a 0.
- Now that we have $\emptyset$, we can construct a second, different object $\{\emptyset\}$. This is a set containing $\emptyset$ as its element. Note that it is not equal to $\emptyset$ itself, because $\exists x(x \in \{\emptyset\})$ is true, whereas for $\emptyset$ this was false. Let's call $\{\emptyset\}$ a 1.
- There are two ways of constructing a 2. We can make it a $\{\{\emptyset\}\}$. But it is more convenient to make $2 \equiv \{\emptyset, \{\emptyset\}\} = \{0, 1\}$.
- Now, we can construct an arbitrary natural number $n+1$ recursively: $n+1 = n \cup \{n\}$. You can check for yourself that this definition is the same as was used to construct 1 and 2.

For this definition of natural numbers $i < j$ can be stated as $i \subset j$ or $i \in j$. This is the only time $i \subset j$ and $i \in j$ mean the same thing! Usually, these two are very different, but we specially defined natural numbers in such a way that both notations mean less-than relation.

6.2 Barber of Seville (Russell's paradox)

Zermelo-Fraenkel set theory was very carefully constructed to rule out "strange" things happening. The original attempts to axiomatize mathematics were prone to the following paradox, discovered by Bertrand Russell. The paradox lies in the definitions of sets in terms of themselves, which, unless ruled out, leads to strange consequences.

Informally, Russell's paradox is illustrated by the following story. In the town of Seville (which has nothing to do with the real town of that name) there is a (male) barber, who shaves everybody who does not shave himself. Who shaves the barber?

If you say that the barber himself does, then he should not because he only shaves people who do not shave themselves. But if he doesn't, then he should for exactly the same reason.

The set-theoretic notion that corresponds to this paradox is definition of a set in terms of itself. Let $B = \{x \mid x \text{ does not shave himself}\}$. This B exactly "defines" the barber. But is $B \in B$? This is a paradox, akin to the liar's paradox, and we will see versions of it coming up in other contexts as well.

Note that defining a set in that way does not always lead to a contradiction. Consider these two barbers[1]:

- Arturo is the barber and any X other that himself A shaves X iff X doesn't shave A.
- Roberto shaves X iff X does shave Roberto.

Neither of these definitions poses a contradiction. However, consider the following puzzle:

Puzzle 1. Can both Arturo and Roberto live in Seville?

Yet another puzzle illustrated how sometimes one can construct sets, but the sets have to satisfy unexpected requirements.

Puzzle 2. In a certain barber's club,

- Every member shaved at least one other member.

[1]Most of the material here is adapted from Raymond Smallian's book *To mock a mockingbird*

- No member shaved himself.
- No member has been shaved by more than one member
- There is one member that has never been shaved by club members.

How many barbers are in the club?

This seems like a strange question to ask – nothing in the puzzle said much about the number of barbers in the club. [2] But indeed these condition determine the number of members: for such a club to exists, there must be infinitely many barbers in it. This is a version of PigeonHole Principle that you have seen before: it says that for infinite numbers of holes, the principle does not hold (at least the way we stated it).

[2] This is somewhat similar to the puzzle about the colour of bear's hide, in a sense that the puzzle contains all the information needed to solve it, given some common knowledge, however the question of the puzzle is seemingly unrelated to the statement: a hunter stands 100 meters to the south of a bear. He walks 100m east, turns to the north and shoots that same bear. What colour is bear's hide?