Scuola Superiore di Catania

Corso Specialistico

a.a. 2018-2019

(Un)decidability, automata, and algorithmic complexity

This course examines some selected topics from the theory of computability, a subfield of mathematical logic.

The first part of the course is devoted to Finite State Automata (FSA), which are at the core of the notion of computability. Though FSA model computability with very limited—most limited, to be precise—amount of memory, they are a wonderful scenario to study algorithms (and launch races about their complexity) that aim at minimizing the amount of resources employed to solve challenging problems. Another interesting aspect for studying FSA is the fact that they can be "read" in many different ways. The two most popular ones are (labelled) graphs and (hereditarily finite) sets. In both cases, a number of problems/techniques come naturally up and suggest extremely stimulating areas of study. In this part of the course, starting from the notion of Finite State Automaton, we quickly review the basic results of the field. Then we illustrate the different ways in which the problem of minimizing the number of states of an automaton accepting a given language can be tackled. In doing so we will move in a number of directions:

(1) Algorithmic: we will study the "classics" in the field of minimization algorithms for deterministic automata, as well as their possible extensions to the non-deterministic case.

(2) Enhancement of expressivity: we will discuss more expressive variants of the notion of FSA, addressing the corresponding minimization problems.

(3) Set-theoretic: we will see a rewriting of the above problems into set-theoretic terms, with matching algorithmic and expressivity issues.

The second part offers an accurate mathematical presentation, as well as a historical recollection, of the main achievements which led to the negative solution of Hilbert's tenth problem: "Does there exist any general algorithm which, for any given Diophantine equation (namely, a polynomial equation with integer coefficients and a finite number of unknowns) can decide whether the equation has a solution with all unknowns taking integer values? Such a renowned negative result, often referred to as Davis-Putnam-Robinson-Matiyasevich Theorem, have set up a formidable–but by no means abstruse–combinatorial machinery, teaching us how to model whatsoever computation by way of Diophantine polynomial equations. In bridging the gap between equations of this kind and the exponential Diophantine equations, the study of Pell's equations with their infinitely many solutions, plays a crucial role. As will also be reported, some fragments of set theory were shown to be undecidable via reductions of Hilbert's Tenth problem.

More in detail, this part of the course will deal with:

4) The Davis-Putnam-Robinson theorem: "Every listable set of n-tuples of natural numbers is representable by means of an exponential Diophantine equation". This will be shown along the lines of a proof due to James Jones and Yuri Matiyasevich, that refers to a characterization of computable functions based on register machines.

(5) Matiyasevich's theorem: "Exponentiation, seen as a set of triples of natural numbers, is representable by means of a polynomial Diophantine equation". This will be shown along lines of a proof due to Julia Robinson and Yuri Matiyasevich, that exploits the rich combinatorics associated with the Pell equation. Combination of this theorem with the above-indicated theorem (1), leads to the very important DPRM theorem: "Every listable set of n-tuples of natural numbers is representable by means of a polynomial Diophantine equation".

(6) Universal Diophantine equation. The above-indicated theorems (1) and (2) yield the algorithmic unsolvability of Hilbert's tenth problem, restrained to all instances of a single, parametric polynomial Diophantine equation: this special equation encompasses, in a precise mathematical sense, the family of all polynomial Diophantine equations.

(7) A set-theoretic reduction of Hilbert’s tenth problem, which allows one to prove the undecidability of the decision problem for set-theoretic formulae with restricted quantifiers and a single quantifier alternation, along with the undecidability of a fragment of set theory with the Cartesian product and a cardinality comparison. By dropping multiplication from the language of polynomial equations, while allowing propositional connectives and any form of quantifier alternation, one obtains the well-known Presburger arithmetic, namely, the first-order theory of natural numbers with addition. In the third part of the course it will be shown that the decision problem for Presburger arithmetic and some of its extensions is solvable. In particular, we prove the decidability of

(8) Presburber arithmetic,

(9) the extension of Presburber arithmetic with homogeneous exponentiation, and

(10) the extension of Presburber arithmetic with sets.