Scuola Superiore di Catania

CORSO SPECIALISTICO
a.a. 2017-2018

Introduction to Computational Complexity

Computational Complexity is a fascinating field of study that lies on the border between theoretical computer science and mathematics. In a nutshell, it classifies computational problems in terms of their "difficulty", i.e. the resources (such as computational time and space) required to solve them.
This classification leads to the introduction of numerous complexity classes such as P, NP, PSPACE, BPP and many others.

Computational Complexity has numerous applications in computer science, mathematics and science in general. Moreover, it is the home of one of the deepest and most fundamental open question in mathematics, namely whether the class P is strictly included in NP or not.

The course is roughly organized in three parts. A tentative description of the contents of the course follows.

Part 1 will be devoted to the introduction of computational models, basic complexity classes (such as the class P, NP, co-NP and PSPACE) and their relationship. More in detail, here we will cover the following topics.
1. Modeling Computation: Turing machines, efficiency and running time. (Un)computability. The class P.
2. The class NP: Reducibility and NP-completeness, the Cook-Levin theorem. coNP, EXP and NEXP.
3. Diagonalization. Time Hierarchy Theorems. Oracle Machines and the limits of diagonalization.
4. Space complexity. Space bounded computation. PSPACE.

Part 2 will further investigate basic complexity classes by introducing topics such as the polynomial hierarchy, randomized computation and boolean circuits. More in detail, the part of the class will be devoted to the following topics.
5. The polynomial hierarchy and alternations.
6. Boolean Circuits. The class P/poly. P/poly and NP. Circuits lower bounds
7. Randomized Computation. Probabilistic Turing Machines. The classes RP, ZPP and BPP. Relations between BPP and other classes.

Finally in **part 3** we will consider slightly more advanced material. A potential topic could be interactive proofs and their interplays with cryptography. Time permitting, we might also introduce the powerful machinery of probabilistically checkable proofs (PCP).

Each part will, roughly, require 10-12 hours.