CS-602

Foundation of probabilistic proofs

Chiesa Alessandro

Cursus	Sem.	Type
Computer and Communication Sciences		Opt.

Language of teaching	English
Credits	6
Session	
Exam	Multiple
Workload	180h
Hours	**56**
Courses	42
Exercises	14
Number of positions	

Frequency

Only this year

Summary

Probabilistic proof system (eg PCPs and IPs) have had a tremendous impact on the theoretical computer science, and have also found practical uses. They underlie delegation of computation protocols and hardness of approximation. This course covers the foundations of probablistic proof systems.

Content

Proofs are at the foundations of mathematics, and verifying the correctness of a mathematical proof is a fundamental computational task. (The P versus NP problem, which deals precisely with the complexity of proof verification, is one of the most important open problems in all of mathematics.) The complexity-theoretic study of proof verification has led to new notions of mathematical proofs, such as Interactive Proofs, Probabilistically Checkable Proofs, and others. These probabilistic proofs have had a tremendous impact on theoretical computer science and, more recently, are playing an exciting role in applied cryptography, computer security, and blockchain technology. Probabilistic proofs are a powerful tool for proving hardness of approximation results, and are an essential building block to achieve delegation of computation (protocols that enable super fast verification of long computations, such as SNARKs).

This course provides an introduction to probabilistic proofs and the beautiful mathematics underlying them, and prepares students for conducting research in this area. Covered topics include arithmetization, the sumcheck protocol, zero knowledge, doubly-efficient interactive proofs, linearity testing, low-degree testing, proof composition, succinct verification, and more.

This courses assumes familiarity with algorithms (asymptotic notation and analysis of algorithms), complexity theory (computation models and basic complexity classes), and some algebra (finite fields and their properties).

Assessment methods

Evaluation: written homeworks and class participation, written final project