Why MCSP Is a More Important Problem Than SAT

Rahul Santhanam
Department of Computer Science, University of Oxford, UK

Abstract

CNF Satisfiability (SAT) and its variants are generally considered the central problems in complexity theory, due to their applications in the theory of NP-completeness, logic, verification, probabilistically checkable proofs and parameterized complexity, among other areas. We challenge this conventional wisdom and argue that analysing the Minimum Circuit Size Problem (MCSP) and its relatives is more important from the perspective of fundamental problems in complexity theory, such as complexity lower bounds, minimal assumptions for cryptography, a robust theory of average-case complexity, and optimal results in hardness of approximation.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

Keywords and phrases Minimum Circuit Size Problem, Satisfiability, Cryptography, Learning, Approximation

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2022.2

Category Invited Talk

Funding Partially funded by EPSRC New Horizons Grant EP/V048201/1.