Highly-Efficient Local Proofs and Codes

Noga Ron-Zewi
Department of Computer Science, University of Haifa, Israel

Abstract

Interactive oracle proofs (IOPs) extend the classical notion of probabilistically-checkable proofs (PCPs) by allowing a verifier to interact with a prover over a small number of rounds, while querying the prover's messages in only a few locations.

A recent line of work gave highly-efficient IOPs outperforming state-of-the-art PCPs, for example, constant-round and constant-query (ZK-)IOPs with only a linear (and even approaching the witness length) amount of communication, as well as (ZK-)IOPs with linear-time prover complexity. These constructions were leveraged in turn to obtain highly-efficient succinct arguments and zero-knowledge proofs.

The improved efficiency was obtained by replacing polynomial-based codes, commonly used in such proof systems, with more efficient (tensor-based) codes. In particular, these constructions bypassed a barrier imposed by the need to encode the computation using a multiplication code.

In the talk I will survey these highly-efficient IOP constructions, and highlight some interesting open problems raised by these works.

2012 ACM Subject Classification Theory of computation → Interactive proof systems

Keywords and phrases Interactive oracle proofs, probabilistically-checkable proofs, error-correcting codes

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.2

Category Invited Talk

Funding Funded/Co-funded by the European Union (ERC, ECCC, 101076663). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

51st International Symposium on Mathematical Foundations of Computer Science (MFCS 2026).
Editors: Michal Koucký and Daniela Petrişan; Article No. 2; pp. 2:1–2:1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany