Arnon, Gal; Chiesa, Alessandro; Yogev, Eylon
A PCP theorem for interactive proofs and applications. (English) Zbl 1497.68207


Summary: The celebrated PCP Theorem states that any language in NP can be decided via a verifier that reads $O(1)$ bits from a polynomially long proof. Interactive oracle proofs (IOP), a generalization of PCPs, allow the verifier to interact with the prover for multiple rounds while reading a small number of bits from each prover message. While PCPs are relatively well understood, the power captured by IOPs (beyond NP) has yet to be fully explored.

We present a generalization of the PCP theorem for interactive languages. We show that any language decidable by a $k(n)$-round IP has a $k(n)$-round public-coin IOP, where the verifier makes its decision by reading only $O(1)$ bits from each (polynomially long) prover message and $O(1)$ bits from each of its own (random) messages to the prover. Our result and the underlying techniques have several applications. We get a new hardness of approximation result for a stochastic satisfiability problem, we show IOP-to-IOP transformations that previously were known to hold only for IPs, and we formulate a new notion of PCPs (index-decodable PCPs) that enables us to obtain a commit-and-prove SNARK in the random oracle model for nondeterministic computations.

For the entire collection see [Zbl 1493.94002].

MSC:
68Q10 Modes of computation (nondeterministic, parallel, interactive, probabilistic, etc.)
68Q11 Communication complexity, information complexity
68Q15 Complexity classes (hierarchies, relations among complexity classes, etc.)
94A60 Cryptography

Keywords: interactive proofs; probabilistically checkable proofs; interactive oracle proofs

Software:
Marlin; Geppetto; libiop

Full Text: DOI

References:
[8] Ben-Sasson, E.; Bentov, I.; Horesh, Y.; Riazi, M.; Boldyreva, A.; Micciancio, D., Scalable zero knowledge with no trusted


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.