Goldreich, Oded; Gur, Tom; Rothblum, Ron D.

Summary: Proofs of proximity are proof systems wherein the verifier queries a sublinear number of bits, and soundness only asserts that inputs that are far from valid will be rejected. In their minimal form, called $MA$ proofs of proximity ($MAP$), the verifier receives, in addition to query access to the input, also free access to a short (sublinear) proof. A more general notion is that of interactive proofs of proximity ($IPP$), wherein the verifier is allowed to interact with an omniscient, yet untrusted prover.

We construct proofs of proximity for two natural classes of properties: (1) context-free languages, and (2) languages accepted by small read-once branching programs. Our main results are:

1. $MAP$s for these two classes, in which, for inputs of length $n$, both the verifier’s query complexity and the length of the $MAP$ proof are $\tilde{O}(\sqrt{n})$.
2. $IPP$s for the same two classes with constant query complexity, poly-logarithmic communication complexity, and logarithmically many rounds of interaction.

MSC:
68Q45 Formal languages and automata
03F20 Complexity of proofs
68Q25 Analysis of algorithms and problem complexity
68T15 Theorem proving (deduction, resolution, etc.) (MSC2010)
68W20 Randomized algorithms

Keywords:
property testing; probabilistic proof systems; interactive proofs

Software:
ALGOL 60

Full Text: DOI

References:


[19] Lewis, P. M.; Stearns, R. E.; Hartmanis, J., Memory bounds for recognition of context-free and context-sensitive languages, (SWCT (FOCS), (1965)), 191-202


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.