Abstract:

We present a new model of probabilistically checkable proof (PCP), which we call "Distributed PCP":

A satisfying assignment \(x \in \{0,1\}^n\) to a CNF formula is shared between two parties (Alice knows \(x_1, \ldots x_{n/2}\), and Bob knows \(x_{n/2+1}, \ldots, x_n\)).

Their goal is to jointly write a PCP for \(x\), while exchanging little or no information.

Using our new framework, we obtain, for the first time, PCP-like reductions from the Strong Exponential Time Hypothesis (SETH) to approximation problems in P.

In particular, we show that (assuming SETH) there are no truly subquadratic approximation algorithms for the following problems:

- Maximum Inner Product over \(\{0,1\}\)-vectors;
- LCS Closet Pair over permutations;
- Approximate Partial Match;
- Approximate Regular Expression Matching; and
- Diameter in Product Metric.

All our inapproximability factors are nearly-tight. In particular, for the first three problems we obtain nearly-polynomial factors of \(2^{(\log n)^{1-o(1)}}\);

only \((1+o(1))\) SETH lower bounds were known for these problems before our work.

Joint work with Amir Abboud.