Eylon Yogev Bar Ilan University

IOPs with Inverse Polynomial Soundness Error

Abstract:

We show that every language in NP has an Interactive Oracle Proof (IOP) with inverse polynomial soundness error and small query complexity. This achieves parameters that surpass all previously known PCPs and IOPs. Specifically, we construct an IOP with perfect completeness, soundness error $1/n$, round complexity $O(\log \log n)$, proof length $\text{poly}(n)$ over an alphabet of size $O(n)$, and query complexity $O(\log \log n)$. This is a step forward in the quest to establish the sliding-scale conjecture for IOPs (which would additionally require query complexity $O(1)$). Our main technical contribution is a high-soundness small-query proximity test for the Reed–Solomon code. We construct an IOP of proximity for Reed–Solomon codes, over a field $F$ with evaluation domain $L$ and degree $d$, with perfect completeness, soundness error (roughly) $\max\{1-\delta, O(\rho^{1/4})\}$ for $\delta$-far functions, round complexity $O(\log \log d)$, proof length $O(|L|/\rho)$ over $F$, and query complexity $O(\log \log d)$; here $\rho = (d+1)/|L|$ is the code rate. In route, we obtain a new high-soundness proximity test for bivariate Reed–Muller codes. The IOP for NP is then obtained via a high-soundness reduction from NP to Reed–Solomon proximity testing with rate $\rho = 1/\text{poly}(n)$ and distance $\delta = 1-1/\text{poly}(n)$ (and applying our proximity test). Our constructions are direct and efficient, and hold the potential for practical realizations that would improve the state-of-the-art in real-world applications of IOPs. Joint work with Gal Arnon and Alessandro Chiesa