Quantum Codes, Local Testability and Interactive Proofs: State of the Art and Open Questions

Thomas Vidick ✉
Weizmann Institute of Science, Rehovot, Israel
California Institute of Technology, Pasadena, CA, USA

Abstract

The study of multiprover interactive proof systems, of locally testable codes, and of property testing are deeply linked, conceptually if not formally, through their role in the proof of the PCP theorem in complexity theory. Recently there has been substantial progress on an analogous research programme in quantum complexity theory. Two years ago we characterized the power of multiprover interactive proof systems with provers sharing entanglement, showing that MIP* =RE [4], a hugely surprising increase in power from the classical result MIP=NEXP of [2]. The following year Panteleev and Kalachev gave the first construction of quantum low-density parity-check codes (QLDPC) [5], thus marking a major step towards the possible realization of good quantum locally testable codes – the classical analogue of which was only constructed quite recently [3]. And finally, less than a year ago Anshu, Breuckmann and Nirkhe used facts evidenced in the construction of good decoders for the new QLDPC codes to resolve the NLTS conjecture [1], widely viewed as a crucial step on the way to a possible quantum PCP theorem.

In the talk I will survey these results, making an effort to motivate and present them to the non-expert. I will explain the connections between them and point to where, in my opinion, our understanding is currently lacking. Along the way I will highlight a number of open problems whose resolution could lead to further progress on one of the most important research programmes in quantum complexity theory.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases quantum interactive proofs, quantum codes

Digital Object Identifier 10.4230/LIPIcs.ICALP.2023.4

Category Invited Talk

References

1 Anurag Anshu, Nikolas Breuckmann, and Chinmay Nirkhe. NLTS Hamiltonians from good quantum codes. *arXiv preprint*, 2022. arXiv:2206.13228.
2 László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1:3–40, 1991.
3 Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 357–374, 2022.
4 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. arxiv e-prints, page. *arXiv preprint*, 2020. arXiv:2001.04383.
5 Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022.