The Hebrew University of Jerusalem
The Rachel and Selim Benin School of Computer Science and Engineering

Ph.D Research Aims.

David Ponarovsky

Under the supervision of Prof. Michael Ben Or

August 2023

Chapter 1

Research Aims.

Although it may seem that quantum computing is just around the corner, we still do not understand it as well as we understand classical computing. The purpose of my Ph.D. studies is to bridge this gap by focusing on the quantum PCP conjecture, which is known to be true in the classical case [Aro+98] and is believed to hold in the quantum regime as well. The conjecture is stated as follows: consider the promise decision problem, where a classical description of a local Hamiltonian is provided. One must determine whether the ground energy is greater than b or less than a, while being promised that $b - a$ is greater than a constant number independent of the description length. This problem is **QMA**-complete, which means that any decision problem whose solution can be verified by a quantum machine in a reasonable time can also be reduced to a decision problem in which, using a quantum machine, one can verify a candidate solution by doing a constant amount of work and failing in probability proportional to the closeness to an actual valid proof.

As the proof for the classical conjecture relies on the existence of error correction codes with specific properties, our strategy is to enhance our understanding of quantum error correction codes. In particular, we aim to develop quantum testable codes, which are codes that allow us to determine whether a given state is in the code by querying a constant amount of bits and failing with a probability proportional to the distance of the state from the code.

The constructions we are examining are variations of the Hyperproduct codes [TZ14], quantum Tanner codes [LZ22], polynomial codes, and mixtures of all three. We also aim to determine what properties, known to be useful for fault tolerance applications, can be induced from local structures. Testability, as mentioned, is one of them. Another one is satisfying a certain multiplication relations between codewords. This property has proven to be useful for efficient distillation of magic states [BH12]. We believe that having good qLDPC codes satisfying that property will result in even better distillation protocols in terms of computing time, space complexity, and immunity to noise.

In summary, our aim is to tackle important problems in quantum complexity that, if answered, would enrich our understanding of quantum computation in a conceptual sense and potentially yield new ways to think about applicable structures, with an emphasis on quantum error correction codes.

Bibliography

[Aro+98]   Sanjeev Arora et al. "Proof Verification and the Hardness of Approximation Problems". In: *J. ACM* 45.3 (May 1998), pp. 501–555. ISSN: 0004-5411. DOI: 10.1145/278298.278306. URL: https://doi.org/10.1145/278298.278306.

[BH12]   Sergey Bravyi and Jeongwan Haah. "Magic-state distillation with low overhead". In: *Physical Review A* 86.5 (2012), p. 052329.

[TZ14]   Jean-Pierre Tillich and Gilles Zemor. "Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength". In: *IEEE Transactions on Information Theory* 60.2 (Feb. 2014), pp. 1193–1202. DOI: 10.1109/tit.2013.2292061. URL: https://doi.org/10.1109%2Ftit.2013.2292061.

[LZ22]   Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes.* 2022. arXiv: 2202.13641 [quant-ph].