Research Proposal

Qian Zhang

March 14, 2021

Quantum Computation had been recognized as a novel model of computation since its formal discussion in the 1990s. There has been noticeable progress on the implementation of Quantum Computing Units in recent decades, while there are still important theoretical questions about the model yet to be answered. My proposed study discusses the theoretical aspect of quantum computer around the central problem:

> Is there an exponential separation between the quantum computation model and the Turing machine? Shor et al. showed in [2] that there exists an $O((\log N)^3)$ time algorithm for factoring a positive integer N, which gives an exponential speedup compared to classical algorithms. If such efficient factoring is impossible on a classical computer, the result would imply $P \neq NP$ and clarify the relationship between quantum computer and classical complexity classes.

This question, of course, refers to the long-standing problem of whether $P \neq NP$ which leads to many significant results and may take years to answer. However, there are problems related to the topic which may serve specific purposes or are of mathematical interest. For example:

> 1. Graph Property Testing. The graph testing problems are known to be hard to achieve significant speedup with quantum algorithms due to symmetry[1]. Ambainis et al. showed in [11] that at most a polynomial advantage is possible for testing expansion and bipartiteness, and asked whether an exponential speedup is ever possible for graph property testing. Andrew et al. showed in [3] that there is a graph property with exponential quantum speedup in the adjacency list model. I am therefore interested in if there is an exponential separation for graph property testing using this model, and what specifically prevents the speedup in other graph representations.
>
> 2. Quantum Communication Complexity. Communicational Complexity is one of the few areas where one can establish unconditional

> exponential separations according to [4]. The model of Communicational Complexity is widely used in complexity theory, and Kundu et al. recently proved in [13] the direct product theorem for one-way quantum communication. I am interested in the power of one-way quantum communication compared to randomized one-way protocol, and the result of applying it, for example, on distribution testing as discussed in [5].

I believe that we are able to better understand the power and limits of the quantum computer model by discussing the above topics. During the PhD program, I am interested in working on the upper and lower bounds of solving graph-theoretic problems in quantum computation context as the main focus.

For example, the CONGEST model considers a setting where nodes communicate over some network graph G with a limited number of bits, and studies the complexity of detecting properties of G or computing graph structures. The CONGEST model, as well as the CONGEST CLIQUE model which allows communication between nodes without an edge, has been extensively studied in recent years [7] and there are encouraging results from using both classical and quantum algorithms. Jurdzinski et al. showed in [6] that there is a distributed randomized algorithm finding Minimum Spanning Tree of a given graph in $O(1)$ rounds, with high probability in the CONGEST CLIQUE model. There is also a result on triangle finding by Izumi et al. which improves the upper bound to $O(n^{0.25})$ round using a quantum distributed algorithm with the CONGEST model in [8]. Censor-Hillel et al. had further worked on the generalized problem of p-clique listing and gave an $O(n^{1-2/p})$-round distributed algorithm that lists all p-cliques K_p in the communication network for each $p \geq 4$ in [9].

In the related problem of finding a $(\Delta + 1)$-vertex coloring in a graph with maximum node degree of Δ, Halldorsson et al. showed in [10] a randomized distributed algorithm which takes $O(\log^5 \log n)$ rounds in CONGEST model, which was the lower bound for the more powerful LOCAL model before. There is an even faster algorithm shown in [12] recently by Halldorsson et al. which computes the vertex coloring in $O(\log \log n)$ CONGEST rounds. I am interested to study if there exists any quantum algorithm that would allow speedup for this problem which can be already solved so quickly in the classical CONGEST model like in [8], and if so, to what exact extent.

The brief overview and comment on current theoretical quantum computation problems conclude my research proposal as a prospective PhD student. By working on these questions, I wish to approach a comprehensive conclusion on the power of quantum computation via different models of computing including but not limited to the ones mentioned above and contribute to our knowledge about the theory of computation in general.

References

[1] Ashley Montanaro, Ronald de Wolf. A Survey of Quantum Property Testing. arXiv:1310.2035.

[2] Shor, Peter W., Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J.Sci.Statist.Comput., 1999, 41 (2): 303–332, doi:10.1137/S0036144598347011, arXiv:quant-ph/9508027v2.

[3] Andrew M. Childs, Daochen Wang. Can graph properties have exponential quantum speedup? arXiv:2001.10520v1.

[4] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, Ronald de Wolf. Exponential separation for one-way quantum communication. arXiv:quant-ph/0611209v3.

[5] Aleksandrs Belovs, Arturo Castellanos, François Le Gall, Guillaume Malod, Alexander A. Sherstov. Quantum Communication Complexity of Distribution Testing. arXiv:2006.14870v1.

[6] Tomasz Jurdzinski, Krzysztof Nowicki. MST in O(1) Rounds of Congested Clique. arXiv:1707.08484.

[7] Andrew Drucker, Fabian Kuhn, Rotem Oshman. On the Power of the Congested Clique Model. PODC '14: Proceedings of the 2014 ACM symposium on Principles of distributed computing, July 2014, Pages 367–376, https://doi.org/10.1145/2611462.2611493.

[8] Taisuke Izumi, François Le Gall, Frédéric Magniez, Quantum Distributed Algorithm for Triangle Finding in the CONGEST Model, arXiv:1908.11488.

[9] Keren Censor-Hillel, Yi-Jun Chang, François Le Gall, Dean Leitersdorf, Tight Distributed Listing of Cliques, arXiv:2011.07405.

[10] Magnús M. Halldórsson, Fabian Kuhn, Yannic Maus, Tigran Tonoyan, Efficient Randomized Distributed Coloring in CONGEST, arXiv:2012.14169.

[11] Andris Ambainis, Andrew M. Childs, and Yi-Kai Liu, Quantum Property Testing for Bounded-degree Graphs, Proceedings of the 14th International Workshop and 15th International Conference on Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 2011, pp. 365–376.

[12] Magnus M. Halldorsson Alexandre Nolin, Superfast Coloring in CONGEST via Efficient Color Sampling, arXiv:2102.04546v2.

[13] Rahul Jain, Srijita Kundu, A Direct Product Theorem for One-Way Quantum Communication, arXiv:2008.08963.