Survey: Advances in Quantum Communication Complexity

Bachelor's Thesis

In a recent paper Hhan [Hha25] proved tight lower bounds for computing discrete logarithms on a quantum computer by employing average-case communication lower bounds. In the discrete logarithm problem relative to a (multiplicative) group $\mathcal{G}$, the input is (g, g^x) with generator $g \in \mathcal{G}$ and $x \sim [|\mathcal{G}|]$ uniformly random and the goal is to compute x. While the problem is believed to be hard classically, a quantum algorithm can apply essentially Shor's algorithm to find x in only $\mathcal{O}(\log |\mathcal{G}|)$ group operations. Hhan proved this to be tight in a model which abstracts away the specific group $\mathcal{G}$ and his high-level idea is to frame the discrete logarithm problem as a communication task. This approach seems very intuitive given that x has Shannon entropy $\log |\mathcal{G}|$.

The proof is conceptually simple but non-trivial to adapt to other problems due the fact that different scenarios may require different communication lower bounds. The original result by Hadiashar [BH14, Section 3] proves a lower bound for classical messages which was recently [KL26] generalized to *flat states* (instead of transmitting a message x, the result now needs to be in a given subspace).

Hence, in this thesis the student is supposed to survey the landscape of quantum communication complexity with a focus on remote state preparation protocols. In particular, we are interested in an analysis of the lower bounds for different types of states. A highly motivated student may also attempt to prove new lower bounds for restricted classes of states.

We emphasize the technically challenging nature of these problems due to the interplay of different topics in quantum information theory and mathematics which is ideal for a *mathematics student*.

Scope of the work

- Give an overview of quantum communication complexity and different models on might consider
- Discuss known lower bounds on remote state prepation tasks.
- Analyze the known bounds for different types of states and tasks.
- **Optional:** Attempt to prove new lower bounds for restricted classes of quantum states.

Requirements

- Strong **linear algebra skills**
- Interest in theoretical computer science
- Motivated in learning about quantum information theory

Contact

Julien Meier, julien.meier@kit.edu (Room 257, Building 50.34).

Literatur

[BH14] Shima Bab Hadiashar. "Communication complexity of remote state preparation". In: (2014). URL: https://dspacemainprd01.lib.uwaterloo.ca/server/api/core/bitstreams/4ec3225c-14e2-45c8-ace7-62d681a9188d/content.

[Hha25] Minki Hhan. “A New Approach to Generic Lower Bounds: Classical/Quantum MDL, Quantum Factoring, and More”. In: *Advances in Cryptology – EUROCRYPT 2025*. Hrsg. von Serge Fehr und Pierre-Alain Fouque. Cham: Springer Nature Switzerland, 2025, S. 345–374. URL: `https://arxiv.org/pdf/2402.11269`.

[KL26] Srijita Kundu und Olivier Lalonde. “Near-optimal entanglement-communication tradeoffs for remote state preparation”. In: *arXiv preprint arXiv:2602.09428* (2026). URL: `https://arxiv.org/pdf/2602.09428`.