

Even More Explicit Separations for Unitary Synthesis

Master's Thesis

At the heart of quantum cryptography lies the idea that one could use quantum states for cryptographic purposes. While earlier approaches deal with information-theoretic security, the last decade has shifted the focus towards the use of *inherently-quantum computational assumptions*. Indeed, there is a wide range of such assumptions with perhaps the most prominent being pseudorandom quantum states that, informally, “look” like actual random states to a computationally-bounded quantum adversary. An attacker that is willing to invest a superpolynomial number of quantum gates will notice the difference, but what if they “only” use a superpolynomial number of classical operations and a *polynomial number of quantum gates*?

The unitary synthesis problem (USP), posed in 2007 by Aaronson and Kuperberg [AK07], deals with essentially the same question but more extreme and phrased from a *complexity-theoretic perspective*:

Is there a universal polynomial-size quantum algorithm $\mathcal{A}$ that can approximate any unitary $U \in \mathbb{C}^{2^n \times 2^n}$ to inverse-exponential precision (in n) given oracle access to a boolean function $f : \{0, 1\}^{\ell(n)} \rightarrow \{0, 1\}$ (that may arbitrarily depend on U)?

In other words, does implementing unitaries on a quantum computer “efficiently” reduce¹ to computing classical functions? If the answer to the USP turned out to be negative, this would imply that there could be quantum cryptographic protocols (namely quantum bit commitments) that exist even if we could solve the Halting problem!

Unsurprisingly, the question is still wide open with fairly little progress. However, in 2024, [LMW24] was finally able to prove a *one-query lower bound* for the USP, i.e., there are families of unitaries that cannot be synthesized with only a single query to an oracle f . What may sound like a funny anecdote, is actually a suprisingly technical yet elegant result: They relax the USP statement to an indistinguishability game and bound the success probability in terms of an operator norm using matrix concentration inequalities. Based on the techniques of [LMW24], a very recent follow-up paper, [DLM26], proved explicit families of unitaries to be hard for one-query adversaries while others admit attacks.

In this thesis, the student is supposed to apply the ideas of [DLM26] to other families of unitaries to build a deeper understanding for the hardness conditions of the one-query USP. Further, we have specific directions in mind on extending their framework and other additional questions on more fine-grained analyses. The actual scope needs to be discussed depending on individual preferences.

Scope of the work

- Analyze additional families of unitaries for one-query synthesis.
- **Optional:** Extend their framework to a (specific) different scenario.
- **Optional:** Analyze the proven lower bounds for “robustness.”

Requirements

- Strong **linear algebra skills**
- Interest in theoretical computer science
- Basic knowledge on quantum information theory

¹Here, the choice of f for given unitary U is allowed to be inefficient while $\ell(n)$ should be polynomial in n .

Contact

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

Please refrain from sending me AI-generated emails.

Literatur

- [AK07] Scott Aaronson und Greg Kuperberg. “Quantum versus classical proofs and advice”. In: *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007, S. 115–128. URL: <https://www.scottaaronson.com/papers/qcap.pdf>.
- [DLM26] Fangqi Dong, Alex Lombardi und Fermi Ma. “Explicit Separations for One-Query Unitary Synthesis”. In: *arXiv preprint arXiv:2607.26478* (2026). URL: <https://arxiv.org/pdf/2607.26478>.
- [LMW24] Alex Lombardi, Fermi Ma und John Wright. “A one-query lower bound for unitary synthesis and breaking quantum cryptography”. In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*. 2024, S. 979–990. URL: <https://arxiv.org/pdf/2310.08870>.