A Collapse-free Quantum Algorithm for a Problem in QSZK

Henrique Hepp[1], **Murilo V. G. da Silva**[1], **Leandro M. Zatesko**[2]

[1]Department of Informatics, Federal University of Paraná, Brazil

[2]Academic Department of Informatics, Federal University of Technology — Paraná, Brazil

{hhepp,murilo}@inf.ufpr.br, zatesko@utfpr.edu.br

Abstract. *The complexity class of the problems that can be solved by a quantum algorithm in a non-adaptive collapse-free model is called* naCQP*. This class was introduced in 2016 by Aaronson et al. to be an apparently slightly larger class than* BQP*: larger enough to include important* NP*-intermediate candidate problems, but likely not to include* NP*-complete problems: Aaronson et al. showed that there is an oracle A for which $\mathsf{NP}^A \not\subseteq \mathsf{naCQP}^A$; and, in a paper published this year in* Theor. Comput. Sci.*, we showed that relative to an oracle A chosen uniformly at random, $(\mathsf{UP} \cap \mathsf{coUP})^A \not\subseteq \mathsf{naCQP}^A$ with probability 1, being $\mathsf{UP} \cap \mathsf{coUP}$ a subclass of* NP*. Amongst the* NP*-intermediate candidate problems in* naCQP *is the entire class* SZK*, of the problems that admit a statistical zero-knowledge interactive proof system. The relation between* QSZK*, which is the class of the problems that admit a* quantum *zero-knowledge interactive proof system, and* naCQP *is unknown, with some believing that there is an oracle A for which $\mathsf{QSZK}^A \not\subseteq \mathsf{naCQP}^A$. A complete promise problem for* QSZK *is the trace distance distinguishability of* mixed *quantum states. We show that this problem, when restricted to* pure *quantum states, is in* naCQP*.*

1. Introduction

Throughout this text, we assume that the reader is familiar with the basics of Computational Complexity and Quantum Computing. For a reference on these topics, we refer the reader to [Arora and Barak 2009] and [Nielsen and Chuang 2010], respectively. We also refer the reader to [Watrous 2002] for definitions concerning statistical and quantum zero-knowledge proofs, although they are not necessary here.

Quantum algorithms have been receiving much attention in the last decades due to their ability to solve in polynomial time some important problems believed to be NP-intermediate, such as Integer Factorisation [Shor 1994] and the Hidden Subgroup Problem for abelian groups [Kitaev 1995]. A noteworthy class of problems believed to be NP-intermediate (although yet not even shown to be contained in NP) is SZK, the class of problems that admit a statistical zero-knowledge interactive proof system. However, SZK is not known yet to be entirely contained in BQP.

Quantum algorithms are not believed to solve NP-complete problems: not only there is an oracle A for which $\mathsf{NP}^A \not\subseteq \mathsf{BQP}^A$, but the same also holds with probability 1 for a uniformly sampled oracle [Bennett et al. 1997]. A limitation of the quantum computing model is that the state collapses after being measured. Aiming to understand how much this limitation is the reason why BQP is unlikely to contain NP, collapse-free models have been proposed [Aaronson et al. 2016]. Surprisingly, if such collapse-free measurements are performed in a *non-adaptive* model

(roughly speaking, the algorithm flow cannot be conditioned on a collapse-free measurement), the corresponding complexity class, called naCQP (*non-adaptive Collapse-Free Quantum Polynomial time*) or PDQP (*Product Dynamical Quantum Polynomial time*), is not believed to solve NP-complete problems either, but it is a superclass of BQP larger enough to include SZK [Aaronson et al. 2016]. We refer the reader to [Aaronson et al. 2016, Hepp et al. 2025] for the technical definition of naCQP.

A promise problem which is complete for SZK is the statistical difference distinguishability of probability distributions (SD), as defined below. In the definition, a boolean circuit that computes a function $f\colon \{0,1\}^m \to \{0,1\}^n$, being $n, m \in \mathbb{Z}_{>0}$, is said to *encode* the probability distribution of the outputs of the circuit, that is, the distribution over $\{0,1\}^n$ given by $\mathbb{P}_{y\in\{0,1\}^n}(y) = |f^{-1}(y)|/2^m$. Also, the *statistical difference* between two probability distributions X_1, X_2 over a universe $\mathcal{U}$ is denoted and defined as

$$\Delta(X_1, X_2) \coloneqq \max_{S\subseteq\mathcal{U}} |\mathbb{P}[X_1 \in S] - \mathbb{P}[X_2 \in S]| = \frac{1}{2}\sum_{x\in\mathcal{U}} |\mathbb{P}[X_1 = x] - \mathbb{P}[X_2 = x]| \,.$$

SD

Given: two positive integers n, m and two boolean circuits C_1, C_2 which compute two functions $f_1, f_2\colon \{0,1\}^m \to \{0,1\}^n$ and encode two probability distributions X_1, X_2, respectively;

decide: *positive instances:* $\Delta(X_1, X_2) \geq 2/3$;
negative instances: $\Delta(X_1, X_2) \leq 1/3$;

promised that one of the cases holds.

The quantum generalisation of SZK is called QSZK. The relation between QSZK and naCQP is unknown, with some believing that there is an oracle A such that $\mathsf{QSZK}^A \not\subseteq \mathsf{naCQP}^A$ [Aaronson 2018]. A promise problem which is complete for QSZK is the trace distance distinguishability of mixed states (QSD), as defined below. In the definition, a mixed quantum state $\rho = \{(|\psi_i\rangle, p_i)\}_i$ is treated as a density operator $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Therefore, the trace distance between two mixed states ρ_0 and ρ_1 is denoted and defined as

$$\|\rho_0 - \rho_1\|_{\mathrm{tr}} = \frac{1}{2}\,\mathrm{tr}\,\sqrt{(\rho_0 - \rho_1)^\dagger(\rho_0 - \rho_1)} = \frac{1}{2}\sum_i |\lambda_i| \,,$$

being $\{\lambda_i\}_i$ the eigenvalues of $\rho_0 - \rho_1$. When $\rho_0 = |\psi_0\rangle\langle\psi_0|$ and $\rho_1 = |\psi_1\rangle\langle\psi_1|$ correspond to two pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it can be checked that $\|\rho_0 - \rho_1\|_{\mathrm{tr}} = \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}$.

QSD

Given: two positive integers n, m and the description of two m-fanin n-fanout quantum circuits Q_0, Q_1, defining two mixed states ρ_0, ρ_1 of n qubits given by $\rho_0 = Q_0|0\rangle^{\otimes m}$ and $\rho_1 = Q_1|0\rangle^{\otimes m}$;

decide: *positive instances:* $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \geq 2/3$;
negative instances: $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq 1/3$;

promised that one of the cases holds.

2. Result

Lemma 1. *When $\rho_0 = |\psi_0\rangle\langle\psi_0|$ and $\rho_1 = |\psi_1\rangle\langle\psi_1|$ are the density operators corresponding to two pure states $|\psi_0\rangle$ and $|\psi_1\rangle$,*

$$\sqrt{\||\psi_0\rangle - |\psi_1\rangle\|_2} \leq \|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq \||\psi_0\rangle - |\psi_1\rangle\|_2^2 \,.$$

Proof. The upper bound follows from the fact that

$$\begin{aligned}\||\psi_0\rangle - |\psi_1\rangle\|_2 &= (\langle\psi_0| - \langle\psi_1|)(|\psi_0\rangle - |\psi_1\rangle) \\ &= 2 - (\langle\psi_0|\psi_1\rangle + \langle\psi_1|\psi_0\rangle) \geq 1 - |\langle\psi_0|\psi_1\rangle|^2 = \|\rho_0 - \rho_1\|_{\mathrm{tr}}^2 .\end{aligned}$$

The lower bound is trivial (recall that $\sqrt{\||\psi_0\rangle - |\psi_1\rangle\|_2}$ is the Euclidean distance). □

Clearly, the bounds in Lemma 1 are not tight, but sufficient for the following.

Theorem 2. $\mathrm{QSD} \in \mathsf{naCQP}$ *when restricted to pure states (i.e. when* $n = m$*).*

Proof. [1] We describe an naCQP algorithm that, given a QSD instance with $n = m$, accepts (rejects) with high probability if the instance is positive (negative). Let $\varepsilon = 2^{-\mathrm{poly}(n)}$. We assume without loss of generality that $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \geq 1 - \varepsilon$ if the instance is positive, and $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq \varepsilon$ if it is negative, which can be achieved in deterministic polynomial time using the Polarisation Lemma for QSD [Watrous 2002].

First, prepare the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle Q_0|0\rangle^{\otimes n} + \frac{1}{\sqrt{2}}|1\rangle Q_1|0\rangle^{\otimes n} .$$

In this state, for $b = 0, 1$, we refer to $|b\rangle$ as the first register, and to $|\phi_b\rangle \coloneqq (Q_b|0\rangle^{\otimes n})$ as the second register. Now, measuring (with collapse) the second register, it collapses to $|y\rangle$ for some $y \in \{0,1\}^n$ with probability $(\mathbb{P}[X_0 = y] + \mathbb{P}[X_1 = y])/2$, being X_b the random variable of the outcomes of measuring $|\phi_b\rangle$. Therefore, we can use the result by [Bennett et al. 1997], which showed how the trace distance between two pure states $|\phi_0\rangle, |\phi_1\rangle$ relates to the statistical difference between the corresponding probability distributions X_0, X_1 of the measurement outcomes:

$$\sqrt{\||\phi_0\rangle - |\phi_1\rangle\|_2} \leq \Delta(X_0, X_1) \leq 4\||\phi_0\rangle - |\phi_1\rangle\|_2 .$$

Perform then three collapse-free measurements in the first register, obtaining three bits b_1, b_2, b_3.. Accept if $b_1 = b_2 = b_3$, and reject otherwise. We show that the algorithm outputs the right answer with probability $\geq 2/3$. If $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \geq 1 - \varepsilon$, then $\Delta(X_0, X_1) \geq \sqrt[4]{1-\varepsilon} \geq 1 - \varepsilon$ and there must be some $S \subseteq \{0,1\}^n$ such that $\sum_{y \in S} \mathbb{P}[X_0 = y] \geq 1 - \varepsilon$ and $\sum_{y \in S} \mathbb{P}[X_1 = y] \leq \varepsilon$. Hence, one can check that the algorithm outputs the wrong answer (i.e. b_1, b_2, b_3 are *not* all equal) with probability

$$\mathbb{P}[err] \leq \frac{3}{2}\left(\sum_y \frac{(\mathbb{P}[X_0 = y])^2\mathbb{P}[X_1 = y]}{(\mathbb{P}[X_0 = y] + \mathbb{P}[X_1 = y])^2} + \sum_y \frac{\mathbb{P}[X_0 = y](\mathbb{P}[X_1 = y])^2}{(\mathbb{P}[X_0 = y] + \mathbb{P}[X_1 = y])^2}\right);$$

and since

$$\begin{aligned}&\sum_y \frac{(\mathbb{P}[X_0 = y])^2\mathbb{P}[X_1 = y]}{(\mathbb{P}[X_0 = y] + \mathbb{P}[X_1 = y])^2} \\ \leq &\sum_{y \in S} \frac{(\mathbb{P}[X_0 = y])^2\mathbb{P}[X_1 = y]}{(\mathbb{P}[X_0 = y])^2} + \sum_{y \in \overline{S}} \frac{(\mathbb{P}[X_0 = y])^2\mathbb{P}[X_1 = y]}{(\mathbb{P}[X_1 = y])^2} \leq 2\varepsilon ,\end{aligned}$$

[1] This proof if heavily inspired by the proof of [Aaronson et al. 2016] for $\mathrm{SD} \in \mathsf{naCQP}$, but with some adaptations.

we have

$$\mathbb{P}[err] \leq \frac{2}{3}(2\varepsilon + 2\varepsilon) = 6\varepsilon < \frac{1}{3}\,.$$

Now assume $\|\rho_0 - \rho_1\|_{\mathrm{tr}} \leq \varepsilon$, which implies $\||\psi_0\rangle - |\psi_1\rangle\|_2 \leq \sqrt{\varepsilon}$ and thus $\Delta(X_0, X_1) \leq 4\sqrt{\varepsilon}$. For $y \in \{0,1\}^n$, let $\delta_y \coloneqq \mathbb{P}[X_1 = y] - \mathbb{P}[X_0 = y]$. The algorithm outputs the wrong answer (i.e. $b_1 = b_2 = b_3$) with probability

$$\begin{aligned}
\frac{1}{2}\sum_y \frac{(\mathbb{P}[X_0 = y])^3 + (\mathbb{P}[X_1 = y])^3}{(\mathbb{P}[X_0 = y] + \mathbb{P}[X_1 = y])^2} &= \frac{1}{2}\sum_y \frac{(\mathbb{P}[X_0 = y])^3 + (\mathbb{P}[X_0 = y] + \delta_y)^3}{(2\mathbb{P}[X_0 = y] + \delta_y)^2} \\
&= \frac{1}{2}\sum_y \Big(\frac{\mathbb{P}[X_0 = y]}{2} + \delta_y \frac{(\mathbb{P}[X_0 = y])^2 + \frac{5}{2}\mathbb{P}[X_0 = y]\delta_y + \delta_y^2}{4(\mathbb{P}[X_0 = y])^2 + 4\mathbb{P}[X_0 = y]\delta_y + \delta_y^2}\Big) \\
&\leq \frac{1}{4} + \frac{1}{2}\sum_y |\delta_y| \leq \frac{1}{4} + 4\sqrt{\varepsilon}\,,
\end{aligned}$$

which is less than $1/3$ for a suitable value of ε. □

References

Aaronson, S. (2018). PDQP/qpoly = ALL. URL: https://scottaaronson.blog/?p=3816.

Aaronson, S., Bouland, A., Fitzsimons, J., and Lee, M. (2016). The space "just above" BQP. In *Proc. 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 271–280.

Arora, S. and Barak, B. (2009). *Computational complexity: a modern approach*. Cambridge University Press.

Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523.

Hepp, H., Silva, M. V. G., and Zatesko, L. M. (2025). Oracle separations for non-adaptive collapse-free quantum computing. In Press.

Kitaev, A. Y. (1995). Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*.

Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th annual symposium on foundations of computer science*, pages 124–134. IEEE.

Watrous, J. (2002). Limits on the power of quantum statistical zero-knowledge. In *Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468. IEEE.