10th Conference on the Theory of Quantum Computation, Communication and Cryptography

TQC'15, May 20–22, 2015, Brussels, Belgium

Edited by

Salman Beigi
Robert König

LIPIcs

LIPIcs – Vol. 44 – TQC 2015 www.dagstuhl.de/lipics

Editors

Salman Beigi
Institute for Research in
Fundamental Sciences
Tehran, Iran
`salman.beigi@gmail.com`

Robert König
Institute for Advanced Study
and Zentrum Mathematik
Technische Universität München
Garching, Germany
`robert.koenig@tum.de`

ACM Classification 1998
E.3 Data Encryption, E.4 Coding and Information Theory, F Theory of Computation

ISBN 978-3-939897-96-5

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at http://www.dagstuhl.de/dagpub/978-3-939897-96-5.

Publication date
November, 2015

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Digital Object Identifier: 10.4230/LIPIcs.TQC.2015.i

ISBN 978-3-939897-96-5 **ISSN 1868-8969** **http://www.dagstuhl.de/lipics**

LIPIcs – Leibniz International Proceedings in Informatics

LIPIcs is a series of high-quality conference proceedings across all fields in informatics. LIPIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

ISSN 1868-8969

http://www.dagstuhl.de/lipics

Contents

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The 10th Conference on the Theory of Quantum Computation, Communication and Cryptography was held at the Université libre de Bruxelles from the 20th to the 22nd of May 2015. Quantum computation, quantum communication, and quantum cryptography are subfields of quantum information processing, an interdisciplinary field of information science and quantum mechanics. The TQC conference series focuses on theoretical aspects of these subfields. The objective of the conference is to bring together researchers so that they can interact with each other and share problems and recent discoveries.

A list of the previous editions of TQC follows:

- TQC 2014, National University of Singapore, Singapore
- TQC 2013, University of Guelph, Canada
- TQC 2012, The University of Tokyo, Japan
- TQC 2011, Universidad Complutense de Madrid, Spain
- TQC 2010, University of Leeds, UK
- TQC 2009, Institute for Quantum Computing, University of Waterloo, Canada
- TQC 2008, University of Tokyo, Japan
- TQC 2007, Nara Institute of Science and Technology, Nara, Japan
- TQC 2006, NTT R&D Center, Atsugi, Kanagawa, Japan

The conference consisted of invited talks, contributed talks and a poster session. The invited talks were given by David DiVincenzo (RWTH Aachen & FZ Jülich), Sean Hallgren (Pennsylvania State University), Laura Mančinska (CQT Singapore) and Ronald de Wolf (CWI Amsterdam). The conference was possible thanks to the financial support of the Belgian Fund for Scientific Research (FNRS), Visit Brussels, Journal of Physics A, Cryptoworks21, the Engineering and Physical Research Council (EPSRC), as well as the Royal Society. We wish to thank the members of the Program Committee and all subreviewers for their precious help. Our warm thanks also go to the members of the Local Organizing Committee, for their considerable efforts in organizing the conference. We would like to thank Marc Herbstritt and Michael Wagner (Dagstuhl Publishing) for their technical help. Finally, we would like to thank the members of the Steering Committee for giving us the opportunity to work for TQC. And, of course, we thank all contributors and participants!

August 2015 Salman Beigi and Robert König

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Local Organizing Committee

Nicolas Cerf
Université libre de Bruxelles

Serge Massar
Université libre de Bruxelles

Stefano Pironio
Université libre de Bruxelles (chair)

Jérémie Roland
Université libre de Bruxelles (chair)

Philippe Spindel
Université de Mons

Frank Verstraete
Ghent University

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Program Committee

Salman Beigi, IPM (chair)
Andrew Childs, University of Maryland
Matthias Christandl, Copenhagen
Toby Cubitt, Cambridge
Andrew Doherty, University of Sydney
Frédéric Dupuis, Aarhus
Sevag Gharibian, UC Berkeley and Virginia Commonwealth
Saikat Guha, BBN Technologies
Michał Horodecki, University of Gdansk
Peter Høyer, Calgary
Iordanis Kerenidis, Paris Diderot
Robert König, Technische Universität München (chair)
Troy Lee, NTU & CQT Singapore
Tobias Osborne, Hannover
Carlos Palazuelos, UCM Madrid
David Pérez-Garcia, UCM Madrid
Ben Reichardt, University of Southern California
Kristan Temme, Caltech
Barbara Terhal, RWTH Aachen
Marco Tomamichel, University of Sydney
Christian Schaffner, University of Amsterdam
Tamás Vértesi, MTA Atomki
Thomas Vidick, Caltech
Pawel Wocjan, University of Central Florida

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Steering Committee

Wim van Dam
University of California, Santa Barbara, USA

Yasuhito Kawano
NTT, Japan

Michele Mosca
IQC and University of Waterloo, Canada

Martin Roetteler
Microsoft Research, USA

Simone Severini
University College London, UK

Vlatko Vedral
University of Oxford, UK &
National University of Singapore, Singapore

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Oracles with Costs

Shelby Kimmel^{1,2}, Cedric Yen-Yu Lin^{2}, and Han-Hsuan Lin^{2}

1 **Joint Center for Quantum Information and Computer Science, University of Maryland, US**

2 **Center for Theoretical Physics, Massachusetts Institute of Technology, US**

Abstract

While powerful tools have been developed to analyze quantum query complexity, there are still many natural problems that do not fit neatly into the black box model of oracles. We create a new model that allows multiple oracles with differing costs. This model captures more of the difficulty of certain natural problems. We test this model on a simple problem, Search with Two Oracles, for which we create a quantum algorithm that we prove is asymptotically optimal. We further give some evidence, using a geometric picture of Grover's algorithm, that our algorithm is exactly optimal.

1998 ACM Subject Classification F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Quantum Algorithms, Query Complexity, Amplitude Amplification

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.1

1 Introduction

The standard oracle model is a powerful paradigm for understanding quantum computers. Tools such as the adversary semidefinite program [12, 13], learning graphs [5, 6], and the polynomial method [4] allow us to accurately characterize the quantum query complexity [1, 7] of many problems of interest.

However, the oracle model does not capture the full power or challenges of quantum computing. For example, problems such as k-SAT do not fit easily into the oracle model. Additionally, while the query complexity of the hidden subgroup problem is known to be polynomial in the size of the problem [11], for some non-abelian groups there is no efficient algorithm.

In this paper, we describe a variation of the oracle model. We have access to two oracles, rather than a single oracle[1], but one oracle is more expensive to use. In the standard oracle model, the figure of merit is the query complexity, which is the minimum number of queries needed to an oracle to evaluate a function. In our model, the figure of merit is the *cost complexity*, which is the minimum cost needed to evaluate a function using multiple oracles with different costs.

To motivate this model, we consider the following fact: in some search problems we want to find an element in a set that satisfies a property that is expensive to test. However, often another less expensive test is available that can narrow down the search range but is not conclusive. We give three examples of problems where such less expensive, less conclusive tests are natural. In each example, Test 1 is more expensive to run but is conclusive, while Test 2 is cheaper to run but allows some non-solutions to pass.

[1] The model can easily be extended to more than two oracles, but for simplicity, we limit ourselves to two.

- In the problem of k-SAT on n bits, we would like to find an assignment $x \in \{0,1\}^n$ such that all clauses are satisfied. Consider an algorithm for k-SAT that runs two types of tests on a possible assignment x:
  1. Check whether all clauses are satisfied.
  2. Check whether some subset of the clauses are satisfied.
- Given a graph A and a set of graphs $\{B_1, \cdots, B_p\}$, we would like to find a graph B_i isomorphic to A. Consider an algorithm that runs two types of tests on a graph B_i:
  1. Check whether B_i is isomorphic to A (say by brute force search).
  2. Check whether the adjacency matrices of B_i and A have the same spectrum.
- In the decision variant of the traveling salesman problem, given a positively weighted N-graph G and a positive number b, we would like to find a tour of the vertices of G that uses cost no more than b. Given a partial tour of length $N/2$, we can run two types of tests:
  1. Check whether the partial tour can be completed to an N-vertex tour that has cost at most b, by using brute force search.
  2. Check whether the sum of the weights of the $N/2$ edges traversed in the partial tour is bigger than b.

In all three examples, the two tests can be implemented as unitaries $\mathcal{O}_1, \mathcal{O}_2$ that act as $\mathcal{O}_i|x\rangle|y\rangle = |x\rangle|y \oplus f_i(x)\rangle$. Here $f_i(x) = 1$ if assignment x passes Test i and $f_i(x) = 0$ otherwise. These two unitaries will play the role of oracles with different costs.

None of the problems listed above are typically thought of as oracle problems, because in each problem, there is more information than can easily be incorporated into a single oracle. However, with multiple oracles, the information can be distributed among different oracles. Using different costs for different oracles allows us to include information about the time required to access information. We see that cost complexity can capture certain aspects of a problem that can not be easily accounted for in the standard oracle model; we hope this model will provide new insight into problems previously thought beyond the tools of query algorithms. We note that we do not expect these techniques to allow us to solve NP-complete problems in polynomial time. Rather, our goal is to potentially improve upon existing exponential time algorithms, and create connections between standard oracle problems and problems that seem far from typical oracle problems.

Problems such as those described above can easily be recast into an oracle problem, which we call Search with Two Oracles (STO). In this work, we focus on the problem of STO. We tightly characterize the quantum cost complexity of this problem, and give several techniques for putting lower bounds on quantum cost complexity. We also show that the cost complexity of STO is the same whether or not the oracles can be accessed using a control operation; that is, accessing the oracles in superposition gives no added power.

We also attempt to exactly bound (rather than asymptotically bound) the cost complexity of STO. Usually, one is not particularly interested in proving exact optimality, but we have several reasons for wanting to explore this problem. Few quantum algorithms are known to be exactly optimal; Grover's algorithm and parity are two examples [10, 4]. STO is a very simple extension of a standard search problem, so it seems like a good candidate problem for obtaining another exact lower bound. Proving that our algorithm is exactly optimal would provide evidence that amplitude amplification is exactly optimal in the case of no additional structure (i.e. when we treat the base algorithm as a black box). Additionally, while we can obtain asymptotically tight bounds for the problem of STO, for a simple extension of STO to $\log N$ oracles (where N is the size of the search space), these techniques fail. However, if we could obtain tighter bounds for STO, we should be able to get a better characterization of the cost complexity for these more complex problems.

Finally, we compare the quantum cost complexity of STO to the classical cost complexity. We show a polynomial reduction in cost for the quantum version. Moreover, we show that the optimal quantum and classical algorithms behave qualitatively differently, highlighting the power of quantum algorithms.

In Section 2, we describe cost complexity and define STO. In Section 3, we describe optimal quantum algorithms for STO, and in Section 4, we put lower bounds on the cost complexity of STO. Finally, we look at the classical cost complexity of STO in Section 5.

2 Cost Complexity, STO, and Relation to Previous Work

Cost complexity is very closely related to query complexity. For background on query complexity, see [1, 7].

We first define cost complexity. In the following, we use the notation $[N] \equiv \{1, \ldots, N\}$. Given the input $(f_1, f_2) \in D$, which is a pair of functions $f_1, f_2 : [N] \to \{0, 1\}$, we want to calculate F where $F : D \to \{0, 1\}$. Let f_1 be associated with cost c_1 and f_2 be associated with cost c_2. Depending on the type of algorithm (e.g. classical, quantum), these two functions are accessed in different ways.

In the classical setting, consider a randomized classical algorithm $\mathcal{A}_c$ for F that makes q_1 queries to f_1, and q_2 queries to f_2. Then the cost of this algorithm is

$$\text{Cost}(\mathcal{A}_c) = q_1 c_1 + q_2 c_2. \tag{1}$$

Let $\mathcal{A}_{c,\epsilon}$ be the set of randomized classical algorithms that solve F with success probability at least $1-\epsilon$ on all inputs in D. Then the *classical randomized cost complexity (RCC)* of F is

$$RCC_\epsilon(F) = \min_{\mathcal{A}_c \in \mathcal{A}_{c,\epsilon}} \text{Cost}(\mathcal{A}_c). \tag{2}$$

In the quantum setting, let $\mathcal{O}_1$ and $\mathcal{O}_2$ be unitaries acting on the Hilbert space $\mathbb{C}^N$ with standard basis states $|i\rangle$ for $i \in [N]$ as $\mathcal{O}_j|i\rangle = (-1)^{f_j(i)}|i\rangle$ for $j \in 1, 2$. Consider a quantum algorithm $\mathcal{A}_q$ that at each time step, can apply $\mathcal{O}_1$ or $\mathcal{O}_2$ or some other unitary that is independent of f_1 and f_2, and which makes q_1 queries to $\mathcal{O}_1$ and q_2 queries to $\mathcal{O}_2$. Then the cost of the algorithm $\mathcal{A}_q$ is

$$\text{Cost}(\mathcal{A}_q) = q_1 c_1 + q_2 c_2. \tag{3}$$

Let $\mathcal{A}_{q,\epsilon}$ be the set of quantum algorithms that solve F with success probability at least $1-\epsilon$ on all inputs in D. Then the *quantum cost complexity (QCC)* of F is

$$QCC_\epsilon(F) = \min_{\mathcal{A}_q \in \mathcal{A}_{q,\epsilon}} \text{Cost}(\mathcal{A}_q). \tag{4}$$

Finally, we consider quantum algorithms that can access oracles in superposition. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be as above, and let $\mathcal{O}_0 = \mathbb{I}$, the $N \times N$ identity matrix. We now consider a quantum algorithm that has access to a controlled operation $C\mathcal{O}$ that acts on the the Hilbert space $\mathbb{C}^3 \otimes \mathbb{C}^N \otimes \mathbb{C}^V$ ($\mathbb{C}^V$ is a workspace register) with standard basis states $|b\rangle|i\rangle|v\rangle$ for $i \in [N]$, $v \in [V]$, and $b \in \{0, 1, 2\}$ as $C\mathcal{O}|b, i\rangle = |b\rangle\mathcal{O}_b|i\rangle|v\rangle$. Suppose the encoded functions are f_1 and f_2. Then if an algorithm $\mathcal{A}_{qs}$ applies $C\mathcal{O}$ a total of T times over the course of the algorithm to states

$$|\eta^t_{f_1,f_2}\rangle = \sum_{b=0}^{2}\sum_{i=1}^{N}\sum_{v=1}^{V} \alpha^t_{f_1,f_2}(b, i, v)|b, i, v\rangle \tag{5}$$

for $t \in [T]$, the cost of the algorithm is

$$\text{Cost}(\mathcal{A}_{qs}) = \max_{f_1,f_2} \sum_{t=1}^{T} \kappa(\eta^t_{f_1,f_2}) \text{ where}$$

$$\kappa(\eta^t_{f_1,f_2}) = \begin{cases} c_1 \text{ if } \sum_{i,v} |\alpha^t_{f_1,f_2}(1,i,v)|^2 \neq 0, \\ c_2 \text{ if } \sum_{i,v} |\alpha^t_{f_1,f_2}(1,i,v)|^2 = 0 \text{ and } \sum_{i,v} |\alpha^t_{f_1,f_2}(2,i,v)|^2 \neq 0, \\ 0 \text{ if } \sum_{i,v} |\alpha^t_{f_1,f_2}(1,i,v)|^2 = 0 \text{ and } \sum_{i,v} |\alpha^t_{f_1,f_2}(2,i,v)|^2 = 0. \end{cases} \tag{6}$$

Let $\mathcal{A}_{qs,\epsilon}$ be the set of quantum algorithms using $\mathcal{CO}$ that solve F with success probability at least $1-\epsilon$ on all inputs in D. Then the *controlled quantum cost complexity (ConQCC)* of F is

$$ConQCC_\epsilon(F) = \min_{\mathcal{A}_{qs} \in \mathcal{A}_{qs,\epsilon}} \text{Cost}(\mathcal{A}_{qs}). \tag{7}$$

The controlled quantum cost complexity is closely related to the time required in the model of variable times introduced by Ambainis in [2].

Note that

$$ConQCC_\epsilon(F) \leq QCC_\epsilon(F) \leq RCC_\epsilon(F). \tag{8}$$

For any of the cost complexities described above, if we do not include a subscript ϵ, then the cost is assumed to apply for the case $\epsilon = 1/3$.

Now that we have defined cost complexity, we introduce the problem of STO as a testbed for tools and ideas that can hopefully be applied to more complex problems. More formally, we give the definition of STO:

▶ **Definition 1** (Search with Two Oracles (STO)). Let N and M be known positive integers and let $S \subseteq [N]$ be an unknown set. There might or might not exist a special item i_*. If i_* exists, then one is promised that $i_* \in S$ and $|S| = M$. If i_* doesn't exist, the size of S is arbitrary. Let f_* and f_S be two functions with domain $[N]$ and range $\{0,1\}$ such that

$$f_*(i) = \begin{cases} 1 & \text{if } i = i_* \\ 0 & \text{if } i \neq i_* \text{ or } i_* \text{ doesn't exist.} \end{cases} \qquad f_S(i) = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{if } i \notin S. \end{cases} \tag{9}$$

Then $\text{STO}(f_*, f_S) = 1$ if i_* exists, and 0 otherwise. c_* is the cost associated with f_* and c_S is the cost associated with f_S, with $c_* \geq c_S$.

c_S and c_* are assumed to depend on N and M, but our results hold for any form of that dependence, so we leave off any explicit relationship.

Cost complexity, and STO in particular, are related to several existing oracle problems. In the problem of STO, the function f_S can be thought of as providing extra information or advice about the function f_*. There have been several studies in which access to a single oracle is supplemented with some extra information that can come in the form of another oracle or classical information, e.g. [14, 15]. Previous works [3, 14] have considered multiple oracles, but not with costs. Furthermore, the additional advice oracles considered in these works tend to be somewhat unnatural, and are tailored to the specific problems considered. As mentioned, $ConQCC$ is related to the model of variable costs studied by Ambainis, in which he considered a single oracle that has different costs for querying different items [2]. We also note that Cerf et al. [9] consider similar quantum algorithms in the context of constraint satisfaction problems, but they do not approach the problem from an oracular perspective.

3 Quantum Algorithms for STO

We now describe quantum algorithms for solving STO[2]. These algorithms use the oracles $\mathcal{O}_*$ and $\mathcal{O}_S$ directly, rather than the controlled version (i.e. $C\mathcal{O}$) of these oracles. All of our algorithms can be viewed as examples of amplitude amplification. Recall

▶ **Theorem 2** (Amplitude Amplification [8]). *Let $T \subset [N]$, $\alpha \in [0,1]$, and let $\mathcal{O}^T$ be an quantum oracle that marks the elements of T. We define*

$$|T\rangle = \frac{1}{\sqrt{|T|}}\sum_{i\in T}|i\rangle. \tag{10}$$

Given an algorithm $\mathcal{A}$ that acts on a state $|\psi_0\rangle$ and produces a state $|\psi_\mathcal{A}\rangle$ such that $|\langle T|\psi_\mathcal{A}\rangle| = p$, one can create a new algorithm $\mathcal{B}$ that applies $\mathcal{O}^T$, $\mathcal{A}$, and $\mathcal{A}^{-1}$ each

$$\tau = \left\lceil \frac{\arcsin\sqrt{1-\alpha} - \arcsin p}{2\arcsin p}\right\rceil \tag{11}$$

times, and which acts on the initial state $|\psi_0\rangle$ and produces a state $|\psi_\mathcal{B}\rangle$ such that

$$|\psi_\mathcal{B}\rangle = \sqrt{1-\alpha}|T\rangle + \sqrt{\alpha}|T^\perp\rangle, \tag{12}$$

where $\langle T|T^\perp\rangle = 0$ and $|T^\perp\rangle \in \mathit{Span}\,(|T\rangle, |\psi_A\rangle)$.

This gives us the following Corollary:

▶ **Corollary 3.** *Let $\mathcal{A}$ and τ be as in Theorem 2, and assume $\mathcal{O}^T$ has cost c_T while $\mathcal{A}$ and $\mathcal{A}^{-1}$ have cost $c_\mathcal{A}$. Then there exists a algorithm $\mathcal{B}$ that applies $\mathcal{O}^T$, $\mathcal{A}$ and $\mathcal{A}^{-1}$ not in superposition, and produces the state $|T\rangle$ with probability $1-\epsilon$ such that*

$$\text{Cost}(\mathcal{B}) = \tau\left(c_T + 2c_\mathcal{A}\right). \tag{13}$$

In the following, we describe three algorithms for STO. We consider the limit that $M, N/M \to \infty$ to simplify our analysis, but this limit still captures the essential behavior of the algorithms. We use the following notation:

$$\begin{aligned}|N\rangle &= \frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i\rangle,\\ |S\rangle &= \frac{1}{\sqrt{M}}\sum_{i\in S}|i\rangle.\end{aligned} \tag{14}$$

We have a slight abuse of notation, since $|N\rangle$ could refer either to the equal superposition state, or the N^{th} standard basis state. However, whenever we write $|N\rangle$, we will always mean the equal superposition state.

The first algorithm we consider ignores $\mathcal{O}_S$ and performs a Grover search for i_* using $\mathcal{O}_*$:

[2] For the purpose of describing these algorithms, we assume that i_* exists. A single application of O_* at the end of the algorithm can be used to check (with appropriate probability) whether or not i_* exists, at a cost of c_*.

▶ **Algorithm 1** (Grover's Search). *Prepare the state $|N\rangle$ at cost 0. Set $\mathcal{A}$ equal to the identity. Then by Corollary 3 there exists an algorithm $\mathcal{B}$ that produces the state $|i_*\rangle$ with probability* $1-\epsilon$ *with cost*

$$c_* \left\lceil \frac{\arcsin\sqrt{1-\epsilon} - \arcsin\frac{1}{\sqrt{N}}}{2\arcsin\frac{1}{\sqrt{N}}} \right\rceil. \tag{15}$$

In the limit of $N \to \infty$, the cost becomes

$$c_* \arcsin\sqrt{1-\epsilon}\sqrt{N}. \tag{16}$$

However, if $\mathcal{O}_S$ comes to us cheaply, we would like to take advantage of it: The following algorithm first rotates $|N\rangle$ to $|S\rangle$ (using $\mathcal{O}_S$), and then rotates $|S\rangle$ to $|i_*\rangle$ (using both $\mathcal{O}_S$ and $\mathcal{O}_*$).

▶ **Algorithm 2.** *Prepare the state $|N\rangle$ at cost 0. Set $\mathcal{A}$ equal to the identity. Since $|\langle N|S\rangle| = \sqrt{M/N}$, by Corollary 3 there exists an algorithm $\mathcal{B}$ that with probability* 1 *produces the state $|S\rangle$ at cost*

$$c_S \left\lceil \frac{\left(\frac{\pi}{2} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil. \tag{17}$$

Now $|\langle i_*|S\rangle| = \sqrt{1/M}$, so using Corollary 3 again, there exists an algorithm $\mathcal{C}$ that with probability $1-\epsilon$ *produces the state $|i_*\rangle$ at cost*

$$\left\lceil \frac{\arcsin\sqrt{1-\epsilon} - \arcsin\frac{1}{\sqrt{M}}}{2\arcsin\frac{1}{\sqrt{M}}} \right\rceil \left(c_* + 2c_S \left\lceil \frac{\left(\frac{\pi}{2} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil \right). \tag{18}$$

Dropping terms of size at most $O(M^{-1/2})$ or $O\left((M/N)^{1/2}\right)$ of the zeroth order terms, the cost becomes

$$\frac{\arcsin\sqrt{1-\epsilon}}{4}\left(2c_*\sqrt{M} + \pi c_S\sqrt{N}\right). \tag{19}$$

Combining Algorithms 1 and 2, we have that

$$\begin{aligned} QCC(STO) &= O\left(\min\left\{c_*\sqrt{N}, c_*\sqrt{M} + c_S\sqrt{N}\right\}\right) \\ &= O\left(\max\left\{c_*\sqrt{M}, c_S\sqrt{N}\right\}\right). \end{aligned} \tag{20}$$

In Section 4, we will show that this cost (Eq. (20)) is asymptotically optimal. This means that Algorithm 2 is always asymptotically optimal, although Algorithm 1 has lower cost when $c_* \approx c_S$. However, it turns out that there is an algorithm that has lower cost than either Algorithm 1 or 2. In Section 4, we give evidence that this final algorithm, which we call the Hybrid Algorithm, is not just asymptotically optimal, but exactly optimal.

The two algorithms we have so far presented can be summarized as follows: Algorithm 1 directly performs Grover rotations to rotate $|N\rangle$ to $|i_*\rangle$, while Algorithm 2 first rotates $|N\rangle$ to $|S\rangle$, then rotates $|S\rangle$ to $|i_*\rangle$. The final algorithm we consider, the Hybrid Algorithm, first rotates $|N\rangle$ to some superposition of $|N\rangle$ and $|S\rangle$, and then rotates to $|i_*\rangle$.

▶ **Algorithm 3** (Hybrid Algorithm). *Prepare the state $|N\rangle$ at cost 0. Set $\mathcal{A}$ equal to the identity. Since $|\langle N|S\rangle| = \sqrt{M/N}$, by Theorem 2 and Corollary 3 there exists an algorithm $\mathcal{B}$ that produces a state $|\psi_{\mathcal{B}}\rangle$ at cost*

$$c_S \left\lceil \frac{\left(\arcsin\sqrt{1-\alpha} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil . \tag{21}$$

where

$$|\psi_{\mathcal{B}}\rangle = \sqrt{1-\alpha}|S\rangle + \sqrt{\alpha}|S^{\perp}\rangle. \tag{22}$$

By Theorem 2, $|S^{\perp}\rangle$ is a linear combination of $|S\rangle$ and $|N\rangle$ but is orthogonal to $|S\rangle$. Therefore, $|S^{\perp}\rangle$ is a superposition of all elements not in S, and so $\langle i_*|S^{\perp}\rangle = 0$. Thus

$$\frac{\sqrt{1-\alpha}}{\sqrt{M}} = \langle \psi_{\mathcal{B}}|i_*\rangle. \tag{23}$$

Applying Corollary 3 again, we can create an algorithm $\mathcal{C}$ that has cost

$$\left\lceil \frac{\arcsin\sqrt{1-\epsilon} - \arcsin\frac{\sqrt{1-\alpha}}{\sqrt{M}}}{2\arcsin\frac{\sqrt{1-\alpha}}{\sqrt{M}}} \right\rceil \left(c_* + 2c_S \left\lceil \frac{\left(\arcsin\sqrt{1-\alpha} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil \right) \tag{24}$$

and produces the state $|i_*\rangle$ with probability $1-\epsilon$. In Appendix A, we show there is a choice of α such that, dropping terms of size at most $O(M^{-1/2})$ or $O((M/N)^{1/4})$ that of the zeroth order terms, the cost is

$$Cost(Hybrid) = \frac{c_S\sqrt{N}\arcsin\sqrt{1-\epsilon}}{2}\sec\left(\phi_{opt} + \sqrt{\frac{M}{N}}\right), \tag{25}$$

where ϕ_{opt} is given by

$$\phi_{opt} = \max\begin{cases} 0 \\ \phi : \tan\left(\phi + \sqrt{\frac{M}{N}}\right) = \phi + \frac{c_*}{c_S}\sqrt{\frac{M}{N}}. \end{cases} \tag{26}$$

When c_S is close to c_*, this algorithm approximates Algorithm 1. When c_S is very small compared to c_*, it approximates Algorithm 2. Otherwise, it, in effect, interpolates between the two algorithms.

4 Lower Bound on Quantum Cost Complexity of STO

Several techniques give asymptotically tight lower bounds on the quantum cost complexity of STO. We will briefly sketch two approaches for bounding the quantum cost complexity (QCC), and then discuss a bound on controlled quantum cost complexity ($ConQCC$) in detail. The fact that so many approaches give good lower bounds is encouraging; this means many techniques from (or variations on) the standard query complexity toolbox can be applied.

Our lower bound on $ConQCC$(STO) is asymptotically tight with the algorithms of Section 3, i.e. Eq. (20), even though those algorithms do not use controlled oracles. Because algorithms that use controlled versions of the oracles are more powerful than oracles that can not access controlled versions (see Eq. (8)), this result proves that not only are our algorithms for STO asymptotically optimal, but having access to a controlled version of the oracles for STO does not give an advantage.

When discussing lower bounds on the cost of STO, we will often refer to the SEARCH problem. We call SEARCH the problem in which one is given a function $f_* : [N] \to \{0,1\}$ such that there is exactly zero or one element i_* such that $f_*(i_*) = 1$, and one would like to determine if there is such an element i_*; in other words, SEARCH is computing $\mathrm{OR}(f_*)$ with a promise on f_*.

Here are brief descriptions of two methods for lower bounding QCC. We describe them in the context of STO, but they could be applied more generally.

Oracle Simulation: Suppose one only has an oracle $\mathcal{O}_*$. Then one could use this to simulate an oracle $\mathcal{O}_S$ by applying $\mathcal{O}_*$, and then subsequently randomly choosing $M-1$ items to mark. If $M \ll N$, with high probability, the chosen $M-1$ items will not include $\mathcal{O}_*$, and this simulated oracle will act identically to a true $\mathcal{O}_S$. Now any algorithm for STO that uses this simulated oracle will actually only use $\mathcal{O}_*$ to find the marked item i_*, and so the problem reduces to SEARCH. Well-known quantum lower bounds on SEARCH [7] then give a lower bound on the total number of queries to either $\mathcal{O}_*$ or the simulated $\mathcal{O}_S$, which in turn can be used to put a lower bound on the cost. For more details on oracle simulation, see Section 5, in which we use oracle simulation to bound the classical cost complexity of STO.

Adversary Method: One can create an adversary matrix whose rows and columns are indexed by pairs of oracles (f_*, f_S). This matrix can be used to create a progress function, and then one can bound the progress that either oracle $\mathcal{O}_*$ or $\mathcal{O}_S$ can make. This gives lower bounds on the queries needed to $\mathcal{O}_*$ and $\mathcal{O}_S$ to evaluate STO, which in turn can be used to lower bound the cost of STO. In Appendix C, we detail how to create this bound for STO.

4.1 Lower Bound on Controlled Quantum Cost Complexity of STO

In this section, in order to lower bound $ConQCC(\mathrm{STO})$, we consider a new problem in the standard query model, which we call Expanded Search with Two Oracles (ESTO). We show that if we had an algorithm $\mathcal{A}$ which could use the control oracle CO to solve STO with cost $c_{\mathcal{A}}$, then we could create a new algorithm $\mathcal{A}'$ to solve ESTO using $O(c_{\mathcal{A}})$ queries. We then use the adversary method to lower bound the query complexity of ESTO, which in turn puts a lower bound on $ConQCC(\mathrm{STO})$. This strategy is inspired by Ambianis's approach for lower bounding the variable times search problem [2].

We first describe the problem ESTO. We suggest referencing Figure 1 during the description of the problem for a graphical interpretation. Let N, M, c_* and c_S be as in STO. Without loss of generality, we can assume $c_*, c_S \gg 1$. If they are not, we can multiply both costs by some large factor K. Then the final cost is exactly a factor of K larger than it would have been with the original costs. (If $c_S = 0$, this approach does not work, but in that case, STO reduces to SEARCH). We define

$$m_* = \max\left\{i : \left\lceil \frac{\pi}{4}\sqrt{i}\right\rceil + 1 \leq c_*, i \in \mathbb{Z}\right\},$$
$$m_S = \max\left\{i : \left\lceil \frac{\pi}{4}\sqrt{i}\right\rceil + 1 \leq c_S, i \in \mathbb{Z}\right\},$$

ESTO queries an unknown function $f : [N(m_S + m_*)] \to \{0,1\}$. We consider $\mathcal{D}_1 = \{1, \ldots, Nm_*\}$ to be the “first part” of the domain of f, and $\mathcal{D}_2 = \{Nm_*{+}1, \ldots, N(m_*{+}m_S)\}$

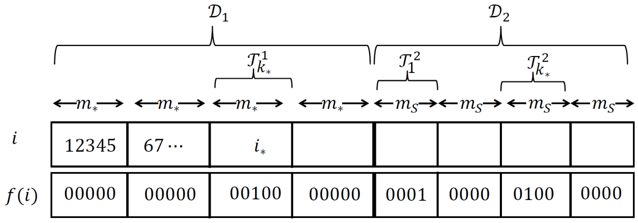


Figure 1 A diagram of a function f for which $\mathrm{ESTO}(f) = 1$. The domain of f is divided into two parts $\mathcal{D}_1$ and $\mathcal{D}_2$. Each of these sets are further divided into N sets of size m_* and m_S respectively. These sets are labeled $\mathcal{T}^1_k$ for sets in $\mathcal{D}_1$, and $\mathcal{T}^2_k$ for sets in $\mathcal{D}_2$. We see there is exactly one value of $i \in \mathcal{D}_1$ with value 1, and it is in the set $\mathcal{T}^1_{k_*}$. In the case shown in this figure, $S = \{1, k_*\}$, so both $\mathcal{T}^2_{k_*}$ and $\mathcal{T}^2_1$ contain exactly one marked item.

to be the "second part" of the domain. We further divide $\mathcal{D}_1$ ($\mathcal{D}_2$) into N blocks of m_* (m_S) elements respectively, where the elements $\mathcal{T}^1_k = \{(k-1)m_* + 1, \ldots, km_*\}$ constitute the k^{th} block of $\mathcal{D}_1$, and the elements $\mathcal{T}^2_k = \{Nm_* + (k-1)m_S + 1, \ldots, Nm_* + km_S\}$ constitute the k^{th} block of $\mathcal{D}_2$.

We are promised that there is either exactly zero or one value $i_* \in \mathcal{D}_1$ such that $f(i_*) = 1$. If there is such an i_*, we label the block it is in by k_*, so $i_* \in T^1_{k_*}$. Furthermore, if i_* exists, there is a set $S \in [N]$ such that $|S| = M$, $k_* \in S$, and for each $k \in S$ there is exactly one value of $i \in \mathcal{T}^2_k$ such that $f(i) = 1$. Given such a function f, $\mathrm{ESTO}(f) = 1$ if there is an item $i_* \in \mathcal{D}_1$ such that $f(i_*) = 1$, and 0 otherwise.

Given an algorithm $\mathcal{A}$ for STO that uses the control oracle $C\mathcal{O}$ and has cost $c_{\mathcal{A}}$, we can create an algorithm $\mathcal{A}'$ to solve ESTO that uses $2c_{\mathcal{A}}$ queries. Let $y^b_j = 1$ for $b \in \{1, 2\}$ if there is an element $i \in \mathcal{T}^b_j$ such that $f(i) = 1$, and 0 otherwise. Then by Claim 2 in [2], there is an algorithm $\mathcal{B}$ that takes $|b, j\rangle|0\rangle|0\rangle \to |b, j\rangle|y^b_j\rangle|\psi^b_j\rangle$ for some state $|\psi^b_j\rangle$ and uses c_* queries if $b = 1$ and c_S queries if $b = 2$. At the cost of doubling the number of queries, we can uncompute the final register. Thus there is an algorithm $\mathcal{B}'$ that takes $|b, j\rangle|0\rangle \to |b, j\rangle|y^b_j\rangle$ and uses $2c_*$ queries if $b = 1$ and $2c_S$ queries if $b = 2$. We also allow for $b = 0$, in which case the algorithm $\mathcal{B}'$ applies the identity.

Then we can solve ESTO using our algorithm $\mathcal{A}$ for STO. In STO we are searching for a specific element $i^* \in [N]$ with certain properties, in ESTO, the search is for a specific block $k^* \in [N]$ with analogous properties. We replace an application of the controlled oracle C-$\mathcal{O}$ to the state $|b, i\rangle$ with $b \in \{0, 1, 2\}$ and $i \in [N]$ with an application of the algorithm $\mathcal{B}'$ to the state $|b, i\rangle$, (which corresponds to searching the block $\mathcal{T}^b_i$, for $b \in \{1, 2\}$ and $i \in [N]$, or doing nothing if $b = 0$). The number of queries required by $\mathcal{B}'$ will be twice cost of the equivalent query made by $\mathcal{A}$. Due to the specific structure of f, this algorithm will solve ESTO with a number of queries equal to $2c_{\mathcal{A}}$.

Now all that is left is to put a lower bound on the number of queries needed to solve ESTO. We use Ambainis's adversary bound:

▶ **Theorem 4** (Basic Adversary Bound [1]). *Let $F(f(1), \ldots, f(N))$ be a function of N $\{0,1\}$-valued variables $f(i)$, and let X, Y be two sets of inputs such that $F(f) \neq F(g)$ if $f \in X$ and $g \in Y$. Let $R \subset X \times Y$ be such that*

- *For every $f \in X$, there exist at least μ different $g \in Y$ such that $(f, g) \in R$.*
- *For every $g \in Y$, there exist at least μ' different $f \in X$ such that $(f, g) \in R$.*
- *For every $f \in X$ and $i \in [N]$, there are at most l different $g \in Y$ such that $(f, g) \in R$ and $f(i) \neq g(i)$.*

- *For every $g \in Y$ and $i \in [N]$, there exist at least l' different $f \in X$ such that $(f, g) \in R$ and $f(i) \neq g(i)$.*

Then, any quantum algorithm computing F with error at most ϵ on all valid inputs uses at least

$$\frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2}\sqrt{\frac{\mu\mu'}{ll'}} \tag{27}$$

queries.

For the sets X and Y, we only consider functions f where in each block $\mathcal{T}_j^b$, there is at most 1 marked item. We denote by $f_{k_*,i_*,S,S'}$ a function where $i_* \in \mathcal{D}_1$ is the marked item, k_* is the block where the i_* sits (or $i_* = k_* = 0$ if there is no marked item in $\mathcal{D}_1$), S is the set of blocks in $\mathcal{D}_2$ that have exactly one marked item in each block, and S' is a list of the $|S|$ items that are marked in the second part of the domain.

Let X be the set of all functions $f_{k_*,i_*,S,S'}$ with $k_* \neq 0$, $i_* \neq 0$, $|S| = M$, and $k_* \in S$. From our definition of ESTO, these are functions for which the algorithm should output 1. Let Y be the set of functions $f_{0,0,T,T'}$ with $|T| = M-1$. Then R is defined by $(f_{k_*,i_*,S,S'}, f_{0,0,T,T'}) \in R$ if and only if $T \subset S$, $T' \subset S'$, and $k_* \notin T$. With this definition of R, we have $\mu = 1$ while $\mu' = (N-M+1)m_*m_S$. Likewise $l = 1$ while $l' = \max\{m_S, m_*\} = m_*$ since $c_* \geq c_S$. Theorem 4 then gives that the number of queries required to solve ESTO, is at least

$$\frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2}\sqrt{(N-M+1)m_S}. \tag{28}$$

Eq. (28) does not tell the full story; we can repeat this procedure with the set X the same as before, but now the set Y includes all functions $f_{0,0,S,S'}$ such that $|S| = M$. Then we choose $(f_{k_*,i_*,S,S'}, f_{0,0,T,T'}) \in R$ if and only if $T = S$ and $T' = S'$. With this definition of R, we have $\mu = 1$, while $\mu' = Mm_*$. Likewise $l = 1$ while $l' = 1$. Again using Theorem 4, we have that the number of queries required to solve ESTO is at least

$$\frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2}\sqrt{Mm_*}. \tag{29}$$

Since $c_*, c_S \gg 1$, we have $m_* = \Omega((c_*)^2)$ and $m_S = \Omega((c_S)^2)$, so combining Eq. (28) and Eq. (29), and using the fact that a lower bound on the query complexity of ESTO gives a lower bound on the controlled quantum cost complexity of of STO, we have

$$\begin{align} ConQCC_\epsilon(\text{STO}) &\geq \frac{1-2\sqrt{\epsilon(1-\epsilon)}}{4} \times \max\left\{\sqrt{Mm_*}, \sqrt{(N-M+1)m_S}\right\} \tag{30}\\ &= \Omega\left(\max\left\{\sqrt{M}c_*, \sqrt{(N-M+1)}c_S\right\}\right). \tag{31}\end{align}$$

With Eq. (20), this bound proves our algorithms are asymptotically optimal. In Figure 2, we compare the bound given by the reduction to ESTO with the Hybrid Algorithm. Even though the functions are asymptotically tight, the forms of these two bounds are quite different.

4.2 Exact Lower Bound for Cost Complexity of STO

In the introduction, we mentioned several reasons for wanting to prove exact optimality of our algorithm for STO. Aside from finding an example besides Grover's algorithm of an exactly optimal algorithm, proving our algorithm for STO is optimal would have several

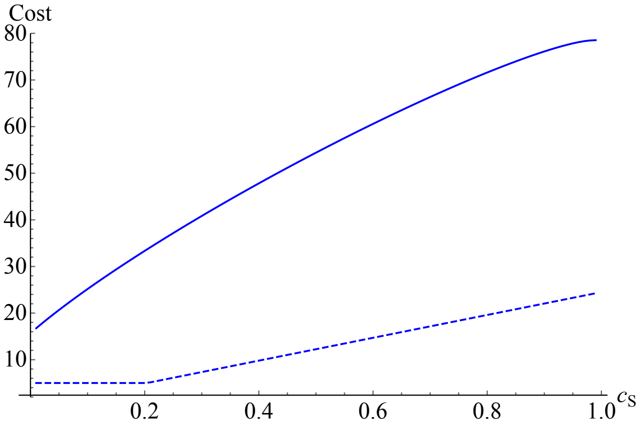


Figure 2 The solid line is the cost of the hybrid algorithm, while the dashed line is the lower bound on the cost given by Eq. (30). The cost is calculated with $c_* = 1$, $N = 10^4$, $M = 400$ and $\epsilon = 0$ while c_S is varied.

other implications. First, the algorithms described in Section 3 are all based on amplitude amplification, so if we can prove these approaches are optimal, that would give evidence that amplitude amplification is an exactly optimal algorithm for certain types of unstructured search problems.

Second, if we consider an extension of STO to many oracles, we can no longer prove asymptotic optimality of our amplitude amplification algorithm. Note that in amplitude amplification, (see Theorem 2), the inner algorithm ($\mathcal{A}$) is applied two times for each application of the oracle that identifies the target state (if $\mathcal{A} = \mathcal{A}^{-1}$). This factor of two is not accounted for in our lower bound of Section 4.1. While this factor of two can be swept under the rug using asymptotic notation, if we consider a problem with k nested oracles, and try to apply a similar strategy as for STO and use nested amplitude amplification, the innermost algorithm will accumulate an extra factor of 2^k in the number of times it must be applied. Using a strategy similar to Section 4.1 to lower bound this problem will not catch that factor of 2^k, for the same reason the factor of 2 is not characterized by the oracle simulation and adversary method. In the case of $k = \log N$ nested oracles, our bounds will no longer be asymptotically tight. Thus, if we can find an exact bound in the case of STO, we might be able to extend it to get asymptotically tight bounds for the case of nested oracles, providing evidence that multiple nestings of amplitude amplification are optimal for certain problems.

We have found that proving an exactly tight lower bound for STO is a challenge, and in fact we can only prove the hybrid algorithm is optimal in a limited setting. The difficulty in proving optimality even in this limited case provides insight into the difficulty of the more general case.

The restricted setting we investigate is to only consider *Grover-like* algorithms.

▶ **Definition 5.** A *Grover-like* algorithm with oracles $\{\mathcal{O}_1, \ldots, \mathcal{O}_l\}$ that act on an N-dimensional Hilbert space must:

- Use only an N-dimensional Hilbert space as its workspace,
- Initialize in the equal superposition state $|N\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$,
- Use only the unitaries $\{\mathcal{O}_1, \ldots, \mathcal{O}_l\}$ and $G = \mathbb{I} - 2|N\rangle\langle N|$, and
- End with a measurement on the standard basis.

If we consider *Grover-like* algorithms for SEARCH, the state of the system is restricted to a 2-dimensional subspace spanned by $|N\rangle$ and $|i_*\rangle$. Since $G^2 = \mathcal{O}_*^2 = \mathbb{I}$, the only possible algorithm is alternating G and $\mathcal{O}_*$, and one can easily track the progress of the state through the two dimensional space towards $|i_*\rangle$, thus trivially proving that in this setting, Grover's algorithm is exactly optimal.

We will see in the proof of Theorem 6 that for STO, the picture becomes much more complicated. In fact, even in the restricted setting of *Grover-like* algorithms, we need an additional assumption to prove optimality. In particular, we show

▶ **Theorem 6** (Exact Lower Bound). *The cost of every Grover-like algorithm for STO that succeeds with probability at least $1-\epsilon$ for a constant ϵ is at least*

$$\frac{c_S\sqrt{N}\arcsin\sqrt{1-\epsilon}}{2}\sec\left(\phi_{opt}+\sqrt{M/N}\right), \tag{32}$$

where ϕ_{opt} satisfies

$$\phi_{opt} = \max\begin{cases} 0, \\ \phi : \tan\left(\phi+\sqrt{\frac{M}{N}}\right) = \phi + \frac{c_*}{c_S}\sqrt{\frac{M}{N}}. \end{cases} \tag{33}$$

We also require the conditions $M, N/M \to \infty$ and $C \to 0$, where

$$C \equiv \frac{c_S\sqrt{N}}{c_*\sqrt{\epsilon}2M\cos\left(\phi_{opt}+\sqrt{M/N}\right)}. \tag{34}$$

Theorem 6 matches the cost of our hybrid algorithm, Eq. (25).

The proof of Theorem 6 can be found in Appendix B; here we provide a very brief sketch. Just as a *Grover-like* algorithm for standard search can be thought of as acting on a two dimensional subspace of the full N-dimensional Hilbert space, a Grover-like algorithm for STO can be thought of as acting on a three-dimensional subspace. We create a progress function as a position of the state in this subspace such that G has no affect on the progress function, while $\mathcal{O}_*$ and $\mathcal{O}_S$ can cause the progress function to increase or decrease. We then show that the increase in the progress function due to one of the oracles, divided by the cost of that oracle, is bounded. In other words, for a given cost, we can only increase the progress function by a certain amount, no matter which oracle is used. We finally take the total change in the progress function necessary to achieve success, and divide by the change in progress per cost to put a lower bound the cost.

5 Classical Cost Complexity of STO

In this section, we give bounds on the classical randomized cost complexity (RCC) of STO. We will examine both the exact and bounded error cost complexity. For the exact cost complexity, we see that there are two classical algorithms that resemble Algorithm 1 and Algorithm 2, but whereas in the quantum case, it is possible to do better with the Hybrid Algorithm, we prove that there is no classical counterpart to the Hybrid Algorithm. In the case of exact and bounded error cost complexity, we see a polynomial increase in cost compared to the quantum case.

In the case of exact classical cost complexity, we have:

▶ **Lemma 7.** *The exact (0-error) classical cost complexity of STO is*

$$RCC_0(STO) = \min\{Nc_*, (N-1)c_S + Mc_*\}. \tag{35}$$

Proof. We consider an adversarial oracle that knows in advance the queries the algorithm will make.

Recall that for $i \in [N]$, f_S identifies whether $i \in S$ and f_* identifies whether $i = i_*$. We say an item has been *completely queried* if it has been queried with f_S, and is found to not be an element of S, or if it has been queried with f_*. Then the adversarial oracle acts in the following way:

- The first $M-1$ items that the algorithm queries using oracle f_S are all elements of S.
- If all elements except one have been queried (but not necessarily completely queried) using either function f_* or f_S, the final element to be queried will be an element of S (even if this element is not queried using f_S).
- The last element to be completely queried is the marked item, if it exists.

Any algorithm acting against this adversarial oracle that makes q queries using f_S, has worst-case cost at least

$$\begin{aligned} &Nc_S + Mc_* && \text{if } q = N, \\ &qc_S + [(N-q) + (M-1)]c_* && \text{if } N-1 \geq q \geq M-1, \\ &qc_S + Nc_* && \text{if } M-1 \geq q \geq 0. \end{aligned} \tag{36}$$

These expressions are minimized at $q = N-1$ or $q = 0$, and we obtain

$$RCC_0(STO) \geq \min\{Nc_*, (N-1)c_S + Mc_*\}. \tag{37}$$

For the upper bound, consider the following two algorithms.

▶ **Algorithm 4.** *Query all items using f_*. This algorithm will find the marked item if it exists with certainty, and has cost Nc_*.*

▶ **Algorithm 5.** *Query all but the last item using f_S. Then:*

- *If M items of S have been found, query f_* on these M items.*
- *If $M-1$ items of S have been found, query f_* on these $M-1$ items, and also the last item (the item that was not queried using f_S).*
- *Otherwise $|S| \neq M$ and therefore no marked item exists.*

This algorithm will find the marked item if it exists with certainty, and has cost $(N-1)c_S + Mc_*$.

Thus we have

$$RCC_0(STO) \leq \min\{Nc_*, (N-1)c_S + Mc_*\}. \tag{38}$$

◀

Algorithm 1 can be thought of as the quantum version of Algorithm 4, while Algorithm 2 can be thought of as the quantum version of Algorithm 5. In the 0-error classical case, these two approaches tell the whole story. However, in the quantum case, you can do better with the Hybrid Algorithm. The Hybrid Algorithm works by doing something very quantum, which is to partially search for the elements of S. In the classical case, this doesn't work. Once you've found an element of S, you've found it; there is no way to partially find an element of S.

With Lemma 7, we've proven that in the 0-error case, we can obtain a polynomial reduction in cost by using a quantum algorithm for STO. Next, we show this polynomial reduction holds even in the case of bounded error algorithms. We do this by reducing STO to the problem of SEARCH. Recall that for SEARCH, we have:

▶ **Lemma 8.** *Any randomized classical algorithm that solves SEARCH with bounded probability must query f_* at least $\Omega(N)$ times.*

Now we can prove the reduction of STO to standard search:

▶ **Lemma 9.** *Any randomized classical algorithm that solves STO with bounded probability of error must use as least $\Omega(N)$ queries to either f_* or f_S, as long as $M/N \leq 1/9$.*

Proof. Suppose there is a randomized algorithm $\mathcal{A}$ that solves STO with probability 3/4 and makes q_* queries to f_* and q_S queries to f_S. Then we will use $\mathcal{A}$ to find i_* in the case when we are given f_* but not f_S. To do this, we will use f_* to create a function that behaves similarly to f_S. We choose a subset $T \in [N]$ with $|T| = M - 1$ at random, and create a function f_T that acts as

$$f_T(i) = \begin{cases} 1 & \text{if } i \in T \\ 0 & \text{if } i \notin T. \end{cases} \tag{39}$$

Then we create the function $\tilde{f}_S$ to simulate f_S, where

$$\tilde{f}_S(i) = f_T(i) \vee f_*(i). \tag{40}$$

Each time we want to query $\tilde{f}_S$, we must query $f_*(i)$. Notice that $\tilde{f}_S$ behaves like a valid f_S function unless i_* exists and $i_* \in T$ (because in this case $\tilde{f}_S$ marks $M - 1$ items instead of M.) $i_* \in T$ with probability $\frac{M-1}{N.}$

We create $\tilde{f}_S$ as above, and we implement $\mathcal{A}$, but every time $\mathcal{A}$ asks us to apply f_S, we instead apply $\tilde{f}_S$. This new algorithm will succeed with probability $3/4(1-(M-1)/N) \geq 2/3$, because it succeeds with probability 3/4 as long as $i_* \notin \mathcal{F}$. This means we have created an algorithm for standard search which uses $q_* + q_S$ queries to f_* and which succeeds with probability 2/3. But by Lemma 8, we must have $q_* + q_S = \Omega(N)$. ◀

Finally, we note that there is an additional restriction on the number of queries to f_*:

▶ **Lemma 10.** *Any randomized classical algorithm that solves STO with bounded probability must use at least $\Omega(M)$ queries to f_*.*

Proof. Suppose the elements of the subset S were known. Then in the worst case, that would still only narrow down the search to M items. (This is the worst case because if $|S| \neq M$, then one immediately knows there is no marked item.) One must then perform a search for one marked item out of M, which requires $\Omega(M)$ queries via Lemma 8. ◀

Now we can state our lower bound on the query cost of STO:

▶ **Theorem 11.** *The bounded error classical randomized cost complexity of STO is*

$$RCC(STO) = \min\left\{\Omega(c_S N + c_* M), \Omega(c_* N)\right\}. \tag{41}$$

Proof. When $M/N \leq 1/9$, we solve the following linear program:

$$\begin{aligned} \text{minimize: } & q_* c_* + q_S c_S \\ \text{subject to: } & q_* \geq f_1(M, \epsilon) \\ & q_* + q_S \geq f_2(N, M, \epsilon). \end{aligned} \tag{42}$$

When $M/N > 1/9$, from Lemma 10, we have have $q_* = \Omega(M) = \Omega(N)$, so the cost is as least $\Omega(c_* M) = \Omega(c_* N)$. ◀

Comparing Eq. (41) with Eq. (20), we see that there is always a separation between the quantum and classical costs of STO. In particular, to get the quantum scaling from the classical scaling, simply replace all M's and N's by $\sqrt{M}$ and $\sqrt{N}$.

6 Conclusions and Open Questions

While query complexity is a well understood and powerful tool for quantifying the power of quantum computers, there are still problems that are not easily characterized by query complexity. Cost complexity is one way of extending the standard query model, and we've argued that this approach has potential applications in constraint satisfaction problems.

While we motivated STO with problems like k-SAT, graph isomorphism, and the traveling salesman problem, it is not obvious how much of a speed-up an STO inspired algorithm for these problems would be. The speed-up in STO depends critically on N, M, c_*, and c_s. It would be interesting to calculate approximately what this relationship is, for example, in a random k-SAT instance. Once this relationship is better understood, we could determine the amount of speed-up an STO algorithm would give for such a problem. However, even with a better understanding of this relationship, it is unlikely that M would be known exactly. In that case, a method such as fixed point search [16] might be helpful.

STO is a very simple extension of a search problem, and thus the methods described here all have a Grover-ish flavor to them. It would be interesting to find well motivated problems for the cost complexity model where other quantum algorithms could be employed.

We have also left open the question of the exact cost of STO. We believe our algorithm is optimal, but it seems new techniques are needed to prove it.

Acknowledgments. The authors would like to thank Edward Farhi, Andrew Childs, and Aram Harrow for illuminating discussions. Funding for SK provided by the Department of Defense. HSL and CYL are supported by the ARO grant Contract Number W911NF-12-0486. CYL gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

References

1 Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proc. 32nd ACM STOC*, pages 636–643. ACM, 2000.

2 Andris Ambainis. Quantum search with variable times. *Theory of Computing Systems*, 47(3):786–807, 2010.

3 Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems – the hardness of quantum rewinding. *arXiv preprint arXiv:1404.6898*, 2014.

4 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001.

5 Aleksandrs Belovs. Learning-graph-based quantum algorithm for k-distinctness. In *Proc. IEEE 53rd FOCS*, pages 207–216. IEEE Computer Society, 2012.

6 Aleksandrs Belovs and Ansis Rosmanis. On the power of non-adaptive learning graphs. *Computational Complexity*, 23(2):323–354, 2014.

7 Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

8 Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv preprint quant-ph/0005055*, 2000.

9 Nicolas J Cerf, Lov K Grover, and Colin P Williams. Nested quantum search and structured problems. *Physical Review A*, 61(3):032303, 2000.

10 Cătălin Dohotaru and Peter Høyer. Exact quantum lower bound for grover's problem. *Quantum Information and Computation*, 9(5-6):533–540, 2009.

11 Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 2004.

12 Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proc. 39th ACM STOC*, pages 526–535, 2007.

13 Troy Lee, Rajat Mittal, Ben W Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proc. 52nd IEEE FOCS*, pages 344–353. IEEE, 2011.

14 Ashley Montanaro. Quantum search with advice. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 77–93. Springer, 2011.

15 Aran Nayebi, Scott Aaronson, Aleksandrs Belovs, and Luca Trevisan. Quantum lower bound for inverting a permutation with advice. *arXiv preprint arXiv:1408.3193*, 2014.

16 Theodore J Yoder, Guang Hao Low, and Isaac L Chuang. Fixed-point quantum search with an optimal number of queries. *Physical review letters*, 113(21):210501, 2014.

A Analysis of the Hybrid Algorithm

Throughout this section, when we are calculating something "to zeroth order", we drop terms whose sizes are $O(M^{-1/2})$ or $O((M/N)^{1/4})$ multiplied by the size of the largest term.

In Section 3, Eq. (24), we showed that the cost of the Hybrid Algorithm is

$$\mathrm{Cost(Hybrid)} = \left\lceil \frac{\arcsin\sqrt{1-\epsilon} - \arcsin\frac{\sqrt{1-\alpha}}{\sqrt{M}}}{2\arcsin\frac{\sqrt{1-\alpha}}{\sqrt{M}}} \right\rceil \times \left(c_* + 2c_S \left\lceil \frac{\left(\arcsin\sqrt{1-\alpha} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil \right). \tag{43}$$

In this appendix, we prove that in the limit of $M \to \infty$ and $N/M \to \infty$, there is a choice of α such that the cost is

$$\mathrm{Cost(Hybrid)} = \frac{c_S\sqrt{N}\arcsin\sqrt{1-\epsilon}}{2}\sec\left(\phi_{opt} + \sqrt{\frac{M}{N}}\right), \tag{44}$$

where ϕ_{opt} is given by

$$\phi_{opt} = \max\begin{cases} 0 \\ \phi : \tan\left(\phi + \sqrt{\frac{M}{N}}\right) = \phi + \frac{c_*}{c_S}\sqrt{\frac{M}{N}}. \end{cases} \tag{45}$$

We first define

$$t = \left\lceil \frac{\left(\arcsin\sqrt{1-\alpha} - \arcsin\sqrt{\frac{M}{N}}\right)}{2\arcsin\sqrt{\frac{M}{N}}} \right\rceil, \tag{46}$$

so t is a non-negative integer. Substituting t for α in Eq. (43), we obtain

$$\begin{aligned}\mathrm{Cost(Hybrid)} =& (2tc_S + c_*) \\ &\times \left\lceil \arcsin\sqrt{1-\epsilon}\left[2\arcsin\left(\frac{\sin\left((2t+1)\arcsin\sqrt{\frac{M}{N}}\right)}{\sqrt{M}}\right)\right]^{-1} - 1/2 \right\rceil.\end{aligned} \tag{47}$$

To zeroth order, this becomes

$$\text{Cost(Hybrid)} = \frac{(2tc_S + c_*)\sqrt{M}\arcsin\sqrt{1-\epsilon}}{2\sin\left((2t+1)\sqrt{\frac{M}{N}}\right)}. \tag{48}$$

Finally, we denote $\phi = 2t\sqrt{M/N}$ to obtain

$$\text{Cost(Hybrid)} = \frac{\left(\phi c_S + \sqrt{\frac{M}{N}}c_*\right)\sqrt{N}\arcsin\sqrt{1-\epsilon}}{2\sin\left(\phi+\sqrt{\frac{M}{N}}\right)}. \tag{49}$$

We take the partial derivative of the cost with respect to ϕ, and set it to zero to find the value of ϕ that gives the smallest cost. We find the cost is minimized when $\phi = \phi_{opt}$, where ϕ_{opt} satisfies

$$\tan\left(\phi_{opt} + \sqrt{M/N}\right) = \phi_{opt} + \frac{c_*}{c}\sqrt{M/N}. \tag{50}$$

Notice that there is always a solution with $\phi_{opt} \in [-\sqrt{M/N}, \pi/2]$. However t is non-negative, so if $\phi_{opt} < 0$ we set $\phi_{opt} = 0$. This condition, along with Eq. (49) and Eq. (50), immediately gives the cost claimed in Eq. (44).

We might not be able to exactly attain this cost, because t must be an integer, so we might only be able to set ϕ close to ϕ_{opt}. We show that even if we can't set ϕ exactly to ϕ_{opt}, we can still attain the cost of Eq. (44), to zeroth order.

There are two cases to consider. In the first case, we assume $(M/N)^{1/4} \le \phi_{opt} \le \pi/2$. We require that t be a non-negative integer, so we choose $t = \left\lceil (\phi_{opt}\sqrt{N})/(2\sqrt{M}) \right\rceil$, and hence we set

$$\phi = \left\lceil \frac{\phi_{opt}}{2}\sqrt{\frac{N}{M}} \right\rceil 2\sqrt{\frac{M}{N}}. \tag{51}$$

For that choice, notice that

$$\phi - \phi_{opt} = O\left((M/N)^{1/2}\right). \tag{52}$$

This allows us to relate terms involving ϕ to those involving ϕ_0:

$$\begin{aligned}
\sin\left(\phi + \sqrt{M/N}\right) &= \sin\left(\phi_{opt} + \sqrt{M/N}\right) \pm O((M/N)^{1/2}) \\
&= \sin\left(\phi_{opt} + \sqrt{M/N}\right)\left(1 \pm O((M/N)^{1/4})\right) \\
&= \left(\phi_{opt} + \frac{c_*}{c_S}\sqrt{M/N}\right)\cos\left(\phi_{opt} + \sqrt{M/N}\right)\left(1 \pm O\left((M/N)^{1/4}\right)\right) \\
&= \left(\phi + \frac{c_*}{c_S}\sqrt{M/N}\right)\cos\left(\phi_{opt} + \sqrt{M/N}\right)\left(1 \pm O\left((M/N)^{1/4}\right)\right),
\end{aligned} \tag{53}$$

where in the first line, we use the angle addition formula and Eq. (52); in the second, we use the assumption that $\phi_{opt} \ge (M/N)^{1/4}$; in the third line we applied Eq. (50); and in the last we have used Eq. (52) and the assumption on the size of ϕ_{opt}. Plugging Eq. (53) into our expression for the cost in Eq. (49), we have that to zeroth order, we obtain Eq. (44), as desired.

We now consider the second case, when $0 \leq \phi_{opt} < (M/N)^{1/4}$. In this case, we simply set $t = 0$, and hence $\phi = 0$. Plugging $\phi = 0$ the cost of Eq. (49), we have, to zeroth order,

$$\text{Cost(Hybrid)} = \frac{\arcsin\sqrt{1-\epsilon}\sqrt{N}}{2} c_*. \tag{54}$$

We will show that Eq. (54) and Eq. (44) are equivalent for $0 \leq \phi_{opt} < (M/N)^{1/4}$. We have

$$\sec\left(\phi_{opt} + \sqrt{M/N}\right) = 1 + O\left((M/N)^{1/4}\right). \tag{55}$$

We can expand Eq. (50) to get

$$c_S = c_*\left(1 - O\left((M/N)^{1/4}\right)\right). \tag{56}$$

Plugging Eqs. (55) and (56) into Eq. (44) and keeping only zeroth order terms, we recover Eq. (54).

B Proof of Theorem 6

In this section, we prove the following theorem:

▶ **Theorem 6** (Exact Lower Bound). *The cost of every Grover-like algorithm for STO that succeeds with probability at least $1-\epsilon$ for a constant ϵ is at least*

$$\frac{c_S\sqrt{N}\arcsin\sqrt{1-\epsilon}}{2}\sec\left(\phi_{opt} + \sqrt{M/N}\right), \tag{32}$$

where ϕ_{opt} satisfies

$$\phi_{opt} = \max\begin{cases} 0, \\ \phi : \tan\left(\phi + \sqrt{\frac{M}{N}}\right) = \phi + \frac{c_*}{c_S}\sqrt{\frac{M}{N}}. \end{cases} \tag{33}$$

We also require the conditions $M, N/M \to \infty$ and $C \to 0$, where

$$C \equiv \frac{c_S\sqrt{N}}{c_*\sqrt{\epsilon 2M}\cos\left(\phi_{opt} + \sqrt{M/N}\right)}. \tag{34}$$

Proof. Throughout this section, when we say to zeroth order, we mean dropping terms of size at most $O(M^{-1/2})$ or $O\left((M/N)^{1/2}\right)$ or $O(C)$ of the zeroth order terms.

Since we only consider the operations $\mathcal{O}_S$, $\mathcal{O}_*$, and G, the state of the system never leaves the three-dimensional space spanned by the orthonormal states

$$\left\{\ |i_*\rangle,\quad |S^-\rangle = \tfrac{1}{\sqrt{M-1}}\textstyle\sum_{i\in S-\{i_*\}}|i\rangle,\quad |S^\perp\rangle = \tfrac{1}{\sqrt{N-M}}\textstyle\sum_{i\notin S}|i\rangle\ \right\}. \tag{57}$$

It turns out that it is more convenient to work in a slightly shifted basis from that of Eq. (57). We instead use the orthonormal basis states:

$$\begin{aligned}
|x\rangle &= \cos\theta_0|i_*\rangle - \sin\theta_0|S^-\rangle, \\
|y\rangle &= \cos\phi_0\sin\theta_0|i_*\rangle + \cos\phi_0\cos\theta_0|S^-\rangle - \sin\phi_0|S^\perp\rangle, \\
|z\rangle &= \sin\phi_0\sin\theta_0|i_*\rangle + \cos\theta_0\sin\phi_0|S^-\rangle + \cos\phi_0|S^\perp\rangle \\
&= |N\rangle.
\end{aligned} \tag{58}$$

We can think of these states as forming the axes of a 3-dimensional space, where a state

$$|\chi\rangle = x|x\rangle + y|y\rangle + z|z\rangle \tag{59}$$

is identified with the point (x, y, z). Then if the algorithm is initialized in the equal superposition state $|z\rangle$, the goal of the algorithm is to move from the $|z\rangle$-axis towards the $|x\rangle$-axis.

Since any normalized state of the system corresponds to a point on the unit sphere in this space, let us now introduce polar coordinates, with the $|x\rangle$-axis as the polar axis. Specifically, we associate the state $|\chi\rangle$ with the polar coordinates (θ, ϕ), where

$$x = \sin\theta, \quad y = \cos\theta\sin\phi, \quad z = \cos\theta\cos\phi \tag{60}$$

for $\theta \in [-\pi/2, \pi/2]$. (The variable ϕ in this section plays a nearly identical role to ϕ in Appendix A, so we use the same variable name.)

If we multiply a state by -1, this transforms the coordinates from (θ, ϕ) to $(-\theta, \phi+\pi)$. Because overall phases do not affect the state, we can apply this transformation for free. In particular, we use it to "pick a gauge" and choose the coordinates that satisfy $\theta \geq 0$.

For a Grover-like algorithm which finds the marked state with high success probability, the algorithm starts at the point $(\theta = 0, \phi = 0)$, and must end near $\theta = \pi/2$. We define a progress function $H(\theta, \phi)$, for $\theta > 0$, as

$$H(\theta, \phi) = \theta - k \min_{\ell\in\mathbb{Z}} |\phi + 2\ell\pi - \pi/2|, \tag{61}$$

where

$$\begin{aligned} k &= \theta_0 \cos(\phi_{opt} + \phi_0), && (62)\\ \phi_0 &= \arcsin\sqrt{M/N}, && (63)\\ \theta_0 &= \arcsin\sqrt{1/M}, && (64)\\ \phi_{opt} &= \max\begin{cases} 0 \\ \phi : \tan(\phi+\phi_0) = \phi + \frac{c_*}{c}\phi_0. \end{cases} && (65)\end{aligned}$$

The second term of $H(\theta, \phi)$ is proportional to the angular distance of ϕ to $\pi/2$ (taken so the distance is $< \pi$).

Before we analyze how each unitary changes the progress function, we will look at the total progress that must occur for the algorithm to succeed. The total progress gained by the algorithm must be larger than the difference between the value of the progress function at the starting point and the end point. We pick the starting point as the *last* time the algorithm increases θ from less than $2\theta_0$ to more than $2\theta_0$, and $\phi \geq 0$. (We require $\phi \geq 0$ for Lemma 12, and we require $\theta \geq 2\theta_0$ in order to calculate the progress due to $\mathcal{O}_*$.) We will show later that such a point will always exist for any successful algorithm, and also that at such a point $\theta < 6\theta_0$. Thus the value of the progress function at the starting point is at most $6\theta_0$.

For the end point of the algorithm, note that the probability of success is

$$\sin^2(\theta) > 1 - \epsilon, \tag{66}$$

to zeroth order. Thus the total change in progress function is at least

$$\arcsin\sqrt{1-\epsilon} - k\pi - 6\theta_0 > \arcsin\sqrt{1-\epsilon} - (6+\pi)\theta_0, \tag{67}$$

where we bound k using Eq. (62), and the $k\pi$ term comes from the worst possible value of ϕ when θ gets sufficiently large.

We note the following: from Eq. (25) and Eq. (62) we see that the cost of the optimal algorithm is at most

$$\frac{c_S \arcsin\sqrt{1-\epsilon}}{\phi_0 k}, \tag{68}$$

and from Eq. (67) the change in the progress function is at least $\arcsin\sqrt{1-\epsilon}-(6+\pi)\theta_0$; therefore the progress per unit cost must be at least $\phi_0 k/c_S$, to zeroth order. It therefore follows that when calculating the change in progress function, we only need to keep track of terms up to order $O(\phi_0 k/c_S)$ per cost. For example, for $\mathcal{O}_*$, we need only keep track of the change in *progress* (not progress per cost) up to order $O(\phi_0 k c_*/c_S)$.

The change in the progress function $H(\theta,\phi)$ due to the unitaries G, $\mathcal{O}_S$, and $\mathcal{O}_*$ can be calculated by how they change the coordinates (θ,ϕ) of a state. After some algebra and using our gauge choice, we obtain

- G: The unitary G is a reflection about the z-axis, and in polar coordinates is the map

  $$G:\ (\theta,\phi)\to(\theta,\pi-\phi). \tag{69}$$

  Comparing with Eq. (61), we see G has no effect on the progress function.

- $\mathcal{O}_S$: The oracle $\mathcal{O}_S$ is a reflection about the state which has polar coordinates $(\theta=0,\phi=-\phi_0)$.

  $$\mathcal{O}_S:\ (\theta,\phi)\to(\theta,\pi-\phi-2\phi_0) \tag{70}$$

  We see that $\mathcal{O}_S$ can change the progress function by at most $2\phi_0 k$. Thus the increase in the progress function per cost due to $\mathcal{O}_S$ is at most

  $$\frac{2\phi_0 k}{c_S}=\frac{2\phi_0\theta_0\cos(\phi_{opt}+\phi_0)}{c_S}. \tag{71}$$

- $\mathcal{O}_*$: The oracle $\mathcal{O}_*$ is a reflection about the state $|i_*\rangle$, which is close to $|x\rangle$. We find $\mathcal{O}_*$ transforms coordinates as

  $$\theta\to\theta+2\theta_0\sin(\phi+\phi_0)+O(\theta_0^2) \tag{72}$$

  $$\phi\to\pi+\phi+O\left(\frac{\theta_0}{\cos\theta}\right). \tag{73}$$

Now we consider how $\mathcal{O}_*$ affects the progress function; unlike the previous cases, which we calculated exactly, we will only analyze this case to zeroth order. We will first show that we can assume $|\phi|\le\pi/2$. Suppose that $|\phi|>\pi/2$ just before we would like to apply $\mathcal{O}_*$. Then instead of applying $\mathcal{O}_*$, we apply $G\mathcal{O}_*G$. One can check that with this replacement, when $\mathcal{O}_*$ is applied, $|\phi|\le\pi/2$. Furthermore one can verify that this replacement causes θ to increase (which can only be good for the progress function), while on the other hand, the value of ϕ changes by at most $O(\theta_0/\cos\theta)$ due to this replacement, resulting in a change in the progress function of size $O(k\theta_0/\sqrt{\epsilon})$ (using Eq. (66) to bound $\cos\theta$). Using our assumption that that $C=o(1)$, this change has order less than $O(\phi_0 k c_*/c_S)$, and so can be discarded using the argument following Eq. (68). We can therefore assume that $\mathcal{O}_*$ is always applied at $|\phi|\le\pi/2$.

Now we can examine the change in the progress function due to the action of $\mathcal{O}_*$. The increase in the progress function is

$$\begin{aligned}&2\theta_0\sin(\phi+\phi_0)+O\left(\theta_0^2\right)\\&-k\left(\min_{\ell\in\mathbb{Z}}|-\phi+2\ell\pi-\pi/2|-\min_{\ell\in\mathbb{Z}}|\phi+2\ell\pi-\pi/2|\right)+O\left(\frac{k\theta_0}{\cos\theta}\right).\end{aligned}\tag{74}$$

Since $|\phi|\leq\pi/2$, the increase in the progress function due to $\mathcal{O}_*$ is less than

$$2\theta_0\sin(\phi+\phi_0)-2\phi\theta_0\cos(\phi_{opt}+\phi_0)+O\left(\frac{\theta_0^2}{\sqrt{\epsilon}}\right),\tag{75}$$

where we have used the value of k from Eq. (62) and bounded $\cos\theta$ with Eq. (66).

Taking the first and second derivatives of Eq. (75) with respect to ϕ, we see that when $\phi\geq 0$, the increase in the progress function is maximized when $\phi=\phi_{opt}$. It turns out that if one applies $\mathcal{O}_*$ at $\phi<0$, it is sometimes possible to achieve a larger increase in progress per cost than when $\phi\geq 0$. However, we show at the end of this section, (Lemma 12), that applying $\mathcal{O}_*$ when $\phi<0$ will always be less efficient (up to higher order terms) in terms of the increase in progress function per cost, than applying $\mathcal{O}_*$ at $\phi=\phi_{opt}$, when viewed in the context of the larger algorithm. Applying the definition of ϕ_{opt} from Eq. (65) to Eq. (75), and using the definition of C from Eq. (34), the increase in the progress function due to $\mathcal{O}_*$ is less than

$$\frac{c_*2\phi_0\theta_0\cos(\phi_{opt}+\phi_0)}{c_S}\left(1+O(\phi_0^2)+O\left(C\right)\right),\tag{76}$$

where the $O(\phi_0^2)$ term accounts for the case that $\phi_{opt}=0$.

From Eq. (71) and Eq. (76) we see that (to zeroth order) the maximum increase in the progress function per cost is the same whether $\mathcal{O}_*$ is applied or $\mathcal{O}_S$ is applied. Dividing the total necessary change in progress (Eq. (67)) by the maximum change in progress per cost (Eq. (76)) gives us the minimum cost:

$$\arcsin\sqrt{1-\epsilon}\frac{c_S}{2\phi_0\theta_0\cos(\phi_{opt}+\phi_0)}\left(1-O(C)-O(M^{-1/2})-O\left((M/N)^{-1/2}\right)\right).\tag{77}$$

In the limit of $N,M\to\infty$ and $C\to 0$, (to zeroth order) we have that the cost is at least

$$\arcsin\sqrt{1-\epsilon}\frac{c_S\sqrt{M}}{2\phi_0\cos(\phi_{opt}+\phi_0)},\tag{78}$$

which matches the cost of Eq. (25).

We now justify why the value of the progress function must be less than $6\theta_0$ when we start tracking it. Immediately before we start tracking the progress function, we have $\theta<2\theta_0$, so the bound on the increase in progress given by Eq. (75) does not necessarily apply. However, it is simple to show that the increase in the progress function due to $\mathcal{O}_*$ is always bounded by $2\theta_0$, where we have dropped terms of $O(\theta_0^2/\sqrt{\epsilon})$ as before. Thus if $\theta<2\theta_0$, and then $\mathcal{O}_*$ is applied, θ can increase by at most $2\theta_0$, and so the new value of θ satisfies $\theta<4\theta_0$. At this point, $\theta>2\theta_0$, but ϕ might be negative. Notice that θ can not increase unless $\mathcal{O}_*$ is applied, (and θ must increase in order to obtain a high probability of success) but $\mathcal{O}_*$ flips the sign of ϕ, so after applying $\mathcal{O}_*$ at most one more time, we will have both the conditions $\theta>2\theta_0$ and $\phi\geq 0$ satisfied, at which point we start tracking the progress function. This tells us that the value of θ will be at most $6\theta_0$ when we start tracking the progress function. ◀

▶ **Lemma 12.** *Suppose there is an algorithm than applies $\mathcal{O}_*$ when $\phi < 0$. Then there is always an alternative algorithm that achieves the same or greater increase in progress for the same or less cost (up to zeroth order), but applies $\mathcal{O}_*$ only when $\phi \geq 0$.*

Proof. We begin by classifying the the possible sequences of $\mathcal{O}_*$, $\mathcal{O}_S$, and G the algorithm can take. We will use notation such that unitaries act from right to left, so $G\mathcal{O}_*$ signifies $\mathcal{O}_*$ acts first, and then G acts.

First look at $\mathcal{O}_*$. We can always assume $\mathcal{O}_*$ is followed by a G; if it is not, insert a GG pair after the $\mathcal{O}_*$. Note in the discussion following Eq. (73), we proved that we can assume $|\phi| < \pi/2$ before applying $\mathcal{O}_*$. With Eqs. (69) and (73) we have

$$G\mathcal{O}_* : \phi \to -\phi + O\left(\frac{\theta_0}{\cos\theta}\right). \tag{79}$$

Since $|\phi| < \frac{\pi}{2}$ before $G\mathcal{O}_*$ acts, we also have $|\phi| < \frac{\pi}{2}$ after $G\mathcal{O}_*$ acts, up to an additive factor of $O\left(\frac{\theta_0}{\cos\theta}\right)$, which we can ignore thanks to the discussion following Eq. (68). Therefore $G\mathcal{O}_*$ maps ϕ inside the $|\phi| < \frac{\pi}{2}$ region.

In between applications of $G\mathcal{O}_*$, there is always a sequence of one of the following forms:

$$(G\mathcal{O}_S)^m, \quad G(G\mathcal{O}_S)^m, \quad (\mathcal{O}_S G)^m, \quad \text{or} \quad G(\mathcal{O}_S G)^m, \tag{80}$$

where m is a non-negative integer that indicates multiple applications of the unitary sequence inside the parenthesis. These are the only possible sequences because $\mathcal{O}_S\mathcal{O}_S = I$ and $GG = I$. Combining the action of G and $\mathcal{O}_S$ in Eqs. (69) and (70) we get

$$(\mathcal{O}_S G)^m : (\theta, \phi) \to (\theta, \phi - 2m\phi_0) \tag{81}$$

$$(G\mathcal{O}_S)^m : (\theta, \phi) \to (\theta, \phi + 2m\phi_0). \tag{82}$$

Thus the 4 sequences of Eq. (80) rotate ϕ by some amount $\pm 2m\phi_0$, possibly followed by the transformation $\phi \to \pi - \phi$.

Now we focus on the algorithm's action on ϕ. Since the $G\mathcal{O}_*$'s are mapping ϕ between points inside the $|\phi| < \frac{\pi}{2}$ region, the four possible sequences of alternating G and $\mathcal{O}_S$ in Eq (80) just connect the value of ϕ after applying $G\mathcal{O}_*$ to the value of ϕ before the next application of $G\mathcal{O}_*$. Generalizing Figure 3, one can see that the shortest path uses either $(G\mathcal{O}_S)^m$ or $(\mathcal{O}_S G)^m$ to connect points inside the $|\phi| < \frac{\pi}{2}$ region. Therefore we do not need to consider the sequences $G(\mathcal{O}_S G)^m$ or $G(G\mathcal{O}_S)^m$.

Next, we show that if one initially has $\phi > 0$, it is never advantageous to again apply $G\mathcal{O}_*$ when $\phi < 0$. Since the algorithm must consist of applications of $G\mathcal{O}_*$ separated by sequences of either $(\mathcal{O}_S G)^m$ or $(G\mathcal{O}_S)^m$, we can enumerate and address the three possible cases that lead us to apply $\mathcal{O}_*$ at some $\phi = \phi_{neg} < 0$ after initially having $\phi \geq 0$. The three possible cases are laid out graphically in Figure 4. In order to prove that none of the cases are optimal, we define the function

$$p_*(\phi) = 2(\theta_0 \sin(\phi + \phi_0) - k\phi) \tag{83}$$

as the change in progress function due to an application of $\mathcal{O}_*$, dropping higher order terms. Note for $\phi \geq 0$, ϕ_{opt} optimizes Eq. (83) as discussed after Eq. (75). We proceed to treat the three cases.

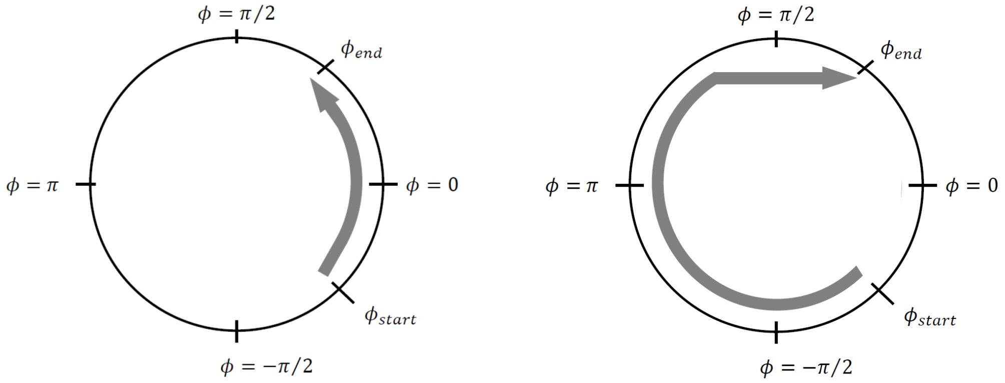


Figure 3 The path in the figure at left uses a sequence $(G\mathcal{O}_S)^m$ to move from ϕ_{start} to ϕ_{end}, whereas the path in figure at right uses a sequence $G(\mathcal{O}_SG)^m$. The path using $(G\mathcal{O}_S)^m$ is shorter, signifying that fewer uses of $\mathcal{O}_S$ are required to move from ϕ_{start} to ϕ_{end}, and thus this is the more efficient path.

Sequence I. We consider the following sequence of operations (see Figure 4):

(i) Start with $\phi_i > 0$. Then apply $G\mathcal{O}_*$ to get to $-\phi_i$.

(ii) Apply $(G\mathcal{O}_S)$ some number of times to increase ϕ to $\phi_{neg} > -\phi_i$.

(iii) Apply $G\mathcal{O}_*$ to get to $-\phi_{neg} < \phi_i$.

The change in progress due only to $\mathcal{O}_*$ in this sequence is

$$\begin{aligned}p_*(\phi_i) + p_*(\phi_{neg}) &= 2(\theta_0 \sin(\phi_i + \phi_0) - k\phi_i)\\ &+ 2(\theta_0 \sin(\phi_{neg} + \phi_0) - k\phi_{neg})\\ &\leq 4[\theta_0 \sin(\frac{\phi_i + \phi_{neg}}{2} + \phi_0) - k\frac{\phi_{neg} + \phi_i}{2}]\\ &= 2p_*(\phi_i + \phi_{neg})\\ &\leq 2p_*(\phi_{opt}),\end{aligned} \tag{84}$$

Since $\phi_{neg} + \phi_i \geq 0$, the average progress due to the two applications of $\mathcal{O}_*$ is worse than if we had applied $\mathcal{O}_*$ at ϕ_{opt} both times. Thus this sequence cannot be optimal.

Sequence II. We consider the following sequence of operations (see Figure 4):

(i) Start with $\phi_i > 0$. Then apply $G\mathcal{O}_*$ to get to $-\phi_i$.

(ii) Apply $(\mathcal{O}_SG)$ some number of times to decrease ϕ to $\phi_{neg} < -\phi_i$.

(iii) Apply $G\mathcal{O}_*$ to get to $-\phi_{neg} > \phi_i$.

Compare Sequence **II** to the following Sequence **2**:

(a) Start with $\phi_i > 0$. Then apply $(G\mathcal{O}_S)$ some number of times to increase ϕ to $-\phi_{neg} > \phi_i$.

The difference in progress between Sequence **II** and Sequence **2** is

$$\begin{aligned}&(2\theta_0 \sin(\phi_i + \phi_0) + 2\theta_0 \sin(\phi_{neg} + \phi_0))\\ =&4\theta_0 \sin(\frac{\phi_i + \phi_{neg}}{2} + \phi_0) \cos(\frac{\phi_i - \phi_{neg}}{2})\\ <&4\theta_0 \sin \phi_0,\end{aligned} \tag{85}$$

since $-\frac{\pi}{4} < \frac{\phi_i+\phi_{neg}}{2} < 0$ and $0 < \frac{\phi_i-\phi_{neg}}{2} < \frac{\pi}{2}$. Sequence **II** and Sequence **2** both use the same number of applications of $\mathcal{O}_S$ (in steps (ii) and (a) respectively). Therefore, the

Sequence **II** has an additional cost $2c_*$ while it only has an added increase in progress of

$$\begin{aligned}4\theta_0 \sin\phi_0 =&2p_*(0)\\ \leq&2p_*(\phi_{opt}).\end{aligned} \tag{86}$$

Therefore Sequence **II** does not attain the increase in progress per cost that one could attain by only applying $\mathcal{O}_*$ at ϕ_{opt}.

Sequence III. We consider the following sequence of operations (see Figure 4):

(i) Start with $\phi_i \geq 0$, then apply $(O_S G)$ some number of times to decrease ϕ to $\phi_{neg} < 0$.

(ii) Apply $G\mathcal{O}_*$ to get to $-\phi_{neg}$.

Compare Sequence **III** to the following Sequence **3**:

(a) Start with $\phi_i \geq 0$, and then apply $(O_S G)$ some number of times to decrease ϕ to ϕ_w such that $2\phi_0 > \phi_w \geq 0$.

(b) Apply $G\mathcal{O}_*$ to get to $-\phi_w$.

(c) Apply (GO_S) some number of times to increase ϕ to $-\phi_{neg} > 0$.

Note that we can always create a sequence with such a ϕ_w because $(O_S G)$ changes ϕ by at most $2\phi_0$ each time. The cost of Sequence **III** is the same as the cost of Sequence **3**. The difference in progress between Sequence **III** and Sequence **3** is

$$\begin{aligned}&2\theta_0 \sin(\phi_{neg} + \phi_0) - 2\theta_0 \sin(\phi_w + \phi_0)\\ \leq&4\theta_0 \cos\left(\frac{\phi_{neg} + \phi_w}{2} + \phi_0\right) \sin\left(\frac{\phi_{neg} - \phi_w}{2}\right)\\ <&0\end{aligned} \tag{87}$$

since $|\frac{\phi_{neg}+\phi_w}{2} + \phi_0| < \frac{\pi}{2}$ and $\frac{\pi}{2} < \frac{\phi_{neg}-\phi_w}{2} < 0$. Therefore Sequence III is not optimal either.

Hence we conclude that applying $\mathcal{O}_*$ at negative ϕ never achieves as much increase in progress per cost as applying $\mathcal{O}_*$ at ϕ_{opt}, and therefore we only need to consider applying $\mathcal{O}_*$ at positive ϕ, at ϕ_{opt}. ◀

C An Adversary Lower Bound

In this section, we will show how to apply the adversary method to the problem of cost complexity of STO.

Suppose we are given access to an oracle $\mathcal{O}_*$, which implements the function f_*, and an oracle $\mathcal{O}_S$, which implements the function f_S. Then any algorithm which solves STO using these oracles, after t steps, produces a state

$$|\psi^t_{f_*,f_S}\rangle = U^t\mathcal{O}_{c_t}\cdots U^2\mathcal{O}_{c_2}U^1\mathcal{O}_{c_1}|\psi^0\rangle, \tag{88}$$

where $c_j \in \{*, S\}$, and U^j are fixed unitaries independent of f_* and f_S.

We create an adversary matrix Γ, a matrix whose rows and columns are indexed by pairs of functions $(f_*, f_S) \in D_{\text{STO}}$, where D_{STO} is the set of valid inputs to STO. Furthermore, we have the condition that that $\Gamma[(f_*, f_S), (g_*, g_S)] = 0$ if $\text{STO}(f_*, f_S) = \text{STO}(g_*, g_S)$. With this notation, we define the progress function:

$$W^t = \sum_{(f_*,f_S),(g_*,g_S)\in D_{\text{STO}}\times D_{\text{STO}}} \Gamma_{(f_*,f_S),(g_*,g_S)} v_{f_*,f_S} v^*_{g_*,g_S} \langle\psi^t_{f_*,f_S}|\psi^t_{g_*,g_S}\rangle \tag{89}$$

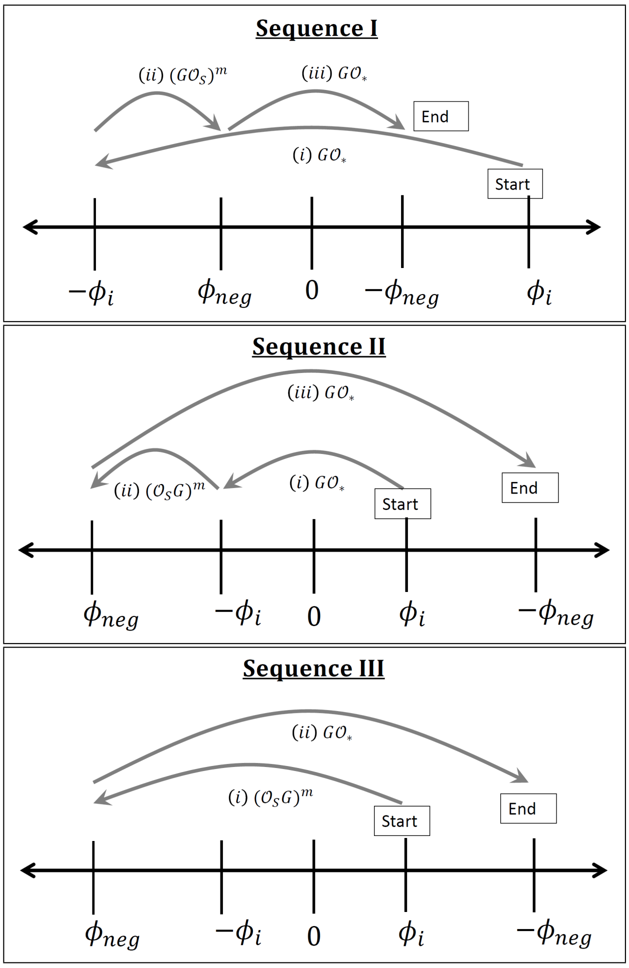


Figure 4 Possible paths that could lead to applying GO_* at a negative value of ϕ, when initially, ϕ has positive value.

for a vector v indexed by the elements of D_{STO}, such that $\|v\| = 1$ and v is an eigenvector of Γ with eigenvalue $\pm\|\Gamma\|$, (where $\|\cdot\|$ signifies the l-2 norm for vectors or the induced l-2 norm for matrices).

Then following [12][3], we have

1. $W^0 = \|\Gamma\|$.
2. $W^T \le \left(2\sqrt{\epsilon(1-\epsilon)} + 2\epsilon\right)\|\Gamma\|$, for any algorithm with probability of error at most ϵ.
3. $W^{t-1} - W^t \le 2\max_i \|\Gamma \circ D_i^{c_t}\|$ where $D_i^{c_t}$ are $|D_{\text{STO}}| \times |D_{\text{STO}}|$ matrices satisfying

$$D_i^*[(f_*, f_S), (g_*, g_S)] = \begin{cases} 0 \text{ if } f_*(i) = g_*(i), \\ 1 \text{ otherwise}, \end{cases} \qquad D_i^S[(f_*, f_S), (g_*, g_S)] = \begin{cases} 0 \text{ if } f_S(i) = f_S(i), \\ 1 \text{ otherwise}. \end{cases}$$

Thus if q_* queries are made to $\mathcal{O}_*$ and q_S queries are made to $\mathcal{O}_S$, we have

$$\|\Gamma\| g(\epsilon) \le q_* \max_i \|\Gamma \circ D_i^*\| + q_S \max_i \|\Gamma \circ D_i^S\| \tag{90}$$

[3] The proofs are identical, so we omit them.

where

$$g(\epsilon)=\frac{1-\left(2\sqrt{\epsilon(1-\epsilon)}+2\epsilon\right)}{2}. \tag{91}$$

We construct the following adversary matrix for STO: $\Gamma[(f_*,f_S),(g_*,g_S)]=1$ if one of the following conditions holds:

- $\mathrm{STO}(f_*,f_S)=1$, $\mathrm{STO}(g_*,g_S)=0$, and $f_S(i)=g_S(i)$ except if $f_*(i^*)=1$, then $g_S(i^*)=0$,
- $\mathrm{STO}(g_*,g_S)=1$, $\mathrm{STO}(f_*,f_S)=0$, and $g_S(i)=f_S(i)$ except if $g_*(i^*)=1$, then $f_S(i^*)=0$.

Otherwise, $\Gamma=0$.

One can calculate (or it is easy to see by analogy to a standard Grover search over $N-M+1$ items) that

$$\begin{aligned}\|\Gamma\|&=\sqrt{N-M+1},\\ \max_i\|\Gamma\circ D_i^{c_t}\|&=1,\\ \max_i\|\Gamma\circ D_i^{S}\|&=1.\end{aligned} \tag{92}$$

Plugging into Eq. (90) we have

$$g(\epsilon)\sqrt{N-M+1}\leq q_*+q_S, \tag{93}$$

so for $N>M/2$, we have

$$QCC(\mathrm{STO})=\Omega(c_S\sqrt{N}). \tag{94}$$

We also consider a second adversary matrix for STO. Let $\Gamma[(f_*,f_S),(g_*,g_S)]=1$ if one of the following conditions holds:

- $\mathrm{STO}(f_*,f_S)=1$, $\mathrm{STO}(g_*,g_S)=0$, and $f_S(i)=g_S(i)$,
- $\mathrm{STO}(g_*,g_S)=1$, $\mathrm{STO}(f_*,f_S)=0$, and $g_S(i)=f_S(i)$.

Otherwise, $\Gamma=0$.

In this case, the adversary matrix only pairs instances such that $\mathcal{O}_S$ is the same in both pairs. Thus it is as if the set S is known ahead of time. In this case, one can calculate (or it is easy to see by analogy to a standard Grover search over M items), that

$$\begin{aligned}\|\Gamma\|&=\sqrt{M}\\ \max_i\|\Gamma\circ D_i^{j_t}\|&=1\\ \max_i\|\Gamma\circ D_i^{S}\|&=0.\end{aligned} \tag{95}$$

Plugging into Eq. (90), we have

$$g(\epsilon)\sqrt{M}\leq q_*, \tag{96}$$

so

$$QCC(\mathrm{STO})=\Omega(c_*\sqrt{M}) \tag{97}$$

Combining Eq. (94) and Eq. (97), we obtain a bound that matches Eq. (20):

$$QCC(\mathrm{STO})=\Omega\left(\max\{c_*\sqrt{M},c_S\sqrt{N}\}\right). \tag{98}$$

The Resource Theory of Steering

Rodrigo Gallego and Leandro Aolita

Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany

Abstract

We present an operational framework for Einstein-Podolsky-Rosen steering as a physical resource. To begin with, we characterize the set of *steering non-increasing operations* (SNIOs) – i.e., those that do not create steering– on arbitrary-dimensional bipartite systems composed of a quantum subsystem and a black-box device. Next, we introduce the notion of *convex steering monotones* as the fundamental axiomatic quantifiers of steering. As a convenient example thereof, we present the *relative entropy of steering.* In addition, we prove that two previously proposed quantifiers, the steerable weight and the robustness of steering, are also convex steering monotones. To end up with, for minimal-dimensional systems, we establish, on the one hand, necessary and sufficient conditions for pure-state steering conversions under stochastic SNIOs and prove, on the other hand, the non-existence of *steering bits*, i.e., measure-independent maximally steerable states from which all states can be obtained by means of the free operations. Our findings reveal unexpected aspects of steering and lay foundations for further resource-theory approaches, with potential implications in Bell non-locality.

1998 ACM Subject Classification J.2 Physics

Keywords and phrases Entanglement, EPR-steering, nonlocality, resource theories

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.27

1 Introduction

Steering, as Schrödinger named it [38], is an exotic quantum effect by which ensembles of quantum states can be remotely prepared by performing local measurements at a distant lab. It allows [43, 23, 34] to certify the presence of entanglement between a user with an untrusted measurement apparatus, Alice, and another with a trusted quantum-measurement device, Bob. Thus, it constitutes a fundamental notion between quantum entanglement [22], whose certification requires quantum measurements on both sides, and Bell non-locality [13], where both users possess untrusted black-box devices. Steering can be detected through simple tests analogous to Bell inequalities [14], and has been verified in a variety of remarkable experiments [29, 8, 37, 7, 20, 39], including steering without Bell non-locality [35] and a fully loop-hole free steering demonstration [44]. Apart from its fundamental relevance, steering has been identified as a resource for one-sided device-independent quantum key-distribution (QKD), where only one of the parts has an untrusted apparatus while the other ones possess trusted devices [9, 21]. There, the experimental requirements for unconditionally secure keys are less stringent than in fully (both-sided) device-independent QKD [4, 1, 2].

The formal treatment of a physical property as a resource is given by a *resource theory.*The basic component of this is a restricted class of operations, called the *free operations*, subject to a physically relevant constraint. The free operations are such that every *free state*, i.e., every one without the property in question, is mapped into a free state, so that the resourceful states can be defined as those not attainable by free operations acting on any free state. Furthermore, the quantification of the resource is also built upon the free operations: The fundamental

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 27–38
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

necessary condition for a function to be a measure of the resource is that it is monotonous – non-increasing – under the free operations. That is, the operations that do not increase the resource on the free states do not increase it on all other states either. Entanglement theory [22] is the most popular and best understood [40, 32, 10, 11] resource theory. There, the constrain on the operations is the unavailability of quantum communication, which yields the local operations assisted by classical communication (LOCCs) [6] as the corresponding free operations. Nevertheless, resource theories have been formulated also for states out of thermal equilibrium [12], asymmetry [3], reference frames [19], and quantum coherence [26, 5], for instance.

In steering theory, systems are described by an ensemble of quantum states, on Bob's side, each one associated to the conditional probability of a measurement outcome (output) given a measurement setting (input), on Alice's. Such conditional ensembles are sometimes called *assemblages* [33, 36, 31]. The free operations for steering, which we call *steering non-increasing operations* (SNIOs), must thus arise from constrains native of a natural scenario where steerable assemblages are useful for some physical task. Curiously, up to now, no attempt for an operational framework of steering as a resource has been reported.

In this submission we develop the resource theory of steering. First, we derive the explicit expression of the most general SNIO, for arbitrarily many inputs and outputs for Alice's black box and arbitrary dimension for Bob's quantum system. We show that this class of free operations emerges naturally from the basic restrictions of QKD with assemblages, i.e., of one-side device-independent QKD [9, 21]. With the derived SNIOs, we provide a formal definition of steering monotones. As an example thereof, we present the relative entropy of steering, for which we also introduce, on the way, the notion of relative entropy between assemblages. In addition, we prove SNIO monotonicity for two other recently proposed steering measures, the steerable weight [36] and the robustness of steering [31], and convexity for all three measures. To end up with, we prove two theorems on steering conversion under stochastic SNIOs for the lowest-dimensional case, i.e., qubits on Bob's side and 2 inputs × 2 outputs on Alice's. In the first one, we show that it is impossible to transform via SNIOs, not even probabilistically, an assemblage composed of pairs of pure orthogonal states into another assemblage composed also of pairs of pure orthogonal states but with a different pair overlap, unless the latter is unsteerable. This yields infinitely many inequivalent classes of steering already for systems of the lowest dimension. In the second one, we show that there exists no assemblage composed of pairs of pure states that can be transformed into any assemblage by stochastic SNIOs. It follows that, in striking contrast to entanglement theory, there exists no operationally well defined, measure-independent maximally steerable assemblage of minimal dimension.

The submission is organized as follows. In Sec. 2 we formally define assemblages and present their basic properties. In Sec. 3 we characterise the SNIOs. In Sec. 4 we introduce the notion of convex steering monotones. In Sec. 5 we present the relative entropy of steering. In Sec. 6 we show convexity and SNIO-monotonicity of the steerable weight and the robustness of steering. In Sec. 7 we study, for minimal-dimensional systems, assemblage conversions under SNIOs and prove the in existence of pure-assemblage steering bits. Finally, in Sec. 8 we present our conclusions and mention some future research directions that our results offer.

Note also, that some proofs and supplemental material can be found in the Appendix of the online version on which this submission is based [17], in which case it will be indicated explicitly.

2 Assemblages and steering

We consider two distant parties, Alice and Bob, who have each a half of a bipartite system. Alice holds a so-called black-box device, which, given a classical input $x \in [s]$, generates a classical output $a \in [r]$, where s and r are natural numbers and the notation $[n] \equiv \{0, \ldots, n-1\}$, for $n \in \mathbb{N}$, is introduced. Bob holds a quantum system of dimension d (*qudit*), whose state he can perfectly characterize tomographically via trusted quantum measurements. The joint state of their system is thus fully specified by an *assemblage*

$$\rho_{A|X} \equiv \{P_{A|X}(a,x), \varrho(a,x)\}_{a\in[r],x\in[s]}, \tag{1}$$

of normalized quantum states $\varrho(a,x) \in \mathcal{L}(\mathcal{H}_B)$, with $\mathcal{L}(\mathcal{H}_B)$ the set of linear operators on Bob's subsystem's Hilbert space $\mathcal{H}_B$, each one associated to a conditional probability $P_{A|X}(a,x)$ of Alice getting an output a given an input x. We denote by $P_{A|X}$ the corresponding conditional probability distribution.

Equivalently, each pair $\{P_{A|X}(a,x), \varrho(a,x)\}$ can be univocally represented by the unnormalized quantum state

$$\varrho_{A|X}(a,x) \equiv P_{A|X}(a,x) \times \varrho(a,x). \tag{2}$$

In turn, an alternative representation of the assemblage $\rho_{A|X}$ is given by the set $\hat{\rho}_{A|X} \equiv \{\hat{\rho}_{A|X}(x)\}_x$ of quantum states

$$\hat{\rho}_{A|X}(x) \equiv \sum_a |a\rangle\langle a| \otimes \varrho_{A|X}(a,x) \in \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_B), \tag{3}$$

where $\{|a\rangle\}$ is an orthonormal basis of an auxiliary extension Hilbert space $\mathcal{H}_E$ of dimension r. The states $\{|a\rangle\}$ do not describe the system inside Alice's box, they are just abstract flag states to represent its outcomes with a convenient bra-ket notation. Expression (3) gives the counterpart for assemblages of the so-called extended Hilbert space representation used for ensembles of quantum states [28]. We refer to $\hat{\rho}_{A|X}$ for short as the *quantum representation* of $\rho_{A|X}$ and use either notation upon convenience.

We restrict throughout to *no-signaling assemblages*, i.e., those for which Bob's reduced state $\varrho_B \in \mathcal{L}(\mathcal{H}_B)$ does not depend on Alice's input choice x:

$$\varrho_B \equiv \sum_a \varrho_{A|X}(a,x) = \sum_a \varrho_{A|X}(a,x') \;\; \forall\, x,x'. \tag{4}$$

The assemblages fulfilling the no-signaling condition (4) are the ones that possess a *quantum realization*. That is, they can be obtained from local quantum measurements by Alice on a joint quantum state $\varrho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ shared with Bob, where $\mathcal{H}_A$ is the Hilbert space of the system inside Alice's box. For any no-signaling assemblage $\rho_{A|X}$, we refer as the *trace of the assemblage* to the x-independent quantity

$$Tr[\rho_{A|X}] \equiv Tr_{EB}[\hat{\rho}_{A|X}] = Tr[\varrho_B] = \sum_a P_{A|X}(a,x), \tag{5}$$

and say that the assemblage is normalized if $Tr[\rho_{A|X}] = 1$ and unnormalized if $Tr[\rho_{A|X}] \leq 1$.

An assemblage $\sigma_{A|X} \equiv \{\varsigma_{A|X}(a,x)\}_{a\in[r],x\in[s]}$, being $\varsigma_{A|X}(a,x) \in \mathcal{L}(\mathcal{H}_B)$ unnormalized states, is called *unsteerable* if there exist a probability distribution P_Λ, a conditional probability distribution $P_{A|X\Lambda}$, and normalized states $\xi(\lambda) \in \mathcal{L}(\mathcal{H}_B)$ such that

$$\varsigma_{A|X}(a,x) = \sum_\lambda P_\Lambda(\lambda) P_{A|X\Lambda}(a,x,\lambda)\, \xi(\lambda) \;\; \forall\, x,a. \tag{6}$$

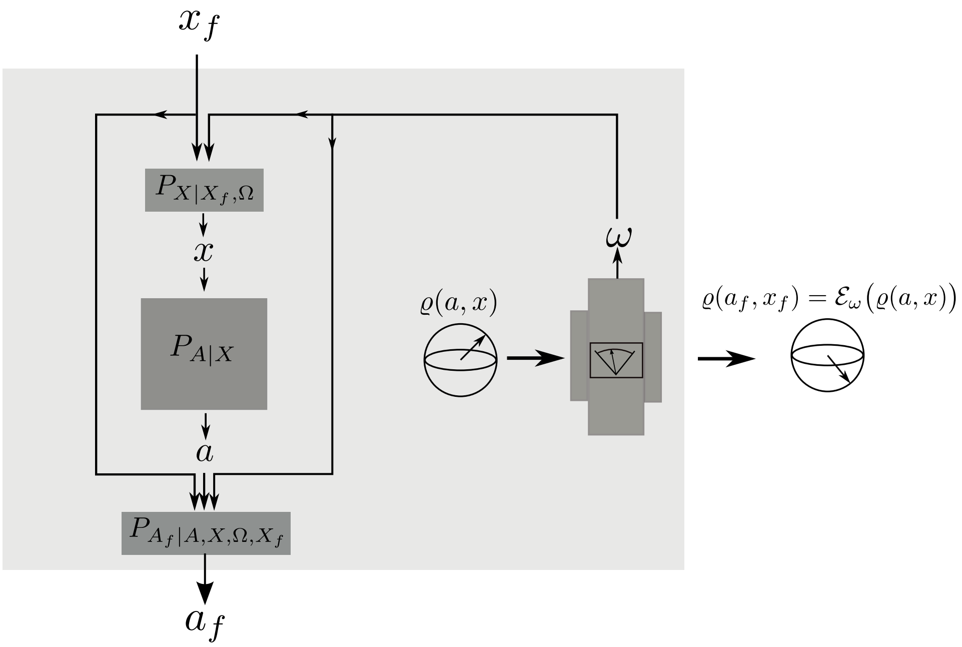


Figure 1 Schematic representation of a SNIO map $\mathcal{M}$: The initial assemblage $\rho_{A|X}$ consists of a black-box, with inputs x and outputs a, governed by the probability distribution $P_{A|X}$, in Alice's hand, and a quantum subsystem in one of the states $\{\varrho(a,x)\}_{a,x}$, in Bob's hands. The final assemblage $\rho_{A_f|X_f}=\mathcal{M}(\rho_{A|X})$ is given by a final black-box, represented by the light-grey rectangle, of inputs x_f and outputs a_f, and a final subsystem, represented outside the light-grey rectangle, in the state $\varrho(a_f,x_f)=\mathcal{E}_\omega(\varrho(a,x))$. To implement $\mathcal{M}$, first, Bob applies, with a probability $P_\Omega(\omega)$, a stochastic quantum operation $\mathcal{E}_\omega$ that leaves his subsystem in the state $\mathcal{E}_\omega(\varrho(a,x))$. He communicates ω to Alice. Then, Alice generates x by processing the classical bits ω and x_f according to the conditional distribution $P_{X|X_f,\Omega}$. She inputs x to her initial device, upon which the bit a is output. Finally, Alice generates the output a_f of the final device by processing x_f, ω, x, and a, according to the conditional distribution $P_{A_f|A,X,\Omega,X_f}$.

Such assemblages can be obtained by sending a shared classical random variable λ to Alice, correlated with the state $\xi(\lambda)$ sent to Bob, and letting Alice classically post-process her random variable according to $P_{A|X\Lambda}$, with $P_{X,\Lambda}=P_X\times P_\Lambda$ so that condition (4) holds. The variable λ is called a *local-hidden variable* and the decomposition (6) is accordingly referred to as a *local-hidden state* (LHS) model. We refer to the set of all unsteerable assemblages as LHS. Any assemblage that does not admit a LHS model as in Eq. (6) is called *steerable*. An assemblage is compatible with classical correlations if, and only if, it is unsteerable.

3 The operational framework

3.1 Physical constraints defining the free operations

QKD consists of the extraction of a secret key from the correlations of local-measurement outcomes on a bipartite quantum state. The most fundamental constraint to which any generic QKD protocol is subject is, of course, the lack of a private safe classical-communication channel between distant labs. Otherwise, if such channel was available, the whole enterprise of QKD would be pointless. This imposes restrictions on the operations allowed so as not to break the security of the protocol. For instance, clearly, the local-measurement outcomes cannot be communicated, as they can be intercepted by potential eavesdroppers who could, with them, immediately crack the key. Of particular relevance for this submission are the assumptions on the measurement devices. In non-device-independent QKD protocols entanglement is the resource and security is proven under the assumption that the users have a specific quantum state and perfectly characterized measurement devices [16]. Knowledge of the state by an eavesdropper does not compromise the security. Therefore, prior to the measurements producing the key, the users are allowed to preprocess the state in any way and exchange information about it, for instance with LOCCs and even eventually disregarding the state and aborting the protocol run. Pre-processing abortions or classical communication can at most provide an eavesdropper with knowledge about the state, not about the key, and therefore do not affect the security.

The situation is different in device-independent QKD (DIQKD) [4, 1, 2]. There, the resource is given by Bell non-local correlations and no assumption is made either on the quantum state or the measurement devices. The users effectively hold black-box measurement devices, whose inputs and outputs are all to which they have access. Since such inputs and outputs are precisely the bits with which the key is established, both classical communication and abortions are forbidden. Communication of outputs can directly reveal the key, as mentioned, whereas abortions and communication of inputs can, due to the locality and detection loopholes, respectively, be maliciously exploited by an eavesdropper to obtain information about the key too. Hence, the natural constrains of DIQKD impose that operations are restricted to well-known [18, 41] paradigm of shared-randomness and local classical information processing.

Steerable assemblages are resources for one-sided DIQKD (1S-DIQKD) [9, 21]. There, while no assumption is made on the bipartite quantum state or Alice's measurement device, Bob's measurement device is perfectly characterized. This is effectively described by assemblages as given in Eq. (1). Thus, it is reasonable to take the natural constrains of 1S-DIQKD as the basic restrictions to define the free operations for steering. The asymmetry in the assumptions on Alice and Bob's devices, results in an asymmetry between the operations allowed to each of them. Alice is subject to the same restrictions as in device-independent QKD, while Bob, to those of non-device-independent QKD. Hence, Alice cannot abort or transmit any information, but, prior to his key-producing measurement, Bob is allowed to implement arbitrary local quantum operations to his subsystem, including stochastic ones with possible abortions, and send any feedback about them to Alice. Altogether, this gives a clear physical motivation for our operational framework: We take SNIOs as the assemblage transformations involving only deterministic classical maps on Alice's side and arbitrary – possibly stochastic – quantum operations on Bob's side assisted by one-way classical communication only from Bob to Alice.[1]. Note that shared randomness, which also does not introduce any security compromise in 1S-DIQKD, can always be recast as one-way classical communication from Bob to Alice and needs, therefore, not be considered explicitly.

[1] Throughout the article, the term "deterministic" is used to refer probability (trace) preserving classical (quantum) maps. These are maps such that, given an input bit (state), generate an output bit (state), respectively, with certainty, i.e., they never cause an abortion. This does not mean that the output cannot be chosen at random. That is, this should not be confused with classical (quantum) maps where the output bit (state) is a Kronecker delta function of the input bit (a unitary transformation of the input state). In turn, the term "stochastic" is used throughout to refer to non probability-preserving classical or non trace-preserving quantum transformations that do not occur with certainty.

3.2 The free operations

More technically, we consider the general scenario of *stochastic SNIOs*, i.e., SNIOs that do not necessarily occur with certainty, which map the initial assemblage $\rho_{A_f|X_f}$ into a final assemblage $\rho_{A_f|X_f}$ (see Fig. 1). Bob's generic quantum operation can be represented by an incomplete generalised measurement. This is described by a completely-positive non trace-preserving map $\mathcal{E} : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_{B\,f})$ defined by

$$\mathcal{E}(\cdot) := \sum_{\omega} \mathcal{E}_{\omega}(\cdot), \text{ with } \mathcal{E}_{\omega}(\cdot) := K_{\omega} \ \cdot \ K_{\omega}^{\dagger}, \tag{7a}$$

$$\text{such that } \sum_{\omega} K_{\omega}^{\dagger} K_{\omega} \leq \mathbb{1}, \tag{7b}$$

where $\mathcal{H}_{B\,f}$ is the final Hilbert space, of dimension d_f, and $K_\omega : \mathcal{H}_B \to \mathcal{H}_{B\,f}$ is the measurement operator corresponding to the ω-th measurement outcome. For any normalized $\varrho_B \in \mathcal{L}(\mathcal{H}_B)$, the trace $Tr[\mathcal{E}(\varrho_B)] \leq 1$ of the map's output $\mathcal{E}(\varrho_B)$ represents the probability that the physical transformation $\varrho_B \to \mathcal{E}(\varrho_B)/Tr[\mathcal{E}(\varrho_B)]$ takes place. In turn, the map $\mathcal{E}_\omega(\cdot)$ describes the post-selection of the ω-th outcome, which occurs with a probability

$$P_{\Omega}(\omega) := Tr[\mathcal{E}_{\omega}(\rho_B)] = Tr[K_{\omega} \varrho_B K_{\omega}^{\dagger}] \leq 1. \tag{8}$$

Since Alice can only process classical information, the allowed one-way communication from Bob to her must be classical too. Thus, it can only consists of the outcome ω of his quantum operation. Classical bit processings are usually referred to as *wirings* [13]. Alice's wirings map $a \in [r]$ and $x \in [s]$ into input and out bits $a_f \in [r_f]$ and $x_f \in [s_f]$, respectively, of the final assemblage, where s_f and r_f are natural numbers. The most general wirings respecting the above constraints are described by conditional probability distributions $P_{X|X_f,\Omega}$ and $P_{A_f|A,X,\Omega,X_f}$ of generating x from ω and x_f and a_f from x_f, ω, x, and a, respectively, as sketched in Fig. 1. Finally, since, as mentioned, her wirings must be deterministic, $P_{X|X_f,\Omega}$ and $P_{A_f|A,X,\Omega,X_f}$ must be normalized probability-preserving distributions.

All in all, the general form of the resulting maps is parametrized in the following definition (see App. A in [17]).

▶ **Definition 1** (Stochastic SNIOs). We define the class SNIO of *(stochastic) SNIOs* as the set of (stochastic) maps $\mathcal{M}$ that take an arbitrary assemblage $\hat{\rho}_{A|X}$ into a final assemblage $\hat{\rho}_{A_f|X_f} := \mathcal{M}(\hat{\rho}_{A|X})$, where

$$\mathcal{M}(\hat{\rho}_{A|X}) := \sum_{\omega} (\mathbb{1} \otimes K_{\omega})\, \mathcal{W}_{\omega}(\hat{\rho}_{A|X})\, (\mathbb{1} \otimes K_{\omega}^{\dagger}), \tag{9}$$

being $\mathcal{W}_\omega$ a *deterministic w*iring map given by

$$\begin{aligned} [\mathcal{W}_{\omega}(\hat{\rho}_{A|X})](x_f) := & \sum_{a_f,a,x} P(x|x_f,\omega) P(a_f|a,x,\omega,x_f) \\ & \times \ (|a_f\rangle\langle a| \otimes \mathbb{1})\, \hat{\rho}_{A|X}(x)\, (|a\rangle\langle a_f| \otimes \mathbb{1}), \end{aligned} \tag{10}$$

with $P(x|x_f,\omega)$ and $P(a_f|a,x,\omega,x_f)$ short-hand notations for the conditional probabilities $P_{X|X_f,\Omega}(x,x_f,\omega)$ and $P_{A_f|A,X,\Omega,X_f}(a_f,a,x,\omega,x_f)$, respectively.

Note that the final assemblage (9) is in general not normalized: Introducing

$$\mathcal{M}_{\omega}(\,\cdot\,) := (\mathbb{1} \otimes K_{\omega})\, \mathcal{W}_{\omega}(\,\cdot\,)\, (\mathbb{1} \otimes K_{\omega}^{\dagger}), \tag{11}$$

such that $\mathcal{M}(\,\cdot\,) = \sum_\omega \mathcal{M}_\omega(\,\cdot\,)$, we obtain, using Eqs. (3), (4), (5), (8), (9), and (10), that

$$Tr[\mathcal{M}(\hat{\rho}_{A|X})] = \sum_\omega Tr[\mathcal{M}_\omega(\hat{\rho}_{A|X})] = \sum_\omega P_\Omega(\omega) \leq 1. \tag{12}$$

As with quantum operations, the trace (12) of $\mathcal{M}(\hat{\rho}_{A|X})$ represents the probability that the physical transformation $\hat{\rho}_{A|X} \to \mathcal{M}(\hat{\rho}_{A|X})/Tr[\mathcal{M}(\hat{\rho}_{A|X})]$ takes place. Analogously, the map $\mathcal{M}_\omega$ describes the assemblage transformation that takes place when Bob post-selects the ω-th outcome, which occurs with probability $Tr[\mathcal{M}_\omega(\hat{\rho}_{A|X})] = P_\Omega(\omega)$. In the particular case where $\mathcal{M}$ is trace-preserving, we refer to it as a *deterministic SNIO.*

Finally, we prove in App. B of Ref. [17] the following theorem.

▶ **Theorem 2** (SNIO invariance of LHS). *Any map of the class* SNIO *takes every unsteerable assemblage into an unsteerable assemblage.*

4 Steering monotonicity

As the natural next step, we introduce an axiomatic approach to define steering measures, i.e., a set of reasonable postulates that a bona fide quantifier of the steering of a given assemblage should fulfill.

▶ **Definition 3** (SNIO-monotonicity and convexity). A function $\mathscr{S}$, from the space of assemblages into $\mathbb{R}_{\geq 0}$, is a *steering monotone* if it fulfils the following two axioms:

(i) $\mathscr{S}(\hat{\rho}_{A|X}) = 0$ for all $\hat{\rho}_{A|X} \in$ LHS.

(ii) $\mathscr{S}$ does not increase, on average, under deterministic SNIOs, i.e.,

$$\sum_\omega P_\Omega(\omega)\mathscr{S}\left(\frac{\mathcal{M}_\omega(\hat{\rho}_{A|X})}{Tr\left[\mathcal{M}_\omega(\hat{\rho}_{A|X})\right]}\right) \leq \mathscr{S}(\hat{\rho}_{A|X}) \tag{13}$$

for all $\hat{\rho}_{A|X}$, with $P_\Omega(\omega) = Tr\left[\mathcal{M}_\omega(\hat{\rho}_{A|X})\right]$ and $\sum_\omega P_\Omega = 1$.

Besides, $\mathscr{S}$ is a *convex steering monotone* if it additionally satisfies the property:

(iii) Given any real number $0 \leq \mu \leq 1$, and assemblages $\hat{\rho}_{A|X}$ and $\hat{\rho}'_{A|X}$, then

$$\mathscr{S}\left(\mu\,\hat{\rho}_{A|X} + (1-\mu)\hat{\rho}'_{A|X}\right) \leq \mu\,\mathscr{S}\left(\hat{\rho}_{A|X}\right) + (1-\mu)\mathscr{S}\left(\hat{\rho}'_{A|X}\right). \tag{14}$$

Condition i) reflects the basic fact that unsteerable assemblages should have zero steering. Condition ii) formalizes the intuition that, analogously to entanglement, steering should not increase – on average – under SNIOs, even if the flag information ω produced in the transformation is available. Finally, condition iii) states the desired property that steering should not increase by probabilistically mixing assemblages. The first two conditions are taken as mandatory necessary conditions, the third one only as a convenient property. Importantly, there exists a less demanding definition of monotonicity. There, the left-hand side of Eq. (13) is replaced by $\mathscr{S}\left(\mathcal{M}(\hat{\rho}_{A|X})/Tr[\mathcal{M}(\hat{\rho}_{A|X})]\right)$. That is, ii') it is demanded only that steering itself, instead of its average over ω, is non-increasing under SNIOs. The latter is actually the most fundamental necessary condition for a measure. However, monotonicity ii) is in many cases (including the present submission) easier to prove and, together with condition iii), implies monotonicity ii'). Hence, we focus throughout on monotonicity as defined by Eq. (13) and refer to it simply as *SNIO monotonicity.* All three known quantifiers of steering, the two ones introduced in Refs. [36, 31] as well as the one we introduce next, turn out to be convex steering monotones in the sense of Definition 3.

5 The relative entropy of steering

The first step is to introduce the notion of *relative entropy* between assemblages. To this end, for any two density operators ϱ and ϱ', we first recall the *quantum von-Neumann relative entropy*

$$S_{\mathrm{Q}}(\varrho\|\varrho') := Tr\left[\varrho\left(\log\varrho - \log\varrho'\right)\right] \tag{15}$$

of ϱ with respect to ϱ' and, for any two probability distributions P_X and P'_X, the *classical relative entropy*, or *Kullback-Leibler divergence*,

$$S_{\mathrm{C}}(P_X\|P'_X) := \sum_x P_X(x)[\log P_X(x) - \log P'_X(x)] \tag{16}$$

of P_X with respect to P'_X. The quantum and classical relative entropies (15) and (16) measure the distinguishability of states and distributions, respectively. To find an equivalent measure for assemblages, we note, for $\hat{\rho}_{A|X}(x)$ given by Eq. (3) and $\hat{\rho}'_{A|X}(x) := \sum_a P'_{A|X}(a,x)|a\rangle\langle a| \otimes \varrho'(a,x)$, that

$$\begin{aligned} S_{\mathrm{Q}}\left(\hat{\rho}_{A|X}(x)\|\hat{\rho}'_{A|X}(x)\right) &= S_{\mathrm{C}}\left(P_{A|X}(\cdot,x)\|P'_{A|X}(\cdot,x)\right) \\ &\quad + \sum_a P_{A|X}(a,x) S_{\mathrm{Q}}\left(\varrho(a,x)\|\varrho'(a,x)\right), \end{aligned} \tag{17}$$

where $P_{A|X}(\cdot,x)$ and $P'_{A|X}(\cdot,x)$ are respectively the distributions over a obtained from the conditional distributions $P_{A|X}$ and $P'_{A|X}$ for a fixed x. That is, the distinguishability between the states $\hat{\rho}_{A|X}(x)$ and $\hat{\rho}'_{A|X}(x) \in \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_B)$ equals the sum of the distinguishabilities between $P_{A|X}(x)$ and $P'_{A|X}(x)$ and between $\varrho(a,x)$ and $\varrho'(a,x) \in \mathcal{L}(\mathcal{H}_B)$, weighted by $P_{A|X}(a,x)$ and averaged over a.

The entropy (17), which depends on x, does not measure the distinguishability between the assemblages $\rho_{A|X}$ and $\rho'_{A|X}$. Since the latter are conditional objects, i.e., with inputs, a general strategy to distinguish them must allow for Alice choosing the input for which the assemblages' outputs are optimally distinguishable. Furthermore, Bob can first apply a generalised measurement on his subsystem and communicate the outcome γ to her, which she can then use for her input choice. This is the most general procedure within the allowed SNIOs. Hence, a generic distinguishing strategy under SNIOs involves probabilistically chosen inputs that depend on γ. Note, in addition, that the statistics of γ generated, described by distributions P_Γ or P'_Γ, encode differences between $\rho_{A|X}$ and $\rho'_{A|X}$ too and must therefore also be accounted for by a distinguishability measure. The following definition incorporates all these considerations.

▶ **Definition 4** (Relative entropy between assemblages). Given any two assemblages $\rho_{A|X}$ and $\rho'_{A|X}$, we define the *assemblage relative entropy* of $\rho_{A|X}$ with respect to $\rho'_{A|X}$ as

$$\begin{aligned} S_{\mathrm{A}}(\rho_{A|X}\|\rho'_{A|X}) &:= \max_{P_{X|\Gamma},\{E_\gamma\}}\Bigg[S_{\mathrm{C}}(P_\Gamma\|P'_\Gamma) \\ &+ \sum_{\gamma,x} P(x|\gamma)P_\Gamma(\gamma)S_{\mathrm{Q}}\left(\frac{\mathbb{1}\otimes E_\gamma\hat{\rho}_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger}{P_\Gamma(\gamma)}\,\Bigg\|\,\frac{\mathbb{1}\otimes E_\gamma\hat{\rho}'_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger}{P'_\Gamma(\gamma)}\right)\Bigg], \end{aligned} \tag{18}$$

where $E_\gamma : \mathcal{H}_B \to \mathcal{H}_B$ are generalised-measurement operators such that $\sum_\gamma E_\gamma^\dagger E_\gamma = \mathbb{1}$, $P_{X|\Gamma}$ is a conditional probability distribution of x given γ, the short-hand notation $P(x|\gamma) :=$

$P_{X|\Gamma}(x,\gamma)$ has been used, and

$$P_\Gamma(\gamma) := Tr[\mathbb{1}\otimes E_\gamma \hat{\rho}_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger] = Tr_B[E_\gamma \varrho_B E_\gamma^\dagger], \tag{19a}$$

$$P'_\Gamma(\gamma) := Tr[\mathbb{1}\otimes E_\gamma \hat{\rho}'_{A|X}(x)\mathbb{1}\otimes E_\gamma^\dagger] = Tr_B[E_\gamma \varrho'_B E_\gamma^\dagger], \tag{19b}$$

where ϱ'_B is Bob's reduced state for the assemblage $\rho'_{A|X}$.

In App. C of Ref. [17], we show that S_A does not increase – on average – under deterministic SNIOs and, as its quantum counterpart S_Q, is jointly convex. Hence, S_A is a proper measure of distinguishability between assemblages under SNIOs.[2]. The first term inside the maximization in Eq. (18) accounts for the distinguishability between the distributions of measurement outcomes γ and the second one for that between the distributions of Alice's outputs and Bob's states resulting from each γ, averaged over all inputs and measurement outcomes. In turn, the maximization over $\{E_\gamma\}$ and $P_{X|\Gamma}$ ensures that these output distributions and states are distinguished using the optimal SNIO-compatible strategy.

We are now in a good position to introduce a convex steering monotone. We do it with a theorem.

▶ **Theorem 5** (SNIO-monotonicity and convexity of $\mathscr{S}_\mathrm{R}$). *The relative entropy of steering $\mathscr{S}_\mathrm{R}$, defined for an assemblage $\rho_{A|X}$ as*

$$\mathscr{S}_R(\rho_{A|X}) := \min_{\sigma_{A|X}\in\mathsf{LHS}} S_A(\rho_{A|X} \parallel \sigma_{A|X}), \tag{20}$$

is a convex steering monotone.

The theorem is proven in App. C in Ref. [17].

6 Other convex steering monotones

Apart from $\mathscr{S}_\mathrm{R}$ two other quantifiers of steering have been recently proposed: the steerable weight [36] and the robustness of steering [31]. In this section, we show that these are also convex steering monotones.

▶ **Definition 6** (Steerable weight [36]). The steerable weight $\mathscr{S}_\mathrm{W}(\rho_{A|X})$ of an assemblage $\rho_{A|X}$ is the minimum $\nu\in\mathbb{R}_{\geq 0}$ such that

$$\rho_{A|X} = \nu\,\tilde{\rho}_{A|X} + (1-\nu)\sigma_{A|X}, \tag{21}$$

with $\tilde{\rho}_{A|X}$ an arbitrary assemblage and $\sigma_{A|X}\in\mathsf{LHS}$.

▶ **Definition 7** (Robustness of steering [31]). The robustness of steering $\mathscr{S}_\mathrm{Rob}(\rho_{A|X})$ of an assemblage $\rho_{A|X}$ is the minimum $\nu\in\mathbb{R}_{\geq 0}$ such that

$$\sigma_{A|X} := \frac{1}{1+\nu}\rho_{A|X} + \frac{\nu}{1+\nu}\,\tilde{\rho}_{A|X} \tag{22}$$

belongs to LHS, with $\tilde{\rho}_{A|X}$ an arbitrary assemblage.

[2] A natural question (which we leave open) is how to define a relative entropy between assemblages that is non-increasing under generic assemblage transformations instead of just SNIOs, so that it can be understood as measure of distinguishability under fully general strategies. That is the case of S_Q, for instance, which is non-increasing under not only LOCCs but also any completely positive map. However, to introduce a steering monotone, SNIO-monotonicity of S_A suffices.

In App. D in Ref. [17], we prove the following theorem.

▶ **Theorem 8** (SNIO-monotonicity and convexity of $\mathscr{S}_{\mathsf{W}}$ and $\mathscr{S}_{\mathsf{Rob}}$). *Both $\mathscr{S}_{W}$ and $\mathscr{S}_{Rob}$ are convex steering monotones.*

To end up with, we note that a steering measure for assemblages containing continuous-variable (CV) bosonic systems in Gaussian states has very recently appeared [24]. Even though our formalism can be straightforwardly extended to CV systems, such extension is outside the scope of the present submission.

7 Assemblage conversions and no steering bits

We say that $\Psi_{A|X}$ and $\Psi'_{A|X}$ are *pure assemblages* if they are of the form

$$\Psi_{A|X} \coloneqq \{P_{A|X}(a,x), |\psi(a,x)\rangle\langle\psi(a,x)|\}_{a,x}, \tag{23a}$$

$$\Psi'_{A|X} \coloneqq \{P'_{A|X}(a,x), |\psi'(a,x)\rangle\langle\psi'(a,x)|\}_{a,x}, \tag{23b}$$

where $|\psi(a,x)\rangle$ and $|\psi'(a,x)\rangle \in \mathcal{H}_B$, and *pure orthogonal assemblages* if, in addition, $\langle\psi(a,x)|\psi(\tilde{a},x)\rangle = \delta_{a\,\tilde{a}} = \langle\psi'(a,x)|\psi'(\tilde{a},x)\rangle$ for all x. Note that pure orthogonal assemblages are the ones obtained when Alice and Bob share a pure maximally entangled state and Alice performs a von-Neumann measurement on her share. We present two theorems about assemblage conversions under SNIOs.

The first one, proven in App. E in Ref. [17], establishes necessary and sufficient conditions for stochastic-SNIO conversions between pure orthogonal assemblages, therefore playing a similar role here to the one played in entanglement theory by Vidal's theorem [42] for stochastic-LOCC pure-state conversions.

▶ **Theorem 9** (Criterion for stochastic-SNIO conversion). *Let $\Psi_{A|X}$ and $\Psi'_{A|X}$ be any two pure orthogonal assemblages with $d = s = r = 2$. Then, $\Psi_{A|X}$ can be transformed into $\Psi'_{A|X}$ by a stochastic SNIO iff: either $\Psi'_{A|X} \in \mathsf{LHS}$ or $P'_{A|X} = P_{A|X}$ and*

$$|\langle\psi'(a,0)|\psi'(a,1)\rangle| = |\langle\psi(a,0)|\psi(a,1)\rangle| \ \forall\ a. \tag{24}$$

In other words, no pure orthogonal assemblage of minimal dimension can be obtained via a SNIO, not even probabilistically, from a pure orthogonal assemblage of minimal dimension with a different state-basis overlap unless the former is unsteerable. Hence, each state-basis overlap defines an inequivalent class of steering, there being infinitely many of them. This is in a way reminiscent to the inequivalent classes of entanglement in multipartite [15] or infinite-dimensional bipartite [30] systems, but here the phenomenon is found already for bipartite systems of minimal dimension.

The second theorem, proven in App. F in [17], rules out the possibility of there being a (non-orthogonal) minimal-dimension pure assemblage from which all assemblages can be obtained.

▶ **Theorem 10** (Non-existence of steering bits). *There exists no pure assemblage with $d = s = r = 2$ that can be transformed into any assemblage by stochastic SNIOs.*

Hence, among the minimal-dimension assemblages there is no operationally well defined *unit of steering*, or *steering bit*, i.e., an assemblage from which all assemblages can be obtained for free and can therefore be taken as a measure-independent maximally steerable assemblage. This is again in striking contrast to entanglement theory, where pure maximally entangled states can be defined without the need of entanglement quantifiers and each one can be transformed into any state by deterministic LOCCs [42, 27].

8 Discussion and outlook

We have introduced the resource theory of Einstein-Podolsky-Rosen steering. The restricted class of free operations for the theory, which we abbreviate by SNIOs, arises naturally from the basic physical constraints in one-sided device-independent QKD. It is composed of all the transformations involving deterministic bit wirings on Alice's side and stochastic quantum operations on Bob's assisted by one-way classical communication from Bob to Alice. With it, we introduced the notion of *convex steering monotones*, presented the *relative entropy of steering* as a convenient example thereof, and proved monotonicity and convexity of two other previously proposed steering measures. In addition, for minimal-dimensional systems, we established necessary and sufficient conditions for stochastic-SNIO conversions between pure-state assemblages and proved the non-existence of *steering bits*.

It is instructive to emphasize that the derived SNIOs correspond to a combination of the operations that do not increase the entanglement of quantum states, stochastic LOCCs, and the ones that do not increase the Bell non-locality of correlations, local wirings assisted by shared randomness. Regarding the latter, a resource-theory approach to Bell non-locality is only partially developed [18, 25, 41]. Hence, our findings are potentially useful also in Bell non-locality. In addition, our submission offers a number of challenges for future research. Namely, for example, the non-existence of steering bits of minimal dimension can be seen as an impossibility of steering dilution of minimal-dimension assemblages in the single-copy regime. We leave as open questions what the rules for steering dilution and distillation are for higher-dimensional systems, mixed-state assemblages, or in asymptotic multi-copy regimes, and what the steering classes are for mixed-state assemblages. Moreover, other fascinating questions are whether one can formulate a notion of *bound steering* or an analogue to the positive-partial-transpose criterion for assemblages.

References

1 A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

2 A. Acín *et al.*, Phys. Rev. Lett. **98**, 230501 (2007).

3 M. Ahmadi, D. Jennings and T. Rudolph, New J. Phys. **15**, 013057 (2013).

4 J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

5 T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).

6 C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

7 A. J. Bennet *et al.*, Phys. Rev. X **2**, 031003 (2012).

8 W. P. Bowen, R. Schnabel, and P. K. Lam, Phys. Rev. Lett. **90**, 043601 (2003).

9 C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).

10 F. G. S. L. Brandão and M. B. Plenio, Nature Phys. **4**, 873 (2008).

11 F. G. S. L. Brandão and M. B. Plenio, Comm. Math. Phys. 295, 829 (2010).

12 F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Phys. Rev. Lett. **111**, 250404 (2013).

13 N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

14 E. G. Cavalcanti, S. J. Jones, H. M. Wiseman and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

15 W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

16 A. K. Ekert, Phys. Rev. Lett. **67**, 661(1991).

17 R. Gallego and L. Aolita. The resource theory of steering. arXiv:1409.5804 (2014).

18 R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. Phys. Rev. Lett. **109**, 070401 (2012).

19 G. Gour and R. W. Spekkens, New J. Phys. **10**, 033023 (2008).

20 V. Händchen *et al.*, Nat. Phot. **6**, 598 (2012).

21 Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).

22 R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

23 S. J. Jones *et al.*, Phys. Rev. A **76**, 052116 (2007).

24 I. Kogias, A. R. Lee, S. Ragy and G. Adesso, arXiv:1410.1637 (2014).

25 B. Lang, T. Vertesi and M. Navascués, arXiv:1402.2850 (2014).

26 F. Levi and F. Mintert, New J. Phys. **16**, 033007 (2014).

27 M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

28 O. Oreshkov and J. Calsamiglia. Phys. Rev. A **79**, 032336 (2009).

29 Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).

30 M. Owari, K. Matsumoto, and M. Murao, Phys. Rev. A **70**, 050301(R) (2004).

31 M. Piani and J. Watrous, arXiv:1406.0530 (2014).

32 M. B. Plenio and S. Virmani, Quant. Inf. Comput. **7**, 1 (2007).

33 M. F. Pusey, Phys. Rev. A **88**, 032313 (2013).

34 M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Rev. Mod. Phys. **81**, 1727 (2009).

35 D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).

36 P. Skrzypczyk, M. Navascués, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).

37 D.-H. Smith *et al.*, Nat. Commun. **3**, 625 (2012).

38 E. Schrödinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).

39 S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, Phys. Rev. A **87**, 022104 (2013).

40 V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

41 J. I. de Vicente, J. Phys. A: Math. Theor. **47**, 424017 (2014).

42 G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).

43 H. M. Wiseman, S. J. Jones and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

44 B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. Wiseman, R. Ursin, A. Zeilinger, New J. Phys. **14**, 053030 (2012).

How Many Quantum Correlations Are Not Local?*

Carlos E. González-Guillén[1], C. Hugo Jiménez[2], Carlos Palazuelos[3], and Ignacio Villanueva[4]

1 **Departamento de Matemáticas del Área Industrial, E.T.S.I. Industriales, UPM, 28006 Madrid, Spain;**
Department of Mathematics and Statistics, University of Ottawa, K1N6N5 Ottawa, ON – Canada
carlos.gguillen@upm.es

2 **Departamento de Matemática, Universidad Federal de Minas Gerais, 30161970 Belo Horizonte, MG – Brasil**
hugo@mat.ufmg.br

3 **Departamento de Análisis Matemático, UCM, 28040 Madrid, Spain;**
Instituto de Ciencias Matemáticas (ICMAT), 28049 Madrid, Spain
carlospalazuelos@ucm.es

4 **Departamento de Análisis Matemático and IMI, UCM, 28040 Madrid, Spain**
ignaciov@ucm.es

Abstract

We study how generic is the property of nonlocality among the set of quantum correlations for bipartite dichotomic measurements. To do so, we consider the characterization of these quantum correlations as those of the form $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$, where the vectors u_i and v_j are in the unit sphere of a real Hilbert space. The important parameters in this description are the number of vectors n and the dimension of the Hilbert space m. Thus, it is natural to study the probability of a quantum correlation being nonlocal as a function of $\alpha = \frac{m}{n}$, where the previous vectors are independent and uniformly distributed in the unit sphere of $\mathbb{R}^m$. In this situation, our main result shows the existence of two completely different regimes: There exists an $\alpha_0 > 0$ such that if $\alpha \leq \alpha_0$, then γ is nonlocal with probability tending to 1 as $n \to \infty$. On the other hand, if $\alpha \geq 2$ then γ is local with probability tending to 1 as $n \to \infty$.

1998 ACM Subject Classification H.1.1 Systems and Information Theory

Keywords and phrases nonlocality, quantum correlations, Bell inequalities, random matrices

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.39

1 Introduction

Local measurements performed by two spatially separated observers on entangled bipartite quantum states can lead to correlations which cannot be explained by Local Hidden Variable Models (LHVM) [7]. This phenomenon, known as *quantum nonlocality*, is one of the most relevant features of quantum mechanics. In fact, though initially discovered in the context of foundations of quantum mechanics, during the last decade quantum nonlocality has become a crucial resource in many applications; some of them are quantum cryptography ([1], [2], [17]), communication complexity ([8]) and random number generators ([15], [18]).

* This work was partially supported by Spanish projects MTM2011-26912, MTM2012-30748, MTM2014-54240-P, QUITEMAD+ and “Ramón y Cajal” program, Mexico’s National Council for Science and Technology postdoctoral grant 180486 and Canadian grants ER-09-06-172 and NSERC discovery grant RGPIN/341303-2010

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 39–47
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Both from the fundamental and the resource point of view, we are interested in quantifying quantum nonlocality. That is, somehow measuring "how much" nonlocality is available in a given situation. The most used tool to quantify nonlocality is the violation of a Bell inequality, and by now there is an abundance of results quantifying the maximum possible violation in a large variety of contexts.

Another important point of view when quantifying a given resource is not only to look at the extremal cases (that is, the maximal violations) but at the "typical" cases. That is, we would like to know not only how much quantum nonlocality we have in certain extremal situations, but also how likely it is to find quantum nonlocality in a random situation.

This second problem is, so far, much less understood than the first. One of the first steps in this direction is [3]. In there, the authors prove that for almost every randomly chosen (in a precisely defined way) XOR game, its quantum value will be strictly bigger than its local value. Put in another way, the result says that almost every such game will serve as a witness that certain quantum correlation is not local.

In this work we study the "dual problem": if we consider a random quantum correlation, how likely is it that it is nonlocal? We state next the definitions needed for a precise formulation of our question.

We will work in the context where two spatially separated observers, Alice and Bob, perform dichotomic (two-outcome) measurements on a bipartite quantum state ρ, each on their part of the system, and consider the correlations between their answers.

According to the postulates of quantum mechanics, a two-outcome measurement for Alice (resp. Bob) is given by $\{A^+, A^-\}$ (resp. $\{B^+, B^-\}$), where $A^\pm$ (resp. $B^\pm$) are projectors acting on a Hilbert space and summing to the identity. We define the observable corresponding to Alice's (Bob's) measurement as $A = A^+ - A^-$ ($B = B^+ - B^-$). The joint correlation of Alice's and Bob's measurement results, denoted by a and b respectively, is $\langle ab \rangle = tr(A \otimes B\rho)$. Motivated by this, we say that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a *quantum correlation matrix* and denote by $\gamma \in \mathcal{Q}$, if there exist a density matrix ρ acting on a tensor product of Hilbert spaces $H_1 \otimes H_2$ and two families of contractive self-adjoint operators $\{A_i\}_{i=1}^n$, $\{B_i\}_{i=1}^n$ acting on H_1 and H_2 respectively such that

$$\gamma_{i,j} = tr(A_i \otimes B_j \rho) \text{ for every } i, j = 1, \cdots, n. \tag{1}$$

That is, γ is a matrix whose entries are the correlations obtained in an Alice-Bob scenario where each of the observers can choose among n different possible dichotomic measurements. On the other hand, we say that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a *local correlation matrix* if it belongs to the convex hull of deterministic correlations. That is,

$$\mathcal{L} = conv\Big\{(\alpha_i\beta_j)_{i,j=1}^n, \alpha_i = \pm 1, \beta_j = \pm 1,\ i, j = 1, \cdots, n\Big\}. \tag{2}$$

Local correlation matrices are precisely those whose entries are the correlations obtained in an Alice-Bob scenario when the measurement procedure can be explained by means of a LHVM. It is well known ([16]) that $\mathcal{L}$ and $\mathcal{Q}$ are convex sets satisfying

$$\mathcal{L} \subsetneq \mathcal{Q} \subsetneq K_G\mathcal{L},$$

where $1.67696... \leq K_G \leq 1.78221...$ is the so called *Grothendieck's constant*. Indeed, the first strict inclusion exactly means that there exist quantum correlations which cannot be explained by means of a LHVM (what we have called quantum nonlocality above) while the second inclusion is a consequence of Grothendieck's inequality (see Theorem 5 below) and a result proved by Tsirelson ([16]) which states that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a quantum correlation matrix if and only if there exist a real Hilbert space H and unit vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ in H such that

$$\gamma_{i,j} = \langle u_i, v_j \rangle \text{ for every } i, j = 1, \cdots, n. \tag{3}$$

We want to choose now a probability distribution on the set of quantum correlations. It is not obvious how to do so. One may try to use expression (1) as a guide, and choose a probability distribution on the set of states ρ and on the set of families of self-adjoint and contractive operators $A_1, \cdots, A_n, B_1, \cdots, B_n$. But it is not obvious how to choose a natural candidate for this second probability distribution.

Instead of that, we look at the equivalent reformulation (3) of a quantum correlation. In this (more mathematical, less physical) expression, there is indeed a natural probability distribution: we can consider the vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ independently uniformly distributed on the unit sphere of $\mathbb{R}^m$. It is well known that this is exactly the same as considering independent normalized m-dimensional gaussian vectors. Due to the Central Limit Theorem, this last fact makes it likely that different physically realistic models yield probability distributions related to this one.

Our results will depend on the relation between the dimension m and the number of questions n. It is simple to see that if one fixes any finite m, the probability that a quantum correlation matrix γ sampled according to the previous procedure is nonlocal tends to one as n tends to infinity. It is also simple to see that if n is fixed and m tends to infinity, then the probability that γ is not local converges to 0. See [12] for details.

Remarkably, our main result says that in the "constant ratio regime", where the ratio $\alpha = \frac{m}{n}$ remains constant as n grows, both extreme cases are possible: γ will be almost surely local for α big enough, whereas γ will be almost surely non local for α small enough.

Specifically, the main result of our work can be condensed as:

▶ **Theorem 1.** *Let n and m be two natural numbers and $\alpha = \frac{m}{n}$. Let us consider $2n$ random vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ independent and uniformly distributed on the unit sphere of $\mathbb{R}^m$ and let us denote by $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$ the corresponding quantum correlation matrix.*

(a) *If $\alpha \leq \alpha_0 \approx 0.004$ then γ is nonlocal with probability tending to one as n tends to infinity.*

(b) *If $\alpha \geq 2$, then γ is local with probability tending to one as n tends to infinity.*

This result shows clearly the need of studying the problem as a function of the parameter $\alpha = \frac{m}{n}$. One possible way to think of this problem is the following: say that we want to sample our vectors on a space of large dimension m. In that case, how many vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ will we need to sample in order to have nonlocality with high probability? Our results show that $n = \frac{m}{2}$ will be too few vectors, whereas $n = \frac{m}{\alpha_0}$ will be enough.

Curiously enough, we will see below that if one considers normalized vectors whose entries are independent Bernoulli variables, the probability of obtaining a nonlocal correlation matrix is zero, since all of them will be local. This means that, in contrast to many other contexts in random matrix theory, considering gaussian and Bernouilli random variables in our problem leads to completely different conclusions.

The probability distribution we consider on the random correlations arises from a mostly mathematical point of view. Despite that, in Section 5 we show a physical model which yields that same probability distribution.

The paper is organized as follows: In Section 2 we introduce some basic results that will illustrate the technics used along the whole paper. The main theorem is divided in two parts, as each of them requires quite different techniques. The precise statement and a sketch of the proof of part a) of the theorem, based on results from random matrix theory, is given in Section 3, while Section 4 states precisely part b) and sketches its proof. Here, the main tools are tensor norms in Banach space theory. In Section 5 we will discuss a physical interpretation of the probability distribution we consider on the set of quantum correlations. The conclusions of our work and future lines of research appear in Section 6.

2 Preliminary results

In this section we state some of the known, or essentially known, previous results which we will need along the paper.

The following proposition can be easily deduced from [9, Lemma 2.2].

▶ **Proposition 2.** *Let $\mathcal{G}_n$ be the gaussian measure on $\mathbb{R}^n$ and let $L \subset \mathbb{R}^n$ be a k-dimensional subspace. For a vector $g = (g_1, \cdots, g_n) \in \mathbb{R}^n$, let $\bar{g} = \frac{g}{\|g\|}$ and let $P_L(\bar{g})$ denote the orthogonal projection of $\bar{g}$ onto L. Then, for any $0 < \rho < 1$ we have*

$$\mathcal{G}_n\left((g_1, \cdots, g_n) \in \mathbb{R}^n : \quad \|P_L(\bar{g})\| \geq \frac{1}{1-\rho}\sqrt{\frac{k}{n}}\right) \leq e^{-\frac{\rho^2 k}{4}},$$

and

$$\mathcal{G}_n\left((g_1, \cdots, g_n) \in \mathbb{R}^n : \quad \|P_L(\bar{g})\| \leq (1-\rho)\sqrt{\frac{k}{n}}\right) \leq e^{-\frac{\rho^2 k}{4}}.$$

▶ Remark. As we already mentioned in the Introduction, it is completely equivalent to sample a unit vector $u \in S^{n-1}$ according to the uniform measure on the sphere μ_n to sample normalized gaussian vectors $g = \frac{1}{\|(g_1, \cdots, g_n)\|}(g_1, \cdots, g_n)$. That is, both probability distributions are exactly the same (see [6, Section 3.3] for a more complete explanation). In particular, Proposition 2 implies an analoguous statement for unitary vectors and Theorem 1 can be equivalently stated as in Theorem 6 and Theorem 9.

We say that a real random $n \times n$ matrix M is bi-orthogonally invariant if the distribution on $M_n(\mathbb{R})$ of M is equal to that of $O_1 M O_2$ for any orthogonal matrices O_1 and O_2. It is well known and easy to check that gaussian matrices are bi-orthogonally invariant.

The following result is well known, but we have not found a reference for it. It is not difficult to write a proof following the ideas of [13, Lemma 4.3.10].

▶ **Proposition 3.** *Let $A \in M_n(\mathbb{R})$ be an $n \times n$ random matrix in some probability space $(\Xi, \mathbb{P})$. If A is bi-orthogonally invariant then there exist random matrices U and V in $(\Xi, \mathbb{P})$ such that*

(i) *U, V follow the Haar distribution in the orthogonal group $\mathcal{O}(n)$.*

(ii) *U and V are independent.*

(iii) *U and V are the matrices whose columns are respectively the left and right singular vectors associated to the ordered singular values of A.*

▶ Remark. We will use later the following easy consequence of Proposition 3: For every $n \in \mathbb{N}$ there exists a probability space Ξ with three $n \times n$ random matrices A, U, V defined on it such that A is a gaussian matrix, U, V are independent and Haar distributed in $\mathcal{O}(n)$, and for almost every $\xi \in \Xi$, $U(\xi)$ and $V(\xi)$ are the right and left singular values of $A(\xi)$ arranged in decreasing order of the singular values.

We will need the Marcenko-Pastur law, describing the distribution of the singular values of random matrices:

▶ **Theorem 4** (Marcenko-Pastur law, [14]). *Let A be an $n \times n$ random matrix whose entries a_{ij} are independent real random variables with mean 0 and variance 1. Let $C \in [0,2]$. With probability $1-o(1)$, the number of singular values λ of A that satisfy $\lambda \geq C\sqrt{n}$ is $(f(C)-o(1))n$ where*

$$f(C) = \frac{1}{2\pi}\int_{x=C^2}^{4}\sqrt{\frac{4}{x}-1}dx.$$

Here, we say that $h = h(n)$ is $o(1)$ if and only if $\lim_{n\to\infty} h(n) = 0$.

Finally, we state the version of Grothendieck's inequality most useful for our purposes (see [10, Page 172]).

▶ **Theorem 5** (Grothendieck's inequality). *There exists a universal constant K_G, such that for every natural number n and for every real matrix $(a_{i,j})_{i,j=1}^n$ we have*

$$\sup\Big\{\Big|\sum_{i,j=1}^n a_{i,j}\langle x_i, y_j\rangle\Big| : x_i, y_j \in B_H\Big\} \leq K_G \sup\Big\{\Big|\sum_{i,j=1}^n a_{i,j}s_it_j\Big| : s_i, t_j = \pm 1\Big\},$$

where the first supremum runs over elements $x_1, \cdots, x_n, y_1, \cdots, y_n$ in the unit ball of a real Hilbert space H.

The exact value of K_G is still unknown but it is known that $1.67696... \leq K_G \leq 1.78221...$.

3 A lower bound for α_0: Part (a) of Theorem 1

The precise statement for the lower bound is the following.

▶ **Theorem 6.** *Let $G = (g_{i,j})_{i,j=1}^{n,m}$ and $H = (h_{i,j})_{i,j=1}^{n,m}$ be two random matrices whose entries are independent real normalized gaussian variables satisfying $\alpha = \frac{m}{n} \in (0,1)$. For every $i, j = 1, \cdots, n$, let $g_i = (g_{i,k})_{k=1}^m$ and $h_j = (h_{j,k})_{k=1}^m$ be the row vectors of G and H respectively . Let us denote $\bar{g}_i = \frac{g_i}{\|g_i\|}$ and $\bar{h}_j = \frac{h_j}{\|h_j\|}$. Then, if $\alpha \leq \alpha_0 \approx 0.004$, the quantum correlation matrix given by $\gamma = (\langle \bar{g}_i | \bar{h}_j\rangle)_{i,j=1}^n$is not local with probability $1-o(1)$.*

The starting point for its proof is the following result, which can be deduced from [3] and the Remark following Proposition 3. It provides an abundance of quantum nonlocal correlations when we consider the dot product of normalized truncations of orthonormal vectors.

▶ **Proposition 7.** *Let $U = (u_{i,j})_{i,j=1}^n, V = (v_{i,j})_{i,j=1}^n$ be two independent orthogonal random matrices distributed according to the Haar measure on the orthogonal group $\mathcal{O}(n)$. Let $\alpha \in (0,1)$ and $m = \alpha n$. We also denote $\delta = f^{-1}(\alpha)$, where f is the Marcenko-Pastur densitiy function as in Theorem 4. Let $\gamma_{i,j} = \langle \frac{\sqrt{n}}{\sqrt{m}}u_i, \frac{\sqrt{n}}{\sqrt{m}}v_j\rangle$ with $u_i = (u_{i,k})_{k=1}^m$ $v_j = (v_{j,k})_{k=1}^m$. Then there exists an $n \times n$ matrix $A = (a_{i,j})_{i,j=1}^n$ such that, with probability $1-o(1)$,*

$$\sum_{i,j=1}^n a_{i,j}\gamma_{i,j} \geq (\delta - o(1))n^{\frac{3}{2}} \quad \textit{and} \quad \omega(A) \leq 1.6651\ldots n^{\frac{3}{2}}.$$

The previous proposition implies that for certain range of $\alpha = \frac{m}{n}$, the first m properly normalized columns of two Haar distributed orthogonal matrices generate a nonlocal quantum correlation with high probability. It also provides a gaussian matrix A that certifies this nonlocality. Note that the vectors $\{u_i\}_i$ (resp. $\{v_j\}_j$) are dependent of each other as they are part of an orthogonal matrix. On the contrary, the vectors that we use to generate our correlation matrix are independent from each other.

Now, we want to approximate this columns in the appropriate norm with the corresponding columns of gaussian matrices. This is achieved with the following result from [11]. Its proof, quite technical, is based on an analysis of the Gram-Schmidt orthonormalization process and a careful use of the concentration of measure phenomenon, where Proposition 2 and similar estimates are used repeatedly.

▶ **Theorem 8** ([11, Theorem 1.1]). *Let n and m be two natural numbers such that $\alpha = \frac{m}{n} \in (0,1)$. Then, there exist matrices $Y_n = (y_{i,j})_{i,j=1}^n$ and $U_n = (u_{ij})_{i,j=1}^n$ whose $2n^2$ entries are real random variables defined on the same probability space Ξ such that*

(i) *$\{y_{i,j}; 1 \leq i,j \leq n\}$ are independent normalized random gaussian variables,*

(ii) *U_n is an orthogonal matrix distributed according to the Haar measure,*

(iii) *If we set $F_i^m(Y_n - \sqrt{n}U_n)$ the i-th row of the matrix $Y_n - \sqrt{n}U_n$ truncated to its first m entries, we have*

$$\mathbb{P}_\Xi\Big(\sup_{i=1,\cdots,n} \big\|F_i^m(Y_n - \sqrt{n}U_n)\big\| > (1+\epsilon)\theta(\alpha)\sqrt{m}\Big) \leq Kne^{C(\epsilon,\alpha)n},$$

where here K is a universal positive constant, $C(\epsilon,\alpha) > 0$ is a constant depending only on ϵ and α and

$$\theta(\alpha) = \sqrt{2 - \frac{4}{3}\frac{(1-(1-\alpha)^{3/2})}{\alpha}}.$$

Finally, Grothendieck's inequality allows us to translate this euclidean approximation between gaussian and orthonormal vectors into a big value of the correlation γ when tested against the witness A. Details can be seen in [12].

To finish this section we mention that if we consider normalized vectors u_i and v_j whose entries are independent Bernoulli variables (rather than gaussian) then we obtain local correlations with probability one. Indeed, if we consider such vectors $u_i = \frac{1}{\sqrt{m}}(\epsilon_1^i, \cdots, \epsilon_m^i)$, $v_j = \frac{1}{\sqrt{m}}(\delta_1^j, \cdots, \delta_m^j)$, we obtain that

$$(\gamma_{i,j})_{i,j=1}^n = \Big(\frac{1}{m}\sum_{k=1}^m \epsilon_k^i \delta_k^j\Big)_{i,j=1}^n.$$

However, for a fixed k, we have that $(\gamma_{i,j}^k)_{i,j=1}^n = \big(\epsilon_k^i \delta_k^j\big)_{i,j=1}^n$ is a deterministic (so local) correlation. Since $(\gamma_{i,j})_{i,j=1}^n$ is written as a convex combination of these objects, we immediately conclude that $(\gamma_{i,j})_{i,j=1}^n$ is a local correlation.

4 An upper bound for α: Part (b) of Theorem 1

The precise statement for the upper bound is the following.

▶ **Theorem 9.** *Let $G = (g_{i,j})_{i,j=1}^{n,m}$ and $H = (h_{i,j})_{i,j=1}^{n,m}$ be two random matrices whose entries are independent real normalized gaussian variables and let $\alpha = \frac{m}{n}$. For every $i,j = 1,\cdots,n$, let $g_i = (g_{i,k})_{k=1}^m$ and $h_j = (h_{j,k})_{k=1}^m$ be the row vectors of G and H respectively . Let us denote $\bar{g}_i = \frac{g_i}{\|g_i\|}$ and $\bar{h}_j = \frac{h_j}{\|h_j\|}$. Then, if $\alpha \geq 2$, the quantum correlation matrix given by $\gamma = (\langle \bar{g}_i | \bar{h}_j \rangle)_{i,j=1}^n$is local with probability larger than $1 - 2ne^{C(\alpha)n}$. Here, $C(\alpha) \in (0,1)$ is a constant depending only on α.*

The proof of Theorem 9 relies on elements from Banach space theory: Given an $n \times n$ matrix with real entries $\Gamma = (\gamma_{i,j})_{i,j=1}^n$, we can regard this matrix as a tensor $\Gamma = \sum_{i,j=1}^n \gamma_{i,j} e_i \otimes e_j \in \mathbb{R}^n \otimes \mathbb{R}^n$. It will be convenient for us to introduce two tensor norms in this space. We define

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} = \inf\Big\{\sum_{k=1}^N \|x_i\|_\infty \|y_i\|_\infty : \Gamma = \sum_{i=1}^N x_i \otimes y_i\Big\},$$

where in this definition, given a vector $z \in \mathbb{R}^n$, we denote $\|z\|_\infty = \max_{i=1,\cdots,n} |z_i|$. This norm is the projective tensor norm on $\ell_\infty^n \otimes \ell_\infty^n$ and it can be equivalently defined (see [10, Chapter 3]) as

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} = \inf\Big\{\sum_{k=1}^N \lambda_k : \lambda_k \geq 0, \Gamma = \sum_{k=1}^N \lambda_k \eta_k\Big\},$$

where here η_k denotes the matrix associated to a deterministic (so local) correlation. That is, for every k we have that $\eta_k = a_k \otimes b_k$ for certain sign vectors $a_k, b_k \in \mathbb{R}^n$.

▶ Remark. It is now clear why we are interested in this norm: For a given matrix A, we trivially have that

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} \leq 1 \text{ if and only if } \Gamma \text{ is local (as a correlation matrix).}$$

On the other hand, we can define another tensor norm by

$$\|\Gamma\|_{\ell_\infty^n(\ell_2^n)} = \max_{i=1,\cdots,n} \|(\gamma_{i,j})_{j=1}^n\|.$$

The following result is the starting point of our proof of Theorem 9. It is a reformulation of the fact, well known in Banach space theory, that $\pi_1(id : \ell_1^n \to \ell_2^n) \leq \sqrt{2}$, where π_1 denotes the 1-summing norm (see for instance [10, Ex 11.5]).

▶ **Theorem 10.** *Given an $n \times n$ matrix with real entries $\Gamma = (\gamma_{i,j})_{i,j=1}^n$, we have that*

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} \leq \sqrt{2}\|\Gamma\|_{\ell_\infty^n(\ell_2^n)}.$$

To prove now Theorem 9, we use concentration of measure results to show that, with our hypothesis, $\|\Gamma\|_{\ell_\infty^n(\ell_2^n)} \leq \frac{1}{\sqrt{2}}$ with exponentially high probability. Details can be seen in [12].

5 A physical interpretation of the result

As we have said before, we consider the correlations arising from randomly uniformly distributed unit vectors as in (3). In principle, this is not a physical procedure. Nevertheless, Tsirelson proved in a constructive way that all matrices given by (3) are quantum correlations. In particular, the following result holds.

▶ **Theorem 11** ([16]). *Let $u_i = (u_{ik})_{k=1}^m, v_l = (v_{jl})_{l=1}^m \in \mathbb{R}^m$ be unit vectors. Let $\gamma = (\langle u_i, v_j\rangle)_{i,j=1}^n$. Let $X_1, \cdots, X_m : H_r \to H_r$ be m Hermitian operators, such that $X_k X_l = -X_l X_k$ if $l \neq k$ and $X_k^2 = \mathbb{1}$, where H_r is an r-dimensional Hilbert space. Then, for every $1 \leq i, j \leq n$,*

$$A_i = \sum_{k=1}^m u_{ik} X_k \text{ and } B_j = \sum_{l=1}^m v_{jl} X_l$$

are Hermitian operators of norm one and

$$\gamma_{i,j} = \langle\psi| A_i \otimes B_j |\psi\rangle,$$

where $|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{s=1}^r |ss\rangle \in H_r \otimes H_r$.

Thus, given a Hilbert space H_r and operators $X_1, \cdots, X_m$ fulfilling the conditions from Theorem 11, the random correlation we are considering can be obtained physically by considering the maximally entangled state $|\psi\rangle \in H_r \otimes H_r$ and observables $\{A_i\}_i$, $\{B_j\}_j$ which are independent random linear combinations of the anticommuting observables $X_1, \cdots, X_m$.

It is known that the smallest r, so that operators $X_1, \cdots, X_m$ as above exist in H_r, is $r = 2^{[(m+1)/2]}$ (see [16]). In this case a particular choice of these operators for even m is:

$$X_{2i-1} = X \otimes \overset{i-1}{\cdots} \otimes X \otimes Y \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \quad \text{for every } i = 1, \cdots, m/2;$$
$$X_{2i} = X \otimes \overset{i-1}{\cdots} \otimes X \otimes Z \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \quad \text{for every } i = 1, \cdots, m/2,$$

where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are the Pauli matrices.

That is, with this particular choice of $X_1, \cdots, X_m$, we can physically generate quantum correlations with our probability distribution by imposing the associated probability distribution on those Pauli product measurements and measuring the maximally entangled state.

Those measurements are closely related to the measurements considered in [19], but note that in our case we increase the dimension, where in [19] the increasing parameter is the number of parties.

The main caveat to our model presented above is that it requires the physical dimension of the system to be exponential in the mathematical dimension m. We expect that there exist physical systems of much smaller dimension that give rise to quantum correlations distributed similarly to the ones we have consider, so that our techniques will apply.

6 Conclusions and future lines of research

We initiate the study of the probability of finding nonlocality among quantum probability distributions. The dual situation, studying the probability of finding games for which quantumness is an advantage over local resources, was initiated in [3].

We consider the simplest case, quantum correlations arising from bipartite dichotomic measurements. In this setting, quantum correlations can be written as the product $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$ of unit vectors u_i, v_j of an m-dimensional real Hilbert space H.

In this set we consider the probability distribution in the quantum correlations induced by considering the unit vectors $u_1, \ldots, u_n, v_1, \ldots, v_n$ independently uniformly distributed in the unit sphere of $\mathbb{R}^m$. This is equivalent to consider these vectors as independent normalized gaussian vectors.

We study the situation where both m and n grow to infinity with the ratio $\alpha = \frac{m}{n}$ constant.

Our main result says that in this setting two extreme situations can happen: if α is small enough (smaller than certain $\alpha_0 \approx 0.004$) then almost every such quantum correlation will be non local. But if α is big enough (greater than 2), then almost every such correlation will be local.

The tools needed to prove the first bound are random matrix theory and concentration of measure. For the second bound, the main tool are tensor norms in Banach space theory.

So far, we do not know what happens when $\alpha_0 < \alpha < 2$. In particular, we do not know if a sharp threshold behaviour between both regimes exists or not. Our techniques maybe can be refined to slightly increase the bound α_0, but they will never reach the relevant case $\alpha_0 = 1$. From the other side, our proof of part b) suggests that a more clever argument could lead to replace 2 by K_G, but again our present approach does not seem to allow for further improvement. Along these lines, it is plausible that a relation between α and K_G describes interesting behaviors of our correlation matrices.

We provide a physical model which gives rise to our probability distribution, but it requires of an exponential (in m) physical dimension. We expect that relevant physical models of lower dimension will give rise to probability distributions close enough to ours, so that related reasonings will apply. This line of research is also open.

Until now we have only addressed the study of bipartite dichotomic quantum correlations. The study of the full probability distribution for two or more parties, or the study of N-partite dichotomic quantum correlations is totally open.

References

1 A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Phys. Rev. Lett. 98, 230501 (2007).

2 A. Acín, N. Gisin, and L. Masanes, *From Bell's Theorem to Secure Quantum Key Distribution*, Phys. Rev. Lett. 97, 120405 (2006).

3 A. Ambainis, A. Backurs, K. Balodis, D. Kravcenko, R. Ozols, J. Smotrovs, M. Virza, *Quantum strategies are better than classical in almost any XOR game*, Automata, Languages, and Programming Lecture Notes in Computer Science Volume 7391, 2012, 25–37.

4 A. Aspect, *Bell's inequality test: more ideal than ever*, Nature 398, 189–190 (1999).

5 A. Aspect, P. Grangier and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. 47, 460 (1981).

6 A. Barvinok, *Measure Concentration. Math 710 Lecture Notes*, Department of Mathematics, University of Michigan (2005).

7 J. S. Bell, *On the einstein-podolsky-rosen paradox*, Physics 1, 195–200 (1964).

8 H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Nonlocality and communication complexity*, Rev. Mod. Phys. 82, 665 (2010).

9 S. Dasgupta, A. Gupta, *An elementary proof of a theorem of Johnson and Lindenstrauss*, Random Struct. Alg. 22(1), 60–65 (2003).

10 A. Defant and K. Floret, *Tensor Norms and Operator Ideals*, North-Holland, (1993).

11 C. E. González-Guillén, C. Palazuelos, I. Villanueva, *Euclidean distance between Haar orthogonal and gaussian matrices.* arXiv:1412.3743.

12 C. E. González-Guillén, C. H. Jimenez, C. Palazuelos, I. Villanueva, *Sampling quantum nonlocal correlations with high probability.* arXiv:1412.4010.

13 F. Hiai and D. Petz, *The semicircle law, free random variables and entropy*, American Mathematical Society Providence, (2000).

14 V. A. Marcenko, L. A. Pastur, *Distribution of eigenvalues for some sets of random matrices*, Math. USSR Sbornik, 1:457–483, (1967).

15 S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, *Random numbers certified by Bell's theorem*, Nature (London) 464, 1021 (2010).

16 B. S. Tsirelson, *Some results and problems on quantum Bell-type inequalities*, Hadronic J. Supp. 8(4), 329–345 (1993).

17 U. Vazirani, T. Vidick, *Fully device-independent quantum key distribution*, available in arXiv:1210.1810 (2012).

18 U. Vazirani, T. Vidick, *Certifiable quantum dice – Or, exponential randomness expansion*, Phil. Trans. R. Soc. A, 370, 3432–3448 (2012).

19 J. J. Wallman, Y.-C. Liang, S. D. Bartlett, *Generating nonclassical correlations without fully aligning measurements*, Phys. Rev. A 83, 022110 (2011).

The Spin-2 AKLT State on the Square Lattice is Universal for Measurement-based Quantum Computation*

Tzu-Chieh Wei[1] **and Robert Raussendorf**[2]

1 **C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy**
State University of New York at Stony Brook, Stony Brook, NY 11794-3840, USA
`tzu-chieh.wei@stonybrook.edu`

2 **Department of Physics and Astronomy, University of British Columbia**
Vancouver, British Columbia, V6T 1Z1, Canada
`rrausen@phas.ubc.ca`

Abstract

One-way quantum computation was first invented using the cluster state. Since then graph states, the generalization of the cluster state, were investigated and understood when they would enable such a measurement-based approach for quantum computation. Are there any other family of states, i.e., states with different entanglement structures, that can also serve as the universal resource for quantum computation? Recent study shows that the Affleck-Kennedy-Lieb-Tasaki (AKLT) states also provide a useful source. Here, we show that the spin-2 state on the square lattice is a universal resource for measurement-based quantum computation. We employ a POVM on all sites that convert the local 5-level system to 2-level, and the post-POVM state is a graph state, whose graph is in general non-planar. We then follow with another round of measurement to recover the planarity of the graphs by thinning. The resultant typical graphs are shown to reside in the supercritical phase of percolation via Monte Carlo simulations and the associated graph states are universal, implying the AKLT state is also universal.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Measurement-based quantum computation, AKLT state, graph state, percolation

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.48

1 Introduction and motivation

Universal quantum computation can be achieved by using local measurements on certain entangled states, such as the cluster state. This measurement-based model of quantum computation (MBQC) [13, 1, 14] provides equivalent power of computation as the standard circuit model. However, not all entangled states can provide the capability for driving a universal quantum computation. A complete classification of entanglement that enables MBQC remains a challenging open question. The quest for more universal resource states will advance our knowledge towards the essential type of entanglement. The family of cluster states or more generally graph states contains abundance supply of resource states. These

* This work was partially supported by NSF, NSERC, Cifar and PIMS.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 48–63
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

states, however, cannot be unique ground states of two-body interacting Hamiltonians [12]. Beyond this family of states, only a handful of other entangled states are known to be universal [6, 3, 2, 10].

Here, we demonstrate that the spin-2 Affleck-Kennedy-Lieb-Tasaki (AKLT) state on the square lattice is a universal resource for measurement-based quantum computation (MBQC). This question has been open since the universality of the spin-3/2 AKLT state on the honeycomb lattice was established [16, 11]. AKLT states can be defined on any graph and are unique ground states of two-body interacting Hamiltonians with suitable boundary conditions. But the quantum computational universality in this family is less explored than the family of cluster or graph states. Together with the results here, the emerging picture from a series of study on the quantum computational universality in the AKLT valence-bond family is as follows [16, 11, 17, 15, 18]. AKLT states involving spin-2 and other lower spin entities are universal if they reside on a frustration-free lattice with any combination of spin-2, spin-3/2, spin-1 and spin-1/2 (consistent with the lattice). Additionally, a frustrated lattice can always be decorated (by adding additional spins) such that the resultant AKLT state is universal.

2 Overall strategy

Our goal is to show that any quantum computation that is efficiently implemented in the circuit model can also be implemented efficiently by a sequence of adaptive local measurements on a spin-2 AKLT state. In other words, we want to show that the spin-2 AKLT state is a universal resource for MBQC.

The overall strategy for demonstrating this is: (1) we need to find a POVM that converts a 5-level state to a 2-level state; (2) we show that the post-POVM state is a graph state; (3) if this graph state has a planar graph then we check whether the graph is percolated; if the graph is non-planar, we need to restore planarity by apply futher active local measurement.

However, it is not guaranteed that the POVM will convert the AKLT state a qubit graph state. Fortunately, the POVM we found in Eq. (1) below allows us to do this. The graphs associated with the post-POVM states are generally not planar and we indeed need to apply some procedure to restore planarity at the cost of measuring and disentangling more qubits. In order to show that the typical graphs are percolated, we need to sample from the exact distribution. For this we manage to prove an exact weight formula for any given POVM outcome, and this allows us to perform Monte Carlo simulations. The most pronounced difference between the spin-3/2 and spin-2 probability weights is that for spin 3/2 all possible combinations of POVM outcomes do indeed occur with non-zero probability (except when the lattice is not bi-colorable) whereas, for the spin-2 case, certain combinations of POVM outcomes do not occur, i.e., have probability zero.

Why our work is interesting? We investigate how particular condensed-matter spin systems (the AKLT family) can be exploited for quantum computation. The framework is the so-called measurement-based quantum computation, one of several experimentally pursued approaches for realizing a quantum computer, which uses entanglement as a resource. Proving a general state can be useful in measurement-based quantum computation remains a theoretical challenge. Our present manuscript represents a significant advancement since our paper in 2011 [16], and together with our other recent works, gives a comprehensive understanding of why some generic states in the so-called AKLT family are useful. AKLT states are important from many perspectives: strong evidence for Haldane's conjecture, precursor of

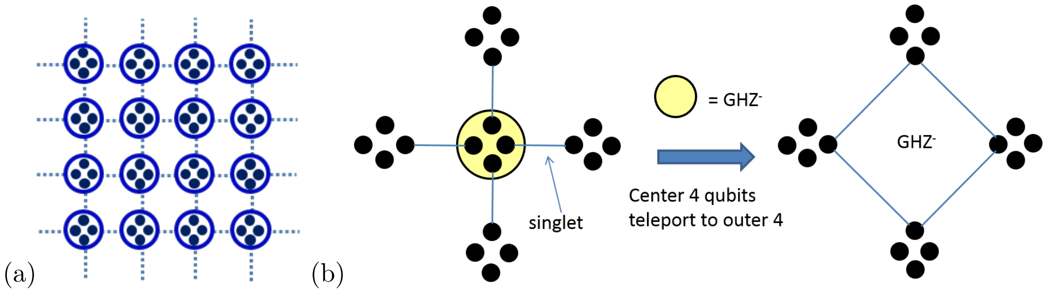


Figure 1 (a) AKLT state. Spin singlets $|\phi\rangle_e = (|01\rangle - |10\rangle)/\sqrt{2}$ of two virtual spins 1/2 are located on the edges of the square lattice. A projection at each lattice site onto the symmetric subspace of four virtual spins creates the AKLT state. (b) Teleportation. A perspective of the action of the POVM K_α in Eq. (1).

the so-called matrix product states and tensor product states (which have been developed to useful numerical tools), examples of symmetry-protected topological ordered states, and with our contribution, quantum computation, etc. We believe our paper is of interest to researchers in various fields, including condensed-matter physics, quantum information and computation, AMO physics (as possible implementation and indeed a proof-of-principle demonstration on 1D AKLT quantum computation was done with entangled photons [8]), statistical mechanics (given some of the techniques we used), and mathematics (such as random graph and probability theory).

3 Reduction from AKLT states to graph states

Let us define the AKLT state on the square lattice. It is useful to view the spin-2 particle on each site is consisting of four virtual qubits. Each virtual qubit forms a singlet state, $|\phi\rangle_e = (|01\rangle - |10\rangle)/\sqrt{2}$, with its corresponding virtual qubit on the neighboring site, with the singlets indicated by the dotted edges; see Fig. 1a. In order to convert the local 5-level system to 2-level, we shall use a POVM measurement below in Sec. 3.1. We shall see that regardless of the POVM outcome, the post-measurement state is a graph state, with its graph being modified from the original square lattice, more or less, randomly. However, the graph is not planar. But it is easier to understand such graphs as resulting from a two-step process: (1) a planar random graph from the square lattice is formed (which we prove in Sec. 3.2); then (2) certain Pauli measurements (due to some of the POVM elements) are then done to change the graph further (which we illustrate in Sec. 3.3).

3.1 Reduction from spin-2 entities to qubits: the generalized measurement

The POVM we shall employ consists of three rank-two elements and three additional rank-one elements [18]:

$$F_\alpha = \sqrt{\frac{2}{3}}\,(|S_\alpha\!=\!2\rangle\langle S_\alpha\!=\!2| + |S_\alpha\!=\!-2\rangle\langle S_\alpha\!=\!-2|),\quad K_\alpha = \sqrt{\frac{1}{3}}\,|\phi_\alpha^-\rangle\langle\phi_\alpha^-|, \tag{1}$$

where $\alpha = x, y, z$ and $|\phi_\alpha^\pm\rangle \equiv (|S_\alpha\!=\!2\rangle \pm |S_\alpha\!=\!-2\rangle)/\sqrt{2}$. The F's are straightforward generalization from the spin-3/2 case [16], but they do not give rise to the completeness relation, which is required for conservation of probabilities. By adding K's, it can be verified that the completeness relation is satisfied: $\sum_\alpha F_\alpha^\dagger F_\alpha + \sum_\alpha K_\alpha^\dagger K_\alpha = I$.

Expressed in terms of the four virtual qubits representing a spin-2 particle, the above operators in the POVM are

$$F_x \quad = \sqrt{\tfrac{2}{3}}(|+^{\otimes 4}\rangle\langle +^{\otimes 4}| + |-^{\otimes 4}\rangle\langle -^{\otimes 4}|), \qquad K_x = \sqrt{\frac{1}{3}}|\mathrm{GHZ}_{\mathrm{x}}^-\rangle\langle \mathrm{GHZ}_{\mathrm{x}}^-|, \tag{2a}$$

$$F_y \quad = \sqrt{\tfrac{2}{3}}(|i^{\otimes 4}\rangle\langle i^{\otimes 4}| + |(\text{–}i)^{\otimes 4}\rangle\langle (\text{–}i)^{\otimes 4}|), \quad K_y = \sqrt{\frac{1}{3}}|\mathrm{GHZ}_{\mathrm{y}}^-\rangle\langle \mathrm{GHZ}_{\mathrm{y}}^-|, \tag{2b}$$

$$F_z \quad = \sqrt{\tfrac{2}{3}}(|0^{\otimes 4}\rangle\langle 0^{\otimes 4}| + |1^{\otimes 4}\rangle\langle 1^{\otimes 4}|), \qquad K_z = \sqrt{\frac{1}{3}}|\mathrm{GHZ}_{\mathrm{z}}^-\rangle\langle \mathrm{GHZ}_{\mathrm{z}}^-|, \tag{2c}$$

where $|\psi^{\otimes 4}\rangle$ is a short-hand notation for $|\psi, \psi, \psi, \psi\rangle$, equivalent to an eigenstate $|S_\alpha\rangle$ of the spin-2 operator in either $\alpha =$ x, y, or z direction. The first three elements are similar to those in spin-3/2 sites, except the number of virtual qubits being four, and correspond to good outcomes of type x, y and z, respectively. Associated with the last three elements, $|\mathrm{GHZ}_{\mathrm{z}}^-\rangle \equiv (|0000\rangle - |1111\rangle)/\sqrt{2}$, $|\mathrm{GHZ}_{\mathrm{x}}^-\rangle \equiv (|++++\rangle - |----\rangle)/\sqrt{2}$, and $|\mathrm{GHZ}_{\mathrm{y}}^-\rangle \equiv (|\mathrm{i},\mathrm{i},\mathrm{i},\mathrm{i}\rangle - |-\mathrm{i},\text{–}\mathrm{i},\text{–}\mathrm{i},\text{–}\mathrm{i}\rangle)/\sqrt{2}$ are the corresponding states and they will be regarded as unwanted outcomes of type x, y, and z, respectively. The effect of these GHZ outcomes is that the neighboring four virtual qubits connected to the center site becomes GHZ entangled, as illustrated in Fig. 1b. It is these GHZ entanglement in the virtual qubits that complicates the measurement-based quantum computation. The reduced density matrix for a single site of the AKLT state is a completely mixed state, and therefore, each unwanted type occurs on average with a probability 1/15. An unwanted outcome associated with K thus occurs with probability $p_{\mathrm{err}} = 3 \times 1/15 = 1/5$. However, as we shall see below in Sec. 5 that not all POVM outcomes associated with sets of $\{F_{\alpha(v)}, K_{\beta(w)}\}$ occur with non-zero probability, due to the correlation present in the AKLT state.

We note that K_α can be rewritten as follows,

$$K_\alpha = \sqrt{1/2}|\phi_\alpha^-\rangle\langle\phi_\alpha^-|F_\alpha = \sqrt{2/3}\,K_\alpha F_\alpha. \tag{3}$$

We can thus think of the POVM Eq. (1) as a two-stage process: (i) first the outcomes on all sites are F's, and (ii) then a number of sites are flipped to K or equivalently a projective measurement is done in the basis $|\phi_\alpha^\pm\rangle$ and the result $|\phi_\alpha^-\rangle$ is post-selected.

Corresponding to step (i), we show in the next section that the post-measurement state

$$\overline{|G_0(\{F\})\rangle} \sim \bigotimes_{v\in\mathcal{L}} F_{\alpha(v)}|\psi_{\mathrm{AKLT}}\rangle \tag{4}$$

is an encoded graph state [16, 17]. The 'bar' is used to indicate that the graph state is 'encoded', i.e., one logical qubit is formed by a few physical spins which we also can a *domain*. We shall omit the bar and write the state as $|G_0\rangle$ instead. In the section after that, we discuss the effect of K's, which is either simply shrinking the size of a domain or inducing a Pauli measurement.

3.2 The exact form of stabilizer generators

In this section we prove that $|G_0\rangle$ is a graph state by deriving the form of the stabilizer operators $\mathcal{K}_c$ for the domain labeled by $\mathcal{C}_c$. It includes all subtle plus and minus signs. The result is general for all states $|G_0\rangle \sim \bigotimes_{v\in\Omega} F_{\alpha_v,v}|\psi_{\mathrm{AKLT}}\rangle$, where F's can be of arbitrary spins. This was already considered in the case of the spin-3/2 AKLT state [16], but the argument used there applies more generally.

Let us first explain the notation. Consider a central vertex $\mathcal{C}_c \in V(G_0(\{F\}))$ and all its neighboring vertices $\mathcal{C}_\mu \in V(G_0)$; see e.g. Fig. 2 for illustration. Each vertex may contain

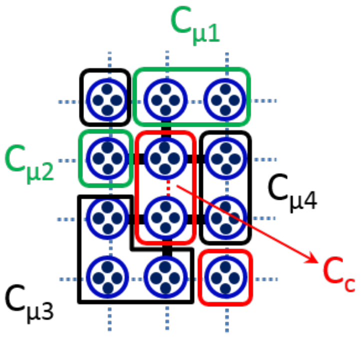


Figure 2 POVM outcomes. The center domain $\mathcal{C}_c$ has $a_c = x$ (red), and its neighboring domains: $\mathcal{C}_{\mu 1}$ and $\mathcal{C}_{\mu 2}$ have $a_{\mu 1} = a_{\mu 2} = y$ (green); $\mathcal{C}_{\mu 3}$ and $\mathcal{C}_{\mu 4}$ have $a_{\mu 3} = a_{\mu 4} = z$ (black).

multiple sites that are connected and are of the same POVM outcome F_α. We shall refer to these sites collectively as a *domain*. Namely, each vertex in graph G_0 is physically a domain. Denote the POVM outcome for all $\mathcal{L}$-sites $v \in \mathcal{C}_c, \mathcal{C}_\mu$ by a_c and a_μ, respectively. Denote by E_μ the set of $\mathcal{L}$-edges that run between $\mathcal{C}_c$ and $\mathcal{C}_\mu$. Denote by E_c the set of $\mathcal{L}$-edges internal to $\mathcal{C}_c$. Denote by C_c the set of all qubits in $\mathcal{C}_c$, and by C_μ the set of all qubits in $\mathcal{C}_\mu$. (Recall that there are 4 qubit locations per $\mathcal{L}$-vertex $v \in \mathcal{C}_c, \mathcal{C}_\mu$.) For any μ and any edge $e \in E_\mu$, let $u(e)$ $[v(e)]$ be the endpoint of e in C_μ $[C_c]$. Then, for all μ and all $e \in E_\mu$ the Pauli operators $-\sigma_{a_\mu}^{(u(e))}\sigma_{a_\mu}^{(v(e))}$ are in the stabilizer of the singlet $\bigotimes_{e\in E(\mathcal{L})} |\phi\rangle_e$.

Choose $b \in \{x, y, z\}$ such that $b \neq a_c$, and let, for any edge $e' \in E_c$, $v_1(e'), v_2(e') \in C_c$ be qubit locations such that $e' = (v_1(e'), v_2(e'))$. Then, for all $e' \in E_c$, $-\sigma_b^{(v_1(e'))}\sigma_b^{(v_2(e'))}$ is in the stabilizer of $\bigotimes_{e\in E(\mathcal{L})} |\phi\rangle_e$.

Thus we have the following operator as the stabilizer for $\bigotimes_{e\in E(\mathcal{L})} |\phi\rangle_e$,

$$\begin{aligned}\mathcal{K}_c &= \bigotimes_{\mu}\bigotimes_{e\in E_\mu} (-1)\sigma_{a_\mu}^{(u(e))}\sigma_{a_\mu}^{(v(e))} \bigotimes_{e'\in E_c} (-1)\sigma_b^{(v_1(e'))}\sigma_b^{(v_2(e'))} \\ &= (-1)^{|E_c|+\sum_\mu |E_\mu|} \bigotimes_{\mu}\bigotimes_{e\in E_\mu} \sigma_{a_\mu}^{(u(e))}\sigma_{a_\mu}^{(v(e))} \bigotimes_{e'\in E_c} \sigma_b^{(v_1(e'))}\sigma_b^{(v_2(e'))}.\end{aligned}$$

We now show that $O_{\mathcal{C}_c}$ commutes with the local POVMs and is therefore also in the stabilizer of $|\Psi(\mathcal{A})\rangle$. First, consider the central domain $\mathcal{C}_c$. The operator $O_{\mathcal{C}_c}$ acts non-trivially on every qubit in C_c, $O_{\mathcal{C}_c}|_l \neq I_l$ for all qubits $l \in C_c$. Furthermore, for all qubits $l \in C_c$, $O_{\mathcal{C}_c}|_l \neq \sigma_{a_c}^{(l)}$. Namely, if $l \in C_c$ is connected by an edge $e \in E_\mu$ to $\mathcal{C}_\mu$, for some μ, then $O_{\mathcal{C}_c}|_l = \sigma_{a_\mu}^{(l)} \neq \sigma_{a_c}^{(l)}$ (for all μ, $a_\mu \neq a_c$ by construction of $G(\mathcal{A})$). Or, if $l \in C_c$ is the endpoint of an internal edge $e' \in E_c$ then $O_{\mathcal{C}_c}|_l = \sigma_b^{(l)} \neq \sigma_{a_c}^{(l)}$ ($a_c \neq b$ by above choice). Therefore, for any $i, j \in C_c$, $O_{\mathcal{C}_c}$ anticommutes with $\sigma_{a_c}^{(i)}$ and $\sigma_{a_c}^{(j)}$, and thus commutes with all $\sigma_{a_c}^{(i)}\sigma_{a_c}^{(j)}$. Thus, $O_{\mathcal{C}_c}$ commutes with the local POVMs F_{a_c} in Eq. (2) on all $v \in \mathcal{C}_c$.

Second, consider the neighboring domains $\mathcal{C}_\mu$. $O_{\mathcal{C}_c}|_{\mathcal{C}_\mu} = \bigotimes_j \sigma_{a_\mu}^{(j)}$ by construction. $O_{\mathcal{C}_0}$ thus commutes with the local POVMs F_{v,a_μ} for all $v \in \mathcal{C}_\mu$ and for all μ.

To give explicit form of the stabilizer operators, we shall take the following convention for b as shown in Table 1. For POVM outcome $a_c = z$, we take $b = x$; for $a_c = x$, we take $b = z$; for $a_c = y$, we take $b = z$. With this choice we have

$$\mathcal{K}_c = (-1)^{|E_c|+\sum_\mu |E_\mu|} \bigotimes_{\mu} (\otimes_{e\in E_\mu} \lambda_{u(e)}) Z_\mu^{|E_\mu|} \bigotimes_{e\in E_\mu} \sigma_{a_\mu}^{v(e)}\sigma_b^{v(e)} X_c.$$

Table 1 The choice of b and $a_{\mu\neq b}$.

a_c	z	x	y
b	x	z	z
$a_{\mu\neq b}$	y	y	x

Table 2 The dependence of stabilizers and encodings on the local POVM outcome. $|\mathcal{C}|$ denotes the total number of sites contained in a domain $\mathcal{C}$ and $i,j = 1\,..\,4|\mathcal{C}|$ (as there are four vitural qubits in a site). The square lattice $\mathcal{L}$ is bi-partite and all sites can be divided into either A or B sublattice, $V(\mathcal{L}) = A\cup B$, and $\lambda_i = 1$ if the virtual qubit $i\in v\in A$ and $\lambda_i = -1$ if $i\in v'\in B$. This is due to the negative sign in the stabilizer generator for a singlet $|\phi\rangle_{ij}$, $(-\sigma_\mu^{[i]}\sigma_\mu^{[j]})|\phi\rangle_{ij} = |\phi\rangle_{ij}$ for an edge (i,j).

POVM outcome	z	x	y
stabilizer generator	$\lambda_i\lambda_j\sigma_z^{[i]}\sigma_z^{[j]}$,	$\lambda_i\lambda_j\sigma_x^{[i]}\sigma_x^{[j]}$	$\lambda_i\lambda_j\sigma_y^{[i]}\sigma_y^{[j]}$
$\overline{X}$	$\bigotimes_{j=1}^{4\lvert\mathcal{C}\rvert}\sigma_x^{[j]}$	$\bigotimes_{j=1}^{4\lvert\mathcal{C}\rvert}\sigma_z^{[j]}$	$\bigotimes_{j=1}^{4\lvert\mathcal{C}\rvert}\sigma_z^{[j]}$
$\overline{Z}$	$\lambda_i\sigma_z^{[i]}$	$\lambda_i\sigma_x^{[i]}$	$\lambda_i\sigma_y^{[i]}$

It is convenient to define $n_{\neq b} \equiv \sum_{\mu,a_\mu\neq b}|E_\mu|$. Then

$$\mathcal{K}_c \;=\; (-1)^{|E_c|+\sum_\mu |E_\mu|}\bigotimes_{\mu}(\otimes_{e\in E_\mu}\lambda_{u(e)})Z_\mu^{|E_\mu|}(\bigotimes_{a_\mu\neq b}\otimes_{e\in E_\mu}\lambda_{v(e)})Q_c, \tag{5}$$

where $Q_c = i^{n_{\neq b}}X_c$ if $n_{\neq b}$ is even and $Q_c = -i^{1+n_{\neq b}}(-1)^{\delta_{a_c,x}}Y_c$ if $n_{\neq b}$ is odd. This gives complete characterization of stabilizer generators, i.e., $Q_c = \pm X_c$ or $Q_c = \pm Y_c$ and the exact sign can be determined. This is essential in checking the incompatibility condition.

Note that the stabilizer operators are not always in the canonical form in which $\mathcal{K}_c|_c = X_c$, i.e., they can be $\pm X_c$ or $\pm Y_c$, but those non-central operators are always Z. But it is easy to find rotations (around logical z-axis) to make them canonical. We shall the basis after such rotations are made the canonical graph-state basis (CGSB).

A few remarks are in order.

1. Each domain on $\mathcal{L}$ supports a single encoded qubit, i.e., the domains $D\subset\mathcal{L}$ are the sites or vertices of the graph G_0, with the encoding as described in Table 2. The encoded qubits form a graph state $\overline{|G_0\rangle}$. When there is no confusion, we shall not distinguish between the graph state $|G_0\rangle$ and its encoded version $\overline{|G_0\rangle}$ and omit the labeling $\{F\}$.
2. The graph G_0 has an edge between the vertices $v(D)$ and $v(D')$, if the domains D and D' are connected by an odd number of edges in $\mathcal{L}$.
3. Be D a domain of type $T\in\{x,y,z\}$ with n_α neighbouring domains of type α. The stabilizer operators for such a graph state are shown in Eq. (5) in terms of encoded logical operators. They are characterized by the so-called stabilizer matrix, and in the case of graph state, is given via the adjacency matrix A_{G_0} of the graph G_0. It is seen that when

$$\begin{aligned} n_y &\mod 2 = 1, && \text{for } T = x,\\ n_x &\mod 2 = 1, && \text{for } T = y,\\ n_y &\mod 2 = 1, && \text{for } T = z, \end{aligned}$$

the stabilizer operator $\mathcal{K}_D$ has a logical Y operator at the support of D. This means that the graph G_0 has a self-loop attached to the domain D, i.e., $(A_{G_0})_{D,D} = 1$.

We recall the definition of a "domain". A domain is a maximal set of neighbouring sites in the lattice $\mathcal{L}$ for which the outcome of the POVM Eq. (1) is F_α or K_α [see Eq. (3)] with the same α. That is, there are domains of x, y and z-type, and neighbouring domains must be of different type. The self-loop is a convenient picture to visualize the graph. But we can perform local logical rotation to transform Y to X so as to remove the self-loop, then the resulting stabilizer operators will be in the canonical form. (Such rotation will also change the basis of logical measurement.) Moreover, we shall often not distinguish between an encoded $\overline{X}$ or $\overline{Y}$ operator from the corresponding X or Y operator, unless necessary.

3.3 POVM outcomes K_α: domain shrinking and logical Pauli measurements

We shall denote by $\{F, K\}$ the POVM outcomes on all sites, by $J_F \subset \mathcal{L}$ the set of sites where the POVM outcome is of F-type, and by $J_K = \mathcal{L}\backslash J_F$ the set of sites where POVM outcome is of K-type. Upon obtaining $\{F, K\}$ we can deduce the state $|G\rangle$ that the original AKLT state is transformed to,

$$|G(\{F,K\})\rangle = \left(\sqrt{\frac{1}{2}}\right)^{|J_K|} \bigotimes_{u\in J_K} |\phi^-_{\alpha(u)}\rangle\langle\phi^-_{\alpha(u)}| \bigotimes_{v\in\mathcal{L}} F_{\alpha(v)}|\psi_{\text{AKLT}}\rangle, \tag{6}$$

where the state is not normalized and the probability of the set of POVM outcomes $\{F, K\}$ occurs is

$$p(\{F,K\}) = \langle G(\{F,K\})|G(\{F,K\})\rangle. \tag{7}$$

We have shown that $|G_0\rangle$ is a graph state, and one can further show the normalization due to F's acting on the AKLT state [16],

$$\underset{u\in\mathcal{L}}{\otimes} F_{\alpha(u)}|\psi_{\text{AKLT}}\rangle = c_0 \left(\frac{1}{\sqrt{2}}\right)^{|\mathcal{E}|-|V|} |G_0\rangle, \tag{8}$$

where c_0 is an outcome-independent overall normalization, V is the set of domains, $\mathcal{E}$ is the set of inter-domain edges (before the modulo-2 operation) and $|G_0\rangle$ is properly normalized to have unit norm [16]. For the encoding using virtual-qubit picture, see Table 2.

Summarizing the above discussion, we have

$$|G(\{F,K\})\rangle = c_0 \left(\sqrt{\frac{1}{2}}\right)^{|\mathcal{E}|-|V|+|J_K|} \left(\bigotimes_{u\in J_K} |\phi^-_{\alpha(u)}\rangle\langle\phi^-_{\alpha(u)}|\right) |G_0(\{F\})\rangle, \tag{9}$$

where $|G_0(\{F\})\rangle$ is assumed to be properly normalized. Without the additional operators $\bigotimes_{u\in J_K} |\phi^-_{\alpha(u)}\rangle\langle\phi^-_{\alpha(u)}|$ the analysis of the computational universality would be the same as in the spin-3/2 case. It is these operators that complicate the situtation. However, as we shall see below their effect is not serious.

Then the effect of measuring in the basis $|\phi^\pm_\alpha\rangle$ corresponds to shrinking or thinning the domain, without affecting the entanglement of the domain with others. This can be understood from the following example. Suppose a two-site domain with $\alpha = x$: the basis states are $|S_x = +2\rangle_1|S_x = -2\rangle_2$ and $|S_x = -2\rangle_1|S_x = +2\rangle_2$, due to the POVM. Let us denote the whole wavefunction of the system as $|\Psi\rangle = a\,|+2\rangle_1|-2\rangle_2 \otimes |\psi_0\rangle_R + b\,|-2\rangle_1|+2\rangle_2 \otimes |\psi_1\rangle_R$, where $|\psi_i\rangle_R$'s denote the corresponding state of other spins. We can rewrite the first spin in $|\phi^\pm_x\rangle$ basis: $|\Psi\rangle = |\phi^+_x\rangle\big(a\,|-2\rangle_2 \otimes |\psi_0\rangle_R + b\,|+2\rangle_2 \otimes |\psi_1\rangle_R\big)/\sqrt{2} + |\phi^-_x\rangle\big(a\,|-2\rangle_2 \otimes |\psi_0\rangle_R - b\,|+2\rangle_2 \otimes |\psi_1\rangle_R\big)/\sqrt{2}\big)$. The measurement outcome ± gives rise the reduced state being $a\,|-2\rangle_2 \otimes |\psi_0\rangle_R \pm b\,|+2\rangle_2 \otimes |\psi_1\rangle_R$. The only difference is that the domain is reduced to a

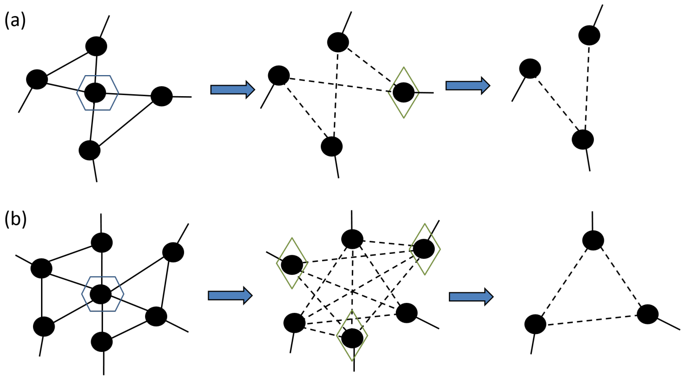


Figure 3 Illustration of graph transformation rules on Y measurements on a spin-2 domains and possible follow-up Z measurement to restore planarity. The hexagon indicates a Y-measured domain, and the diamonds indicate active Z measurements.

single site, but the quantum information remains the same (up to an inconsequential phase). But now if we continue to measure the second spin in the same way, this correponds to a logical X measurement and will change the entanglement structure for the remaining spins. In general, the effect of all $|\phi_\alpha^-\rangle\langle\phi_\alpha^-|$ (associated with K_α) in multi-site domains $\mathcal{C}$ is thus equivalent to a logical measurement of X operator.

Thus for each domain we need to distinguish two cases: (a) Fewer then all sites in an α-domain are affected by the POVM outcome K_α. Then, the domain is simply shrunk, and the graph G is unaffected. (b) All sites in an α-domain are affected by the POVM outcome K_α. Then, the encoded qubit residing on that domain is measured in the X-basis. If the latter happens, in terms of CGSB, measurement can be either a logical X or a logical Y measurement, and the state resulting from such measurement is again a graph state, and the new graph can be deduced from simple graph rules [7]; see Fig. 3 for illustration for Y-measurement.

4 Restoring planarity

We previously established simple criteria for computational universality of random planar graph states [16, 17], namely their corresponding graphs need to have a traversing path, and the domains need to be microscopic. The latter requirement for domains to be microscopic was checked numerically in several trivalent lattices [16, 17, 15] and also holds here via percolation argument. Therefore, what is needed to check is the former criterion. However, due to X- or Y-measured domains, the resultant graphs are no longer planer. After the POVM Eq. (1) we therefore apply a further round of active measurements with the purpose of restoring planarity of the encoded graph state.

What we choose to do here, specifically, is to first remove connected POVM "measured" (regardless of whether it is X- or Y-measured) domains by actively measuring their enclosing/neighboring domains in the logical Z basis, so as to remove these connected "measured" domains [7] at the cost of removing the enclosing domains as well. We also remove all X-measured domains and isolated *multi-site* (i.e. those with more than 2 sites) Y-measured domains by the same procedure. The non-planarity caused by these POVM "measured" domains is recovered quasi-locally; see Fig. 4.

Then we proceed to deal with the remaining isolated Y-measured domains which contain either one single or two sites (which can have at most 6 neighboring sites and hence domains).

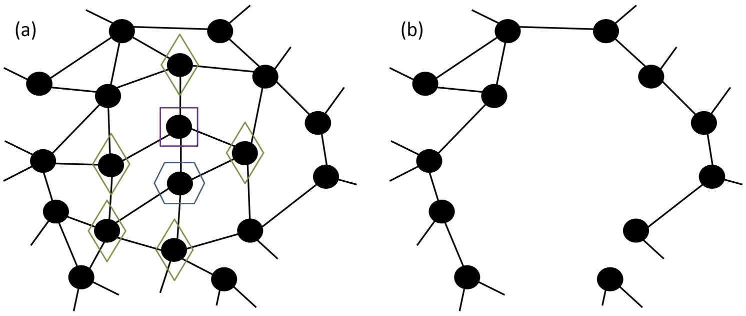


Figure 4 (color online) Part of a random graph for domains (solid circles). (a) The square indicates an X-measured domain and the hexagon indicates a Y-measured domain. In this example, the two measured domains are neighbors, and the effect on the graph will induce non-planarity. A simple approach is to apply active Z measurement on those domains (indicated by the diamonds) that enclose these connected X or Y-measured domains, similar to the game of go. (b) The upshot of the active Z measurements will remove these X/Y-measured domains as well as active Z-measured domains but will restore planarity.

The effect of Y-measured domains on the graph is to apply local complementation before removing the vertices corresponding to the Y-measured domains. If the Y-measured domain has three or fewer neighboring domains, the local complentation still preserves planarity. But when the nunber of neighbors is four or more, we then actively apply Z measurement on some of the neighboring domains (see Fig. 3) to maintain local planarity of the graph.

In the end we are left with a planar graph state, whose graph may or may not be percolated. If for large enough system and with finite nonzero probability, the graphs obtained after the above procedure are in the supercritical phase, then the resultant graph states can be used for universal MBQC, implying the original AKLT state is universal as well. Our simulations indicate that we need to use L of order 80 or larger in order to show that the graphs are in the supercritical phase with high probability such as 90%; see Fig. 5.

To carry out the simulations, we still need to sample the configuration $\{F, K\}$ according to the exact distribution $p(\{F, K\})$ [16]. In Section 5 we describe the formula.

5 Exact weight formula and simulation results

The exact sampling is needed, as random assignment of F and K POVM outcomes does not correctly reflect the correlation that these outcomes must obey due to multipartite entanglement in the AKLT state. Moreover, many of randomly chosen assignment of F and K are not valid measurement outcomes (as see below by the incompatibility condition). This latter complication sets the spin-2 case apart from the spin-3/2 case (in addition to the POVM itself). Employing the exact sampling also enables us to estimate the probability (at least the lower bound) of obtaining a universal resource state from performing the reduction procedure. We note that as long as the reduction procedure gives a finite, nonzero success probability in the large system limit then the original state is still regarded as a universal resource state (though of probabilistic nature). The weight formula that we discuss below will enable the exact sampling in the numerical simulations.

The weight formula. Let us recapitulate the notations introduced in Sec. 3.3. Consider a spin-2 AKLT state on a bi-colorable lattice $\mathcal{L}$ (generalization to non-bicolorable lattices is possible), and POVM elements F_α and K_α ($\alpha = x, y, z$). Denote by $J_F \subset \mathcal{L}$ the set of sites

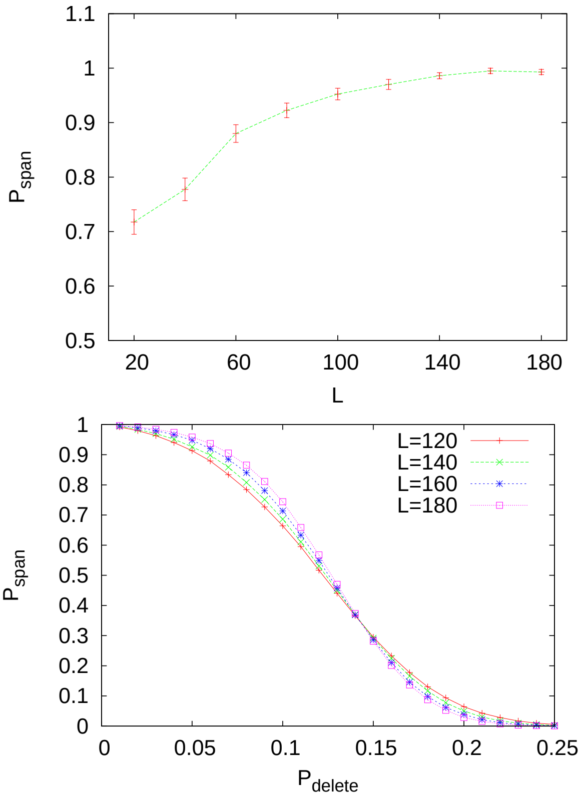


Figure 5 (a) Left panel: $p_{\rm span}$ vs. L (with $N = L^2$ the total number of sites) at $p_{\rm delete} = 0$. As L increases $p_{\rm span}$ also increases. This is obtained with exact sampling. (b) Right panel: $p_{\rm span}$ vs. $p_{\rm delete}$ (with $N = L^2$ the total number of sites) with $L = 120, 140, 160, 180$. The threshold of $p_{\rm delete}$ is approximately 0.142(3). The crossing for these curves indicates that there is a percolation transition from the supercritical to subcritical phase in the thermodynamic limit.

where the POVM outcome is of F-type and by $J_K = \mathcal{L}\backslash J_F$ the set of sites where POVM outcome is of K-type. Here additionally we denote by D_K the set of *domains* where the number of K-type POVM elements is equal to the total number of sites in the domain. Denote $\{F, K\}$ the set of POVM outcomes corresponding to $F^{(v)}_{\alpha(v)}$ and $K^{(w)}_{\beta(w)}$ and the probability for such occurrence is $p(\{F, K\})$.

We have introduced the graph state $|G_0\rangle$ in Eq. (4). Let us also label the set of all domains (i.e. vertices of the G_0) by V, the set of all inter-domain edges in $\mathcal{L}$ by $\mathcal{E}$ and the set of all edges of G_0 by E. Note that E is obtained from $\mathcal{E}$ by a modulo-2 operation [16].

As explained in Sec. 3.3, the effect of K-type POVM elements on a strict subset of sites in a domain only shrinks the size of a domain, whereas K-type POVM measurement on *all* sites in a domain in D_K amounts to the measurement (on $|G_0\rangle$) of an encoded logical X with respect to the encoding in Table 2. The stablizer operators for $|G_0\rangle$ in this encoding can be either $\pm X_c \bigotimes_{\mu\in{\rm Nb}(c)} Z_\mu$ or $\pm Y_c \bigotimes_{\mu\in{\rm Nb}(c)} Z_\mu$ (see Appendix 3.2), where Nb(c) denotes the set of neighbors of vertex c. But one can perform local logical-qubit rotations such that all stabilizer operators are of the canonical form $X_c \bigotimes_{\mu\in{\rm Nb}(c)} Z_\mu$, but then the effect of K-type POVM elements in a domain inside D_K amounts to the measurement of an encoded observable either X or Y. We have referred to this latter basis as the canonical graph-state basis (CGSB) earlier.

Now we introduce a $|V| \times |D_K|$ binary-valued matrix H with its entries defined as follows,

$$H_{\mu\nu} = 0, \text{ if } [\mathcal{K}_\mu, O_\nu] = 0, \tag{10a}$$

$$H_{\mu\nu} = 1, \text{ if } \{\mathcal{K}_\mu, O_\nu\} = 0, \tag{10b}$$

where $\mathcal{K}_\mu$ is the stabilizer operator associated with the vertex (or domain) $\mu \in V$ of the graph G, $O_\nu \equiv (-1)^{|V_\mu|} X_\mu$ is proportional to a logical Pauli X operator, and $\nu \in D_K$; see also Sec. 3.2. Let $\dim\big(\ker(H)\big)$ denote the dimension of the kernel of matrix H. We are ready to introduce the following lemma.

▶ **Lemma 1.** *If there exists a set Q (subset of D_K) such that $-\otimes_{\mu\in Q} O_\mu$ is in the stablizer group $\mathcal{S}(|G_0\rangle)$ of the state $|G_0\rangle$, then $p(\{F, K\}) = 0$. Otherwise,*

$$p(\{F, K\}) = c \left(\frac{1}{2}\right)^{|\mathcal{E}|-|V|+2|J_K|-\dim\big(\ker(H)\big)}, \tag{11}$$

where c is a constant.

We subsequently refer to the above condition for $p(\{F, K\}) = 0$ as the *incompatability condition*. The incompatibility condition implies that not all POVM outcomes labeled by F_α and K_α can occur. When there is no K outcome, Eq. (11) reduces to $p = c\,2^{|V|-|\mathcal{E}|}$ of previous results [16]. The correlation of F's and K's at different sites is reflected either in the incompatibility condition (if it is met) or else in the factor $\dim\big(\ker(H)\big)$. The probability distribution of $\{F, K\}$ is thus very far from independent and random. For the proof of the lemma, see Appendix A.

Numerical simulations. With the weight formula we can sample the exact distribution of physically allowed POVM outcomes $\{F, K\}$ and carry out the procedure to restore planarity of the random graphs associated with the post-POVM states. The sampling is obtained by using the standard Metropolis algorithm for updating $\{F, K\}$ configurations. One notable distinction is that we will need to avoid configurations that satisfies the incompatibility condition. First, we check whether the random graphs after our procedure have a spanner cluster by showing p_{span} for different L, and we see that it increases as L increases and approaches to unity; see Fig. 5. This suggests that for L large enough, the random graphs resulting from the thinning procedure are percolated. Then, we perform site percolation numerical experiment on these random graphs by removing each vertex with a probability p_{delete} and record the probability of a spanning cluster p_{span}. The crossing of curves in Fig. 5 for different sizes indicates that there is a percolation transition (at $p^*_{\text{delete}} \approx 0.142$) from the supercritical to subcritical phase in the thermodynamic limit. This shows that our random graph states (whose graphs are sitting at $p_{\text{delete}} = 0$) can be used to generate a network of entanglement that is universal for measurement-based quantum computation. This shows that the original AKLT state is also universal.

6 Concluding remarks

The family of Affleck-Kennedy-Lieb-Tasaki states provides a versatile playground for universal quantum computation. The merit of these states is that by appropriately choosing boundary conditions they are unique ground states of two-body interacting Hamiltonians, possibly with a spectral gap above the ground states. Here we have overcome several obstacles and shown that the spin-2 AKLT state on the square lattice is also a universal resource for measurement-based quantum computation. We were able to derive an exact weight formula for any given POVM outcome. Combined with a thinning procedure to restore planarity of random graph states, we performed Monte Carlo simulations and demonstrated that the assoicated planar random graphs from the procedure are residing in the supercritical phase.

The emerging picture from our series of study on the quantum computational universality in the two-dimensional AKLT valence-bond family is as follows. AKLT states involving spin-2 and other lower spin entities are universal if they reside on a two-dimensional frustration-free regular lattice with any combination of spin-2, spin-3/2, spin-1 and spin-1/2 (consistent with the lattice). Additionally, the effect of frustrated lattice may not be serious and can always be decorated (by adding additional spins) such that the resultant AKLT state is universal. We conjecture that the result hold in three dimensions as well.

Another direction of generalization is to investigate the robustness of the resource under small perturbations, e.g., slightly away from the AKLT Hamiltonian. A slight and simpler variation [5] is to consider the AKLT deformed spin-2 AKLT state with some deformation parameters, for which we give more detail in our arXiv paper [20]. One can also consider the frustrated kagomé lattice and deform it in a way to connect to a cluster state [4]. Furthermore, how would the quantum computational power of AKLT-like states make transition and how would they compare with the usual phases of matter [19]. We leave these for future consideration.

Acknowledgements. This work was supported by the National Science Foundation under Grants No. PHY 1314748 and No. PHY 1333903 (T.-C. W.) and by NSERC, Cifar and IARPA (R. R.).

References

1 H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nature Phys. **5**, 19 (2009).

2 J.-M. Cai, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. A **82**, 052309 (2010).

3 X. Chen, B. Zeng, Z.-C. Gu, B. Yoshida, and I. L. Chuang, Phys. Rev. Lett. **102**, 220501 (2009).

4 A. S. Darmawan and S. D. Bartlett , New J. Phys. **16**, 073013 (2014).

5 A. S. Darmawan, G. K. Brennen, and S. D. Bartlett, New J. Physics, **14**, 013023 (2012).

6 D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).

7 M. Hein, W. Dur, J. Eisert, R. Raussendorf, M.Van den Nest, and H.-J. Briegel, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati, D. Shepelyansky, P. Zoller, and G. Benenti, International School of Physics Enrico Fermi Vol. 162 (IOS Press, Amsterdam, 2006); also in arXiv:quant-ph/0602096.

8 R. Kaltenbaek, J. Lavoie, B. Zeng, S. D. Bartlett, and K. J. Resch, Nature Physics **6**, 850 (2010).

9 Ç. K. Koç and S. N. Arachchige, J. Parallel and Distributed Computing **13**, 118 (1991).

10 See e.g. the review by L. C. Kwek, Z. Wei, and B. Zeng, Int. J. Mod. Phys. B **26**, 1230002 (2012).

11 A. Miyake, Ann. Phys. (Leipzig) **326**, 1656 (2011).

12 M. A. Nielsen, Rep. Math. Phys. **57**, 147 (2006).

13 R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

14 R. Raussendorf and T.-C. Wei, Annual Review of Condensed Matter Physics **3**, pp.239-261 (2012).

15 T.-C. Wei, Phys. Rev. A **88**, 062307 (2013).

16 T.-C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).

17 T.-C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. A **86**, 032328 (2012).

18 T.-C. Wei, P. Haghnegahdar, R. Raussendorf, Phys. Rev. A **90**, 042333, (2014).

19 T.-C. Wei, Y. Li, and L. C. Kwek, Phys. Rev. A **89**, 052315 (2014).

20 T.-C. Wei and R. Raussendorf, arXiv:1501.07571.

A Proof of the weight formula

Let us mention first the following fact that (b is chosen according to a_c in Table 1),

$$\langle G_0|O_{\rm rest}\otimes_{i\in I_c}\sigma_b^{[i]}|G_0\rangle = 0, \tag{12}$$

if I_c is a strict subset of virtual qubits in any domain $\mathcal{C}$ (i.e. $|I_c|<4|\mathcal{C}|$) and σ_b is chosen according to Table 1 ($O_{\rm rest}$ denotes operators not in the support of domain $\mathcal{C}$). This can easily be proved by the fact that one can choose a stabilizer $S_{jq}\equiv\lambda_j\lambda_q\sigma_{a_c}^{[j]}\sigma_{a_c}^{[q]}$ (see Table 2), where $j\in I_c$ and $q\in\mathcal{C}$ but $q\notin I_c$, so that $(\otimes_{i\in I_c}(\sigma_b^{[i]})$ and S_{jq} anticommutes. Hence,

$$\begin{aligned} &\langle G_0|O_{\rm rest}(\otimes_{i\in I_c}\sigma_b^{[i]})|G_0\rangle = \langle G_0|O_{\rm rest}(\otimes_{i\in I_c}\sigma_b^{[i]})S_{jk}|G_0\rangle \\ = &-\langle G_0|S_{jk}O_{\rm rest}(\otimes_{i\in I_c}\sigma_b^{[i]})|G_0\rangle = -\langle G_0|O_{\rm rest}(\otimes_{i\in I_c}\sigma_b^{[i]})|G_0\rangle, \end{aligned}$$

showing that the expectation value is identically zero.

Let us also note the following useful relation regarding to the 4-qubit GHZ associated with the corresponding POVM outcome K_α,

$$|\mathrm{GHZ}_\alpha^-\rangle\langle\mathrm{GHZ}_\alpha^-| = \Pi_\alpha\frac{(1-\sigma_{b_\alpha}^{[v;1]}\sigma_{b_\alpha}^{[v;2]}\sigma_{b_\alpha}^{[v;3]}\sigma_{b_\alpha}^{[v;4]})}{2}\Pi_\alpha, \tag{13}$$

where Π_α ($\alpha=x,y,z$) is a projection to a two-dimensional subspace, equivalently an identity operator on the code subspace and can be safely omitted when acting on the graph state $|G_0\rangle$. Specificially, $\Pi_x = |++++\rangle\langle++++|+|----\rangle\langle----|$, $\Pi_y = |i,i,i,i\rangle\langle i,i,i,i|+|-i,-i,-i,-i\rangle\langle -i,-i,-i,-i|$ and $\Pi_z=|0000\rangle\langle 0000|+|1111\rangle\langle 1111|$. The label b_α denotes the corresponding type b if $a_c=\alpha$; see Table 1.

For a given domain (with a given type α), the POVM outcome on any site in the domain can be either F_α or K_α. Regarding the number n_K of K outcomes, there are two scenarios: (i) n_K is less than the total number $|V_c|$ of sites in that domain $\mathcal{C}$; (ii) $n_K=|V_c|$.

For case (i), the effect of all those K in terms of the probability distribution (or the weight formula) is to multiply a factor of 2^{-n_K}, i.e., (using $J\in\mathcal{C}$ to denotes the set of those sites with K)

$$\begin{aligned} &\langle G_0|O_{\rm rest}\left(\otimes_{v\in J}|\mathrm{GHZ}_{\alpha(v)}^-\rangle\langle\mathrm{GHZ}_{\alpha(v)}^-|\right)|G_0\rangle = \langle G_0|O_{\rm rest}\otimes_{v\in J}\frac{(1-\sigma_b^{[v;1]}\sigma_b^{[v;2]}\sigma_b^{[v;3]}\sigma_b^{[v;4]})}{2}|G_0\rangle \\ =&2^{-n_K}\langle G_0|O_{\rm rest}|G_0\rangle, \end{aligned}$$

where $O_{\rm rest}$ denotes operators not in the support of domain $\mathcal{C}$, and we have used

$$\langle G_0|O_{\rm rest}\otimes_{v\in J}(\sigma_b^{[v;1]}\sigma_b^{[v;2]}\sigma_b^{[v;3]}\sigma_b^{[v;4]})|G_0\rangle = 0.$$

For case (ii), when we expand all the $2^{|V_c|}$ terms in $\otimes_{v\in\mathcal{C}}(1-\sigma_b^{[v;1]}\sigma_b^{[v;2]}\sigma_b^{[v;3]}\sigma_b^{[v;4]})/2$, the only two nonvanishing contributions are $1/2^{|V_c|}$ and $(-1)^{|V_c|}(\otimes_{i=1}^{4|\mathcal{C}|}\sigma_b^{[i]})/2^{|V_c|}=(-1)^{|V_c|}X_c/2^{|V_c|}$.

In terms of logical X, the effect of all K is equivalent to $P_c = (1+O_c)/2^{|V_c|}$, where the $O_c = (-1)^{|V_c|} X_c$. That is

$$\langle G_0|O_{\rm rest}\left(\otimes_{v\in C}|{\rm GHZ}^-_{\alpha(v)}\rangle\langle{\rm GHZ}^-_{\alpha(v)}|\right)|G_0\rangle = \langle G_0|O_{\rm rest}\otimes_{v\in C}\frac{(1-\sigma_b^{[v;1]}\sigma_b^{[v;2]}\sigma_b^{[v;3]}\sigma_b^{[v;4]})}{2}|G_0\rangle$$
$$= 2^{-|V_c|}\langle G_0|O_{\rm rest}(1+O_c)|G_0\rangle.$$

Here we also see that the effect of all K in domain $\mathcal{C}$ is to measurement the logical qubit $\mathcal{C}$ in the logical X, followed by a post-selection of the result corresponding to either positive (if $|V_c|$ is even) or negative (if $|V_c|$ is oddd) eigenvalue of X.

With the above preparation, we can move on to the proof. Now consider a spin-2 AKLT state on a bi-colorable lattice $\mathcal{L}$ (generalization to non-bicolorable lattices is possible), and POVM elements F_α and K_α ($\alpha = x, y, z$). Denote by $J_F \subset \mathcal{L}$ the set of sites where the POVM outcome is of F-type and by $J_K = \mathcal{L}\backslash J_F$ the set of sites where POVM outcome is of K-type. We should, strictly speaking, use $\alpha(v)$ to denote the type of x, y, z at site v. When there is no confusion, we simply write α.

Proof of Lemma 1. For simplicity let us denote the AKLT state by $|\psi\rangle$ below. The probability $p(\{F,K\})$ for obtaining POVM measurements $\{F,K\}$ described above is

$$p(\{F,K\}) = \langle\psi|\bigotimes_{v\in J_F}F^{(v)\dagger}_{\alpha(v)}F^{(v)}_{\alpha(v)}\bigotimes_{w\in J_K}K^{(w)\dagger}_{\alpha(w)}K^{(w)}_{\alpha(w)}|\psi\rangle$$
$$= \left(\frac{3}{2}\right)^{|J_K|}\langle\psi|\bigotimes_{v\in J_F}F^{(v)\dagger}_{\alpha(v)}F^{(v)}_{\alpha(v)}\bigotimes_{w\in J_K}F^{(w)\dagger}_{\alpha(w)}K^{(w)\dagger}_{\alpha(w)}K^{(w)}_{\alpha(w)}F^{(w)}_{\alpha(w)}|\psi\rangle$$
$$= \left(\frac{1}{2}\right)^{|J_K|}\langle\psi|\bigotimes_{v\in \mathcal{L}}F^{(v)\dagger}_{\alpha(v)}\bigotimes_{w\in J_K}|{\rm GHZ}^-_{\alpha(w)}\rangle\langle{\rm GHZ}^-_{\alpha(w)}|\bigotimes_{u\in\mathcal{L}}F^{(u)}_{\alpha(u)}|\psi\rangle.$$

In the second equality we have used the fact that $K_\alpha = \sqrt{3/2}K_\alpha F_\alpha$, and in the third equality we have combined all F's and written explicitly K_α's in terms of the four-qubit GHZ projectors.

Now we know from Ref. [16] that

$$\bigotimes_{u\in\mathcal{L}}F^{(u)}_{\alpha(u)}|\psi\rangle = c_0\left(\frac{1}{\sqrt{2}}\right)^{|\mathcal{E}|-|V|}|G_0\rangle, \tag{14}$$

where $|G_0\rangle$ is an encoded graph state whose graph G_0 is specified by the POVM elements $\{F\}$, V is the set of domains of same-outcome POVM measurements, and $\mathcal{E}$ is the set of inter-domain edges (before the modulo-2 operation) [16]. The formula (14) was originally stated for the honeycomb lattice, but holds for all bipartite lattices. (For non-bipartite lattices, an additional condition needs to be imposed relating to geometric frustration [15]. Namely, if any domain contains a cycle with odd number of sites, such $\{F\}$ will not appear.) Combining the above two results we find that

$$p(\{F,K\}) = |c_0|^2\left(\frac{1}{2}\right)^{|\mathcal{E}|-|V|+|J_K|}\times\langle G_0|\left(\bigotimes_{v\in J_K}|{\rm GHZ}^-_{\alpha(v)}\rangle\langle{\rm GHZ}^-_{\alpha(v)}|\right)|G_0\rangle. \tag{15}$$

Using Eq. (13) and the results in the beginning of the section, we know that for those GHZ-projections in a domain such that their number is less than the total number of sites in the domain, i.e., case (i) discussed above, their contribution is to mulitiply by a factor 2^{-n_K}. For those such that the two numbers are equal, i.e., case (ii), these GHZ-projections (in a domain) can be replaced by $P_c = (1+O_c)/2^{|V_c|}$, where the $O_c = (-1)^{|V_c|}X_c$, and c labels the domain. Thus,

$$p(\{F,K\}) = |c_0|^2 \left(\frac{1}{2}\right)^{|\mathcal{E}|-|V|+2|J_K|} \times \langle G_0| \underset{c\in D_K}{\otimes} (I_c + O_c)|G_0\rangle, \tag{16}$$

where we use D_K to label the domains that contain the same number of K operators as the total number of internal sites.

Next we demonstrate the first part of the Lemma. Assume that, for some subset $Q \in D_K$, the observable $-\otimes_{c\in Q} O_c \in \mathcal{S}(|G_0\rangle)$. Then,

$$\begin{aligned} & \langle G_0| \underset{\mu\in D_K}{\otimes} (I_\mu + O_\mu)|G_0\rangle = \langle G_0| \underset{\nu\in D_K\setminus Q}{\otimes} (I_\nu + O_\nu) \underset{\mu\in Q}{\otimes} (I_\mu + O_\mu) \left(-\underset{c\in Q}{\otimes} O_c\right)|G_0\rangle \\ = \quad & -\langle G_0| \underset{\nu\in D_K\setminus Q}{\otimes} (I_\nu + O_\nu) \underset{c\in Q}{\otimes} (O_c + I_c)|G_0\rangle = -\langle G_0| \underset{\mu\in D_K}{\otimes} (I_\mu + O_\mu)|G_0\rangle = 0. \end{aligned}$$

In the third line we have used the fact $O_\mu^2 = I_\mu$. Let us also note that being product of Pauli operators, O_μ either commutes or anticommutes with another product of Pauli operators.

Next, we demonstrate the second part of the Lemma, i.e., finding $p(\{F,K\})$ when it is not identically zero. Consider a subset of domains $Q \subset D_K$. If $\otimes_{\mu\in Q} O_\mu \notin \pm\mathcal{S}(|G_0\rangle)$, then $\langle G_0|\otimes_{\mu\in Q} O_\mu|G_0\rangle = 0$ (note that μ is an index for the domain, not an index for the site). Furthermore, if the incompatibility condition is not satisfied, then $\otimes_{\mu\in Q} O_\mu \in \pm\mathcal{S}(|G_0\rangle)$ implies that $\otimes_{\mu\in Q} O_\mu \in \mathcal{S}(|G_0\rangle)$, and therefore $\langle G_0|\otimes_{\mu\in Q} O_\mu|G_0\rangle = 1$. We now exapnd the projector $\otimes_{c\in D_K}(I_c + O_c)$ in the matrix element,

$$\langle G_0| \underset{c\in D_K}{\otimes} (I_c + O_c)|G_0 = \langle G_0| \sum_{Q\subset D_K} \underset{\mu\in Q}{\otimes} O_\mu|G_0\rangle = |M|, \tag{17}$$

where the set M is defined as $M = \{O(Q) \equiv \otimes_{\mu\in Q} O_w | Q \subset D_K \,\text{and}\, O(Q) \in \mathcal{S}(|G_0\rangle)\}$. Actually M has the following equivalent formulation which will turn out to be useful,

$$M = \{O(Q) \equiv \underset{\mu\in Q}{\otimes} O_\mu | Q \subset D_K \ \text{and}\, [O(Q), S] = 0, \forall S \in \mathcal{S}(|G_0\rangle)\}. \tag{18}$$

Using this latter characterization of M, we now turn to the counting for $|M|$. We describe every subset Q of D_K by its characteristic vector $\mathbf{q}$, defined as follows: if $\mu \in Q$ then $q_\mu = 1$, or if $\mu \notin Q$, then $q_\mu = 0$. Furthermore we define a binary-valued matrix H of dimension $|V| \times |D_K|$ (where $|V|$ denotes total number of domains), whose entries are

$$\begin{aligned} & H_{\mu\nu} = 0, \text{ if } [\mathcal{K}_\mu, O_\nu] = 0, \\ & H_{\mu\nu} = 1, \text{ if } \{\mathcal{K}_\mu, O_\nu\} = 0, \end{aligned}$$

where $\mu \in V$ (the set of all domains) and $\nu \in D_K$ (the set of those domains with equal number of K's and sites). Then for any $Q \subset D_K$, $O(Q) \in M$ if and only if $H\mathbf{q} \bmod 2 = \mathbf{0}$. Therefore,

$$|M| = 2^{\dim\left(\ker(H)\right)}. \tag{19}$$

Putting everything into the expression for $p(\{F,K\})$ we obtain the equation (11),

$$p(\{F,K\}) = |c_0|^2 \left(\frac{1}{2}\right)^{|\mathcal{E}|-|V|+2|J_K|-\dim\left(\ker(H)\right)},$$

and the lemma is proved. ◀

We remark that checking the kernel of a binary matrix can be done via, e.g., the Gauss elimination method; see e.g. [9]. Furthermore, to check the incompatibility condition it is sufficient to check the products of O_μ associated with all basis vectors $\mathbf{q}$'s in the kernel. If none of them satisifies it, then the incompatibility condition is not satisified.

Quantum Capacity Can Be Greater Than Private Information for Arbitrarily Many Uses

David Elkouss[1,2] and Sergii Strelchuk[3]

1 Departamento de Análisis Matemático and Instituto de Matemática Interdisciplinar, Universidad Complutense de Madrid, 28040 Madrid, Spain
delkouss@ucm.es

2 QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
D.ElkoussCoronas@tudelft.nl

3 Department of Applied Mathematics and Theoretical Physics,
University of Cambridge, Cambridge CB3 0WA, U.K.
ss870@cam.ac.uk

Abstract

The quantum capacity of a quantum channel is always smaller than the capacity of the channel for private communication. However, both quantities are given by the infinite regularization of respectively the coherent and the private information. Here, we construct a family of channels for which the private and coherent information can remain strictly superadditive for unbounded number of uses. We prove this by showing that the coherent information is strictly larger than the private information of a smaller number of uses of the channel. It turns out that even though the quantum capacity is upper bounded by the private capacity, the non-regularized quantities can be interleaved. From an operational point of view, the private capacity can be used for gauging the practical value of quantum channels for secure communication and, consequently, for key distribution. We thus show that in order to evaluate the interest a channel for this task it is necessary to optimize the private information over an unlimited number of uses of the channel.

1998 ACM Subject Classification H.1.1 Systems and Information Theory, E.4 Coding and information theory.

Keywords and phrases Quantum channels, capacity, private information

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.64

1 Introduction

How well is it possible to characterize the resources available to transmit information? In classical information theory, this proves to be fully within our computational abilities: given a description of a channel, answering the question about its capacity to convey information to the receiver is straightforward. However, our world is inherently quantum and when one turns to the channels which transmit quantum information – the amount of resources required to compute their capacities is unknown at best. To compute a number of different types of capacity of the quantum channel, defined as regularized quantities [15, 10, 18, 20, 5, 16, 2, 8], it is necessary to perform an unbounded optimization over the number of the copies of the channel. The action of a channel $\mathcal{N}^{A\to B}$ can be defined via an isometry $V^{A\to BE}$: $\mathcal{N}^{A\to B}(\rho) = \mathrm{tr}_E V\rho V^*$, and its complementary channel is $\mathcal{N}_c^{A\to E}(\rho) = \mathrm{tr}_B V\rho V^*$. In the following, we will omit the register superscripts when it does not add to clarity.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 64–72
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The quantum and classical capacity of a channel [15, 10, 18, 20, 5] are given by:

$$\mathcal{Q}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}), \tag{1}$$

$$\mathcal{C}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{C}^{(1)}(\mathcal{N}^{\otimes n}) \tag{2}$$

where

$$\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} H(B) - H(E), \tag{3}$$

$$\mathcal{C}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B). \tag{4}$$

The optimization of the quantum capacity is performed over all valid states on the input register A while the optimization of the classical capacity is performed over $\mathcal{R}$ the set of classical-quantum states of the form $\rho^{XA} = \sum_x p_x |x\rangle\langle x|^X \otimes \rho_x^A$. Where X is an auxiliary classical register, H is the von Neumann entropy and $I(X;B)$ is the quantum mutual information.

From the above expressions it follows that one has to optimize over an *infinite* number of copies of the channel in order to compute its capacity. Do we have to resort to the regularized expression in order to compute the capacity of a quantum channel? It has recently been shown that at least in the case of the quantum capacity this is unavoidable [6, 22] even when we attempt to answer the question whether the channel has any capacity at all [4]. For the classical capacity, which is known to be superadditive for two uses of the channel [9], there is some evidence that ultimately the regularization might not be required [17, 24].

Arguably, the biggest practical success of quantum information theory to date is the possibility of quantum key distribution (QKD). QKD allows two distant parties to agree on a secret key independent of any eavesdropper. The required assumptions are: access to a quantum channel with positive private capacity and the validity of quantum physics[1]. On the other hand, key distribution is a primitive that can only be implemented with classical resources if one is willing to constrain the power of the eavesdropper. Even though there exist practical QKD schemes which enable secure communication over large distances with high key rates [3, 13, 11, 19], some of the fundamental questions about the capacity to transmit secure correlations remain unanswered.

The private capacity $\mathcal{P}$ of a channel is used to describe the ability of the channel to send secure messages to the receiver [5, 1]. It has a clear operational interpretation as the maximum rate at which the sender, Alice, can send private *classical* communication to the receiver, Bob. It is defined as follows:

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}). \tag{5}$$

That is the private capacity is given by the regularization of $\mathcal{P}^{(1)}(\mathcal{N})$, the private information of the channel, which is given by

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B) - I(X;E). \tag{6}$$

One can view private capacity as the optimal rate of reliable communication keeping Eve in a product state with Alice and Bob.

[1] In order to characterize the channel and to implement a specific QKD protocol one might need a public authentic classical channel or a small preshared secret.

This capacity characterizes the optimal rates of QKD. A better understanding of this quantity would allow to evaluate precisely the usefulness of communications channels for practical QKD links. For instance, the private capacity of Gaussian channels [25] remains open. Beyond the pure loss channel [27] only lower bounds on the private information of a single use are known.

Despite the significance of the private information, we still understand very little about its behaviour when the communication channel is used many times. Authors in [21, 12] provide evidence that $\mathcal{P}^{(1)}(\mathcal{N})$ is superadditive for two channel uses, although the magnitude of this effect is quantitatively very small. Recently, it has been shown the existence of two quantum channels $\mathcal{N}_1, \mathcal{N}_2$ with $\mathcal{C}(\mathcal{N}_1) \leq 2, \mathcal{P}(\mathcal{N}_2) = 0$ for which $\mathcal{P}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq 1/2 \log d$, where d is the dimension of the output of the joint channel [23]. This example shows that the private capacity is a superadditive quantity (this was also proved in [14] using a different construction).

Here we show that private information can be strictly superadditive for an arbitrarily large number of uses of the channel. More precisely, we prove the following theorem:

▶ **Theorem 1.** *For any n there exists a quantum channel $\mathcal{N}_n$ such that for $n > k \geq 1$:*

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}_n^{\otimes k}) < \frac{1}{k+1}\mathcal{Q}^{(1)}(\mathcal{N}_n^{\otimes k+1}). \tag{7}$$

This proves that entangled inputs increase the private information of a quantum channel and this effect persists for an *arbitrary* number of channel uses. As a bonus, we obtain a qualitatively different proof for the unbounded superadditivity of the coherent information [4].

The following relation holds for any channel [26]:

$$\mathcal{Q}^{(1)}(\mathcal{N}_n) \leq \mathcal{P}^{(1)}(\mathcal{N}_n) \leq \mathcal{C}^{(1)}(\mathcal{N}_n). \tag{8}$$

This means, that even though the coherent information is upper bounded by the private information and the quantum capacity is upper bounded by the private capacity, Theorem 1 implies that the non-regularized quantities can be interleaved.

We now introduce the key components of our construction which are required to prove Theorem 1.

2 Main construction

We first introduce *switch channels*:

$$\mathcal{N}^{SA\to SB}(\rho^{SA}) = \sum_i P_i^{S\to S} \otimes \mathcal{N}_i^{A\to B}(\rho^{SA}). \tag{9}$$

A switch channel consists of two input registers S and A of dimensions d and n respectively. Register S is measured in the standard basis and conditioned on the measurement outcome i a *component* channel $\mathcal{N}_i$ is applied to the second register. The computation of $\mathcal{P}^{(1)}(\mathcal{N})$ when $\mathcal{N}$ is of the form (9) can be simplified; it suffices to restrict inputs to a special form. The equivalent result for the quantum capacity was proved in [7].

▶ **Lemma 2.** *Consider a switch channel $\mathcal{N}^{SA\to SB}$ and let $\mathcal{T} = \{\rho : \rho = \sum_x p_x |x\rangle\langle x|^X \otimes |s\rangle\langle s|^S \otimes \rho_x^A\}$. Then*

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{1\leq s<n} \mathcal{P}^{(1)}(\mathcal{N}_s), \tag{10}$$

and $\mathcal{P}^{(1)}(\mathcal{N})$ can be achieved by some $\rho \in \mathcal{T}$.

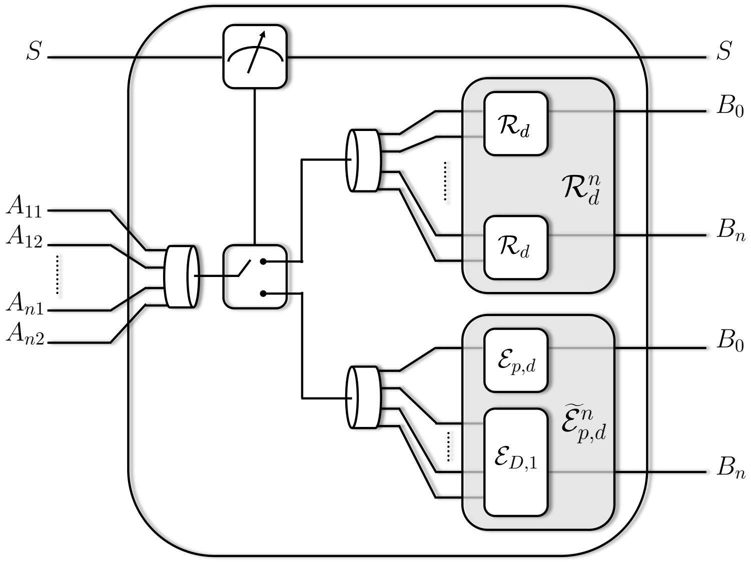


Figure 1 The channel has two input registers the control register S and the data register A. The control register is measured in the computational basis and depending on the output either the erasure channel $\widetilde{\mathcal{E}}^n_{p,d}$ or n copies of the d-dimensional rocket channel are applied.

Proof. The channel complementary to a switch channel is also a switch channel with component channels $\{\mathcal{N}_i^c\}_{i=1}^n$ complementary to $\{\mathcal{N}_i\}_{i=1}^n$ [4]. We denote the output systems of the complementary channel by S and E. Let $\rho \in \mathcal{R}$ be the input state that maximizes $\mathcal{P}^{(1)}(\mathcal{N})$, then $\mathcal{N}$ takes ρ to $\sum_{x,s} p_x p_{s|x} |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \mathcal{N}_s(\rho_{s|x})$ and $\mathcal{N}^c$ takes ρ to $\sum_{x,s} p_x p_{s|x} |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \mathcal{N}_s^c(\rho_{s|x})$. The following chain of inequalities holds:

$$I(X;BS) - I(X;ES) \tag{11}$$

$$= \sum_s p_s \Big(I(X;B|S=s) - I(X;E|S=s) \Big) \tag{12}$$

$$\leq \max_s \Big(I(X;B|S=s) - I(X;E|S=s) \Big) \tag{13}$$

$$\leq \max_s \mathcal{P}^{(1)}(\mathcal{N}_s). \tag{14}$$

The first equality follows because S is a classical system. The first inequality follows by choosing the value of s which maximizes the difference between the mutual informations. The second one since the difference between the between the mutual informations to the receiver and the environment is upper bounded by the private information of the channel $\mathcal{N}_s$. This upper bound is achievable by an input state of the form $\sigma^{XSA} = \sum_x p_x |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \rho_x$ where $\mathrm{tr}_S(\sigma^{XSA})$ is the state that achieves the private information of channel $\mathcal{N}_s$. Finally note that $\sigma^{XSA} \in \mathcal{T}$. ◀

There are two types of channels which we will use in place of $\mathcal{N}_i$. The first channel is the erasure channel:

$$\mathcal{E}_{p,d}^{A\to B}(\rho_A) = (1-p)\rho_B + p|e\rangle\langle e|_B \tag{15}$$

where $|e\rangle\langle e|$ is the erasure flag and d the dimension of the input register A. For $p \leq 1/2$ the erasure channel is degradable and $\mathcal{Q}(\mathcal{E}_{p,d}) = \mathcal{P}(\mathcal{E}_{p,d}) = \max\{0, (1-2p)\log d\}$, and $\mathcal{C}(\mathcal{E}_{p,d}) = (1-p)\log d$.

For any quantum channel $\mathcal{N}$ used alongside $\mathcal{E}_{p,d}$ the classical capacity is additive:

▶ **Lemma 3.** *For all quantum channels $\mathcal{N}$*

$$\mathcal{C}^{(1)}\left(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}\right)=\mathcal{C}^{(1)}(\mathcal{N})+n\mathcal{C}^{(1)}(\mathcal{E}_{p,d}). \tag{16}$$

Proof. The inequality $\mathcal{C}^{(1)}\left(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}\right)\geq\mathcal{C}^{(1)}(\mathcal{N})+n\mathcal{C}^{(1)}(\mathcal{E}_{p,d})$ is trivial. In order to prove the other direction consider the following chain of inequalities:

$$\begin{aligned}
\mathcal{C}^{(1)}(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}) &= \mathcal{C}^{(1)}(\mathcal{M}\otimes\mathcal{E}_{p,d}) && (17)\\
&= \max_\rho I(X;B_1B_2) && (18)\\
&= \max_\rho (1-p)I(X;B_1A_2)+pI(X;B_1) && (19)\\
&\leq (1-p)\mathcal{C}^{(1)}(\mathcal{M}\otimes I)+p\mathcal{C}^{(1)}(\mathcal{M}) && (20)\\
&= \mathcal{C}^{(1)}(\mathcal{M})+(1-p)\log d && (21)\\
&= \mathcal{C}^{(1)}(\mathcal{N})+n(1-p)\log d. && (22)
\end{aligned}$$

The first equality follows by identifying $\mathcal{M}$ with $\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n-1}$. We let A_1, A_2 and B_1, B_2 be the input and output of $\mathcal{M}$ and $\mathcal{E}_{p,d}$ respectively. The second equality is just the definition of the classical information (see Eq. 2). The third equality breaks the mutual information depending on the erasure channel transmitting or erasing. The inequality follows by maximizing each of the two mutual informations individually. The fourth inequality follows by taking into account that the classical information of the identity is additive and the last one by applying the same argument recursively for $n-1$ times. ◀

Intuitively, Lemma 3 states that the erasure channel cannot convey more information than an identity channel of dimension d^{1-p} even in the presence of other channels. Furthermore, we can use the expression for the classical capacity to obtain a trivial bound for the private information. It turns out that this trivial bound is tight and is saturated by the channel construction that we introduce below.

The second channel that we use alongside $\mathcal{E}_{p,d}$ is a d-dimensional 'rocket' channel, $\mathcal{R}_d$ [23]. It consists of two d-dimensional input registers A_1 and A_2 and a d-dimensional output register B. A_1 and A_2 are first subject to a random unitary and then jointly decoupled with a controlled dephasing gate. Then, the contents of A_1 becomes the output of the channel and the contents of A_2 is traced out. Bob also receives the classical description of the unitaries which acted on A_1 and A_2. Since dephasing occurs after the input registers have been scrambled by a random unitary, it is very hard for Alice to code for such channel, hence it has a very low classical capacity: $\mathcal{C}(\mathcal{R}_d)\leq 2$.

Our switch channel construction has the following form:

$$\mathcal{N}_{n,p,d}=P_0\otimes\mathcal{R}_d^n+P_1\otimes\widetilde{\mathcal{E}}_{p,d}^n \tag{23}$$

That is, it allows Alice to choose between $\mathcal{R}_d^n=\mathcal{R}_d^{\otimes n}$ and $\widetilde{\mathcal{E}}_{p,d}^n=\mathcal{E}_{p,d}\otimes\mathcal{E}_{1,d^{2n-1}}$ – a d-dimensional erasure channel padded with a full erasure channel to match the input dimension of $\mathcal{R}_d^n$.

2.1 Upper bound

To upper bound the private information of $\mathcal{N}_{n,p,d}$ we only need to optimize over all the possible different choices of $\mathcal{R}_d^n$ and $\widetilde{\mathcal{E}}_{p,d}^n$. Thus, the upper bound for $\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k})$ for $k\geq 1$

reads:

$$\begin{aligned}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}) &= \max_{0\le i\le k} \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes i}\otimes(\mathcal{R}_d^n)^{\otimes k-i})\\ &\le \max\begin{cases}\mathcal{C}^{(1)}((\mathcal{R}_d^n)^{\otimes k})\\ \max\limits_{1\le i\le k-1}\mathcal{C}^{(1)}(\mathcal{E}_{p,d}^{\otimes i}\otimes(\mathcal{R}_d^n)^{\otimes k-i}),\\ \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes k})\end{cases}\\ &\le \max\begin{cases}2kn,\\ (2n+(k-1)(1-p)\log d)\,.\\ (1-2p)\,k\log d\end{cases}\end{aligned} \tag{24}$$

2.2 Superadditivity of $\mathcal{P}^{(1)}$

First, we present the input state such that for $j>i$ uses and for some range of parameters allows to conclude that the private information for j uses is higher than the upper bound (24) for i uses. This state has the form:

$$\rho=\bigotimes_{k=1}^{j-1}\left(\Phi^+_{\widetilde{A}_k A_{k1}^{[1]}}\otimes\Phi^+_{A_{k2}^{[1]}A_{11}^{[k+1]}}\otimes\sigma_A\right) \tag{25}$$

where $\Phi^+_{AB}=1/d\sum_{i,j=1}^d|ii\rangle\langle jj|$. For the first use Alice chooses the rocket channel and for the remaining $j-1$ uses of the channel she selects $\mathcal{E}_{p,d}^n$. We denote with superscript $[k]$ the k-th use of the channel and the subscript ij indicates the input register as pictured in Fig. 1. The state can be read operationally as follows: Alice keeps the $\widetilde{A}_{km}$ registers and sends $A_{k1}^{[1]}$ through the first input of k-th $\mathcal{R}_d$ channel, $A_{k2}^{[1]}$ through the second (which will be subsequently discarded by the channel) and $A_{11}^{[k]}$ through $\mathcal{E}_{p,d}$. The remaining inputs do not play any role, so Alice can send any pure state σ_A through $\mathcal{E}_{D,1}$ and $\mathcal{R}_d^{[k]}$ for $k>j$. It is easy to verify that:

$$\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes j},\rho)=\frac{(j-1)(1-p)}{j}\log d. \tag{26}$$

This immediately gives a lower bound for the private information. Now, we are ready to prove Theorem 1.

Proof.

Fix $d=2^{4n^2/(1-2p)}$ and $p=\frac{11}{24}$. Then the regularized upper bounds (24) for $\mathcal{P}^{(1)}$ after k uses of the channel have the form:

$$U_k^1=\frac{2n}{k}, \tag{27}$$

$$U_k^2=\frac{2n(13(k-1)n+1)}{k} \tag{28}$$

and

$$U_k^3=4n^2; \tag{29}$$

the lower bound (26) after $k+1$ uses of the channel has the form:

$$L_{k+1}=\frac{26kn^2}{k+1}. \tag{30}$$

Consider the differences $D_k^i = -U_k^i + L_{k+1}$ for $i = 1, 2, 3$. Then, a simple substitution shows that:

$$D_k^1 = \frac{26kn^2}{k+1} - \frac{2n}{k}, \tag{31}$$

$$D_k^2 = -\frac{2n(k - 13n + 1)}{k(k+1)} \tag{32}$$

and

$$D_k^3 = \frac{2(11k-2)n^2}{k+1}. \tag{33}$$

All of the differences are positive for $n > k \geq 1$. ◀

The results of the theorem indicate that in order to compute the *exact* private capacity of a channel $\mathcal{N}$ it is necessary to compute $\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n})$ for an arbitrary number of uses n. In addition, we found an example whereby for each n and $1 \leq k < n$ having access to one additional copy of the channel up to n provides the parties with the largest possible gain in the capacity, proportional to the output dimension of the channel. Note, that for the channel $\mathcal{N}_{n,p,d}$ strict superadditivity of both private and coherent information holds for all number of uses of the channel up to n. This is markedly different from all previously known channel constructions which exhibit various superadditivity effects for quantum channel capacities. Such constructions exhibited superadditivity for some fixed number of uses of the channel t versus $t+c$ for some c. Our construction above shows that the private and coherent information of the *same* channel can be strictly superadditive for an arbitrary number of channel uses.

3 Discussion

In this paper we have constructed a family of channels for which the private and coherent information can remain strictly superadditive any number of uses of the channel. We are able to prove this result by showing that the private information of k uses of the channel is smaller than the coherent information of $k+1$ uses. That is, both quantities can be interleaved use after use for the first n uses of the channel. This shows that even though the quantum capacity is upper bounded by the infinite regularization of the private information, the quantum capacity can be larger than a finite regularization of the private information.

The private capacity of a quantum channel characterizes its ability to convey classical information securely. We proved that in order to compute the private capacity it is necessary to consider regularized expressions (5).

The results shown here raise questions about the properties that a channel has to verify such that its different capacities can be computed exactly using only finitely many (preferably only a few) copies of the channel.

Acknowledgements. We thank David Perez García and Māris Ozols for many useful discussions and feedback. SS acknowledges the support of Sidney Sussex College and European Union under project QALGO (Grant Agreement No. 600700). DE acknowledges financial support from the European CHIST-ERA project CQC (funded partially by MINECO grant PRI-PIMCHI-2011-1071) and from Comunidad de Madrid (grant QUITEMAD+-CM, ref. S2013/ICE-2801). This work has been partially supported by STW, QuTech and by the project HyQuNet (Grant No. TEC2012-35673), funded by Ministerio de Economía y Competitividad (MINECO), Spain. This work was made possible through the support of grant #48322 from the John Templeton Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

References

1 Ning Cai, Andreas Winter, and Raymond W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004.

2 Filippo Caruso, Vittorio Giovannetti, Cosmo Lupo, and Stefano Mancini. Quantum channels and memory effects. *Reviews of Modern Physics*, 86(4):1203–1259, December 2014.

3 L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters*, 104(2):021101, 2014.

4 Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. Unbounded number of channel uses may be required to detect quantum capacity. *Nat Commun*, 6, 03 2015.

5 I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *Information Theory, IEEE Transactions on*, 51(1):44–55, Jan 2005.

6 David P. DiVincenzo, Peter W. Shor, and John A. Smolin. Quantum-channel capacity of very noisy channels. *Phys. Rev. A*, 57(2):830–839, Feb 1998.

7 Motohisa Fukuda and Michael M. Wolf. Simplifying additivity problems using direct sum constructions. *Journal of mathematical physics*, 48(7):072101, 2007.

8 Saikat Guha, Patrick Hayden, Hari Krovi, Seth Lloyd, Cosmo Lupo, Jeffrey H. Shapiro, Masahiro Takeoka, and Mark M. Wilde. Quantum enigma machines and the locking capacity of a quantum channel. *Physical Review X*, 4(1):011016, 2014.

9 Matthew B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, Apr 2009.

10 A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273, January 1998.

11 Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

12 Oliver Kern and Joseph M. Renes. Improved one-way rates for bb84 and 6-state protocols. *Quantum Information & Computation*, 8(8):756–772, 2008.

13 Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 2015.

14 Ke Li, Andreas Winter, XuBo Zou, and GuangCan Guo. Private capacity of quantum channels is not additive. *Phys. Rev. Lett.*, 103(12):120501, Sep 2009.

15 Seth Lloyd. Capacity of the noisy quantum channel. *Phys. Rev. A*, 55(3):1613–1622, Mar 1997.

16 Rex A. C. Medeiros and Francisco M. De Assis. Quantum zero-error capacity. *International Journal of Quantum Information*, 3(01):135–139, 2005.

17 Ashley Montanaro. Weak multiplicativity for random quantum channels. *Communications in Mathematical Physics*, 319(2):535–555, 2013.

18 Benjamin Schumacher and Michael D. Westmoreland. Optimal signal ensembles. *Physical Review A*, 63(2):022308, January 2001.

19 Kaoru Shimizu, Toshimori Honjo, Mikio Fujiwara, Toshiyuki Ito, Kiyoshi Tamaki, Shigehito Miki, Taro Yamashita, Hirotaka Terai, Zhen Wang, and Masahide Sasaki. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area. *Journal of Lightwave Technology*, 32(1):141–151, 2014.

20 Peter W. Shor. The quantum channel capacity and coherent information, 2002. Lecture Notes, MSRI Workshop on Quantum Computation.

21 Graeme Smith, Joseph M. Renes, and John A. Smolin. Structured codes improve the bennett-brassard-84 quantum key rate. *Phys. Rev. Lett.*, 100(17):170502, 2008.

22 Graeme Smith and John A. Smolin. Degenerate quantum codes for pauli channels. *Phys. Rev. Lett.*, 98(3):030501, Jan 2007.

23 Graeme Smith and John A. Smolin. Extensive nonadditivity of privacy. *Phys. Rev. Lett.*, 103(12):120503, Sep 2009.

24 Graeme Smith and John A. Smolin. An exactly solvable model for quantum communications. *Nature*, 504:263–267, 2013.

25 Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

26 M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

27 Michael M. Wolf, David Pérez-García, and Geza Giedke. Quantum capacities of bosonic channels. *Phys. Rev. Lett.*, 98:130501, Mar 2007.

Semidefinite Programs for Randomness Extractors

Mario Berta[1], Omar Fawzi[2,3], and Volkher B. Scholz[4]

1 **Institute for Quantum Information and Matter, Caltech**
Pasadena, CA 91125, USA
2 **Department of Computing and Mathematical Sciences, Caltech**
Pasadena, CA 91125, USA
3 **LIP*, École Normale Supérieure de Lyon**
Lyon, 69007, France
4 **Institute for Theoretical Physics, ETH Zürich**
Zürich, 8093, Switzerland

Abstract

Randomness extractors are an important building block for classical and quantum cryptography. However, for many applications it is crucial that the extractors are quantum-proof, i.e., that they work even in the presence of quantum adversaries. In general, quantum-proof extractors are poorly understood and we would like to argue that in the same way as Bell inequalities (multi prover games) and communication complexity, the setting of randomness extractors provides a operationally useful framework for studying the power and limitations of a quantum memory compared to a classical one.

We start by recalling how to phrase the extractor property as a quadratic program with linear constraints. We then construct a semidefinite programming (SDP) relaxation for this program that is tight for some extractor constructions. Moreover, we show that this SDP relaxation is even sufficient to certify quantum-proof extractors. This gives a unifying approach to understand the stability properties of extractors against quantum adversaries. Finally, we analyze the limitations of this SDP relaxation.

1998 ACM Subject Classification E.4 Coding and Information Theory

Keywords and phrases Randomness Extractors, Quantum adversaries, Semidefinite programs

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.73

1 Introduction

1.1 Randomness extractors

A randomness extractor is a procedure to distill from a weakly random system as much (almost) uniform random bits as possible. Such objects are essential in many cryptographic protocols, in particular in quantum key distribution and device independent randomness expansion [3, 26, 12, 24, 35]. In this context, the process of transforming a partly private string into one that is almost uniformly random from the adversary's point of view is called privacy amplification [5, 4]. Even though we take a cryptographic point of view in this paper, we should mention that randomness extractors are very useful combinatorial objects in particular in the study of the computational power of randomness (see [34] for a survey).

More precisely, a randomness extractor is described by a family of functions $\text{Ext} = \{f_s\}_{s \in D}$ where $f_s : N \to M$. We use $N = 2^n$ to denote the input system (consisting of strings of n

[*] UMR 5668 LIP – ENS Lyon – CNRS – UCBL – INRIA, Université de Lyon

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 73–91
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

bits), $M = 2^m$ (bit-strings of length m) to denote the output system, and $D = 2^d$ (d bits) to denote the seed system that labels the functions f_s. Note that in a slight abuse of notation, we use the same letter for the actual set of inputs/outputs as well as its size. We say that Ext is a (k, ϵ)-extractor if for any random variable X taking values in N,

$$H_{\min}(X) := -\log p_{\text{guess}}(X) \geq k \quad \Longrightarrow \quad f_{U_D}(X) \text{ is } \epsilon\text{-close to } U_M \ , \tag{1}$$

where U_D is uniformly distributed on D and independent of X and U_M denotes the uniform distribution over M. As mentioned in the equation, the min-entropy $H_{\min}(X)$ is defined by the maximum probability of success in guessing a source X with only the knowledge of the distribution p of X. In this case, we simply have $H_{\min}(X) = -\log \max p(x)$. To quantify the distance between distributions, we use the total variation distance.[1] Equation (1) can thus be more explicitly written as

$$\forall x \in N,\ p(x) \leq 2^{-k} \quad \Longrightarrow \quad \frac{1}{D} \sum_{\substack{s \in D \\ y \in M}} \left| \sum_{x : f_s(x) = y} p(x) - \frac{1}{M} \right| \leq \epsilon \ . \tag{2}$$

Even though the concept was already present in [5, 4], the definition of randomness extractors was formulated in [23]. The typical example of a family $\{f_s\}_s$ of functions that satisfy this condition are randomly chosen functions. In fact, one can show [29, 25] that choosing D functions f_s independently at random among all the functions from N to M satisfies equation (2) with the following parameters

$$m = k - 2\log(1/\epsilon) - O(1) \quad \text{and} \quad d = \log(n-k) + 2\log(1/\epsilon) + O(1) \ . \tag{3}$$

In fact, we even know that these parameters cannot be improved except for additive constants [25]. Probabilistic constructions are interesting, but for applications we usually want the functions f_s to be efficiently computable. The most famous example of an explicit extractor is given by two-universal hash functions [5, 4, 17]. However, this construction has a seed size d that of the order of n, very far from the $\log n$ achieved by probabilistic constructions (3). Constructing efficiently computable extractors that match the parameters of randomly chosen functions has been the subject of a large body of research. Starting with the work of Nisan and Ta-Shma [22] and followed by Trevisan's breakthrough result [33], there has been a lot of progress in achieving polylogarithmic seed size, and there are now many intricate constructions that come close to the parameters in (3) (see the review articles [28, 34]).

1.2 Quantum-proof randomness extractors

For applications in classical and quantum cryptography (see, e.g., [26, 20]) and for constructing device independent randomness amplification and expansion schemes (see, e.g., [11, 21, 13]) it is important to find out if extractor constructions also work when the input source is correlated to another (possibly quantum) system Q. That is, we would like that for all classical-quantum input density matrices $\rho_{QN} = \sum_{x \in N} \rho(x) \otimes |x\rangle\langle x|$ acting on QN with conditional min-entropy

$$H_{\min}(N|Q)_\rho := -\log p_{\text{guess}}(N|Q)_\rho \geq k \ , \tag{4}$$

[1] It is more convenient here to use simply the ℓ_1 norm between the distributions, ignoring the $\frac{1}{2}$ factor in the usual definition of the total variation distance.

where $p_{\text{guess}}(N|Q)$ denotes the maximal probability of guessing the system N given Q, the output is uniform and independent of Q,[2]

$$\frac{1}{D}\sum_{\substack{s\in D\\ y\in M}}\left\|\sum_{x:f_s(x)=y}\rho(x)-\frac{1}{M}\sum_{x\in N}\rho(x)\right\|_1 \leq \epsilon\ . \tag{5}$$

As observed in [19, Proposition 1], if we restrict the system Q to be classical with respect to some basis $\{|e\rangle\}_{e\in Q}$ then every (k,ϵ)-extractor as in (2) is also a $\big(k+\log(1/\epsilon),2\epsilon\big)$-extractor in the sense of (5). That is, even when the input source is correlated to a classical system Q, every extractor construction still works (nearly) equally well for extracting randomness. However, if Q is quantum no such generic reduction is known and extractor constructions that also work for quantum Q are called quantum-proof.[3] Examples of (approximately) quantum-proof extractors include:

- Spectral (k,ϵ)-extractors are quantum-proof $(k,2\sqrt{\epsilon})$-extractors [8, Theorem 4]. This includes in particular two-universal hashing [26, 32], two-wise independent permutations [30], as well as sample and hash based constructions [18].
- One-bit output (k,ϵ)-extractors are quantum-proof $(k+\log(1/\epsilon),3\sqrt{\epsilon})$-extractors [19, Theorem 1].
- (k,ϵ)-extractors constructed along Trevisan [33] are quantum-proof $\big(k+\log(1/\epsilon),3\sqrt{\epsilon}\big)$-extractors [14, Theorem 4.6] (see also [2]).

We emphasize that all these stability results are specifically tailored proofs that make use of the structure of the particular extractor constructions. In contrast to these findings it was shown by Gavinsky *et al.* [16, Theorem 1] that there exists a valid (though contrived) extractor for which the decrease in the quality of the output randomness has to be at least $\epsilon\mapsto\Omega(m\epsilon)$.[4] As put forward by Ta-Shma [31, Slide 84], this then raises the question if the separation found by Gavinsky *et al.* is maximal, that is:

> *Is every (k,ϵ)-extractor a quantum-proof $\big(O(k+\log(1/\epsilon)),O(m\sqrt{\epsilon})\big)$-extractor or does there exists an extractor that is not quantum-proof with a large separation, say $\epsilon\mapsto(2^m\epsilon)^{\Omega(1)}$?*

We note that such a stability result would make every extractor with reasonable parameters (approximately) quantum-proof. However, for reasons discussed later it is unclear if such a generic quantum-proof reduction is possible and small sets of randomly chosen functions are interesting candidates to study this possibly large classical/quantum separation.

1.3 Our results

- We write the extractor condition (2) as a quadratic optimization program. The optimal value for this program denoted as $\mathrm{C}(\mathrm{Ext},k)$ is the smallest error ϵ such that Ext is a (k,ϵ)-extractor. We then construct a semidefinite programming (SDP) relaxation for this program whose optimal value is denoted $\mathrm{SDP}(\mathrm{Ext},k)$. This program gives an efficiently computable procedure to certify that a family of functions Ext is a (k,ϵ)-extractor for $\epsilon=\mathrm{SDP}(\mathrm{Ext},k)$.

[2] Other notions for weaker quantum adversaries have also been discussed in the literature, e.g., in the bounded storage model (see [14, Section 1] for a detailed overview).

[3] Note that the dimension of Q is unbounded and that it is a priori unclear if there exist any extractor constructions that are quantum-proof (even with arbitrarily worse parameters).

[4] Since the quality of the output randomness of Gavinsky *et al.*'s construction is bad to start with, the decrease $\epsilon\mapsto\Omega(m\epsilon)$ for quantum Q already makes the extractor fail completely in this case.

- We show that this certification procedure gives us much more: it certifies that Ext is a *quantum-proof* $(k, \sqrt{2}\epsilon)$-extractor. Thus, we give a general efficient method for proving that an extractor is quantum-proof. This technique can recover in a unified way many of the currently known methods for constructing quantum-proof extractors. In particular, we can show that constructions based on two-universal hashing [27, 32] are quantum-proof, and that any extractor with entropy deficit $n - k$ or output size m small is quantum-proof [6] (for $m = 1$ this was first shown in [19]). This latter result is a basic building block for showing that Trevisan based extractors are quantum-proof [14].
- We consider the limitations of this SDP relaxation. Even though $\mathrm{SDP}(\mathrm{Ext}, k)$ is a tight bound on $\mathrm{C}(\mathrm{Ext}, k)$ for many extractor constructions, there can be a large gap between these two values. In particular, if $\mathrm{Ext}_{\mathrm{rand}}$ is given by a small number of randomly chosen functions, then $\mathrm{C}(\mathrm{Ext}_{\mathrm{rand}}, k) \ll \mathrm{SDP}(\mathrm{Ext}_{\mathrm{rand}}, k)$. This shows that the method we propose cannot be used to prove that a small set of randomly chosen functions define good extractors. This means that other techniques would be needed to determine whether $\mathrm{Ext}_{\mathrm{rand}}$ is a quantum-proof extractor or not.

2 Preliminaries

2.1 Quantum information

In quantum theory, a system is described by an inner-product space, that we denote here by letters like N, M, Q.[5] Note that we use the same symbol Q to label the system, the corresponding inner-product space and also the dimension of the space. Let $\mathrm{Mat}_Q(S)$ be the vector space of $Q \times Q$ matrices with entries in S. Whenever S is not specified, it is assumed to be the set of complex numbers $\mathbb{C}$, i.e., we write $\mathrm{Mat}_Q(\mathbb{C}) =: \mathrm{Mat}_Q$. The state of a system is defined by a positive semidefinite operator ρ_Q with trace 1 acting on Q. The set of states on system Q is denoted by $\mathcal{S}(Q) \subset \mathrm{Mat}_Q(\mathbb{C})$. The inner-product space of a composite system QN is given by the tensor product of the inner-product spaces $Q \otimes N =: QN$. From a joint state $\rho_{QN} \in \mathcal{S}(QN)$, we can obtain marginals on the system Q by performing a partial trace of the N system $\rho_Q := \mathrm{Tr}_N[\rho_{QN}]$. The state ρ_{QN} of a system QN is called quantum-classical (with respect to some basis) if it can be written as $\rho_{QN} = \sum_x \rho(x) \otimes |x\rangle\langle x|$ for some basis $\{|x\rangle\}$ of N and some positive semidefinite operators $\rho(x)$ acting on Q with $\sum_x \mathrm{Tr}[\rho(x)] = 1$. We denote the maximally mixed state on system N by υ_N.

To measure the distance between two states, we use the trace norm $\|A\|_1 := \mathrm{Tr}[\sqrt{A^* A}]$, where A^* is the conjugate transpose of A. In the special case when A is diagonal, $\|A\|_1$ becomes the familiar ℓ_1 norm of the diagonal entries. Moreover, the Hilbert-Schmidt norm is defined as $\|A\|_2 := \sqrt{\mathrm{Tr}[A^* A]}$, and when A is diagonal this becomes the usual ℓ_2 norm. Another important norm we use is the operator norm, or the largest singular value of A, denoted by $\|A\|_\infty$. When A is diagonal, this corresponds to the familiar ℓ_∞ norm of the diagonal entries. For a probability distribution P_N on the set N, $\|P_N\|_{\ell_\infty}$ corresponds to the optimal probability with which P_N can be guessed successfully. We write

$$H_{\min}(N)_P := -\log \|P_N\|_{\ell_\infty} , \tag{6}$$

the min-entropy of P_N. More generally, the conditional min-entropy of N given Q is used to quantify the uncertainty in the system N given the system Q. The conditional min-entropy

[5] In the following all spaces are assumed to be finite-dimensional.

is defined as

$$H_{\min}(N|Q)_\rho := -\log \min_{\sigma_Q \in \mathcal{S}(Q)} \left\|(\mathrm{id}_N \otimes \sigma_Q^{-1/2})\rho_{NQ}(\mathrm{id}_N \otimes \sigma_Q^{-1/2})\right\|_\infty , \tag{7}$$

with generalized inverses. Note that in the special case where the system Q is trivial, we have $H_{\min}(N)_\rho = -\log \|\rho_N\|_\infty$.

2.2 Semidefinite programming

Semidefinite programs (SDP) are a large class of optimization problems that can be efficiently solved. Even if one is not explicitly interested in solving it numerically, a semidefinite program often has appealing properties such as strong duality. Semidefinite programming has been extensively used in various contexts in quantum information.

We use a formulation of semidefinite programs sometimes called vector programs. For some fixed values $\alpha_{x,x'}, \beta_{x,x',k}$ and γ_k, the optimization program can be written as follows:

$$\text{maximize} \quad \sum_{x,x'} \alpha_{x,x'} \vec{a}_x \cdot \vec{a}_{x'} \tag{8}$$

$$\text{subject to} \quad \sum_{x,x'} \beta_{x,x',k} \vec{a}_x \cdot \vec{a}_{x'} \leq \gamma_k \quad \text{for all } k \tag{9}$$

Here the optimization is over all vector $\vec{a}_x$ (of arbitrary finite dimension) that satisfy the constraints stated above. Note that we can always assume that the dimension of the vectors $\vec{a}_x$ is bounded by the number of vectors, i.e., the size of the set x runs over.

3 Quadratic programs for randomness extractors

It is useful to see the definition of extractors using the following optimization program:

$$\underline{\text{Error for extractor Ext} = \{f_s\}}$$

$$\mathrm{C}(\mathrm{Ext}, k) := \text{maximize} \quad \frac{1}{D} \sum_{s,y} \sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M} \right) p(x) \beta_{s,y} \tag{10}$$

$$\text{subject to} \quad 0 \leq p(x) \leq 2^{-k} \tag{11}$$

$$\sum_x p(x) = 1 \tag{12}$$

$$-1 \leq \beta_{s,y} \leq 1 \tag{13}$$

▶ **Definition 1.** Ext is a (k, ϵ)-extractor if and only if $\mathrm{C}(\mathrm{Ext}, k) \leq \epsilon$.

To relate this to the definition given in the introduction, it suffices to observe that the optimal choice for $\beta_{s,y}$ is the sign of $\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) p(x)$ so the objective function becomes $\frac{1}{D} \sum_{s,y} \left|\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) p(x)\right|$. The conditions (11) and (12) ensure that the input distribution has min-entropy at least k.

To simplify the program (10) we note that this function is convex in the distribution p and so the maximum is attained in the extreme points of the feasible region. These are simply the distributions that are uniform over a set of size at least 2^k. So we can equivalently write

$$\mathrm{C}(\mathrm{Ext}, k) = \max \left\{ \sum_{s,y} \left| \frac{1}{KD} \sum_{x \in L} \delta_{f_s(x)=y} - \frac{1}{MD} \right| : L \subseteq N, L \geq 2^k \right\} , \tag{14}$$

where again in a slight abuse of notation, we use the letter L for the actual set as well as its size. As the expression being maximized is the ℓ_1 norm between two probability distributions, we can write it as:

$$\mathrm{C}(\mathrm{Ext},k) = 2 \cdot \max \left\{ \frac{1}{KD} \sum_{x \in L, (y,s) \in R} \delta_{f_s(x)=y} - \frac{R}{MD} : L \subseteq N, L \geq 2^k, R \subseteq M \times D \right\} . \tag{15}$$

This allows us to interpret $\mathrm{C}(\mathrm{Ext},k)$ in graph-theoretic terms. For that we introduce a bipartite graph with left vertex set N and right vertex set $M \times D$, and there is an edge between vertices x and (y,s) if and only if $f_s(x) = y$. By writing $E(L,R)$ for the set of edges with one endpoint in L and the other endpoint in R, this expression is simply

$$\mathrm{C}(\mathrm{Ext},k) = 2 \cdot \max \left\{ \frac{E(L,R)}{2^k D} - \frac{R}{MD} : L \subseteq N, L \geq 2^k, R \subseteq M \times D \right\} . \tag{16}$$

Written in this way, we see that the optimization in $\mathrm{C}(\mathrm{Ext},k)$ is a kind of bipartite densest subgraph problem. Algorithms for a slightly different problem known as the densest K-subgraph problem have been extensively studied, see e.g., [15, 9]. The best known approximation algorithms for this problem achieve a factor of N^α for some constant α, but even ruling out constant factor approximations is only known using quite strong assumptions [1].

We can similarly write a program for the error of Ext against potentially quantum adversaries:

<u>Error for extractor Ext $= \{f_s\}$ against quantum adversaries</u>

$$\mathrm{Q}(\mathrm{Ext},k) := \text{maximize} \quad \frac{1}{D} \sum_{s,y} \sum_{x} \left(\delta_{f_s(x)=y} - \frac{1}{M} \right) \mathrm{Tr}\left[\rho(x) B_{s,y}\right] \tag{17}$$

$$\text{subject to} \quad 0 \leq \rho(x) \leq 2^{-k}\sigma \tag{18}$$

$$\sum_x \mathrm{Tr}[\rho(x)] = 1 \tag{19}$$

$$\mathrm{Tr}[\sigma] = 1 \tag{20}$$

$$\|B_{s,y}\|_\infty \leq 1 \tag{21}$$

Here the maximization is understood over all $\rho(x)$ of arbitrary dimension. Unlike for SDPs for which one can give an upper bound on the dimension of the vector of an optimal solution, no such bound is know in this setting. In fact, we do not even know if the quantity Q is computable.

▶ **Definition 2.** Ext is a quantum-proof (k,ϵ)-extractor if and only if $\mathrm{Q}(\mathrm{Ext},k) \leq \epsilon$.

To see that this definition coincides with the definition given in the introduction, observe that for fixed $\rho(x)$, the maximum over $B_{s,y}$ of the quantity $\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) \mathrm{Tr}\left[\rho(x) B_{s,y}\right]$ is $\| \sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) \rho(x)\|_1$. The constraints on $\rho(x)$ and σ ensure that the state $\sum_x \rho(x) \otimes |x\rangle\langle x|$ has conditional min-entropy at least k.

4 Semidefinite relaxations for randomness extractors

4.1 A relaxation for the extractor condition

Motivated by the fact that the two quantities $\mathrm{C}(\mathrm{Ext},k)$ and $\mathrm{Q}(\mathrm{Ext},k)$ are generally difficult to understand, we introduce a SDP that, as we show later, provides a relaxation for both of these quantities. For Ext $= \{f_s\}_{s \in D}$ and fixed k, we define:

$$\underline{\text{SDP relaxation for error of Ext} = \{f_s\}}$$

$$\mathrm{SDP}(\mathrm{Ext}, k) := \text{maximize} \quad \frac{1}{D}\sum_{s,y,x}\left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\vec{a}_x \cdot \vec{b}_{s,y} \tag{22}$$

$$\text{subject to} \quad 0 \le \vec{a}_x \cdot \vec{a}_{x'} \le 2^{-k}\cdot q(x) \tag{23}$$

$$q(x) \le 2^{-k} \tag{24}$$

$$\sum_x q(x) = 1 \tag{25}$$

$$\sum_{x,x'} \vec{a}_x \cdot \vec{a}_{x'} \le 1 \tag{26}$$

$$\|b_{s,y}\|_2 \le 1 \tag{27}$$

We maximize over all possible dimensions of the vectors $\vec{a}_x$ and $\vec{b}_x$. Moreover, the Cauchy-Schwarz inequality implies that the optimal choice for $\vec{b}_{s,y}$ is

$$\frac{\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\vec{a}_x}{\|\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\vec{a}_x\|_2} \ , \tag{28}$$

and thus the objective function of the SDP relaxation becomes

$$\frac{1}{D}\sum_{s,y}\left\|\sum_x\left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\vec{a}_x\right\|_2 \ , \tag{29}$$

subject to the constraints on the vectors $\vec{a}_x$ stated in (22). By simply plugging $\vec{a}_x = p(x)$, $q(x) = p(x)$ and $\vec{b}_{s,y} = \beta_{s,y}$, we see that this SDP gives an upper bound on the extractor program (10).

▶ **Proposition 3.** *For any* Ext *and* k*,* $\mathrm{C}(\mathrm{Ext}, k) \le \mathrm{SDP}(\mathrm{Ext}, k)$*. In other words, if* $\mathrm{SDP}(\mathrm{Ext}, k) \le \epsilon$*, then* Ext *is a* (k, ϵ)*-extractor.*

This gives a computationally efficient criterion for certifying that an extractor is good. As we show in Section 4.3, this method can certify that many important constructions are good extractors. However, this technique does in general not give a tight characterization of extractors and there can be a large gap between the values $\mathrm{C}(\mathrm{Ext}, k)$ and $\mathrm{SDP}(\mathrm{Ext}, k)$ as we will see in Section 4.4.

4.2 A relaxation for the error against quantum adversaries

A very interesting property about the SDP (22) is that it also gives an upper bound on the error of an extractor against quantum adversaries. This means that if an extractor satisfies the stronger property $\mathrm{SDP}(\mathrm{Ext}, k) \le \epsilon$ then it is not only a (k, ϵ)-extractor but also a quantum proof $(k, \sqrt{2}\epsilon)$-extractor.

▶ **Theorem 4.** *For any* Ext *and* k*, we have*

$$\mathrm{C}(\mathrm{Ext}, k) \le \mathrm{Q}(\mathrm{Ext}, k) \le \sqrt{2}\cdot\mathrm{SDP}(\mathrm{Ext}, k) \ . \tag{30}$$

Proof. Let $\rho = \sum_x \rho(x) \otimes |x\rangle\langle x|$ be a quantum state on QN with $H_{\min}(N|Q)_\rho \ge k$. By the definition of the conditional min-entropy, this implies that there exists $\sigma \in \mathcal{S}(Q)$ such that $\rho(x) \le 2^{-k}\sigma$ for all $x \in N$. We now define the average state $\bar{\rho} = \sum_x \rho(x)$ and $\omega = \frac{\bar{\rho}+\sigma}{2}$, as well as the vectors $\vec{a}_x$ as the list of entries of the matrix $\frac{1}{\sqrt{2}}\omega^{-1/4}\rho(x)\omega^{-1/4}$. This is so that we have $\vec{a}_x \cdot \vec{a}_{x'} = \frac{1}{2}\mathrm{Tr}[\omega^{-1/2}\rho(x)\omega^{-1/2}\rho(x')]$. As the trace of the product of two positive semidefinite operators is nonnegative, we have $\vec{a}_x \cdot \vec{a}_{x'} \geq 0$. Moreover, we have

$$\vec{a}_x \cdot \vec{a}_{x'} = \frac{1}{2}\mathrm{Tr}[\omega^{-1/2}\rho(x)\omega^{-1/2}\rho(x')] \leq \frac{1}{2}\mathrm{Tr}[\omega^{-1/2}\rho(x)\omega^{-1/2}2^{-k}\sigma] \tag{31}$$

$$\leq \frac{1}{2} \cdot 2^{-k}\mathrm{Tr}[\omega^{-1/2}\rho(x)\omega^{-1/2}2\omega] \leq 2^{-k}\mathrm{Tr}[\rho(x)] \ . \tag{32}$$

We set $q(x) = \mathrm{Tr}[\rho(x)]$. Note that we have $q(x) = \mathrm{Tr}[\rho(x)] \leq 2^{-k}\mathrm{Tr}[\sigma] = 2^{-k}$ and $\sum_x q(x) \leq 1$. We can also write

$$\sum_{x,x'} \vec{a}_x \cdot \vec{a}_{x'} = \frac{1}{2}\mathrm{Tr}[\omega^{-1/2}\bar{\rho}\omega^{-1/2}\bar{\rho}] \leq \frac{1}{2}\mathrm{Tr}[\omega^{-1/2}\bar{\rho}\omega^{-1/2}2\omega] \leq 1 \ . \tag{33}$$

We now analyze the objective function. We use the following Hölder-type inequality for operators $\|\alpha\beta\gamma\|_1 \leq \||\alpha|^4\|_1^{1/4}\||\beta|^2\|_1^{1/2}\||\gamma|^4\|_1^{1/4}$, see e.g., [10, Corollary IV.2.6]. The error the extractor makes on input ρ is given by

$$\frac{1}{D}\sum_{s,y}\left\|\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\rho(x)\right\|_1$$

$$\leq \frac{1}{D}\sum_{s,y}\|\omega\|_1^{1/4}\left\|\left(\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\omega^{-1/4}\rho(x)\omega^{-1/4}\right)^2\right\|_1^{1/2}\|\omega\|_1^{1/4} \tag{34}$$

$$= \frac{1}{D}\sum_{s,y}\sqrt{\mathrm{Tr}\left[\sum_{x,x'}\left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\left(\delta_{f_s(x')=y} - \frac{1}{M}\right)\omega^{-1/2}\rho(x)\omega^{-1/2}\rho(x')\right]} \tag{35}$$

$$= \frac{1}{D}\sum_{s,y}\sqrt{\sum_{x,x'}\left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\left(\delta_{f_s(x')=y} - \frac{1}{M}\right)2 \cdot \vec{a}_x \cdot \vec{a}_{x'}} \tag{36}$$

$$= \frac{\sqrt{2}}{D}\sum_{s,y}\left\|\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right)\vec{a}_x\right\|_2 \ . \tag{37}$$

This proves that the error the extractor makes in the presence of quantum adversaries is upper bounded by $\sqrt{2} \cdot \mathrm{SDP}(\mathrm{Ext}, k)$. ◀

4.3 Applications

We now give several applications of the SDP relaxation. We show that many results about quantum-proof extractors can be shown with the SDP quantity. First, let us consider general results that do not use the structure of the functions in Ext but simply the extractor's parameters. We know the advantage obtained by a quantum adversary compared to a classical one can by bounded by a function of the number of output bits m or the min-entropy deficit $n-k$ [6] (for $m = 1$ this was first shown in [19]). In particular, if m or $n-k$ are small, then the quantum advantage cannot be large. We show that this is actually a property of the SDP.

▶ **Theorem 5.** *For any* Ext *and* k*, we have for any* $\epsilon > 0$*,*

$$\mathrm{SDP}\big(\mathrm{Ext}, k + \log(1/\epsilon)\big) \leq \sqrt{2^m}\sqrt{\mathrm{C}(\mathrm{Ext}, k) + \epsilon} \tag{38}$$

$$\mathrm{SDP}(\mathrm{Ext}, k) \leq 3K_G 2^{n-k}\mathrm{C}(\mathrm{Ext}, k-1) \ , \tag{39}$$

where $K_G \leq 1.8$ *is Grothendieck's constant.*

Proof. As Ext is usually clear from the context, we use $\mathrm{C}(k)$ and $\mathrm{SDP}(k)$ for $\mathrm{C}(\mathrm{Ext}, k)$ and $\mathrm{SDP}(\mathrm{Ext}, k)$. To prove (38), we consider an optimal solution for $\mathrm{SDP}(k + \log(1/\epsilon))$. Define $p(x, x') = \vec{a}_x \cdot \vec{a}_{x'}$, with $\bar{p}(x) = \sum_{x'} p(x, x')$. Now consider the set $S_\epsilon = \{x \in N : \bar{p}(x) \le \epsilon q(x)\}$. Then $\sum_{x \in S_\epsilon} \bar{p}(x) \le \epsilon \sum_{x \in S_\epsilon} q(x) \le \epsilon$. Using the fact that $\vec{a}_x$ define a feasible solution for $\mathrm{SDP}(k + \log(1/\epsilon))$, we have for $x \notin S_\epsilon$, $p(x, x') \le 2^{-(k+\log(1/\epsilon))} q(x) \le 2^{-k} \bar{p}(x)$. We can then write using the Cauchy Schwarz inequality,

$$\frac{1}{D} \sum_{s,y} \left\| \sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) \vec{a}_x \right\|_2 \le \sqrt{\frac{1}{D} \sum_{s,y} \left\| \sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) \vec{a}_x \right\|_2^2} \sqrt{2^m} \ . \tag{40}$$

We now look at the expression $\frac{1}{D} \sum_{s,y} \left\| \sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) \vec{a}_x \right\|_2^2$ which equals

$$\frac{1}{D} \sum_{s,y} \sum_{x,x'} \left(\delta_{f_s(x)=y} - 2^{-m}\right) \cdot \left(\delta_{f_s(x')=y} - 2^{-m}\right) p(x, x') \tag{41}$$

$$\le \frac{1}{D} \sum_{s,y} \sum_x \left| \sum_{x'} \left(\delta_{f_s(x)=y} - 2^{-m}\right) \cdot \left(\delta_{f_s(x')=y} - 2^{-m}\right) p(x, x') \right| \tag{42}$$

$$\le \frac{1}{D} \sum_{s,y} \sum_x \left| \sum_{x'} \left(\delta_{f_s(x')=y} - 2^{-m}\right) p(x, x') \right| \ . \tag{43}$$

We separate the sum into $x \in S_\epsilon$ and $x \notin S_\epsilon$ and get

$$\frac{1}{D} \sum_{s,y} \sum_x \left| \sum_{x'} \left(\delta_{f_s(x')=y} - 2^{-m}\right) p(x, x') \right| \tag{44}$$

$$= \frac{1}{D} \sum_{s,y} \sum_x \bar{p}(x) \left| \sum_{x'} \left(\delta_{f_s(x')=y} - 2^{-m}\right) \frac{p(x, x')}{\bar{p}(x)} \right| \tag{45}$$

$$= \sum_{x \in S_\epsilon} \bar{p}(x) \frac{1}{D} \sum_{s,y} \left| \sum_{x'} \left(\delta_{f_s(x')=y} - 2^{-m}\right) \frac{p(x, x')}{\bar{p}(x)} \right| \tag{46}$$

$$+ \sum_{x \notin S_\epsilon} \bar{p}(x) \frac{1}{D} \sum_{s,y} \left| \sum_{x'} \left(\delta_{f_s(x')=y} - 2^{-m}\right) \frac{p(x, x')}{\bar{p}(x)} \right| \le \epsilon + \mathrm{C}(k) \ , \tag{47}$$

which proves (38).

We now prove the inequality (39). For that, we simply upper bound $\mathrm{SDP}(\mathrm{Ext}, k)$ by forgetting several constraints and then apply Grothendieck's inequality (Theorem 9). Observe first that for any feasible vectors $\vec{a}_x$ for the SDP, we have $\|\vec{a}_x\|_2^2 \le 2^{-k} q(x) \le 2^{-2k}$.

$$\mathrm{SDP}(\mathrm{Ext}, k) \le \max \left\{ \frac{1}{D} \sum_{s,y,x} \left(\delta_{f_s(x)=y} - 2^{-m}\right) \vec{a}_x \cdot \vec{b}_{s,y} : \|\vec{a}_x\|_2 \le 2^{-k}, \|\vec{b}_{s,y}\|_2 \le 1 \right\} \tag{48}$$

$$\le K_G \max \left\{ \frac{1}{D} \sum_{s,y,x} \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x b_{s,y} : |a_x| \le 2^{-k}, |b_{s,y}| \le 1 \right\} \tag{49}$$

$$= K_G \max \left\{ \frac{1}{D} \sum_{s,y} \left| \sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x \right| : |a_x| \le 2^{-k} \right\} \ . \tag{50}$$

We partition the set of $x \in N$ into $\{x : a_x \geq 0\}$ and $\{x : a_x < 0\}$ and write

$$\left|\sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x\right| \leq \left|\sum_{x:a_x\geq 0} \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x\right| \tag{51}$$

$$+ \left|\sum_{x:a_x<0} \left(\delta_{f_s(x)=y} - 2^{-m}\right) (-a_x)\right| . \tag{52}$$

Let us write $\alpha_+ := \sum_{x:a_x\geq 0} a_x$. If $\alpha_+ \geq 1$, then we define $p_+(x) = \frac{\max\{a_x,0\}}{\alpha_+}$. Observing that $\alpha_+ \leq 2^{n-k}$, we have

$$\frac{1}{D}\sum_{s,y}\left|\sum_{x:a_x\geq 0} \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x\right| = \alpha_+ \cdot \frac{1}{D}\sum_{s,y}\left|\sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) p_+(x)\right| \tag{53}$$

$$\leq \alpha_+\mathrm{C}(k + \log(\alpha_+)) \leq 2^{n-k}\mathrm{C}(k) , \tag{54}$$

where we have used the abbreviation $\mathrm{C}(k) = \mathrm{C}(\mathrm{Ext}, k)$. Otherwise (if $\alpha_+ < 1$), we define $p_+(x) = \max\{a_x, 0\} + (1 - \alpha_+)2^{-n}$. We get

$$\frac{1}{D}\sum_{s,y}\left|\sum_{x:a_x\geq 0} \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x\right| \tag{55}$$

$$= \frac{1}{D}\sum_{s,y}\left|\sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) \left(p_+(x) - (1 - \alpha_+)2^{-n}\right)\right| \tag{56}$$

$$\leq \frac{1}{D}\sum_{s,y}\left|\sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) p_+(x)\right| + (1 - \alpha_+)\frac{1}{D}\sum_{s,y}\left|\sum_x \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) 2^{-n}\right| \tag{57}$$

$$\leq \mathrm{C}(k - 1) + (1 - \alpha_+)\mathrm{C}(n) . \tag{58}$$

With a similar argument for the set $\{x : a_x < 0\}$, we reach the bound

$$\frac{1}{D}\sum_{s,y}\left|\sum_x \left(\delta_{f_s(x)=y} - 2^{-m}\right) a_x\right| \tag{59}$$

$$\leq \max\{2 \cdot 2^{n-k}\mathrm{C}(k), \mathrm{C}(k - 1) + \mathrm{C}(n) \tag{60}$$

$$+ 2^{n-k}\mathrm{C}(k), 2\mathrm{C}(k - 1) + (1 - \alpha_+ - \alpha_-)\mathrm{C}(n)\} \leq 3 \cdot 2^{n-k}\mathrm{C}(k - 1) . \tag{61}$$

Finally, we get $\mathrm{SDP}(k) \leq 3K_G 2^{n-k}\mathrm{C}(k - 1)$. ◀

Some specific constructions are also known to be quantum-proof, in particular constructions based on two-universal hash functions [26, 27, 32]. This type of construction is captured by spectral extractors [8]. For an extractor $\mathrm{Ext} = \{f_s\}_{s\in D}$ we define the linear maps [Ext] and τ that map vectors of dimension N to vectors of dimension DM as follows:

$$[\mathrm{Ext}]\left(\sum_x p(x)|x\rangle\langle x|_N\right) = \frac{1}{D}\cdot\sum_{s,y}\sum_x \delta_{f_s(x)=y}p(x)|y\rangle\langle y|_M \otimes |s\rangle\langle s|_D \tag{62}$$

$$\tau\left(\sum_x p(x)|x\rangle\langle x|_N\right) = \left(\sum_x p(x)\right) v_M \otimes v_D . \tag{63}$$

Note that we used a quantum notation and identified vectors with diagonal matrices. A spectral (k,ϵ)-extractor is then defined via the largest eigenvalue bound

$$\lambda_1\Big([\mathrm{Ext}]^* \cdot [\mathrm{Ext}] - \tau^* \cdot \tau\Big) \leq 2^{k-m-d}\epsilon\ , \tag{64}$$

where $*$ refers to the adjoint of a linear map. We prove next that for spectral extractor, there can be at most a quadratic gap between $\mathrm{C}(\mathrm{Ext},k)$ and $\mathrm{SDP}(\mathrm{Ext},k)$.

▶ **Theorem 6.** *Let* $\mathrm{Ext}_{\mathrm{spec}} = \{f_s\}_{s\in D}$ *be a spectral* (k,ϵ)*-extractor as defined in* (64)*. Then, we have*

$$\mathrm{SDP}(\mathrm{Ext}_{\mathrm{spec}},k) \leq \sqrt{\epsilon}\ . \tag{65}$$

The proof can be found in Appendix B. Another class of extractors that are quantum-proof are Trevisan based constructions [14, 2]. These are particularly important to understand because they are the only known quantum-proof constructions with short seed $d = O(\mathrm{poly}(\log n))$ (cf. the optimal parameters (3)). Trevisan's construction can be thought of as a composition of one-bit output extractors cleverly interleaved by slightly reusing the seed. Specifically, the construction is based on a family of subsets $S_1,\ldots,S_m \subset \{1,\ldots,d\}$ such that for each i we have

$$|S_i| = l \quad \text{and} \quad \sum_{j<i} 2^{|S_i\cap S_j|} \leq r(m-1)\ , \tag{66}$$

for some $r > 0$. Such a family $\{S_i\}_{i\in\{1,\ldots,m\}}$ is also called weak (l,r)-design. Now, take a one-bit output extractor $\mathrm{Ext}_{\mathrm{one}} = \{g_t\}_{t\in\{0,1\}^l}$ with $g_t : N \to \{0,1\}$, and a weak (l,r)-design as defined in (66). Trevisan then defines a m-bit output extractor

$$\mathrm{Ext}_{\mathrm{Trev}} = \{f_s\}_{s\in D} \quad \text{with} \quad f_s : N \to M \tag{67}$$

$$f_s(x) := g_{s|S_1}(x) \circ g_{s|S_1}(x) \circ \cdots \circ g_{s|S_m}(x)\ , \tag{68}$$

where $s|S_i$ denotes the l-bits of s that correspond to the position indexed by the set S_i, and $\circ$ means concatenation.[6] The basic idea of the proof is to bound the quality of $\mathrm{Ext}_{\mathrm{Trev}}$ as a function of the quality of $\mathrm{Ext}_{\mathrm{one}}$. Then (using Theorem 5) one can relate the quality of $\mathrm{Ext}_{\mathrm{one}}$ against quantum adversaries to its quality against classical adversaries. We give (in the Appendix) a concise proof of this result using our notation in terms of the quantum program (17).

▶ **Theorem 7.** *Let* $\{S_i\}_{i\in\{1,\ldots,m\}}$ *be a weak* (l,r)*-design as defined in* (66)*, and* $\mathrm{Ext}_{\mathrm{one}} = \{g_t\}_{t\in\{0,1\}^l}$ *be a one-bit output extractor. Then, we have for Trevisan's extractor* $\mathrm{Ext}_{\mathrm{Trev}} = \{f_s\}_{s\in D}$ *as defined in* (67)*–*(68)*,*

$$\mathrm{Q}(\mathrm{Ext}_{\mathrm{Trev}},k) \leq m\cdot \mathrm{Q}(\mathrm{Ext}_{\mathrm{one}},k-r(m-1)) \tag{69}$$

$$\leq 2m\cdot\sqrt{\mathrm{C}(\mathrm{Ext}_{\mathrm{one}},k-r(m-1)-\log(1/\epsilon))+\epsilon}\ , \tag{70}$$

for any $\epsilon > 0$.

[6] Actual parameters for Trevisan based extractor constructions are, e.g, discussed in detail in [14, Section 5].

4.4 Gap between C and SDP

In this section, we show that there can be a large gap between the value C and SDP. In fact, we show that SDP cannot be used to prove that randomly chosen functions are good randomness extractors. As discussed in (3), random functions are good extractors with essentially optimal parameters. In other words, for a family of functions $\mathrm{Ext}_{\mathrm{rand}} = \{f_s\}_{s\in D}$ chosen at random, we have with very high probability that

$$\mathrm{C}(\mathrm{Ext}_{\mathrm{rand}}, k) \leq \epsilon \quad \text{for} \quad m = k - 2\log(1/\epsilon) - O(1) \tag{71}$$

$$d = \log(n-k) + 2\log(1/\epsilon) + O(1)\ . \tag{72}$$

In contrast to this, we find that the SDP relaxation for random constructions can become very large for sufficiently small min-entropy k.

▶ **Theorem 8.** *Let* $\mathrm{Ext} = \{f_s\}_{s\in D}$ *be a family of functions such that*

$$\gamma_1 \frac{DN^2}{M} \leq \sum_{x,x',s} \delta_{f_s(x)=f_s(x')} \leq \gamma_2 \frac{DN^2}{M}\ , \tag{73}$$

and $k \leq \log\left(\gamma_1 \frac{N}{M}\right)$*. Then, we have*

$$\mathrm{SDP}(\mathrm{Ext}, k) \geq \frac{1}{2}\sqrt{\frac{M}{\gamma_2 D}}\ . \tag{74}$$

When the functions f_s are chosen at random, then the condition (73) is satisfied with very high probability for constant values of γ_1 and γ_2 (see Proposition 11 for a proof). Hence, we find that for instance if $k = n/2$, $m = n/4$ and $d = O(\log n)$, with high probability $\mathrm{SDP}(\mathrm{Ext}_{\mathrm{rand}}, k) \gg 2$, whereas we have with very high probability $\mathrm{C}(\mathrm{Ext}_{\mathrm{rand}}, k) \leq \frac{1}{n}$. As clearly $\mathrm{Q}(\mathrm{Ext}, k) \leq 2$, this also shows that Q can be much smaller than SDP.

Moreover we can show that for Trevisan's extractor, we cannot replace $\mathrm{Q}(\mathrm{Ext}_{\mathrm{Trev}})$ with $\mathrm{SDP}(\mathrm{Ext}_{\mathrm{Trev}}, k)$ in general in Theorem 7. This is because if the one-bit extractors $\{g_t\}$ in Trevisan's construction are chosen at random, then it is possible to show that the condition (73) is satisfied with high probability for constant values of γ_1 and γ_2 (see Proposition 11 for a proof).

Proof of Theorem 8. Use $\vec{a}_x = \alpha^{-1/2} \cdot \sum_{s,y} \delta_{f_s(x)=y} |s\rangle|y\rangle$, $\alpha = \sum_{x,x'} \sum_{s,y} \delta_{f_s(x)=y} \delta_{f_s(x')=y}$. By definition the normalization condition $\sum_{x,x'} \vec{a}_x \cdot \vec{a}_{x'} \leq 1$ is satisfied. Moreover, for any fixed x, x', we have

$$\vec{a}_x \cdot \vec{a}_{x'} = \frac{1}{\alpha} \sum_{s,y} \delta_{f_s(x)=y} \delta_{f_s(x')=y} \leq \frac{D}{\alpha} \leq \frac{1}{\gamma_1} \frac{M}{N^2} \leq \frac{1}{\gamma_1} \frac{M}{N} q(x)\ , \tag{75}$$

where we used the lower bound on γ_1 and we choose $q(x) = 1/N$. Now if $k \leq \log\left(\gamma_1 \frac{N}{M}\right)$, the min-entropy condition for the vectors is satisfied. Now let us analyze the objective function by choosing $\vec{b}_{s,y} = |s\rangle|y\rangle$. We find

$$\frac{1}{D} \sum_{s,y} \sum_{x} \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) \vec{a}_x \cdot \vec{b}_{s,y} = \frac{1}{D} \sum_{s,y} \sum_{x} \left(\delta_{f_s(x)=y} - \frac{1}{M}\right) \alpha^{-1/2} \delta_{f_s(x)=y} \tag{76}$$

$$= \frac{1}{D\alpha^{1/2}} \sum_{s,x} \left(1 - \frac{1}{M}\right) = \frac{N}{\alpha^{1/2}} \left(1 - \frac{1}{M}\right) \geq \frac{1}{2}\sqrt{\frac{M}{\gamma_2 D}}\ , \tag{77}$$

which proves the claim. ◀

5 Discussion

Theorem 8 shows limitations of the SDP relaxation presented here. In fact, even though the error of the extractor $\mathrm{C}(\mathrm{Ext}, k)$ and $\mathrm{Q}(\mathrm{Ext}, k)$ are clearly bounded by 2, the value $\mathrm{SDP}(\mathrm{Ext}, k)$ can be much larger. In [7], we present an improved SDP relaxation that has the property of always being bounded by 2. In addition, we propose a converging hierarchy of SDPs that gives increasingly tight characterizations of quantum-proof extractors.

Acknowledgments. We acknowledge discussions with Matthias Christandl, Fabian Furrer, Patrick Hayden, Christopher Portmann, Renato Renner, Oleg Szehr, Marco Tomamichel, Thomas Vidick, Stephanie Wehner, Reinhard Werner, and Andreas Winter. Part of this work was done while OF and VBS where visiting the Institute for Quantum Information and Matter at Caltech and we would like to thank John Preskill and Thomas Vidick for their hospitality. Most of this work was done while OF was at ETH Zurich supported by the the European Research Council grant No. 258932. Additional funding was provided by the EU under the project "Randomness and Quantum Entanglement" (RAQUEL). VBS was supported by an ETH postdoctoral fellowship.

References

1 Noga Alon, Sanjeev Arora, Rajsekar Manokaran, Dana Moshkovitz, and Omri Weinstein. Inapproximability of densest k-subgraph from average case hardness. Manuscript, available at `http://www.csc.kth.se/~rajsekar/papers/dks.pdf`, 2011.

2 Avraham Ben-Aroya and Amnon Ta-Shma. Better short-seed quantum-proof extractors. *Theoretical Computer Science*, 419:17–25, 2012.

3 Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. International Conference on Computers, Systems and Signal Processing*, 1984.

4 Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41:1915–1923, 1995.

5 Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM journal on Computing*, 17:210–229, 1988.

6 Mario Berta, Omar Fawzi, and Volkher B. Scholz. Quantum-proof randomness extractors via operator space theory. *arXiv preprint arXiv:1409.3563*, 2014.

7 Mario Berta, Omar Fawzi, and Volkher B. Scholz. Quantum bilinear programs. *arXiv preprint arXiv:1506.08810*, 2015.

8 Mario Berta, Omar Fawzi, Volkher B. Scholz, and Oleg Szehr. Variations on classical and quantum extractors. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1474–1478, 2014.

9 Aditya Bhaskara, Venkatesan Guruswami, Moses Charikar, Aravindan Vijayaraghavan, and Yuan Zhou. Polynomial integrality gaps for strong SDP relaxations of Densest k-subgraph. In *Proc. of the 23rd Annual ACM-SIAM Symp. on Discrete Algorithms (SODA'12)*, 2012.

10 R. Bhatia. *Matrix Analysis*. Springer, 1997.

11 Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors. *arXiv preprint arXiv:1402.4797*, 2014.

12 Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44:095305, 2011.

13 Matthew Coudron and Henry Yuen. Infinite randomness expansion and amplification with a constant number of devices. In *Proc. of the 46th Annual ACM Symp. on Theory of Computing*, STOC'14, pages 427–436. ACM, 2014.

14 A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41:915–940, 2012.

15 Uriel Feige and Michael Seltser. On the densest k-subgraph problem. *Algorithmica*, 29:2001, 1997.

16 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proc. of the 39th Annual ACM Symp. on Theory of Computing*, STOC'07, pages 516–525. ACM, 2007.

17 Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28:1364–1396, 1999.

18 R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. *Information Theory, IEEE Transactions on*, 57:4760–4787, 2011.

19 R. König and B. Terhal. The bounded-storage model in the presence of a quantum adversary. *Information Theory, IEEE Transactions on*, 54:749–762, 2008.

20 R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *Information Theory, IEEE Transactions on*, 58:1962–1984, 2012.

21 Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *arXiv preprint arXiv:1402.0489*, 2014.

22 Noam Nisan and Amnon Ta-Shma. Extracting randomness: a survey and new constructions. *Journal of Computer and System Sciences*, 58:148–173, 1999.

23 Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 51:43–52, 1996.

24 Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464:1021–1024, 2010.

25 J. Radhakrishnan and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics*, 13:2–24, 2000.

26 Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zurich, 2005.

27 Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer Berlin Heidelberg, 2005.

28 Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

29 Michael Sipser. Expanders, randomness, or time versus space. *Journal of Computer and System Sciences*, 36:379 – 383, 1988.

30 Oleg Szehr. Decoupling theorems. Master's thesis, ETH Zurich, 2011.

31 Amnon Ta-Shma. Extractors against classical and quantum adversaries. *Tutorial QCrypt*, 2013.

32 M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *Information Theory, IEEE Transactions on*, 57:5524–5535, 2011.

33 Luca Trevisan. Construction of extractors using pseudo-random generators (extended abstract). In *Proc. of the 31st Annual ACM Symposium on Theory of Computing*, STOC'99, pages 141–148. ACM, 1999.

34 Salil P. Vadhan. *Pseudorandomness.* Now Publishers Inc., Hanover, MA, USA, 2012.

35 Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: Or, true random number generation secure against quantum adversaries. In *Proc. of the 44th Annual ACM Symp. on Theory of Computing*, STOC'12, pages 61–76, New York, NY, USA, 2012. ACM.

A Useful Lemmas

▶ **Theorem 9** (Grothendieck's inequality). *For any real matrix $\{A_{ij}\}$, we have*

$$\max\left\{\sum_{i,j} A_{ij}\vec{a}_i\cdot\vec{b}_j : \|\vec{a}_i\|_2\le 1, \|\vec{b}_j\|_2\le 1\right\} \tag{78}$$

$$\le K_G\cdot\max\left\{\sum_{i,j} A_{ij}a_i b_j : a_i, b_j\in\mathbb{R}, |a_i|\le 1, |b_j|\le 1\right\}\ . \tag{79}$$

▶ **Theorem 10** (Chernoff bound). *Let $X_i\in\{0,1\}$ be independent and identically distributed random variables, and $\mu := \mathbf{E}\{\sum_i X_i\}$. Then, we have*

$$\mathbf{P}\left\{\sum_i X_i \ge (1+\delta)\mu\right\} \le \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu} \quad \textit{for any } \delta>0 \tag{80}$$

$$\mathbf{P}\left\{\sum_i X_i \le (1-\delta)\mu\right\} \le \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu} \quad \textit{for any } 0<\delta<1\ . \tag{81}$$

B Missing Proofs

Proof of Theorem 6. We start with the expression $\frac{1}{D}\sum_{s,y}\|\sum_x\left(\delta_{f_s(x)=y}-\frac{1}{M}\right)\vec{a}_x\|_2$ for the SDP, where the vectors $\vec{a}_x$ fulfill the conditions stated in (22). Using Cauchy-Schwarz, we may bound

$$\frac{1}{D}\sum_{s,y}\left\|\sum_x\left(\delta_{f_s(x)=y}-\frac{1}{M}\right)\vec{a}_x\right\|_2 \le \left(\frac{1}{D}\sum_{s,y}\left\|\sum_x\left(\delta_{f_s(x)=y}-\frac{1}{M}\right)\vec{a}_x\right\|_2^2\right)^{1/2} 2^{m/2}\ . \tag{82}$$

We now take a closer look at the expression in the brackets. Expanding the norm squared gives rise to the expression

$$\frac{1}{D}\sum_{s,y}\left(\sum_x\left(\delta_{f_s(x)=y}-\frac{1}{M}\right)\vec{a}_x\right)\cdot\left(\sum_{x'}\left(\delta_{f_s(x')=y}-\frac{1}{M}\right)\vec{a}_{x'}\right) \tag{83}$$

$$\begin{aligned}&=\frac{1}{D}\sum_{s,y}\left(\sum_x\delta_{f_s(x)=y}\vec{a}_x\right)\cdot\left(\sum_{x'}\delta_{f_s(x')=y}\vec{a}_{x'}\right)\\ &\quad-\frac{1}{D}\sum_{s,y}\frac{1}{M}\sum_{x,x'}\delta_{f_s(x)=y}\vec{a}_x\cdot\vec{a}_{x'}\\ &\quad-\frac{1}{D}\sum_{s,y}\frac{1}{M}\sum_{x,x'}\delta_{f_s(x')=y}\vec{a}_x\cdot\vec{a}_{x'}\\ &\quad+\frac{1}{D}\frac{1}{M^2}\sum_{s,y}\sum_{x,x'}\vec{a}_x\cdot\vec{a}_{x'}\ .\end{aligned} \tag{84}$$

Let us examine the cross terms:

$$\frac{1}{D}\sum_{s,y}\frac{1}{M}\sum_{x,x'}\delta_{f_s(x)=y}\vec{a}_x\cdot\vec{a}_{x'} = \frac{1}{D}\sum_s\frac{1}{M}\sum_{x,x'}\vec{a}_x\cdot\vec{a}_{x'}\ , \tag{85}$$

since for each fixed pair $s, x \in D \times N$ there is exactly one $y \in M$ such that $f_s(x) = y$. The second cross term evaluates analogously to the same value, which is also equal to the fourth term in the expansion of the norm, and hence we are left with

$$\frac{1}{D}\sum_{s,y}\left(\sum_x \delta_{f_s(x)=y}\vec{a}_x\right)\cdot\left(\sum_{x'}\delta_{f_s(x')=y}\vec{a}_{x'}\right) - \frac{1}{D}\sum_{s,y}\frac{1}{M}\left(\sum_x \vec{a}_x\right)\cdot\frac{1}{M}\left(\sum_{x'}\vec{a}_{x'}\right) . \tag{86}$$

Introducing the maps ψ_s and τ from $\ell_2(N)$ to $\ell_2(M)$,

$$\psi_s : \vec{e}_x \mapsto \sum_y \delta_{f_s(x)=y}\vec{e}_y \quad \text{and} \quad \tau : \vec{e}_x \mapsto \frac{1}{M}\sum_y \vec{e}_y \tag{87}$$

this may be written as

$$\frac{1}{D}\sum_s \psi_s(\vec{a})\cdot\psi_s(\vec{a}) - \tau(\vec{a})\cdot\tau(\vec{a}) , \tag{88}$$

where the dot now means taking the scalar product in the Hilbert space $\ell_2(M) \otimes \mathcal{H}$ and we set $\vec{a} = \sum_x \vec{e}_x \otimes \vec{a}_x \in \ell_2(N) \otimes \mathcal{H}$. However, this is up to a factor of $\frac{1}{D}$ exactly the defining expression of a spectral extractor. Hence we may bound

$$\frac{1}{D}\sum_s \psi_s(\vec{a})\cdot\psi_s(\vec{a}) - \tau(\vec{a})\cdot\tau(\vec{a}) \leq 2^k\frac{\epsilon}{M}\|\vec{a}\|^2 . \tag{89}$$

The last norm evaluates to

$$\|\vec{a}\|^2 = \sum_x \vec{a}_x\cdot\vec{a}_x \leq 2^{-k}\sum_x q(x) = 2^{-k} , \tag{90}$$

and comparison with (82) gives the desired bound. ◀

Proof of Theorem 7. Consider a feasible solution of (17) given by $\rho(x), \sigma, B_{s,y}$ all acting on a Hilbert space Q. The objective function can be written as

$$\begin{aligned}
&\frac{1}{2^d}\sum_{s,y,x}\left(\delta_{f_s(x)=y} - 2^{-m}\right)\mathrm{Tr}[\rho(x)\,B_{s,y}] \\
&= \frac{1}{2^d}\sum_{s,x}\sum_{y\in\{0,1\}}\left(\sum_{t=0}^{m-1}\frac{1}{2^{m-t-1}}\prod_{k=1}^{t+1}\delta_{f_s(x)_k=y_k} - \frac{1}{2^{m-t}}\prod_{k=1}^{t}\delta_{f_s(x)_k=y_k}\right)\mathrm{Tr}[\rho(x)\,B_{s,y}] \quad (91)\\
&= \sum_{t=0}^{m-1}\frac{1}{2^d}\sum_{s,x}\sum_{y_1,y_2,\dots y_{t+1}}\prod_{k=1}^{t}\delta_{f_s(x)_k=y_k}\left(\delta_{f_s(x)_{t+1}=y_{t+1}} - \frac{1}{2}\right)\mathrm{Tr}[\rho(x)\,C_{s,y_1,y_2,\dots,y_{t+1}}] ,
\end{aligned} \tag{92}$$

where we defined

$$C_{s,y_1,\dots,y_t,y_{t+1}} := \frac{1}{2^{m-t-1}}\sum_{y_{t+2},\dots,y_m\in\{0,1\}} B_{s,y_{t+2},\dots,y_m} . \tag{93}$$

We now start using the particular structure of the extractor in (68). From now, we fix the value of t and the dependence on t of many variables are omitted to lighten the notation. The seed s can be specified by $a = s|S_{t+1} \in \{0,1\}^l$ and $b = s|S_{t+1}^c \in \{0,1\}^{d-l}$ where S_{t+1}^c is the complement on S_{t+1} in the set $\{1,\ldots,d\}$. We will thus interchangeably use s and (a,b). Using this notation with the structure of f_s, we obtain

$$\frac{1}{2^d}\sum_{s,y,x}\left(\delta_{f_s(x)=y}-2^{-m}\right)\mathrm{Tr}[\rho(x)\,B_{s,y}]$$

$$=\sum_{t=0}^{m-1}\frac{1}{2^d}\sum_{\substack{x\\ a\in\{0,1\}^l\\ b\in\{0,1\}^{d-l}}}\ \sum_{y_1,y_2,\ldots y_{t+1}}\delta_{h_{x,b}(a)=y_1\ldots y_t}\left(\delta_{g_a(x)=y_{t+1}}-\frac{1}{2}\right)\mathrm{Tr}[\rho(x)\,C_{a,b,y_1,y_2,\ldots,y_{t+1}}] \tag{94}$$

$$=\sum_{t=0}^{m-1}\frac{1}{2^l}\sum_{\substack{x\\ a\in\{0,1\}^l}}\ \sum_{z\in\{0,1\}}\left(\delta_{g_a(x)=z}-\frac{1}{2}\right)\frac{1}{2^{d-l}}\sum_{b\in\{0,1\}^{d-l}}\mathrm{Tr}[\rho(x)\,C_{a,b,h_{x,b}(a),z}] \tag{95}$$

where $h_{x,b}(a)$ represents the first t bits of $f_s(x)$. Note that for a fixed x and b, the outcome of this function only depends on the bits of s that belong to one of the sets $S_1,\ldots,S_t$. In particular, the first bit of $h_{x,b}$ only depends on the substring of a corresponding to indices in $S_1\cap S_{t+1}$. Thus, for any x,b, the function $h_{x,b}$ belongs to the family $\mathcal{F}_t$ of functions $h:\{0,1\}^l\to\{0,1\}^t$ for which the j-th bit h^j of h is a function $h^j:\{0,1\}^{S_j\cap S_{t+1}}\to\{0,1\}$. Thus, for any x,b only $\sum_{j=1}^{t}2^{|S_j\cap S_{t+1}|}\leq r(m-1)$ bits are sufficient to fully describe the function $h_{x,b}$. As a result, $|\mathcal{F}_t|\leq 2^{r(m-1)}$.

Let us define new positive operators on a larger $Q\otimes H\otimes G$ system as

$$\hat{\rho}(x):=\frac{1}{2^{d-l}}\sum_{\substack{b\in\{0,1\}^{d-l}\\ h\in\mathcal{F}_t}}\rho(x)\otimes\delta_{h=h_{x,b}}|h\rangle\langle h|_H\otimes|b\rangle\langle b|_G \tag{96}$$

$$\hat{\sigma}:=\frac{1}{|\mathcal{F}_t|2^{d-l}}\sum_{\substack{b\in\{0,1\}^{d-l}\\ h\in\mathcal{F}_t}}\sigma\otimes|h\rangle\langle h|_H\otimes|b\rangle\langle b|_G \tag{97}$$

$$\hat{C}_{a,z}:=\sum_{b,h\in\mathcal{F}_t}C_{a,b,h(a),z}\otimes|h\rangle\langle h|\otimes|b\rangle\langle b|\ . \tag{98}$$

Note that $\hat{\sigma}$ as well as $\sum_x\hat{\rho}(x)$ have unit trace and $\|\hat{C}_{a,z}\|_\infty\leq 1$. In addition,

$$\hat{\rho}_x\leq\frac{1}{2^{d-l}}\sum_{\substack{b\in\{0,1\}^{d-l}\\ h\in\mathcal{F}_t}}\rho(x)\otimes|h\rangle\langle h|_H\otimes|b\rangle\langle b|_G\leq|\mathcal{F}_t|2^{-k}\hat{\sigma}\leq 2^{-k+r(m-1)}\hat{\sigma}\ , \tag{99}$$

where we used the fact that $\rho(x)\leq 2^{-k}\sigma$. This shows that the newly defined operators $\hat{\rho}(x),\hat{\sigma},\hat{C}_{a,z}$ satisfy the constraints of (17) for the extractor $\mathrm{Ext}_{\mathrm{one}}$ with min-entropy $k-r(m-1)$. Looking at the value of the objective function for this solution, we obtain

$$\frac{1}{2^l}\sum_{a,z,x}\left(\delta_{g_a(x)=z}-\frac{1}{2}\right)\mathrm{Tr}[\hat{\rho}(x)\hat{C}_{a,z}]=\frac{1}{2^l}\sum_{a,z,x}\left(\delta_{g_a(x)=z}-\frac{1}{2}\right)\mathrm{Tr}[\hat{\rho}(x)\hat{C}_{a,z}] \tag{100}$$

$$=\frac{1}{2^l}\sum_{a,z,x}\left(\delta_{g_a(x)=z}-\frac{1}{2}\right)\frac{1}{2^{d-l}}\sum_{b}\mathrm{Tr}[\rho(x)C_{a,h(a),z}]\ , \tag{101}$$

which is exactly the t-th term in the sum in (95). To relate $\mathrm{Q}(\mathrm{Ext}_{\mathrm{one}},k-r(m-1))$ to $\mathrm{C}(\mathrm{Ext}_{\mathrm{one}},k-r(m-1)-\log(1/\epsilon))+\epsilon$, we use Theorem 4 and Theorem 5. ◀

▶ **Proposition 11.** *Suppose the functions $f_s : N \to M$ from the family $\{f_s\}_{s \in D}$ are chosen at random with $f_s(x)$ and $f_{s'}(x')$ uniformly distributed and independent whenever $x \neq x'$. Then, we have for $N \geq 16$ that*

$$\mathbf{P}\left\{\left|\sum_{x,x',s} \delta_{f_s(x)=f_s(x')} - \left(DN + \frac{DN(N-1)}{M}\right)\right| \geq \frac{1}{2}\frac{DN(N-1)}{M}\right\} \leq \frac{1}{16} \; . \tag{102}$$

This of course includes the case when the functions f_s are chosen uniformly and independently, but also the case of Trevisan's construction where the one-bit extractor is a randomly chosen function.

Proof of Proposition 11. We start by separating the cases $x = x'$ and $x \neq x'$,

$$\sum_{x,x',s} \delta_{f_s(x)=f_s(x')} = DN + \sum_{s,x\neq x'} \delta_{f_s(x)=f_s(x')} \; . \tag{103}$$

We compute the expectation over the choice of f:

$$\mathop{\mathbf{E}}_{f}\left\{\sum_{s,x\neq x'} \delta_{f_s(x)=f_s(x')}\right\} = DN(N-1)\frac{1}{M} \; , \tag{104}$$

simply using the fact then for $x \neq x'$, $f_s(x)$ and $f_s(x')$ are independently chosen. We now would like to show that with high probability this random variable is close to its expectation. For that we compute the second moment

$$\mathop{\mathbf{E}}_{g}\left\{\left(\sum_{s,x\neq x'} \delta_{f_s(x)=f_s(x')}\right)^2\right\} \tag{105}$$

$$= \sum_{s_1,s_2,x_1\neq x_2,x'_1\neq x'_2} \mathbf{P}\left\{f_{s_1}(x_1) = f_{s_1}(x'_1), f_{s_2}(x_2) = f_{s_2}(x'_2)\right\} \tag{106}$$

$$= \sum_{s_1,s_2,x_1\neq x_2,x'_1\neq x'_2,\{x_1,x'_1\}\neq\{x_2,x'_2\}} \mathbf{P}\left\{f_{s_1}(x_1) = f_{s_1}(x'_1), f_{s_2}(x_2) = f_{s_2}(x'_2)\right\} \tag{107}$$

$$+ \sum_{s_1,s_2,x_1\neq x_2,x'_1\neq x'_2,\{x_1,x'_1\}=\{x_2,x'_2\}} \mathbf{P}\left\{f_{s_1}(x_1) = f_{s_1}(x'_1), f_{s_1}(x_2) = f_{s_1}(x'_2)\right\} \tag{108}$$

$$\leq D^2N(N-1)(N(N-1)-2)\frac{1}{M^2} \tag{109}$$

$$+ 2\sum_{s_1,s_2,x_1\neq x_2} \mathbf{P}\left\{f_{s_1}(x_1) = f_{s_1}(x'_1)\right\} \tag{110}$$

$$= D^2N(N-1)(N(N-1)-2)\frac{1}{M^2} + 2D^2N(N-1)\frac{1}{M} \; . \tag{111}$$

As a result the variance is at most

$$\mathbf{Var}\left\{\sum_{s,x\neq x'} \delta_{f_s(x)=f_s(x')}\right\} \tag{112}$$

$$\leq D^2N(N-1)(N(N-1)-2)\frac{1}{M^2} + 2D^2N(N-1)\frac{1}{M} - \left(DN(N-1)\frac{1}{M}\right)^2 \tag{113}$$

$$\leq 2D^2N(N-1)\frac{1}{M} \; . \tag{114}$$

Using Chebyshev's inequality gives with a standard deviation $\sigma \leq \sqrt{2}D\sqrt{N(N-1)/M}$ we have

$$\mathbf{P}\left\{\left|\sum_{s,x\neq x'}\delta_{f_s(x)=f_s(x')}-\frac{DN(N-1)}{M}\right|\geq 4\sigma\right\}\leq\frac{1}{16}\ . \tag{115}$$

But $4\sigma \leq 4\sqrt{2}D\sqrt{N(N-1)/M} \leq \frac{1}{2}\frac{DN(N-1)}{M}$ for $N \geq 16$. ◀

New Constructions for Quantum Money

Marios Georgiou[1] and Iordanis Kerenidis[2]

1 The Graduate Center of the City University of New York
365 5th Avenue, New York, NY 10016, US
mgeorgiou@gradcenter.cuny.edu

2 CNRS-LIAFA-University Paris 7 Diderot
Batiment Sophie Germain, 8 Place FM/13, Paris 75013, France
jkeren@liafa.univ-paris-diderot.fr

Abstract

We propose an information theoretically secure secret-key quantum money scheme in which the verification of a coin is classical and consists of only one round; namely, a classical query from the user to the bank and an accept/reject answer from the bank to the user. A coin can be verified polynomially (on the number of its qubits) many times before it expires. Our scheme is an improvement on Gavinsky's scheme [5], where three rounds of interaction are needed and is based on the notion of quantum retrieval games.

Moreover, we propose a public-key quantum money scheme which uses one-time memories as a building block and is computationally secure in the random oracle model. This construction is derived naturally from our secret-key scheme using the fact that one-time memories are a special case of quantum retrieval games.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Quantum Money, Quantum Cryptography, Quantum Retrieval Games

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.92

1 Introduction

Wiesner [15] in the early '80s proposed the idea of creating money whose unforgeability is guaranteed by the laws of quantum mechanics. Quantum states seemed an ideal way to encode money, since the no-cloning theorem of quantum states could possibly lead to a no-cloning theorem of money.

Informally, a quantum money scheme consists of two main processes; a process Bank that creates valid coins and a process Ver that verifies whether a coin is valid. The use of such a scheme is straightforward; the authorized bank will produce valid money by running the process Bank and the users will be able to pay each other and verify that a coin \$ is valid by running the process Ver(\$).

In Wiesner's construction a coin consists of several BB84 states (that form a big state ρ) together with a classical identification string s. The verification of the coin (ρ, s) is a simple one round protocol in which the user of a coin sends the full coin to the bank and the bank replies with a yes/no answer. The answer of the bank depends on its secret key (which corresponds to s) as well as the outcomes it gets by applying a measurement on the computational or Hadamard basis to ρ. These kinds of schemes are known as (secret-key) *quantum money with quantum verification* since the user has to communicate quantumly with the bank.

Until recently, the question of whether there exist quantum money schemes where the verification protocol consists only of classical communication was open. Gavinsky [5] answered this question in the affirmative by creating the first *secret-key quantum money scheme with classical verification.* His scheme makes use of a new quantum cryptographic idea, that of *quantum retrieval games* (QRGs) and its security is information theoretic. However, a clear drawback in contrast to Wiesner's scheme is that the verification of a coin consists of three rounds of interaction between the user and the bank, thus forcing the bank to maintain a temporary memory for each verification session. In 2013 Molina et al. [11] proposed a new quantum money scheme with classical verification. In this scheme two rounds (four messages) are needed for the verification of a coin. Moreover, a drawback of the scheme is that it requires the bank to be stateful and keep track of which coin belongs to which user.

In 2012, Aaronson and Christiano [1] proposed the idea of *public-key quantum money* where no communication with the bank is needed in order to verify the coin. In such a scheme, although information theoretic security is impossible, computationally secure schemes may still exist. Classically, it is impossible to create public key money schemes since, in that case, a coin would consist only of a bitstring and, therefore, the copy of a coin would be trivial. Public-key quantum money are essentially the optimal kind of money we could hope for since they can be used as ordinary cash. Although some schemes have been proposed as candidates for public-key quantum money [1, 4], all of them are based on non-standard computational hardness conjectures. Moreover, recently one of the two schemes proposed in [1] was cryptanalyzed by Pena et al. [14].

Our contributions are twofold. First, we give the first information theoretically secure quantum money scheme that requires only classical communication with the bank, tolerates errors and the verification consists of a single round, a query to the bank and an answer. The important contribution of this scheme compared to that of Gavinsky [5] is that in the latter, the verification requires a three-round interaction with the bank and, therefore, the bank has to maintain a temporary session memory. Moreover, we have made the proof more modular and conceptually simpler by introducing a new cryptographic primitive as tool for the security analysis.

Second, we create a public-key quantum money scheme from one-time memories in the random oracle model. Considering hash functions as random oracles is a common tool for the security proofs of cryptographic schemes which is invoked when standard properties of hash functions (such as collision resistance) are not enough. Briefly, a hash function behaves as a random oracle if on each query it returns a uniformly random element in its range, being in the same time consistent with the previous queries; e.i. on the same query it returns the same answer.

One-time memories are a very natural special case of quantum retrieval games and, thus, our public-key construction is a simple modification of our secret-key scheme. In our construction we also make use of the notion of a quantum money mini-scheme proposed by Aaronson and Christiano [1] (see subsection 2.2). A clear advantage of this scheme compared to other works in the literature [3, 7, 12] is the direct application of one-time memories to quantum money without going through one-time programs and this makes our scheme more efficient. In both our schemes the number of allowed verifications is polynomial on the size of the coins. Our contributions, compared to previous work are summarized in Table 1.

The paper is structured as follows; in section 2 we give the definitions of secret-key and public-key quantum money as well as the corresponding secret-key and public-key mini-schemes. In section 3 we give the necessary tools for the security analysis of our schemes. Last, in sections 4 and 5 we present our secret-key and public-key constructions respectively.

Table 1 Comparison between different quantum money schemes. The "Verif." column indicates whether the interaction of the verification protocol is Quantum or Classical, the "#Ver." column indicates the number of verifications allowed before the coin expires, where n is the number of qubits of the coin and the "Rounds" column indicates the number of rounds of interaction needed in order to verify a coin.

Scheme	Key	Verif.	Security	#Ver.	Rounds
[15]	Secret	Quantum	cryptanalyzed [13, 11]	$\exp(n)$	1
[5]	Secret	Classical	Information theoretic	$\mathrm{poly}(n)$	3
[11]	Secret	Classical	Information theoretic	$\mathrm{poly}(n)$	2
Ours	Secret	Classical	Information theoretic	$\mathrm{poly}(n)$	1
[1] (noise-free)	Public	–	cryptanalyzed [14]	$\exp(n)$	–
[1] (noisy)	Public	–	conj. on polynomials	$\exp(n)$	–
[4]	Public	–	conj. on knots	$\exp(n)$	–
Ours	Public	–	security of OTM	$\mathrm{poly}(n)$	–

2 Quantum Money Definitions

In this section we give the definitions for quantum money. We first define secret-key quantum money schemes where there is a verification protocol run between a user and the bank in order to verify a coin. We give a definition of secret-key quantum money mini-schemes, and claim that there is a direct way to go from a mini-scheme to a full scheme [5], similar to the public-key case [1]. Then, we give the definition proposed by Aaronson and Christiano [1] of a public-key quantum money scheme as well as the mini-scheme and we state their *standard construction* theorem that makes a full public-money scheme out of a mini-scheme using signatures.

2.1 Secret-key Quantum Money

Informally, a secret-key quantum money scheme consists of an algorithm that is used by the bank in order to create valid coins, and a protocol that is run between a holder of a coin and the bank in order for the holder to verify that the coin is valid. The security requirement states that it is impossible for an algorithm to create more coins than what it had in the beginning.

▶ **Definition 1** (Secret-key Quantum Money). A quantum money scheme with classical verification consists of an algorithm Bank and a verification protocol Ver such that

1. $\mathrm{Bank}(1^n) = \$ = (\rho, \mathrm{sn})$ is the algorithm that creates a quantum coin \$ where ρ is a quantum state and sn is a classical serial number.
2. Ver is a protocol with classical communication, run for a coin \$, between a holder H of a number of coins and the bank B. The final message of this protocol is a bit b sent by the bank, that corresponds to whether the coin is valid or not. Denote by $\mathrm{Ver}_H^B(\$)$ this final bit.

- Correctness: The scheme is correct if for every honest holder H, $\Pr[\mathrm{Ver}_H^B(\mathrm{Bank}(1^n)) = 1] = 1 - \mathrm{negl}(n)$.
- Security: The scheme is secure if for any quantum adversary $\mathcal{F}$ who possesses q coins, interacts at most t times with the bank and finally produces q' coins $\$_1, \cdots, \$_{q'}$ it holds

that

$$\Pr\left[\left(\bigwedge_{i\in[q']} \mathrm{Ver}_H^B(\$_i)=1\right)\wedge(q'>q)\right]\leq \mathrm{poly}(t)\cdot\mathrm{negl}(n)$$

where H is any honest holder.

In general, the security parameter n corresponds to the number of qubits a valid coin consists of. Note that, although the adversary $\mathcal{F}$ may deviate from the verification protocol in an attempt to create more coins, these coins will be checked for validity by an honest holder who will correctly follow the protocol. Note that the previous definition gives information theoretic security; the adversary $\mathcal{F}$ is not restricted to be computationally efficient.

As studied by Aaronson and by Gavinsky, it is enough to prove the security of a smaller scheme (*mini-scheme*) in order to guarantee security of the full scheme. In the mini-scheme, the adversary $\mathcal{F}$ possesses only one coin \$ and interacts t times with the bank in order to create two coins. Therefore, the security game of the mini-scheme is as before, but the adversary is allowed to run Ver only for its unique coin \$. In this case where the verification includes interaction with the bank, note that the coin does not need to have a classical serial number.

▶ **Definition 2** (Secret-key Quantum Money Mini-Scheme). A quantum money mini-scheme with classical verification consists of an algorithm Bank and a verification protocol Ver such that

1. $\mathrm{Bank}(1^n)=\$=\rho$ is the algorithm that creates a quantum coin \$ where ρ is a quantum state.
2. Ver is a classical protocol, run between a holder H of \$ and the bank B. The final message of this protocol is a bit $b\in\{0,1\}$ sent by the bank, that corresponds to whether the coin is valid or not. Denote by $\mathrm{Ver}_H^B(\$)$ this final bit.

- Correctness: The scheme is correct if for every honest holder H, $\Pr[\mathrm{Ver}_H^B(\mathrm{Bank}(1^n))=1]=1-\mathrm{negl}(n)$.
- Security: The scheme is secure if for any quantum adversary $\mathcal{F}$ who interacts at most t times with the bank and finally produces two coins $\$_1,\$_2$ it holds that

$$\Pr\left[\left(\mathrm{Ver}_H^B(\$_1)=1\wedge\mathrm{Ver}_H^B(\$_2)=1\right)\right]\leq\mathrm{poly}(t)\cdot\mathrm{negl}(n)$$

where H is any honest holder.

In order to go from a secret-key quantum money mini-scheme to a full scheme, it is enough for the bank to add a serial number to a coin of the mini-scheme. Then, consulting that serial number the bank can run the verification protocol of the mini-scheme for that coin.

▶ **Lemma 3** (Mini-scheme to full scheme [5]). *There exists a secure secret-key quantum money full scheme with classical verification if and only if there exists a secure secret-key quantum money mini-scheme with classical verification.*

2.2 Public-key Quantum Money

We now give the definition of a public-key quantum money scheme [1]. In this case we have three algorithms; one that creates a public key and a secret key, one that uses the secret key to create coins, and one that uses the public key to verify that a coin is valid.

▶ **Definition 4** (Quantum Money [1]). A public-key quantum money scheme M consists of three algorithms:

1. $\mathrm{KeyGen}(1^n) = (\mathrm{sk}, \mathrm{pk})$ that returns a secret key sk and a public key pk.
2. $\mathrm{Bank}(\mathrm{sk}) = \$$ a randomized algorithm that takes as input the secret key and returns a coin \$.
3. $\mathrm{Ver}(\mathrm{pk}, \$) = 0/1$ that takes as input the public key pk, and a potential coin \$ and either accepts or rejects.

- Correctness: M is correct if for a pair $(\mathrm{sk}, \mathrm{pk})$ that is output of KeyGen it holds that

$$\mathrm{Ver}(\mathrm{pk}, \mathrm{Bank}(\mathrm{sk})) = 1 - \mathrm{negl}(n)$$

- Security: M is secure if for any polynomial time quantum adversary $\mathcal{F}$ that takes as input the public key pk and q valid coins $\$_1, \cdots, \$_q$ and outputs q' potential coins $\$'_1, \cdots, \$'_{q'}$ it holds that

$$\Pr\left[\left(\bigwedge_{i\in[q']} \mathrm{Ver}(\mathrm{pk}, \$'_i) = 1\right) \wedge (q' > q)\right] = \mathrm{negl}(n)$$

Here, n is the security parameter of the scheme and corresponds to the number of bits of sk as well as the number of qubits of each coin.

Now, as before, we give the notion of public key mini-schemes. A mini-scheme consists only of an algorithm that creates a coin and an algorithm that verifies a coin. Here the coin is of the form (s, ρ) where s is a classical string and ρ is a quantum state. Although anyone can create a coin that passes the verification test (the creation algorithm is public), the security property states that no algorithm that takes a coin with serial number s can create an extra valid coin with the same serial s.

► **Definition 5** (Quantum Money mini-scheme [1])**.** A public-key quantum money mini-scheme M consists of two algorithms:

1. $\mathrm{Bank}(1^n) = \$ = (s, \rho)$ a randomized algorithm that returns a coin \$, where s is a classical serial number and ρ is a quantum state.
2. $\mathrm{Ver}(\$) = 0/1$ that takes as input a potential coin \$ and either accepts or rejects.

- Correctness: M is correct if it holds that $\mathrm{Ver}(\mathrm{Bank}(1^n)) = 1$
- Security: M is secure if for any polynomial time quantum adversary $\mathcal{F}$ that takes as input a coin (s, ρ) and outputs two quantum states ρ_1, ρ_2 it holds that

$$\Pr\left[(\mathrm{Ver}(s, \rho_1) = 1 \wedge \mathrm{Ver}(s, \rho_2) = 1)\right] = \mathrm{negl}(n)$$

Here, n corresponds to the number of qubits of ρ.

The tool that Aaronson and Christiano use in order to go from a public money mini-scheme to a full scheme is digital signatures that are secure against quantum adversaries.

► **Definition 6.** A signature scheme S consists of three algorithms:

1. $\mathrm{KeyGen}(1^n) = (\mathrm{sk}, \mathrm{pk})$ that returns a secret key sk and a public key pk.
2. $\mathrm{Sign}(\mathrm{sk}, m) = s$ that takes as input a secret key and a message m and returns its signature s.
3. $\mathrm{Ver}(\mathrm{pk}, m, s) = 0/1$ that takes as input the public key pk, a message m and a potential signature s and either accepts or rejects.

- Correctness: S is correct if for a pair $(\mathrm{sk}, \mathrm{pk})$ that is output of KeyGen it holds that

$$\mathrm{Ver}(\mathrm{pk}, m, \mathrm{Sign}(\mathrm{sk}, m)) = 1$$

- Security: The security of S is defined by the following game between a Challenger $\mathcal{C}$ and an adversary $\mathcal{F}$. $\mathcal{C}$ runs $\mathrm{KeyGen}(1^n)$ and creates a pair $(\mathrm{sk}, \mathrm{pk})$ and gives pk to $\mathcal{F}$. $\mathcal{F}$ picks messages $m_1, \cdots, m_q$ of its choice and gives them to $\mathcal{C}$. $\mathcal{C}$ using sk signs these messages and replies with their signatures $s_1, \cdots, s_q$. Finally, $\mathcal{F}$ outputs a message-signature pair (m^*, s^*) and wins if this pair is different from all other pairs (m_i, s_i) for all $i \in [q]$ and if $\mathrm{Ver}(\mathrm{pk}, m^*, s^*) = 1$. S is existentially unforgeable under non-adaptive chosen message attacks if for every polynomial time quantum adversary $\mathcal{F}$ it holds that $\Pr[\mathrm{Ver}(\mathrm{pk}, m^*, s^*) = 1] = \mathrm{negl}(n)$.

Here, n is the security parameter of the scheme and corresponds to the number of bits of sk.

▶ **Theorem 7** (Standard Construction [1]). *If there exists a secure public-key quantum money mini-scheme and if there exists an existentially unforgeable under non-adaptive chosen message attacks signatures scheme, then there exists a secure public-key quantum money scheme.*

Briefly, in this standard construction, a full coin consists of a coin from the mini-scheme combined with a signature of its serial number.

In the following, therefore, we focus on constructing a secret-key and a public-key mini-scheme and these can be extended to full schemes using the previous constructions.

3 Tools for security analysis

In this section we define an important tool towards the construction of quantum money, that of *quantum retrieval games* (QRG). From a QRG we go through some intermediate notions of QRG that are more convenient for our money schemes and prove the equivalence between them.

3.1 Quantum Retrieval Games

Suppose that we have an encoding function that takes as input a classical string x and gives as output an encoding $\widetilde{\rho}_x$, which in the quantum case is a mixed quantum state. Suppose, furthermore, that x is chosen from some distribution and is described by a random variable X. How easy is it for an algorithm that takes as input only $\widetilde{\rho}_x$ to answer a question about x? A good way to formalize this question is via a relation σ. Then, we would like to know how well an optimal algorithm can find an answer a such that $(x, a) \in \sigma$. For example, σ could be the identity ($(x, a) \in \sigma$ if and only if $x = a$) or a function g ($(x, a) \in \sigma$ if and only if $a = g(x)$). In the most general setting σ is a relation and therefore there are several valid answers. Informally, in a quantum retrieval game, an algorithm takes as input $\widetilde{\rho}_x$ and wants to find an answer for x. In order to succeed in this, it has to find the best decoding procedure that, when applied to $\widetilde{\rho}_x$, will give a valid answer. In the quantum case, the best decoding procedure corresponds to the best measurement of the state $\widetilde{\rho}_x$ and the probability that this best measurement will give a valid answer is called the *physical value* of the game.

Note that if $\widetilde{\rho}_x$ is a mixed quantum state it holds that $\mathrm{Tr}[\widetilde{\rho}_x] = 1$. By defining $\rho_x = \Pr[X = x] \cdot \widetilde{\rho}_x$ we can integrate the randomness of x into the state ρ_x. Note that $\rho_x \succeq 0$, $\mathrm{Tr}[\rho_x] \leq 1$, $\Pr[X = x] = \mathrm{Tr}[\rho_x]$ and $\mathrm{Tr}[\sum_x \rho_x] = \mathrm{Tr}[\sum_x \Pr[X = x] \cdot \widetilde{\rho}_x] = \sum_x \Pr[X = x] \cdot \mathrm{Tr}[\widetilde{\rho}_x] = 1$.

It is common to call the string x a *secret* that takes values from a set of secrets S, a a potential *answer* that takes values from a set of answers A and ρ_x the quantum state that is the encoding of x. A decoding procedure is a general measurement on the state ρ_x with operators $\{m_a\}_{a \in A}$, each one corresponding to a possible answer.

$$\begin{aligned} &\text{maximize} && \sum_{(x,a)\in\sigma} \langle m_a, \rho_x\rangle \\ &\text{subject to} && \sum_{a\in A} m_a = I \\ & && m_a \succeq 0 \qquad \forall a \in A \end{aligned}$$

Figure 1 Physical value.

$$\begin{aligned} &\text{maximize} && \frac{\sum_{(x,a)\in\sigma} \langle m_a, \rho_x\rangle}{\sum_{x,a} \langle m_a, \rho_x\rangle} \\ &\text{subject to} && \sum_{a\in A} m_a \preceq I \\ & && m_a \succeq 0 \qquad \forall a \in A \end{aligned}$$

Figure 2 Selective value.

▶ **Definition 8** (Quantum Retrieval Games [5]). Let $S, A \subseteq \mathbb{N}$, $\sigma \subseteq S \times A$ and $\forall x \in S$ let $\rho_x \succeq 0$ such that $\mathrm{Tr}[\sum_{x\in S} \rho_x] = 1$. Then the tuple $G = (S, A, \{\rho_x\}_{x\in S}, \sigma)$ is called a quantum retrieval game (QRG). The physical value of G is denoted by $\mathrm{PVal}(G)$ and is the maximum probability of correctly decoding a state; i.e. producing an answer $a \in A$ such that $(x, a) \in \sigma$ (where the probability is taken over the randomness of x and the randomness of the decoding procedure).

The physical value of a game can be expressed as the solution of the semidefinite program of Figure 1. In several cases we are interested in an upper bound of the physical value of a game. Towards this, it is convenient to define the *selective value* of the game $\mathrm{SVal}(G)$ which describes the best decoding probability when the measurements $\{m_a\}_{a\in A}$ satisfy the property: $\sum_{a\in A} m_a \preceq I$. In other words, the selective value of the game corresponds to the solution of the relaxation of the SDP of the physical value (Figure 2) and in general it is not achievable, yet easier to manipulate. It is clear that the selective value of a game is always greater or equal to its physical value and, thus, an upper bound of the selective value gives also an upper bound of the physical value. The following theorem by Pastawski et al. [16] suggests an easy way to compute the selective value of a game.

▶ **Theorem 9** (Selective Value [16]). *Let $G = (S, A, \{\rho_x\}_{x\in S}, \sigma)$ be a* QRG *and let $\rho = \sum_{x\in S} \rho_x$. If ρ is invertible then* $\mathrm{SVal}(G) = \max_a \|O_a\|$, *where $O_a = \sum_{x:(x,a)\in\sigma} \rho^{-1/2}\rho_x\rho^{-1/2}$ and $\|\cdot\|$ denotes the operator norm.*

This equality is useful since it is possible to find the selective value of a game without going through any specific measurement.

In the case we want to play a big QRG that consists of playing in parallel many small QRGs, it is useful to know what happens to the physical value of that big game. The following lemma states that the selective value of such a game is multiplicative and therefore the probability of winning all the QRGs drops exponentially fast on the number of small games.

▶ **Lemma 10** (Parallel Repetition [16]). *Let $G_1 = (S_1, A_1, \{\rho_{1x_1}\}_{x_1\in S_1}, \sigma_1)$ and $G_2 = (S_2, A_2, \{\rho_{2x_2}\}_{x_2\in S_2}, \sigma_2)$ be two* QRG*s. Let also $S = S_1 \times S_2$, $A = A_1 \times A_2$, $\rho_{x_1x_2} = \rho_{1x_1} \otimes \rho_{2x_2}$ and $(x_1x_2, a_1a_2) \in \sigma$ if and only if $(x_1, a_1) \in \sigma_1$ and $(x_2, a_2) \in \sigma_2$. Then for the game $G = (S, A, \{\rho_{x_1x_2}\}_{(x_1,x_2)\in S}, \sigma)$ it holds that* $\mathrm{SVal}(G) = \mathrm{SVal}(G_1) \cdot \mathrm{SVal}(G_2)$.

Let M_1, M_2 be the solutions that optimize the selective value for the games G_1, G_2 respectively. Then the previous equality states that the optimal solution for the product game G is just the product of the two solutions. This provides an upper bound on the physical value of the product game G, which is the product of the selective values of the games G_1, G_2. It is clear that by taking the product of n games with constant selective value ϵ, we can create a game whose physical value is at most ϵ^n.

For the construction of our money scheme, it is useful to define another notion of a QRG, that of 1-out-of-2 QRG. Here, an algorithm is given as before a state ρ_x, but now two relations σ_a, σ_b. The basic property that we expect from such a game is that it should be impossible for any quantum algorithm (quantum measurement), to answer with high probability both relations correctly, but it is still possible to answer correctly one of them.

▶ **Definition 11** (1-out-of-2 QRG)**.** For a set of secrets S, set of answers A, and two relations σ_a, σ_b we define: $G_a = (S, A, \{\rho_x\}_{x\in S}, \sigma_a)$, $G_b = (S, A, \{\rho_x\}_{x\in S}, \sigma_b)$, $G_c = (S, A \times A, \{\rho_x\}_{x\in S}, \sigma)$ where $(x, (a, b)) \in \sigma$ if and only if $(x, a) \in \sigma_a$ and $(x, b) \in \sigma_b$. We say that $G = (S, A, \{\rho_x\}_{x\in S}, \sigma_a, \sigma_b, \sigma)$ is an $\varepsilon - \binom{2}{1}$QRG if it satisfies the following properties:

1. Correctness: There exist measurements $M^{(a)}, M^{(b)}$ such that $(M^{(a)}(\rho_x), x) \in \sigma_a$ and $(M^{(b)}(\rho_x), x) \in \sigma_b$. Equivalently: $\mathrm{PVal}(G_a) = \mathrm{PVal}(G_b) = 1$
2. Security: $\mathrm{PVal}(G_c) \leq \varepsilon$
3. Independence: Each answer in σ_b is independent of the set of answers in σ_a. Formally, let S_a be the random variable containing all answers in σ_a and let B be the random variable of any answer in σ_b. Then for any set of answers $A' \subseteq A$ and any answer $b \in A$, it holds that
$$\Pr[S_a = A' \wedge B = b] = \Pr[S_a = A'] \cdot \Pr[B = b]$$
where the probability is taken over the randomness of the secret x. Symmetrically, each answer in σ_a is independent of the set of answers in σ_b.

In the independence property note that the two sets of answers for the two relations are not necessarily mutually independent, therefore knowing all answers to σ_a may give the adversary an advantage if he wants to find more than one answer to σ_b. This property will be useful for a technical part of our proof below. We will call a $\binom{2}{1}$QRG secure if $c = 1 - \mathrm{negl}(n)$ and $\varepsilon \leq \mathrm{negl}(n)$ where n is the size of the secret x.

Theoretically, it is possible to create games with perfect correctness. However, in practice it is reasonable to assume that errors may occur and therefore, the correctness may not be guaranteed. In this case, we can assume that the games G_a and G_b cannot be answered correctly with probability 1 but only with a constant probability $c < 1$. Then, we can define an 1-out-of-2 game as $(c, \varepsilon) - \binom{2}{1}$QRG where ε is again the security of the scheme. We can show that if we repeat such a game n times, we can create a $(c', \varepsilon') - \binom{2}{1}$QRG where c' is now exponentially close to 1 and ε' is exponentially close to 0.

▶ **Lemma 12.** *Let c, ε, δ be positive constants such that $\delta = \frac{2c-\varepsilon-1}{3}$. If there exists a $(c, \varepsilon) - \binom{2}{1}$QRG G, then there exists a $\left(1 - e^{-\frac{cn}{2}\delta^2}, e^{-\frac{\varepsilon n}{3}\delta^2}\right) - \binom{2}{1}$QRG G'.*

Note that even though the original "small" game may have a considerably large error probability, we can achieve a quantum retrieval game that tolerates the errors with probability exponentially close to 1.

3.2 QRGs with Verification

We now define a new version of QRG, that of QRG *with verification* ($\binom{2}{1}$QRGv) that is useful for the construction of our money schemes. Informally, in a $\binom{2}{1}$QRGv, an adversary has some extra help for finding an answer to σ_a and σ_b; he is allowed to ask multiple queries of whether an answer is correct for a relation. What we require from such a game, is that the winning probability of any such adversary does not increase more than polynomially on the number of queries it asks.

▶ **Definition 13** ($\binom{2}{1}$QRGv)**.** Let $G = (S, A, \{\rho_x\}_{x\in S}, \sigma_a, \sigma_b, \sigma)$ be a $(c, \varepsilon) - \binom{2}{1}$QRG. We define the following game G between an adversary $\mathcal{F}$ and an algorithm $\mathcal{C}$. $\mathcal{C}$ prepares a normalized state $\rho_x / \mathrm{Tr}[\rho_x]$ of the game G and gives it to $\mathcal{F}$. Then $\mathcal{F}$ is allowed to interact with $\mathcal{C}$ at most t times in the following way:

1. $\mathcal{F}$ picks a $\sigma' \in \{\sigma_a, \sigma_b\}$, generates an answer d and sends (σ', d) to $\mathcal{C}$.
2. $\mathcal{C}$ returns 1 if and only if $(x, d) \in \sigma'$.

After t interactions $\mathcal{F}$ outputs (a_1^*, a_2^*) and wins if and only if $(x, (a_1^*, a_2^*)) \in \sigma$. We say that G is a $(c, \varepsilon) - \binom{2}{1}$ quantum retrieval game with verification ($\binom{2}{1}$QRGv) if it satisfies the following properties:

1. Correctness: Given any state $\rho_x/\mathrm{Tr}[\rho_x]$ the probability of answering σ_a (or σ_b) is at least c.
2. Soundness: For any t and for any adversary $\mathcal{F}$ interacting the way defined above, it holds that $\Pr[\mathcal{F} \text{ wins}] \leq \mathrm{poly}(t) \cdot \varepsilon$

We would like to argue the following: allowing such an adversary $\mathcal{F}$ to check whether a query (σ', d) is correct, does not increase considerably his probability of winning. Therefore, for an exponentially small ε an adversary would require a superpolynomial number of such interactions in order to have a non-negligible probability of winning. Towards this, we define below a more restricted version of the game and we show that this definition is equivalent to that of a $\binom{2}{1}$QRGv.

We now restrict the adversary $\mathcal{F}$ in the following manner. Suppose that $\mathcal{F}$ is allowed to interact with $\mathcal{C}$ as previously and the i-th interaction is the first interaction when he sends to $\mathcal{C}$ some (σ', a) such that $(x, a) \in \sigma'$ (without loss of generality we can assume that $\sigma' = \sigma_a$). Then, for the remaining $t - i$ interactions $\mathcal{F}$ is allowed to play only with σ_b. We call this game a *restricted* 1-out-of-2 quantum retrieval game with verification ($\binom{2}{1}$rQRGv) and the adversary $\mathcal{F}$ a restricted adversary. It can be proven that since finding an answer for σ_a is independent from any answer of σ_b, these two games are equivalent. In other words, allowing the adversary to succeed in more than one interaction with the same relation σ' does not help him win the game more than succeeding only once for σ'.

► **Lemma 14.** *Let $G = (S, A, \{\rho_x\}_{x\in S}, \sigma_a, \sigma_b, \sigma)$ be a $(c, \varepsilon) - \binom{2}{1}$QRGv. Then G is also a $(c, \varepsilon) - \binom{2}{1}$rQRGv.*

Using the previous lemma we can show that an adversary that is allowed to ask at most t queries regarding the relations σ_a, σ_b does not increase significantly his probability of winning. More specifically, it can be shown that if the original $\binom{2}{1}$QRG has security ε then allowing interaction, increases the winning probability at most quadratically in t.

► **Theorem 15.** *If there exists a $(c, \varepsilon) - \binom{2}{1}$QRG G' then there exists a $(c, \varepsilon) - \binom{2}{1}$QRGv G. In particular, any adversary against G has winning probability of at most $4t^2 \cdot \varepsilon$, where t is the number of queries.*

3.3 One-time Memories

For the creation of our public-key scheme we will use the notion of one-time memories (OTM) defined by Goldwasser et al in [7]. OTM are essentially devices which contain two secrets x_a, x_b, however, we are able to extract only one of these secrets. There is a very natural connection between $\binom{2}{1}$QRG and OTMs as we will see below.

► **Definition 16.** A $(c, \varepsilon)-$one-time memory (OTM) is a device that has the following behavior. Suppose that the device is programmed with two n-bit messages x_a, x_b chosen from some distribution D. Then:

1. Correctness: There exists an honest strategy $M^{(a)}$ that interacts with the device and recovers the message x_a with probability c. Likewise, there is an honest strategy $M^{(b)}$ that interacts with the device and recovers the message x_b with probability c.

2. Security: For any strategy M, if X is the random variable corresponding to the classical output of M, then $\Pr[X = (x_a, x_b)] \leq \varepsilon$.

We will call the OTM secure if $c = 1 - \text{negl}(n)$ and $\varepsilon = \text{negl}(n)$.

Note that in this paper, we deal with quantum OTM, namely the "device" is a quantum state ρ_{x_a,x_b}. Although secure OTM are impossible in the plain quantum model even with computational assumptions, Liu [8, 9, 10] has shown that OTM are possible in the isolated qubits model, where an adversary can use only local operations and classical communication. His OTM construction is a quantum state that consists of qubits that do not need to be entangled and thus it is easier and more efficiently implementable.

It is not hard to see that OTM are equivalent to $\binom{2}{1}$QRG restricted so that the relations σ_a, σ_b are, in fact, functions.

▶ **Lemma 17.** *There exists a secure* $\binom{2}{1}$QRG $G = (S, A, \{\rho_x\}_{x\in S}, \sigma_a, \sigma_b, \sigma)$ *such that the relations* σ_a, σ_b *are functions if and only if there exists a secure* OTM.

Proof. Using G we can create an OTM with secrets $x_a = \sigma_a(x)$ and $x_b = \sigma_b(x)$. The OTM device is simply ρ_x. Clearly, if there exists an algorithm that can retrieve both secrets from the OTM then this algorithm can also break G. For the opposite direction, the role of the encoding ρ_x is played by the OTM device, which is a quantum state. The secret x of G is defined as the concatenation of x_a and x_b and the functions σ_a, σ_b are defined such that $\sigma_a(x_a|x_b) = x_a$ and $\sigma_b(x_a|x_b) = x_b$. Clearly, if there exists an algorithm that can retrieve answers for both σ_a and σ_b from the encoding ρ_x then this algorithm can also break the OTM. ◀

Similarly to the QRG with verification, we can define $(c,\varepsilon)-$*one-time memories with verification* (OTMv); where the adversary is allowed to choose $d \in \{a, b\}$ and $y \in \{0,1\}^n$ and ask whether $x_d = y$. Again, a secure OTMv means that $c \geq 1 - \text{negl}(n)$ and $\varepsilon \leq \text{negl}(n)$. However, as we have shown, such a power does not really help the adversary.

Finally, a *hash based* OTMv (hOTM) is an OTMv where the adversary instead of being allowed to interact in order to find an answer, it is given as input the hashes of the two answers $H(x_a), H(x_b)$. This way, if an answer is correct, the adversary can verify that on its own. It can be shown that if the original OTMv is secure, then the hash based OTMv is still secure in the random oracle model.

A random oracle is essentially an oracle that behaves as follows. First, it keeps a list L of pairs of the form (x, y) where x is an element of its domain and y is an element of its range. In the beginning L is empty. On input x_0, first it searches L for a pair of the form (x_0, y_0), and if such a pair exists in L then it returns y_0. Otherwise, it picks a uniformly random element y_0 from its range, inserts (x_0, y_0) in the list L, and returns y_0. Hash functions are usually assumed to have this ideal property when other properties such as one-wayness or collision resistance are not enough for a security proof. When hash functions are used as random oracles in a proof that a scheme is secure, we say that the scheme is secure in the random oracle model.

▶ **Definition 18.** A hash based one-time memory (hOTM) is a device that has the following behavior. Suppose that the device is programmed with two n-bit messages x_a, x_b chosen from some distribution D. Then:

1. Correctness: There exists an honest strategy $M^{(a)}$ that interacts with the device and recovers the message x_a with probability $c = 1 - \text{negl}(n)$. Likewise, there is an honest strategy $M^{(b)}$ that interacts with the device and recovers the message x_b with probability $c = 1 - \text{negl}(n)$.

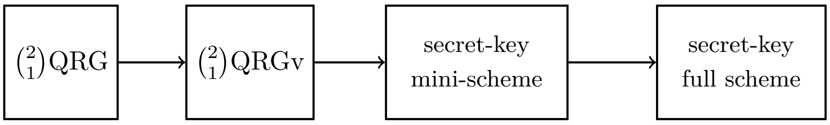


Figure 3 From a $\binom{2}{1}$QRG to a secret-key quantum money scheme.

2. Security: For any polynomial time strategy M that takes as input the hash values $H(x_a), H(x_b)$, if X is the random variable corresponding to the classical output of M, then $\Pr[X = (x_a, x_b)] \leq \text{negl}(n)$

Note that in contrast to the previous definitions, the security of a hOTM is computational.

▶ **Lemma 19.** *A secure* OTMv *is also a secure* hOTM *in the random oracle model.*

Proof. Suppose that there exists a polynomial algorithm $\mathcal{F}$ that is able to break the hOTM property. We can create an algorithm $\mathcal{A}$ against the OTMv property. $\mathcal{A}$ takes as input a state ρ_{x_a,x_b} and is allowed to ask verification queries of the form (d, y), where $d \in \{a, b\}$ and receive an answer 1 if and only if $x_d = y$. $\mathcal{A}$ initiates $\mathcal{F}$ by choosing two random values (α, β) as the hashes of the answers and giving to $\mathcal{F}$ the tuple $(\rho_{x_a,x_b}, \alpha, \beta)$. When $\mathcal{F}$ asks for the hash of a value y, $\mathcal{A}$ makes two queries of the form $(a, y), (b, y)$ and if one of them accepts, $\mathcal{A}$ returns to $\mathcal{F}$ the value α or β depending on which of the two queries accepted. If none of the two accepted, then $\mathcal{A}$ returns a random (but consistent with the previous queries) value to $\mathcal{F}$ as a hash of y. When $\mathcal{F}$ outputs its two final answers (x_a^*, x_b^*), $\mathcal{A}$ also outputs (x_a^*, x_b^*). We can see that $\mathcal{F}$ always takes proper answers to its queries ($\mathcal{F}$ is allowed to ask only for hash values) and therefore works as if it attacks the hOTM. Since $\mathcal{F}$ is a polynomial algorithm, it cannot ask more that a polynomial number of hash values and therefore $\mathcal{A}$ cannot have asked more than a polynomial number of queries. Thus, if the winning probability of $\mathcal{F}$ is non-negligible, $\mathcal{A}$ has also a non-negligible winning probability. ◀

4 Secret-key Quantum Money Construction

In this section we create a secret-key mini-scheme and we analyze its security. Our scheme, in contrast to that proposed by Gavinsky [5], allows a one-round protocol between the bank and the user to accomplish the verification of a coin: a query to the bank and an answer by the bank that states whether the coin is valid or not. Therefore, in our scheme the bank does not need to maintain memory during the verification procedure; it just consults its secret database and returns the result. In the scheme of Gavinsky, however, the verification protocol consists of three rounds during which, the bank has to maintain a temporary memory associated with a specific coin. Furthermore, unlike the scheme of Gavinsky, our proof of security is simpler, more modular and it includes noise and losses.

Gavinsky has shown that a $\binom{2}{1}$QRG with the following parameters exists:

▶ **Theorem 20** (Hidden Matching QRG [5, 6])**.** *There exists a* $(1 - 2^{-n}, 2^{-n}) - \binom{2}{1}$QRG G*.*

Starting from this and using theorem 15 we can create a $\binom{2}{1}$QRGv with the same parameters. Our construction is essentially a way of going from a $\binom{2}{1}$QRGv to a mini-scheme. Then, using the reduction from a mini-scheme to a full-scheme, the existence of a $\binom{2}{1}$QRG leads to the existence of a full quantum money scheme. The sequence of reductions appears in Figure 3.

We now propose our construction that uses a $\binom{2}{1}$QRGv to create a mini-scheme. The algorithm Bank and the protocol Ver are defined as follows:

Bank(1^{n^2}) :

1. For $i \in [n]$ create $G_i = (S, A, \{\rho_{x_i}\}_{x_i}, \sigma_a, \sigma_b, \sigma)$, $(1 - 2^{-n}, 2^{-n}) - \binom{2}{1}$QRGv.
2. Create a classical binary register r of size n and initialize it to 0^n.
3. Return the state $\$ = (\bigotimes_i \rho_{x_i}, r)$ as a coin for the mini-scheme.

Verification protocol for a coin $\$ = (\bigotimes_i \rho_{x_i}, r)$:

1. The holder creates an empty set L. Then, for each $i \in [n]$ such that $r_i = 0$, the holder puts i in the set L with probability $1/n^{1/3}$. For each $i \in L$ the holder picks at random a relation $\sigma'_i \leftarrow \{\sigma_a, \sigma_b\}$ and applies to ρ_{x_i} the measurement $M^{(a)}$ if $\sigma'_i = \sigma_a$ or $M^{(b)}$ if $\sigma'_i = \sigma_b$, in order to retrieve an answer d_i. Furthermore, for all $i \in L$ the holder sets $r_i = 1$. Finally, the holder sends to the bank the i's he has picked, the relation he has picked for each i, as well as the answers d_i.
2. The bank compares the answers it has received with its secret $x_1 \cdots x_n$ and accepts if all answers are correct; namely if for all $i \in L$ it holds that $(x_i, d_i) \in \sigma'_i$.

▶ Remark. The coin is returned to the bank for replacement when the hamming weight of r is greater than $n/4$ (more than $n/4$ of the ρ_{x_i} are marked as used). Note that the scheme consists of $O(n^2)$ qubits in total (there are n states ρ_{x_i} and each state consists of $O(n)$ qubits) and that the verification protocol consists of only one round.

▶ **Theorem 21.** *The scheme is secure; namely any (even computationally unbounded) adversary who interacts with the bank at most t times has winning probability of at most $e^{-n^{1/3}/8} + 4t^2 \cdot n \cdot 2^{-n}$.*

Proof. Suppose there is an adversary $\mathcal{F}$ for the mini-scheme, namely when $\mathcal{F}$ receives as input a valid coin \$ and after running t verification protocols with the bank, he can produce two coins $\$' = (\rho'_1, \cdots, \rho'_n, r'), \$'' = (\rho''_1, \cdots, \rho''_n, r'')$ that can pass the verification protocol with non-negligible probability ε greater than $p(t) \cdot 2^{-n}$, for all polynomials p. Then, one can create an adversary $\mathcal{A}$ for the $(1 - 2^{-n}, 2^{-n}) - \binom{2}{1}$QRGv, namely when $\mathcal{A}$ receives from the algorithm $\mathcal{C}$ as input a state ρ^* that is the encoding of a secret x^*, and after interacting t times with the algorithm $\mathcal{C}$, he can win the game with probability greater than $p(t) \cdot 2^{-n}$ for all polynomials p. By theorem 15 this also implies breaking the security of the $\binom{2}{1}$QRG.

Let $\mathcal{A}$ receive as input the state ρ^*, that is the encoding of a secret x^*. He creates an input for $\mathcal{F}$ in the following way:

Bank(1^{n^2}):

1. Pick at random $i^* \leftarrow [n]$.
2. For $i \in [n] - \{i^*\}$ create $G_i = (S, A, \{\rho_{x_i}\}_{x_i}, \sigma_a, \sigma_b, \sigma)$ where G_i is a $(1 - 2^{-n}, 2^{-n}) - \binom{2}{1}$QRGv.
3. Create a classical binary register r of size n and initialize it to 0^n.
4. Return to $\mathcal{F}$ the coin $\$ = (\rho, r)$, where $\rho = \rho_{x_1} \otimes \cdots \otimes \rho_{x_{i^*-1}} \otimes \rho^* \otimes \rho_{x_{i^*+1}} \otimes \cdots \otimes \rho_{x_n}$.

In other words, $\mathcal{A}$ creates a totally valid coin, but in the i^*-th position he puts the state he has as input. For clarity we will denote the secret x^* as x_{i^*}. Note that $\mathcal{A}$ is able to pretend to be the honest bank during the verification protocol with $\mathcal{F}$, since for all $i \in [n] - \{i^*\}$ he knows the answers to the relations, whereas for the i^*-th state, he can use his own interaction with the algorithm $\mathcal{C}$ in order to decide whether the query asked by $\mathcal{F}$ is correct. Therefore, $\mathcal{A}$ simulates the verification protocol between the bank and $\mathcal{F}$ in the following way:

1. $\mathcal{A}$ receives from $\mathcal{F}$ a set L of i's, a set of challenges $\sigma'_i \in \{\sigma_a, \sigma_b\}$ and a set of answers d_i for each $i \in L$.
2. $\mathcal{A}$ returns 1 if all answers are correct; namely, if $(x_i, d_i) \in \sigma'_i$ for all $i \in L$. Note that for those i's that are different from i^*, $\mathcal{A}$ can easily consult his own secret x_i in order to find if the answer is correct. However, for $i = i^*$, $\mathcal{A}$ can make a query (σ'_{i^*}, d_{i^*}) to the algorithm $\mathcal{C}$ in order to find if the answer d_{i^*} is correct.

Hence, $\mathcal{A}$ can provide $\mathcal{F}$ with a valid initial coin and simulate the bank in the t verification protocols with $\mathcal{F}$, and in the end, he receives from $\mathcal{F}$ two coins $\$' = (\rho'_1, \cdots, \rho'_n, r'), \$'' = (\rho''_1, \cdots, \rho''_n, r'')$ that can pass a verification protocol with an honest verifier with non-negligible probability ε. For the two coins $\$', \$''$ to be considered as valid, there must be at least $3/4n$ of the ρ'_i's denoted as valid and at least $3/4n$ of the ρ''_i's denoted as valid (a state ρ'_i is denoted as valid if $r'_i = 0$). Therefore, there are at least $n/2$ indices i such that $r'_i = r''_i = 0$. We want to argue that there must be an index i among them for which $\mathcal{A}$ can win the $\binom{2}{1}$QRGv game with probability greater than $p(t) \cdot 2^{-n}$ for all polynomials p, otherwise the probability that the adversary $\mathcal{F}$ could create two valid coins is negligible.

Let $I = \{i : r'_i = r''_i = 0\}$. Since the coins $\$', \$''$ are denoted as valid, it holds that $|I| \geq n/2$. Assume now that two honest verifiers Ver$'$ and Ver$''$ run the verification protocol for the two coins respectively. Let L^a, L^b be the sets chosen by the honest verifiers and $L' = \{i \in L^a \cap L^b : \sigma'_i = \sigma_a \wedge \sigma''_i = \sigma_b\}$, where σ'_i, σ''_i are the relations chosen for the index i by the verification protocols for the two coins. In other words, L' contains the indices that where chosen by both Ver$'$ and Ver$''$ in such a way that Ver$'$ chose σ_a for this i and Ver$''$ chose σ_b for this i. It holds that $\Pr[i \in L^a \cap L^b] = 1/n^{2/3}$ and $\Pr[i \in L'] = 1/4n^{2/3}$. Therefore, $\Pr[\forall i \in I : i \notin L'] = \Pr[L' = \emptyset] \leq (1 - 1/4n^{2/3})^{n/2} = e^{-n^{1/3}/8}$, since $|I| = n/2$. In other words, the probability that there exists an i with $r'_i = r''_i = 0$ such that Ver$'$ chose it during the verification protocol and picked the relation σ_a for it and Ver$''$ also chose it and picked σ_b for it, is exponentially close to 1. Now it holds that

$$\begin{aligned}
&\Pr[\mathcal{F} \text{ wins}] = \Pr[\text{Ver}'(\$') = 1 \wedge \text{Ver}''(\$'') = 1] \\
&= \Pr[L' = \emptyset] \cdot \Pr[\text{Ver}'(\$') = 1 \wedge \text{Ver}''(\$'') = 1 | L' = \emptyset] \\
&+ \Pr[\text{Ver}'(\$') = 1 \wedge \text{Ver}''(\$'') = 1 \wedge L' \neq \emptyset] \\
&\leq e^{-n^{1/3}/8} + \Pr[\text{Ver}'(\$') = 1 \wedge \text{Ver}''(\$'') = 1 \wedge L' \neq \emptyset] \\
&\leq e^{-n^{1/3}/8} + \Pr[\exists i \in L' : (M^{(a)}(\rho'_i), x_i) \in \sigma_a \wedge (M^{(b)}(\rho''_i), x_i) \in \sigma_b]
\end{aligned}$$

where $M^{(a)}, M^{(b)}$ are the measurements applied to the states of the QRG's in order to retrieve an answer to σ_a, σ_b respectively. The last line comes from the fact that if L' is not empty and both verifications succeed, then both verifications must succeed for all $i \in L'$. Therefore, if $\Pr[\mathcal{F} \text{ wins}] = \varepsilon$ is non-negligible then $\Pr[\exists i \in L' : (M^{(a)}(\rho'_i), x_i) \in \sigma_a \wedge (M^{(b)}(\rho''_i), x_i) \in \sigma_b] \geq \varepsilon - e^{-n^{1/3}/8}$ is non-negligible as well. This trivially implies that $\Pr[\exists i \in [n] : (M^{(a)}(\rho'_i), x_i) \in \sigma_a \wedge (M^{(b)}(\rho''_i), x_i) \in \sigma_b] \geq \varepsilon - e^{-n^{1/3}/8}$. In other words, with

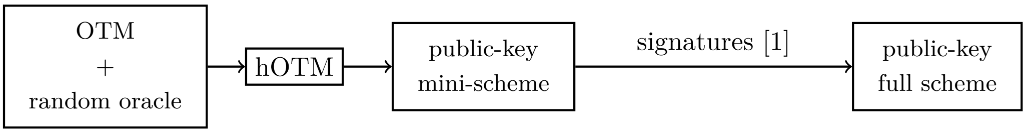


Figure 4 From an OTM to a full public-key quantum money scheme. OTMs in the random oracle model give hOTM. hOTM imply public-key mini-schemes which, together with signatures, imply public-key quantum money.

non-negligible probability there exists an index i for which both verifications succeed. At this point it is clear that the goal of $\mathcal{A}$ is just to guess that index i and put ρ^* in that position.

Overall, the adversary $\mathcal{A}$ works as follows: Upon receiving as input the state ρ^*, he picks a random position i^*, creates the valid coin for $\mathcal{F}$ as we described above, receives the states ρ'_{i^*} and ρ''_{i^*} from $\mathcal{F}$ and returns the answers $\left(M^{(a)}(\rho'_{i^*}), M^{(b)}(\rho''_{i^*})\right)$. Now it holds that

$$
\begin{aligned}
\Pr[\mathcal{A}\text{ wins}] &= \Pr[(M^{(a)}(\rho'_{i^*}), x_{i^*}) \in \sigma_a \wedge (M^{(b)}(\rho''_{i^*}), x_{i^*}) \in \sigma_b] \\
&\geq \Pr[(M^{(a)}(\rho'_{i^*}), x_{i^*}) \in \sigma_a \wedge (M^{(b)}(\rho''_{i^*}), x_{i^*}) \in \sigma_b | \\
&\qquad \exists i \in [n] : (M^{(a)}(\rho'_{i}), x_{i}) \in \sigma_a \wedge (M^{(b)}(\rho''_{i}), x_{i}) \in \sigma_b] \\
&\cdot \Pr[\exists i \in [n] : (M^{(a)}(\rho'_{i}), x_{i}) \in \sigma_a \wedge (M^{(b)}(\rho''_{i}), x_{i}) \in \sigma_b] \\
&\geq \frac{1}{n} \cdot \Pr[\exists i \in L' : (M^{(a)}(\rho'_{i}), x_{i}) \in \sigma_a \wedge (M^{(b)}(\rho''_{i}), x_{i}) \in \sigma_b] \\
&\geq \left(\varepsilon - e^{-n^{1/3}/8}\right)/n
\end{aligned}
$$

which contradicts the fact that the security of the $\binom{2}{1}$QRGv is 2^{-n}.

Therefore, since by theorem 15 the maximum winning probability of $\mathcal{A}$ is $4t^2 \cdot 2^{-n}$, the maximum winning probability of $\mathcal{F}$ is $e^{-n^{1/3}/8} + 4t^2 \cdot 2^{-n} \cdot n$. ◀

5 Public-key Quantum Money Construction

In the construction of a public key scheme, it suffices to create a secure public-key mini-scheme, and this, combined with signatures, can give a full scheme [1]. The advantage of our construction is that it is a simple modification of the previous secret key one: the answers of the bank are encoded in their hash values. Therefore, instead of requiring from the user to communicate with the bank in order to find out if an answer is valid, the bank announces the hash values of the answers. It is clear that for a regular QRG there may exist too many answers and hence giving all these hashes as part of the coin would violate the correctness of the scheme. Hence, for our construction, we need to use QRG with functions or equivalently one-time memories. Despite the fact that quantum one-time memories do not exist unconditionally, they exist in the isolated qubits model.

▶ **Theorem 22** ([8, 9, 10]). *There exists a secure* OTM *in the isolated qubits model.*

Using this, together with lemma 19, we get the following corollary.

▶ **Corollary 23.** *There exists a secure* hOTM *in the isolated qubits-random oracle model.*

Our purpose, now, is to go from hOTM to a public-key mini-scheme. The sequence of reductions appears in Figure 4.

Since for each OTM there are only two secrets, a hashing of each answer can be given as part of the coin. Then the verification algorithm works similarly to the secret key scheme. It chooses each state-game with probability $1/n^{1/3}$, it chooses at random whether to retrieve the first (x_a) or the second (x_b) secret for each game, it measures the OTM (using $M^{(a)}$ or $M^{(b)}$) in order to retrieve an answer and finally it verifies that the hash value of that answer is the same as the one given. So the two algorithms Bank and Ver of the mini-scheme are the following:

Bank(1^{n^2}) :

1. For $i \in [n]$ create the OTM ρ_i with secrets $x_i^a, x_i^b \in \{0,1\}^n$.
2. Create a classical binary register r of size n and initialize it to 0^n.
3. Return $\$ = ((h_1, g_1), \cdots, (h_n, g_n), \rho_1, \cdots, \rho_n, r)$ as a coin for the mini-scheme, where $h_i = H(x_i^a)$, $g_i = H(x_i^b)$ and H is the hash function. The string $(h_1, g_1), \cdots, (h_n, g_n)$ corresponds to the classical serial number of the coin (that has to be signed in order to give a full coin), and $(\rho_1, \cdots, \rho_n, r)$ is the quantum state.

Ver($(h_1, g_1), \cdots, (h_n, g_n), \rho_1, \cdots, \rho_n, r$):

1. Create an empty set L. Then, for each $i \in [n]$ such that $r_i = 0$, put i in the set L with probability $1/n^{1/3}$.
2. For each $i \in L$ pick at random $d_i \leftarrow \{a, b\}$ and measure ρ_i in order to retrieve an answer $x_i \in \{x_i^a, x_i^b\}$; i.e. $x_i = M^{(d_i)}(\rho_i)$.
3. For all $i \in L$ set $r_i = 1$.
4. Accept if for all $i \in L$ it holds that $H(x_i) = h_i$ (if $d_i = a$) or $H(x_i) = g_i$ (if $d_i = b$).

As before, the coin is returned to the bank for replacement when the hamming weight of r is greater that $n/4$.

► **Theorem 24.** *The scheme is secure.*

Proof sketch. The proof follows the same steps as that of the secret-key scheme; a good adversary $\mathcal{F}$ against the mini-scheme can lead to a good adversary $\mathcal{A}$ against the hOTM. $\mathcal{F}$ takes as input a coin $\$ = (\text{sn}, \rho)$, where $\text{sn} = (h_1, g_1), \cdots, (h_n, g_n)$ and $\rho = (\rho_1, \cdots, \rho_n, r)$. At the end, $\mathcal{F}$ outputs two states $\rho' = (\rho_1', \cdots, \rho_n', r')$, $\rho'' = (\rho_1'', \cdots, \rho_n'', r'')$ such that both $\$' = (\text{sn}, \rho')$ and $\$'' = (\text{sn}, \rho'')$ pass the verification test with non-negligible probability. Note that these two states pass successfully the verification algorithm with the same serial sn and therefore with the same hash values. As before, we can show that the number of indices that are denoted as valid in both coins are at least $n/2$. Furthermore, the probability that none of them is able to pass the two verification algorithms is negligible (otherwise the winning probability of $\mathcal{F}$ would be negligible). Thus, a non-negligible counterfeiting probability ε of $\mathcal{F}$ implies a non-negligible probability of $\mathcal{A}$ to break the hOTM. ◄

6 Conclusions

We created a secret-key quantum money scheme that is unconditionally secure and has optimal communication: a single round of classical communication. We also provided a conceptually simpler and more modular proof. Moreover, if we instantiate the $\binom{2}{1}$QRG with the Hidden Matching $\binom{2}{1}$QRG, we can tolerate an error rate of up to 12.5%; see lemma 12 in Appendix A. Note that in every verification of the coin we invalidate on average $n^{1/3}$ quantum states (each consisting of n qubits) and thus the number of allowed verifications before the coin is returned to the bank is $n/(4 \cdot n^{1/3}) = n^{2/3}/4$. Therefore, for a coin of say 10^{12} qubits, we succeed 2,500 verifications on average. A polynomial number of verifications is optimal for unconditionally secure schemes, nevertheless, a natural question that still remains open is whether we can have computationally secure secret-key schemes that allow exponentially many classical verifications.

In addition, we showed how a simple extension of our secret key construction can give rise to a public-key quantum money scheme that is computationally secure against quantum adversaries in the random oracle model given one-time memories. We note that previous schemes were also based on non-standard computational assumptions. The main open question is to construct public-key quantum money that are provably secure based on some standard cryptographic assumptions such as one-way functions.

Acknowledgements. We thank Jamie Sikora for bringing to our attention the semidefinite approach of QRG. This work was partially supported by the ERC project QCC, the ANR project RDAM and the EU project QAlgo.

References

1 Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the 44th Symposium on Theory of Computing*, pages 41–60. ACM, 2012.

2 Ziv Bar-Yossef, Thathachar S Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 128–137. ACM, 2004.

3 Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. *Advances in Cryptology–CRYPTO 2013*, pages 344–360, 2013.

4 Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 276–289. ACM, 2012.

5 Dmitry Gavinsky. Quantum money with classical verification. In *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on*, pages 42–52. IEEE, 2012.

6 Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525. ACM, 2007.

7 Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum. One-time programs. *Advances in Cryptology–CRYPTO 2008*, pages 39–56, 2008.

8 Yi-Kai Liu. Building one-time memories from isolated qubits. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 269–286. ACM, 2014.

9 Yi-Kai Liu. Privacy amplification in the isolated qubits model. *arXiv preprint arXiv:1410.3918*, 2014.

10 Yi-Kai Liu. Single-shot security for one-time memories in the isolated qubits model. *arXiv preprint arXiv:1402.0049*, 2014.

11 Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for wiesner's quantum money. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 45–64. Springer, 2013.

12 Michele Mosca and Douglas Stebila. Quantum coins. Error-Correcting Codes, Finite Geometries and Cryptography. Contemporary Mathematics, volume 523, pages 35-47. American Mathematical Society, 2010, 2009.

13 Daniel Nagaj and Or Sattath. An adaptive attack on wiesner's quantum money based on interaction-free measurement. *arXiv preprint arXiv:1404.1507*, 2014.

14 Marta Conde Pena, Jean-Charles Faugère, and Ludovic Perret. Algebraic cryptanalysis of a quantum money scheme the noise-free case. In *Public-Key Cryptography–PKC 2015*, pages 194–213. Springer, 2015.

15 Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

16 Norman Yao, Fernando Pastawski, Liang Jiang, Mikhail Lukin, and Ignacio Cirac. Unforgeable noise-tolerant quantum tokens. *Bulletin of the American Physical Society*, 57, 2012.

A Instantiating a QRG

As shown above, the existence of a $(c, \varepsilon) - \binom{2}{1}$ QRG implies the existence of a secret-key quantum money scheme as long as c is reasonably large and ε is any constant smaller than 1. To instantiate such a quantum money scheme one has to give specific quantum retrieval games with this property.

Hidden Matching QRG [2, 5]

▶ **Definition 25.** The Hidden Matching $\binom{2}{1}$QRG $G = (S, A, \{\rho_x\}_{x\in S}, \sigma_a, \sigma_b, \sigma)$ is defined the following way: $S = \{0,1\}^4$, $A = \{0,1\} \times \{0,1\}$, $|\psi_x\rangle = \frac{1}{2}\sum_{i\in[4]}(-1)^{x_i}|i\rangle$, $\rho_x = \frac{1}{16}|\psi_x\rangle\langle\psi_x|$. The relation σ_a is defined as $(x,(a,b)) \in \sigma_a$ if and only if the following holds: if $a = 0$ then $x_1 \oplus x_2 = b$; if $a = 1$ then $x_3 \oplus x_4 = b$. Similarly, the relation σ_b is defined as $(x,(a,b)) \in \sigma_b$ if and only if the following holds: if $a = 0$ then $x_1 \oplus x_3 = b$; if $a = 1$ then $x_2 \oplus x_4 = b$.

▶ **Lemma 26.** *The Hidden Matching is a* $(1, \frac{3}{4}) - \binom{2}{1}$QRG.

Proof. The correctness in a noise-free environment we can be succeeded with zero error probability. Indeed, if we want to find an answer for the relation σ_a we measure in the basis $\{\frac{|1\rangle+|2\rangle}{\sqrt{2}}, \frac{|1\rangle-|2\rangle}{\sqrt{2}}, \frac{|3\rangle+|4\rangle}{\sqrt{2}}, \frac{|3\rangle-|4\rangle}{\sqrt{2}}\}$ and we return the values $(a,b) = (0,0),(0,1),(1,0),(1,1)$ respectively. If we want to find an answer for the relation σ_b we measure in the basis $\{\frac{|1\rangle+|3\rangle}{\sqrt{2}}, \frac{|1\rangle-|3\rangle}{\sqrt{2}}, \frac{|2\rangle+|4\rangle}{\sqrt{2}}, \frac{|2\rangle-|4\rangle}{\sqrt{2}}\}$ and we return $(a,b) = (0,0),(0,1),(1,0),(1,1)$ respectively. For the security of the game, we use Theorem 9. By definition, we have $(x,(a_1,b_1),(a_2,b_2)) \in \sigma$ if and only if $(x,(a_1,b_1)) \in \sigma_a$ and $(x,(a_2,b_2)) \in \sigma_b$. It holds that $\rho = \sum_{x\in\{0,1\}^4}\rho_x = \frac{1}{4}I$ and therefore $\rho^{\frac{1}{2}} = 2I$. In order to find the selective value of the game $(S, A \times A, \{\rho_x\}_{x\in S}, \sigma)$ it is enough to consider one value of O_a for some possible answer $a \in A \times A$. For example, by taking $a = ((0,0),(0,0))$ the values of x that satisfy $(x,a) \in \sigma$ are $0000, 0001, 1110, 1111$ and the corresponding density matrices are $\frac{1}{16}\frac{1}{4}\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$, $\frac{1}{16}\frac{1}{4}\begin{bmatrix}1&1&1&-1\\1&1&1&-1\\1&1&1&-1\\-1&-1&-1&1\end{bmatrix}$, $\frac{1}{16}\frac{1}{4}\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}$, $\frac{1}{16}\frac{1}{4}\begin{bmatrix}1&1&1&-1\\1&1&1&-1\\1&1&1&-1\\-1&-1&-1&1\end{bmatrix}$. Therefore, $O_{((0,0),(0,0))} = \frac{1}{4}\begin{bmatrix}1&1&1&0\\1&1&1&0\\1&1&1&0\\0&0&0&1\end{bmatrix}$ and thus it holds that $\|O_{((0,0),(0,0))}\| = \frac{3}{4} = \mathrm{SVal}(G)$.

For the independence property, we know that for any $a_{12}, a_{34} \in \{0,1\}$ it holds that $\Pr[x_1 \oplus x_2 = a_{12} \wedge x_3 \oplus x_4 = a_{34}] = 1/4$ and for any bit $b \in \{0,1\}$, it holds that $\Pr[x_1 \oplus x_3 = b] = 1/2$. Moreover, $\Pr[x_1 \oplus x_2 = a_{12} \wedge x_3 \oplus x_4 = a_{34} \wedge x_1 \oplus x_3 = b] = 1/8$ and thus we see that the event $x_1 \oplus x_3 = b$ is independent from the event $x_1 \oplus x_2 = a_{12} \wedge x_3 \oplus x_4 = a_{34}$. The same of course holds for the event $x_2 \oplus x_4 = b$. ◀

By Lemma 12, it is enough to guarantee that $c \geq \frac{7}{8} + \delta$ for some constant δ in order succeed an exponentially good error tolerance. Thus, the hidden matching $\binom{2}{1}$QRG can tolerate up to 12.5% of errors.

B Technical proofs

Proof of lemma 12. Let $G = (S, A, \{\rho_x\}_{x \in S}, \sigma_a, \sigma_b, \sigma)$. We create the following game $G' = (S', A', \{\rho'_x\}_{x \in S'}, \sigma'_a, \sigma'_b, \sigma')$ by taking the product of n games G. Then we require that $(x_1 \cdots x_n, a_1 \cdots a_n) \in \sigma'_a$ if at least $c - \delta$ of the (x_i, a_i) are in σ_a and $(x_1 \cdots x_n, b_1 \cdots b_n) \in \sigma'_b$ if at least $c - \delta$ of the (x_i, b_i) are in σ_b. Furthermore, by definition, it holds that $(x_1 \cdots x_n, (a_1 \cdots a_n, b_1 \cdots b_n)) \in \sigma'$ if $(x_1 \cdots x_n, a_1 \cdots a_n) \in \sigma'_a$ and $(x_1 \cdots x_n, b_1 \cdots b_n) \in \sigma'_b$.

Since $\delta > 0$, we have $c > (1+\varepsilon)/2$ and hence $c - \delta > 1/2$. This implies there exist at least $2c - 2\delta - 1 = \varepsilon + \delta$ common values (i's such that $(x_i, a_i) \in \sigma_a$ and $(x_i, b_i) \in \sigma_b$). Therefore, $(x_1 \cdots x_n, (a_1 \cdots a_n, b_1 \cdots b_n)) \in \sigma'$ implies that there exist at least $\varepsilon + \delta$ of the (x_i, a_i, b_i) that are in σ.

We then analyze its Correctness and its Security. The Correctness c' of G' is guaranteed via the straightforward strategy of independently measuring each of the n states in the basis that corresponds to σ_a or to σ_b. Let X_i be the binary random variable that equals to 1 if and only if the i-th measurement was successful. Let $X = \sum_{i \in [n]} X_i$. Then $\mathbb{E}[X] = cn$ and, since the X_i's are independent, using Chernoff bound, we have that

$$c' \geq 1 - e^{-\frac{cn}{2}\delta^2}$$

For the Security ε' of the game, we know that the selective value is always greater or equal to the physical value and that the former is equal to the product of the individual selective values. Therefore, as mentioned before, the best measurement strategy that answers correctly both questions, cannot be better than independently playing the optimal strategy for each of the n small games. Let Y_i be the binary random variable that equals to 1 if and only if the i-th measurement was successful. Let, also, $Y = \sum_{i \in [n]} Y_i$. Then, as before, $\mathbb{E}[Y] = \varepsilon n$ and, since the Y_i's are independent

$$\varepsilon' \leq e^{-\frac{\varepsilon n}{3}(2c - 2\delta - 1 - \varepsilon)^2} = e^{-\frac{\varepsilon n}{3}\delta^2}$$

which is exponentially small in n. ◀

Proof of lemma 14. The correctness of $\binom{2}{1}$QRGv and $\binom{2}{1}$rQRGv is exactly the same. Furthermore, it is clear that if a non-restricted adversary has probability ε to win, this probability cannot increase by restricting this adversary. In order to show the equivalence between the two definitions, it remains to show that a non-restricted adversary has no more power than a restricted adversary. Without loss of generality, we assume that the first successful query was for σ_a. Then, one more success for σ_a does not help the adversary towards finding an answer for σ_a (since, it already knows one). Furthermore, by the independence property, even knowing all the answers for σ_a does not give the adversary extra power to find an answer to σ_b. Therefore, restricting the adversary to one successful query per relation, does not decrease his winning probability. More details will appear in the full version of the paper. ◀

Proof of Theorem 15. The proof of correctness is straightforward. We focus on the security of G. By lemma 14 it suffices to show that G' implies an $\binom{2}{1}$rQRGv. By contradiction, assume that there exists an adversary $\mathcal{F}$ against the $\binom{2}{1}$rQRGv G, who interacts t times with $\mathcal{C}$ and wins the game with probability $q > p(t) \cdot \varepsilon$ for all polynomials p. We can use

$\mathcal{F}$ in order to create an adversary $\mathcal{F}'$ who is able to attack the original $\binom{2}{1}$QRG G' with probability greater than ε. Since $\mathcal{F}$ is restricted after succeeding one interaction with σ_a it will continue interacting only by picking σ_b in its queries. Let E_1, E_2, E_3, E_4 be the events that $\mathcal{F}$ does not succeed in any interaction, $\mathcal{F}$ succeeds only in a σ_a interaction, $\mathcal{F}$ succeeds only in a σ_b interaction, $\mathcal{F}$ succeeds in both σ_a and σ_b interactions, respectively. Note that, since $\mathcal{F}$ is restricted, only these four events may occur. Denote the probabilities of these events by p_1, p_2, p_3, p_4 respectively. The idea is for $\mathcal{F}'$ to guess a priori which of the four events will occur and which queries will be successful. If these guesses are correct then $\mathcal{F}$ will not notice any difference with a real scenario (where $\mathcal{F}$ is playing a real $\binom{2}{1}$rQRGv game). These guesses can succeed with probability proportional to an inverse polynomial and if they succeed then $\mathcal{F}'$ can break the QRG. Thus, $\mathcal{F}'$ can break the non-interactive game the following way.

1. $\mathcal{F}'$ takes as input ρ_x and forwards it to $\mathcal{F}$.
2. $\mathcal{F}'$ guesses uniformly at random $i \leftarrow [4]$ which corresponds to which of the four types of attacks $\mathcal{F}$ will play.
   a. If $i = 1$ then in every interaction $\mathcal{F}'$ returns a 0 to $\mathcal{F}$. When $\mathcal{F}$ returns its final answers (a_1^*, a_2^*), $\mathcal{F}'$ returns (a_1^*, a_2^*).
   b. If $i = 2$ then $\mathcal{F}'$ chooses at random one of the σ_a queries and answers it with 1. To all the others, $\mathcal{F}'$ answers with 0. When $\mathcal{F}$ returns its final answers (a_1^*, a_2^*), $\mathcal{F}'$ returns (a_1^*, a_2^*).
   c. If $i = 3$ then $\mathcal{F}'$ chooses at random one of the σ_b queries and answers it with 1. To all the others, $\mathcal{F}'$ answers with 0. When $\mathcal{F}$ returns its final answers (a_1^*, a_2^*), $\mathcal{F}'$ returns (a_1^*, a_2^*).
   d. If $i = 4$ then $\mathcal{F}'$ chooses at random one of the σ_a and one of σ_b questions and answers them with 1. After the second positive answer, $\mathcal{F}'$ stops simulating $\mathcal{F}$ and returns as (a_1^*, a_2^*) the queries that he answered with 1.

Then the winning probability of $\mathcal{F}'$ can be computed as follows

$$\begin{aligned} q = {} & \Pr[\mathcal{F}\text{wins}] \\ = {} & p_1 \Pr[\mathcal{F}\text{wins}|E_1] + p_2 \Pr[\mathcal{F}\text{wins}|E_2] + p_3 \Pr[\mathcal{F}\text{wins}|E_3] + p_4 \Pr[\mathcal{F}\text{wins}|E_4] \\ \leq {} & \Pr[\mathcal{F}\text{wins}|E_1] + \Pr[\mathcal{F}\text{wins}|E_2] + \Pr[\mathcal{F}\text{wins}|E_3] + \Pr[\mathcal{F}\text{wins}|E_4] \\ \leq {} & \Pr[\mathcal{F}'\text{wins}|E_1] + \Pr[\mathcal{F}'\text{wins}|E_2] \cdot t + \Pr[\mathcal{F}'\text{wins}|E_3] \cdot t + \Pr[\mathcal{F}'\text{wins}|E_4] \cdot t^2 \\ \leq {} & t^2 \cdot \Big(\Pr[\mathcal{F}'\text{wins}|E_1] + \Pr[\mathcal{F}'\text{wins}|E_2] + \Pr[\mathcal{F}'\text{wins}|E_3] + \Pr[\mathcal{F}'\text{wins}|E_4] \Big) \\ = {} & 4t^2 \cdot \Pr[\mathcal{F}'\text{wins}] \end{aligned}$$

where the third line comes from the fact that $\mathcal{F}'$ has probability $1, \frac{1}{t}, \frac{1}{t}$ and $\frac{1}{t^2}$ respectively to correctly respond to $\mathcal{F}$'s queries. In other words, with probability $1/4t^2$ the view of $\mathcal{F}$ is identical to a real interaction. Therefore for any polynomial p it holds that

$$\frac{p(t)}{4t^2} \cdot \varepsilon < \Pr[\mathcal{F}'\text{wins}]$$

and in particular for $p(t) = 4t^2$ it holds that $\varepsilon < \Pr[\mathcal{F}'\text{wins}]$ which contradicts the fact that G' is a $(c, \varepsilon) - \binom{2}{1}$QRG. Hence we see that a $\binom{2}{1}$QRG implies a $\binom{2}{1}$QRGv. ◀

Decoherence in Open Majorana Systems

Earl T. Campbell

Department of Physics & Astronomy, University of Sheffield
Sheffield, United Kingdom
earltcampbell@gmail.com

Abstract

Coupling to a thermal bath leads to decoherence of stored quantum information. For a system of Gaussian fermions, the fermionic analog of linear or Gaussian optics, these dynamics can be elegantly and efficiently described by evolution of the system's covariance matrix. Taking both system and bath to be Gaussian fermionic, we observe that decoherence occurs at a rate that is independent of the bath temperature. Furthermore, we also consider a weak coupling regime where the dynamics are Markovian. We present a microscopic derivation of Markovian master equations entirely in the language of covariance matrices, where temperature independence remains manifest. This is radically different from behaviour seen in other scenarios, such as when fermions interact with a bosonic bath. Our analysis applies to many Majorana fermion systems that have been heralded as very robust, topologically protected, qubits. In these systems, it has been claimed that thermal decoherence can be exponentially suppressed by reducing temperature, but we find Gaussian decoherence cannot be cooled away.

1998 ACM Subject Classification J.2 Physics

Keywords and phrases Majorana, Topological, Gaussian, Thermalization, Decoherence

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.111

1 Introduction

Thermalization through interaction with an external bath is one of the principal mechanisms by which quantum systems lose information. In quantum technologies, rapid thermalisation destroys their advantage over classical counterparts. By better understanding these processes, one hopes to identify and engineer physical systems that act as more robust stores of quantum information. In topologically ordered systems, information is stored non-locally within the degenerate ground space of some large many-body system. The primary benefit of topology is robustness against random adiabatic fluctuations in the system Hamiltonian. Damage from such noise is exponentially suppressed with system size. Topological systems also have an energy gap Δ between the degenerate ground space and excited states, and are said to be protected by the gap against thermal excitations. A common claim [29] is that thermal processes occur at a rate $e^{-\Delta/T}$, which is sometimes called the Arrhenius law. The bold conclusion is that topology can exponentially eliminate noise merely by increasing system size and decreasing temperature.

Of all topological systems, Majorana zero modes have attracted the most attention. It was theorized that a so-called Kitaev wire supports Majorana zero modes at edges, which could be realised in simple solid state hetrostructures [1], for example a nanowire coupled to a conventional s-wave superconductor [22]. This drove a series of experiments, eventually leading to observations of Majorana edge modes [27, 28, 16]. Beyond topological robustness, Majorana zero-modes also possess the braiding statistics of non-Abelian Ising anyons. Though insufficient for direct quantum computation, braiding Ising anyons can

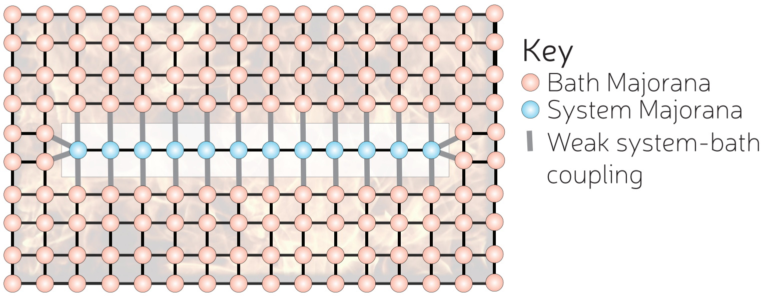


Figure 1 A chain of cool Majorana fermions weakly coupled to a large thermal 2-dimensional bath of Majorana fermions. This provides an example of the general paradigm we work within, though our results apply to all Gaussian systems.

demonstrate nonlocality, teleportation and superdense coding [11]. Furthermore, Ising anyon braiding can be promoted to full quantum computing when supplemented with some nontopological (noisy) operations [6, 13].

The physics of these Majorana systems is especially tractable as their Hamiltonians are quadratic in fermion creation and annihilation operators. We say such a system is Gaussian, or quasifree fermionic, in analogy with Gaussian linear optics. Gaussian states can be described purely in terms of the expectation value of quadratic observables, which are captured by a covariance matrix. Furthermore, some dissipative processes can be described within this powerful covariance matrix formalism [5, 32, 33, 34, 15, 8, 3], and allow single fermions to hop between system and bath via $a_S^\dagger a_B$. Single fermion hopping violates conservation of fermion parity in the system, which is otherwise respected by unitary evolution. It is a toxic process that can cause errors without creating excitations, circumventing arguments that energy penalties suppress thermal processes to a rate $e^{-\Delta/T}$. In particular, Majorana modes in the Kitaev wire (see Fig. 1) have been shown to decohere due to fermion hopping at rates independently of system size or the system gap [10, 25], and we will review these results in detail. This article considers all Gaussian fermionic systems, not just the Kitave wire, and how they decohere as a function of temperature. A single fermion appearing in the system will have a partner appear in the environment, and so perhaps there is hope that a gapped bath Hamiltonian will provide an energy penalty inhibiting these processes.

We present a very general, yet simple, argument that decoherence is independent of temperature, assuming only that the system-bath is governed by a Gaussian Hamiltonian. We extend this argument by providing a microscopic derivation of a master equation in the weak coupling regime, and again observe temperature independent decoherence. When fermions couple to bosonic baths, or through quartic fermion-fermion interactions $a_S^\dagger a_S a_B^\dagger a_B$, one would instead find a non-trivial temperature dependence. Any real physical system will experience noise from multiple sources, mostly with temperature dependent rates. However, fermionic hopping presents a constant background noise that cannot be suppressed through cooling. This adds to a growing body of work [18, 23, 35, 30] that shows the outlook for Majorana fermions makes them less promising quantum memories than initially supposed. Our conclusions can be avoided by going beyond Gaussian fermions, for instance by making use of complex many-body interactions used in the passive quantum memories reviewed in Ref. [9]. We discuss how our results demonstrate a break down of the Arrhenius law, whilst still satisfying a notion of detailed balance. Decoherence of two-level systems, such as spins, has been studied when they couple to spin or fermion baths [24, 37] where a temperature dependence is observed but at low temperatures relaxation rates plateau, similarly breaking the Arrhenius law. Throughout, we use the phrase thermalize as synonymous with equilibrate or approach steady state. The reader should not infer that the steady state is the thermal Gibbs distribution with respect the system Hamiltonian and ambient temperature, as may not be the case.

2 Covariance Matrix Formalism

Here we present standard techniques for working with Gaussian fermions [5, 32, 33, 34, 15, 8, 3], and use them to show that decoherence is independent of bath temperature. Relaxation of Gaussian fermionic open systems has be studied in detail (see e.g. Refs. [21, 38], but these did not include a model of the bath as also composed of Gaussian fermions. The first step is to map n Dirac fermions (e.g. electrons) with annihilation and creation operators $\{a_n, a_n^\dagger\}$ into $2n$ Majorana operators

$$c_{2n-1} = a_n + a_n^\dagger \ , \ c_{2n} = i(a_n - a_n^\dagger). \tag{1}$$

They are still fermionic in anti-commutation $\{c_j, c_k\} = \delta_{j,k}$, but differ from Dirac fermions in that they satisfy $c_j^\dagger = c_j$ and $c_j^2 = 1$. For any quantum state ρ, the covariance matrix has real elements composed of second moments

$$\Gamma_{j,k} = \frac{i}{2}\mathrm{tr}[(c_j c_k - c_k c_j)\rho]. \tag{2}$$

Due to fermion anticommutation, the covariance matrix is skew-symmetric $\Gamma^T = -\Gamma$. Because of conservation of fermion parity, first moments always vanish $\mathrm{tr}(c_j\rho) = 0$. For Gaussian states, expectation values of higher moments are determined by the covariance matrix via Wick's theorem. Likewise a quadratic Hamiltonian $\hat{H}$ is described by a matrix H so that

$$\hat{H} = \frac{i}{4}\sum_{j,k} H_{j,k} c_j c_k. \tag{3}$$

Again, H must be real for the Hamiltonian to be Hermitian, and furthermore H can always be chosen skew-symmetric $H = -H^T$. For a closed quantum system evolving unitarily, the covariance matrix evolves according to

$$\frac{d\Gamma(t)}{dt} = [\Gamma(t), H], \tag{4}$$

where $[\cdot,\cdot]$ is the commutator. For a time independent Hamiltonian, this results in

$$\Gamma(t) = e^{Ht}\Gamma(0)e^{H^T t}. \tag{5}$$

A joint system-bath covariance matrix has the form

$$\Gamma = \begin{pmatrix} \Gamma_S & -\Gamma_C^T \\ \Gamma_C & \Gamma_B \end{pmatrix}, \tag{6}$$

where Γ_S and Γ_B represent, respectively, the system and bath covariance matrices, and Γ_C records system-bath correlations. In other words, given a state ρ with covariance matrix Γ, tracing out the bath gives a reduced density matrix $\mathrm{tr}_B(\rho)$ with covariance matrix Γ_S. We define $\{\cdots\}_B$ to denote this process of reducing the covariance matrix, so $\{\Gamma\}_B = \Gamma_S$. In general, the reduced covariance matrix of an open quantum system will be

$$\Gamma_S(t) = \{e^{Ht}\Gamma(0)e^{H^T t}\}_B. \tag{7}$$

For an uncorrelated system $\Gamma_C = 0$, the covariance matrix has a direct sum form $\Gamma = \Gamma_S \oplus \Gamma_B$. The direct sum is linear, so that uncorrelated states have the form $\Gamma = (\Gamma_S \oplus \mathbf{0}) + (\mathbf{0} \oplus \Gamma_B)$, where $\mathbf{0}$ denotes an all zero matrices. The covariance reduction $\{\cdots\}_B$ is also linear, and so uncorrelated states evolve to

$$\Gamma_S(t) = \{e^{Ht}(\Gamma_S \oplus \mathbf{0})e^{H^T t}\}_B + \{e^{Ht}(\mathbf{0} \oplus \Gamma_B)e^{H^T t}\}_B. \tag{8}$$

Notice that the first term is independent of the bath variables such as temperature, and can be more compactly written as

$$\{e^{Ht}(\Gamma_S \oplus \mathbf{0})e^{H^T t}\}_B = D(t)\Gamma_S D(t)^T, \tag{9}$$

where $D(t) := \{e^{Ht}\}_B$. We are interested in the rate of decoherence. How quickly will two states become indistinguishable? Consider two different initial covariance matrices $\Gamma^{\tilde{\rho}} = \Gamma_S^{\tilde{\rho}} \oplus \Gamma_B$ and $\Gamma^{\rho} = \Gamma_S^{\rho} \oplus \Gamma_B$, e.g. describing logical encodings of qubit states. The time evolved difference between these covariance matrices is

$$\delta(t) := \Gamma_S^{\rho}(t) - \Gamma_S^{\tilde{\rho}}(t) = D(t)(\Gamma_S^{\rho} - \Gamma_S^{\tilde{\rho}})D(t)^T. \tag{10}$$

We observe that this is entirely independent of the bath temperature. As $\delta(t) \to \mathbf{0}$, the states becomes indistinguishable. Using $||\cdots||$ to denote the operator norm (the largest singular value) of a matrix, it is straightforward to show

$$\mathrm{tr}[i\tilde{c}_j\tilde{c}_k(\rho - \tilde{\rho})] \leq ||\delta(t)||, \tag{11}$$

where $\tilde{c}_j$ and $\tilde{c}_k$ are any pair of anti-commuting Majorana operators. Therefore, small $||\delta(t)||$ entails low probability of distinguishing ρ and $\tilde{\rho}$ through a single Gaussian measurement. We show later that this statement can be extended to completely general measurements. The operator norm is submultiplicative and transpose invariant so that

$$||\delta(t)|| \leq ||D(t)||^2||(\Gamma_S^{\rho} - \Gamma_S^{\tilde{\rho}})|| \leq 2||D(t)||^2, \tag{12}$$

with smaller $||D(t)||$ entailing more decoherence. We have used $||(\Gamma_S^{\rho} - \Gamma_S^{\tilde{\rho}})|| \leq 2$ to present an upperbound that is also independent of the initial state. Without system-bath interactions $D(t) = e^{H_S t}$ is unitary so that $||D(t)|| = 1$, but interactions lead to dissipation and $||D(t)|| < 1$. Under very general conditions we have determined that Gaussian decoherence occurs, quite remarkably, independently of the bath temperature. In some instances $||D(t)||$ may decrease with time, only to revive later. However, for a sufficiently complex bath we expect Markovian behavior lead to exponentially fast decoherence $||D(t)|| = e^{-\lambda t}$ for some λ. Next we introduce the formalism of Gaussian fermionic master equations, and then proceed to perform a microscopic derivation assuming weak-coupling. In such derivations various approximations are made, yet we find they respect temperature invariance.

3 Gaussian fermionic master equations

Here we review Gaussian fermionic master equations following Refs. [5, 32, 8]. The dynamical equation for such a system is

$$\frac{d\Gamma(t)}{dt} = X\Gamma(t) + \Gamma(t)X^T + Y, \tag{13}$$

where, for dissipative dynamics, X is not necessarily skew-symmetric. In general, $X = -H-P$ where H represents the unitary component (and is skew symmetric) and P represents the dissipative part (and is symmetric and positive). Typically, dissipative systems will have one steady state Γ_{ss} that satisfies $X\Gamma_{ss} + \Gamma_{ss}X^T = -Y$, and then

$$\Gamma(t) = e^{Xt}(\Gamma(0) - \Gamma_{ss})e^{X^T t} + \Gamma_{ss}. \tag{14}$$

These very general dynamical equations are the covariance matrix representation of a class of Lindblad master equations of the form

$$\frac{d\rho(t)}{dt} = i[H, \rho(t)] + \sum_{\mu}(2L_\mu \rho(t) L_\mu^\dagger - \{L_\mu^\dagger L_\mu, \rho(t)\}), \tag{15}$$

where the Hamiltonian H must be of the quadratic form introduced in Eq. (3) and the Lindblad operators are linear in Majorana operators

$$L_\mu = \sum_j l_{\mu,j} c_j. \tag{16}$$

One can prove [15, 8] that such a master equation gives rise to a Gaussian quantum channel with

$$X = -H - (M + M^*), \tag{17}$$
$$Y = 4i(M + M^*), \tag{18}$$

where M has elements $M_{j,k} = \sum_\mu l_{\mu,j} l^*_{\mu,k}$. The matrices X and Y will always be real so that $X^T = X^\dagger$ and $Y^T = Y^\dagger$. In the literature, there is some discussion of how such systems decohere Majorana qubits. However, prior work has centered on only the Kitave wire and has not considered how variables in Lindblad equations depend on the underlying system parameters.

4 Rates of thermalisation

We quantify the decoherence by the operator norm of $\delta(t) := \Gamma^{\rho}_S(t) - \Gamma^{\tilde{\rho}}_S(t)$. In general, $||\delta(t)|| \leq 2||D(t)||^2$ and from the previous section we see that $D(t) = e^{Xt}$. Theorem IX.3.1 of Bhatia [4] shows that for any X, we have $||e^{Xt}|| \leq ||e^{(X+X^\dagger)t/2}||$ as previously employed in this setting by Bravyi-König [8]. Using the shorthand $P := (X + X^\dagger)/2$, this entails

$$||\delta(t)|| \leq 2||e^{-Pt}||^2 = 2e^{-2\lambda_P t}. \tag{19}$$

We know λ_P is non-negative, so provided P does not have any zero eigenvalues there will be exponentially rapid decoherence. It is well known that decoherence rates are governed by the spectral properties of P. Our contribution is investigation of the dependence of this spectrum on microscopic factors.

The above statement holds for any pair of Gaussian states and any Gaussian channel. We are also interested in the more specific scenario where the Gaussian states lie in the degenerate groundspace of a physical Hamiltonian. Eigenstates of this Hamiltonian can be simultaneously diagonalised, and similarly their covariance matrices can be simultaneously brought into Williamson normal form. There exists a orthogonal matrix O, such that for every pure Gaussian ψ that is a eigenstate of the Hamiltonian we have

$$\Gamma^\psi = O\left(\bigoplus_j \gamma_j^\psi \tilde{\rho}\right) O^T, \tag{20}$$

where $\gamma_j^\psi \in \{\pm 1\}$ distinguish different eigenstates, and

$$\tilde{\rho} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{21}$$

For some values of j, the numbers γ_j^ψ tell us whether there is an excitation present. However, for degenerate Hamiltonians there are a set of degeneracy indices G, such that γ_j^ψ can vary without creating excitations for all $j \in G$. Therefore, the covariance matrices of groundstates break up into two blocks $\Gamma^\psi = O[\Gamma_G^\psi \oplus \Gamma_E]O^T$ where Γ_E is the same for all groundstates, and

$$\Gamma_G^\psi = \bigoplus_{j \in G} \gamma_j^\psi \tilde{\rho}. \tag{22}$$

Let us consider two encoded ground states $|\psi\rangle$ and $|\phi\rangle$. We deduce that $\delta = \Gamma^\psi - \Gamma^\phi = O[(\Gamma_G^\psi - \Gamma_G^\phi) \oplus \mathbf{0}]O^T$ where $\mathbf{0}$ is a zero matrix.

The matrix representing Hamiltonian dynamics has the same block structure as the covariance matrices, so that $H = O[H_G \oplus H_E]O^T$. When such a system is exposed to an environment, its dynamics are dictated by some matrix X. In many situations (including weakly coupled Markovian systems), X will obtain the same block structure as H, so that $X = O[H_G \oplus X_E]O^T$. It follows that

$$\delta(t) := \Gamma^\psi(t) - \Gamma^\phi(t) = O[e^{X_G t}(\Gamma_G^\psi - \Gamma_G^\phi)e^{X_G^T t} \oplus \mathbf{0}]O^T. \tag{23}$$

Defining $P_G = (X_G + X_G^\dagger)/2$, and using the same arguments as earlier we find

$$||\delta(t)|| \le e^{-2\lambda_{P_G} t}||(\Gamma_G^\psi - \Gamma_G^\phi)|| \le 2e^{-2\lambda_{P_G} t}. \tag{24}$$

Therefore, the decoherence of encoded ground states is governed by the spectrum of $P_G = -(X_G + X_G^\dagger)/2$.

The above arguments tell us that two initial Gaussian states undergoing Markovian dynamics will exponentially converge towards having identical covariance matrices. Therefore, the probability of distinguishing these states through a single Gaussian measurement decreases exponentially in time. However, a non-Gaussian measurement or multiple Gaussian measurements could prove more successful. In general, any strategy for distinguishing two states can always be captured by an observable M with eigenvalues ±1, with an average success probability

$$\mathrm{Pr} = \frac{1}{2}(1 + \mathrm{tr}[M(\rho - \tilde{\rho})]). \tag{25}$$

It is well known that $\mathrm{Pr} \le \frac{1}{2}||\rho - \tilde{\rho}||_{\mathrm{tr}}$ where the trace norm is $||A||_{\mathrm{tr}} := \mathrm{tr}[\sqrt{A^\dagger A}]$. Therefore, we aim to show convergence in 1-norm. We again compare two initial pure states encoding a qubit into 4 Majorana modes, and find that the time evolved density matrices states $\rho(t)$ and $\tilde{\rho}(t)$ satisfies

$$||\rho - \tilde{\rho}||_{\mathrm{tr}} \le 2e^{-2\lambda_{P_G} t}, \tag{26}$$

This follows quickly from Eq. (24) as we show in App. A.

5 Derivation of master equation

In this section we present a weak-coupling derivation of a Gaussian master equation in the covariance matrix formalism. Many of the steps directly mirror those made in a textbook density matrix derivation (see e.g. Chap 3 of Ref. [31]). We assume both the system, the heat bath and their interaction is entirely Gaussian. In addition, we make the usual assumptions involved in deducing master equations, notably that system-bath coupling is weak and that the system-bath are effectively uncorrelated at all times. The whole system-bath dynamics are described by a Hamiltonian with block matrix structure

$$H = \begin{pmatrix} H_S & -H_I^T \\ H_I & H_B \end{pmatrix}, \tag{27}$$

where H_S and H_B represent, respectively, the system and bath Hamiltonians and satisfy $H_x = -H_x^T$ for $x = S, B$. The interaction is represented by H_I^T a real-valued, not necessarily square, matrix. The initial ($t = 0$) system-bath convariance matrix has the form

$$\Gamma(0) = \begin{pmatrix} \Gamma_S(0) & 0 \\ 0 & \Gamma_B \end{pmatrix}. \tag{28}$$

Before proceeding we shift to an interaction picture, defining

$$\Gamma_{\text{int}}(t) := e^{(H_S \oplus H_b)t} \Gamma(t) e^{-(H_S \oplus H_b)t}. \tag{29}$$

It follows that

$$\frac{d\Gamma_{\text{int}}(t)}{dt} = [\Gamma_{\text{int}}(t), H_{\text{int}}(t)], \tag{30}$$

where

$$H_{\text{int}}(t) = e^{(H_S \oplus H_B)t} \begin{pmatrix} 0 & -H_I \\ H_I & 0 \end{pmatrix} e^{-(H_S \oplus H_B)t}. \tag{31}$$

This simplifies to

$$H_{\text{int}}(t) = \begin{pmatrix} 0 & -H_I^T(t) \\ H_I(t) & 0 \end{pmatrix}, \tag{32}$$

where $H_I(t) = e^{H_B t} H_I e^{-H_S t}$. Once in the interaction picture, we integrate over time to find

$$\Gamma_{\text{int}}(t) = \Gamma_{\text{int}}(0) + \int_0^t [\Gamma_{\text{int}}(s), H_{\text{int}}(s)] ds. \tag{33}$$

Therefore the time derivative is

$$\frac{d\Gamma_{\text{int}}(t)}{dt} = [\Gamma_{\text{int}}(0), H_{\text{int}}(t)] + \int_0^t [[\Gamma_{\text{int}}(s), H_{\text{int}}(s)], H_{\text{int}}(t)] ds. \tag{34}$$

We are only interested in the system covariance matrix, which is the covariance reduction $\{...\}_B$ of the above expression. It is straightforward to verify $\{[\Gamma_{\text{int}}(0), H_{\text{int}}(t)]\}_B = 0$, so

$$\frac{d\{\Gamma_{\text{int}}(t)\}_B}{dt} = \int_0^t \{[[\Gamma_{\text{int}}(s), H_{\text{int}}(s)], H_{\text{int}}(t)]\}_B ds. \tag{35}$$

Next, we assume the coupling is weak and that the system stays uncorrelated from the bath. Formally, this entails that $\Gamma_{\text{int}}(s) \rightarrow \{\Gamma_{\text{int}}(t)\}_B \oplus \Gamma_B$, and also that $H_{\text{int}}(s) \rightarrow H_{\text{int}}(t - s)$

and the integral is extended to infinity. Such assumptions directly mirror those made on the level of Hilbert spaces and result in the expression

$$\frac{d\tilde{\Gamma}(t)}{dt} = \int_0^\infty \{[[\Gamma_{\rm int}(t), H_{\rm int}(t-s)], H_{\rm int}(t)]\}_B ds, \tag{36}$$

where have made use of the shorthand $\tilde{\Gamma}(t) := \{\Gamma_{\rm int}(t)\}_B$. Next we may use our knowledge of the block structure of the covariance matrices to evaluate the commutator, and find

$$\begin{aligned}\{[[\Gamma_{\rm int}(t), H_{\rm int}(t-s)], H_{\rm int}(t)]\}_B = &-H_I^T(t)H_I(t-s)\tilde{\Gamma}(t) - \tilde{\Gamma}(t)H_I^T(t-s)H_I(t)\\ &+ H_I^T(t)\Gamma_B H_I(t-s) + H_I^T(t-s)\Gamma_B H_I(t).\end{aligned}$$

Combining this with Eq. (36), and collecting terms to match Eq. (13) we have

$$\frac{d\tilde{\Gamma}(t)}{dt} = X\tilde{\Gamma} + \tilde{\Gamma}X^T + Y, \tag{37}$$

where

$$\begin{aligned} X &= -\int_0^\infty H_I^T(t)H_I(t-s)ds, \qquad (38)\\ Y &= \int_0^\infty H_I^T(t)\Gamma_B H_I(t-s) + H_I^T(t-s)\Gamma_B H_I(t)ds.\end{aligned}$$

We have succeeded in deriving a form of a Gaussian quantum channel. Though to make these equations meaningful we require that the integrals converge to finite values. For finite size matrices the integrands will be periodic functions and typically do not converge to a finite value. Whereas, in the limit of infinite matrices the eigenvalue spectrum may become continuous and the integrand may vanish in the large s limit. Furthermore, to yield Markovian dynamics the resulting X and Y must be time independent. Before proceeding we can already observe that all Γ_B dependence has vanished from X.

Presently, the matrix X still carries an overt time dependence, which can be removed by making the secular approximation (SA). First we recall the explicit time dependence, $H_I(t) = e^{H_B t}H_I e^{-H_S t}$ so that

$$\begin{aligned} X &= \int_0^\infty e^{H_S t}H_I^T e^{-H_B t}e^{H_B(t-s)}H_I e^{-H_S(t-s)}ds,\\ &= \int_0^\infty e^{H_S t}H_I^T e^{H_B s}H_I e^{-H_S(t-s)}ds. \qquad (39)\end{aligned}$$

We proceed by noting that H_S is real and skew-Hermitian, so it has imaginary eigenvalues $i\omega_j$, eigenvectors $|j\rangle$, and a diagonal form

$$H_S = i\sum_j \omega_j |j\rangle\langle j|. \tag{40}$$

This entails

$$X = -\sum_{j,k}\int_s^\infty e^{i(\omega_j-\omega_k)t}|j\rangle\langle k|f_{j,k}(s)e^{i\omega_k s},$$

where

$$f_{j,k}(s) = \langle j|H_I^T e^{-H_B s}H_I|k\rangle. \tag{41}$$

The SA asserts that terms with rapidly oscillating phases $e^{i(\omega_j-\omega_k)t}$ can be neglected, except of course when $\omega_j - \omega_k = 0$. This is valid at times longer than the reciprocal of the smallest energy gaps, $t \gg [\min_{\omega_j \neq \omega_k} |\omega_j - \omega_k|]^{-1}$. For now, we assume this to be true, but later we will show that a much weaker energy gap condition entails many of the same features. Making the SA leads to:

$$X = -\sum_j \sum_{k;\omega_k=\omega_j} |j\rangle\langle k| \int_0^\infty e^{i\omega_k s} f_{j,k}(s) ds \tag{42}$$

We see that SA has removed any dependence on t making time evolution Markovian. Furthermore, the SA forces X to commute with H_S, and so X has the same block-diagonal structure as H_S.

All matrices can be decomposed into $X = -H - P$ where $H^\dagger = -H$ and $P^\dagger = P$. Performing just such a decomposition of X we can show, via Bochner's theorem, that the Hermitian part P has eigenvalues that are real and nonnegative (see App. C). Furthermore, both matrices have real-valued elements, so $H^\dagger = H^T$ and $P^\dagger = P^T$, which entails that H has purely imaginary eigenvalues, just as expected. In Sec. 4 we saw that decoherence rates are governed by P. Recall that P_G is the restriction of P to the kernel of H_S (equivalently the groundspace of the associated Hamiltonian, assuming $E_0 = 0$), and the decoherence rates between groundstates are governed by the spectrum of P_G. Furthermore, this restricted P_G matrix naturally emerges when one considers a relaxed SA assumption.

Recall that the validity of SA required that all energy gaps are large compared to a relevant time scale. Many interesting topological systems have a degenerate groundspace with a large gap to the first excited state, but then the spectrum of excitations will be dense or even a continuum in the large system limit. This means that SA cannot be used to eliminate transitions between different excited states. However, provided the groundspace is gapped from excitations, we will have a limited application of SA that decouples X into $O(X_G \oplus X_E)O^T$ and with X_G describing the dynamics within the ground space. Although SA will not apply to the dynamics X_E of the excitations, we saw in Sec. 4 that decoherence in the groundspace is governed by only X_G. In particular, it is dictated by the largest eigenvalue of P_G.

6 Detailed balance and the Arrhenius law

The bath temperature only influences what state we converge to, and not how quickly we get there. This conclusion is quite remarkable. So much so, that naively it seems to violate some basic tenet of physics. Two candidates are the Arrhenius law and detailed balance.

The Arrhenius law is an empirical rule of thumb that has been successful in modeling chemical reactions. Recently, it has been suggested that it may also apply to quantum memories, though violations have been observed in various settings [24, 37, 40]. The Arrhenius law predicts that decoherence times scale as $e^{\Delta/T}$ where Δ is the system gap. We have a gapped degenerate ground space, but quasiparticles from the environment can poison the system without creating an excitation. From this perspective perhaps we should consider $\Delta = 0$, and our temperature independence to be consistent with the Arrhenius law. However, although we have focused on ground space decoherence our observation apply also to the dynamics of excitations with a discrete spectrum. That is, the rate at which excitation populations equilibrate is also temperature independent! Indeed, the Arrhenius law is not a universal law and we conclude that it is absolutely violated in the domain of Gaussian fermions.

Detailed balance is a form of microscopic reversibility. It states that at thermal equilibrium the population transfer is symmetric for each process. Consequently, the rate of transitions must depend on the temperature. At first this seems to imply that decoherence rates must be temperature dependent. Indeed, detailed balance has been used to study decoherence times of spin (qubit) systems with the toric code Hamiltonian [2] and cubic code Hamiltonian [7]. These results revealed an exponential temperature dependence, and so one may expect this feature to be generic. Though these are highly non-Gaussian systems. In the Gaussian setting, Temme *et al.* [38] have rigorously proved very general bounds on thermalization rates. Their analysis appears to show an explicit temperature dependence, but closer inspection reveals variables that depend on the specific features of the bath. These variables can be set, whilst still respecting detailed balance, to precisely cancel all temperature dependence. We have seen that when the whole system-bath is Gaussian, this is indeed what happens. To further illustrate that temperature independence is consistent with detailed balance we present in App. B a very simple classical Markov process where convergence rates decouple from temperature. Detailed balance has an esteemed history going back to Boltzmann, who proclaimed it a key axiom of statistical mechanics and used it to great effect. However, there has been a recent surge of interest in non-equilibrium statistical mechanics, where detailed balance is violated, both in quantum [39, 14] and classical settings [12].

7 Comments on prior work

Mazza *et al.* [25] studied the effect of various noise models on the 1-dimensional Kitaev chain. Their main result is that various Hamiltonian perturbations will decohere the system, but this decoherence is suppressed by increasing the length of the Kitaev chain. Mazza *et al.* conclude their paper by also discussing a more destructive noise model, open systems dynamics (see pg.4 of Ref. [25]). This model is a master equation with the Hamiltonian of the standard Kitaev wire (with chemical potential set to zero), and Lindblad operators

$$L_\mu = \eta a^\dagger_\mu = \eta \frac{1}{2}(c_{2\mu-1} + i c_{2\mu}), \tag{43}$$

which allows for fermions hopping to the environment and where we use η to parameterize the strength of the hopping. They give numerical plots for decoherence of this model, but it can also be understood analytically. We proceed by casting these master equations in the language of covariance matrices, and find

$$M = \frac{\eta^2}{4} \bigoplus_j \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \tag{44}$$

Composing $M + M^*$ will cancel the imaginary parts, giving

$$X = -H - (M + M^*) = -H - \frac{\eta^2}{2} 1, \tag{45}$$

Note that the eigenvalues of H are purely imaginary so that e^{Ht} is unitary, but the dissipative component adds a constant real negative component. We have that $D(t) = e^{Xt} = e^{-\eta^2 t/2} e^{Rt}$ and $e^{X^T t} = e^{-\eta^2 t/2} e^{H^T t}$. Therefore, decoherence occurs at the rate $||D(t)|| = e^{-\eta^2 t/2}$. Here it is clear that system size and Hamiltonian gap play no role, provided η is not a function of these variables. Mazza *et al.* do not discuss how η itself might depend on the energy gap or on temperature.

Budich *et al.* [10] made similar observations. They considered two models where only the end of a Kitaev wire couples to the environment. In both models the system-environment coupling has the form $H_{\text{int}} = A_{\text{bath}} c_1$ where A_{bath} is some operator acting on the bath. They also considered the standard Kitaev chain with zero chemical potential, so that the interaction commuted with the system Hamiltonian. They observed rapid decoherence of Majorana edge modes, with no dependence on the energy gap. These toy models are excellent ways to illustrate a serious deficit in prior claims to effectiveness of topological protection of Majorana edge modes. However, they tell us little about what to expect when the interaction and Hamiltonian do not commute. Furthermore, one may also wish to consider much more exotic models, such as Majorana fermions in 2D systems or even higher dimensions. These gaps in previous work are now filled by the more general insights presented here.

8 Conclusions and acknowledgements

We have seen that decoherence of Gaussian fermionic systems cannot be reduced by cooling. For Markovian dynamics, we provided a microscopic derivation of the master equation in the weak coupling limit, leading to exponentially fast decoherence. Therefore, to use Gaussian systems as a quantum memory they must be either highly non-Markovian or have minimal tunneling with any nearby Gaussian heat baths. Eliminating tunneling is potentially challenging when in any of the many popular proposals for acquiring topological order through the proximity effect [17, 36]. In these proposals, electron hopping with an external s-wave superconductor is the mechanism by which topological robustness is acquired. Both electron hopping and the superconducting Hamiltonian are Gaussian, and so this opens the door to temperature invariant decoherence. For such systems it is urgent that we acquire a better understanding of the proximity effect from an open systems perspective.

After completing this work, the author forwarded the manuscript to Leonardo Mazza who in return kindly shared several unpublished yet interesting results [26, 19, 20]. These tackle related problems of interactions with fermionic baths, including various numerical simulations of small fermionic (and bosonic) baths and numerous analytic insights. Particularly relevant is Sec. 7 of his PhD thesis [26], where Mazza makes several observations also made here, although does he not remark on the temperature independence of decoherence rates.

We thank Pieter Kok and Keith Burnett for interesting discussions on Majorana fermions that lead to this research. We thank Michael Kastoryano, Tomaz Prozen, Jens Eisert and Leonardo Mazza for comments on the manuscript.

References

1 Jason Alicea. New directions in the pursuit of majorana fermions in solid state systems. *Reports on Progress in Physics*, 75(7):076501, 2012.

2 Robert Alicki, Mark Fannes, and Michal Horodecki. On thermalization in kitaev's 2d model. *Journal of Physics A: Mathematical and Theoretical*, 42(6):065303, 2009.

3 H. Bernigau, M. J. Kastoryano, and J. Eisert. Mutual information area laws for thermal free fermions. *Journal of Statistical Mechanics: Theory and Experiment*, 2015(2):P02008, 2015.

4 Rajendra Bhatia. *Matrix analysis*, volume 169. Springer, 1997.

5 Sergey Bravyi. Lagrangian representation for fermionic linear optics. *Quant. Inf. and Comp.*, 3:216, 2005.

6 Sergey Bravyi. Universal quantum computation with the $\nu = 5/2$ fractional quantum hall state. *Phys. Rev. A*, 73:042313, 2006.

7 Sergey Bravyi and Jeongwan Haah. Quantum self-correction in the 3d cubic code model. *Physical review letters*, 111(20):200501, 2013.

8 Sergey Bravyi and Robert König. Classical simulation of dissipative fermionic linear optics. *arXiv preprint arXiv:1112.2184*, 2011.

9 Benjamin J. Brown, Daniel Loss, Jiannis K. Pachos, Chris N. Self, and James R. Wootton. Quantum memories at finite temperature. *arXiv preprint arXiv:1411.6643*, 2014.

10 Jan Carl Budich, Stefan Walter, and Björn Trauzettel. Failure of protection of majorana based qubits against decoherence. *Phys. Rev. B*, 85:121405, Mar 2012.

11 Earl T. Campbell, Matty Hoban, and Jens Eisert. Majorana fermions and non-locality. *Quant. Info. Comm.*, 14:0981, 2014.

12 T. Chou, K. Mallick, and R. K. P. Zia. Non-equilibrium statistical mechanics: from a paradigmatic model to biological transport. *Reports on progress in physics*, 74(11):116601, 2011.

13 Fernando de Melo, Piotr Piotr Cwiklinski, and Barbara M. Terhal. The power of noisy fermionic quantum computation. *New J. Phys.*, 15(1):013015, 2013.

14 Konstantin E. Dorfman, Dmitri V. Voronine, Shaul Mukamel, and Marlan O. Scully. Photosynthetic reaction center as a quantum heat engine. *Proceedings of the National Academy of Sciences*, 110(8):2746–2751, 2013.

15 J. Eisert and T. Prosen. Noise-driven quantum criticality. *arXiv preprint arXiv:1012.5013*, 2010.

16 Marcel Franz. Majorana's wires. *Nat Nano*, 8(3):149–152, 03 2013.

17 Liang Fu and C. L. Kane. Superconducting proximity effect and majorana fermions at the surface of a topological insulator. *Phys. Rev. Lett.*, 100:096407, Mar 2008.

18 G. Goldstein and C. Chamon. Decay rates for topological memories encoded with majorana fermions. *Phys. Rev. B*, 84:205109, Nov 2011.

19 Matteo Ippoliti. Quantum recovery operations. Master's thesis, Universita di Pisa, 2014.

20 Matteo Ippoliti, Vittorio Giovannetti, Matteo Rizzi, and Leonardo Mazza. In preparation.

21 Michael J Kastoryano and Jens Eisert. Rapid mixing implies exponential decay of correlations. *Journal of Mathematical Physics*, 54(10):102201, 2013.

22 A. Yu Kitaev. Unpaired majorana fermions in quantum wires. *Physics-Uspekhi*, 44(10S):131, 2001.

23 Francois Konschelle and Fabian Hassler. Effects of nonequilibrium noise on a quantum memory encoded in majorana zero modes. *Phys. Rev. B*, 88:075431, Aug 2013.

24 Li-Chung Ku and Clare C. Yu. Decoherence of a josephson qubit due to coupling to two-level systems. *Phys. Rev. B*, 72:024526, Jul 2005.

25 L. Mazza, M. Rizzi, M. D. Lukin, and J. I. Cirac. Robustness of quantum memories based on majorana zero modes. *Phys. Rev. B*, 88:205142, Nov 2013.

26 Leonardo Mazza. *Quantum Simulation of Topological States of Matter.* PhD thesis, Technische Universität München, 2012.

27 V. Mourik, K. Zuo, S. M. Frolov, S. R. Plissard, E. P. A. M. Bakkers, and L. P. Kouwenhoven. Signatures of majorana fermions in hybrid superconductor-semiconductor nanowire devices. *Science*, 336(6084):1003–1007, 2012.

28 Stevan Nadj-Perge, Ilya K. Drozdov, Jian Li, Hua Chen, Sangjun Jeon, Jungpil Seo, Allan H. MacDonald, B. Andrei Bernevig, and Ali Yazdani. Observation of majorana fermions in ferromagnetic atomic chains on a superconductor. *Science*, 346(6209):602–607, 2014.

29 Chetan Nayak, Steven H. Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, 80(3):1083, 2008.

30 Fabio L. Pedrocchi and David P. DiVincenzo. Majorana braiding with thermal noise. *arXiv 1505.03712*, 2015.

31 Francesco Petruccione and Heinz-Peter Breuer. *The theory of open quantum systems.* Oxford university press, 2002.

32 Tomaž Prosen. Third quantization: a general method to solve master equations for quadratic open fermi systems. *New Journal of Physics*, 10(4):043026, 2008.

33 Tomaž Prosen. Spectral theorem for the lindblad equation for quadratic open fermionic systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2010(07):P07020, 2010.

34 Tomaž Prosen and Bojan Žunkovič. Exact solution of markovian master equations for quadratic fermi systems: thermal baths, open xy spin chains and non-equilibrium phase transition. *New Journal of Physics*, 12(2):025016, 2010.

35 Diego Rainis and Daniel Loss. Majorana qubit decoherence by quasiparticle poisoning. *Phys. Rev. B*, 85:174533, May 2012.

36 Jay D. Sau, Roman M. Lutchyn, Sumanta Tewari, and S. Das Sarma. Robustness of majorana fermions in proximity-induced superconductors. *Phys. Rev. B*, 82:094522, Sep 2010.

37 Alexander Shnirman, Gerd Schön, Ivar Martin, and Yuriy Makhlin. Low- and high-frequency noise from coherent two-level systems. *Phys. Rev. Lett.*, 94:127002, Apr 2005.

38 Kristan Temme, Fernando Pastawski, and Michael J. Kastoryano. Hypercontractivity of quasi-free quantum semigroups. *Journal of Physics A: Mathematical and Theoretical*, 47(40):405303, 2014.

39 Hannu Wichterich, Markus J. Henrich, Heinz-Peter Breuer, Jochen Gemmer, and Mathias Michel. Modeling heat transport through completely positive maps. *Physical Review E*, 76(3):031115, 2007.

40 Beni Yoshida. Violation of the arrhenius law below the transition temperature. *arXiv preprint arXiv:1404.0457*, 2014.

A Trace norm convergence

We assume initial states of the form $\rho(0) = |\psi\rangle\langle\psi| = |\psi_G\rangle\langle\psi_G| \otimes M_{G^\perp}$ and $\tilde{\rho}(0) = |\phi\rangle\langle\phi| \otimes M_{G^\perp}$ encoding different qubit states. These initial states differ only on 4-Majorana modes within the groundspace, and the evolution of the covariance matrix shows that this property holds at later times so that

$$\rho(t) = \rho_G(t) \otimes M_{G^\perp} \ , \ \tilde{\rho}(t) = \tilde{\rho}_G(t) \otimes M_{G^\perp}. \tag{46}$$

Therefore,

$$\begin{aligned} ||\rho(t) - \tilde{\rho}(t)||_{\text{tr}} &= ||(\rho_G(t) - \rho'_G(t)) \otimes M_{G^\perp}||_{\text{tr}} \\ &= ||\rho_G(t) - \rho'_G(t)||_{\text{tr}}, \end{aligned} \tag{47}$$

where we have used $||A \otimes B||_{\text{tr}} = ||A||_{\text{tr}}||B||_{\text{tr}}$ and $||M_{G^\perp}||_{\text{tr}} = 1$. The Hilbert space of 4 Majorana modes supports one qubit in the even parity subspace and one qubit in the odd parity subspace. In other words, $\rho_G(t) = \rho_G^{(0)}(t) \oplus \rho_G^{(1)}(t)$ and similarly $\tilde{\rho}_G(t) = \tilde{\rho}_G^{(0)}(t) \oplus \tilde{\rho}_G^{(1)}(t)$. Using $||A \oplus B||_{\text{tr}} = ||A||_{\text{tr}} + ||B||_{\text{tr}}$ we have

$$||\rho(t) - \tilde{\rho}(t)||_{\text{tr}} = \sum_{x=0,1} ||\rho_G^{(x)}(t) - \tilde{\rho}_G^{(x)}(t)||_{\text{tr}}. \tag{48}$$

For a single qubit, we have $||\rho||_{\text{tr}} = \max_{\tilde{\rho} \in \mathcal{B}} \text{tr}[\tilde{\rho}\rho]$ where the maximum is over all single qubit Hermitian unitary operators, such as the Pauli spin operators. In a Majorana encoding the Pauli spin operators, indeed all single qubit Hermitian unitary operators, are quadratic observables. These expectation values never exceed the operator norm of the $\delta(t)$. Therefore,

$$||\rho(t) - \tilde{\rho}(t)||_{\text{tr}} \leq ||\delta(t)||. \tag{49}$$

Finally, we make use of Eq. (24) to arrive at Eq. (26).

B Remarks on detailed balance

Here we describe the concept of detailed balance for 2-state systems. We show in this simple setting the concept is consistent with temperature invariant decoherence rates. Furthermore, we show that Gaussian 2-mode Markov processes always obey this principle. Consider, a classical system with two possible states, with probabilities described by a Markov chain

$$v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} p \\ 1-p \end{pmatrix}. \tag{50}$$

For simplicity we consider time to be in discrete steps, with a transition matrix

$$P = \begin{pmatrix} P_{1\to 1} & P_{2\to 1} \\ P_{1\to 2} & P_{2\to 2} \end{pmatrix}, \tag{51}$$

so that $v(t) = P^t v$. Conserving flow of probability requires $P_{k\to 1} + P_{k\to 2} = 1$ for $k = 1, 2$.

We say π is a stationary state of P, if $P\pi = \pi$, and where $\pi := (\alpha, 1-\alpha)$. The process P satisfies detailed balance if

$$P_{1\to 2}\alpha = P_{2\to 1}(1-\alpha). \tag{52}$$

One can think of π as a thermal distribution, so $\alpha = Z\exp(-E_1\beta)$ and $(1-\alpha) = Z\exp(-E_2\beta)$, where $Z = \exp(-E_1\beta) + \exp(-E_2\beta)$ is the partition function. As usual, β is inverse temperature. In this thermal language, detailed balance entails that

$$\frac{P_{2\to 1}}{P_{1\to 2}} = \frac{\alpha}{1-\alpha} = \exp(\Delta\beta), \tag{53}$$

where Δ is the energy gap $E_2 - E_1$. It appears that the (ratio of) transition rates depend on the temperature of the steady state, and so one might be tempted to conclude that convergence rates likewise depend on temperature.

The conservation of probability and detailed balance give 3 independent linear constraints on P, out of the 4 parameters of the matrix. Therefore, the space of valid matrices is 1-dimensional and includes

$$P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, P_\pi = \begin{pmatrix} \alpha & \alpha \\ 1-\alpha & 1-\alpha \end{pmatrix}. \tag{54}$$

Both matrices satisfy Eq. (52). Furthermore, for all Markov chains v we have $P_1 v = v$ and $P_\pi v = \pi$. The whole set of suitable matrices is contained in the span of these matrices,

$$\begin{aligned} P_\eta &= (1-\eta)P_1 + \eta P_\pi \\ &= \begin{pmatrix} \eta\alpha + (1-\eta) & \eta\alpha \\ \eta(1-\alpha) & \eta(1-\alpha) + (1-\eta) \end{pmatrix}, \end{aligned} \tag{55}$$

with $0 \leq \eta \leq \min[1/\alpha, 1/(1-\alpha)] \leq 2$ to ensure $P_{i\to j} \in [0,1]$. Within these limits, η is a free parameter. We consider a general initial probability distribution it always has the form $v = \pi + p\tilde{\rho}$ for some value p, where $\tilde{\rho} = (1, -1)$. It is easy to confirm $P_1\tilde{\rho} = \tilde{\rho}$ and $P_\pi\tilde{\rho} = 0$. Therefore, $Pv = (1-\eta)v + \eta\pi = \pi + p(1-\eta)\tilde{\rho}$ and for t time steps this extends to

$$v(t) = P^t v = \pi + p(1-\eta)^t\tilde{\rho}. \tag{56}$$

This clearly shows exponentially rapid convergence to the equilibrium state at a speed governed by η. More precisely, using any norm $||\ldots||$ to measure distance we have

$$||v(t) - \pi|| = p|1-\eta|^t||\tilde{\rho}||. \tag{57}$$

The convergence speed is entirely independent of temperature, and only depends on the free parameter η. The only temperature dependence lies in $\eta \leq \min[1/\alpha, 1/(1-\alpha)]$, since α depends on temperature. However, $\alpha \in [0,1]$ and so the range $\eta \in [0,1]$ is valid at all temperatures. Therefore we can consider a family of Markov process with varying temperature and constant $\eta \in [0,1]$. This family is consistent with detailed balance, but has a convergence rate independent of temperature.

The convergence rate could vary with temperature if η is a non-constant function of temperature. Although, there is no reason *a piori* to favour one function for η over another. Certainly, many possible temperature dependencies are consistent with detailed balance. Unless, one has a physical model of the encompassing system and can perform a microscopic derivation of the Markov process, and so derive η. This is exactly what we have performed for the case of Gaussian fermions, showing the analogous result of temperature independent η. Lastly, we remark that this entire discussion can be recast in continuous time by considering P to be the generator of a Markov process with transition matrix $Q(t) = e^{Pt}$.

It is still interesting to ask if Gaussian Markov processes obey detailed balance. Let us just consider a pair of modes, with a 2-by-2 covariance matrix

$$\Gamma = \begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix} \tag{58}$$

The physical system is in one of two states (superpositions are disallowed by fermion parity superselection), with probability $p = (1+\lambda)/2$ and $1-p = (1-\lambda)/2$. A Markov process maps $\Gamma \to X\Gamma X^T + Y$ where Y is skew-symmetric. Under this process, we find some x, y such that $\lambda \to x\lambda + y$. Therefore, $p \to px + \frac{1}{2}(1+y-x)$ and the probability transition matrix has the form

$$P = \begin{pmatrix} \frac{1}{2}(1+x+y) & \frac{1}{2}(1-x+y) \\ \frac{1}{2}(1-x-y) & \frac{1}{2}(1+x-y) \end{pmatrix} \tag{59}$$

In the steady state $p_{\mathrm{ss}} = p_{\mathrm{ss}}x + \frac{1}{2}(1+y-x)$ and so that

$$\begin{aligned} p_{\mathrm{ss}} &= \frac{1-x+y}{2(1-x)}, \\ 1-p_{\mathrm{ss}} &= \frac{1-x-y}{2(1-x)}. \end{aligned}$$

Therefore,

$$\frac{p_{\mathrm{ss}}}{1-p_{\mathrm{ss}}} = \frac{1-x+y}{1-x-y} = \frac{P_{2\to 1}}{P_{1\to 2}} \tag{60}$$

so that detailed balance is satisfied for all x, y.

C Application of Bochner's theorem

Here we show that the Hermitian part of X has strictly negative eigenvalues. The proof makes use of Bochner's theorem, which relates properties of functions to their Fourier transform. To introduce this theorem, we first define the concept of functions of positive-type

▶ **Definition 1.** An absolutely integrable function $\phi : \mathbb{C} \to \mathbb{C}$ is of positive type if for all sets of complex numbers $\{c_1, c_2, \ldots\}$ the following summation is real-valued and positive

$$\sum_{n,m} c_n^* c_m \phi(c_n - c_m) \geq 0. \tag{61}$$

Note that being of positive type is very different from a function taking positive values. Now we can state

▶ **Theorem 2.** *Bochner's theorem: Let ϕ be an absolutely integrable function. The fourier transformed function $\tilde{\phi}$ is a real-valued positive function if and only if ϕ is of positive type.*

Returning to the problem at hand, $B = (X + X^\dagger)/2$ is Hermitian by construction. From Eq. (41) we already have an expression for X, and considering $X^\dagger$ we observe that

$$\begin{aligned} X^\dagger &= -\sum_j \sum_{k,\omega_k=\omega_j} |k\rangle\langle j| \int_0^\infty e^{i\omega_k s} f^*_{j,k}(s)ds, \\ &= \sum_j \sum_{k,\omega_k=\omega_j} |k\rangle\langle j| \int_0^{-\infty} e^{i\omega_k s} f^*_{j,k}(-s)ds, \end{aligned} \tag{62}$$

where we have made the change of variables $s \to -s$. Switching the order of integration,

$$X^\dagger = -\sum_j \sum_{k,\omega_k=\omega_j} |k\rangle\langle j| \int_{-\infty}^0 e^{i\omega_k s} f^*_{j,k}(-s)ds. \tag{63}$$

Next, we use that $f^*_{j,k}(-s) = f_{k,j}(s)$, which can be seen from

$$\begin{aligned} f^*_{j,k}(-s) &= \langle j|H_I^\dagger e^{H_B s} H_I|k\rangle^\dagger, \\ &= \langle k|H_I^\dagger e^{-H_B^\dagger s} H_I|j\rangle, \end{aligned} \tag{64}$$

and using $H_B^\dagger = H_B^T = -H_B$ we have the result. Applying this to our expression for $X^\dagger$, and switching the dummy variables $j \leftrightarrow k$ gives

$$X^\dagger = -\sum_j \sum_{k,\omega_k=\omega_j} |j\rangle\langle k| \int_{-\infty}^0 e^{i\omega_k s} f_{j,k}(s)ds. \tag{65}$$

This differs from X in only the domain of the integral and so

$$X^\dagger + X = -\sum_j \sum_{k,\omega_k=\omega_j} |j\rangle\langle k| \int_{-\infty}^\infty e^{i\omega_k s} f_{j,k}(s)ds.$$

For each set of variables, j, k, the integral is a Fourier transform of $f_{j,k}$ evaluated at ω_k, so

$$X^\dagger + X = -\sum_j \sum_{k,\omega_k=\omega_j} |j\rangle\langle k| \tilde{f}_{j,k}(s)ds.$$

Notice, we have denoted Fourier transforms with a tilde. Next, we show that $f_{j,k}$ is of positive-type. For all $\{c_1, c_2, \ldots\}$

$$\sum_{n,m} c_n^* c_m f_{j,k}(c_n - c_m) = \langle w|w\rangle, \tag{66}$$

where

$$|w\rangle = \sum_m c_m e^{H_B c_m} H_I|k\rangle. \tag{67}$$

Since $\langle w|w\rangle \geq 0$, we can apply Bochner's theorem and conclude that all $\tilde{f}_{j,k}(\omega_k)$ are positive and real. If H_S is a nondegenerate matrix, then there would be no multiplicity of eigenvectors with the same eigenvalue and $-\tilde{f}_{k,k}(\omega_k)$ would represent the real-negative eigenvalues of $X + X^\dagger$. However, for degenerate matrices there is a freedom of choice in the basis $\{|k\rangle\}$, but we can always set this to be the eigenbasis of $X + X^\dagger$. Therefore, $X + X^\dagger$ has real negative eigenvalues.

On the Closure of the Completely Positive Semidefinite Cone and Linear Approximations to Quantum Colorings

Sabine Burgdorf[1], Monique Laurent[1,2], and Teresa Piovesan[1]

1 Centrum Wiskunde & Informatica (CWI)
Amsterdam, The Netherlands
2 Tilburg University
Tilburg, The Netherlands

Abstract

We investigate structural properties of the completely positive semidefinite cone $\mathcal{CS}_+^n$, consisting of all the $n \times n$ symmetric matrices that admit a Gram representation by positive semidefinite matrices of any size. This cone has been introduced to model quantum graph parameters as conic optimization problems. Recently it has also been used to characterize the set $\mathcal{Q}$ of bipartite quantum correlations, as projection of an affine section of it. We have two main results concerning the structure of the completely positive semidefinite cone, namely about its interior and about its closure. On the one hand we construct a hierarchy of polyhedral cones which covers the interior of $\mathcal{CS}_+^n$, which we use for computing some variants of the quantum chromatic number by way of a linear program. On the other hand we give an explicit description of the closure of the completely positive semidefinite cone, by showing that it consists of all matrices admitting a Gram representation in the tracial ultraproduct of matrix algebras.

1998 ACM Subject Classification G.1.2 [Mathematics in Computing] Approximation, F.2.2 [Analysis of Algorithms and Problem Complexity] Nonnumerical Algorithms and Problems, F.2.1 [Analysis of Algorithms and Problem Complexity] Numerical Algorithms and Problems

Keywords and phrases Quantum graph parameters, Trace nonnegative polynomials, Copositive cone, Chromatic number, Quantum Entanglement, Nonlocal games, Von Neumann algebra

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.127

1 Introduction

General background

Entanglement, one of the most peculiar features of quantum mechanics, allows different parties to be correlated in a non-classical way. Properties of entanglement can be studied through the set of bipartite quantum correlations, commonly denoted as $\mathcal{Q}$, consisting of the conditional probabilities that two physically separated parties can generate by performing measurements on a shared entangled state. More formally, a conditional probability distribution $(P(a,b|x,y))_{a\in A,b\in B,x\in X,y\in Y}$ is called *quantum* if $P(a,b|x,y) = \psi^\dagger E_x^a \otimes F_y^b \psi$ for some unit vector ψ in a finite dimensional Hilbert space $\mathcal{H}$ and some sets of positive semidefinite matrices (aka measurement operators) $\{E_x^a : a \in A\}$ and $\{F_y^b : b \in B\}$ satisfying $\sum_{a\in A} E_x^a = I$ and $\sum_{b\in B} F_y^b = I$ for all $x \in X, y \in Y$. Clearly, we can equivalently assume that the unit vector ψ is real valued and that E_x^a, F_y^b are real valued positive symmetric operators. We will assume this throughout the paper. Here we consider the case of two parties (aka the bipartite setting) and the sets X, Y (resp., A, B) model the possible inputs

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 127–146
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

(resp., outputs) of the two parties, assumed throughout to be finite. While the set of classical correlations (those obtained using only local and shared randomness) forms a polytope so that membership can be decided using linear programming, the set $\mathcal{Q}$ of quantum correlations is convex but with infinitely many extreme points and its structure is much harder to characterize. An open question in quantum information is whether allowing an infinite amount of entanglement, i.e., allowing the Hilbert space $\mathcal{H}$ in the above definition to be infinite dimensional, gives rise to a probability distribution P which is not quantum [28]. In other words, it is not known whether the set of quantum correlations $\mathcal{Q}$ is closed.

A setting which is frequently used to study the power of quantum correlations is the one of *nonlocal games*. In a nonlocal game a referee gives to each of the two cooperating players a question and, without communication throughout the game, they have to answer. According to some known predicate, which depends on the two questions and on the two answers, the referee determines whether the players have won or lost the game. In a quantum strategy the players can use quantum correlations to answer. The *quantum coloring game* is a particular nonlocal game that has received a substantial amount of attention lately [1, 8, 25, 24, 14, 19, 23]. Here, each of the two players receives a vertex of a fixed graph G. They win if they output the same color upon receiving the same vertex or if they output different colors on pairs of adjacent vertices. The *quantum chromatic number* $\chi_q(G)$ is the minimum number of colors that the players must use as output set in order to win the coloring game on all input pairs with a quantum strategy. It is not hard to see that if the players are restricted to classical strategies then the minimum number of colors they need to win the game on all input pairs is exactly the classical chromatic number $\chi(G)$.

Like its classical analog the quantum chromatic number is an NP-hard graph parameter [14]. Moreover, it is also lower bounded by the theta number [25], which can be efficiently computed with semidefinite programming. However, it appears to be hard to find non-trivial improved upper and lower bounds to $\chi_q(G)$. With the intention of better understanding $\chi_q(G)$ and other related quantum graph parameters, two of the authors have introduced the *completely positive semidefinite cone* $\mathcal{CS}_+^n$ [19].

Throughout $\mathcal{S}^n$ is the set of real symmetric $n \times n$ matrices and $\mathcal{S}_+^n$ the subset of positive semidefinite matrices; $\langle X, Y\rangle = \mathsf{Tr}(XY)$ is the trace inner product and $\mathsf{Tr}(X) = \sum_{i=1}^n X_{ii}$ for $X, Y \in \mathcal{S}^n$. Then, $\mathcal{CS}_+^n$ consists of all matrices A that admit a Gram representation by positive semidefinite matrices, i.e., such that $A = (\langle X_i, X_j\rangle)_{i,j=1}^n$ for some matrices $X_1, \ldots, X_n \in \mathcal{S}_+^d$ and $d \geq 1$. (When we do not want to specify the size of the matrices in $\mathcal{CS}_+^n$ we omit the superscript and write $\mathcal{CS}_+$.) Using an equivalent formulation of the quantum chromatic number proven in [8], it is shown in [19] that the parameter $\chi_q(G)$ can be rewritten as a feasibility program over the completely positive semidefinite cone:

$$\chi_q(G) = \min t \in \mathbb{N} \text{ s.t. } \exists A \in \mathcal{CS}_+^{nt},\ A \in \mathcal{A}^t \text{ and } L_{G,t}(A) = 0. \tag{1.1}$$

Here, n is fixed and equal to the number of vertices of the graph G while t is the variable that triggers the size of the matrix variable A in the above program. Indeed, A is indexed by $V(G) \times [t]$. With $\mathcal{A}^t$ we represent the affine space in $\mathcal{S}^{nt}$ defined by the equations

$$\sum_{i,j\in[t]} A_{ui,vj} = 1 \text{ for } u, v \in V(G), \tag{1.2}$$

and with $L_{G,t} : \mathcal{S}^{nt} \to \mathbb{R}$ we denote the linear map defined by

$$L_{G,t}(A) = \sum_{u\in V(G), i\neq j\in[t]} A_{ui,uj} + \sum_{uv\in E(G), i\in[t]} A_{ui,vi}. \tag{1.3}$$

Notice that any matrix in $\mathcal{CS}_+$ is positive semidefinite. Moreover it has nonnegative entries because the inner product of two positive semidefinite matrices is nonnegative. Hence the condition $L_{G,t}(A)=0$ is equivalent to requiring that all the terms in the sum in (1.3) are equal to zero. The constraint $A\in\mathcal{A}^t$ models that the players are using a conditional probability distribution for their strategy, while $L_{G,t}(A)=0$ imposes that they have a winning strategy for the coloring game. The structure of the matrix cone $\mathcal{CS}_+$ is still largely unknown. In particular it is not known whether the cone $\mathcal{CS}_+$ is a closed set.

By replacing in (1.1) the cone $\mathcal{CS}_+$ by its closure $\mathrm{cl}(\mathcal{CS}_+)$, we get another graph parameter, denoted as $\widetilde{\chi}_q(G)$. Namely,

$$\widetilde{\chi}_q(G)=\min t\in\mathbb{N} \text{ s.t. } \exists A\in \mathrm{cl}(\mathcal{CS}_+^{nt}),\ A\in\mathcal{A}^t \text{ and } L_{G,t}(A)=0. \tag{1.4}$$

Clearly, $\widetilde{\chi}_q(G)\le\chi_q(G)$, with equality if $\mathcal{CS}_+$ is closed. This parameter, which was introduced in [19], will be studied in this paper.

Interestingly, Mančinska and Roberson [20] showed recently that the set $\mathcal{Q}$ of quantum bipartite correlations can also be described in terms of the completely positive semidefinite cone. They show that $\mathcal{Q}$ can be obtained as the projection of an affine section of the completely positive semidefinite cone.

▶ **Theorem 1** ([20]). *A conditional probability distribution $P=(P(a,b|x,y))$ with input sets X,Y and output sets A,B is quantum (i.e., $P\in\mathcal{Q}$) if and only if there exists a matrix $R\in\mathcal{CS}_+$ indexed by $(X\times A)\cup(Y\times B)$ satisfying the conditions:*

$$\sum_{a,a'\in A}R_{xa,x'a'}=1 \textit{ for all } x,x'\in X, \tag{1.5}$$

$$\sum_{b,b'\in B}R_{yb,y'b'}=1 \textit{ for all } y,y'\in Y, \tag{1.6}$$

$$\sum_{a\in A,b\in B}R_{xa,yb}=1 \textit{ for all } x\in X,y\in Y, \tag{1.7}$$

$$R_{xa,yb}=P(a,b|x,y) \textit{ for all } a\in A,b\in B,x\in X,y\in Y. \tag{1.8}$$

In other words, $\mathcal{Q}=\pi(\mathcal{CS}_+^N\cap\mathcal{B}^t)$ where $N=|(X\times A)\cup(Y\times B)|$, $\mathcal{B}^t$ is the affine space defined by the constraints (1.5), (1.6) and (1.7), and π is the projection onto the subspace indexed by $(X\times A)\times(Y\times B)$ (defined by (1.8)).

Notice that any feasible matrix R to the above program has the form $\begin{pmatrix} R_1 & P\\ P^T & R_2\end{pmatrix}$, where R_1 is indexed by $X\times A$, R_2 is indexed by $Y\times B$ and each entry of P is such that $P_{xa,yb}=P(a,b|x,y)$.

As shown in [20], if the completely positive semidefinite cone is closed then the set $\mathcal{Q}$ of quantum bipartite correlations too is closed. Indeed, the constraints (1.5)-(1.7) imply that the set $\mathcal{CS}_+\cap\mathcal{B}^t$ is bounded. Hence, if $\mathcal{CS}_+$ is closed then $\mathcal{CS}_+\cap\mathcal{B}^t$ is compact and thus its projection $\mathcal{Q}=\pi(\mathcal{CS}_+\cap\mathcal{B}^t)$ is compact.

Our contributions

The results of this paper are twofold. First we construct a hierarchy of polyhedral cones that asymptotically covers the interior of the completely positive semidefinite cone $\mathcal{CS}_+$. Moreover we show how this hierarchy can be used to study the quantum chromatic number. In particular we build a hierarchy of linear programs, among which one of them permits to compute the variant $\widetilde{\chi}_q(G)$ in (1.4) of the parameter $\chi_q(G)$. This idea can also be applied to compute variants of other versions of the quantum chromatic number; we will indicate how to do that for the variant $\widetilde{\chi}_{qa}(G)$ of the parameter $\chi_{qa}(G)$ considered in [23]. See below for some details and Sections 2 and 3 for the proofs.

As a second main contribution we provide an explicit description of the closure of the cone $\mathcal{CS}_+$, in terms of tracial ultraproducts of matrix algebras. Moreover we exhibit a larger cone, containing $\mathcal{CS}_+$, which can be interpreted as an infinite dimensional analog of $\mathcal{CS}_+$. This cone consists of the matrices which admit a Gram representation by (a specific class of) positive semidefinite operators on a possibly infinite dimensional Hilbert space instead of Gram representations by *finite* positive semidefinite matrices. We can in fact show that this larger cone is indeed a closed cone and that it is equal to $\mathrm{cl}(\mathcal{CS}_+)$ if Connes' embedding conjecture holds true. Since the description of these cones involve quite some notation and concepts from operator theory we skip a preliminary description of the used methods and refer directly to Section 4 which can be read independently of the other part.

In summary, our results give structural information about the completely positive semidefinite cone $\mathcal{CS}_+$ which come in two flavors, depending whether we consider its interior or its boundary.

We now give some more details about our first contribution. In a nutshell, the idea for building the hierarchy of polyhedral cones is to discretize the set of positive semidefinite matrices by rational ones with bounded entries. Namely, given an integer $r \geq 1$, we define the cone $\mathcal{C}_r^n$ as the conic hull of all matrices A that admit a Gram representation by $r \times r$ positive semidefinite matrices $X_1, \dots, X_n$ whose entries are rational with denominator at most r and satisfy $\sum_{i=1}^n \mathsf{Tr}(X_i) = 1$. We show that the cones $\mathcal{C}_r^n$ and their dual cones $\mathcal{D}_r^n = \mathcal{C}_r^{n*}$ satisfy the following properties:

$$\mathrm{int}(\mathcal{CS}_+^n) \subseteq \bigcup_{r\geq 1} \mathcal{C}_r^n \subseteq \mathcal{CS}_+^n \quad \text{and} \quad \mathcal{CS}_+^{n*} = \bigcap_{r\geq 1} \mathcal{D}_r^n.$$

Moreover, for any fixed r, linear optimization over the cone $\mathcal{C}_r^n$ can be performed in polynomial time in terms of n. This discretization idea was also used in the classical (scalar) setting, where a hierarchy of polyhedral cones is constructed to approximate the completely positive cone (consisting of all matrices that admit a Gram representation by nonnegative vectors) and its dual, the copositive cone (see [29]). Our construction is in fact inspired by this classical counterpart. Discretization is also widely used in optimization to build good approximations for polynomial optimization problems over the standard simplex or for evaluating tensor norms (see e.g. [3], [17], the recent work [6] and references therein).

One of the difficulties in using the cone $\mathcal{CS}_+$ for studying the quantum parameter $\chi_q(G)$ or general quantum correlations in $\mathcal{Q}$ stems from the fact that the additional affine conditions posed on the matrix $A \in \mathcal{CS}_+$ imply that it must lie on the boundary of the cone $\mathcal{CS}_+$. This is the case for instance for the conditions that A must belong to the affine space $\mathcal{A}^t$ in (1.2), or the condition $L_{G,t}(A) = 0$ in (1.3), or the conditions (1.5), (1.6) and (1.7). Since we do not know whether the cone $\mathcal{CS}_+$ is closed, this is why we may get different parameters depending whether we use the cone $\mathcal{CS}_+$ or its closure.

In order to be able to exploit the fact that the cones $\mathcal{C}_r^n$ asymptotically cover the full interior of $\mathcal{CS}_+^n$, we will relax the affine constraints (using a small perturbation) to ensure the existence of a feasible solution in the interior of the cone $\mathcal{CS}_+$. In this way we will be able to get a hierarchy of parameters that can be computed through linear programming and give the exact value of $\widetilde{\chi}_q(G)$. We remark that this result is existential, we can prove the existence of a linear program permitting to compute the quantum parameter but we do not know at which stage this happens. This result should be seen in the light of a recent result of the same flavor proved in [23]. The authors of [23] consider yet another variant

$\chi_{qc}(G)$ of the quantum parameter $\chi_q(G)$, satisfying $\chi_{qc}(G) \leq \chi_q(G)$, and they show that $\chi_{qc}(G)$ can be computed with a positive semidefinite program (also not explicitly known). The definition of $\chi_{qc}(G)$ is given below.

Link to other variants of the quantum chromatic number

In the papers [24, 23], Paulsen and coauthors have introduced many variants of the quantum chromatic number motivated by the study of quantum correlations. We recall two of them, the parameters $\chi_{qa}(G)$ and $\chi_{qc}(G)$, in order to pinpoint the link to our parameter $\widetilde{\chi}_q(G)$ and to our approach.

Recall that the quantum chromatic number $\chi_q(G)$ is the minimum number of colors that the players must use to always win the corresponding coloring game with a quantum strategy. In other words, this is the minimum integer t for which there exists a probability $P = (P(i,j|u,v)) \in \mathcal{Q}$ with input sets $X = Y = V(G)$ and output sets $A = B = [t]$, such that $P(i,j|u,u) = 0$ for all $i \neq j \in [t]$ and $u \in V(G)$, and $P(i,i|u,v) = 0$ for all $i \in [t]$ and $uv \in E(G)$. For convenience, in the following paragraphs we will omit the dependence of P on t, which should be considered as implicit. Forcing the probability of these combinations of inputs and output to be zero imposes that the players have a winning strategy. We combine those constraints into a single one by defining the linear map $\mathcal{L}_{G,t} : \mathbb{R}^{(nt)^2} \to \mathbb{R}$ by

$$\mathcal{L}_{G,t}(P) = \sum_{i \neq j \in [t], u \in V(G)} P(i,j|u,u) + \sum_{i \in [t], uv \in E(G)} P(i,i|u,v).$$

Then, the players have a winning strategy if and only if the probability P satisfies $\mathcal{L}_{G,t}(P) = 0$. The following is the original definition of $\chi_q(G)$ in [8]:

$$\chi_q(G) = \min t \in \mathbb{N} \text{ s.t. } \exists P \in \mathcal{Q} \text{ with } \mathcal{L}_{G,t}(P) = 0.$$

In [8] it is shown that in the coloring game the optimal quantum strategy is symmetric: the two players perform the same action upon receiving the same input. This special additional structure of the coloring game is the reason why $\chi_q(G)$ can be equivalently reformulated as in (1.1).

The parameter $\chi_{qa}(G)$ defined in [24] asks the probability P to be in the closure of $\mathcal{Q}$:

$$\chi_{qa}(G) = \min t \in \mathbb{N} \text{ s.t. } \exists P \in \text{cl}(\mathcal{Q}) \text{ with } \mathcal{L}_{G,t}(P) = 0.$$

Hence, the following relationship holds: $\chi_{qa}(G) \leq \chi_q(G)$.

The authors of [24] (see also [23]) furthermore considered probability distributions arising from the relativistic point of view. Roughly, instead of assuming that the measurement operators act on different Hilbert spaces so that joint measurements have a tensor product structure, in the relativistic model the measurement operators act on a common Hilbert space and the operators of the two parties commute mutually. In this case, joint measurement operators have a product structure. More formally, a correlation $P = (P(a,b|x,y))$ is obtained from relativistic quantum field theory if it is of the form $P(a,b|x,y) = \psi^\dagger E_x^a F_y^b \psi$, where ψ is a unit vector in a (possibly infinite dimensional) Hilbert space $\mathcal{H}$, E_x^a and F_y^b are positive operators on $\mathcal{H}$ satisfying $\sum_{a \in A} E_x^a = I = \sum_{b \in B} F_y^b$ for all $x \in X, y \in Y$ and $E_x^a F_y^b = F_y^b E_x^a$ for all $a \in A, b \in B, x \in X, y \in Y$. We denote by $\mathcal{Q}_c$ the set of quantum bipartite correlations arising from the relativistic point of view. The set $\mathcal{Q}_c$ is closed (see e.g. [12, Proposition 3.4]) and the following inclusions hold:

$$\mathcal{Q} \subseteq \text{cl}(\mathcal{Q}) \subseteq \mathcal{Q}_c. \tag{1.9}$$

Deciding whether equality $\mathcal{Q}_c = \mathrm{cl}(\mathcal{Q})$ holds is known to be equivalent to Connes' embedding conjecture (see [22, 12, 15]) and deciding whether $\mathcal{Q}_c = \mathcal{Q}$ is known as Tsirelson's problem.

In [24] the parameter $\chi_{qc}(G)$ is defined as

$$\chi_{qc}(G) = \min t \in \mathbb{N} \text{ s.t. } \exists P \in \mathcal{Q}_c \text{ with } \mathcal{L}_{G,t}(P) = 0.$$

In [23] it is shown that $\chi_{qc}(G)$ can be computed by a positive semidefinite program (after rounding). This result is existential, meaning that the program is not explicitly known. For this the authors of [23] use the semidefinite programming hierarchy developed by Navascués, Pironio and Acín [21] for noncommutative polynomial optimization. This technique can be applied since the definition of $\chi_{qc}(G)$ is in terms of products of operators. Note that this technique cannot be applied to the parameters $\chi_{qa}(G)$ and $\chi_q(G)$ whose definitions involve tensor products of operators. It is not know whether the parameters $\chi_{qa}(G)$ and $\chi_q(G)$ can be written as semidefinite programs. As pointed out in [23], in view of the inclusions in (1.9), the following relationships hold between the parameters:

$$\chi_{qc}(G) \leq \chi_{qa}(G) \leq \chi_q(G).$$

Using Theorem 1, we can reformulate the parameters $\chi_q(G)$ and $\chi_{qa}(G)$ as feasibility problems over affine sections of the cones $\mathcal{CS}_+$ and $\mathrm{cl}(\mathcal{CS}_+)$, respectively. Namely, we have

$$\begin{aligned} \chi_q(G) &= \min t \text{ s.t. } \exists P \in \pi(\mathcal{CS}_+^{2nt} \cap \mathcal{B}^t) \text{ with } \mathcal{L}_{G,t}(P) = 0, \quad \text{and} \\ \chi_{qa}(G) &= \min t \text{ s.t. } \exists P \in \mathrm{cl}(\pi(\mathcal{CS}_+^{2nt} \cap \mathcal{B}^t)) \text{ with } \mathcal{L}_{G,t}(P) = 0. \end{aligned}$$

Recall that we introduced the variant $\widetilde{\chi}_q(G)$ by replacing the cone $\mathcal{CS}_+$ by its closure in the definition (1.1) of $\chi_q(G)$. Analogously, we introduce the variant $\widetilde{\chi}_{qa}(G)$ by replacing $\mathcal{CS}_+$ by its closure in the above definition of $\chi_{qa}(G)$. Namely,

$$\widetilde{\chi}_{qa}(G) = \min t \text{ s.t. } \exists P \in \pi(\mathrm{cl}(\mathcal{CS}_+^{2nt}) \cap \mathcal{B}^t) \text{ with } \mathcal{L}_{G,t}(P) = 0. \tag{1.10}$$

Note that the set $\mathrm{cl}(\mathcal{CS}_+) \cap \mathcal{B}^t$ is bounded, thus compact, so that its projection $\pi(\mathrm{cl}(\mathcal{CS}_+) \cap \mathcal{B}^t)$ is compact too. Hence the inclusion $\mathcal{CS}_+ \cap \mathcal{B}^t \subseteq \mathrm{cl}(\mathcal{CS}_+) \cap \mathcal{B}^t$ implies:

$$\mathrm{cl}(\pi(\mathcal{CS}_+ \cap \mathcal{B}^t)) \subseteq \pi(\mathrm{cl}(\mathcal{CS}_+) \cap \mathcal{B}^t)$$

and thus the following relationship: $\widetilde{\chi}_{qa}(G) \leq \chi_{qa}(G)$. In Section 3 we will show that $\widetilde{\chi}_{qa}$ can be computed with a linear program.

Moreover, note that if a matrix A is feasible for the program (1.4) defining $\widetilde{\chi}_q(G)$, then the matrix $R = \left(\begin{smallmatrix} A & A \\ A & A \end{smallmatrix}\right)$ is feasible for the program (1.10) defining $\widetilde{\chi}_{qa}(G)$. Hence, $\widetilde{\chi}_{qa}(G) \leq \widetilde{\chi}_q(G)$ holds.

The relationship between the parameters $\chi_q(G), \chi_{qc}(G), \chi_{qa}(G)$ and $\widetilde{\chi}_{qa}(G), \widetilde{\chi}_q(G)$ can be summarized as follows:

$$\begin{array}{ccccc} \chi_{qc}(G) & \leq & \chi_{qa}(G) & \leq & \chi_q(G) \\ & & \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} \\ & & \widetilde{\chi}_{qa}(G) & \leq & \widetilde{\chi}_q(G) \end{array}$$

2 Polyhedral approximations of $\mathcal{CS}_+$ and its dual cone $\mathcal{CS}_+^*$

In this section we construct hierarchies of polyhedral cones converging asymptotically to the completely positive cone and its dual. We start in Section 2.1 by recalling the definition of $\mathcal{CS}_+$ and of $\mathcal{CS}_+^*$ as well as some useful properties and introduce the new hierarchy in Section 2.2. The construction of our polyhedral hierarchy is directly inspired from the classical case where analogous hierarchies of polyhedral cones exist for approximating the completely positive cone $\mathcal{CP}^n$ and the copositive cone $\mathcal{COP}^n$; in Appendix A we recall this construction.

2.1 The completely positive semidefinite cone and its dual

The completely positive semidefinite cone was introduced in [19] to study graph parameters arising from quantum nonlocal games and quantum information theory. It has also been considered implicitly in [13].

Recall that a matrix $A \in \mathcal{S}^n$ is positive semidefinite if and only if it admits a Gram representation by vectors, i.e., if $A = (\langle x_i, x_j\rangle)_{i,j=1}^n$ for some $x_1, \dots, x_n \in \mathbb{R}^d$ and $d \geq 1$. We write $A \succeq 0$ (resp., $A \succ 0$) when A is positive semidefinite (resp., positive definite) and $\mathcal{S}_+^n$ is the set of positive semidefinite matrices.

▶ **Definition 2.** The completely positive semidefinite cone $\mathcal{CS}_+^n$ is the set of symmetric matrices A which admit a Gram representation by positive semidefinite matrices, i.e., $A = (\langle X_i, X_j\rangle)_{i,j}$ for some $X_1, \dots, X_n \in \mathcal{S}_+^d$ and $d \in \mathbb{N}$.

The completely positive cone $\mathcal{CP}^n$ is the set of symmetric matrices that admit a Gram representation by nonnegative vectors: $A \in \mathcal{CP}^n$ if $A = (\langle x_i, x_j\rangle)_{i,j}$ for some $x_1, \dots, x_n \in \mathbb{R}_+^d$ and $d \in \mathbb{N}$. Hence $\mathcal{CP}^n$ can be considered as the classical analog of $\mathcal{CS}_+^n$. Clearly every completely positive semidefinite matrix is positive semidefinite and nonnegative, and every completely positive matrix is completely positive semidefinite. That is, we have the following relationships between these cones:

$$\mathcal{CP}^n \subseteq \mathcal{CS}_+^n \subseteq \mathcal{S}_+^n \cap \mathbb{R}_+^{n\times n}.$$

In [19] it is shown that all these inclusions are strict for $n \geq 5$ (see also [13]). For $n \leq 4$ it is well known that $\mathcal{CP}^n = \mathcal{S}_+^n \cap \mathbb{R}_+^{n\times n}$. For this and other properties of $\mathcal{CP}$ we refer the reader to the book [5]. Both $\mathcal{CP}^n$ and $\mathcal{S}_+^n$ are closed cones, while we do not know whether $\mathcal{CS}_+^n$ is closed.

Moving on to the dual side, as noted in [19], the dual cone of $\mathcal{CS}_+^n$ has a simple characterization in terms of trace nonnegative polynomials. Given a matrix $M \in \mathcal{S}^n$, define the polynomial $p_M = \sum_{i,j=1}^n M_{ij}x_ix_j$ in n noncommutative variables. Then M belongs to the dual cone $\mathcal{CS}_+^{n*}$ precisely when $\mathsf{Tr}(p_M(X_1, \dots, X_n)) \geq 0$ for all n-tuples $\underline{X} = (X_1, \dots, X_n) \in \cup_{d\geq 1}(\mathcal{S}_+^d)^n$. If we require nonnegativity only for all $\underline{X} \in \mathbb{R}_+^n$ (i.e., the case $d = 1$), which amounts to requiring that the polynomial p_M takes nonnegative values when evaluated at any point in $\mathbb{R}_+^n$, then the matrix M is said to be *copositive*; $\mathcal{COP}^n$ denotes the cone of copositive matrices. The cones $\mathcal{CP}^n$ and $\mathcal{COP}^n$ are dual to each other: $\mathcal{COP}^n = \mathcal{CP}^{n*}$ and, by duality, we have the inclusions:

$$\mathcal{S}_+^n + (\mathcal{S}^n \cap \mathbb{R}_+^{n\times n}) \subseteq \mathcal{CS}_+^{n*} \subseteq \mathcal{COP}^n.$$

As will be explained in detail in Section 3, in order to be able to use our polyhedral hierarchy, we will need to have matrices that are in the interior of $\mathcal{CS}_+$. Recall that a matrix $A \in \mathcal{CS}_+$ lies in the interior of $\mathcal{CS}_+$ if and only if $\langle A, M\rangle > 0$ for all nonzero matrices $M \in \mathcal{CS}_+^*$. Hence, A lies in the boundary of $\mathcal{CS}_+$ if and only if there exists a nonzero matrix $M \in \mathcal{CS}_+^*$ such that $\langle A, M\rangle = 0$. For further reference we observe that matrices in $\mathcal{CS}_+$ with a zero entry, or lying in the affine spaces $\mathcal{A}^t$ or $\mathcal{B}^t$, lie in the boundary of $\mathcal{CS}_+$.

▶ **Lemma 3.** *Consider a matrix A in the cone $\mathcal{CS}_+$ (of appropriate size). Then A lies in the boundary of $\mathcal{CS}_+$ in any of the following cases:* (i) *A has a zero entry;* (ii) *A belongs to the affine space $\mathcal{A}^t$ defined by (1.2), or* (iii) *A belongs to the affine space $\mathcal{B}^t$ defined by the conditions* (1.5), (1.6) *and* (1.7).

2.2 The new cones $\mathcal{C}_r^n$ and $\mathcal{D}_r^n$

We now introduce the cones $\mathcal{C}_r^n$, which will form a hierarchy of inner approximations for the cone $\mathcal{CS}_+^n$, and the cones $\mathcal{D}_r^n$, which will form a hierarchy of outer approximations for the dual cone $\mathcal{CS}_+^{n*}$. These cones are in fact dual to each other, so it suffices to define the cones $\mathcal{D}_r^n$. The idea is simple and analogous to the idea used in the classical (scalar) case: instead of requiring trace nonnegativity of the polynomial p_M over the full set $\cup_{d\geq 1}(\mathcal{S}_+^d)^n$, we only ask trace nonnegativity over specific finite subsets. We start with defining the set

$$\mathbf{\Delta}_n = \{\underline{X} = (X_1,\ldots,X_n) \in \bigcup_{d\geq 1}(\mathcal{S}_+^d)^n : \sum_{i=1}^n \mathsf{Tr}(X_i) = 1\}, \tag{2.1}$$

which can be seen as the dimension-free matrix analog of the standard simplex Δ_n in $\mathbb{R}^n$. As we now observe, a matrix M belongs to $\mathcal{CS}_+^{n*}$ if and only if its associated polynomial p_M is trace nonnegative on all n-tuples of *rational* matrices in $\mathbf{\Delta}_n$ (see Appendix C for a proof).

▶ **Lemma 4.** *$M \in \mathcal{CS}_+^{n*}$ if and only if $\mathsf{Tr}(p_M(\underline{X})) \geq 0$ for all $\underline{X} \in \mathbf{\Delta}_n$ with rational entries.*

This motivates introducing the following subset $\mathbf{\Delta}(n,r)$ of the set $\mathbf{\Delta}_n$, obtained by considering only n-tuples of rational positive semidefinite matrices with denominator at most r. This set can be seen as a matrix analog of the rational grid point subsets of the standard simplex Δ_n and it permits to define the new cones $\mathcal{D}_r^n$.

▶ **Definition 5.** Given an integer $r \in \mathbb{N}$, define the set

$$\mathbf{\Delta}(n,r) = \{\underline{X} \in \mathbf{\Delta}_n : \text{ each } X_i \text{ has rational entries with denominator} \leq r\}$$

and define the cone

$$\mathcal{D}_r^n = \{M \in \mathcal{S}^n : \mathsf{Tr}(p_M(\underline{X})) \geq 0 \ \forall \underline{X} \in \mathbf{\Delta}(n,r)\}.$$

Next we show that the cone $\mathcal{D}_r^n$ is a polyhedral cone. Indeed, as we observe below, although the set $\mathbf{\Delta}(n,r)$ is not finite, we may without loss of generality replace in the definition of $\mathcal{D}_r^n$ the set $\mathbf{\Delta}(n,r)$ by its subset $\underline{\mathbf{\Delta}}(n,r)$, obtained by restricting to $r \times r$ matrices $X_1,\ldots,X_n$. The next lemma is proved in Appendix C.

▶ **Lemma 6.** *Define the set*

$$\underline{\mathbf{\Delta}}(n,r) = \{\underline{X} \in (\mathcal{S}_+^r)^n : \sum_{i=1}^n \mathsf{Tr}(X_i) = 1, \textit{each } X_i \textit{ has rational entries with denominator} \leq r\}.$$

Then, equality holds:

$$\mathcal{D}_r^n = \{M \in \mathcal{S}^n : \mathsf{Tr}(p_M(\underline{X})) \geq 0 \ \forall \underline{X} \in \underline{\mathbf{\Delta}}(n,r)\}.$$

▶ **Lemma 7.** *For any fixed r, the cardinality of the set $\underline{\mathbf{\Delta}}(n,r)$ is polynomial in terms of n. More precisely, let γ_r denote the number of $r \times r$ positive semidefinite matrices whose entries are rational with denominator at most r and whose trace is at most one. Then, $|\underline{\mathbf{\Delta}}(n,r)| \leq (\gamma_r)^r$ if $n \leq r$, and $|\underline{\mathbf{\Delta}}(n,r)| \leq \binom{n}{r}(\gamma_r)^r$ if $n > r$.*

Notice that $\mathsf{Tr}(p_M(\underline{X})) = \sum_{i,j} M_{ij}\langle X_i, X_j\rangle$ for any $\underline{X} = (X_1, \ldots, X_n)$. Hence, the cone $\mathcal{D}^n_r$ can be equivalently defined as the set of matrices $M \in \mathcal{S}^n$ satisfying the (finitely many) linear inequalities: $\sum_{i,j=1}^n M_{ij}\langle X_i, X_j\rangle \geq 0$ for all $(X_1, \ldots, X_n) \in \underline{\mathbf{\Delta}}(n,r)$. This implies:

▶ **Corollary 8.** *The cone $\mathcal{D}^n_r$ is a polyhedral cone.*

As $\underline{\mathbf{\Delta}}(n,r) \subseteq \underline{\mathbf{\Delta}}(n,r+1)$, the sets $\mathcal{D}^n_r$ form a hierarchy of outer approximations for $\mathcal{CS}^{n*}_+$:

$$\mathcal{CS}^{n*}_+ \subseteq \mathcal{D}^n_{r+1} \subseteq \mathcal{D}^n_r \subseteq \cdots \subseteq \mathcal{D}^n_1.$$

Hence, $\mathcal{CS}^{n*}_+ \subseteq \bigcap_{r\geq 1} \mathcal{D}^n_r$. In fact, as a direct application of Lemma 4, equality holds.

▶ **Theorem 9.** $\mathcal{CS}^{n*}_+ = \bigcap_{r\geq 1} \mathcal{D}^n_r$.

We will also use the following property of the cones $\mathcal{D}^n_r$.

▶ **Lemma 10.** *Consider a sequence of matrices $(M_r)_{r\geq 1}$ in $\mathcal{S}^n$ converging to a matrix $M \in \mathcal{S}^n$. If $M_r \in \mathcal{D}^n_r$ for all r, then $M \in \mathcal{CS}^{n*}_+$.*

We now turn to the description of the dual cone $\mathcal{C}^n_r := \mathcal{D}^{n*}_r$. As a direct application of Lemma 6, we can conclude that $\mathcal{C}^n_r$ is the set of conic combinations of matrices which have a Gram representation by matrices in $\underline{\mathbf{\Delta}}(n,r)$; that is,

$$\mathcal{C}^n_r = \text{cone}\{A \in \mathcal{S}^n : A = (\langle X_i, X_j\rangle)^n_{i,j=1} \text{ for some } (X_1, \ldots, X_n) \in \underline{\mathbf{\Delta}}(n,r)\}. \tag{2.2}$$

By construction, the cones $\mathcal{C}^n_r$ are polyhedral and they form a hierarchy of inner approximations of $\mathcal{CS}^n_+$: $\mathcal{C}^n_1 \subseteq \cdots \subseteq \mathcal{C}^n_r \subseteq \mathcal{C}^n_{r+1} \subseteq \mathcal{CS}^n_+$, with strict inclusion.

▶ **Lemma 11.** *For any $n \geq 2$ and $r \geq 1$, we have strict inclusions: $\mathcal{C}^n_r \subsetneq \mathcal{C}^n_{r+1} \subsetneq \mathcal{CS}^n_+$.*

Proof. The only fact which needs a proof is that each inclusion is strict. It suffices to show this for $n = 2$, since one can extend a matrix A in $\mathcal{C}^2_r$ to a matrix in $\mathcal{C}^n_r$ by adding all zero coordinates, and the same for $\mathcal{CS}_+$. For this we consider a rank 1 matrix $A = vv^T$, where $v = (1\ a)^T$ and a is a nonnegative scalar. Then $A \in \mathcal{CS}^2_+$. If we choose a to be an irrational number then A cannot belong to any cone $\mathcal{C}^2_r$ and, if we choose $a = 1/(r+1)$, then A belongs to $\mathcal{C}^2_{r+1}$ but not to $\mathcal{C}^2_r$. ◀

We now show that the union of the cones $\mathcal{C}^n_r$ covers the interior of the cone $\mathcal{CS}^n_+$.

▶ **Theorem 12.** *We have the inclusions:*

$$\text{int}(\mathcal{CS}^n_+) \subseteq \bigcup_{r\geq 1} \mathcal{C}^n_r \subseteq \mathcal{CS}^n_+.$$

Proof. We only need to show the first inclusion. For this, consider a matrix A in the interior of the cone $\mathcal{CS}^n_+$ and assume that A does not belong to $\bigcup_{r\geq 1} \mathcal{C}^n_r$. Then, for each $r \geq 1$, there exists a hyperplane separating A from the (closed convex) cone $\mathcal{C}^n_r$. That is, there exists a matrix $M_r \in \mathcal{D}^n_r$ such that $\langle M_r, A\rangle < 0$ and $\|M_r\| = 1$. Since all matrices M_r lie in a compact set, the sequence $(M_r)_r$ admits a converging subsequence $(M_{r_i})_{i\geq 1}$ which converges to a matrix $M \in \mathcal{S}^n$. By Lemma 10, we know that the matrix M belongs to the cone $\mathcal{CS}^{n*}_+$ and thus $\langle A, M\rangle \geq 0$. On the other hand, as $\langle A, M_{r_i}\rangle < 0$ for all i, by taking the limit as i tends to infinity, we get that $\langle A, M\rangle \leq 0$. Hence we obtain $\langle A, M\rangle = 0$, which contradicts the assumption that A lies in the interior of $\mathcal{CS}^n_+$. ◀

It is easy to give an explicit description of the cones $\mathcal{C}^n_r$ for small r. For example, $\mathcal{C}^n_1$ is the set of $n \times n$ diagonal nonnegative matrices and $\mathcal{C}^n_2$ is the convex hull of the matrices E_{ii} and $E_{ii} + E_{ij} + E_{jj}$ (for $i, j \in [n]$), where E_{ij} denote the elementary matrices in $\mathcal{S}^n$.

3 LP lower bounds to the quantum chromatic number

In this section we use the polyhedral hierarchy $\mathcal{C}_r^n$ $(r \geq 1)$ to show that the parameter $\widetilde{\chi}_q(G)$ in (1.4) can be written as a linear program. We recall the definition of $\widetilde{\chi}_q(G)$:

$$\widetilde{\chi}_q(G) = \min t \in \mathbb{N} \text{ s.t. } \exists A \in \mathrm{cl}(\mathcal{CS}_+^{nt}),\ A \in \mathcal{A}^t \text{ and } L_{G,t}(A) = 0, \tag{3.1}$$

where the affine space $\mathcal{A}^t$ is defined in (1.2) and the map $L_{G,t}$ in (1.3). A first natural approach for building a linear relaxation of $\widetilde{\chi}_q(G)$ is to replace the cone $\mathrm{cl}(\mathcal{CS}_+^{nt})$ in the definition of $\widetilde{\chi}_q(G)$ by the subcone $\mathcal{C}_r^n$, leading to the parameter

$$\ell_r(G) = \min t \in \mathbb{N} \text{ s.t. } \exists A \in \mathcal{C}_r^{nt},\ A \in \mathcal{A}^t \text{ and } L_{G,t}(A) = 0.$$

As $\mathcal{C}_r^{nt} \subseteq \mathcal{CS}_+^{nt}$, we have $\widetilde{\chi}_q(G) \leq \chi_q(G) \leq \ell_r(G)$. Moreover the sequence $(\ell_r(G))_r$ is monotone nonincreasing and thus has a limit (it becomes stationary). However it is not clear whether the limit is equal to $\chi_q(G)$. If one could claim that for $t = \chi_q(G)$ there is a feasible matrix A for the program (3.1) which lies in the interior of $\mathcal{CS}_+^{nt}$ then, by Theorem 12, A would belong to some cone $\mathcal{C}_r^{nt}$ which would imply equality $\chi_q(G) = \ell_r(G)$. However, this idea cannot work because, as observed in Lemma 3, any matrix feasible for (3.1) lies in the boundary of $\mathcal{CS}_+^{nt}$. To go around this difficulty, our strategy is to relax the affine constraints in (3.1) so to allow feasible solutions in the interior of $\mathcal{CS}_+^{nt}$.

More precisely, given an integer $k \geq 1$, we consider the affine space $\mathcal{A}_k^t$ defined by the inequalities: $|\sum_{i,j} A_{ui,vj} - 1| \leq \frac{1}{k}$ for all $u, v \in V(G)$. We define the parameter:

$$\lambda_k(G) = \min t \text{ s.t. } \exists A \in \mathrm{cl}(\mathcal{CS}_+^{nt}),\ A \in \mathcal{A}_k^t \text{ and } L_{G,t}(A) \leq \frac{1}{k}. \tag{3.2}$$

In a first step we show that $\lambda_k(G) = \widetilde{\chi}_q(G)$ for k large enough.

▶ **Lemma 13.** *For any graph G, there exists $k_0 \in \mathbb{N}$ such that $\widetilde{\chi}_q(G) = \lambda_k(G)$ for all $k \geq k_0$.*

Proof. Notice that $\lambda_k(G) \leq \widetilde{\chi}_q(G)$ holds for every $k \in \mathbb{N}$. Indeed, any matrix solution for $\widetilde{\chi}_q(G)$ is also a solution for $\lambda_k(G)$. Moreover, as the sequence $(\lambda_k(G))_{k\in\mathbb{N}}$ is a monotone nondecreasing sequence of natural numbers upper bounded by $\widetilde{\chi}_q(G)$, there exists a k_0 such that $\lambda_k(G) = \lambda_{k_0}(G)$ for all $k \geq k_0$. Let $t = \lambda_{k_0}(G)$. For all $k \geq k_0$ there exists a matrix $A_k \in \mathrm{cl}(\mathcal{CS}_+^{nt})$ with $A_k \in \mathcal{A}_k^t$ and $L_{G,t}(A_k) \leq \frac{1}{k}$. Consider the sequence $(A_k)_{k \geq k_0}$, which is bounded as all A_k lie in $\mathcal{A}_{k_0}^t$. Therefore, the sequence has a converging subsequence to, say, A where $A \in \mathrm{cl}(\mathcal{CS}_+^{nt})$, $A \in \mathcal{A}^t$ and $L_{G,t}(A) = 0$. Hence, A is a feasible solution for $\widetilde{\chi}_q(G)$ and $\widetilde{\chi}_q(G) \leq t = \lambda_{k_0}(G) = \lambda_k(G)$ for all $k \geq k_0$. ◀

In a second step we show that the new parameter $\lambda_k(G)$ can be computed by a linear program. For this we replace in the definition of $\lambda_k(G)$ the cone $\mathrm{cl}(\mathcal{CS}_+^{nt})$ by the polyhedral cone $\mathcal{C}_r^{nt}$, leading to the following parameter:

$$\lambda_k^r(G) = \min t \text{ s.t. } \exists A \in \mathcal{C}_r^{nt},\ A \in \mathcal{A}_k^t \text{ and } L_{G,t}(A) \leq \frac{1}{k}. \tag{3.3}$$

Notice that this parameter $\lambda_k^r(G)$ can be computed through a linear program since $\mathcal{C}_r^{nt}$ is polyhedral. We will show that for any graph G there exist integers k_0 and r_0 such that $\widetilde{\chi}_q(G) = \lambda_{k_0}^{r_0}(G)$. We emphasize that this is an existential result: we do not know for which integers k_0 and r_0 such a convergence happens. One of the ingredients to prove the result is to show the existence of a matrix in the interior of $\mathcal{CS}_+$ satisfying certain constraints. To this end, we will use the matrix $Z = I + J \in \mathcal{S}^{nt}$ where I and J are, respectively, the identity and the all-ones matrices. (See Appendix C for the proof of the following lemma.)

▶ **Lemma 14.** *The matrix $Z = I + J \in \mathcal{S}^{nt}$ lies in the interior of $\mathcal{CS}_+$. Moreover, we have that $\sum_{i,j\in[t]} Z_{ui,uj} = t^2 + t$ for all $u \in V(G)$, $\sum_{i,j\in[t]} Z_{ui,vj} = t^2$ for all $u \neq v \in V(G)$ and $L_{G,t}(Z) = nt^2 - nt + mt$, where m is the number of edges of the graph G.*

▶ **Theorem 15.** *For any graph G there exist k_0 and $r_0 \in \mathbb{N}$ such that $\widetilde{\chi}_q(G) = \lambda_k^r(G)$ for all $k \geq k_0$ and all $r \geq r_0$. Moreover $\lambda_{k_0}^{r_0}(G)$, and thus $\widetilde{\chi}_q(G)$, can be computed via a linear program.*

Proof. From Lemma 13 we know that there exists $k_0 \in \mathbb{N}$ such that $\lambda_k(G) = \widetilde{\chi}_q(G)$ for all $k \geq k_0$. In view of this, we just need to show that for this k_0 there exists an integer $r_0 \in \mathbb{N}$ for which $\lambda_{k_0}^{r_0}(G) = \lambda_{k_0}(G)$. Let $t = \lambda_{k_0}(G) = \widetilde{\chi}_q(G)$.

By the definitions (3.2) and (3.3) and the inclusion relationship between the cones $\mathcal{C}_r^{nt}$, we have that the sequence of natural numbers $(\lambda_{k_0}^r)_{r\in\mathbb{N}}$ is nonincreasing and it is lower bounded by $\lambda_{k_0}(G)$. Hence, there exists a natural number r_0 such that $\lambda_{k_0}^r(G) = \lambda_{k_0}^{r_0}(G)$ for all $r \geq r_0$. We are left to prove that $\lambda_{k_0}^{r_0}(G) \leq \lambda_{k_0}(G) = t$.

To this end, we show that there exists a matrix $Y_{k_0} \in \mathrm{int}(\mathcal{CS}_+)$ with $Y_{k_0} \in \mathcal{A}_{k_0}^t$ and $L_{G,t}(Y_{k_0}) \leq \frac{1}{k_0}$. This will suffice since then, by Theorem 12, $Y_{k_0} \in \mathcal{C}_{r_0}^{nt}$ for some r_0. Therefore, Y_{k_0} satisfies the conditions in program (3.3) and thus $\lambda_{k_0}^{r_0}(G) \leq t = \lambda_{k_0}(G)$. To show the existence of such a matrix Y_{k_0}, let $A \in \mathrm{cl}(\mathcal{CS}_+)$ be a feasible solution of the program (3.1) defining $\widetilde{\chi}_q(G) = t$ and consider the matrix $Z = I + J$ which belongs to $\mathrm{int}(\mathcal{CS}_+)$ (by Lemma 14). Then, any convex combination $Z_\varepsilon = (1-\varepsilon)A + \varepsilon Z$ (for $0 < \varepsilon < 1$) lies in the interior of $\mathcal{CS}_+$. If we can tune ε so that the new matrix Z_ε satisfies the conditions in program (3.3), then we can choose $Y_{k_0} = Z_\varepsilon$ and we are done. We claim that selecting $\varepsilon := \min\{\frac{1}{k_0(t^2+t-1)}, \frac{1}{k_0(nt^2-nt+mt)}\}$ will do the trick. Indeed, for this choice of ε we have $Z_\varepsilon \in \mathrm{int}(\mathcal{CS}_+)$ and $L_{G,t}(Z_\varepsilon) = \varepsilon L_{G,t}(Z) \leq \frac{1}{k_0}$ (use Lemma 14). Moreover, $Z_\varepsilon \in \mathcal{A}_{k_0}^t$ since for all $u, v \in V(G)$ the following holds

$$\big|\sum_{i,j\in[t]} Y_{k_0}(ui,vj) - 1\big| = \big|(1-\varepsilon) + \varepsilon \sum_{i,j\in[t]} Z_{ui,vj} - 1\big| \leq \big|-\varepsilon + \varepsilon \sum_{i,j\in[t]} Z_{ui,uj}\big| = \big|\varepsilon(t^2+t-1)\big| \leq \frac{1}{k_0}.$$

Summarizing, from Lemma 13 we know that there exists an integer $k_0 \in \mathbb{N}$ such that $\lambda_{k_0}(G) = \widetilde{\chi}_q(G)$ and we just proved that for this k_0 there exists an integer $r_0 \in \mathbb{N}$ with the property that $\lambda_{k_0}^{r_0}(G) = \lambda_{k_0}(G) = \widetilde{\chi}_q(G)$. ◀

The same result holds for the parameter $\widetilde{\chi}_{qa}(G)$ introduced in (1.10). For clarity we repeat its definition in the following form:

$$\widetilde{\chi}_{qa}(G) = \min t \in \mathbb{N} \text{ s.t. } \exists A \in \mathrm{cl}(\mathcal{CS}_+^{2nt}), A \in \mathcal{B}^t \text{ with } \mathcal{L}_{G,t}(\pi(A)) = 0.$$

Note the analogy with the definition (3.1) of $\widetilde{\chi}_q(G)$. The only difference is that we now work with matrices A of size $2nt$ (instead of nt) lying in the affine space $\mathcal{B}^t$ (instead of $\mathcal{A}^t$) and satisfying $\mathcal{L}_{G,t}(\pi(A)) = 0$ (instead of $L_{G,t}(A) = 0$). In analogy to the parameter $\lambda_k(G)$ we can define the parameter $\Lambda_k(G)$ by doing these replacements and defining the relaxed affine space $\mathcal{B}_k^t$ in the same way as $\mathcal{A}_k^t$ was defined from $\mathcal{A}^t$. Then the analog of Lemma 13 holds: there exists an integer k_0 such that $\widetilde{\chi}_{qa}(G) = \Lambda_k(G)$ for all $k \geq k_0$. Next, replacing the cone $\mathrm{cl}(\mathcal{CS}_+^{2nt})$ by $\mathcal{C}_r^{2nt}$, we get the following parameter $\Lambda_k^r(G)$ (the analog of $\lambda_r^k(G)$):

$$\Lambda_k^r(G) = \min t \in \mathbb{N} \text{ s.t. } A \in \mathcal{C}_r^{2nt}, A \in \mathcal{B}_k^t \text{ with } \mathcal{L}_{G,t}(\pi(A)) \leq \frac{1}{k}.$$

The analog of Theorem 15 holds, whose proof is along the same lines and thus omitted.

▶ **Theorem 16.** *For any graph G, there exist k_0 and $r_0 \in \mathbb{N}$ such that $\widetilde{\chi}_{qa}(G) = \Lambda_k^r(G)$ for all $k \geq k_0$ and $r \geq r_0$. Hence the parameter $\widetilde{\chi}_{qa}(G)$ can be computed by a linear program.*

▶ **Remark 17.** The above approach applies also to other quantum graph parameters like the communication entanglement-assisted coloring number $\chi^*(G)$ [7] and analogous variants $\alpha_q(G)$ [25] and $\alpha^*(G)$ [10] of the classical independence number $\alpha(G)$. Hence these parameters can be expressed by means of a linear program. This applies more generally to binary constraint system games since, as pointed out by Ji [14], they can be represented as generalized graph coloring problems to which our approach can be applied.

Similar results can also be obtained for the following class of optimization problems:

$$\min\langle C, A\rangle \text{ s.t. } A \in \mathrm{cl}(\mathcal{CS}_+^n), A \in \mathcal{A} \text{ with } \mathcal{L}(A) = 0,$$

where $C \in \mathcal{S}^n$, $\mathcal{L}$ a linear functional nonnegative on $\mathcal{CS}_+^n$, and $\mathcal{A} \subseteq \mathcal{S}^n$ an affine space such that $\mathcal{A} \cap \mathcal{CS}_+^n$ is bounded. Then a double hierarchy can be defined in analogous manner, yielding a sequence of two-parameters linear programs, which converge *asymptotically* to the optimum value of the above optimization program.

4 The closure of $\mathcal{CS}_+$

In the Introduction we have mentioned that if the completely positive semidefinite cone would be closed, then the set of quantum correlations would be closed as well (see also [20]). Although we still do not know whether $\mathcal{CS}_+$ is closed, in this section we make a small progress by giving a new description of the closure of $\mathcal{CS}_+$, using the tracial ultraproduct of matrix algebras $\mathbb{R}^{k\times k}$. More precisely, the closure $\mathrm{cl}(\mathcal{CS}_+)$ consists of the symmetric matrices having a Gram representation by positive semidefinite operators which belong to the above mentioned tracial ultraproduct. This ultraproduct will be an algebra of bounded operators on an infinite dimensional Hilbert space.

A connection between $\mathrm{cl}(\mathcal{CS}_+)$ and the Gram matrices of operators on infinite dimensional Hilbert spaces has already been made by two of the authors in [19]. Namely, let $\mathcal{S}^{\mathbb{N}}$ denote the vector space of all infinite symmetric matrices $X = (X_{ij})$ indexed by $\mathbb{N}$ with finite L_2-norm $\sum_{i,j\geq 1} X_{ij}^2 < \infty$, equipped with the inner product $\langle X, Y\rangle = \sum_{i,j\geq 1} X_{ij}Y_{ij}$. Using this notation, we let $\mathcal{CS}_{\infty+}^n$ denote the convex cone of matrices $A \in \mathcal{S}^n$ having a Gram representation by positive semidefinite matrices in $S^{\mathbb{N}}$. Then it is shown in [19] that $\mathcal{CS}_+ \subseteq \mathcal{CS}_{\infty+} \subseteq \mathrm{cl}(\mathcal{CS}_{\infty+}) = \mathrm{cl}(\mathcal{CS}_+)$ holds. In particular, the closure of $\mathcal{CS}_+$ a priori contains matrices having a Gram representation by infinite dimensional matrices.

Tracial ultraproducts of matrix algebras, or more generally of finite von Neumann algebras, are an adapted version of classical ultraproducts from model theory. Since the methods used might be not familiar to the reader, we recap the construction of tracial ultraproducts. Then we introduce the new cone $\mathcal{CS}_{\mathcal{U}+}$ and show that it is equal to the closure of $\mathcal{CS}_+$. Finally, we present a possibly larger cone $\mathcal{CS}_{\mathrm{vN}+}$, containing $\mathcal{CS}_+$, which can be seen as an infinite dimensional analog of the completely positive semidefinite cone. This cone turns out to be closed. Furthermore, $\mathcal{CS}_{\mathrm{vN}+}$ would be equal to $\mathrm{cl}(\mathcal{CS}_+)$ if the embedding problem of Connes had an affirmative answer. More details about the algebras involved in the general case as well as on the embedding problem of Connes are given in Appendix B.

4.1 Tracial ultraproducts

The construction of tracial ultraproducts is a standard technique in von Neumann algebras, see, e.g., the appendix of [4]. Classically one considers complex Hilbert spaces but the construction works similarly over real Hilbert spaces. Alternatively one can use the complex construction and 'realify' the resulting algebra afterwards, see for instance [2, 18].

Ultraproducts are constructions with respect to an ultrafilter. We will only consider ultrafilters on $\mathbb{N}$. Throughout $\mathcal{P}(\mathbb{N})$ is the collection of all subsets of $\mathbb{N}$.

▶ **Definition 18.** An ultrafilter on the set $\mathbb{N}$ is a subset $\mathcal{U} \subseteq \mathcal{P}(\mathbb{N})$ satisfying the conditions:
(a) $\emptyset \notin \mathcal{U}$,
(b) if $A \subseteq B \subseteq \mathbb{N}$ and $A \in \mathcal{U}$ then $B \in \mathcal{U}$,
(c) if $A, B \in \mathcal{U}$ then $A \cap B \in \mathcal{U}$,
(d) for every $A \in \mathcal{P}(\mathbb{N})$ either $A \in \mathcal{U}$ or $\mathbb{N} \setminus A \in \mathcal{U}$.

In particular, any two elements in $\mathcal{U}$ need to have non-empty intersection (from (1) and (3)), which allows only two kinds of ultrafilters: Either every element of $\mathcal{U}$ contains a common element $n_0 \in \mathbb{N}$ or $\mathcal{U}$ contains the cofinite sets of $\mathbb{N}$. We are only interested in the second kind of ultrafilters, which are called *free ultrafilters*. For a given free ultrafilter $\mathcal{U}$ on $\mathbb{N}$ we can define the *ultralimit* $\lim_{\mathcal{U}} a_k$ of a bounded sequence $(a_k)_{k\in\mathbb{N}}$ of real numbers as follows:

$$\lim_{\mathcal{U}} a_k = a \text{ if } \{k \in \mathbb{N} : |a_k - a| < \varepsilon\} \in \mathcal{U} \quad \text{for all } \varepsilon > 0. \tag{4.1}$$

Let us have a look at ultralimits in a less formal way. If we have a non-free ultrafilter, i.e., $\mathcal{U} = \{A \in \mathcal{P}(\mathbb{N}) : k_0 \in A\}$ for some $k_0 \in \mathbb{N}$, then $\lim_{\mathcal{U}} a_k = a_{k_0}$ for any sequence $(a_k)_{k\in\mathbb{N}} \subseteq \mathbb{R}$. The case of a free ultrafilter is more interesting. Then the ultralimit of a bounded sequence $(a_k)_{k\in\mathbb{N}}$ will be one of its accumulation points. For example, the sequence given by $a_k := (-1)^k$ for all $k \in \mathbb{N}$ has two accumulation points, and both can be attained as an ultralimit depending on the choice of the ultrafilter $\mathcal{U}$. In fact, considering the set $2\mathbb{N}$ of even numbers, we get by conditions (3) and (4) that any ultrafilter contains either $2\mathbb{N}$ or its complement (the odd numbers $2\mathbb{N}+1$) but not both. Hence there is an ultrafilter $\mathcal{U}$ (containing $2\mathbb{N}$) with $\lim_{\mathcal{U}} a_k = 1$ and an ultrafilter $\mathcal{U}'$ (containing $2\mathbb{N}+1$) with $\lim_{\mathcal{U}'} a_k = -1$.

▶ **Remark 19.** Any bounded sequence of real numbers has an ultralimit and this is unique for fixed $\mathcal{U}$. In particular, if $\lim_{k\to\infty} a_k = a$ then $\lim_{\mathcal{U}} a_k = a$ for any free ultrafilter $\mathcal{U}$ on $\mathbb{N}$.

We can use ultralimits to construct the tracial ultraproduct of a sequence $(\mathbb{R}^{d_k \times d_k})_{k\in\mathbb{N}}$ of matrix algebras for $d_k \in \mathbb{N}$. To simplify notation we let $\mathcal{M}_k = \mathbb{R}^{k\times k}$ denote the matrix algebra of all $k \times k$ matrices and we consider the full sequence $(\mathcal{M}_k)_{k\in\mathbb{N}}$, but the same construction would work for the sequence $(\mathcal{M}_{d_k})_{k\in\mathbb{N}}$. Here we assume that each $\mathcal{M}_k$ is endowed with the normalized trace $\mathsf{tr}_k = \frac{1}{k}\mathsf{Tr}$ (if the dimension k is clear we might simply write tr) and the corresponding inner product, so that $\|I\|_2 = \mathsf{tr}(I) = 1$ for the identity matrix. For $T \in \mathcal{M}_k$, $\|T\|$ denotes its operator norm and $\|T\|_2$ its L_2-norm, that satisfy $\|ST\|_2 \leq \|S\|\|T\|_2$ for $S, T \in \mathcal{M}_k$. Define the C^*-algebra

$$\ell^\infty(\mathbb{N}, (\mathcal{M}_k)_k) := \{(T_k)_{k\in\mathbb{N}} \in \prod_{k\in\mathbb{N}} \mathcal{M}_k : \sup_{k\in\mathbb{N}} \|T_k\| < \infty\}.$$

Every free ultrafilter $\mathcal{U}$ on $\mathbb{N}$ defines a two-sided ideal

$$\mathcal{I}_{\mathcal{U}} := \{(T_k)_{k\in\mathbb{N}} \in \ell^\infty(\mathbb{N}, (\mathcal{M}_k)_k) : \lim_{\mathcal{U}} \|T_k\|_2 = 0\},$$

which is well-defined since sequences in $\ell^\infty(\mathbb{N}, (\mathcal{M}_k)_k)$ are also bounded in the Hilbert-Schmidt norm. The ideal $\mathcal{I}_{\mathcal{U}}$ is a maximal ideal and therefore it is closed with respect to the operator norm. The quotient algebra

$$\mathcal{M}_{\mathcal{U}} := \ell^\infty(\mathbb{N}, (\mathcal{M}_k)_k)/\mathcal{I}_{\mathcal{U}}$$

is called the *tracial ultraproduct* of $(\mathcal{M}_k)_k$ along $\mathcal{U}$. Using the Cauchy-Schwarz inequality it is easy to show that the map

$$\tau_{\mathcal{U}} : \mathcal{M}_{\mathcal{U}} \to \mathbb{R}, \quad (T_k)_{k\in\mathbb{N}} + \mathcal{I}_{\mathcal{U}} \mapsto \lim_{\mathcal{U}} \mathsf{tr}_k(T_k)$$

is well-defined and defines a tracial state (or trace) on $\mathcal{M}_{\mathcal{U}}$, i.e., $\tau_{\mathcal{U}}$ is a normalized positive linear map satisfying $\tau_{\mathcal{U}}(T^*T) = \tau_{\mathcal{U}}(TT^*)$ for any $T \in \mathcal{M}_{\mathcal{U}}$. In fact, $\mathcal{M}_{\mathcal{U}}$ is a finite von Neumann algebra of type II_1 (see Appendix B for definitions). In particular, $\mathcal{M}_{\mathcal{U}}$ is a subalgebra of bounded operators on an infinite dimensional Hilbert space. As von Neumann algebras are in particular C^* algebras, positive semidefinite operators are exactly squares of (symmetric) operators.

4.2 Ultraproduct description of $\mathrm{cl}(\mathcal{CS}_+)$

We are now ready to define the new cone $\mathcal{CS}_{\mathcal{U}+}$ which will turn out to be equal to the closure of $\mathcal{CS}_+$. For this, we fix a free ultrafilter $\mathcal{U}$ on $\mathbb{N}$ and consider the tracial ultraproduct $\mathcal{M}_{\mathcal{U}} = \ell^\infty(\mathbb{N}, (\mathcal{M}_k)_k)/\mathcal{I}_{\mathcal{U}}$ where again $\mathcal{M}_k$ denotes the full matrix algebra $\mathbb{R}^{k\times k}$ for any $k \in \mathbb{N}$. Using this we define

$$\mathcal{CS}_{\mathcal{U}+} := \{A \in \mathcal{S}_+ : A = (\tau_{\mathcal{U}}(X_iX_j)) \text{ for some positive semidefinite } X_1, \dots, X_n \in \mathcal{M}_{\mathcal{U}}\}.$$

We note that the trace $\tau_{\mathcal{U}}$ is normalized (i.e., $\tau_{\mathcal{U}}(I) = 1$) whereas we used the (not normalized) trace Tr in the definition of $\mathcal{CS}_+$. However, both descriptions agree up to rescaling of the X_i's.

To show that the closure of $\mathcal{CS}_+$ is a subset of $\mathcal{CS}_{\mathcal{U}+}$ we will consider a sequence of matrices $A^{(k)} \in \mathcal{CS}_+^n$ converging to some $A \in \mathcal{S}^n$, i.e., $\lim_{k\to\infty} A_{ij}^{(k)} = A_{ij}$ for all $i, j \in [n]$. A priori, for each k, there exist an integer d_k and matrices $X_1^{(k)}, \dots, X_n^{(k)} \in \mathcal{S}_+^{d_k}$ such that $A^{(k)} = (\mathsf{tr}(X_i^{(k)} X_j^{(k)}))$. The next lemma says that without loss of generality we can assume $d_k = k$ for all $k \in \mathbb{N}$ (see the Appendix C for a proof).

▶ **Lemma 20.** *If $(X_k)_k, (Y_k)_k \in \prod_{k\in\mathbb{N}} \mathcal{S}_+^{d_k}$ are such that the sequence $(\mathsf{tr}_{d_k}(X_kY_k))_{k\in\mathbb{N}}$ converges to some $a \in \mathbb{R}$, then there exist $(X'_k)_k, (Y'_k)_k \in \prod_{k\in\mathbb{N}} \mathcal{S}_+^k$ with $\mathsf{tr}_k(X'_kY'_k) \to a$ as $k \to \infty$.*

We proceed by showing that the closure of $\mathcal{CS}_+$ is equal to $\mathcal{CS}_{\mathcal{U}+}$. This is done in two steps.

▶ **Lemma 21.** *For any free ultrafilter $\mathcal{U}$ on $\mathbb{N}$, we have $\mathrm{cl}(\mathcal{CS}_+) \subseteq \mathcal{CS}_{\mathcal{U}+}$.*

Proof. Let $A \in \mathrm{cl}(\mathcal{CS}_+)$ be given. Then there is a sequence of matrices $A^{(k)} \in \mathcal{CS}_+$ converging to A: $\lim_{k\to\infty} A_{ij}^{(k)} = A_{ij}$ for all $i, j \in [n]$. For each k, there exist positive semidefinite matrices $X_1^{(k)}, \dots, X_n^{(k)}$ such that $A^{(k)} = (\mathsf{tr}(X_i^{(k)} X_j^{(k)}))$. By Lemma 20 we can assume that $X_1^{(k)}, \dots, X_n^{(k)} \in \mathcal{S}_+^k$. As the matrices $A^{(k)}$ are bounded the matrices $X_i^{(k)}$ are bounded as well. Hence the sequence $(X_i^{(k)})_k$ belongs to $\ell^\infty(\mathbb{N}, (\mathcal{M}_k))$ and we can consider its image X_i in the tracial ultrapower $\mathcal{M}_{\mathcal{U}}$. By the theorem of Łos (see e.g. [11, Prop. 4.3] and references therein) the operators X_i are positive semidefinite since all $X_i^{(k)}$ are positive semidefinite. It suffices now to show that $A = (\tau_{\mathcal{U}}(X_iX_j))$ since then we can conclude that $A \in \mathcal{CS}_{\mathcal{U}+}$. For this observe that, by the definition of $\tau_{\mathcal{U}}$, we have: $\tau_{\mathcal{U}}(X_iX_j) = \lim_{\mathcal{U}} \mathsf{tr}(X_i^{(k)} X_j^{(k)}) = \lim_{\mathcal{U}} A_{ij}^{(k)}$. On the other hand, as the sequence $(A_{ij}^{(k)})_k$ converges to A_{ij}, in view of Remark 19, we have that $\lim_{\mathcal{U}} A_{ij}^{(k)} = A_{ij}$. This concludes the proof. ◀

▶ **Theorem 22.** *For any free ultrafilter $\mathcal{U}$ on $\mathbb{N}$, equality* $\mathrm{cl}(\mathcal{CS}_+) = \mathcal{CS}_{\mathcal{U}+}$ *holds.*

Proof. In view of Lemma 21 we only have to show the inclusion $\mathcal{CS}_{\mathcal{U}+} \subseteq \mathrm{cl}(\mathcal{CS}_+)$. Let $A \in \mathcal{CS}_{\mathcal{U}+}$. By assumption, $A = (\tau_{\mathcal{U}}(X_iX_j))$ for some positive semidefinite operators $X_1, \dots, X_n \in \mathcal{M}_{\mathcal{U}}$. As the operators X_i are positive semidefinite, there exist operators $Y_i \in \mathcal{M}_{\mathcal{U}}$ such that $X_i = Y_i^2$ for $i \in [n]$, where each element Y_i is given by a sequence of symmetric matrices $(Y_i^{(k)})_k \in \prod_k \mathcal{M}_k$. Further, by definition of $\tau_{\mathcal{U}}$, for any $s \in \mathbb{N}$, the index set $I_s = \{k \in \mathbb{N} : |\tau_{\mathcal{U}}(Y_i^2Y_j^2) - \mathsf{tr}((Y_i^{(k)})^2(Y_j^{(k)})^2)| \leq \frac{1}{s}$ for all $i,j \in [n]\}$ belongs to $\mathcal{U}$ and is therefore non-empty. Thus we find for any $s \in \mathbb{N}$ an index $k_s \in I_s$. Hence the operators $X_i^{(s)} := (Y_i^{(k_s)})^2$ belong to $\mathcal{S}_+^{k_s}$ and satisfy

$$\left|\tau_{\mathcal{U}}(X_iX_j) - \mathsf{tr}(X_i^{(s)}X_j^{(s)})\right| < \frac{1}{s} \quad \text{for all } i,j \in [n] \quad \text{and all } s \geq 1. \tag{4.2}$$

For each s, the matrix $A^{(s)} := (\mathsf{tr}(X_i^{(s)}X_j^{(s)}))$ belongs to the cone $\mathcal{CS}_+$. Moreover it follows from (4.2) that the sequence $(A^{(s)})_s$ converges to the matrix A as s tends to ∞. This shows that A belongs to the closure of $\mathcal{CS}_+$, which concludes the proof. ◀

We would like to conclude with another possible description of the closure of $\mathcal{CS}_+$ in the case that Connes' embedding conjecture turns out to be true.

As mentioned at the beginning of the section, the closure of $\mathcal{CS}_+$ contains the cone $\mathcal{CS}_{\infty+}$, i.e., it contains symmetric matrices which have a Gram representation by some class of positive semidefinite infinite dimensional matrices. Also the given description of $\mathrm{cl}(\mathcal{CS}_+)$ as $\mathcal{CS}_{\mathcal{U}+}$ involves Gram representations by operators on an infinite dimensional Hilbert space. In regard to the relativistic model of quantum correlations where one allows *all* (possibly infinite dimensional) Hilbert spaces one might ask for the most general infinite dimensional version of $\mathcal{CS}_+$. Since one is restricted to operators for which one can define an inner product (or a trace), a decent candidate for the infinite dimensional analog of $\mathcal{CS}_+$ is

$$\mathcal{CS}^n_{\mathrm{vN}+} := \{A \in \mathcal{S}^n_+ : A = (\tau_{\mathcal{N}}(X_iX_j)) \text{ for a finite vN algebra } \mathcal{N} \text{ and psd } X_1, \dots, X_n \in \mathcal{N}\},$$

where we allow *any* finite von Neumann algebra $\mathcal{N}$ (with trace $\tau_{\mathcal{N}}$). Obviously we have the chain of inclusions $\mathcal{CS}_+ \subseteq \mathcal{CS}_{\mathcal{U}+} \subseteq \mathcal{CS}_{\mathrm{vN}+}$.

Moreover, using the general theory of tracial ultraproducts of von Neumann algebras (instead of just matrix algebras), one can show with a similar line of reasoning as in Lemma 21 that $\mathcal{CS}_{\mathrm{vN}+}$ is closed. Indeed, take a sequence of matrices $A^{(k)} \in \mathcal{CS}^n_{\mathrm{vN}+}$ converging to some $A \in \mathcal{S}^n$. Then $\lim_{k\to\infty} A^{(k)}_{ij} = A_{ij}$ for all $i,j \in [n]$ and for each k, there exist a finite von Neumann algebra $\mathcal{N}_k$ with trace τ_k and bounded positive operators $X_1^{(k)}, \dots, X_n^{(k)} \in \mathcal{N}_k$ such that $A^{(k)} = (\tau_k(X_i^{(k)}X_j^{(k)}))$. Fixing a free ultrafilter $\mathcal{U}$ one can conclude that the images X_i of the sequences $(X_i^{(k)})_k$ in the tracial ultraproduct $\mathcal{N}_{\mathcal{U}} = \ell^\infty(\mathbb{N}, (\mathcal{N}_k)_k)/\mathcal{I}_{\mathcal{U}}$ of the corresponding finite von Neumann algebras provide a Gram representation for A in the von Neumann algebra $\mathcal{N}_{\mathcal{U}}$. Hence the following statement holds.

▶ **Theorem 23.** $\mathcal{CS}_{\mathrm{vN}+}$ *is a closed cone.*

Summarizing we have the inclusions:

$$\mathrm{cl}(\mathcal{CS}^n_+) = \mathcal{CS}^n_{\mathcal{U}+} \subseteq \mathcal{CS}^n_{\mathrm{vN}+} \subseteq \mathcal{S}^n_+ \cap \mathbb{R}^{n\times n}_+.$$

In this context, we would like to mention that [13] shows the strict inclusion $\mathcal{CS}^n_{\mathrm{vN}+} \subsetneq \mathcal{S}^n_+ \cap \mathbb{R}^{n\times n}_+$ for any $n \geq 5$. Finally, if Connes' embedding conjecture is true, one can show, using Proposition 25 from Appendix B, that $\mathrm{cl}(\mathcal{CS}_+) = \mathcal{CS}_{\mathrm{vN}+}$.

Acknowledgments. We thank one of the referees for pointing out that the original proof of Theorem 22 could be simplified to the elementary proof given above. S. B. and T. P. were funded by the SIQS European project. S. B. was also funded by the NWO TOP project 617.001.351.

References

1 D. Avis, J. Hasegawa, Y. Kikuchi and Y. Sasaki. A quantum protocol to win the graph coloring game on all Hadamard graphs. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E89-A(5):1378–1381, 2006.

2 S. Ayupov, A. Rakhimov and S. Usmanov. *Jordan, real and Lie structures in operator algebras.* Mathematics and its Applications, 418, Kluwer Academic Publishers Group, Dordrecht, 1997.

3 I. M. Bomze and E. de Klerk. Solving standard quadratic optimization problems via linear, semidefinite and copositive programming. *Journal of Global Optimization*, 24:163–185, 2002.

4 N. P. Brown and N. Ozawa. *C^*-algebras and finite-dimensional approximations.* Graduate Studies in Mathematics, 88, American Mathematical Society, Providence, RI, 2008.

5 A. Berman and N. Shaked-Monderer. *Completely Positive Matrices.* World Scientific, River Edge (NJ), London, Singapore, 2003.

6 F. G. S. L. Brandão and A. Harrow. Replacing hierarchies by nets. In preparation.

7 J. Briët, H. Buhrman, M. Laurent, T. Piovesan and G. Scarpa Entanglement-assisted zero-error source-channel coding. *IEEE Transactions on Information Theory,* 61(2):1–15, 2015.

8 P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter. On the quantum chromatic number of a graph. *Electronic Journal of Combinatorics*, 14(R81):1, 2007.

9 B. Collins and K. J. Dykema. A linearization of Connes' embedding problem. *New York J. Math.*, 14, pp. 617–641, 2008.

10 T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104(23):230503, 2010.

11 I. Farah, B. Hart, and D. Sherman. Model theory of operator algebras II: model theory. *Israel J. Math.*, 201(1), pp. 477–505, 2014.

12 T. Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(5):1250012, 2012.

13 P. Frenkel and M. Weine. On vector configurations that can be realized in the cone of positive matrices. *Linear Algebra and its Applications*, 459:465–474, 2014.

14 Z. Ji. Binary constraint system games and locally commutative reductions. *arXiv:1310:3794*, 2013.

15 M. Junge, M. Navascués, C. Palazuelos, D. Pérez-Garcia, V. B. Scholz and R. F. Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, 52(1):012102, 2011.

16 E. de Klerk and D. V. Pasechnik. Approximation of the stability number of a graph via copositive programming. *SIAM Journal on Optimization*, 12(4):875–892, 2002.

17 E. de Klerk, M. Laurent and P. Parrilo. A PTAS for the minimization of polynomials of fixed degree over the simplex. *Theoretical Computer Science,* 361(2-3):210–225, 2006.

18 B. Li. *Real operator algebras.* World Scientific Publishing Co. Inc., River Edge, NJ, 2003.

19 M. Laurent and T. Piovesan. Conic approach to quantum graph parameters using linear optimization over the completely positive semidefinite cone. *arXiv:1312.6643*, 2013.

20 L. Mančinska and D. E. Roberson. Note on the correspondence between quantum correlations and the completely positive semidefinite cone. 2014. Available online under http://quantuminfo.quantumlah.org/memberpages/laura/corr.pdf

21 M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10:073013, 2008.

22 N. Ozawa. About the Connes embedding conjecture. *Japanese Journal of Mathematics*, 8(1):147–193,2013.

23 V. I. Paulsen, S. Severini, D. Stahlke, I. G. Todorov, and A. Winter. Estimating quantum chromatic numbers. *arXiv:1407.6918*, 2014.

24 V. I. Paulsen and I. G. Todorov. Quantum chromatic numbers via operator systems. *The Quaterly Journal of Mathematics*, 66(2):677–692, 2015.

25 D. E. Roberson and L. Mančinska. Graph homomorphisms for quantum players. *arXiv:1212.1724*, 2012.

26 V. Scholz and R. Werner. Tsirelson's problem. *arXiv:0812.4305*, 2008.

27 M. Takesaki. *Theory of operator algebras. II.* Encyclopaedia of Mathematical Sciences 125, Operator Algebras and Non-commutative Geometry, 6, Springer-Verlag, Berlin, 2003.

28 S. Wehner, M. Christandl, and A. C. Doherty. A lower bound on the dimension of a quantum system given measured data. *Physical Review A*, 78, 062112, 2008.

29 E. A. Yildirim. On the Accuracy of Uniform Polyhedral Approximations of the Copositive Cone. *Optimization Methods and Software*, 27(1):155–173, 2012.

A Polyhedral approximations of $\mathcal{CP}^n$ and $\mathcal{COP}^n$

As mentioned above, the copositive cone $\mathcal{COP}^n$ consists of all matrices $M \in \mathcal{S}^n$ for which the polynomial $p_M = \sum_{i,j=1}^n M_{ij}x_ix_j$ is nonnegative over $\mathbb{R}^n_+$. Alternatively, a matrix $M \in \mathcal{S}^n$ is copositive if and only if the polynomial p_M is nonnegative over the standard simplex

$$\Delta_n = \{x \in \mathbb{R}^n_+ : \sum_{i=1}^n x_i = 1\}.$$

The idea for constructing outer approximations of the copositive cone is simple and relies on requiring nonnegativity of the polynomial p_M over all rational points in the standard simplex with given denominator r and letting r grow. This idea is made explicit in [29] and goes back to earlier work on how to design tractable approximations for quadratic optimization problems over the standard simplex [3, 16] and more general polynomial optimization problems [17]. More precisely, for an integer $r \geq 1$, define the sets

$$\Delta(n,r) = \{x \in \Delta_n : rx \in \mathbb{Z}^n\}, \quad \widetilde{\Delta}(n,r) = \bigcup_{s=1}^r \Delta(n,s)$$

where we restrict to rational points in Δ_n with given denominators. The sets $\widetilde{\Delta}(n,r)$ are nested within the standard simplex: $\widetilde{\Delta}(n,r) \subseteq \widetilde{\Delta}(n,r+1) \subseteq \Delta_n$. Now, following Yildirim [29], define the cone:

$$\mathcal{O}^n_r = \{M \in \mathcal{S}^n : x^\mathsf{T} M x \geq 0 \ \forall x \in \widetilde{\Delta}(n,r)\},$$

and its dual cone $\mathcal{O}^{n*}_r$, which is the conic hull of all matrices of the form vv^T for some $v \in \widetilde{\Delta}(n,r)$. By construction, the cones $\mathcal{O}^n_r$ form a hierarchy of outer approximations for $\mathcal{COP}^n$ and their dual cones form a hierarchy of inner approximations for $\mathcal{CP}^n$:

$$\mathcal{COP}^n \subseteq \mathcal{O}^n_{r+1} \subseteq \mathcal{O}^n_r \quad \text{and} \quad \mathcal{O}^{n*}_r \subseteq \mathcal{O}^{n*}_{r+1} \subseteq \mathcal{CP}^n.$$

Yildirim [29] shows the following convergence results.

▶ **Theorem 24** ([29]). *We have: $\mathcal{COP}^n = \bigcap_{r\geq 1} \mathcal{O}^n_r$. Moreover, $\operatorname{int}(\mathcal{CP}^n) \subseteq \bigcup_{r\geq 1} \mathcal{O}^{n*}_r \subseteq \mathcal{CP}^n$ and $\mathcal{CP}^n$ is equal to the closure of the set $\bigcup_{r\geq 1} \mathcal{O}^{n*}_r$.*

B Von Neumann algebras and Connes' embedding problem

We give a short overview of what is needed for our purpose; for details we refer to the book [27].

A *von Neumann algebra* $\mathcal{N}$ is a unital $*$-subalgebra of the $*$-algebra $\mathcal{B}(\mathcal{H})$ of bounded operators on a Hilbert space $\mathcal{H}$ that is closed in the weak operator topology. The *weak operator topology* is the weakest topology on $\mathcal{B}(\mathcal{H})$ such that the functional $\mathcal{B}(\mathcal{H}) \to \mathbb{C}$ which maps $T \mapsto \langle Tx, y\rangle$ is continuous for any $x, y \in \mathcal{H}$. In other words, a sequence $(T_i)_i \in \mathcal{B}(\mathcal{H})$ converges to $T \in \mathcal{B}(\mathcal{H})$ if for all $x, y \in \mathcal{H}$ the sequence $(\langle T_i x, y\rangle)_i$ converges to $\langle Tx, y\rangle$.

A *factor* is a von Neumann algebra with trivial center. Every von Neumann algebra on a separable Hilbert space is isomorphic to a direct integral of factors, which is the appropriate analog of matrix block decomposition.

A factor $\mathcal{F}$ is *finite* if it possesses a normal, faithful, tracial state $\tau : \mathcal{F} \to \mathbb{C}$. In particular, we can always assume that $\tau(I) = 1$. This tracial state τ is unique and gives rise to the Hilbert-Schmidt norm on $\mathcal{F}$ given by $\|T\|_2^2 := \tau(T^*T)$ for $T \in \mathcal{F}$. A von Neumannn algebra is *finite* if it decomposes into finite factors. Every finite von Neumann algebra comes with a trace, which might not be unique.

Von Neumann algebras can be classified into two types depending on the behavior of their projections (i.e., the elements $P \in \mathcal{N}$ satisfying $P = P^* = P^2$). If for a given finite factor $\mathcal{F}$ with trace τ the range of τ over all projections $P \in \mathcal{F}$ is discrete, then $\mathcal{F}$ is of *type* I. A von Neumann algebra is of type I if it consists only of type I factors. Any finite type I von Neumann algebra is isomorphic to a matrix algebra over $\mathbb{C}$. The only other possibility for a finite factor is that τ maps projections (surjectively) onto $[0, 1]$. Those are II_1 factors, and a von Neumann algebra is of type II_1 if it is finite and contains at least one II_1 factor.

Connes' embedding problem asks to which extent II_1 factors are close to matrix algebras. Murray and von Neumann showed that there is a unique II_1 factor $\mathcal{R}$ which contains an ascending sequence of finite-dimensional von Neumann subalgebras, i.e. matrix algebras, with dense union. This factor $\mathcal{R}$ is called the *hyperfinite* II_1 *factor*. There are several constructions of $\mathcal{R}$, e.g., as infinite tensor product $\overline{\bigotimes}_{n\in\mathbb{N}} M_2(\mathbb{C})$ of the von Neumann algebras $M_2(\mathbb{C})$, which is the weak closure of the algebraic tensor product $\bigotimes_{n\in\mathbb{N}} M_2(\mathbb{C})$. In fact, any infinite countable sequence of matrix algebras will do.

Connes conjectured that all separable II_1 factors embed (in a trace-preserving way) into an ultrapower $\mathcal{R}^{\mathcal{U}}$ of the hyperfinite II_1 factor $\mathcal{R}$, where the ultrapower $\mathcal{R}^{\mathcal{U}}$ is just a short-hand notation for the ultraproduct $\ell^\infty(\mathbb{N}, (\mathcal{R})_k)/\mathcal{I}_{\mathcal{U}}$. Since $\mathcal{R}$ contains ascending sequences of matrix algebras with dense union, any matrix algebra $\mathcal{M}_k$ embeds into $\mathcal{R}$. One can extend these embeddings of $\mathcal{M}_k$ into $\mathcal{R}$ to an embedding of the tracial ultraproduct $\mathcal{M}_{\mathcal{U}}$ into $\mathcal{R}^{\mathcal{U}}$ (using a more general construction of ultralimits), hence the finite von Neumann algebra $M_{\mathcal{U}}$ satisfies Connes' embedding conjecture.

This conjecture is equivalent to a huge variety of other important conjectures in, e.g., operator theory, noncommutative real algebraic geometry and quantum information theory. In particular, as we already mentioned in the introduction, it is equivalent to deciding whether $\mathrm{cl}(\mathcal{Q}) = \mathcal{Q}_c$ holds.

For the alternative description of $\mathrm{cl}(\mathcal{CS}_+)$ in the case that Connes' embedding conjecture is a true statement, we will use the following result on finite von Neumann algebras which embed into $\mathcal{R}^{\mathcal{U}}$. The claim is that tracial moments of an embeddable finite factor can be approximated up to arbitrary precision by matricial tracial moments. This is stated more formally in the next proposition, for a proof see e.g. [9].

▶ **Proposition 25.** *Let $(\mathcal{F},\tau)$ be a II_1 factor which embeds into $\mathcal{R}^{\mathcal{U}}$ for some free ultrafilter $\mathcal{U}$. Then $\mathcal{F}$ has matricial microstates, i.e., for any $n \in \mathbb{N}$ and given self-adjoint $T_1,\dots,T_n \in \mathcal{F}$ the following holds: for every $s \in \mathbb{N}$ and $\varepsilon > 0$ there exists $d \in \mathbb{N}$ and $B_1,\dots,B_n \in \mathcal{S}^d$ such that*

$$|\tau(T_{i_1}\cdots T_{i_t}) - \mathsf{tr}(B_{i_1}\dots B_{i_t}))| < \varepsilon \quad \textit{for all } i_1,\dots,i_t \in [n], t \le s.$$

C Additional proofs

The proofs of Lemma 3, 7 and 10 are easy and thus omitted.

Proof of Lemma 4

Instead of Lemma 4 we prove the following more elaborate version.

▶ **Lemma 26.** *For $M \in \mathcal{S}^n$, the following assertions are equivalent:*

(i) *$M \in \mathcal{CS}_+^{n*}$, i.e., $\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} \in \cup_{d\ge1}(\mathcal{S}_+^d)^n$.*

(ii) *$\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} \in \mathbf{\Delta}_n$.*

(iii) *$\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} = (X_1,\dots,X_n) \in \mathbf{\Delta}_n$ with $X_1 \succ 0,\dots,X_n \succ 0$.*

(iv) *$\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} = (X_1,\dots,X_n) \in \mathbf{\Delta}_n$ with $X_1 \succ 0,\dots,X_n \succ 0$ and with rational entries.*

(v) *$\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} \in \mathbf{\Delta}_n$ with rational entries.*

Proof. The implications (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv), (i) $\Longrightarrow$ (v) and (v) $\Longrightarrow$ (iv) are clear. We will show that (iv) $\Longrightarrow$ (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i).

The implication (ii) $\Longrightarrow$ (i) follows by scaling: Let $\underline{X} \in (\mathcal{S}_+^d)^n$ with $\lambda = \sum_{i=1}^n \mathsf{Tr}(X_i) > 0$ (else, $\underline{X}$ is identically zero and $\mathsf{Tr}(p_M(\underline{X})) = 0$). Then, $\underline{X}/\lambda \in \mathbf{\Delta}_n$ and thus $\mathsf{Tr}(p_M(\underline{X}/\lambda)) \ge 0$, which implies $\mathsf{Tr}(p_M(\underline{X})) \ge 0$.

The remaining implications follow using continuity arguments. Namely, for (iv) $\Longrightarrow$ (iii), use the fact that the set of rational positive definite matrices is dense within the set of positive definite matrices and, for (iii) $\Longrightarrow$ (ii), use the fact that the set of positive definite matrices is dense within the set of positive semidefinite matrices (combined with rescaling). ◀

Proof of Lemma 6

We show that

$$\mathcal{D}_r^n = \{M \in \mathcal{S}^n : \mathsf{Tr}(p_M(\underline{X})) \ge 0\ \forall \underline{X} \in \underline{\mathbf{\Delta}}(n,r)\}.$$

Proof. The inclusion "$\supseteq$" is clear since $\underline{\mathbf{\Delta}}(n,r) \subseteq \mathbf{\Delta}(n,r)$.

To show the reverse inclusion, take a matrix M such that $\mathsf{Tr}(p_M(\underline{X})) \ge 0$ for all $\underline{X} \in \underline{\mathbf{\Delta}}(n,r)$. Consider a n-tuple $\underline{X} = (X_1,\dots,X_n) \in \mathbf{\Delta}(n,r)$. The matrices $X_1,\dots,X_n$ are rational with denominator at most r, $\sum_{i=1}^n \mathsf{Tr}(X_i) = 1$ and $X_1,\dots,X_n \in \mathcal{S}_+^d$ with $d > r$ (else there is nothing to prove). For each $i \in [n]$, set $I_i = \{k \in [d] : X_i(k,k) \neq 0\}$ and notice that $\mathsf{Tr}(X_i) \ge |I_i|/r$ (since each diagonal entry $X_i(k,k)$ indexed by $k \in I_i$ is at least $1/r$). Hence we have $1 = \sum_{i=1}^n \mathsf{Tr}(X_i) \ge \sum_{i=1}^n |I_i|/r$, implying $\sum_{i=1}^n |I_i| \le r$. Then we can find a set I containing $I_1 \cup \ldots \cup I_n$ with cardinality $|I| = r$. As each matrix X_i has only zero entries outside of its principal submatrix $X_i[I]$ indexed by I, it follows that $\mathsf{Tr}(p_M(X_1,\dots,X_n)) = \mathsf{Tr}(p_M(X_1[I],\dots,X_n[I])) \ge 0$, where the last inequality follows from the fact that $(X_1[I],\dots,X_n[I])$ belongs to the set $\underline{\mathbf{\Delta}}(n,r)$. ◀

Proof of Lemma 14

We will only show that the matrix $Z = I + J \in \mathcal{S}^{nt}$ lies in the interior of $\mathcal{CS}_+$, the other claims are direct verification.

Proof. Assume that there exists a matrix $M \in \mathcal{CS}_+^{nt*}$ such that $\langle M, I + J\rangle = 0$; we show that $M = 0$. Indeed, as both I and J lie in $\mathcal{CS}_+^{nt}$ we get that $\mathsf{Tr}(M) = 0$ and $\langle J, M\rangle = 0$. Observe that since M is copositive its diagonal entries are nonnegative and thus equal to 0, which in turn implies that all its entries must be nonnegative. Combining with $\langle J, M\rangle = 0$, we deduce that M is identically zero. ◀

Proof of Lemma 20

Lemma 20 says that if we have $(X_k)_k, (Y_k)_k \in \prod_{k\in\mathbb{N}} \mathcal{S}_+^{d_k}$ such that $(\mathsf{tr}_{d_k}(X_kY_k))_{k\in\mathbb{N}}$ converges to some $a \in \mathbb{R}$, then there exist $(X_k')_k, (Y_k')_k \in \prod_{k\in\mathbb{N}} \mathcal{S}_+^k$ with $\mathsf{tr}_k(X_k'Y_k') \to a$ as $k \to \infty$.

Proof. By possibly reordering the indices we can assume that the sequence $(d_k)_{k\in\mathbb{N}}$ is monotonically nondecreasing. First, we modify the sequence $(X_k)_k$ in such a way that $d_k \le k$ holds for all $k \in \mathbb{N}$. For this, if there is some $k \in \mathbb{N}$ with $d_k > k$ we repeat the preceding element X_{k-1} exactly $d_k - k$ times before the element X_k. For instance, if $X_1 \in \mathbb{R}_+$ and $X_2 \in \mathcal{S}_+^3$ (i.e., $d_1 = 1$ and $d_2 = 3$), we replace the sequence $(X_1, X_2, X_3, \dots)$ by $(X_1, X_1, X_2, X_3, \dots)$. Then the position of X_k is shifted by $d_k - k$ to $k + d_k - k = d_k$. If $k = 1$ we simply add $d_1 - 1$ zero matrices before X_1. We do the same with the sequence $(Y_k)_k$. Then the new sequence of inner products is obtained from the original sequence $(\mathsf{tr}_{d_k}(X_kY_k))_{k\in\mathbb{N}}$ by replacing each $\mathsf{tr}_{d_k}(X_kY_k)$ by $d_k - k + 1$ copies of it if $d_k > k$, and thus still converges to the limit a.

Thus we can now assume that $d_k \le k$ for all $k \in \mathbb{N}$. We set $X_k' := \sqrt{\frac{k}{d_k}}(X_k \oplus 0_{k-d_k}) \in \mathcal{S}_+^k$ and $Y_k' := \sqrt{\frac{k}{d_k}}(Y_k \oplus 0_{k-d_k}) \in \mathcal{S}_+^k$ for every $k \in \mathbb{N}$. Then we have

$$\mathsf{tr}_k(X_k'Y_k') = \frac{1}{k}\,\mathsf{Tr}(X_k'Y_k') = \frac{1}{k}\frac{k}{d_k}\,\mathsf{Tr}(X_kY_k) = \mathsf{tr}_{d_k}(X_kY_k)$$

for every $k \in \mathbb{N}$. Hence the final sequence $(\mathsf{tr}_k(X_k'Y_k'))_{k\in\mathbb{N}}$ still converges to a. ◀

Making Existential-unforgeable Signatures Strongly Unforgeable in the Quantum Random-oracle Model

Edward Eaton[1] **and Fang Song**[1,2]

1 **Department of Combinatorics & Optimization, University of Waterloo, Canada**
`{eeaton,fang.song}@uwaterloo.ca`

2 **Institute for Quantum Computing, University of Waterloo, Canada**

Abstract

Strongly unforgeable signature schemes provide a more stringent security guarantee than the standard existential unforgeability. It requires that not only forging a signature on a new message is hard, it is infeasible as well to produce a new signature on a message for which the adversary has seen valid signatures before. Strongly unforgeable signatures are useful both in practice and as a building block in many cryptographic constructions.

This work investigates a generic transformation that compiles any existential-unforgeable scheme into a strongly unforgeable one, which was proposed by Teranishi et al. [30] and was proven in the classical random-oracle model. Our main contribution is showing that the transformation also works against *quantum* adversaries in the *quantum* random-oracle model. We develop proof techniques such as adaptively programming a quantum random-oracle in a new setting, which could be of independent interest. Applying the transformation to an existential-unforgeable signature scheme due to Cash et al. [10], which can be shown to be quantum-secure assuming certain lattice problems are hard for quantum computers, we get an efficient quantum-secure strongly unforgeable signature scheme in the quantum random-oracle model.

1998 ACM Subject Classification E.3 Public key cryptosystems

Keywords and phrases digital signatures, strongly unforgeable, quantum random-oracle, lattices

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.147

1 Introduction

Digital signature is a fundamental primitive in modern cryptography and has numerous applications. In a signature scheme, a signer uses his/her secret key to generate a signature on a message. Anyone who knows the corresponding public key can verify the integrity of the message and that it comes from the genuine signer. A standard security notion for digital signatures is called *existential-unforgeable* under *adaptive chosen-message-attacks* (eu-acma in short). Basically it means that an adversary, without knowing the secret key of a user, cannot forge a valid signature on a *new* message. This should hold even if the adversary has seen a few signatures generated by the honest user on messages adaptively chosen by the adversary. Another important security notion, stronger than eu-acma, is called *strongly* existential-unforgeable (su-acma). Here, in addition to eu-acma, it should be infeasible to forge a *new* signature on a previously signed message. Aside from applications in some practical scenarios [26], su-acma signatures turn out to be a very powerful tool in other cryptographic constructions. For instance they are used in transforming encryption schemes

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 147–162
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

that are secure under chosen-plain-text attacks into secure schemes under *chosen-ciphertext-attacks* [13, 6]; and in constructing identity-based blind signatures [15] and group signature schemes [2, 5].

Strongly unforgeable signature schemes can be obtained from existential-unforgeable ones via generic transformations [29, 18, 30]. The transformation in [30] (referred to as TOO hereafter) is particularly interesting because it only needs a mild computational assumption and the overhead it causes to the efficiency is small. This work studies this transformation in the quantum setting, where adversaries have the power of processing quantum information. We want to ask: *does* TOO *transformation still hold in the presence of quantum adversaries, and furthermore can we obtain quantum-secure* su-acma *signatures systematically?*

There is no quick answer to this question. In general a classically secure cryptographic construction can completely fall apart against quantum adversaries for at least two reasons. First of all, quantum computers can solve some problems efficiently which are otherwise believed hard classically. This breaks the computational assumption in many constructions. For example, many existing eu-acma signature schemes, the starting point of the transformation, are based on factoring or discrete logarithm. The TOO transformation itself also uses the discrete logarithm problem. They are immediately broken by Shor's quantum algorithms [27]. Naturally we may want to switch to *quantum-safe* assumptions. For example, we assume certain lattice problems are hard even against quantum algorithms and then construct crypto-systems based on them [25, 4]. However, this does not fix everything immediately due to another reason, which is more subtle. Security of a construction is established by a security reduction, which is a proof by contradiction showing that if a scheme is not secure, then one can break a computational assumption. Unfortunately, as pointed out by a line of works (e.g., [35, 16, 31, 28]), classical security reductions may not hold in the presence of quantum adversaries due to technical difficulties such as *quantum rewinding.*

There is an additional complication, which turns out to be the main difficulty towards making the TOO transformation go through in the quantum setting. Classically, TOO is proven in the random-oracle model (RO), where a hash function is treated as a truly random function and all users evaluate the hash function by querying the random function. However once an adversary becomes quantum, we should naturally allow the queries to be in quantum superposition. This is formalized as the quantum random-oracle model (QRO) [7]. The bad news is that many classical tricks in RO become difficult to apply in QRO, if not entirely impossible. For starters, classically it is trivial to answer random-oracle queries on-the-fly by generating fresh random value for new queries while maintaining a table to keep consistency. It is not obvious that some similar trick can handle quantum superposition queries. There have been a host of works in recent years developing proof techniques in QRO [36, 33, 32], but many classical techniques are still missing their counterparts in QRO.

Our Contributions. Our main result is showing that the TOO transformation still works against quantum adversaries in the quantum random-oracle model under reasonable computational assumptions. Specifically, we first make a simple observation that classically the TOO transformation actually holds using any (generic) chameleon hash function, rather than the specific instantiation by the discrete log problem. As our central contribution, we prove that once the chameleon hash function and the eu-acma signature scheme are both quantum-safe, then TOO transformation will produce a quantum-safe su-acma signature scheme in the quantum random-oracle model. In our proof, we develop a technique that allows for adaptively programming a quantum random-oracle in a new setting. We hope this technical can find applications and extensions elsewhere.

Once we have the transformation ready, we demonstrate instantiations of the building blocks to obtain concrete quantum-safe su-acma schemes. Using tools from [28], it is easy to verify that the bonsai-tree signature scheme by Cash et al. [10] is eu-acma against quantum adversaries assuming some lattice problem is quantum-safe[1]. In [10], a chameleon hash function was also proposed based on the same computational assumptions, which is easy to check that it is quantum-safe as well. Putting these pieces together, we can get a quantum-safe su-acma scheme.

Overview of Our Proof Techniques in QRO. As we mentioned earlier, many proof techniques in classical RO do not immediately go through in the QRO model. Roughly speaking, the classical proof for the TOO transformation relies on two features in the classical RO model: the history of queries that an adversary makes to the RO can the recorded, and at various steps one can assign a fresh random value on an input, since the response at an input needs not to be determined before being queried. Both become difficult in the quantum setting. Copying quantum superposition queries which are unknown quantum states is generally impossible, and apparently a single quantum query of the form $\sum |x, y\rangle \mapsto \sum |x, \mathcal{O}(x) \oplus y\rangle$ would "see" the function values at all inputs. It is hence unclear how to change $\mathcal{O}(x)$ later without being caught.

The first issue turns out to be non-essential. The purpose of keeping the RO queries is to make sure some special input x^* has not been queried by the adversary. Otherwise x^* can be used to break some assumption. In the quantum setting, we can just pick one of the queries at random and measure it. If the overall amplitude that adversary intends to query at x^* is high, the probability we recover x^* is only reduced by essentially a poly-factor (the number of the adversary's RO queries).

We then come up with a technique for adaptively programming a QRO in a new setting. Namely we want to change the function value at various inputs that the adversary has partial control (e.g., the prefix of these inputs are chosen by the adversary). Intuitively this is possible when these inputs still have sufficient uncertainty to the adversary. There exist techniques previously when these input strings are *information-theoretically* undetermined, possessing a high min-entropy for example [32, 34]. In contrast, in our case these inputs are *computationally* difficult to decide by the adversary. Namely, these inputs remain uncertain to the adversary unless some computational assumption is broken. We show that this is already sufficient freedom for programming the answers on these inputs. Being a little more specific, we show that the computational assumption implies *indistinguishability* of two functions which a distinguisher can have quantum access to: one is the all-zero function, and the other marks a set of strings that could be used to break the computational assumption. This may be interpreted as a computational analogue of the Grover search lower bound in quantum query complexity. This enables us to program a quantum random-oracle adaptively. Basically, the random-oracle embeds one of the preceding functions, and programming the random-oracle roughly amounts to switching between the two functions. Since the two functions are indistinguishable, any efficient quantum algorithm querying the random-oracle cannot notice whether we have re-programmed the quantum random-oracle. From a technical point of view, these claims may not sound very surprising. Nonetheless, we view them as an interesting conceptual shift, which is similar in spirit to [11] where the authors showed that *computational* constraints can force measurement on a quantum state and cause collapse to particular

[1] Actually, we observe a tighter security reduction so that a slightly weaker assumption on the lattice problem is sufficient.

subspaces. Our techniques also complements existing ones that are of information-theoretical flavor.

Related Works. Boneh and Zhandry [8] considered a stronger type of quantum attacks on signature schemes where an adversary can query a signing oracle in superposition. They proposed general transformations which amplify schemes that are secure against ordinary quantum adversaries (i.e., those who only issue classical signing query as we consider in this work), to achieve security under attacks with superposition signing queries. In contrast, the transformation in our work only considers ordinary quantum adversaries, but tries to amplify in terms of the type of forgeries that an adversary can produce. Lyubashevsky [21, 22] applied the Fiat-Shamir paradigm to construct lattice-based su-acma signatures in the random-oracle model from identification schemes. However whether these schemes are quantum-secure is unclear, because proving quantum security of the identification schemes faces the difficulty of quantum rewinding. More importantly, there is negative evidence that Fiat-Shamir paradigm may not hold in general in the QRO model [12, 1]. Dagdelen et al. [12] showed that a variant of Fiat-Shamir works in the QRO model, but only for a very special form of identification schemes. In a recent work by Unruh [34], a general transformation is proposed, which can produce (quantum-safe) strongly-unforgeable signatures in the QRO model from general Σ-protocols. However the overhead is much larger than the Fiat-Shamir transformation, and the resulting signature schemes are less efficient than what can be obtained from our work. We remark that there is a generic Merkle-tree approach that produces su-acma schemes out of su-acma one-time signature schemes, which should still hold against quantum adversaries. Therefore in principle, lattice-based one-time signatures, as in [23], would suffice for full-fledged quantum-safe su-acma schemes. However the resulting scheme is usually far less efficient and costly to manage (because it is typically stateful).

2 Preliminary

We review necessary definitions and cryptographic tools in this section.

▶ **Definition 1** (Signature Scheme). A **signature scheme** is composed of a triplet of probabilistic polynomial-time algorithms (G, S, V), satisfying the following:

- G is the key generation algorithm. On running, it produces a pair, (pk, sk). pk is the public key, or verification key, while sk is the secret key, or signing key.
- S is the signing algorithm. Upon input of a message M from a message space $\mathcal{M}$, as well as a secret key sk, it produces a signature σ on that message.
- V is the verification algorithm. It takes in a message M, a signature σ, and a public key pk, and will output either 'accept' or 'reject'.

Signature schemes must satisfy the **correctness requirement**, which is that for any (pk, sk) generated by G, and any $M \in \mathcal{M}$, if $\sigma \leftarrow S(M, sk)$ then $V(M, \sigma, pk) =$ 'accept'.

A standard security notion for signature schemes is **existential unforgeability under adaptive chosen message attack** (eu-acma).

▶ **Definition 2** (Existential Unforgeability under Adaptive Chosen Message Attack). Consider the following game between a challenger $\mathcal{C}$ and a forger $\mathcal{A}$:

- $\mathcal{C}$ runs G, and send the resulting pk to $\mathcal{A}$.
- $\mathcal{A}$ sends up to q messages $M_1, M_2, ..., M_q$ to $\mathcal{C}$, one at a time. For each message $\mathcal{C}$ receives, she sends back $\sigma_i = S(M_i, sk)$ to $\mathcal{A}$.

- $\mathcal{A}$ finally outputs a pair (M^*, σ^*) to $\mathcal{C}$. We call this a valid forgery if $M^* \neq M_i \forall i \in \{1, ..., q\}$ and $V(M^*, \sigma^*, pk) =$ 'accept'.

If, for polynomially bounded q, it is computationally infeasible for $\mathcal{A}$ to come up with a valid forgery, the scheme is said to be existentially unforgeable under adaptive chosen message attack.

▶ **Definition 3** (Strong Unforgeability under Adaptive Chosen Message Attack)**. Strong unforgeability under Adaptive Chosen Message attack**, or **su-acma**, is defined in the same way as eu-acma, except that the pair (M^*, σ^*) that $\mathcal{A}$ eventually submits must only require that $(M^*, \sigma^*) \neq (M_i, \sigma_i)$ for all i, instead of the requirement that $M^* \neq M_i$. This change means that the forgery $\mathcal{A}$ submits may either be a new message, or may be a message that $\mathcal{C}$ has already signed, but with a new signature.

Note that by allowing $\mathcal{A}$ to submit more kinds of forgeries, if it is still computationally infeasible for $\mathcal{A}$ to succeed, then we know that this type of forgery also cannot be created, making the scheme in a sense stronger.

Chameleon hash functions. Chameleon hash functions were introduced by Krawczyk and Rabin [19]. We need a slight generalization proposed in [10]. A family $\mathcal{H}$ of chameleon hash function is a collection of functions h that takes in a message m from a message space $\mathcal{M}$ and some randomness r from a randomness space $\mathcal{R}$, and outputs to a range $\mathcal{Y}$, ie, $h : \mathcal{M} \times \mathcal{R} \to \mathcal{Y}$. The randomness space is associated with some efficiently sampleable distribution. There are three properties we need for a family of chameleon hash functions:

- (Chameleon property) We require an algorithm HG that samples a hash function $h \in \mathcal{H}$ together with trapdoor information td satisfying that for any $m \in \mathcal{M}$ and $y \in \mathcal{Y}$, it is possible to efficiently sample $r \leftarrow h_{td}^{-1}(m, y)$ under the distribution associated with $\mathcal{R}$ such that $h(m, r) = y$.
- (Uniformity) For $h \leftarrow \mathcal{H}$ and $r \leftarrow \mathcal{R}$, $(h, h(m, r))$ is uniform over $(\mathcal{H}, \mathcal{Y})$ up to negligible statistical distance.
- (Collision resistance) For a hash function $h \leftarrow \mathcal{H}$, it is computationally infeasible for an adversary to find $(m, r), (m', r')$, with $(m, r) \neq (m', r')$ such that $h(m, r) = h(m', r')$.

Quantum Random-Oracle Model. The random oracle model is a technique used in cryptographic proofs. In it, Hash functions are replaced with random oracles. An adversary is given access to query this random oracle by providing an input, x, and is returned the response, $\mathcal{O}(x)$. These random oracles exist to replace hash functions in our proof. When we examine the proof in the context of quantum computers, Boneh et al. [7] have pointed out that since superposition queries to hash functions are possible, to truly capture this in a model allowing quantum computers, we must allow superposition queries to the random oracle. So we will allow superpositions of queries to our random oracle, $\sum a_x |x, y\rangle$, which will be responded to with a superposition of answers, $\sum a_x |x, y \oplus \mathcal{O}(x)\rangle$.

A cryptographic scheme is said to be *quantum-safe* (or quantum-secure) if the security conditions still hold once the adversaries become efficient quantum computers. We do not go into more precise definitions. See for example [16] for details.

3 Getting SU from EU in QRO

In this section we prove our main theorem.

▶ **Theorem 4.** *There exists a generic conversion that takes an quantum-safe* eu-acma *signature scheme* $\Sigma = (G, S, V)$ *and a family of quantum-safe collision-resistant chameleon hash functions* $\mathcal{H}$ *and produces a quantum-safe* su-acma *signature scheme* $\Sigma' = (G', S', V')$ *in the quantum random-oracle model.*

3.1 The Transformation

We first recall the TOO transformation [30] with a minor change. We use a generic chameleon hash function instead of an instantiation from the discrete log problem.

- G'. On input a security parameter 1^n, do the following:
  - Run G, obtaining (pk, sk).
  - Run HG obtaining a chameleon hash function h with trapdoor td.
  - Set $pk' = (pk, h)$ and $sk' = (sk, td)$.
- S'. On input of message M, do the following:
  - Sample a random C from the range of h.
  - Sign C using the signing algorithm S, obtaining $\sigma = S(C, sk)$
  - Compute $m = \mathcal{O}(M \| \sigma)$, where $\mathcal{O}$ is a hash function (to be replaced with a random oracle in the proof).
  - Using the trapdoor information td, find an r such that $h(m, r) = C$.
  - Output $\sigma' = (\sigma, r)$.
- V'. On input of a message M and a signature $\sigma' = (\sigma, r)$, do the following:
  - Compute $m = \mathcal{O}(M \| \sigma)$ and $C = h(m, r)$.
  - Output 'Accept' if and only if $V(C, \sigma, pk) =$ 'Accept' (otherwise, output 'Reject').

The correctness of the algorithm can be seen easily. If σ' was a signature generated on M using S', then C will be the same C generated during the running of S', and is precisely what σ is a signature for.

3.2 Main Technical Lemma: Adaptively Programming a Quantum RO

To prove the main theorem, we demonstrate a new scenario where we can adaptively program a quantum random-oracle. This extends existing works (e.g [32, 33, 34]) from information-theoretical setting to a computational setting, and we believe it is potentially useful elsewhere. We will formalize a probabilistic game which we call *witness-search.* It potentially captures the essence of numerous security definitions for cryptographic schemes (e.g. signatures). Then we show that the (computational) hardness of witness-search allows for adaptively programming a quantum random-oracle.

Let Samp be an instance-sampling algorithm. On input 1^n, Samp generates public information pk, description of a predicate P, and a witness w satisfying $P(pk, w) = 1$. Define a witness-search game WS as below.

Witness-Search Game WS

1. Challenger $\mathcal{C}$ generates $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$. Ignore w. Let $W_{pk} := \{w : P(pk, w) = 1\}$ be the collection of valid witnesses.
2. $\mathcal{A}$ receives pk and produces a string $\hat{w}$ as output.
3. We say $\mathcal{A}$ wins the game if $\hat{w} \in W_{pk}$.

We say WS(Samp) is hard, if for any poly-time $\mathcal{A}$, $\Pr[\mathcal{A} \text{ wins}] \leq \mathsf{negl}(n)$. For instance, Samp could be the KeyGen algorithm of a signature scheme. pk consists of the public key and description of the signature scheme. Predicate P is the verification algorithm and a witness consists of a valid message-signature pair. Security of the signature scheme implies hardness of $\mathsf{WS}(\mathsf{Samp})$.

▶ **Lemma 5** (Hardness of Witness-Search to Programming QRO). *Let two experiments E and E' be as below. If* WS *is hard, then* $\mathrm{ADV} := |\Pr_E[b=1] - \Pr_{E'}[b=1]| \leq \mathsf{negl}(n)$.

Note that E' differs from E only in that we reprogram the random oracle at some point in E'.

Experiment E

1. Generate $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$.
2. $\mathcal{O} \leftarrow \mathcal{F}$ is drawn uniformly at random from the collection of all functions $\mathcal{F}$.
3. $\mathcal{A}_1$ receives pk as input and makes at most q_1 queries to $\mathcal{O}$. $\mathcal{A}_1$ produces a classical string x.
4. Set $z := \mathcal{O}(x\|w)$.
5. $\mathcal{A}_2$ gets (x, w, z) and may access the final state of $\mathcal{A}_1$. $\mathcal{A}_2$ makes at most q_2 queries to $\mathcal{O}$. It outputs $b \in \{0,1\}$ at the end.

Experiment E'

1. Generate $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$.
2. $\mathcal{O} \leftarrow \mathcal{F}$ is drawn uniformly at random from the collection of all functions $\mathcal{F}$.
3. $\mathcal{A}_1$ makes at most q_1 queries to $\mathcal{O}$. It produces a classical string x.
4. Pick a random $z \in_R \mathsf{Range}(\mathcal{O})$. Reprogram $\mathcal{O}$ to $\mathcal{O}'$: $\mathcal{O}'(y) = \mathcal{O}(y)$ except that $\mathcal{O}'(x\|w) = z$.
5. $\mathcal{A}_2$ gets (x, w, z) and may access the final state of $\mathcal{A}_1$. $\mathcal{A}_2$ makes at most q_2 queries to $\mathcal{O}'$. It outputs $b \in \{0,1\}$ at the end.

To prove Lemma 5, we need another lemma below to pave the road. Roughly we want to argue that if witness-search is hard, then given an oracle which is either the all-zero function or a function that marks the witness set W_{pk}, no efficient algorithms can distinguish them. This may be intuitively interpreted as a computational analogue of Grover search lower bound. Its proof can be found in Appendix B.

▶ **Lemma 6.** *Let f be the all-zero function, and f_S be the characteristic function of a set S. Namely $f_S(x) = 1$ iff. $x \in S$. Define two experiments G and G' as below. If* $\mathsf{WS}(\mathsf{Samp})$ *is hard, then for any efficient $\mathcal{A}$ making $q \leq poly(n)$ queries,* $|\Pr_G[b=1] - \Pr_{G'}[b=1]| \leq \mathsf{negl}(n)$.

Experiment G

1. Generate $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$.
2. $\mathcal{A}$ is given pk and (quantum) access to f. $\mathcal{A}$ makes at most q queries to f and afterwards w is given to $\mathcal{A}$. It outputs $b \in \{0,1\}$ and aborts.

Proof of Lemma 5. We use a hybrid argument to prove the theorem. Define $E_i, i = 1, \ldots, 4$ as follows.

- $E_1 := E$. ($\mathcal{A}_1^{\mathcal{O}}/\mathcal{A}_2^{\mathcal{O}}$ in short.)
- E_2: identical to E_1 except that in step 3, $\mathcal{O}$ is replaced by $\bar{\mathcal{O}}$ where $\bar{\mathcal{O}}(y) = \mathcal{O}(y)$ but $\bar{\mathcal{O}}(y) = 0$ for any $y = \cdot\|w$ where $w \in W_{pk}$. ($\mathcal{A}_1^{\bar{\mathcal{O}}}/\mathcal{A}_2^{\mathcal{O}}$)

Experiment G'

1. Generate $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$. Let $f_{pk} := f_{W_{pk}}$, where $W_{pk} = \{w : P(w) = 1\}$. (i.e., $f_{pk}(x) = 1$ iff. $x \in W_{pk}$)
2. $\mathcal{A}$ is given pk and (quantum) access to f_{pk}. $\mathcal{A}$ makes at most q queries to f_{pk} and afterwards w is given to $\mathcal{A}$. It output $b \in \{0, 1\}$ and aborts.

- E_3: identical to E_2 except that after step 3, we use $\mathcal{O}'$ as defined in E' instead of $\mathcal{O}$. Observe that E_3 can also be obtained from E' by substitute $\bar{\mathcal{O}}$ for $\mathcal{O}$ in step 3. $(\mathcal{A}_1^{\bar{\mathcal{O}}}/\mathcal{A}_2^{\mathcal{O}'})$
- $E_4 := E'$. $(\mathcal{A}_1^{\mathcal{O}}/\mathcal{A}_2^{\mathcal{O}'})$

Define $\mathrm{ADV}_i := \left|\Pr_{E_i}[b = 1] - \Pr_{E_{i+1}}[b = 1]\right|$. We will show that ADV_1 and ADV_3 are both negligible using Lemma 6. $\mathrm{ADV}_2 = 0$ since in both E_2 and E_3, the function values for W_{pk} are assigned uniformly at random and independent of anything else. Therefore we conclude that $\mathrm{ADV} = |\Pr_E[b = 1] - \Pr_{E'}[b = 1]| \leq \sum \mathrm{ADV}_i = \mathsf{negl}(n)$.

We are only left to prove that $\mathrm{ADV}_1 \leq \mathsf{negl}(n)$, and $\mathrm{ADV}_3 \leq \mathsf{negl}(n)$ follows by similar argument. Suppose for contradiction that there exist $(\mathcal{A}_1, \mathcal{A}_2)$ such that $\mathrm{ADV}_1 \geq 1/p(n)$ for some polynomial $p(\cdot)$. We show that this will lead to a contradiction to Lemma 6 that $|\Pr_G[b = 1] - \Pr_{G'}[b = 1]| \leq \mathsf{negl}(n)$, which in turn contradicts the hardness of witness-search. To see this, we construct an algorithm D from $(\mathcal{A}_1, \mathcal{A}_2)$ that runs in G and G' such that $|\Pr_G[b = 1 : D] - \Pr_{G'}[b = 1 : D]| \geq 1/p(n)$. Let F be an oracle which ignores the first part of the input and then applies either all-zero function f or f_{pk} (as defined in G') on the second part. Let g be a random function. Define another oracle $H := g \circ F$ that implements the following transformation:

$$\begin{aligned}
|x, y\rangle \mapsto & |x, y\rangle \otimes |0\rangle \quad \text{append an auxiliary register} \\
\mapsto & |x, y\rangle \otimes |\overline{F(x)}\rangle \quad \text{compute the negation of } F \text{ on aux.} \\
\mapsto & |x, y \oplus \overline{F(x)} \cdot g(x)\rangle \otimes |\overline{F(x)}\rangle \quad \text{controlled-}g \\
\mapsto & |x, y \oplus \overline{F(x)} \cdot g(x)\rangle \quad \text{uncompute negation of } F \text{ and disgard aux.}
\end{aligned}$$

Observe that if F is induced from f then H is identical to a random function $\mathcal{O}$. Whereas if F comes from f_{pk} then H is identical to $\bar{\mathcal{O}}$ as in E_2. For an algorithm that queries at most q times to H, we can sample h from a family of $2q$-wise independent functions and simulate H efficiently (with access to F) without any noticeable difference.

Construction of D

1. D receives pk and an oracle F (one of the two candidates above).
2. D simulates oracle $H = g \circ F$ as defined above. D then simulates $\mathcal{A}_1$, for each of query from $\mathcal{A}_1$, it is answered by H with (two) oracle calls to F. Let x be the output of $\mathcal{A}_1$.
3. D receives w (from external challenger). It then simulates $\mathcal{A}_2$ on input $(x, w, z := H(x\|w))$ and oracle queries are answered by h.
4. D outputs the output of $\mathcal{A}_2$.

It is easy to see that if F is induced from f, the view of $\mathcal{A}_1$ and $\mathcal{A}_2$ is identical to that of E_1. Likewise if F is induced by f_{pk} then it is the same view as in E_2. Therefore $|\Pr_G[b = 1 : D] - \Pr_{G'}[b = 1 : D]| = |\Pr_{E_1}[b = 1 : (\mathcal{A}_1, \mathcal{A}_2)] - \Pr_{E_2}[b = 1 : (\mathcal{A}_1, \mathcal{A}_2)]| \geq 1/p(n)$. This gives a contradiction. ◀

3.3 Proof of Theorem 4

Brief Review of Classical Proof. Classical proof roughly goes as follows: consider a forger $\mathcal{A}$. If (M^*, σ'^*) is the forgery that $\mathcal{A}$ eventually submits, we will let $C^* = h(\mathcal{O}(M^* \| \sigma^*), r^*)$. Similarly, for a signing query made by the forger M_i, we let $C_i = h(\mathcal{O}(M_i \| \sigma_i), r_i)$.

We then analyze two separate cases. First the instance where $C^* \neq C_i$ for all i. In this case we show that this gives a break to the existential unforgeability of the signature scheme Σ, by way of (C^*, σ^*). Next, we examine the case where $C^* = C_i$ for some i. In this case we show that $(\mathcal{O}(M^* || \sigma^*), r^*)$ and $(\mathcal{O}(M_i || \sigma_i), r_i)$ provide a break to the collision resistance of the chameleon hash function.

For completeness the full classical proof is included in Appendix A. It is adapted from [30] and we use a generic chameleon hash function instead of a concrete instantiation from the discrete logarithm problem. There are also changes which by our opinion make the proof easier to understand.

Proof in the quantum random-oracle model. Let $\mathcal{A}$ be the forger making at most q queries, and let ϵ be the probability that $\mathcal{A}$ succeeds in her forgery. We construct $\mathcal{B}$ that either breaks existential unforgeablity of Σ or can find collisions in $\mathcal{H}$.

- **Case 1**: We define this case as occurring when $C^* \neq C_i$ for all i.
  Firstly, $\mathcal{B}$ will be acting as a quantum random oracle for $\mathcal{C}$. To do this, $\mathcal{B}$ simply chooses a $2q$-wise independent hash function, $\mathcal{O}$, and for any query $\mathcal{A}$ makes, $\Sigma\alpha_{x,z}|x, z\rangle$, $\mathcal{B}$ responds with $\Sigma\alpha_{x,z}|x, \mathcal{O}(x) \oplus z\rangle$.

Construction of Existential Forger $\mathcal{B}$

1. $\mathcal{B}$ receives a public key pk from the challenger $\mathcal{C}$
2. $\mathcal{B}$ simulates a variant of the strongly-unforgeable game with $\mathcal{A}$:
   (i) $\mathcal{B}$ generates $(h, td) \leftarrow HG(1^n)$. Initiate $\mathcal{A}$ with $pk' = (pk, h)$
   (ii) $\mathcal{B}$ simulates a random-oracle using a $2q$-wise independent hash function.
   (iii) On the ith signing query M_i from $\mathcal{A}$, $\mathcal{B}$ chooses a random C_i. It then signs C_i by submitting it to $\mathcal{C}$, obtaining σ_i. It computes $m_i = \mathcal{O}(M_i || \sigma_i)$, and using the trapdoor information td, finds an r_i such that $h(m_i, r_i) = C_i$. It sends $\sigma'_i = (\sigma_i, r_i)$ to $\mathcal{A}$.
4. Let $(M^*, (\sigma^*, r^*))$ be the final forgery produced by $\mathcal{A}$. Output (C^*, σ^*) as the forgery.

  From $\mathcal{A}$'s point of view, a $2q$-wise independent function is identical to a random function [36]. Noting that $C^* \neq C_i$ for all i, and the C_i's are precisely what was submitted to $\mathcal{C}$ for signing queries, and finally, seeing as this is a valid forgery, so $V(C^*, \sigma^*) =' accept'$, we can see that $\mathcal{B}$ submits $(C^*, \sigma*)$ as a valid new forgery, breaking the existential unforgeability of Σ and winning his game with $\mathcal{C}$. Thus in this case whenever $\mathcal{A}$ succeeds, so does $\mathcal{B}$, and so the probability $\mathcal{B}$ succeeds given we are in this case is ϵ.
- **Case 2**: This case is defined as occurring when $C^* = C_i$ for some i. In this case we will show a reduction to break the collision resistance of the chameleon hash function.
  It is easy to see that $\mathcal{B}$ finds a valid collision as long as $\mathcal{A}$ produces a valid forgery, with overwhelming probability. This is because if $C^* = C_i$, then $h(\mathcal{O}(M^* || \sigma^*), r^*) = h(\mathcal{O}(M_i || \sigma_i), r_i)$. We simply need to ensure that this is not a trivial collision. Note that since this must be a new forgery, $(M^*, \sigma^*, r^*) \neq (M_i, \sigma_i, r_i)$. If $r^* \neq r_i$, we are done. Otherwise, we can see that $M^* || \sigma^* \neq M_i || \sigma_i$, and thus since the values for $\mathcal{O}(M_i || \sigma_i)$ were chosen uniformly at random, $\mathcal{O}(M^* || \sigma^*) \neq \mathcal{O}(M_i || \sigma_i)$ with overwhelming probability.

Construction of Collision-Finding Adversary $\mathcal{B}$

1. $\mathcal{B}$ receives h from the challenger, which is sampled from the Chameleon hash function family.
2. $\mathcal{B}$, playing the role of a challenger, simulates a variant of the strongly-unforgeable game with $\mathcal{A}$:
   - (i) $\mathcal{B}$ generates $(pk, sk) \leftarrow G(1^n)$. Initialize $\mathcal{A}$ with $pk' = (pk, h)$. For $i = \{1, \ldots, q\}$, $\mathcal{B}$ generates m_i uniformly at random and $r_i \leftarrow \mathcal{R}$ (according to the specification of h). $\mathcal{B}$ computes $C_i := h(m_i, r_i)$ and $\sigma_i := S(sk, C_i)$.
   - (ii) $\mathcal{B}$ simulates a random-oracle in the usual way (i.e. t-wise independent hash function).
   - (iii) On the ith signing query M_i from $\mathcal{A}$, $\mathcal{B}$ reprograms the random-oracle: $\mathcal{O}(M_i\|\sigma_i) \leftarrow m_i$ and returns (σ_i, r_i) to $\mathcal{A}$.
4. Let $(M^*, (\sigma^*, r^*))$ be the final forgery produced by $\mathcal{A}$. We know $C^* = C_i$ for some i. Output $(\mathcal{O}(M^*||\sigma^*), r^*), (\mathcal{O}(M_i||\sigma_i), r_i)$ as the collision.

Therefore if we let EVT be the event that $\mathcal{A}$ produces a valid forgery, we only need to show that EVT occurs with probability $\Omega(\varepsilon)$ in the construction of $\mathcal{B}$. We prove it by a hybrid argument which transforms the standard strongly unforgeable game into the variant as in the construction of $\mathcal{B}$. We will show that the probablity of EVT is esstially preserved in the hybrid argument.

Let Hyd_0 the standard strongly-unforgeable game with $\mathcal{A}$. By hypothesis $\Pr[\mathsf{EVT} : \mathsf{Hyd}_0] \geq \varepsilon$. Consider the first hybrid Hyd_1 that makes only one change to Hyd_0: when the challenger answers a signing query, instead of querying the random-oracle $\mathcal{O}$ to obtain $m_i := \mathcal{O}(M_i\|\sigma_i)$, it samples a random m_i and programs the random oracle so that $\mathcal{O}(M_i\|\sigma) = m_i$. Note that in particular the challenger still uses the trapdoor to find $r_i \leftarrow h^{-1}(C_i, m_i)$. By Lemma 5, we claim that[2] $\Pr[\mathsf{EVT} : \mathsf{Hyd}_0] - \Pr[\mathsf{EVT} : \mathsf{Hyd}_1]| \leq \mathsf{negl}(n)$. Specifically we instantiate Samp as follows. pk will consists of a public key for Σ, hash function h, and random messages C_i. P will be the verification algorithm of Σ. $w := \sigma_i = S(sk, C_i)$ is the signature generated by $\mathcal{B}$ in 2.i), and W_{pk} consists of all strings that form a valid signature of C_i under Σ. $\mathsf{WS}(\mathsf{Samp})$ is hard because Σ is existential-unforgeable.

Hyd_2 is obtained by a small change in Hyd_1. Instead of sampling a random C_i, it is obtained by computing $h(m_i, r_i)$ from random (m_i, r_i). This change only causes (statistically) a negligible error. This is because if $h \leftarrow \mathcal{H}$ and $r_i \leftarrow \mathcal{R}$ then $C_i := h(m_i, r_i)$ will be uniformly random by the uniformity property of $\mathcal{H}$. In addition the chameleon property of $\mathcal{H}$ tells us that $r_i \leftarrow h_{td}^{-1}(C_i, m_i)$ is distributed statistically close to sampling $r_i \leftarrow \mathcal{R}$. Therefore the order of generating C_i and r_i does not matter.

Thus we see that $\mathcal{B}$ is able to break the collision-resistance property of the Chameleon hash function.

In sum, we have shown that if there is an adversary $\mathcal{A}$ breaking Σ', then there is an adversary who manages to break either the collision resistance of the chameleon hash function $\mathcal{H}$, or the existential unforgeability of the original signature scheme Σ with probablity $\Omega(\varepsilon)$. This contradicts the security of Σ and $\mathcal{H}$ if $\varepsilon \geq 1/poly(n)$. Thus we conclude that Theorem 4 holds.

[2] More precisely, we need to introduce sub-hybrids and each sub-hybrid makes such a change for just one signing query.

4 Discussion

Obtaining a quantum-safe su-acma signature scheme. In [10], the authors presented a scheme for generating chameleon hash functions, based off the short integer solution problem for lattices. They also demonstrate a reduction showing an efficient algorithm to break the collision resistance of the hash function implies an efficient algorithm to break the short integer solution problem for lattices. Using results from [28] this reduction can be shown to carry through to the quantum setting. As this problem is currently believed to be hard even for quantum computers, these chameleon hash functions' collision resistance remains even when faced with a quantum adversary. This chameleon hash function scheme can therefore be used in the transformation in this paper to get a quantum-secure transformation. This transformation, used with any quantum-safe eu-acma signature scheme will give a quantum-safe su-acma scheme in the quantum random-oracle model.

When implementing the scheme with the chameleon hash function from [10] we can see what the overhead would be in an actual realization. Let $n \geq 1, q \geq 2$, and $m = O(n \log q)$. Let k be the output length of the hash function. Then the public key, pk' will now carry with it a $\mathbb{Z}_q^{n\times m}$ matrix, so $|pk'| = |pk| + n(k+m)$. The secret key now includes a specialized lattice basis, which can be written as an $m \times m$ matrix over $\mathbb{Z}_q$, giving us $|sk'| = |sk| + m^2$. Finally, the signature overhead is the inclusion of a vector in $\mathbb{Z}_q^m$, so $|\sigma'| = |\sigma| + m$.

A signature scheme based off the Short Integer Solution problem for lattices is also presented in [10]. Examining the proof presented there with tools from [28], we can see that this signature scheme is quantum-safe eu-acma. Applying this transformation to this scheme, we obtain a quantum-safe su-acma signature scheme. In fact, we can show that the reduction shown in [10] is not as tight as it could be, and for a message of length k and at most Q queries, we can show that for adversary $\mathcal{F}$ and reduction $\mathcal{S}$, we have that $\mathrm{ADV}_{SIS}(\mathcal{S}^{\mathcal{F}}) \geq \mathrm{ADV}(\mathcal{F})_{SIG}^{\mathsf{eu\text{-}acma}}/(Q(k - \log Q))$. This is a small improvement over the result of the paper, showing that $\mathrm{ADV}_{SIS}(\mathcal{S}^{\mathcal{F}}) \geq \mathrm{ADV}(\mathcal{F})_{SIG}^{\mathsf{eu\text{-}acma}}/(Q(k-1)+1)$

Future directions. Our work has studied a very specific transformation that gives a systematic way of getting quantum-safe su-acma signatures. There are a few more transformations in the plain model (i.e. without a random-oracle) [29, 20, 18, 17]. We conjecture that they also hold against quantum adversaries. If this is the case, it will be meaningful to evaluate all these transformations and figure out which one is preferable under specific applications. On the other hand, we chose the Bonsai-tree signature scheme [10] to instantiate the TOO transformation. There are many recent improvements on lattice-based signatures in terms of key size and computational efficiency [9, 24, 14], which are shown to be eu-acma classically. If they can be shown to be quantum-safe, they we can get more efficient quantum-safe su-acma schemes in the quantum random-oracle model.

Acknowledgements. The authors are grateful to Andrew Childs for helpful discussions. EE was supported by NSERC on an undergraduate research award at the Institute for Quantum Computing, University of Waterloo. FS acknowledges support from NSERC, CryptoWorks21, ORF and US ARO.

References

1 Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 474–483. IEEE, 2014.

2 Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Advances in Cryptology – CRYPTO 2000*, pages 255–270. Springer, 2000.

3 Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

4 Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-quantum cryptography*. Springer, 2009.

5 Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Advances in Cryptology – CRYPTO 2004*, pages 41–55. Springer, 2004.

6 Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM Journal on Computing*, 36(5):1301–1328, 2006.

7 Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology – ASIACRYPT 2011*, pages 41–69. Springer, 2011.

8 Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Proceedings of CRYPTO 2013*, 2013.

9 Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *Public Key Cryptography – PKC 2010*, pages 499–517. Springer, 2010.

10 David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, 2012.

11 Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In *Theory of Cryptography (TCC)*, pages 374–393. Springer, 2004.

12 Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The fiat–shamir transformation in a quantum world. In *Advances in Cryptology – ASIACRYPT 2013*, pages 62–81. Springer, 2013.

13 Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Review*, 45(4):727–784, 2003.

14 Léo Ducas and Daniele Micciancio. Improved short lattice signatures in the standard model. In *Advances in Cryptology – CRYPTO 2014*, pages 335–352. Springer, 2014.

15 David Galindo, Javier Herranz, and Eike Kiltz. On the generic construction of identity-based signatures with additional properties. In *Advances in Cryptology – ASIACRYPT 2006*, pages 178–193. Springer, 2006.

16 Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *Advances in Cryptology – CRYPTO 2011*, pages 411–428. Springer, 2011.

17 Qiong Huang, Duncan S Wong, Jin Li, and Yi-Ming Zhao. Generic transformation from weakly to strongly unforgeable signatures. *Journal of Computer Science and Technology*, 23(2):240–252, 2008.

18 Qiong Huang, Duncan S. Wong, and Yiming Zhao. Generic transformation to strongly unforgeable signatures. In *Applied Cryptography and Network Security*, pages 1–17. Springer, 2007.

19 Hugo Krawczyk and Tal Rabin. Chameleon hashing and signatures. In *Proc. of NDSS*, pages 143–154, 2000.

20 Jin Li, Kwangjo Kim, Fangguo Zhang, and Duncan S. Wong. Generic security-amplifying methods of ordinary digital signatures. In *Applied Cryptography and Network Security*, pages 224–241. Springer, 2008.

21 Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In *Advances in Cryptology – ASIACRYPT 2009*, pages 598–616. Springer, 2009.

22 Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Advances in Cryptology – EUROCRYPT 2012*, pages 738–755. Springer, 2012.

23 Vadim Lyubashevsky and Daniele Micciancio. Asymptotically efficient lattice-based digital signatures. In *Theory of Cryptography*, pages 37–54. Springer, 2008.

24 Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology – EUROCRYPT 2012*, pages 700–718. Springer, 2012.

25 Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post-quantum cryptography*, pages 147–191. Springer, 2009.

26 Markus Rückert. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles. In *Post-Quantum Cryptography*, pages 182–200. Springer, 2010.

27 Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

28 Fang Song. A note on quantum security for post-quantum cryptography. In *Post-Quantum Cryptography*, pages 246–265. Springer, 2014.

29 Ron Steinfeld, Josef Pieprzyk, and Huaxiong Wang. How to strengthen any weakly unforgeable signature into a strongly unforgeable signature. In *Topics in Cryptology – CT-RSA 2007*, pages 357–371. Springer, 2006.

30 Isamu Teranishi, Takuro Oyama, and Wakaha Ogata. General conversion for obtaining strongly existentially unforgeable signatures. In *Progress in Cryptology – INDOCRYPT 2006*, pages 191–205. Springer, 2006.

31 Dominique Unruh. Quantum proofs of knowledge. In *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012. Preprint on IACR ePrint 2010/212.

32 Dominique Unruh. Quantum position verification in the random oracle model. In *Crypto 2014*, volume 8617 of *LNCS*, pages 1–18. Springer, August 2014. Preprint on IACR ePrint 2014/118.

33 Dominique Unruh. Revocable quantum timed-release encryption. In *Advances in Cryptology – EUROCRYPT 2014*, pages 129–146. Springer, 2014.

34 Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Advances in Cryptology – EUROCRYPT 2015*, pages 755–784. Springer, 2015.

35 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

36 Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Proceedings of CRYPTO 2012*, 2012.

A Classical Proof

Let $\mathcal{A}$ be the forger, $\mathcal{B}$ the reduction, and $\mathcal{C}$ be the challenger. In each case, $\mathcal{B}$ and $\mathcal{A}$ will be playing a game of strong unforgeability. Let the probability that $\mathcal{A}$ succeeds be ϵ. In Case 1, $\mathcal{C}$ and $\mathcal{B}$ will play a game of existential unforgeability on the signature scheme σ. In case 2, $\mathcal{C}$ and $\mathcal{B}$ will play a game of collision resistance on the chameleon hash function h. We show that if the probability $\mathcal{A}$ succeeds in her forgery is ϵ, then the probability that $\mathcal{B}$ succeeds is $\geq \frac{1}{2}\epsilon - \mathsf{negl}(n)$. At the beginning of the reduction, $\mathcal{B}$ will flip a coin, and guess which case the adversary's forgery will fall under. Clearly, $\mathcal{B}$ will be correct with probability $\frac{1}{2}$.

In our reduction, let the forgery that $\mathcal{A}$ eventually submits be $(M^*, \sigma'^* = (\sigma^*, r^*))$ Let $C^* = h(\mathcal{O}(M^*||\sigma^*), r^*)$. Similarly, for each M_i the forger submits to the signing oracle for signing, there is an associated σ'_i and C_i.

- **Case 1**: $C^* \neq C_i$ for all i. We show that whenever the forger succeeds in creating a valid forgery of this type, the reduction succeeds in breaking the existential unforgeability of the original scheme $\Sigma = (G, S, V)$.

  $\mathcal{C}$ and $\mathcal{B}$ will be playing a game of existential unforgeability, while $\mathcal{B}$ and $\mathcal{A}$ will be playing a game of strong unforgeability. We will show that whenever $\mathcal{A}$ wins her game, $\mathcal{B}$ wins his (so long as the forgery is of the type described above).

  The games will play out as follows:

  Firstly, $\mathcal{B}$ will act as the random oracle for $\mathcal{A}$. In the first case at least (and this will change only slightly case to case), he can do this in the following way. Whenever $\mathcal{A}$ queries the random oracle with a query, $\mathcal{B}$ looks up in a maintained table if that query has been made before. If it has, he responds with the value he responded with before. If it has not, he generates a random number and responds with that.

  Now we discuss how the game of strong unforgeability transpires.

  $\mathcal{C}$ sends $\mathcal{B}$ a public key pk from the Σ scheme. $\mathcal{B}$ will generate a chameleon hash function h, (with corresponding trapdoor td) and send the public key and hash function to $\mathcal{A}$ as $pk' = (pk, h)$.

  $\mathcal{A}$ will start submitting messages M_i to $\mathcal{B}$ for signing. For each query, $\mathcal{B}$ does the following:

  - Choose a random $\tilde{m}_i$ and $\tilde{r}_i$ and compute $C_i = H(\tilde{m}_i, \tilde{r}_i)$
  - Sign C_i by submitting it to $\mathcal{C}$ as a signing query, obtaining σ_i
  - Query $M_i||\sigma_i$ to the random oracle, obtaining $m_i = \mathcal{O}(M_i||\sigma_i)$
  - Using the trapdoor information td, find an r_i such that $h(m_i, r_i) = C_i$.
  - $\sigma_i' = (\sigma_i, r_i)$
  - Send σ_i' to $\mathcal{A}$

  Eventually, $\mathcal{A}$ will submit a valid forgery $M^*, \sigma'^* = (\sigma^*, r^*)$.

  Then, $\mathcal{B}$ takes these, and computes $C^* = h(\mathcal{O}(M^*||\sigma^*), r^*)$.

  Noting that $C^* \neq C_i$ for all i, and the C_i's are precisely what was submitted to $\mathcal{C}$ for signing queries, and finally, seeing as this is a valid forgery, so $V(C^*, \sigma^*) =' accept'$, we can see that $\mathcal{B}$ submits $C^*, \sigma*$ as a valid new forgery, breaking the existential unforgeability of Σ and winning his game with $\mathcal{C}$.

  Thus in this case whenever $\mathcal{A}$ succeeds, so does $\mathcal{B}$, and so the probability $\mathcal{B}$ succeeds given we are in this case is ϵ.

- **Case 2**: This case is defined as occurring when $C^* = C_i$ for some i. In this case we will show a reduction to break the collision resistance of the chameleon hash function.

  To start with, $\mathcal{C}$ sends $\mathcal{B}$ the description of a chameleon hash function h, which $\mathcal{B}$ will find a collision for.

  $\mathcal{B}$ then runs the key generation algorithm of the signature scheme Σ, obtaining (pk, sk). He then sends $pk' = (pk, h)$ to $\mathcal{A}$.

  For each signing query M_i that $\mathcal{A}$ sends to $\mathcal{B}$, $\mathcal{B}$ does the following:

  - Choose a random m_i and r_i and compute $C = h(m_i, r_i)$
  - Sign C_i using the signing algorithm S, obtaining $\sigma = S(C, sk)$
  - Reprogram the random oracle so that $\mathcal{O}(M_i||\sigma_i) = m_i$.
  - $\sigma_i' = (\sigma_i, r_i)$
  - Send σ_i' to $\mathcal{A}$.

  Note that we have now permitted $\mathcal{B}$ to reprogram the random oracle for the purposes of this proof. Thus it is necessary to show that $\mathcal{A}$ will still output a valid forgery.

  When $\mathcal{A}$ eventually submits her forgery, (M^*, σ^*), we can see that $C^* = C_i$ for some i. This implies that $h(\mathcal{O}(M_i||\sigma_i), r_i) = h(\mathcal{O}(M^*||\sigma^*), r^*)$ for that i. This shows us a collision for the chameleon hash function h, which is what $\mathcal{B}$ is looking for. But we must take care to ensure that it isn't a trivial collision.

Note that $(M_i, \sigma_i, r_i) \neq (M^*, \sigma^*, r^*)$, simply because both the message and signature of the forgery can't be the same as that of one of the M_i's. So at least one of these values is different.

If $r_i \neq r^*$, we are done. Otherwise, it must be the case that $M^*||\sigma^* \neq M_i||\sigma_i$. In this case, since the values for the random oracle are chosen uniformly at random, with overwhelming probability, $\mathcal{O}(M^*||\sigma^*) \neq \mathcal{O}(M_i||\sigma_i)$, giving $\mathcal{B}$ a collision for h.

So in this case, $\mathcal{B}$ will succeed as long as $\mathcal{A}$ does up to a negligible probability by Lemma 7. So the probability $\mathcal{B}$ succeeds is $\geq \epsilon - \mathsf{negl}(n)$

▶ **Lemma 7.** *For a forger $\mathcal{A}$, let $\mathcal{B}_1$ and $\mathcal{B}_2$ be as below, and have them play a game of strong unforgeability with $\mathcal{A}$. Then*

$$|Pr_{\mathcal{B}_1}(\mathcal{A}\ wins) - Pr_{\mathcal{B}_2}(\mathcal{A}\ wins)| \leq \mathsf{negl}(n),$$

as long as the underlying signature scheme is existentially unforgeable.

$\mathcal{B}_1$ is defined to operate exactly as the transformation dictates. $\mathcal{B}_2$ will operate as $\mathcal{B}$ was defined to in Case 2 above.

Proof. Say the difference in probability that $\mathcal{A}$ wins was not negligible. As the distribution of all values is the same, the only difference from $\mathcal{A}$'s perspective was that the value of $\mathcal{O}(M_i||\sigma_i)$ was changed for each i.

But clearly the only way to have the information that they changed is if $\mathcal{A}$ had already queried $\mathcal{O}(M_i||\sigma_i)$. But if $\mathcal{A}$ does this with non-negligible probability, then we could construct a reduction to break the existential forgeability of the signature scheme by playing strong unforgeability with $\mathcal{A}$, and before submitting each C_i to the signing oracle, checking to see if $\mathcal{A}$ had queried $M_i||\sigma_i$ to the random oracle. With non-negligible probability, the reduction finds a σ_i that is a valid forgery. So he submits this along with C_i and has broken the existential unforgeability of the scheme. ◀

Therefore in both cases, as long as $\mathcal{B}$ successfully guesses which case the forgery will fall under, he manages to successfully break either the collision resistance of the chameleon hash function h, or the existential unforgeability of the original signature scheme Σ. Since $\mathcal{B}$ correctly guesses what case he is in half of the time, his probability of success is $\geq \frac{1}{2}\epsilon - \mathsf{negl}(n)$.

B Proof of Lemma 6

Proof. Let $\mathcal{A}$ be an arbitrary algorithm running in G (or G'). Consider another algorithm B that runs in an experiment EXT as follows:

Extraction Experiment EXT

1. Generate $(pk, w, P) \leftarrow \mathsf{Samp}(1^n)$. Ignore w.
2. B receives pk and picks $j \in_R \{1, \dots, q\}$ at random.
3. B simulates $\mathcal{A}$ on pk and (quantum) access to f. Just before $\mathcal{A}$ making the jth query to f, B measures the register that contains $\mathcal{A}$'s query. Let z be the measurement outcome.

Let $p_B := \Pr_{EXT}[z \in W_{pk}]$ be the probability that the output of E is a valid witness. Let $\epsilon := |\Pr_G[b = 1] - \Pr_{G'}[b = 1]|$. In both experiment G and G', pk is selected at random according to Samp. Let P_{pk} be the probability that pk is outputted. Then

$$\begin{aligned}
\epsilon =& \left|\Pr_G[b=1] - \Pr_{G'}[b=1]\right| \\
=& \left|\sum_{pk} \Pr_G[b=1|pk] \cdot P_{pk} - \sum_{pk} \Pr_{G'}[b=1|pk] \cdot P_{pk}\right| \\
=& \sum_{pk} P_{pk} \left|\Pr_G[b=1|pk] - \Pr_{G'}[b=1|pk]\right| .
\end{aligned}$$

Let $\epsilon_{pk} := |\Pr_G[b=1|pk] - \Pr_{G'}[b=1|pk]|$. Let $|\phi_i\rangle$ be the superposition of $\mathcal{A}^G$ on input pk when the i'th query is made. Then let $q_y(|\phi_i\rangle)$ be the sum of squared magnitudes in $\mathcal{A}$ querying the oracle on the string y.

Let $S = [q] \times W_{pk}$. Let $\delta_{pk} = \sum_{(i,y)\in S} q_y(|\phi_i^{pk}\rangle)$. We employ a theorem by Bennet et al. [3], that states that $\| |\phi_i^{pk}\rangle - |\tilde{\phi}_i^{pk}\rangle \| \leq \sqrt{q \cdot \delta_{pk}}$. (Here $|\tilde{\phi}_i^{pk}\rangle$ is defined in the same way as $|\phi_i^{pk}\rangle$ but with G' rather than G).

The same paper [3] also bounds the probability of being able to distinguish the two states, which corresponds to our probability of distinguishing the two experiments, ϵ_{pk}, telling us that

$$\epsilon_{pk} \leq 4 \cdot \left\| |\phi_i^{pk}\rangle - |\tilde{\phi}_i^{pk}\rangle \right\| \leq 4\sqrt{q \cdot \delta_{pk}} .$$

Now note that P_B^{pk} (that is, the probability that EXT outputs a valid witness given pk is chosen) can be written as

$$\begin{aligned}
P_B^{pk} =& \sum_{i\in[0,q]} \left(\Pr[i \text{ chosen}] \cdot \sum_{(j,y)\in S: j=i} q_y(|\phi_j^{pk}\rangle) \right) \\
=& \frac{1}{q} \sum_{i\in[0,q]} \sum_{(j,y)\in S: j=i} q_y(|\phi_j^{pk}\rangle) \\
=& \frac{1}{q} \sum_{(i,y)\in S} q_y(|\phi_i^{pk}\rangle) = \frac{1}{q}\delta_{pk}
\end{aligned}$$

So we can see that $\epsilon_{pk} \leq 4q\sqrt{P_B^{pk}}$. Then

$$\epsilon = \sum_{pk} P_{pk}\epsilon_{pk} \leq 4q \sum_{pk} P_{pk} \sqrt{P_B^{pk}} \overset{(*)}{\leq} 4q \sqrt{\sum_{pk} P_{pk} P_B^{pk}} = 4q\sqrt{P_B} ,$$

where (*) applies Jensen's inequality. Finally, notice that B can be viewed as an adversary in the witness-search game $\mathsf{WS}(\mathsf{Samp})$. Therefore, we conclude that $p_B \leq \mathsf{negl}(n)$ by the hypothesis that $\mathsf{WS}(\mathsf{Samp})$ is hard and hence $|\Pr_G[b=1] - \Pr_{G'}[b=1]| \leq \mathsf{negl}(n)$. ◀

A Universal Adiabatic Quantum Query Algorithm

Mathieu Brandeho and Jérémie Roland

Université libre de Bruxelles, Quantum Information and Communication
1050 Brussels, Belgium
{mbrandeh,jroland}@ulb.ac.be

Abstract

Quantum query complexity is known to be characterized by the so-called quantum adversary bound. While this result has been proved in the standard discrete-time model of quantum computation, it also holds for continuous-time (or Hamiltonian-based) quantum computation, due to a known equivalence between these two query complexity models. In this work, we revisit this result by providing a direct proof in the continuous-time model. One originality of our proof is that it draws new connections between the adversary bound, a modern technique of theoretical computer science, and early theorems of quantum mechanics. Indeed, the proof of the lower bound is based on Ehrenfest's theorem, while the upper bound relies on the adiabatic theorem, as it goes by constructing a universal adiabatic quantum query algorithm. Another originality is that we use for the first time in the context of quantum computation a version of the adiabatic theorem that does not require a spectral gap.

1998 ACM Subject Classification F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Quantum Algorithms, Query Complexity, Adiabatic Quantum Computation, Adversary Method

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.163

1 Introduction

The quantum adversary method was originally introduced by Ambainis [2] for lower-bounding the *quantum query complexity* $Q(f)$ of a function f. It is based on optimizing a matrix Γ assigning weights to pairs of inputs. It was later shown by Høyer et al. [18] that using negative weights also provides a lower bound, which is stronger for some functions. A series of works [26, 27, 25] then led to the breakthrough result that this *generalized* adversary bound, which we will simply call adversary bound from now on, actually characterizes the quantum query complexity of any function f with boolean output and binary input alphabet. This is shown by constructing a tight algorithm based on the dual of the semidefinite program corresponding to the adversary bound[1]. Finally, Lee et al. [21] have generalized this result to the quantum query complexity of state conversion, where instead of computing a function $f(x)$, one needs to convert a quantum state $|\rho_x\rangle$ into another quantum state $|\sigma_x\rangle$.

All these results where obtained in the usual discrete-time query model, where each query corresponds to applying a unitary oracle O_x. In this model, an algorithm then consists in a series of input-independent unitaries $U_1, U_2, \dots, U_T$, interleaved with oracle calls O_x. Another natural model is the continuous-time (or Hamiltonian-based) model where the oracle corresponds to a Hamiltonian H_x, and the algorithm consists in applying a possibly

[1] Note that constructing a tight algorithm for a specific problem using this method requires to find an optimal feasible point for the semidefinite program, so that this method is not necessarily constructive. The same limitation will affect the universal adiabatic algorithm in the present article.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 163–179
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

time-dependent, but input-independent, *driver* Hamiltonian $H_D(t)$, together with the oracle Hamiltonian. The two models are related by the fact that the unitary oracle O_x can be simulated by applying the Hamiltonian oracle H_x for some constant amount of time. This implies that the continuous-time model is at least as powerful as the discrete-time model. In the other direction, Cleve et al. [11] have shown that the discrete-time model can simulate the continuous-time model up to at most a sublogarithmic overhead, which implies that the continuous- and discrete-time models are equivalent up to a sublogarithmic factor. Lee et al. [21] later improved this result to a full equivalence of both models, by showing that the fractional query model, an intermediate model proved in [11] to be equivalent to the continuous-time model, is also lower bounded by the adversary bound, so that all these models are characterized by this same bound (in the case of functions, a similar result can be obtained by extending an earlier proof of Yonge-Mallo, originally considering the adversary bound with positive weights, to the case of negative weights [30]).

Even though these results imply that the continuous-time quantum query complexity is characterized by the adversary bound, they do not provide an explicit Hamiltonian-based query algorithm, except the one obtained from the discrete-time algorithm by replacing each unitary oracle call by the application of the Hamiltonian oracle for a constant amount of time. The resulting Hamiltonian of this algorithm then involves many discontinuities (at all times in between unitary gates), which is not very satisfying from the point of view of physics, where *reasonable* Hamiltonians are smooth. However, such discontinuities are not unavoidable, as for some problems, continuous-time query algorithms based on smooth Hamiltonians are known.

The first example is unstructured search, for which Farhi and Gutmann [15] proposed a continuous-time analogue of Grover's algorithm based on a simple time-independent Hamiltonian (later, van Dam et al. [29], as well as Roland and Cerf [28], independently proposed an adiabatic version of this algorithm, based on a slowly varying Hamiltonian). Algorithms were also developed in the continuous-time model for various problems such as spatial search [8, 10, 16], oracle identification [23], or element distinctness [9]. In a seminal paper, Farhi et al. [13] proposed a quantum algorithm for the NAND-tree based on scattering a wave incoming on the tree, using a time-independent Hamiltonian. It is precisely this algorithm that, through successive extensions, led to the tight algorithm based on the adversary bound for any function in [27], but most of these extensions were using the discrete-time model.

In this article, we give a new continuous-time quantum query algorithm for any state conversion algorithm based on a slowly varying Hamiltonian, and also provide a direct proof of its optimality based on Ehrenfest's theorem, hence proving that the quantum query complexity of any state conversion problem is characterized by the adversary bound. The soundness of the adiabatic evolution used in our algorithm relies on a lemma from Avron and Elgart [4], which does not require the usual gap condition but only weaker spectral conditions, and was originally introduced to study atoms in quantized radiation fields. To the best of our knowledge, it is the first time that such an adiabatic theorem without a gap condition is used in the context of quantum computation.

The structure of the article is as follows. Section 2 is devoted to preliminaries: in Subsection 2.1, we define the necessary mathematical notions; in Subsection 2.4, we recall the quantum adiabatic evolution and quantum adiabatic theorems; in Subsection 2.2, we recall notions of quantum query complexity; and in Section 2.3, the discrete-time adversary method. Original contributions start in Section 3, where we give a direct proof that the adversary bound remains a lower bound for continuous-time quantum query complexity (Theorem 20).

Finally, in Section 4, we present our adiabatic quantum query algorithm **AdiaConvert**, and show that it is optimal, implying the characterization of the bounded-error quantum query complexity (Theorem 21).

2 Preliminaries

2.1 Definitions

Throughout this article, $\mathbb{X}$ and Σ are finite sets and n is a positive integer. Σ represents the alphabet and $\mathbb{X}$ represents a subset of words of length n: $x \in \mathbb{X} \subset \Sigma^n$.

▶ **Definition 1** (Matrix norms and inner product)**.** Let A and B be n-by-n matrices

- Inner product: $\langle A, B\rangle = \mathrm{tr}(A^*B)$, where A^* is the adjoint matrix of A,
- Hadamard product: $(A \circ B)_{ij} = A_{ij} \,.\, B_{ij}$,
- Operator norm: $\|A\| = \max_{|v\rangle} \frac{\|A|v\rangle\|}{\||v\rangle\|} = \max_{|u\rangle,|v\rangle} \frac{\langle u|A|v\rangle}{\||u\rangle\|.\||v\rangle\|}$,
- Trace norm: $\|A\|_{\mathrm{tr}} = \max_B \frac{\langle A,B\rangle}{\|B\|}$.

These definitions imply the following properties:

▶ **Lemma 2.** *For any n-by-n matrices A, B, C, we have*

- $\langle A \circ C, B\rangle = \langle A, B \circ C^*\rangle$
- $\langle A, B\rangle \leq \|A\|_{\mathrm{tr}} \cdot \|B\|$

In this context, the following matrix norm will be useful:

▶ **Definition 3** (γ_2 norm)**.** Let $\mathcal{D}$ be a finite set, A a $|\mathcal{D}|$-square matrix. The norm $\gamma_2(A)$ is defined as

$$\begin{aligned}\gamma_2(A) &= \min_{\substack{m\in\mathbb{N}\\ |u_x\rangle,|v_y\rangle\in\mathbb{C}^m}} \left\{ \max_{x\in\mathcal{D}} \max\left\{\| \,|u_x\rangle\, \|^2, \| \,|v_y\rangle\, \|^2\right\} \middle| \forall\, x,y \in \mathcal{D},\ A_{x,y} = \langle u_x|\ v_y\rangle \right\},\\ &= \max_{\substack{|u\rangle,|v\rangle\\ \||u\rangle\|=\||v\rangle\|=1}} \|A \circ |u\rangle\langle v|\|_{\mathrm{tr}}.\end{aligned}$$

In particular, it is shown in [21] that the dual of the Adversary bound can be seen as a variation of the γ_2 norm dubbed the filtered γ_2 norm.

▶ **Definition 4** (Filtered γ_2 norm)**.** Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two finite sets, A, $Z_1, \dots, Z_n$ matrices with $|\mathcal{D}_1|$ rows and $|\mathcal{D}_2|$ columns, and $Z = \{Z_1, \dots, Z_n\}$. The norm $\gamma_2(A|Z)$ is defined as

$$\begin{aligned}\gamma_2(A|Z) = &\min_{\substack{m\in\mathbb{N}\\ |u_{x,j}\rangle,|v_{y,j}\rangle\in\mathbb{C}^m}} \max\left\{ \max_{x\in\mathcal{D}_1} \sum_j \| \,|u_{x,j}\rangle\, \|^2, \max_{y\in\mathcal{D}_2} \sum_j \| \,|v_{y,j}\rangle\, \|^2 \right\}\\ &\quad\text{subject to}\quad \forall (x,y) \in \mathcal{D}_1 \times \mathcal{D}_2, \quad A_{x,y} = \sum_j (Z_j)_{x,y} \langle u_{x,j}|\ v_{y,j}\rangle\,,\\ = &\max_{\Gamma} \quad \|\Gamma \circ A\| \qquad \text{subject to} \quad \forall j \ \ \|\Gamma \circ Z_j\| \leq 1.\end{aligned}$$

▶ **Claim 5** ([22])**.** *For any matrices A, B where $A \circ B$ is defined, $\|A \circ B\| \leq \gamma_2(A).\|B\|$.*

The Hadamard product fidelity is introduced in [22] to characterize the output condition of quantum query problems. Whereas the usual fidelity compares density matrices, the Hadamard product fidelity compares Gram matrices (note that if ρ is a Gram matrix and $|u\rangle$ is a normalized state, then $\rho \circ |u\rangle\langle u|$ is a density matrix).

▶ **Definition 6** (Hadamard product fidelity). The Hadamard product fidelity between two Gram matrices ρ and σ is defined as

$$\mathcal{F}_H(\rho, \sigma) = \min_{|u\rangle : \||u\rangle\| = 1} \mathcal{F}(\rho \circ |u\rangle\langle u|, \sigma \circ |u\rangle\langle u|),$$

where $\mathcal{F}(\rho', \sigma')$ is the fidelity between two density matrices ρ' and σ', defined as $\mathcal{F}(\rho', \sigma') = \operatorname{tr}\sqrt{\sqrt{\rho'}\,\sigma'\sqrt{\rho'}}$.

We similary define the Hadamard product distance from the trace distance.

▶ **Definition 7** (Hadamard product distance). The Hadamard product distance between two Gram matrices ρ and σ is defined as

$$\mathcal{D}_H(\rho, \sigma) = \max_{|u\rangle : \||u\rangle\| = 1} \mathcal{D}(\rho \circ |u\rangle\langle u|, \sigma \circ |u\rangle\langle u|),$$

where $\mathcal{D}(\rho', \sigma')$ is the trace distance between two density matrices ρ' and σ', defined as $\mathcal{D}(\rho', \sigma') = \frac{1}{2}\|\rho' - \sigma'\|_{\mathrm{tr}}$.

▶ **Theorem 8** ([17]). *For any density matrices ρ, σ, we have $1 - \mathcal{D}(\rho, \sigma) \leq \mathcal{F}(\rho, \sigma) \leq \sqrt{1 - \mathcal{D}^2(\rho, \sigma)}$.*

▶ **Corollary 9.** *For any Gram matrices ρ, σ, we have $1 - \mathcal{D}_H(\rho, \sigma) \leq \mathcal{F}_H(\rho, \sigma) \leq \sqrt{1 - \mathcal{D}_H^2(\rho, \sigma)}$.*

▶ **Definition 10** (Distance between quantum states). We say that two normalized quantum states $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ are ε-distant if $\||\phi\rangle - |\psi\rangle\| \leq \varepsilon$.

2.2 Quantum query complexity

In classical computation, a query algorithm computes a function $f : \mathbb{X} \subset \Sigma^n \to B$ where the input $x \in \mathbb{X}$ can only be accessed through queries to an oracle that, on input $j \in [n]$, outputs $x_j \in \Sigma$. A query algorithm can be seen as a decision tree [7] where each vertex represents a decision taken after one query. The depth of the tree then corresponds to the number of queries used by this algorithm to compute f in the worst case. The *query complexity of f* is the minimum depth of all decision trees computing f exactly.

In quantum computation, query complexity can be generalized to state conversion problems, where one should convert a quantum state $|\rho_x\rangle$ into another state $|\sigma_x\rangle$, each depending on the input x, which can once again only be accessed via an oracle. The evaluation of a function f is the particular case where initial states are independent of x, and final states are orthonormal for x, y such that $f(x) \neq f(y)$. For any set of quantum states $\{|\rho_x\rangle\}_x$, it is enough to consider the Gram matrix $\rho_{x,y} = \langle\rho_x|\, \rho_y\rangle$, because if $\langle\rho_x|\, \rho_y\rangle = \langle\rho'_x|\, \rho'_y\rangle$ for all x, y, then there exists a unitary transformation U independent of x such that $|\rho_x\rangle = U\,|\rho'_x\rangle$ for all x. This implies that a query algorithm for the set of states $\{|\rho\rangle\}_x$ can be converted into a query algorithm for the set of states $\{|\rho'\rangle\}_x$ without additive cost, and *vice versa.* We will therefore denote by a pair of Gram matrices (ρ, σ) the problem of converting a set of states $\{|\rho_x\rangle\}_x$ into another set of states $\{|\sigma_x\rangle\}_x$.

In the discrete-time model of quantum query complexity, we can consider without loss of generality an oracle O_x acting on an n-dimensional input register and a $(|\Sigma| + 1)$-dimensional output register as

$$O_x : \begin{cases} |j\rangle\,|\bar{0}\rangle \mapsto |j\rangle\,|x_j\rangle & \forall j \in [n] \\ |j\rangle\,|x_j\rangle \mapsto |j\rangle\,|\bar{0}\rangle & \forall j \in [n] \\ |j\rangle\,|y\rangle \mapsto |j\rangle\,|y\rangle & \forall j \in [n], y \in \Sigma \setminus \{x_j\} \end{cases} \tag{1}$$

where $\bar{0}$ is an additional output alphabet symbol, that can be seen as a blank symbol. A query algorithm in this model is then given by a succession of input-independent unitaries U_t interleaved with oracle calls O_x. The discrete-time quantum query complexity $Q_0^{\mathrm{dt}}(\rho,\sigma)$ is the minimum number of oracle calls of any such algorithm converting ρ to σ exactly. (Note that there exist alternative definitions for the oracle O_x, but they only affect the definition of $Q_0^{\mathrm{dt}}(\rho,\sigma)$ by at most a constant factor.)

In the continuous-time model, the oracle is a Hamiltonian $H_{\mathcal{Q}}(x)$ of the general form

$$H_{\mathcal{Q}}(x) = \sum_{j=1}^{n} |j\rangle\langle j| \otimes h(x_j), \tag{2}$$

where each $\{h(y)\}_{y\in\Sigma}$ is hermitian and satisfies $\|h(y)\| \leq 1$. In particular, the choice $h(y) = |y^-\rangle\langle y^-|$, where

$$|y^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\bar{0}\rangle \pm |y\rangle), \tag{3}$$

can be considered as the Hamiltonian analogue of the unitary oracle O_x in equation (1), since it is easy to check that $O_x = e^{-iH_{\mathcal{Q}}(x)\Delta T}$ for $\Delta T = \pi$. A query algorithm in this model then corresponds to applying a Hamiltonian $H_x(t)$ of the form

$$H_x(t) = H_{\mathcal{D}}(t) + \alpha(t)H_{\mathcal{Q}}(x) \tag{4}$$

where $H_{\mathcal{D}}(t)$ is the driver Hamiltonian independent of the input x, and $|\alpha(t)| \leq 1$ for all $t \in [0,T]$. The continuous-time quantum query complexity $Q_0^{\mathrm{ct}}(\rho,\sigma)$ is the minimum computing time T of any such algorithm converting ρ to σ exactly.

For scenarios where we accept errors, we must distinguish two cases : *coherent* and *non-coherent* quantum state conversion. Concretely, a computation will typically use some extra workspace and may therefore generate a state $|\sigma_x, J_x\rangle$, where $|J_x\rangle$ is the final state of the workspace. This might not be desirable if the state generation is used as a subroutine in a larger quantum algorithm, where we would like to use interferences between the states $|\sigma_x\rangle$ for different x's. In that case, we would like to be able to reset the state $|J_x\rangle$ to a default state, so that it does not affect interferences.

We therefore define the following output conditions (both for the discrete- and continuous-time models)

▶ **Definition 11** (Output condition). A quantum query algorithm acting as unitary $\mathcal{U}_x$ for input x converts ρ to σ with error at most ε if

- (coherent case) $\forall x \in \mathbb{X}$, $\mathrm{Re}(\langle\sigma_x, 0|\,\mathcal{U}_x|\rho_x, 0\rangle) \geq \sqrt{1-\varepsilon}$,
- (non-coherent case) $\forall x \in \mathbb{X}$, $\exists\,|J_x\rangle$, $\mathrm{Re}(\langle\sigma_x, J_x|\,\mathcal{U}_x|\rho_x, 0\rangle) \geq \sqrt{1-\varepsilon}$.

Note that a sufficient condition for $\mathrm{Re}(\langle\phi|\,\psi\rangle) \geq \sqrt{1-\varepsilon}$ is that these states are $\sqrt{\varepsilon}$-distant. Moreover, the output condition for the coherent case has been shown [22] to be equivalent to $\mathcal{F}_H(\sigma,\sigma') \geq \sqrt{1-\epsilon}$, where σ' is the Gram matrix of the output states $|\sigma'_x\rangle = \mathcal{U}_x\,|\rho_x, 0\rangle$. Similarly, in the non-coherent case the output conditions can be rewritten as $\mathcal{F}_H(\sigma \circ J, \sigma') \geq \sqrt{1-\epsilon}$, where J is any Gram matrix of unit vectors (corresponding to any set of states $|J_x\rangle$). This implies that bounded-error and zero-error quantum query complexities are related as follows.

▶ **Lemma 12** ([22]). *For any $|\mathbb{X}|$-by-$|\mathbb{X}|$ Gram matrices ρ,σ, we have*

$$Q_\varepsilon^\bullet(\rho,\sigma) = \min_{\sigma'}\left\{Q_0^\bullet(\rho,\sigma') : \mathcal{F}_H(\sigma,\sigma') \geq \sqrt{1-\epsilon}\right\} \tag{5}$$

$$Q_\varepsilon^{\mathrm{nc},\bullet}(\rho,\sigma) = \min_{\sigma'}\left\{Q_0^\bullet(\rho,\sigma') : \mathcal{F}_H(\sigma\circ J,\sigma') \geq \sqrt{1-\epsilon}, J\circ\mathbb{1} = \mathbb{1}\right\} \tag{6}$$

where the superscript nc *denotes the non-coherent query complexity (otherwise we consider the coherent case by default), and the superscript* $\bullet$ *is either* dt *or* ct*.*

Computing a function f is equivalent to generating the Gram matrix $F_{x,y} = \delta_{f(x),f(y)}$ from the all-1 Gram matrix $\mathbb{J}_{x,y} = 1$. In that case, it is not necessary to generate the state coherently, but one can convert a non-coherent algorithm into a coherent algorithm, so that we can consider the coherent case without loss of generality.

▶ **Lemma 13** ([22]). *For any function f and associated Gram matrix $F_{x,y} = \delta_{f(x),f(y)}$, we have $Q_\varepsilon^\bullet(f) = Q_\varepsilon^{\mathrm{nc},\bullet}(\mathbb{J}, F)$ and*

$$Q_\varepsilon^{\mathrm{nc},\bullet}(\mathbb{J}, F) \leq Q_\varepsilon^\bullet(\mathbb{J}, F) \leq 2Q_{1-\sqrt{1-\varepsilon}}^{\mathrm{nc},\bullet}(\mathbb{J}, F).$$

2.3 Adversary methods

The quantum adversary method is one of main methods to prove lower bounds on quantum query complexity (the other main method is the polynomial method [5]). Its basic principle is rather simple: it consists in defining a so-called progress function W whose value is high at the beginning of the algorithm and should be low at the end of the algorithm if it is successful. By bounding the change in the progress function for each oracle call, one then bounds the minimum number of oracle calls necessary for success.

More precisely, let $|\phi_x(t)\rangle$ be the state of the algorithm on input x after t queries, and Φ_t be the Gram matrix of those states. We define a progress function

$$W(\Phi_t) = \langle \Gamma \circ vv^*, \Phi_t \rangle \,,$$

where Γ is a $|\mathbb{X}|$-by-$|\mathbb{X}|$ hermitian matrix, called the *adversary matrix*, and v a unit vector. We also define the matrices Δ_j with entries $(\Delta_j)_{x,y} = 1 - \delta_{x_j,y_j}$. The adversary method relies on the fact that if Γ is chosen so that it satisfies $\|\Gamma \circ \Delta_j\| \leq 1$ for all $j \in [n]$, then the progress function can only increase by one after each query (see e.g. [18]), that is, $|W(\Phi_{t+1}) - W(\Phi_t)| \leq 1$. The difference of the values of the progress function between $\Phi_0 = \rho$ and $\Phi_T = \sigma$ is then given by

$$W(\Phi_0) - W(\Phi_T) = \langle \Gamma \circ vv^*, \rho - \sigma \rangle = \langle \Gamma \circ (\rho - \sigma), vv^* \rangle \leq T$$

By optimizing over Γ and v, we obtain the adversary bound:

▶ **Definition 14** ([21, 22], Adversary bound)**.**

$$\begin{aligned} \mathrm{Adv}^\star(\rho, \sigma) &= \max_\Gamma \|\Gamma \circ (\rho - \sigma)\| && \text{subject to} \quad \forall j \in [n], \quad \|\Gamma \circ \Delta_j\| \leq 1, \\ &= \gamma_2(\rho - \sigma | \Delta) && \text{where} \quad \Delta = \{\Delta_1, \dots, \Delta_n\}. \end{aligned}$$

As shown in [21], $\mathrm{Adv}^\star$ defines a distance between Gram matrices, sometimes called *the query distance.* The following simple proposition, comparing the query distance to the Hadamard product distance $\mathcal{D}_H$, will be used in the proof of Theorem 21.

▶ **Proposition 15.** *For any Gram matrices ρ, σ of size n, $\mathcal{D}_H(\rho, \sigma) \leq \mathrm{Adv}^\star(\rho, \sigma)$.*

Proof. Since the trace distance may be written as $\mathcal{D}(\rho', \sigma') = \max_{P:\|P\|\leq 1} \frac{1}{2} \langle P, (\rho' - \sigma') \rangle$, we can reformulate the Hadamard product distance in Definition 7 as

$$\mathcal{D}_H(\rho, \sigma) = \max_{\substack{P:\|P\|\leq 1/2 \\ |u\rangle:\||u\rangle\|=1}} \langle P, (\rho - \sigma) \circ |u\rangle\langle u| \rangle = \max_{P:\|P\|\leq 1/2} \|P \circ (\rho - \sigma)\|.$$

We observe that this form is similar to $\mathrm{Adv}^{\star}$ in Definition 14, except for the constraints on P and Γ. We conclude the proof by showing that the constraint on P is stronger, that is, if $\|P\| \leq 1/2$ then $\|P \circ \Delta_i\| \leq 1$ for all $i \in [n]$.

Let $\mathbb{J}$ be the all-one matrix, and $i \in [n]$. We have

$$\|P \circ \Delta_i\| \leq \|P\| + \|P \circ (\mathbb{J} - \Delta_i)\| \leq \Big(1 + \gamma_2(\mathbb{J} - \Delta_i)\Big)\|P\|,$$

where the inequalities follows from the triangle inequality and Claim 5, respectively. We finally bound $\gamma_2(\mathbb{J} - \Delta_i)$ using the minimization form in Definition 3 and an appropriate choice for $\{|u_x\rangle, |v_x\rangle\}_x$. Choosing $|u_x\rangle = |v_x\rangle = |x_i\rangle$, we have $\langle u_x|\, v_y\rangle = (\mathbb{J} - \Delta_i)_{x,y} = \delta_{x_i,y_i}$, so that $\gamma_2(\mathbb{J} - \Delta_i) \leq 1$. ◀

2.4 Adiabatic quantum computation

Adiabatic quantum computation is a quantum computational model originally proposed by Farhi et al. [14] for solving instances of the satisfiability problem. This model is based on the quantum adiabatic theorem introduced by Born and Fock [6] and describing a physical system evolving under a slowly varying Hamiltonian:

> *A quantum system with a time-dependent Hamiltonian remains in its instantaneous eigenstate if the Hamiltonian variation is slow enough and there is a large gap between its eigenvalue and the rest of the spectrum of the Hamiltonian.*

It was later proved that the adiabatic model is equivalent to standard quantum computation [1]. This statement, as well as the correctness of most adiabatic algorithms, rely on the existence of a spectral gap.

In order to formally describe adiabatic quantum computation, let us first define the notion of adiabatic process.

▶ **Definition 16.** An **adiabatic process** on the Hilbert space $\mathcal{H}$ is defined by a triplet $\{H(s), P(s), \tau\}$ with $s \in [0,1]$ where

(a) $H(s)$ is a twice differentiable map from $[0,1]$ to the space of bounded linear self-adjoint operators $B(\mathcal{H})$, equipped with the graph norm of $H(0)$.

(b) $P(s)$ are a family of orthogonal rank-one projections onto an eigenvector of $H(s)$ with continuous eigenvalue $\lambda(s)$,

(c) $\tau \in \mathbb{R}^+$ is the time scale, which defines the time as $t(s) = s\tau$.

For such an adiabatic process, we can define the unitary operator $U_A(s)$ corresponding to an idealized evolution, which maps the eigenvector in the range of $P(0)$ to the eigenvector in the range of $P(s)$, that is, $U_A(s)P(0)U_A^*(s) = P(s)$. Furthermore, the physical evolution, represented by unitary operator $U_\tau(s)$, can be obtained from the Schrödinger equation

$$i\partial_s U_\tau(s) = \tau H(s) U_\tau(s). \tag{7}$$

Let us note that the analytical conditions given in Definition 16 ensure the existence and uniqueness of the solution $U_\tau(s)$ of this equation with initial condition $U_\tau(0) = \mathbb{1}$ [24].

The quantum adiabatic theorem can be summarized by the following statement

$$\lim_{\tau\to\infty} U_\tau(s)P(0) = U_A(s)P(0) = P(s)U_A(s).$$

Thus $U_\tau(s)P(0)$ converge to $U_A(s)P(0)$ for large τ, and the norm of their difference defines the error of the adiabatic process.

▶ **Definition 17.** The **error** $\varepsilon_{AP}(s)$ of an adiabatic process $\{H(s), P(s), \tau\}$ is defined as

$$\varepsilon_{AP}(s) = \left\| \left[U_\tau(s) - U_A(s) \right] P(0) \right\|, \qquad \text{with} \quad \varepsilon_{AP} = \varepsilon_{AP}(1).$$

This definition implies that at the end of the adiabatic evoltion, the physical state will be ε_{AP}-distant from the ideal state.

How slow should the process be, or, equivalently, how large should τ be, to ensure a small enough adiabatic error? The *folk adiabatic condition* requires the following bound:

$$\tau \gg \int_0^1 \frac{\|\partial_s H_\tau(s)\|}{g(s)^2} ds, \tag{8}$$

where the gap $g(s)$ represents the minimal distance between the eigenvalue $\lambda(s)$ and the rest of spectrum of $H(s)$. However this *folk adiabatic condition* is not always sufficient, but rigorous conditions have been given e.g. by Jansen et al. [19]. Indeed, they proved the following statement (where we introduce the notation $\dot{A}(s) = \partial_s A(s)$).

▶ **Theorem 18** ([19]). *Let $\{H(s), P(s), \tau\}$ be an adiabatic process with a gap $g = \min_{s\in[0,1]} g(s)$, $\dot{H}$, $\ddot{H}$ are bounded operators, and $\varepsilon > 0$, if*

$$\tau \geq \frac{1}{\varepsilon}\left[\frac{\|\dot{H}(0)\| + \|\dot{H}(1)\|}{g^2} + \max_{s\in[0,1]} \frac{\|\ddot{H}(s)\|^2}{g^2} + 7\frac{\|\dot{H}(s)\|^2}{g^3}\right],$$

then $\varepsilon_{AP} \leq \varepsilon$.

The adiabatic process used in our algorithm introduced in Section 4 does not necessarily exhibit a gap, and for this reason we use another lemma from Avron and Elgart [4].

▶ **Lemma 19** ([4]). *Let $\{H(s), P(s), \tau\}$ be an adiabatic process and $\varepsilon > 0$. Suppose that the commutator equation*

$$\dot{P}(s)P(s) = [H(s), X(s)] \tag{9}$$

accepts as solution operator $X(s)$ such that both $X(s)$ and $\dot{X}(s)$ are bounded. If

$$\tau \geq \max_{s\in[0,1]} \frac{1}{\varepsilon}\left[2\|X(s)\| + \|\dot{X}(s)P(s)\|\right],$$

then $\varepsilon_{AP} \leq \varepsilon$.

This version of the lemma is actually a special case of the statement proved by Avron and Elgart, adapted to the case of continuous-time quantum computation. For completeness we reproduce a self-contained proof of this version of the lemma in Appendix A.

3 Adversary lower bound in the continuous-time model

In this section we give a direct proof that the adversary method $\text{Adv}^\star(\rho, \sigma)$ is a lower-bound for the zero-error quantum query complexity in the continuous-time model.

▶ **Theorem 20.** *For any $|\mathbb{X}|$-by-$|\mathbb{X}|$ Gram matrices ρ, σ, we have*

$$Q_0^{\text{ct}}(\rho, \sigma) \geq \frac{1}{2}\text{Adv}^\star(\rho, \sigma),$$

$$Q_\varepsilon^{\text{ct}}(\rho, \sigma) \geq \frac{1}{2} \min_{\sigma' : \mathcal{F}_H(\sigma, \sigma') \geq \sqrt{1-\epsilon}} \text{Adv}^\star(\rho, \sigma').$$

Proof. Let $|\phi_x(t)\rangle$ be the state of the algorithm on input x at time $t \in [0, T]$, and Φ_t be the Gram matrix of those states. Let Γ be a $|\mathbb{X}|$-by-$|\mathbb{X}|$ hermitian matrix and $|v\rangle$ be a $|\mathbb{X}|$-dimensional unit vector. We consider the following superposition of states:

$$|\Phi_t\rangle = \sum_x v_x \, |x\rangle_{\mathcal{I}} \, |\phi_x(t)\rangle_{\mathcal{A}} \qquad \text{with} \qquad \mathrm{tr}_{\mathcal{A}} \, |\Phi_t\rangle\langle\Phi_t| = \Phi_t \circ |v\rangle\langle v|,$$

where $\mathcal{A}$ is the actual register of the algorithm, while $\mathcal{I}$ is a (virtual) input register that is introduced for the sake of analysis.

Since each state $|\phi_x(t)\rangle$ evolves under the influence of a Hamiltonian $H_x(t)$ as in Equation (4), the state $|\Phi_t\rangle$ evolves under the influence of a global Hamiltonian

$$H(t) = \sum_x |x\rangle\langle x| \otimes H_x(t). \tag{10}$$

Similarly to Subsection 2.3, we consider a progress function

$$\begin{aligned} W(\Phi_t) &= \langle \Gamma \circ |v\rangle\langle v| \, , \Phi_t \rangle \\ &= \mathrm{tr}_{\mathcal{I}} \left[\Gamma (\Phi_t \circ |v\rangle\langle v|) \right] \\ &= \langle \Phi_t | \, \Gamma \otimes \mathbb{1}_{\mathcal{A}} \, |\Phi_t\rangle \\ &\equiv \langle \Gamma \rangle_t \end{aligned}$$

where we use the usual notation $\langle\Gamma\rangle_t$ for the expectation value of observable Γ when measuring state $|\Phi_t\rangle$. From Ehrenfest's theorem [12], this expectation value evolves as

$$\frac{d\,\langle\Gamma\rangle_t}{dt} = -i \, \langle [\Gamma, H(t)] \rangle_t + \left\langle \frac{\partial \Gamma}{\partial t} \right\rangle_t ,$$

where the second term is zero since Γ is time-independent. Therefore, we have

$$\begin{aligned} \frac{dW(\Phi_t)}{dt} &= -i \, \langle \Phi_t | \, [\Gamma, H(t)] \, |\Phi_t\rangle \\ &= -i \sum_{x,y} v_x v_y^* \Gamma_{yx} \, \langle \phi_y(t) | \, H_x(t) - H_y(t) \, |\phi_x(t)\rangle \\ &= -i\alpha(t) \sum_{x,y} v_x v_y^* \Gamma_{yx} \sum_{j : x_j \neq y_j} \langle \phi_y(t) | \, |j\rangle\langle j| \otimes [h(x_j) - h(y_j)] \, |\phi_x(t)\rangle \\ &= -i\alpha(t) \sum_j \sum_{x,y} (1 - \delta_{x_j y_j}) v_x v_y^* \Gamma_{yx} [\Phi_t^j]_{yx} \\ &= -i\alpha(t) \sum_j \left\langle \Gamma \circ \Delta_j , \Phi_t^j \circ |v\rangle\langle v| \right\rangle , \end{aligned}$$

where we have defined the matrices $[\Phi_t^j]_{yx} = \langle \phi_y(t) | \, |j\rangle\langle j| \otimes [h(x_j) - h(y_j)] |\phi_x(t)\rangle$. Using the properties of the inner product and the fact that $|\alpha(t)| \leq 1$, we may bound the variation of the progress function as

$$\begin{aligned} \left| \frac{dW(\Phi_t)}{dt} \right| &\leq \left| \sum_j \left\langle \Gamma \circ \Delta_j , \Phi_t^j \circ |v\rangle\langle v| \right\rangle \right| \\ &\leq \sum_j \|\Gamma \circ \Delta_j\| . \|\Phi_t^j \circ |v\rangle\langle v|\|_{\mathrm{tr}}, \\ &\leq \sum_j \|\Gamma \circ \Delta_j\| . \gamma_2(\Phi_t^j), \\ &\leq \max_j \|\Gamma \circ \Delta_j\| \cdot \left[\sum_j \gamma_2(\Phi_t^j) \right]. \end{aligned}$$

We now show that $\sum_j \gamma_2(\Phi_t^j) \leq 2$. First, as $\{|j\rangle\langle j|\}_{j\in[n]}$ is a set of orthogonal projectors defined from the orthogonal basis $\{|j\rangle\}_{j\in[n]}$, we have $\sum_j \gamma_2(\Phi_t^j) = \gamma_2(\sum_j \Phi_t^j)$.

Using the minimization form in Definition 3, we show that there exist $\{|u_x\rangle, |v_x\rangle\}_x$ such that $\sum_j \left[\Phi_t^j\right]_{yx} = \langle u_y|\, v_x\rangle$ and $\max_x \left\{ \max\{\| |v_x\rangle \|^2, \| |u_x\rangle \|^2\}\right\} \leq 2$. Indeed, let

$$|u_x\rangle = -H_{\mathcal{Q}}(x)\,|\phi_x(t)\rangle\,|0\rangle + |\phi_x(t)\rangle\,|1\rangle\,, \qquad |v_x\rangle = |\phi_x(t)\rangle\,|0\rangle + H_{\mathcal{Q}}(x)\,|\phi_x(t)\rangle\,|1\rangle\,.$$

Then, we have $\langle u_y|\, v_x\rangle = \sum_j [\Phi_t^j]_{yx}$, and the upper-bound on the norms of these vectors follows from the conditions $\|h(y)\| \leq 1$ for all y, which imply $\|H_{\mathcal{Q}}(x)\| \leq 1$ for all x.

Since $\sum_j \gamma_2(\Phi_t^j) \leq 2$, the last bound then reduces to

$$\left|\frac{dW(\Phi_t)}{dt}\right| \leq 2\max_j \|\Gamma \circ \Delta_j\|.$$

Moreover, for a zero-error algorithm, we also have

$$\begin{aligned}
\big|\,\langle \Gamma \circ (\sigma - \rho), vv^*\rangle\,\big| &= \big|W(\Phi_T) - W(\Phi_0)\big| \\
&= \left|\int_0^T \frac{dW(\Phi_t)}{dt}\right| \\
&\leq T \max_{t\in[0,T]} \left|\frac{dW(\Phi_t)}{dt}\right| \\
&\leq 2T \max_j \|\Gamma \circ \Delta_j\|.
\end{aligned}$$

By optimizing over Γ and $|v\rangle$, we obtain the zero-error adversary bound $T \geq \frac{1}{2}\mathrm{Adv}^\star(\rho,\sigma)$, which proves the first part of the theorem. The second part then directly follows from Lemma 12. ◀

4 Adiabatic quantum query algorithm

In this section, we build an adiabatic quantum query algorithm **AdiaConvert**$(\rho, \sigma, \varepsilon)$, for solving the quantum state conversion problem (ρ, σ), with an error ε and a running time $\tau = O(\mathrm{Adv}^\star(\rho,\sigma)/\varepsilon)$. Together with Theorem 20, this implies that the adversary method characterizes the quantum query complexity in the time-continuous model for bounded error.

▶ **Theorem 21.** *For any* $|\mathbb{X}|$*-by-*$|\mathbb{X}|$ *Gram matrices* ρ, σ*, we have*

$$Q_\varepsilon^{\mathrm{ct}}(\rho,\sigma) = O\Big(\frac{\mathrm{Adv}^\star(\rho,\sigma)}{\varepsilon}\Big).$$

Description of AdiaConvert

The algorithm acts on a Hilbert space $\mathcal{H} = \mathcal{H}_{\mathcal{O}} \oplus \mathcal{H}_{\mathcal{Q}} \otimes \mathcal{H}_{\mathcal{W}}$ where $\mathcal{H}_{\mathcal{O}}$ is the output register, $\mathcal{H}_{\mathcal{Q}}$ the query register and $\mathcal{H}_{\mathcal{W}}$ a workspace register. Without loss of generality, we can make the initial and target states orthogonal by adding an ancilla qubit in state $|0\rangle$ for $|\rho_x\rangle$ and $|1\rangle$ for $|\sigma_x\rangle$. We then define a continuous path from $|\rho_x\rangle\,|0\rangle$ to $|\sigma_x\rangle\,|1\rangle$:

$$\begin{aligned}
\left|k_x^+(s)\right\rangle_{\mathcal{O}} &= \cos\theta(s)\,|0,\rho_x\rangle_{\mathcal{O}} + \sin\theta(s)\,|1,\sigma_x\rangle_{\mathcal{O}}\,, \\
\left|k_x^-(s)\right\rangle_{\mathcal{O}} &= -\sin\theta(s)\,|0,\rho_x\rangle_{\mathcal{O}} + \cos\theta(s)\,|1,\sigma_x\rangle_{\mathcal{O}}\,,
\end{aligned}$$

where $\theta(s) = \frac{\pi}{2}s$ and $s \in [0,1]$.

From Definition 14, let $\left\{ |u_{x,i}\rangle , |v_{x,i}\rangle \right\}_{x,i}$ be vectors witnessing $\gamma_2(\rho - \sigma|\Delta) = W$, with $W \overset{\text{def}}{=} \mathrm{Adv}^{\star}(\rho, \sigma)$. We use those states to define the following non-normalized states:

$$\left|\Psi_x^+(s,\varepsilon)\right\rangle = \left|k_x^+(s)\right\rangle_{\mathcal{O}} + \frac{\varepsilon}{\sqrt{W}} \sum_i \left|i, x_i^+\right\rangle_{\mathcal{Q}} |u_{x,i}\rangle_{\mathcal{W}} ,$$

$$\left|\Psi_x^-(s,\varepsilon)\right\rangle = \left|k_x^-(s)\right\rangle_{\mathcal{O}} + \xi(s)\frac{\sqrt{W}}{\varepsilon} \sum_i \left|i, x_i^-\right\rangle_{\mathcal{Q}} |v_{x,i}\rangle_{\mathcal{W}} ,$$

where $\left|x_i^{\pm}\right\rangle$ is defined by (3), and $\xi(s) = 2\cos\theta(s)\sin\theta(s)$. Note that we have $\left\langle x_i^- \middle| y_i^+ \right\rangle = \frac{1}{2}\left[1 - \delta_{x_i,y_i}\right]$. We also let $|\psi_x^{\pm}(s,\varepsilon)\rangle$ be their normalized versions.

The algorithm uses as driver Hamiltonian the projection $\Lambda(s,\varepsilon)$ on the vector space $V(s,\varepsilon) = \mathrm{span}\{|\Psi_x^-(s,\varepsilon)\rangle \,|x \in \mathbb{X}\}$, and as oracle Hamiltonian, $\Pi_x = \sum_i |i, x_i^-\rangle\langle i, x_i^-|_{\mathcal{Q}} \otimes \mathbb{1}_{\mathcal{W}}$ (note that $\|\Pi_x\| \leq 1$).

```
**AdiaConvert**$(\rho, \sigma, \varepsilon)$
1 Prepare the state $|0, \rho_x\rangle$.
2 If $\mathrm{Adv}^{\star}(\rho,\sigma) < \varepsilon/2$, do nothing.
3 Otherwise apply the Hamiltonian $H_x(s,\varepsilon) = \Lambda(s,\varepsilon) - \Pi_x$,
    where $s = t/\tau$ and $\tau = 15\frac{\mathrm{Adv}^{\star}(\rho,\sigma)}{\varepsilon^2}$, from $t = 0$ to $t = \tau$.
```

The action of the algorithm is simple, first, if $\mathrm{Adv}^{\star}(\rho, \sigma) < \varepsilon/2$, then we claim, using Proposition 15 and Corollary 9, that ρ and σ are closed enough, and satisfies the coherent output condition given in Definition 11.

Otherwise, in order to convert the initial state $|0, \rho_x\rangle$ into a state close enough to the target state $|1, \sigma_x\rangle$, we consider the state $|\psi_x^+(s,\varepsilon)\rangle$, which is ε-distant to the state $|k_x^+(s)\rangle$ interpolating between the initial and target state. We then use the adiabatic process $\{H_x(s,\varepsilon), P_x(s,\varepsilon), \tau\}$ with failure ε, where $P_x(s,\varepsilon)$ is the rank-1 orthogonal projection on the state $|\psi_x^+(s,\varepsilon)\rangle$. The correctness of the adiabatic evolution is based on Lemma 19, where the solution of Equation (9) follows from Item 5 in Proposition 22. Therefore the final state is 3ε-distant from the target state since the algorithm incurs error ε at the initial state, during the adiabatic process, and at the target state. This implies that we solve the quantum state generation problem with error at most $9\varepsilon^2$, and in turn that $Q^{\mathrm{ct}}_{9\varepsilon^2}(\rho,\sigma) \leq 15\mathrm{Adv}^{\star}(\rho,\sigma)/\varepsilon^2$.

The proof of Theorem 21 is the consequence of the existence of the optimal quantum query algorithm **AdiaConvert**. As the number of query involved are given by the time scale τ, the demonstration relies on the derivation of an adiabatic bound linear in $\mathrm{Adv}^{\star}$.

In order to prove Theorem 21, we first derive several useful properties of the algorithm **AdiaConvert**.

▶ **Proposition 22.** *For any $s, \varepsilon \in [0,1]$ and for all $x \in \mathbb{X}$*

1. $N_x(\varepsilon) \overset{\text{def}}{=} \|\,|\Psi_x^+(s,\varepsilon)\rangle\,\| \leq 1 + \varepsilon^2/2,$
2. $|k_x^+(s)\rangle$ *and* $|\psi_x^+(s,\varepsilon)\rangle$ *are ε-distant,*
3. $\Lambda(s,\varepsilon)\,|\psi_x^+(s,\varepsilon)\rangle = 0,$
4. $|\psi_x^+(s,\varepsilon)\rangle$ *is an eigenvector of $H_x(s,\varepsilon)$ with eigenvalue $\lambda_x(s,\varepsilon) = 0$,*
5. $\langle\psi_x^+(s,\varepsilon)|\left(\partial_s\,|\psi_x^+(s,\varepsilon)\rangle\right) = 0,$
6. $\partial_s\,|\Psi_x^+(s,\varepsilon)\rangle = \frac{\pi}{2}H_x(s,\varepsilon)\,|\Psi_x^-(s,\varepsilon)\rangle\,,$
7. $\|\,|\Psi_x^-(s,\varepsilon)\rangle\,\|^2 \leq 1 + W^2/\varepsilon^2.$

Let us note that Item **5** is the key property that prevents the instantaneous state $|\psi_x^+(s,\varepsilon)\rangle$ from leaking to degenerate subspaces of eigenvalue 0.

Proof.

1. By Definition 4, we have $\sum_i \| \, |u_{x,i}\rangle \, \|^2 \leq \gamma_2(\rho - \sigma|\Delta) = W$, so that
$$N_x^2(\varepsilon) = \Big\| \, \big|\Psi_x^+(s,\varepsilon)\big\rangle \, \Big\|^2 = 1 + \frac{\varepsilon^2}{W}\sum_i \Big\| \, |u_{x,i}\rangle \, \Big\|^2 \leq 1 + \varepsilon^2.$$
Item **1** then follows from the inequality $\sqrt{1+\delta} \leq 1 + \delta/2$, for $\delta \in [0,1]$.
2. The scalar product of these vectors gives
$$\big\langle \psi_x^+(s,\varepsilon)\big| \, k_x^+(s)\big\rangle = \frac{1}{N_x(\varepsilon)}\big\langle \Psi_x^+(s,\varepsilon)\big| \, k_x^+(s)\big\rangle = \frac{1}{N_x(\varepsilon)} \geq 1 - \varepsilon^2/2.$$
Since this scalar product is real, we have
$$\big\| |k_x^+(s)\rangle - \big|\psi_x^+(s,\varepsilon)\big\rangle \big\|^2 = 2 - 2\big\langle \psi_x^+(s,\varepsilon)\big| \, k_x^+(s)\big\rangle \leq \varepsilon^2.$$
3. Remember $\Lambda(s,\varepsilon)$ is the projection on subspace $V(s,\varepsilon) = \mathrm{span}\{|\Psi_x^-(s,\varepsilon)\rangle \, | x \in \mathbb{X}\}$. Therefore, it suffices to show that for all $x, y \in \mathbb{X}$, $\big\langle \Psi_x^+(s,\varepsilon)\big| \, \Psi_y^-(s,\varepsilon)\big\rangle = 0$. By definition of $|\Psi_x^+(s,\varepsilon)\rangle$ and $|\Psi_x^-(s,\varepsilon)\rangle$, we have
$$\big\langle \Psi_x^+(s,\varepsilon)\big| \, \Psi_y^-(s,\varepsilon)\big\rangle = -\cos\theta(s)\sin\theta(s)\big[\rho_{x,y} - \sigma_{x,y} - \sum_{j:x_j \neq y_j} \langle u_{x,j}| \, v_{y,j}\rangle\big].$$
The right hand side is then zero due to the properties of $\big\{ \, |u_{x,i}\rangle \, , |v_{x,i}\rangle \, \big\}_{x,i}$ in Definition 14.
4. From Item **3** we already know that $\Lambda(s,\varepsilon)\,|\psi_x^+(s,\varepsilon)\rangle = 0$. Then by the definition of $H_x(s,\varepsilon)$, we must calculate $\Pi_x\,|\psi_x^+(s,\varepsilon)\rangle$,
$$\Pi_y\,\big|\psi_x^+(s,\varepsilon)\big\rangle \propto \sum_i [1 - \delta_{x_i,y_i}]\,\big|i, x_i^+, u_{x,i}\big\rangle\,,$$
which is exactly zero for $x = y$.
5. The property follows from
$$\partial_s\,\big|\psi_x^+(s,\varepsilon)\big\rangle = \frac{1}{N_x(\varepsilon)}\partial_s\,\big|\Psi_x^+(s,\varepsilon)\big\rangle = \frac{\pi}{2N_x(\varepsilon)}\,\big|k_x^-(s)\big\rangle$$
and the fact that $\langle\psi_x^+(s,\varepsilon)| \, k_x^-(s)\rangle \propto \langle k_x^+(s)| \, k_x^-(s)\rangle = 0$.
6. $$\begin{aligned}\partial_s\,\big|\Psi_x^+(s,\varepsilon)\big\rangle &= \frac{\pi}{2}\,\big|k_x^-(s)\big\rangle \\ &= \frac{\pi}{2}\Big(\mathbb{1} - \Pi_x\Big)\,\big|\Psi_x^-(s,\varepsilon)\big\rangle \\ &= \frac{\pi}{2}\Big[\Big(\Lambda(s,\varepsilon) - \Pi_x\Big) + \Big(\mathbb{1} - \Lambda(s,\varepsilon)\Big)\Big]\,\big|\Psi_x^-(s,\varepsilon)\big\rangle \\ &= \frac{\pi}{2}H_x(s,\varepsilon)\,\big|\Psi_x^-(s,\varepsilon)\big\rangle\,.\end{aligned}$$
In the second line, Π_x acts as the identity on $\big|i, x_i^-\big\rangle$. In the third line, the second term is zero by definition of $\Lambda(s,\varepsilon)$.
7. Similarly to the proof of Item **1** all vectors $|v_{x,i}\rangle$ have their norm bounded by W
$$\Big\| \, |\Psi_x^-(s,\varepsilon)\rangle \, \Big\|^2 = 1 + \xi^2(s)\frac{W}{\varepsilon^2}\sum_i \Big\| \, |v_{x,i}\rangle \, \Big\|^2 \leq 1 + \frac{W^2}{\varepsilon^2}.$$
Noting that $\xi(s) = \sin(2\theta(s))$. ◀

Proof of Theorem 21. Let $W = \mathrm{Adv}^{\star}(\rho,\sigma)$. We show that **AdiaConvert** solves the quantum state conversion in time $\tau = 15\frac{W}{\varepsilon^2}$ with error at most $9\varepsilon^2$. Let us first consider the case where $W < \varepsilon/2$. Then, Proposition 15 implies $\mathcal{D}_H(\rho,\sigma) < \varepsilon/2$, and Corollary 9 concludes that $\mathcal{F}_H(\rho,\sigma) > 1-\varepsilon/2 > \sqrt{1-\varepsilon}$, so that the coherent output condition is already satisfied by the initial Gram matrix.

We now assume that $W \geq \varepsilon/2$. Before we go any further, we must justify that the triplet $\{H_x(s,\varepsilon),\, P_x(s,\varepsilon), \tau\}$ is an adiabatic process as defined in Definition 16. First by definition, the state $|\psi_x^{\pm}(s,\varepsilon)\rangle$ is s-smooth on $[0,1]$. It follows that $H_x(s,\varepsilon)$ and $P_x(s,\varepsilon)$ are also s-smooth. Moreover, by Item **4** of Proposition 22, $|\psi_x^{+}(s,\varepsilon)\rangle$ is an eigenstate of $H_x(s,\varepsilon)$ with a constant eigenvalue $\lambda_x(s,\varepsilon) = 0$.

In order to bound the error of the adiabatic process ε_{AP} with Lemma 19, we define an operator $X_x(s,\varepsilon)$, solution of Equation (9), where $X_x(s,\varepsilon)$ and $\dot{X}_x(s,\varepsilon)P_x(s,\varepsilon)$ are bounded.

Let $X_x(s,\varepsilon) = \frac{\pi}{2N_x(\varepsilon)} \left|\Psi_x^{-}(s,\varepsilon)\right\rangle\!\left\langle\psi_x^{+}(s,\varepsilon)\right|$, Items **5** and **6** of Proposition 22 imply

$$[H_x(s,\varepsilon), X_x(s,\varepsilon)] = H_x(s,\varepsilon)X_x(s,\varepsilon) = \dot{P}_x(s,\varepsilon)P_x(s,\varepsilon).$$

To obtain ε_{AP} we derive a bound for $X_x(s,\varepsilon)$ and $\dot{X}_x(s,\varepsilon)P_x(s,\varepsilon)$.

First, we have

$$\|X_x(s,\varepsilon)\|^2 = \left[\frac{\pi}{2N_x(\varepsilon)}\right]^2 \left\| \left|\Psi_x^{-}(s,\varepsilon)\right\rangle \right\|^2.$$

From Item **7** of Proposition 22 and the fact that $W \geq \varepsilon/2$, we obtain

$$\| \left|\Psi_x^{-}(s,\varepsilon)\right\rangle \|^2 \leq 1 + \frac{W^2}{\varepsilon^2} \leq 5\frac{W^2}{\varepsilon^2},$$

knowing that $N_x(\varepsilon) \geq 1$ we obtain the bound : $\|X_x(s,\varepsilon)\| \leq \frac{\pi\sqrt{5}}{2}\frac{W}{\varepsilon}$.

Second, to bound $\|\dot{X}_x(s,\varepsilon)P_x(s,\varepsilon)\|$ we derive $X_x(s,\varepsilon)$

$$\dot{X}_x(s,\varepsilon) = \frac{\pi}{2N_x(\varepsilon)}\partial_s\big(\left|\Psi_x^{-}(s,\varepsilon)\right\rangle\big)\left\langle\psi_x^{+}(s,\varepsilon)\right| + \frac{\pi^2}{4N_x(\varepsilon)}\left|\Psi_x^{-}(s,\varepsilon)\right\rangle\!\left\langle k_x^{-}(s)\right|.$$

After adding $P_x(s,\varepsilon)$ on the right, the second term disappears following Item **5** of Proposition 22, and we have

$$\begin{aligned}
\|\dot{X}_x(s,\varepsilon)P_x(s,\varepsilon)\|^2 &= \left[\frac{\pi}{2N_x(\varepsilon)}\right]^2 \left\|\partial_s \left|\Psi_x^{-}(s,\varepsilon)\right\rangle\right\|^2 \\
&\leq \left[\frac{\pi}{2}\right]^2 \left(\frac{\pi^2}{4} + \pi^2\cos^2(\pi s)\frac{W}{\varepsilon^2}\sum_i \| \left|v_{x,i}\right\rangle \|^2\right) \\
&\leq \left[\frac{\pi}{2}\right]^2 \pi^2 \left(\frac{1}{4} + \frac{W^2}{\varepsilon^2}\right) \\
&\leq \left[\frac{\pi}{2}\right]^2 2\pi^2 \frac{W^2}{\varepsilon^2}.
\end{aligned}$$

Thereby we have all the required conditions to use Lemma 19 for the adiabatic process $\{H_x(s,\varepsilon), P_x(s,\varepsilon), \tau\}$, which ensures that $\varepsilon_{AP} \leq \varepsilon$ if

$$\tau \geq \frac{15W}{\varepsilon^2} \geq \frac{1}{\varepsilon}\left[\frac{W}{\varepsilon}\left(\pi\sqrt{5} + \frac{\pi^2}{\sqrt{2}}\right)\right].$$

Let $\left|\psi_x^{f}\right\rangle$ be the output state. Since the initial state $|0,\rho_x\rangle$ and the target state $|1,\sigma_x\rangle$ are ε-distant from $|\psi_x^{+}(0,\varepsilon)\rangle$ and $|\psi_x^{+}(1,\varepsilon)\rangle$ (Item **2** of Proposition 22) and the adiabatic process introduces an additional error of $\varepsilon_{AB} \leq \varepsilon$, the output state $\left|\psi_x^f\right\rangle$ and the target state $|1, \sigma_x\rangle$ are 3ε-distant, which implies that $\mathrm{Re}(\left\langle\psi_x^f\right| 1, \sigma_x\rangle) \geq \sqrt{1-9\varepsilon^2}$. Therefore, we obtain

$$Q^{\mathrm{ct}}_{9\varepsilon^2}(\rho, \sigma) \leq 15\frac{W}{\varepsilon^2},$$

which implies the theorem by setting $\varepsilon' = 9\varepsilon^2$. ◀

Acknowledgements. This work was supported by the Belgian ARC project COPHYMA and the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n. 600700 (QALGO).

References

1 Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, and Seth Lloyd. Adiabatic quantum computation is equivalent to standard quantum computation. In *Proceedings of the 45th Annual Symposium on the Foundations of Computer Science*, pages 42–51, New York, 2004. IEEE Computer Society Press.

2 Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

3 J. E. Avron, R. Seiler, and L. G. Yaffe. Adiabatic theorems and applications to the quantum Hall effect. *Communications in Mathematical Physics*, 110(1):33–49, March 1987.

4 Joseph E. Avron and Alexander Elgart. Adiabatic Theorem without a Gap Condition. *Communications in Mathematical Physics*, 203(2):445–463, June 1999.

5 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48:778–797, 2001.

6 M. Born and V. Fock. Beweis des adiabatensatzes. *Zeitschrift für Physik*, 51(3-4):165–180, 1928.

7 Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288(1):21–43, 2002.

8 Andrew Childs and Jeffrey Goldstone. Spatial search by quantum walk. *Physical Review A*, 70(2):022314, August 2004.

9 Andrew M. Childs. On the Relationship Between Continuous- and Discrete-Time Quantum Walk. *Communications in Mathematical Physics*, 294(2):581–603, October 2009.

10 Andrew M. Childs and Jeffrey Goldstone. Spatial search and the Dirac equation. *Physical Review A*, 70(4):042312, October 2004.

11 Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando D. Somma, and David Yonge-Mallo. Efficient discrete-time simulations of continuous-time quantum query algorithms. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 409–416. ACM, 2009.

12 P. Ehrenfest. Bemerkung über die angenäherte Gültigkeit der klassischen Mechanik innerhalb der Quantenmechanik. *Zeitschrift fur Physik*, 45:455–457, 1927.

13 Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum algorithm for the Hamiltonian NAND tree. *Theory of Computing*, 4:169–190, 2008.

14 Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. arXiv:0001106, 2000.

15 Edward Farhi and Sam Gutmann. An analog analogue of a digital quantum computation. arXiv:9612026, 1996.

16 Iain Foulger, Sven Gnutzmann, and Gregor Tanner. Quantum Search on Graphene Lattices. *Physical Review Letters*, 112(7):070504, February 2014.

17 Christopher A. Fuchs and Jeroen van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. In *IEEE Transactions on Information Theory*, volume 45, pages 1216–1227, 1999.

18 Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 526–535. ACM, 2007.

19 S. Jansen, M.-B. Ruskai, and R. Seiler. Bounds for the adiabatic approximation with applications to quantum computation. *J. Math. Phys.*, 48(10):102111, 2007.

20 Tosio Kato. On the Adiabatic Theorem of Quantum Mechanics. *Journal of the Physical Society of Japan*, 5(6):435–439, November 1950.

21 Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 344–353. IEEE Computer Society, 2011.

22 Troy Lee and Jérémie Roland. A strong direct product theorem for quantum query complexity. *Computational Complexity*, 22(2):429–462, 2013.

23 Carlos Mochon. Hamiltonian oracles. *Physical Review A – Atomic, Molecular, and Optical Physics*, 75(4), 2007.

24 M. Reed and B. Simon. *Methods of modern mathematical physics. 2. Fourier analysis, self-adjointness.* Fourier Analysis, Self-adjointness. Academic Press, 1975.

25 Ben Reichardt and Robert Špalek. Span-program-based quantum algorithm for evaluating formulas. *Theory of Computing*, 8(13):291–319, 2012.

26 Ben W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 544–551. IEEE Computer Society, 2009.

27 Ben W. Reichardt. Reflections for quantum query algorithms. In *Proceedings of the 22nd ACM-SIAM Symposium on Discrete Algorithms*, pages 560–569, 2011.

28 Jérémie Roland and Nicolas J. Cerf. Quantum search by local adiabatic evolution. *Physical Review A*, 65:042308, 2002.

29 W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? *Proceedings 2001 IEEE International Conference on Cluster Computing*, pages 279–287, 2002.

30 David Yonge-Mallo. Adversary lower bounds in the Hamiltonian oracle model. arXiv:1108.2479, 2011.

A Appendix: Adiabatic theorem without a gap condition

In this section we give an adapted version of the proof of Lemma 19 in [4]. We derive an upper bound on the error ε_{AP} caused by the adiabatic process without a gap condition. We use the same notations as in Subsection 2.4.

▶ **Lemma 23** ([4]). *Let $\{H(s), P(s), \tau\}$ be an adiabatic process and $\varepsilon > 0$. Suppose that the commutator equation*

$$\dot{P}(s)P(s) = [H(s), X(s)] \tag{11}$$

accepts as solution operator $X(s)$ such that both $X(s)$ and $\dot{X}(s)$ are bounded. If

$$\tau \geq \max_{s\in[0,1]} \frac{1}{\varepsilon}\Big[2\|X(s)\| + \|\dot{X}(s)P(s)\|\Big],$$

then $\varepsilon_{AP} \leq \varepsilon$.

Proof of Lemma 19

In order to bound the quantity ε_{AP}, we would like to describe an idealized adiabatic evolution $U_A(s)$ that transports the projector $P(0)$ to $P(s)$, such that $U_A(s)P(0) = P(s)U_A(s)$. To achieve this, we use a technique given by [20] (later improved in [3]), and define $H_A(s)$ as the *adiabatic Hamiltonian*

$$H_A(s) = \lambda(s)\mathbb{1} + \frac{i}{\tau}[\dot{P}(s), P(s)], \tag{12}$$

where $[\cdot,\cdot]$ is the commutator. We define $U_A(s)$ as the solution of the Schrödinger equation for this Hamiltonian, that is,

$$i\partial_s U_A(s) = \tau H_A(s)U_A(s), \tag{13}$$

with the initial condition $U_A(0) = \mathbb{1}$. The existence and uniqueness of $U_A(s)$ follows from the analytical properties in Definition 16. Moreover we show that $U_A(s)$ has the desired property.

▶ **Lemma 24** ([20], Intertwining property)**.**

$$U_A(s)P(0) = P(s)U_A(s). \tag{14}$$

The proof of this property uses the following fact.

▶ **Fact 25.** *For any orthogonal projector P we have $P = P^2$, so that $\dot{P} = \dot{P}P + P\dot{P}$ and $P\dot{P}P = 0$.*

Proof of Lemma 24. Since $U_A(s)$ is the solution of the differential equation $i\partial_s X(s) = \tau H_A(s)X(s)$ with $X(0) = \mathbb{1}$, then every other solution of this equation has the form $X(s) = U_A(s)X(0)$. All we need to do is prove that $P(s)U_A(s)$ is also a solution. Indeed, this implies that $P(s)U_A(s) = U_A(s)X(0)$, and by setting $s = 0$ we obtain $P(0) = X(0)$. Using Fact 25, we have

$$\begin{aligned}
i\partial_s\big(P(s)U_A(s)\big) &= i\dot{P}(s)U_A(s) + P(s)\tau H_A(s)U_A(s)\\
&= i\dot{P}(s)U_A(s) + \tau\lambda(s)P(s)U_A(s) + iP(s)[\dot{P}(s), P(s)]U_A(s)\\
&= \tau\lambda(s)P(s)U_A(s) + i\big(\dot{P}(s) - P(s)\dot{P}(s)\big)U_A(s)\\
&= \tau\lambda(s)P(s)U_A(s) + i\dot{P}(s)P(s)U_A(s)\\
&= \big(\tau\lambda(s)\mathbb{1} + i[\dot{P}(s), P(s)]\big)P(s)U_A(s)\\
&= \tau H_A(s)P(s)U_A(s)
\end{aligned}$$

◀

In order to prove Lemma 19, we need two more claims.
Note that $\varepsilon_{AP}(s)$ can be rewritten as $\|\big(\Omega(s) - \mathbb{1}\big)P(0)\|$, where $\Omega(s) = U_\tau^*(s)U_A(s)$.

▶ **Claim 26.** $\dot{\Omega}(s)P(0) = U_\tau^*(s)\dot{P}(s)U_A(s)P(0)$

Proof. Using (7) and (12), we note that $\dot{\Omega}(s) = U_\tau^*(s)\Big[i\tau\big(H(s)-\lambda(s)\mathbb{1}\big)+[\dot{P}(s), P(s)]\Big]U_A(s)$. The claim follows from the intertwining property (Lemma 24), Fact 25 and $H(s)P(s) = \lambda(s)P(s)$. ◀

▶ **Claim 27.** *Let $\Phi(s) = e^{-i\tau\lambda(s)}\mathbb{1}$ and $V_A(s) = \Phi^*(s)U_A(s)$. Then $V_A(s)$ satisfies the intertwining property* (14)*, that is, $V_A(s)P(0) = P(s)V_A(s)$, as well as the Schrödinger equation $\dot{V}_A(s) = [\dot{P}(s), P(s)]V_A(s)$.*

Proof. The fact that $V_A(s)$ satisfies the intertwining property is immediate since $U_A(s)$ satisfies this property and $\Phi(s)$, being proportional to the identity, commutes with any operator. The fact that it satisfies the Schrödinger equation follows from the facts that $\Phi(s)$ satisfies $i\dot{\Phi}(s) = \tau\lambda(s)\Phi(s)$, $U_A(s)$ satisfies $i\dot{U}_A(s) = \tau H_A(s)U_A(s)$, and both terms of $H_A(s) = \lambda(s)\mathbb{1} + \frac{i}{\tau}[\dot{P}(s), P(s)]$ commute. ◀

Let $X(s)$ an operator solution of $\dot{P}(s)P(s) = [H(s), X(s)]$, then

$$\begin{aligned}
&\big(\Omega(s) - \mathbb{1}\big)P(0)\\
&= \int_0^s \dot{\Omega}(s')ds'P(0)\\
&= \int_0^s U_\tau^*(s')\dot{P}(s')U_A(s')ds'P(0)\\
&= \int_0^s U_\tau^*(s')\Phi(s')\dot{P}(s')V_A(s')ds'P(0)\\
&= \int_0^s U_\tau^*(s')\Phi(s')[H(s'), X(s')]V_A(s')ds'P(0)\\
&= \int_0^s U_\tau^*(s')\Phi(s')[H(s') - \lambda(s')]X(s')V_A(s')ds'P(0)\\
&= \frac{1}{i\tau}\int_0^s \partial_{s'}[U_\tau^*(s')\Phi(s')]X(s')V_A(s')ds'P(0)\\
&= \frac{1}{i\tau}\Big[U_\tau^*(s')\Phi(s')X(s')V_A(s')\Big]_0^s P(0) - \frac{1}{i\tau}\int_0^s U_\tau^*(s')\Phi(s')\partial_{s'}[X(s')V_A(s')]ds'P(0)\\
&= \frac{1}{i\tau}\Big[U_\tau^*(s')X(s')U_A(s')\Big]_0^s P(0) - \frac{1}{i\tau}\int_0^s U_\tau^*(s')[\dot{X}(s') + X(s')\dot{P}(s')]U_A(s')ds'P(0)
\end{aligned}$$

We explain line by line:

(1 → 2) We use Claim 26.

(2 → 3) We rearrange the expression using $U_A(s) = \Phi(s)V_A(s)$ and the fact that $\Phi(s)$ commutes with any operator.

(3 → 4) We use the intertwining property for $V_A(s)$ (Claim 27) and Equation (11).

(6 → 7) We integrate by parts.

The third term in the last line is null, because $X(s) = X(s)P(s)$ and the intertwining property (Lemma 24) yields the expression $P\dot{P}P$, which is zero by Fact 25. Using the triangle inequality, the fact that a norm is preserved by unitary operations and can only decrease under projections, we finally have

$$\begin{aligned}
\varepsilon_{AP}(s) &= \|\big(\Omega(s) - \mathbb{1}\big)P(0)\|\\
&\le \frac{1}{\tau}\Big[\|X(0)\| + \|X(s)\| + s \max_{s'\in[0,s]} \|\dot{X}(s')P(s')\|\Big]\\
&\le \frac{1}{\tau}\max_{s\in[0,1]}\Big[2\|X(s)\| + \|\dot{X}(s)P(s)\|\Big]
\end{aligned}$$

This conclude the proof. ◀

Quantum Enhancement of Randomness Distribution

Raul Garcia-Patron[1], William Matthews[2], and Andreas Winter[3]

1 **Quantum Information and Communication**
Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
rgarciap@ulb.ac.be

2 **Department of Applied Mathematics and Theoretical Physics**
University of Cambridge, Cambridge CB3 0WA, U.K.
wm266@statslab.cam.ac.uk

3 **ICREA & Física Teòrica: Informació i Fenòmens Quàntics,**
Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain
andreas.winter@uab.cat

Abstract

The capability of a given channel to transmit information is, a priori, distinct from its capability to distribute random correlations. Despite that, for classical channels, the capacity to distribute information and randomness turns out to be the same, even with the assistance of auxiliary communication. In this work we show that this is no longer true for quantum channels when feedback is allowed. We prove this by constructing a channel that is noisy for the transmission of information but behaves as a virtual noiseless channel for randomness distribution when assisted by feedback communication. Our result can be seen as a way of unlocking quantum randomness internal to the channel.

1998 ACM Subject Classification E.4 Coding and Information Theory

Keywords and phrases Quantum Shannon theory, noisy channels, capacity, randomness

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.180

1 Summary

Randomness and information are different concepts. We think of information of as that which is sent as a specific message to another person or machine. On the other hand, randomness can be intuitively understood as the outcome of a noisy process. Information and randomness being different concepts, the capability to distribute them over a channel could, a priori, be inequivalent resources. More precisely, the capability to distribute a bit of randomness is a weaker resource than the potential to communicate a bit of information over a channel, because if Alice is capable of distributing a bit of information to Bob over a noisy channel she can also locally generate a pair of correlated bits and transmit one to Bob, generating a bit of shared randomness. Therefore, the capacity $R(\mathcal{E})$ of randomness distribution of a noisy channel $\mathcal{E}$ is in principle higher than that of information communication $C(\mathcal{E})$, i.e., $C(\mathcal{E}) \leq R(\mathcal{E})$.

We may also ask about the capacity of a channel to communicate or distribute randomness when auxiliary classical communication is allowed. For communication, we thus have the capacity of the channel assisted by feedback $C_{\leftarrow}$, the capacity assisted by auxiliary forward communication $C_{\rightarrow}$ and the capacity assisted by two-way classical communication $C_{\leftrightarrow}$. Since

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 180–190
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the auxiliary *forward* communication can be used to communicate by itself, we must subtract the amount of auxiliary forward communication from the gross communication rates in the definitions of the later two quantities. For the distribution of shared randomness we can similarly define rates $R_{\leftarrow}$, $R_{\rightarrow}$, $R_{\leftrightarrow}$, but in this case we must subtract both forward and backward auxiliary communication, as both of these may be used to establish shared randomness by themselves.

In the setting with feedback assistance, the tradeoff between the gross rate of randomness distribution and the rate of feedback allowed was characterised (among many other things) by Ahlswede and Csiszár in [2]. A corollary of their result is that $R_{\leftarrow}(\mathcal{E}) = C(\mathcal{E})$ for classical channels. To our knowledge the only previous work studying the generation of shared randomness in a quantum scenario was the work of Devetak and Winter [6] on the distillation of common randomness from bipartite quantum states. That work considered a static scenario of distillation of randomness from a quantum state already shared between Alice and Bob, where in this manuscript we are interested on a dynamic scenario of randomness distribution over quantum channels.

In section 3 we show that, for general quantum channels $\mathcal{E}$, the entanglement-assisted capacity [12] of $\mathcal{E}$, $C_E(\mathcal{E})$, is an upper bound on the largest of the randomness distribution capacities, $R_{\leftrightarrow}(\mathcal{E})$. Since $C_E(\mathcal{E})$ is equal to $C(\mathcal{E})$ for classical-quantum channels (which include classical channels), this establishes the equality

$$R(\mathcal{E}) = R_{\leftarrow}(\mathcal{E}) = R_{\rightarrow}(\mathcal{E}) = R_{\leftrightarrow}(\mathcal{E}) = C(\mathcal{E})$$

for such channels. A simple argument can be used to show that we also have

$$C(\mathcal{E}) = C_{\leftarrow}(\mathcal{E}) = C_{\rightarrow}(\mathcal{E}) = C_{\leftrightarrow}(\mathcal{E})$$

for such classical-quantum channels, so in this case all eight quantities are then same. When the channel is classical

$$C(\mathcal{E}) = \max_{P_X} I(X:Y), \tag{1}$$

where X and Y are the input and output to a single use of the channel $\mathcal{E}$ with X distributed according to P_X [1].

As opposed to the classical regime, where all capacities turn out to be equal, in the quantum scenario randomness distribution and communication remain equivalent only when we consider unassisted or forward assisted classical communication. That is, for general channels $\mathcal{E}$, we have $C(\mathcal{E}) = R(\mathcal{E}) = C_{\rightarrow}(\mathcal{E}) = R_{\rightarrow}(\mathcal{E})$, as shown in subsection 4.1.

In section 4.2 we show that, for quantum-classical channels $\mathcal{E}$, feedback allows the upper bound in terms of $C_E(\mathcal{E})$ to be achieved, and therefore

$$R_{\leftarrow}(\mathcal{E}) = R_{\leftrightarrow}(\mathcal{E}) = C_E(\mathcal{E}).$$

On the other hand, since quantum-classical channels are entanglement-breaking, a result of Bowen and Nagarajan [3] tells us that $C_{\leftarrow}(\mathcal{E}) = C(\mathcal{E})$, so any quantum-classical channel with $C(\mathcal{E}) < C_E(\mathcal{E})$ also demonstrates a separation $C_{\leftarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$. Holevo has shown that there are many such channels [4], and we give an explicit example, where the randomness distribution protocol is noiseless, in subsection 4.3.

2 Definitions

Our definitions in this section are based on those used by Ahlswede and Csiszár in [2], and Devetak and Winter [6].

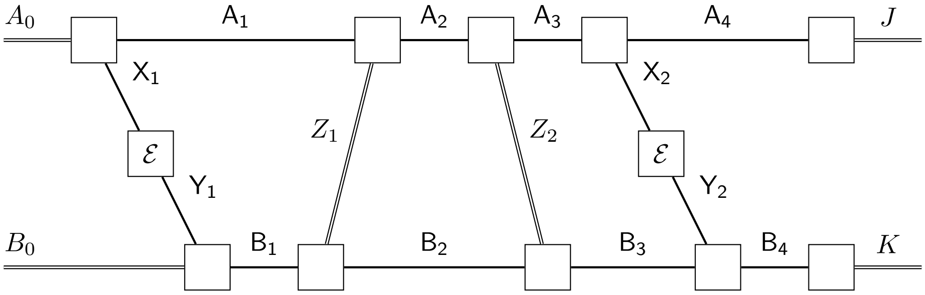


Figure 1 An example of a two-way assisted randomness distillation protocol which makes two uses of the channel $\mathcal{E}$. Time runs left to right. Classical systems are shown as double lines, quantum systems as solid lines. Empty boxes represent local processing. We denote by A_j Alice's system, and by B_j Bob's system, immediately after step j of the protocol. The communication is either forward communication via one use of the noisy channel $\mathcal{E}$, where Alice inputs X_i and Bob receives the output Y_i, or forward/backward auxiliary noiseless classical communication Z_i.

A **two-way assisted** randomness distribution protocol for a channel $\mathcal{E}$ consists of local generation of random variables A_0 and B_0 followed by a finite number of steps, each consisting of communication followed by local processing. The communication is either (i) forward communication via one use of the noisy channel $\mathcal{E}$, where Alice makes an input X_i and Bob receives the output Y_i; (ii) forward auxiliary noiseless classical communication; (iii) backward auxiliary noiseless classical communication.

Suppose we have a protocol of $n + m$ steps where n of the steps are of type (i) and the other m steps are of type (ii) or (iii). We denote by A_j Alice's system, and by B_j Bob's system, immediately after step j of the protocol. At the end of the protocol, Alice must produce random variable J and Bob must produce K, both of which take values in the same alphabet $\mathcal{A}_K$, by local processing of their respective final systems A_{m+n} and A_{m+n}. An example of such a protocol with $n = m = 2$ is illustrated in Figure 1.

We require that

$$\log|\mathcal{A}_K| \leq \exp(cn) \tag{2}$$

for some constant c independent of n (but depending on the channel $\mathcal{E}$). We say that the protocol is **ϵ-good** if $\Pr(J \neq K) \leq \epsilon$. By Fano's inequality and (2), an ϵ-good protocol has

$$H(K|J) \leq \epsilon cn + 1 \tag{3}$$

We denote the data transmitted in each instance of auxiliary communication (regardless of whether it is forward or backward) by Z_k, where $k \in \{1, \ldots, m\}$, in temporal order.

If the total auxiliary communication $Z := Z^{(m)} := (Z_1, \ldots, Z_m)$ has $|\mathcal{A}_Z|$ possible values (we require this number to be finite for any given protocol), then this alone would allow the parties to establish $\log|\mathcal{A}_Z|$ bits of perfect common randomness without using $\mathcal{E}$ at all! We therefore subtract $\log|\mathcal{A}_Z|$ from the final amount of common randomness established and hence define the **net rate** of the protocol is

$$\frac{1}{n}(H(K) - \log|\mathcal{A}_Z|).$$

A **forward-assisted** randomness distribution protocol is one in which all steps are of type (i) or (ii). A **back-assisted** randomness distribution protocol is one in which all steps are of type (i) or (iii). An **unassisted** randomness distribution protocol is one in which all steps are of type (i).

▶ **Definition 1.** We say a net rate R is achieved by two-way protocols for channel $\mathcal{E}$ if for all $\epsilon > 0$ and all sufficiently large n, there is an ϵ-good protocol for n noisy channel uses with net rate no less than R. We define $R_{\leftrightarrow}(\mathcal{E})$ to be the supremum of net rates achieved by two-way protocols; $R_{\rightarrow}(\mathcal{E})$ to be the supremum of net rates achieved by forward-assisted protocols; $R_{\leftarrow}(\mathcal{E})$ to be the supremum of net rates achieved by back-assisted protocols; and $R(\mathcal{E})$ to be the supremum of net rates achieved by unassisted protocols;

It follows immediately from the definitions that

$$R(\mathcal{E}) \le R_{\rightarrow}(\mathcal{E}) \le R_{\leftrightarrow}(\mathcal{E}) \text{ and } R(\mathcal{E}) \le R_{\leftarrow}(\mathcal{E}) \le R_{\leftrightarrow}(\mathcal{E}). \tag{4}$$

3 Classical equality between information and randomness distribution

In this section we will show that $R_{\leftrightarrow}(\mathcal{E})$ can be no larger than the entanglement-assisted capacity of $\mathcal{E}$, $C_E(\mathcal{E})$. Since $C_E(\mathcal{E}) = C(\mathcal{E})$ for classical channels (and, more generally, for classical-quantum channels), this establishes that

$$C(\mathcal{E}) = R_{\leftarrow}(\mathcal{E}) = R_{\rightarrow}(\mathcal{E}) = R_{\leftrightarrow}(\mathcal{E})$$

for such channels. We note that common randomness distribution via a classical channel $\mathcal{E}$ and noiseless feedback was considered by Ahslwede and Csiszar in [2], and that the equality $C(\mathcal{E}) = R_{\leftarrow}(\mathcal{E})$ is a corollary of their Theorem 4.3.

It was shown by Bennett, Shor, Smolin and Thapliyal [12], that the entanglement-assisted classical capacity of a channel $\mathcal{E}_{\mathsf{Y}\leftarrow\mathsf{X}}$ is given by

$$C_E(\mathcal{E}) = \max_{\rho_{\mathsf{RX}}} I(\mathsf{R} : \mathsf{Y})_{\mathcal{E}_{\mathsf{Y}\leftarrow\mathsf{X}}\rho_{\mathsf{RX}}}. \tag{5}$$

We will show that the same formula is an upper bound on $R_{\leftrightarrow}(\mathcal{E})$.

▶ **Theorem 2.** *For any channel $\mathcal{E}$, $R_{\leftrightarrow}(\mathcal{E}) \le C_E(\mathcal{E})$.*

Proof. Let us consider a protocol which makes n uses of the channel $\mathcal{E}$ and m auxiliary communication steps. For $k \in \{1, \dots, n\}$, let X_k denote the input system, and Y_k the output system, for the k-th use of the noisy channel.

Initially, Alice and Bob have systems A_0 and B_0 which are uncorrelated in that $I(\mathsf{A}_0 : \mathsf{B}_0) = 0$. We may assume without loss of generality that any local randomness used in the protocol is already present in the state of these systems. We may assume without loss of generality that at each step Alice and Bob have retained a full record of all auxiliary communication up to that step.

Suppose that at step j of the protocol, Bob sends Alice Z_k by auxiliary back communication. Then we may bound

$$\begin{aligned} I(\mathsf{A}_j : \mathsf{B}_j) &\overset{(a)}{\le} I(\mathsf{A}_{j-1} Z_k : \mathsf{B}_j) \overset{(b)}{\le} I(\mathsf{A}_{j-1} Z_k : \mathsf{B}_{j-1}) \\ &= I(\mathsf{A}_{j-1} : \mathsf{B}_{j-1}) + H(Z_k|\mathsf{A}_{j-1}) - H(Z_k|\mathsf{A}_{j-1}\mathsf{B}_{j-1}) \\ &\overset{(c)}{\le} I(\mathsf{A}_{j-1} : \mathsf{B}_{j-1}) + H(Z_k|\mathsf{A}_{j-1}) \overset{(d)}{\le} I(\mathsf{A}_{j-1} : \mathsf{B}_{j-1}) + H(Z_k|Z^{(k-1)}) \end{aligned} \tag{6}$$

where (a) and (b) are data processing, (c) is because, since Z_k is classical, $H(Z_k|\mathsf{A}_{j-1}\mathsf{B}_{j-1}) \ge 0$ and (d) is because A_{j-1} includes $Z^{(k-1)}$. A similar argument establishes the same inequality when Alice sends Bob Z_k by auxiliary forward communication, instead.

Now consider the case where Alice makes an input X_k to the noisy channel $\mathcal{E}$ at step j, with Bob receiving output Y_k. Then

$$\begin{aligned}
I(\mathsf{A}_j : \mathsf{B}_j) &\overset{(a)}{\leq} I(\mathsf{A}_j : \mathsf{B}_{j-1}\mathsf{Y}_k)\\
&= I(\mathsf{A}_j : \mathsf{Y}_k) + I(\mathsf{A}_j : \mathsf{B}_{j-1}|\mathsf{Y}_k)\\
&= I(\mathsf{A}_j : \mathsf{Y}_k) + I(\mathsf{A}_j\mathsf{Y}_k : \mathsf{B}_{j-1}) - I(\mathsf{Y}_k : \mathsf{B}_{j-1})\\
&\overset{(b)}{\leq} I(\mathsf{A}_j : \mathsf{Y}_k) + I(\mathsf{A}_j\mathsf{Y}_k : \mathsf{B}_{j-1})\\
&\overset{(c)}{\leq} I(\mathsf{A}_j : \mathsf{Y}_k) + I(\mathsf{A}_{j-1} : \mathsf{B}_{j-1})\\
&\overset{(d)}{\leq} C_E(\mathcal{E}) + I(\mathsf{A}_{j-1} : \mathsf{B}_{j-1}).
\end{aligned} \tag{7}$$

Here, (a) and (c) are by data processing, (b) is positivity of mutual information, and (d) is by the result of Bennett, Shor, Smolin and Thapliyal.

Recall that $Z := Z^{(m)}$ is the total record of auxiliary communication. Starting with $I(\mathsf{A}_{n+m} : \mathsf{B}_{n+m})$, and repeatedly invoking the inequality (6) or (7) depending on the type of step, we obtain

$$\begin{aligned}
I(\mathsf{A}_{n+m} : \mathsf{B}_{n+m}) &\leq I(\mathsf{B}_0 : \mathsf{A}_0) + nC_E(\mathcal{E}) + \sum_{k=1}^{m} H(Z_k|Z^{(k-1)})\\
&= nC_E(\mathcal{E}) + H(Z)\\
&\leq nC_E(\mathcal{E}) + \log|\mathcal{A}_Z|,
\end{aligned} \tag{8}$$

where the equality is by the chain rule and $I(\mathsf{B}_0 : \mathsf{A}_0) = 0$. Finally, we bound the net rate R of the protocol by

$$\begin{aligned}
R &= \frac{1}{n}(H(K) - \log|\mathcal{A}_Z|) = \frac{1}{n}(I(K : J) + H(K|J) - \log|\mathcal{A}_Z|)\\
&\overset{(a)}{\leq} \frac{1}{n}(I(\mathsf{A}_{n+m} : \mathsf{B}_{n+m}) + H(K|J) - \log|\mathcal{A}_Z|)\\
&\overset{(b)}{\leq} \frac{1}{n}(nC_E(\mathcal{E}) + \log|\mathcal{A}_Z| + nc\epsilon + 1 - \log|\mathcal{A}_Z|)\\
&\overset{(c)}{=} C_E(\mathcal{E}) + c\epsilon + 1/n
\end{aligned}$$

where (a) is data processing, (b) is by inequalities (8) and (3), and (c) by is Shannon's noisy channel coding theorem. Recalling the definition of $R_{\leftrightarrow}$, we have established that

$$R_{\leftrightarrow}(\mathcal{E}) \leq C_E(\mathcal{E}). \tag{9}$$

◀

We also claimed that $C(\mathcal{E}) = C_{\leftarrow}(\mathcal{E}) = C_{\rightarrow}(\mathcal{E}) = C_{\leftrightarrow}(\mathcal{E})$ for classical-quantum channels. In fact, we can show that this is true of any entanglement-breaking channel. The general equality $C(\mathcal{E}) = C_{\leftarrow}(\mathcal{E})$ is established in the next section. Now, note that we can write

$$C_{\leftrightarrow}(\mathcal{E}) = \sup_m \{C_{\leftarrow}(\mathcal{E} \otimes \mathcal{A}_m) - \log m\}$$

where $\mathcal{A}_m$ is a classical identity channel with m input symbols. Since $\mathcal{E}$ and $\mathcal{A}_m$ are both entanglement-breaking, we have

$$C_{\leftarrow}(\mathcal{E} \otimes \mathcal{A}_m) = C(\mathcal{E} \otimes \mathcal{A}_m) = C(\mathcal{E}) + C(\mathcal{A}_m) = C(\mathcal{E}) + \log m$$

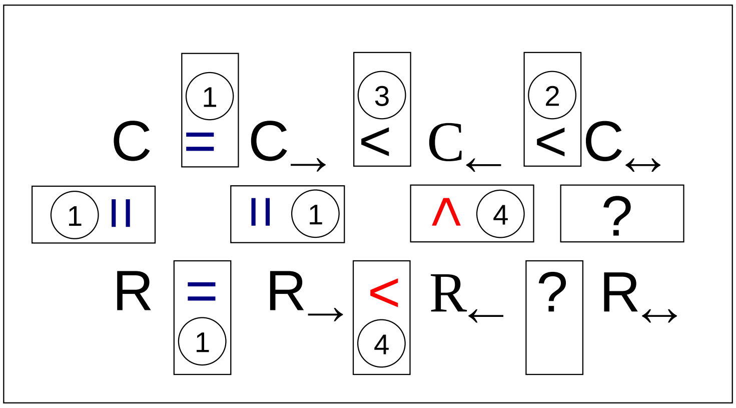


Figure 2 Relations between the communication (C) and randomness distribution (R) capacities. Note that an equality means that both capacities are equal for all channels; On the other hand, an inequality means that we know of at least one channel where one is strictly higher, which does not preclude the possibility that for other channels they may be equal. (1) It is easy to prove $C = R = C_{\rightarrow} = R_{\rightarrow}$, see Section 4.1 below. (2) Corollary of [11], using echo-correctable channels. (3) Corollary of [9], using random-phase coupling channels. (4) Our result in subsection 4.2. The relations between $R_{\leftarrow}(\mathcal{E})$, $R_{\leftrightarrow}(\mathcal{E})$ and $C_{\leftrightarrow}(\mathcal{E})$, i.e., whether they are equal for all channels or there are some examples of strict separation between them, remains an open question.

by Bowen-Nagarajan [3], the HSW theorem [7, 8], and the fact that the Holevo information is additive for entanglement breaking channels [10]. Therefore,

$$C_{\leftarrow}(\mathcal{E}) = C_{\leftrightarrow}(\mathcal{E}) = C(\mathcal{E})$$

for entanglement-breaking $\mathcal{E}$.

4 Quantum scenario

As opposed to the classical scenario, where all capacities of randomness distribution and information transmission, collapse into a single quantity given by Shannon's capacity, quantum channels have a richer behaviour depicted in Figure 2. The only similarity between the quantum and classical scenario is restricted to the unassisted and forward assisted capacities where, as shown in subsection 4.1 below, one can prove the equality

$$C(\mathcal{E}) = R(\mathcal{E}) = C_{\rightarrow}(\mathcal{E}) = R_{\rightarrow}(\mathcal{E}). \tag{10}$$

The situation changes radically for feedback and two-way assisted capacities. It was shown in [11] that by concatenating an *echo-correctable channel* and a depolarizing channel one can obtain an entanglement-breaking channel exhibiting a strict separation $C_{\leftarrow}(\mathcal{E}) < C_{\leftrightarrow}(\mathcal{E})$. Subsequently, in [9], the possibility of a strict separation $C_{\rightarrow}(\mathcal{E}) < C_{\leftarrow}(\mathcal{E})$ was shown using random-phase coupling channels (also informally called *rocket* channels). In subsection 4.2 below we show that there can be a separation $C_{\leftarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$. As a corollary we also obtain the separation $R_{\rightarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$.

4.1 Equality between unassisted and forward-assisted capacities

It is straightforward to see that $C(\mathcal{E}) \leq C_{\rightarrow}(\mathcal{E})$ and $R(\mathcal{E}) \leq R_{\rightarrow}(\mathcal{E})$ (assistance can only increase the rate), $C(\mathcal{E}) \leq R(\mathcal{E})$ (if you can send a bit of information you can also distribute

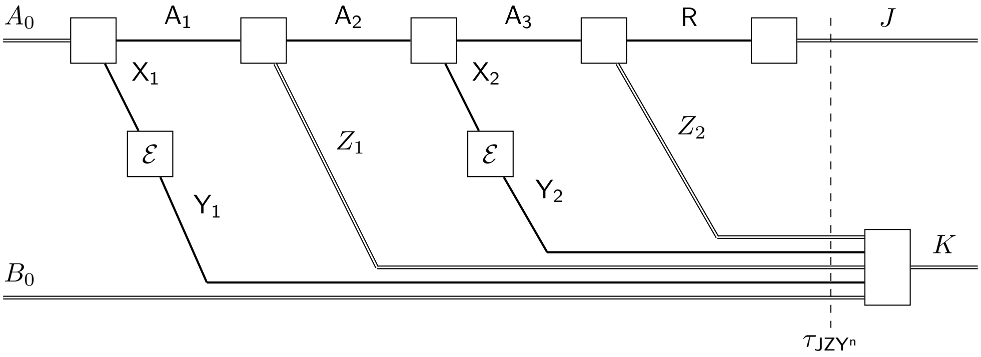


Figure 3 An example of a forward assisted randomness distillation protocol which makes two uses of the channel $\mathcal{E}$. Without loss of generality, Bob waits until receiving all communication from Alice to perform his local processing, and obtain K.

a bit of shared randomness) and similarly $C_{\rightarrow}(\mathcal{E}) \leq R_{\rightarrow}(\mathcal{E})$, because in both cases we only subtract the assisting forward communicaiton. In order to prove the equality between unassisted and forward-assisted capacities in eq. (10), it is sufficient to prove that the highest of the four capacities, $R_{\rightarrow}(\mathcal{E})$, is upper-bounded by the lowest of them, i.e. that $R_{\rightarrow}(\mathcal{E}) \leq C(\mathcal{E})$.

Since Bob does not send anything back to Alice during a forward-assisted protocol, there is no loss of generality if Alice makes all n uses of the noisy channel, sends all auxiliary classical communication and computes her share of the common randomness, J, before Bob does anything, as illustrated in Figure 3. We denote by R all systems retained by Alice, from which she computes her share of the common randomness.

Let $\mathsf{X^n}$ be the n input systems, and $\mathsf{Y^n}$ the n output systems, for the n uses of the noisy channel $\mathcal{E}^{\otimes n}$. We introduce a register Z which stores the value of the auxiliary forward communication Z, which can take one of $|\mathcal{A}_Z|$ values. After Alice has made all her communication to Bob, the state of the $\mathsf{ZY^nR}$ system is

$$\sigma_{\mathsf{ZY^nR}} = \sum_z p(z)|z\rangle\langle z|_{\mathsf{Z}} \otimes \mathcal{E}^{\otimes n}_{\mathsf{Y^n}\leftarrow\mathsf{X^n}}\rho^{(z)}_{\mathsf{X^nR}} \tag{11}$$

where $\rho^{(z)}_{\mathsf{X^nR}}$ is the state of the $\mathsf{X^nR}$, conditioned on $Z = z$. Now, Alice performs a measurement $E(j)$ (POVM of outcome j) on the system R to obtain her share J of the common randomness, which is stored in register J. At this point the state of the system is

$$\tau_{\mathsf{JZY^n}} = \sum_z q(j|z)p(z)|j\rangle\langle j|_{\mathsf{J}} \otimes |z\rangle\langle z|_{\mathsf{Z}} \otimes \mathcal{E}^{\otimes n}_{\mathsf{Y^n}\leftarrow\mathsf{X^n}}\rho^{(z,j)}_{\mathsf{X^n}}, \tag{12}$$

where

$$q(j|z)\rho^{(z,j)}_{\mathsf{X^n}} := \mathrm{Tr}_{\mathsf{R}} E(j)_{\mathsf{R}}\rho^{(z)}_{\mathsf{X^nR}}$$

defines the states $\rho^{(z,j)}_{\mathsf{X^n}}$ and conditional distribution $q(j|z)$.

Then Bob performs a measurement on the $\mathsf{ZY^n}$ system to obtain his share of randomness K. We can bound the mutual information between the shares by

$$\begin{aligned} I(J:K) &\overset{(a)}{\leq} I(\mathsf{J}:\mathsf{ZY^n})_\tau = I(\mathsf{J}:\mathsf{Y^n})_\tau + I(\mathsf{J}:\mathsf{Z}|\mathsf{Y^n})_\tau \\ &= I(\mathsf{J}:\mathsf{Y^n})_\tau + H(\mathsf{Z})_\tau - I(\mathsf{Z}:\mathsf{Y^n})_\tau - H(\mathsf{Z}|\mathsf{J},\mathsf{Y^n})_\tau \\ &\overset{(b)}{\leq} I(\mathsf{J}:\mathsf{Y^n})_\tau + H(\mathsf{Z})_\tau \overset{(c)}{\leq} \chi(\mathcal{E}^{\otimes n}) + \log|\mathcal{A}_Z| \end{aligned} \tag{13}$$

where (a) is data processing, (b) is because τ is separable with respect to the $\mathsf{Z}/\mathsf{JY}^\mathsf{n}$ bipartition so $H(\mathsf{Z}|\mathsf{JY}^\mathsf{n}) \geq 0$, and by positivity of mutual information, and (c) is because $I(\mathsf{J} : \mathsf{Y}^\mathsf{n}) \leq \chi(\mathcal{E}^{\otimes n})$. We use this to bound the net rate R of the protocol thus

$$\begin{aligned} R =& \frac{1}{n}(H(K) - \log|\mathcal{A}_Z|) = \frac{1}{n}(I(K:J) + H(K|J) - \log|\mathcal{A}_Z|) \\ \leq& \frac{1}{n}(\chi(\mathcal{E}^{\otimes n}) + \log|\mathcal{A}_Z| + H(K|J) - \log|\mathcal{A}_Z|) \leq \frac{1}{n}\chi(\mathcal{E}^{\otimes n}) + c\epsilon + 1/n, \end{aligned}$$

and therefore $R_{\rightarrow}(\mathcal{E}) \leq \lim_{n\to\infty} \frac{1}{n}\chi(\mathcal{E}^{\otimes n}) = C(\mathcal{E})$, where the equality is the Holevo-Schumacher-Westmoreland theorem [7, 8].

4.2 Quantum-classical channels; separation $C_{\leftarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$

Suppose that $\mathcal{E}_{Y\leftarrow\mathsf{X}}$ is a **quantum-classical** channel. That is, a channel of the form

$$\mathcal{E}_{Y\leftarrow\mathsf{X}} : \rho_\mathsf{X} \mapsto \sum_{y\in\mathcal{A}_Y} |y\rangle\langle y|_Y \mathrm{tr} E(y)_\mathsf{X}\rho_\mathsf{X} \tag{14}$$

where $\{E(y)_\mathsf{X} : y \in \mathcal{A}_Y\}$ is a POVM on X. In this case we can show that there is a back-assisted randomness distribution which achieves the upper-bound $C_E(\mathcal{E})$ for two-way assisted protocols, and therefore:

▶ **Theorem 3.** *For quantum-classical channels $\mathcal{E}_{Y\leftarrow\mathsf{X}}$, $R_{\leftarrow}(\mathcal{E}) = R_{\leftrightarrow}(\mathcal{E}) = C_E(\mathcal{E})$.*

We just need to show achievability: One way that n uses of a quantum-classical channel can be used to produce randomness with auxiliary back communication is as follows. Alice locally prepares n copies of a state ψ_{RX} and applies the n uses of the channel to X^n. This results in n copies of a quantum-classical state

$$\sum_y p(y)\rho(y)_\mathsf{R} \otimes |y\rangle\langle y|_Y = \mathcal{E}_{Y\leftarrow\mathsf{X}}\psi_{\mathsf{RX}} \tag{15}$$

being shared between Alice and Bob, with Bob holding the classical register Y, and $p(y) := \mathrm{tr}_{\mathsf{RX}} E(y)_\mathsf{X}\psi_{\mathsf{RX}}$ and $\rho(y)_\mathsf{R} := \mathrm{tr}_\mathsf{X} E(y)_\mathsf{X}\psi_{\mathsf{RX}}/p(y)$. Now, in the proof of the classical-quantum Slepian-Wolf theorem of Devetak and Winter [5] it was shown that, for any $0 < \epsilon < 1/2$ and $\delta > 0$, and all sufficiently large n, we can find $|\mathcal{A}_Z|$ disjoint subsets $\{C_z : z \in \mathcal{A}_Z\}$ of $\mathcal{A}_Y^n$ such that

(i) the probability that Y^n fails to belong to one of the subsets is not more than 2ϵ,

(ii) given the knowledge $Y^n \in C_z$, Alice can perform a measurement on R^n which identifies Y^n with probability of error no more than ϵ,

(iii) $\frac{1}{n}\log|\mathcal{A}_Z| \leq H(Y|\mathsf{R}) + 2\delta$.

This suggests the following protocol: Bob takes $K = Y^n$ as his share of the common randomness (so $H(K) = nH(Y)$) and sends Alice the identity Z of a subset C_Z containing Y^n (if such exists) whereupon Alice measures R^n to obtain an estimate J of Y^n. This protocol has $\Pr(K \neq J) \leq 3\epsilon$ and net rate

$$\frac{1}{n}(H(K) - \log|\mathcal{A}_Z|) \geq H(Y) - H(Y|\mathsf{R}) - 2\delta = I(Y:\mathsf{R}) - 2\delta.$$

Therefore, by optimising over the choice of ψ_{XR} in the protocol, we have established that

$$R_{\leftarrow}(\mathcal{E}) \geq \max_{\psi_{\mathsf{XR}}} I(Y:\mathsf{R})_{\mathcal{E}_{Y\leftarrow\mathsf{X}}\psi_{\mathsf{XR}}} = C_E(\mathcal{E}), \tag{16}$$

where $C_E(\mathcal{E})$ is the entanglement-assisted capacity of $\mathcal{E}$, and the equality is the theorem of Bennett, Shor, Smolin and Thapliyal [12].

Now, quantum-classical channels are entanglement breaking. It was shown by Bowen and Nagarajan [3] that classical feedback cannot increase the classical capacity of entanglement breaking channels, so we have $C_{\leftarrow}(\mathcal{E}) = C(\mathcal{E})$. Meanwhile, in [4], Holevo has given examples of quantum-classical channels with $C_E(\mathcal{E}) > C(\mathcal{E})$. By Theorem 3 and Bowen-Nagarajan, these channels also exhibit a separation $R_{\leftarrow}(\mathcal{E}) > C_{\leftarrow}(\mathcal{E})$. To be more specific, consider the case where the POVM elements determining $\mathcal{E}$ are rank-one projectors onto pair-wise linearly independent subspaces. Then $C(\mathcal{E}) \leq C_E(\mathcal{E}) = \log d$, and Holevo shows that the inequality is strict *unless* the the POVM is a orthonormal basis measurement [4].

4.3 Specific example

Given two rank-1 projective measurements $E^{(0)}$ and $E^{(1)}$ on a d-dimensional system X with outcomes in $\{1, \ldots, d\}$ we may construct a quantum-classical channel $\mathcal{F}_{Y \leftarrow \mathsf{X}}$ whose input system is X and whose output is a pair $Y = (M, G)$ where M is a bit chosen uniformly at random, and G is the result of performing the measurement $E^{(M)}$ on X. So, M tells us which basis was measured and G tells us the result of that measurement. Without loss of generality we can take $E^{(0)}$ to be the computational basis measurement.

Since the POVM corresponding to this classical-quantum channel has rank-one elements we already know that

$$R_{\leftarrow}(\mathcal{F}) = C_E(\mathcal{F}) = \log d. \tag{17}$$

In Figure 4 we illustrate a protocol which distributes $1 + \log d$ bits of perfectly correlated randomness with one use of $\mathcal{F}$ and a single bit of communication from Bob to Alice, thus attaining a net rate of $\log d$ bits per channel use, perfectly.

On the other hand, if we choose $E^{(1)}$ so that the two measurement bases are mutual unbiased, it is not hard to establish that $C_{\leftarrow}(\mathcal{F}) = C(\mathcal{F}) = \chi(\mathcal{F}) \leq \frac{1}{2}\log d$: The first two equalities are because the channel is entanglement breaking. It remains to upper bound the Holevo information $\chi(\mathcal{F})$. Suppose that the input to the channel is drawn from an ensemble $\{(p(w), \psi^{(w)}) : w = 1, \ldots k\}$ with ensemble average $\rho = \sum_{w=1}^{k} p(w)\psi^{(w)}$. Maximising

$$H(M,G)_\rho - \sum_w p(w) H(M,G)_{\psi^{(w)}} \tag{18}$$

over all ensembles, we obtain the Holevo information $\chi(\mathcal{F})$, and since the channel is entanglement breaking, we know that $C_{\leftarrow}(\mathcal{F}) = C(\mathcal{F}) = \chi(\mathcal{F})$. Clearly

$$H(M,G)_\rho \leq 1 + \log d \tag{19}$$

while, for any state ψ,

$$\begin{aligned} H(M,G)_\psi =& H(M) + H(G|M=0)_\psi \Pr(M=0) + H(G|M=1)_\psi \Pr(M=1) \\ =& 1 + \frac{1}{2}\left(H(G|M=0)_\psi + H(G|M=1)_\psi\right). \end{aligned}$$

If the measurements correspond to mutually unbiased bases then, according to Maassen and Uffink's entropic uncertainty relation [14], we have

$$H(M,G)_\psi \geq 1 + \frac{1}{2}\log d, \tag{20}$$

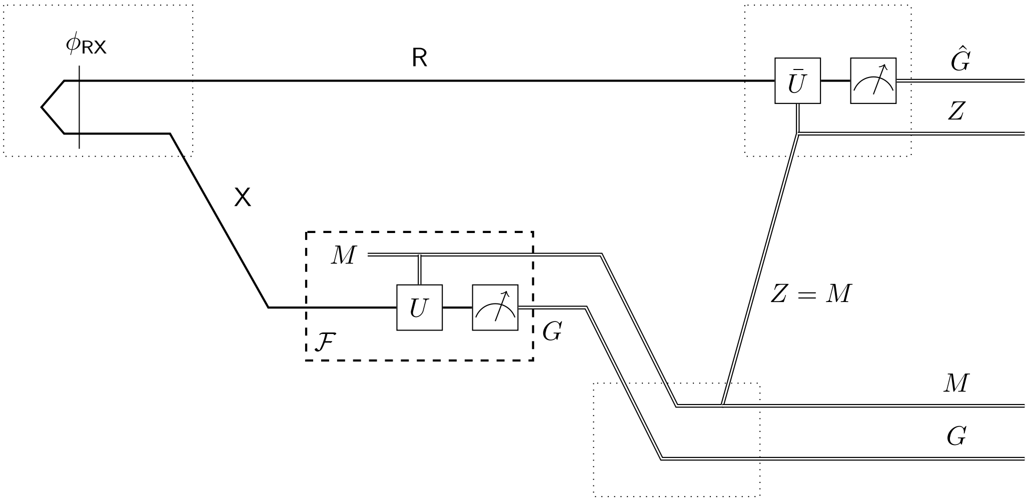


Figure 4 Sharing $1 + \log d$ bits of perfect randomness with one use of the channel $\mathcal{F}$ (the contents of the dashed rectangle) and one bit of back communication: Alice locally prepares a maximally entangled state ϕ_{RX} and inputs X to the channel. We can view the channel as performing a unitary controlled by the bit M and then performing a computational basis measurement to yield G. Alice sets $Z = M$ and sends Z to Bob, who performs $\bar{U}$ (the complex conjugate of U) iff $Z = 1$ and then performs a computational basis measurement on R to yield a value $\hat{G}$. By the $U \otimes \bar{U}$ invariance of ϕ, $\hat{G} = G$ with probability one, so if Alice sets $J = (\hat{G}, Z)$ and Bob sets $K = (G, M)$ then $\Pr(K = J) = 1$, and K is uniformly distributed. Local operations are surrounded by dotted lines.

and substituting the bounds (19) and (20) into (18),

$$C_{\leftarrow}(\mathcal{E}) = C(\mathcal{E}) = \chi(\mathcal{E}) \leq \frac{1}{2} \log d.$$

This upper bound is indeed tight for both, $C_{\leftarrow}(\mathcal{E})$ and $C(\mathcal{E})$, as the channel $\mathcal{E}$ can be transformed with some post-processing on Bob's side into an erasure channel (if $M = 1$ erase register G) of error probability $1/2$. Therefore (feedback-assisted) error-correcting codes for the erasure channel can be used to saturate the bound $C(\mathcal{E}) = C_{\leftarrow}(\mathcal{E}) = 1/2 \log d$.

5 Conclusion

Despite being, a priori, different things, we have seen that the capacity for a classical channel to distribute shared randomness and to send information are the same, with arbitrary classical assistance. For quantum channels, we have shown that the entanglement-assisted capacity $C_E(\mathcal{E})$ is a general upper bound for $R_{\leftrightarrow}(\mathcal{E})$, and shown that this bound can be achieved using only back-communication for quantum-classical channels. Using this result we have established that strict separations $C_{\leftarrow}(\mathcal{E}) < R_{\leftarrow}(\mathcal{E})$ are possible for quantum-classical channels. We give an explicit example for which $R_{\leftarrow}(\mathcal{E}) = \log d$ while $C_{\leftarrow}(\mathcal{E}) = \frac{1}{2} \log d$.

Our result shows that contrary to what is predicted by classical information theory, where the optimal way of distributing randomness is to generate it locally and distribute it through the channel, quantum mechanics allows for the activation of randomness initially locked inside the channel, which boost the amount of shared randomness generated in the process.

References

1 T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (Wiley, New York, 1991).

2 R. Ahlswede and I. Csiszár, IEEE Trans. Info. Theory **39,** pp. 1121–1132 (1993).

3 G. Bowen and R. Nagarajan, IEEE Trans. Inform. Theory 51, 320 (2005).

4 A. Holevo, Problems of Information Transmission, vol. 48 (2012), pp. 1–10.

5 I. Devetak and A. Winter, Phys. Rev. A 68, 042301 (2003)

6 I. Devetak and A. Winter, IEEE Trans. Info. Theory **50,** 3183 (2004).

7 A. Holevo, IEEE Transactions on Information Theory 44(1):269–273 (1996).

8 B. Schumacher, M. Westmoreland, Phys. Rev. A 56:131–138 (1997).

9 G. Smith and J. A. Smolin, Phys. Rev. Lett. 103, 120503 (2009).

10 Additivity of the classical capacity of entanglement-breaking quantum channels. Journal of Mathematical Physics, 43(9):4334–4340, (2002).

11 C. H. Bennett, I. Devetak, P. W. Shor, and J. A. Smolin, Phys. Rev. Lett. 96, 150502 (2006).

12 C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, IEEE Trans. Info. Theory **48,** 2637 (2002).

13 L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183,** 14 (1993).

14 H. Maassen, and J. Uffink, Phys. Rev. Lett. 60, 1103 (1988)

Implementing Unitary 2-Designs Using Random Diagonal-unitary Matrices

Yoshifumi Nakata*[1], Christoph Hirche†[1], Ciara Morgan[1], and Andreas Winter[2]

1 **Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover, Germany**
{yoshifumi.nakata,christoph.hirche,ciara.morgan}@itp.uni-hannover.de

2 **ICREA & Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain**
andreas.winter@uab.cat

Abstract

Unitary 2-designs are random unitary matrices which, in contrast to their Haar-distributed counterparts, have been shown to be efficiently realized by quantum circuits. Most notably, unitary 2-designs are known to achieve decoupling, a fundamental primitive of paramount importance in quantum Shannon theory. Here we prove that unitary 2-designs can be implemented approximately using random diagonal-unitaries.

1998 ACM Subject Classification H.1.1 Systems and Information Theory

Keywords and phrases Unitary 2-designs, commuting quantum circuits

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.191

1 Introduction

With coherent implementations of quantum circuits becoming a reality, the question of the practical realization of protocols in quantum information science has been a particular focus of the field in recent years. Indeed, quantum information theory itself is concerned with the evolution of quantum systems and decoupling represents one of the most fundamental primitives [1, 2, 3, 4]. Moreover, this protocol characterizes the conditions under which two, initially correlated, quantum systems will decohere completely, after evolution and the protocol itself is achieved using so-called Haar random unitaries [5, 6].

While Haar random unitaries are a powerful theoretical tool, the number of gates required to achieve their implementation grows exponentially in the system size. Unitary designs represent finite approximations of Haar random unitaries and, unitary 2-designs in particular, have been shown to efficiently achieve the decoupling protocol [7]. Moreover, unitary designs and the analysis of their performance have been widely studied [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. Unitary 2-designs have been shown to be achieved using Clifford circuits [8, 9] and random quantum circuits [12, 13, 14, 15] and among the most notable of results is the recent breakthrough of Cleve *et al.* [18] demonstrating a "near linear" implementation of an exact unitary 2-design.

[*] Now at: Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan – nakata@qi.t.u-tokyo.ac.jp.

[†] Now at: Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain – christoph.hirche@uab.cat.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 191–205
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

This motivates the question of how simply unitary 2-designs can be achieved. In this paper we show that unitary 2-designs can be realized to arbitrary precision by random diagonal-unitaries. Along with theoretical interest, the significance of this result lies in its simple implementation. Indeed, a quantum circuit for the implementation consists of repeating single-qubit phase gates, the controlled-Z gates, and the Hadamard gates. The first two parts are commuting, and they can be applied, in principle, simultaneously. Moreover, the depth of the non-commuting part, i.e. the Hadamard gates, is $O(1)$. These features of our implementation leads to a vast reduction in the execution time of the overall circuit. This work also provides a concrete application of commuting quantum circuits. Little is known about their concrete applications [19, 20] though they are known to provide a quantum advantage in computational tasks [21, 22]. The present authors have also shown that the decoupling theorem can be achieved by random-diagonal unitaries [23].

The article is organised as follows. We begin by introducing the necessary definitions and notation in Section 2. The main results are presented in Section 3, with the statement that unitary 2-designs can be achieved using random diagonal-unitary matrices given by Theorem 5 and the implementation given by Corollary 6. Proofs of the main results are presented in Section 4, along with statements of the necessary lemmas. Indeed, Lemma 8 is of particular importance in our analysis.

2 Preliminaries

2.1 Notation

We consider a system composed of N qubits and denote by $\mathcal{H}$, the corresponding Hilbert space and by $d = 2^N$ the dimension of $\mathcal{H}$. The set of bounded operators and states on $\mathcal{H}$ are denoted by $\mathcal{B}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{B}(\mathcal{H}) | \rho \geq 0, \mathrm{tr}\rho = 1\}$, respectively.

We will make use of various norms throughout the article, defined as follows. The p-norm of $X \in \mathcal{B}(\mathcal{H})$ is defined by $\|X\|_p := (\mathrm{tr}|X|^p)^{1/p}$ for $p \geq 1$. For a superoperator $\mathcal{C} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, we use a family of superoperator norms $\|\mathcal{C}\|_{q\to p}$ $(q, p \geq 1)$ and the diamond norm [24] defined by

$$\|\mathcal{C}\|_{q\to p} = \sup_{X\neq 0} \frac{\|\mathcal{C}(X)\|_p}{\|X\|_q}, \qquad \|\mathcal{C}\|_\diamond := \sup_k \|\mathcal{C} \otimes \mathrm{id}_k\|_{1\to 1}, \tag{1}$$

respectively, where $\mathrm{id_k}$ is the identity map acting on a Hilbert space of dimension k. Note that it is known that $k \leq d$ is sufficient to obtain the diamond norm [24].

2.2 Random unitary matrices and their t-designs

We begin with the definition of random unitary matrices, before discussing their role in quantum information science, leading to the definition of unitary t-designs and approximations.

▶ **Definition 1** (Haar random unitary matrices [25]). Let $\mathcal{U}(d)$ be the unitary group of degree d, and denote the Haar measure (i.e. the unique unitarily invariant probability measure, thus often called uniform distribution) on $\mathcal{U}(d)$ by $\mathrm{H}_{\mathcal{U}(d)}$. A *Haar random unitary matrix* U is a $\mathcal{U}(d)$-valued random variable distributed according to the Haar measure, $U \sim \mathrm{H}_{\mathcal{U}(d)}$.

▶ **Definition 2** (Random $\mathbf{X}$- and $\mathbf{Z}$-diagonal-unitary matrices [19]). Let $\mathcal{D}_{W,\mathrm{diag}}$ be the set of unitary matrices diagonal in the Pauli-W basis $\{|n\rangle_W\}_{n=0}^{d-1}$ $(W = X, Z)$, given by $\left\{\sum_{n=0}^{d-1} e^{i\varphi_n} |n\rangle\langle n|_W : \varphi_n \in [0, 2\pi) \text{ for } n \in [0, \ldots, d-1]\right\}$. Let D_W denote a probability measure on it induced by a uniform probability measure on its parameter space $[0, 2\pi)^d$. A *random W-diagonal-unitary matrix* D^W is a $\mathcal{D}_{W,\mathrm{diag}}$-valued random variable distributed according to D_W, $D^W \sim \mathrm{D}_W$.

The random unitary matrices, defined above, have been applied to a wide variety of problems in quantum information science (see e.g. [16] for a summary) and have been used to investigate typical properties in physical systems [26, 27, 28, 29]. However, they cannot be efficiently implemented by quantum circuits, since the number of random numbers needed for the implementation scales exponentially with the number of qubits in the system. This fact has lead to the investigation of their approximation, that is, to the definition and performance analysis of *unitary t-designs* [8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18].

Indeed, a unitary t-design is a random variable taking values in the unitary group that simulate, up to the tth order, the statistical moments of a given random unitary matrix. To define a unitary t-design for a random unitary matrix U, let $\mathcal{G}_U^{(t)}(X)$ be a superoperator given by $\mathcal{G}_U^{(t)}(X) := \mathbb{E}_U[U^{\otimes t} X U^{\dagger \otimes t}]$ for any $X \in \mathcal{B}(\mathcal{H}^{\otimes t})$, where $\mathbb{E}_U$ represents an expectation over U. Then, an ϵ-approximate unitary t-design is defined as follows.

▶ **Definition 3** (ϵ-approximate unitary t-designs [9, 14])**.** A random unitary matrix $U \in \mathcal{U}(d)$ is called an ϵ-approximate unitary t-design if $\|\mathcal{G}_U^{(t)} - \mathcal{G}_{U_H}^{(t)}\|_\diamond \leq \epsilon$, where U_H is a Haar random unitary matrix.

▶ **Definition 4** (ϵ-approximate diagonal-unitary t-designs [19])**.** A random diagonal-unitary matrix $U \in \mathcal{D}_{W,\mathrm{diag}}$ $(W = X, Z)$ is called an ϵ-approximate W-diagonal-unitary t-design if $\|\mathcal{G}_U^{(t)} - \mathcal{G}_{D^W}^{(t)}\|_\diamond \leq \epsilon$, where D^W is a random W-diagonal unitary matrix.

In these definitions, the designs are called *exact* when $\epsilon = 0$. Note that there are various definitions of ϵ-approximate unitary t-designs, a summary of which can be found in Ref. [16]. Most definitions are equivalent in the sense that, if U is an ϵ-approximate unitary t-design in one definition, it is also an ϵ'-approximate unitary t-design in other definitions for $\epsilon' = \mathrm{poly}(d^t)\epsilon$.

3 Main results

3.1 A unitary 2-design by random diagonal-unitary matrices

We study an implementation of a unitary 2-design using random diagonal-unitary matrices. We alternately apply independent random Z- and X-diagonal-unitary matrices, and show that this strategy approaches a unitary 2-design, after a number of repetitions ℓ. A random unitary matrix obtained by this process is given by

$$D[\ell] := D^Z_{\ell+1} D^X_\ell D^Z_\ell \cdots D^X_2 D^Z_2 D^X_1 D^Z_1. \tag{2}$$

where D_i^W are independent W-diagonal-unitary matrices $(i = 1, \ldots, \ell + 1,\ W = X, Z)$. The $D[\ell]$ can, equivalently, be expressed as

$$D[\ell] = \prod_{i=\ell}^{1} D_i^{\prime Z} D_i^X D_i^Z, \tag{3}$$

where all random diagonal-unitary matrices are taken independently. We will use this particular expression of $D[\ell]$ in the remainder of the article.

Note that, since a random X-diagonal-unitary matrix can be obtained by conjugating a random Z-diagonal-unitary matrix by Hadamard gates, $D[\ell]$ can equivalently be expressed as

$$D[\ell] = D^Z_{2\ell+1} \prod_{i=2\ell}^{1} (H^{\otimes N} D^Z_i), \tag{4}$$

where $H^{\otimes N}$ is the tensor product of N Hadamard gates acting on all N qubits. From this point of view, the Hadamard gates are the only non-commuting part of $D[\ell]$. We will use this expression when we consider an efficient implementation of $D[\ell]$ in Subsection 3.2.

Our main result shows that $D[\ell]$ quickly approaches a unitary 2-design with increasing ℓ. The formal statement is given by Theorem 5 below.

▶ **Theorem 5** (**$D[\ell]$** is an approximate unitary 2-design). *A random unitary matrix $D[\ell]$, acting on N qubits, is an ϵ-approximate unitary 2-design for $\ell \geq 2 + \frac{1}{N}(1 + \log 1/\epsilon)$. Conversely, $D[\ell]$ cannot be an ϵ-approximate unitary 2-design if $\ell \leq \frac{1}{N} \log 1/\epsilon$.*

▶ Remark. The significance of Theorem 5 lies in the efficiency of its implementation. Moreover, since a random unitary matrix $D[\ell]$ can be separated into commuting (random Z-diagonal-unitary matrices) and non-commuting (the Hadamard gates) parts, and the number of non-commuting gates for the implementation scales linearly with the system size, this construction of an approximate unitary 2-design has a simple practical implementation. We expand upon this point in the following subsection.

3.2 Implementation of $D[\ell]$ by a quantum circuit

We show that a unitary 2-design achieved by $D[\ell]$ can be efficiently implemented by a quantum circuit. We do so by only considering a random Z-diagonal-unitary matrix D^Z, since $D[\ell]$ is composed simply of D^Z along with Hadamard matrices.

Since the exact implementation of D^Z is not efficient, we replace it by a random diagonal unitary matrix that *is* efficiently implementable. As we only need the second moments of D^Z for the implementation of a unitary 2-design, this is achieved by an exact Z-diagonal-unitary 2-design. An efficient implementation of an exact Z-diagonal-unitary t-design by a diagonal quantum circuit for any $t \in \mathbf{N}$ is provided in Ref. [30]. As its corollary, an exact Z-diagonal-unitary 2-design is implemented in the following way.

▶ **Corollary 6** (Exact implementation of Z-diagonal-unitary **2**-designs). *An exact Z-diagonal-unitary 2-design is obtained by applying single-qubit phase gates* $\mathrm{diag}\{1, e^{i\varphi_k}\}$ *on all qubits, where each phase φ_k is randomly and independently chosen from $\{0, 2\pi/3, 4\pi/3\}$ with $k \in [1, \ldots, N]$, followed by probabilistic applications of the controlled-Z gate on every pair of qubits, where each controlled-Z gate is applied with probability* $1/2$.

Using this implementation, an approximate unitary 2-design can be implemented by repeating the following three steps (see also Fig. 1):

1. Apply single-qubit phase gates $\mathrm{diag}(1, e^{i\varphi})$, which are diagonal in the Pauli-Z basis, with $\varphi \in \{0, 2\pi/3, 4\pi/3\}$ a random phase on all qubits.
2. Apply the controlled-phase gates $\mathrm{diag}(1, 1, 1, e^{i\theta})$, diagonal in the Pauli-$Z$ basis, with a random phase $\theta \in \{0, \pi\}$ on all pairs of qubits.
3. Apply the Hadamard gates on all qubits.

Note that the two-qubit phase gate, applied in the second step, is equivalent to a random application of the controlled-Z gate with probability $1/2$ in Corollary 6, since θ is randomly

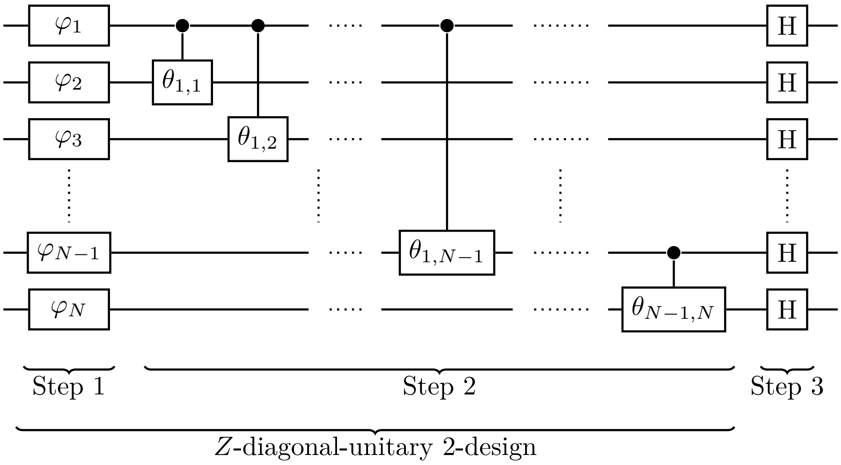


Figure 1 The figure depicts a building block of the quantum circuit that implements a unitary 2-design according to $D[\ell]$, given by Eq. (4). All the gates in the implementation of a Z-diagonal-unitary 2-design are diagonal in the Pauli-Z basis and, hence, can be applied simultaneously. One- and two-qubit gates in the first and the second step are given by $\mathrm{diag}(1, e^{i\varphi_k})$ and $\mathrm{diag}(1, 1, 1, e^{i\theta_{l,r}})$, respectively. The phases φ_k $(k = 1, \cdots, N)$ and $\theta_{l,r}$ $(l, r = 1, \cdots, N,\ l \neq r)$ are chosen from $\{0, 2\pi/3, 4\pi/3\}$ and $\{0, \pi\}$, respectively, uniformly at random. The one-qubit gates H represent the Hadamard gates.

chosen from $\{0, \pi\}$. We conclude from Theorem 5 and Corollary 6 that an ϵ-approximate unitary 2-design can be implemented with at most $3N(N + \frac{1}{2} \log 1/\epsilon) + O(N)$ one- or two-qubit gates, most of which are commuting. Numerical evidence for this observation has previously been found in Ref. [12, 13]

In terms of the number of gates, this implementation is as efficient as most of the previously known implementations of a unitary 2-design [9, 8, 14], but is not as efficient as a recently discovered near-linear construction of an exact unitary 2-design [18]. Our implementation of a unitary 2-design has another merit in view of commutativity of the gates, resulting in an instant property of the circuit in the sense that all the commuting parts of the circuit can be, in principle, applied simultaneously. In many physical systems for a quantum circuit, quantum gates are implemented by adding external electromagnetic fields [31]. If the circuit is composed of non-commuting gates, each field implementing a quantum gate should be applied in sequence, which results in a relatively long implementation time. In contrast, no ordering is imposed for commuting circuits and all the fields can be applied at once. Since our construction of a unitary 2-design uses a quantum circuit, where only the non-commuting part is the third step and is depth one, the practical time of our implementation is drastically reduced compared to the implementations using non-commuting gates scattered over the circuits. This also results in a robust implementation. Hence, our construction of a unitary 2-design may be preferable to other constructions from an experimental point of view.

This construction is also preferable for measurement-based quantum computation (MBQC) [32, 33]. In MBQC, computation is performed by single-qubit measurements on a certain type of multi-partite entangled pure states, known as cluster states. The measurement basis for implementing quantum gates, with the exception of Clifford gates, depends on the outcomes of previous measurements. This adaptivity of measurement basis in MBQC makes it challenging to experimentally perform. When we implement a unitary 2-design by $D[\ell]$ in MBQC, adaptive measurements are not necessary since all the gates are either commuting (the first and the second steps) or Clifford (the third step). The implementation is also uniform in the sense that it is invariant under permutations of qubits. Hence, a unitary 2-design is obtained by simple MBQC where all the qubits in a cluster state can be simultaneously measured in prefixed bases.

4 Proofs

4.1 Auxiliary lemmas

In the following we provide the lemmas needed in the proof of Theorem 5. We begin by introducing some additional notation.

We denote the Pauli-Z and Pauli-X bases by $\{|i\rangle\}_{i=0,\cdots,d-1}$ and $\{|\alpha\rangle\}_{\alpha=0,\cdots,d-1}$, respectively. That is, the Pauli-Z basis is always labelled by Latin alphabets and the Pauli-X basis by Greek ones. We also denote the coefficients of $|\alpha\rangle$ in the basis of $\{|i\rangle\}$ by $\alpha_i/\sqrt{d}$, namely, $\alpha_i = \sqrt{d}\langle i|\alpha\rangle$. Similarly, we define $i_\alpha := \sqrt{d}\langle\alpha|i\rangle$. Note that they are always ± 1, and $\alpha_i = i_\alpha$. We also use the following quantity f^{ij}_{kl};

$$f^{ij}_{kl} = \frac{2}{d^3}\left(\sum_{\alpha=0}^{d-1} \alpha_i\alpha_j\alpha_k\alpha_l\right)^2. \tag{5}$$

The f^{ij}_{kl} satisfy the following relations (see Appendix A for the proof).

▶ **Lemma 7.** *The quantity f^{ij}_{kl} is in $\{0, 2/d\}$ and satisfies $f^{ij}_{kl} = f^{kl}_{ij}$, $\sum_{i>j} f^{ij}_{kl} = 1$ and $\sum_{s>t} f^{ij}_{st} f^{st}_{kl} = f^{ij}_{kl}$.*

We use several operators in $\mathcal{B}(\mathcal{H}^{\otimes 2})$. First, we denote by $\mathbb{I}$, $\mathbb{F}$, $\mathbb{L}_Z$, and $\mathbb{L}_X$, the identity operator, the swap operator defined by $\sum_{i,j}|ij\rangle\langle ji|$, $\mathbb{L}_Z := \sum_i |ii\rangle\langle ii|$, and $\mathbb{L}_X := \sum_\alpha |\alpha\alpha\rangle\langle\alpha\alpha|$, respectively. The operator $\mathbb{L}_W$ is defined in the Pauli-W basis and is dependent on the basis. We also denote by P_{sym} and P_{anti} the projection operators onto the symmetric and antisymmetric subspaces of $\mathcal{H}^{\otimes 2}$, which are equal to $(\mathbb{I}+\mathbb{F})/2$ and $(\mathbb{I}-\mathbb{F})/2$, respectively. Using these operators, we define states Π_{sym}, Π_{anti}, and Λ_W $(W = X, Z)$, which are given by $P_{\text{sym}}/\text{tr}P_{\text{sym}}$, $P_{\text{anti}}/\text{tr}P_{\text{anti}}$, and $\mathbb{L}_W/\text{tr}\mathbb{L}_W$, respectively. The normalization factors are given by

$$\text{tr}P_{\text{sym}} = \frac{d(d+1)}{2}, \quad \text{tr}P_{\text{anti}} = \frac{d(d-1)}{2}, \quad \text{tr}\mathbb{L}_W = d. \tag{6}$$

The main part of the proof is concerned with the completely-positive and trace-preserving (CPTP) map $\mathcal{R}$ from $\mathcal{B}(\mathcal{H}^{\otimes 2})$ to itself defined by $\mathcal{R} = \mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X} \circ \mathcal{G}^{(2)}_{D^Z}$, where $\mathcal{G}^{(2)}_U$ for a random unitary matrix U is defined in Subsection 2.

▶ **Lemma 8.** *Let B be the basis in $\mathcal{H}^{\otimes 2}$ given by $\{|ii\rangle\}_{i=0}^{d-1} \cup \{|\phi_{ij}\rangle\}_{i>j} \cup \{|\psi_{ij}\rangle\}_{i>j}$, where $|\phi_{ij}\rangle := \frac{1}{\sqrt{2}}(|ij\rangle + |ji\rangle)$ and $|\psi_{ij}\rangle := \frac{1}{\sqrt{2}}(|ij\rangle - |ji\rangle)$. Then, for all $|p\rangle \neq |q\rangle \in B$ and all integers ℓ, it holds $\mathcal{R}^\ell(|p\rangle\langle q|) = 0$, and*

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = (1-d^{-2\ell})\Pi_{\text{sym}} + d^{-2\ell}\Lambda_Z \tag{7}$$

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|) = a_\ell\Pi_{\text{sym}} + b_\ell\Lambda_Z + d^{-\ell}\sum_{k>l} f^{ij}_{kl}\,|\phi_{kl}\rangle\langle\phi_{kl}| \tag{8}$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|) = (1-d^{-\ell})\Pi_{\text{anti}} + d^{-\ell}\sum_{k>l} f^{ij}_{kl}\,|\psi_{kl}\rangle\langle\psi_{kl}|\,, \tag{9}$$

where

$$a_\ell = 1 - \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)}, \tag{10}$$

$$b_\ell = 2\frac{d^\ell - 1}{d^{2\ell}(d-1)}. \tag{11}$$

Proof. We first investigate $\mathcal{R}(|ii\rangle\langle kk|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|)$, and $\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|)$ ($i > j$ and $k > l$). As each input state is in the Pauli-Z basis, we obtain

$$\mathcal{R}(|ii\rangle\langle kk|) = \delta_{ik}\mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X}(|ii\rangle\langle ii|) \tag{12}$$

$$\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|) = \delta_{ik}\delta_{jl}\mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X}(|\phi_{ij}\rangle\langle\phi_{ij}|) \tag{13}$$

$$\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|) = \delta_{ik}\delta_{jl}\mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X}(|\psi_{ij}\rangle\langle\psi_{ij}|). \tag{14}$$

Using the relation $\mathcal{G}^{(2)}_{D^X}(|ii\rangle\langle ii|) = \frac{1}{d^2}\big(\mathbb{I} + \mathbb{F} - \mathbb{L}_X\big)$, and $\mathbb{I}$ and $\mathbb{F}$ are invariant under $\mathcal{G}^{(2)}_{D^Z}$, the $\mathcal{R}(|ii\rangle\langle kk|)$ is calculated to be

$$\mathcal{R}(|ii\rangle\langle kk|) = \frac{1}{d^2}\delta_{ik}\bigg[\big(1 - \frac{1}{d}\big)\big(\mathbb{I} + \mathbb{F}\big) + \frac{1}{d}\mathbb{L}_Z\bigg]. \tag{15}$$

Note that this implies that $\mathcal{R}(|ii\rangle\langle ii|)$ is independent of i. For $\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|)$ and $\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|)$, simple calculations lead to

$$\mathcal{G}^{(2)}_{D^X}(|ij\rangle\langle ij|) = \frac{1}{d^2}\bigg(\mathbb{I} + \sum_{\alpha,\beta}\alpha_i\alpha_j\beta_i\beta_j\,|\alpha\beta\rangle\langle\beta\alpha| - \mathbb{L}_X\bigg) \tag{16}$$

$$\mathcal{G}^{(2)}_{D^X}(|ij\rangle\langle ji|) = \frac{1}{d^2}\bigg(\sum_{\alpha,\beta}\alpha_i\alpha_j\beta_i\beta_j\,|\alpha\beta\rangle\langle\alpha\beta| + \mathbb{F} - \mathbb{L}_X\bigg), \tag{17}$$

and similar relations for $\mathcal{G}^{(2)}_{D^Z}(|\alpha\beta\rangle\langle\alpha\beta|)$ and $\mathcal{G}^{(2)}_{D^Z}(|\alpha\beta\rangle\langle\beta\alpha|)$. Hence, we obtain

$$\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|) = \frac{1}{d^2}\delta_{ik}\delta_{jl}\bigg[\big(1 - \frac{2}{d}\big)\big(\mathbb{I} + \mathbb{F}\big) + \frac{2}{d}\mathbb{L}_Z + d\sum_{s>t} f^{ij}_{st}\,|\phi_{st}\rangle\langle\phi_{st}|\bigg] \tag{18}$$

$$\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|) = \frac{1}{d^2}\delta_{ik}\delta_{jl}\bigg[\mathbb{I} - \mathbb{F} + d\sum_{s>t} f^{ij}_{st}\,|\psi_{st}\rangle\langle\psi_{st}|\bigg], \tag{19}$$

where we use, e.g. $\alpha_i = i_\alpha$ for the derivation.

We next show that other terms, such as $\mathcal{R}(|\phi_{ij}\rangle\langle kk|)$, $\mathcal{R}(|\psi_{ij}\rangle\langle kk|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{kl}|)$ and their conjugates, are zero. Amongst these terms, all except $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ and its conjugate vanish after the first application of $\mathcal{G}^{(2)}_{D^Z}$. For $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \mathcal{G}^{(2)}_{D^Z} \circ \mathcal{G}^{(2)}_{D^X}(|\phi_{ij}\rangle\langle\psi_{ij}|)$, since $|\phi_{ij}\rangle\langle\psi_{ij}|$ is not changed by $\mathcal{G}^{(2)}_{D^Z}$. The $\mathcal{G}^{(2)}_{D^X}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ term is expanded to be

$$\mathcal{G}^{(2)}_{D^X}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \frac{1}{2}\bigg(\mathcal{G}^{(2)}_{D^X}(|ij\rangle\langle ij|) - \mathcal{G}^{(2)}_{D^X}(|ij\rangle\langle ji|) + \mathcal{G}^{(2)}_{D^X}(|ji\rangle\langle ij|) - \mathcal{G}^{(2)}_{D^X}(|ji\rangle\langle ji|).\bigg) \tag{20}$$

This is calculated using Eqs. (16) and (17). As the right hand sides of both Eqs. (16) and (17) are invariant under the exchange of i and j, $\mathcal{G}^{(2)}_{D^X}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ is zero, which implies $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \mathcal{R}(|\psi_{ij}\rangle\langle\phi_{ij}|) = 0$.

Finally, we investigate $\mathcal{R}^\ell(|ii\rangle\langle ii|)$, $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$, and $\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$. Since we have

$$\mathcal{R}(\mathbb{L}_Z) = \frac{1}{d}\bigg[\big(1 - \frac{1}{d}\big)\big(\mathbb{I} + \mathbb{F}\big) + \frac{1}{d}\mathbb{L}_Z\bigg], \tag{21}$$

from Eq. (15), $\mathcal{R}(\mathbb{I}) = \mathbb{I}$, and $\mathcal{R}(\mathbb{F}) = \mathbb{F}$, it is observed from Eq. (15) that $\mathcal{R}^\ell(|ii\rangle\langle ii|)$ is a linear combination of $\mathbb{I} + \mathbb{F}$ and $\mathbb{L}_Z$. Using this fact, it is straightforward to obtain

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = \frac{1 - d^{-2\ell}}{d(d+1)}(\mathbb{I} + \mathbb{F}) + d^{-2\ell-1}\mathbb{L}_Z, \tag{22}$$

which is rewritten, in terms of $\Pi_{\mathrm{sym}} = \frac{1}{d(d+1)}(\mathbb{I} + \mathbb{F})$ and $\Lambda_Z = \frac{1}{d}\mathbb{L}_Z$, as

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = (1 - d^{-2\ell})\Pi_{\mathrm{sym}} + d^{-2\ell}\Lambda_Z. \tag{23}$$

Similarly, $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$ ($\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$) is given by a linear combination of $\mathbb{I} + \mathbb{F}$, $\mathbb{L}_Z$, and $\sum_{s>t} f_{st}^{ij} |\phi_{st}\rangle\langle\phi_{st}|$ ($\mathbb{I} - \mathbb{F}$ and $\sum_{s>t} f_{st}^{ij} |\psi_{st}\rangle\langle\psi_{st}|$). This can be seen to hold, since

$$\mathcal{R}\Big(\sum_{s>t} f_{st}^{ij} |\phi_{st}\rangle\langle\phi_{st}|\Big) = \frac{1}{d^2}\Big[\big(1 - \frac{2}{d}\big)\big(\mathbb{I} + \mathbb{F}\big) + \frac{2}{d}\mathbb{L}_Z\Big] + \frac{1}{d}\sum_{s>t}\sum_{k>l} f_{st}^{ij} f_{kl}^{st} |\phi_{kl}\rangle\langle\phi_{kl}| \tag{24}$$

$$= \frac{1}{d^2}\Big[\big(1 - \frac{2}{d}\big)\big(\mathbb{I} + \mathbb{F}\big) + \frac{2}{d}\mathbb{L}_Z\Big] + \frac{1}{d}\sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle\phi_{kl}|, \tag{25}$$

where we have used $\sum_{s>t} f_{st}^{kl} = 1$ and $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{kl}^{ij}$ due to Lemma 7, and similarly

$$\mathcal{R}\Big(\sum_{s>t} f_{st}^{ij} |\psi_{st}\rangle\langle\psi_{st}|\Big) = \frac{1}{d^2}\big(\mathbb{I} - \mathbb{F}\big) + \frac{1}{d}\sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle\psi_{kl}|. \tag{26}$$

Hence, to obtain $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$ and $\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$, we set

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|) = a_\ell^{(+)}(\mathbb{I} + \mathbb{F}) + b_\ell^{(+)}\mathbb{L}_Z + c_\ell^{(+)}\sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle\phi_{kl}| \tag{27}$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|) = a_\ell^{(-)}(\mathbb{I} - \mathbb{F}) + c_\ell^{(-)}\sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle\psi_{kl}|, \tag{28}$$

and derive the coefficients using their recurrence relations. From Eqs. (18) and (19), the coefficients for $n = 1$ are given by

$$a_1^{(+)} = \frac{1}{d^2}\big(1 - \frac{2}{d}\big), \quad b_1^{(+)} = \frac{2}{d^3}, \quad c_1^{(+)} = \frac{1}{d}, \tag{29}$$

$$a_1^{(-)} = \frac{1}{d^2}, \quad c_1^{(-)} = \frac{1}{d}. \tag{30}$$

From Eqs. (18), (19), (25), and (26), recurrence relations for $a_\ell^{(\pm)}$, $b_\ell^{(+)}$, and $c_\ell^{(\pm)}$ are given by

$$a_{\ell+1}^{(+)} = a_\ell^{(+)} + \frac{1}{d}\big(1 - \frac{1}{d}\big)b_\ell^{(+)} + \frac{1}{d^2}\big(1 - \frac{2}{d}\big)c_\ell^{(+)}, \quad b_{\ell+1}^{(+)} = \frac{b_\ell^{(+)}}{d^2} + \frac{2c_\ell^{(+)}}{d^3}, \quad c_{\ell+1}^{(+)} = \frac{c_\ell^{(+)}}{d}, \tag{31}$$

and

$$a_{\ell+1}^{(-)} = a_\ell^{(+)} + \frac{c_\ell^{(-)}}{d^2}, \quad c_{\ell+1}^{(-)} = \frac{c_\ell^{(-)}}{d}. \tag{32}$$

Solving these relations, we obtain

$$a_\ell^{(+)} = \frac{1}{d(d+1)} - \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell+1}(d^2 - 1)}, \quad b_\ell^{(+)} = \frac{2(d^\ell - 1)}{d^{2\ell+1}(d - 1)}, \quad c_\ell^{(+)} = d^{-\ell}, \tag{33}$$

and

$$a_\ell^{(-)} = \frac{1-d^{-\ell}}{d(d-1)}, \quad c_\ell^{(-)} = d^{-\ell}. \tag{34}$$

Thus, we have

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|) = \left(1 - \frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d-1)}\right)\Pi_{\mathrm{sym}} + 2\frac{d^\ell-1}{d^{2\ell}(d-1)}\Lambda_Z + \frac{1}{d^\ell}\sum_{k>l} f_{kl}^{ij}\,|\phi_{kl}\rangle\langle\phi_{kl}| \tag{35}$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|) = \big(1 - \frac{1}{d^\ell}\big)\Pi_{\mathrm{anti}} + \frac{1}{d^\ell}\sum_{k>l} f_{kl}^{ij}\,|\psi_{kl}\rangle\langle\psi_{kl}|\,. \tag{36}$$

This concludes the proof. ◀

We will also make use of upper and lower bounds of the diamond norm, in terms of a superoperator norm.

▶ **Lemma 9.** *Let $\mathcal{C}$ be a linear map from $\mathcal{B}(\mathcal{H})$ ($\mathrm{dim}\mathcal{H} = D$) to $\mathcal{B}(\mathcal{H}')$ ($\mathrm{dim}\mathcal{H}' = D'$). Then,*

$$\|\mathcal{C}\|_{1\to1} \leq \|\mathcal{C}\|_\diamond \leq \sqrt{DD'}\|\mathcal{C}\|_{1\to1}. \tag{37}$$

Lemma 9 is a well-known relation (see, e.g. [16]). Nevertheless, for the sake of completeness, we present a proof below.

Proof. The first inequality holds by definition. To show the second inequality, we use a property of a superoperator norm $\|\mathcal{E}\|_{1\to2}$ such that, for any map $\mathcal{E}$ acting on $\mathcal{B}(\mathcal{H}_K)$ where $\mathcal{H}_K$ is a K-dimensional Hilbert space, $\|\mathcal{E}\otimes\mathrm{id}_k\|_{1\to2} = \|\mathcal{E}\|_{1\to2}$ for $k \in \mathbf{N}$ [34]. It also satisfies the following chain of inequalities $\|\mathcal{E}\|_{1\to2} \leq \|\mathcal{E}\|_{1\to1} \leq \sqrt{K}\|\mathcal{E}\|_{1\to2}$ due to $\|X\|_2 \leq \|X\|_1 \leq \sqrt{K}\|X\|_2$ for $X \in \mathcal{B}(\mathcal{H}_K)$. Using these relations, we obtain

$$\|\mathcal{C}\|_\diamond = \|\mathcal{C}\otimes\mathrm{id_D}\|_{1\to1} \leq \sqrt{DD'}\|\mathcal{C}\otimes\mathrm{id_D}\|_{1\to2} = \sqrt{DD'}\|\mathcal{C}\|_{1\to2} \leq \sqrt{DD'}\|\mathcal{C}\|_{1\to1}. \tag{38}$$

◀

4.2 Proof of the main result

Proof. Now we can prove Theorem 5. To this end, we investigate $\|\mathcal{G}_{D[\ell]}^{(2)} - \mathcal{G}_{U_H}^{(2)}\|_{1\to1}$, where U_H is a Haar random unitary matrix. In terms of the operators $\rho \in \mathcal{B}(\mathcal{H}^{\otimes2})$ satisfying $\|\rho\|_1 = 1$, it is given by

$$\sup_{\substack{\rho\in\mathcal{B}(\mathcal{H}^{\otimes2})\\ \|\rho\|_1=1}} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1. \tag{39}$$

Note that ρ may be assumed to be Hermitian, but not necessarily positive semidefinite.

Due to Schur-Weyl duality [35], the latter term $\mathcal{G}_{U_H}^{(2)}(\rho)$ is given by

$$\mathcal{G}_{U_H}^{(2)}(\rho) = (\mathrm{tr}P_{\mathrm{sym}}\rho)\Pi_{\mathrm{sym}} + (\mathrm{tr}P_{\mathrm{anti}}\rho)\Pi_{\mathrm{anti}}. \tag{40}$$

On the other hand, the former term $\mathcal{G}^{(2)}_{D[\ell]}(\rho)$ is equal to $\mathcal{R}^\ell(\rho)$ since

$$\begin{aligned}\mathcal{G}^{(2)}_{D[\ell]}(\rho) &= \mathbb{E}_{D[\ell]}[(D[\ell])^{\otimes 2}\rho(D[\ell])^{\dagger\otimes 2}] &(41)\\ &= \prod_{i=\ell}^{1}\mathbb{E}_{D_i'^Z}\mathbb{E}_{D_i^X}\mathbb{E}_{D_i^Z}[\big(U_i'^Z D_i^X D_i^Z\big)^{\otimes 2}\rho\big(D_i'^Z D_i^X D_i^Z\big)^{\dagger\otimes 2}] &(42)\\ &= \left(\mathcal{G}^{(2)}_{D^Z}\circ\mathcal{G}^{(2)}_{D^X}\circ\mathcal{G}^{(2)}_{D^Z}\right)^\ell(\rho) &(43)\\ &= \mathcal{R}^\ell(\rho), &(44)\end{aligned}$$

where the second line is obtained using the fact that the random diagonal-unitary matrices are independent.

Due to Lemma 8, for all $\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2})$, we have

$$\begin{aligned}\mathcal{R}^\ell(\rho) = \big((1-d^{-2\ell})s_0 + a_\ell s_1\big)\Pi_{\mathrm{sym}} + (d^{-2\ell}s_0 + b_\ell s_1)\Lambda_Z + (1-d^{-\ell})s_2\Pi_{\mathrm{anti}}\\ + d^{-\ell}\sum_{i>j}\sum_{k>l} f^{ij}_{kl}\big(\rho_{\phi_{ij}}|\phi_{kl}\rangle\langle\phi_{kl}| + \rho_{\psi_{ij}}|\psi_{kl}\rangle\langle\psi_{kl}|\big), \quad (45)\end{aligned}$$

where a_ℓ and b_ℓ are given by Lemma 8, $\rho_{\phi_{ij}} = \mathrm{tr}\rho\,|\phi_{ij}\rangle\langle\phi_{ij}|$, $\rho_{\psi_{ij}} = \mathrm{tr}\rho\,|\psi_{ij}\rangle\langle\psi_{ij}|$, $s_0 = \mathrm{tr}\rho\mathbb{L}_Z$, $s_1 = \mathrm{tr}\rho(P_{\mathrm{sym}} - \mathbb{L}_Z)$, and $s_2 = \mathrm{tr}\rho P_{\mathrm{anti}}$. Using $\mathrm{tr}P_{\mathrm{sym}}\rho = s_0 + s_1$, this leads to

$$\begin{aligned}\mathcal{G}^{(2)}_{U_H}(\rho) - \mathcal{G}^{(2)}_{D[\ell]}(\rho) = \big(d^{-2\ell}s_0 + (1-a_\ell)s_1\big)\Pi_{\mathrm{sym}} - (d^{-2\ell}s_0 + b_\ell s_1)\Lambda_Z + d^{-\ell}s_2\Pi_{\mathrm{anti}}\\ - d^{-\ell}\sum_{i>j}\sum_{k>l} f^{ij}_{kl}\big(\rho_{\phi_{ij}}|\phi_{kl}\rangle\langle\phi_{kl}| + \rho_{\psi_{ij}}|\psi_{kl}\rangle\langle\psi_{kl}|\big). \quad (46)\end{aligned}$$

Since $\Pi_{\mathrm{sym}} = \frac{2}{d(d+1)}\big(\sum_i |ii\rangle\langle ii| + \sum_{i>j}|\phi_{ij}\rangle\langle\phi_{ij}|\big)$, $\Pi_{\mathrm{anti}} = \frac{2}{d(d-1)}\sum_{i>j}|\psi_{ij}\rangle\langle\psi_{ij}|$, and $\Lambda_Z = \frac{1}{d}\sum_i |ii\rangle\langle ii|$, Eq. (46) is already diagonal in the basis $B = \{|ii\rangle\}_{i=0}^{d-1}\cup\{|\phi_{ij}\rangle\}_{i>j}\cup\{|\psi_{ij}\rangle\}_{i>j}$. Thus, its 1-norm is exactly calculated to be

$$\begin{aligned}\|\mathcal{G}^{(2)}_{U_H}(\rho) - \mathcal{G}^{(2)}_{D[\ell]}(\rho)\|_1 = d\left|\frac{2}{d(d+1)}\big(d^{-2\ell}s_0 + (1-a_\ell)s_1\big) - \frac{1}{d}(d^{-2\ell}s_0 + b_\ell s_1)\right|\\ + \sum_{k>l}\left(\left|\frac{2}{d(d+1)}\big(d^{-2\ell}s_0 + (1-a_\ell)s_1\big) - d^{-\ell}\sum_{i>j}f^{ij}_{kl}\rho_{\phi_{ij}}\right| + \left|\frac{2}{d(d-1)}d^{-\ell}s_2 - d^{-\ell}\sum_{i>j}f^{ij}_{kl}\rho_{\psi_{ij}}\right|\right).\\ (47)\end{aligned}$$

The first term in Eq. (47) is simply equal to $\frac{|2s_1-(d-1)s_0|}{d^{2\ell}(d+1)}$, which is smaller than or equal to $\frac{2|s_1|+(d-1)|s_0|}{d^{2\ell}(d+1)}$ due to the triangle inequality. In the following, we evaluate upper and lower bounds of the second and the third terms.

The second term is bounded from above, again due to the triangle inequality, by

$$\sum_{k>l}\left(\frac{2}{d(d+1)}\big(d^{-2\ell}|s_0| + |1-a_\ell||s_1|\big) + d^{-\ell}\sum_{i>j}f^{ij}_{kl}|\rho_{\phi_{ij}}|\right), \quad (48)$$

where we have used the fact that f^{ij}_{kl} is non-negative. Substituting a_ℓ and using Lemma 7, i.e., $\sum_{k>l} f^{ij}_{kl} = 1$, it is bounded from above by

$$\frac{(d-1)|\mathrm{tr}\rho\mathbb{L}_Z|}{d^{2\ell}(d+1)} + \frac{(d^{\ell+1}+d^\ell-2)|\mathrm{tr}\rho(P_{\mathrm{sym}}-\mathbb{L}_Z)|}{d^{2\ell}(d+1)} + \frac{1}{d^\ell}\mathrm{tr}|\rho|(P_{\mathrm{sym}}-\mathbb{L}_Z). \quad (49)$$

Similarly, an upper bound of the third term in Eq. (47) is given by $\frac{1}{d^\ell}(|\mathrm{tr}\rho P_{\mathrm{anti}}| + \mathrm{tr}|\rho| P_{\mathrm{anti}})$.

From these upper bounds, an upper bound of $\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1$ is given as follows, using $|s_0| = |\mathrm{tr}\rho\mathbb{L}_Z| \leq \mathrm{tr}|\rho|\mathbb{L}_Z$, $|s_1| = |\mathrm{tr}\rho(P_{\mathrm{sym}} - \mathbb{L}_Z)| \leq \mathrm{tr}|\rho|(P_{\mathrm{sym}} - \mathbb{L}_Z)$, $|s_2| = |\mathrm{tr}\rho P_{\mathrm{anti}}| \leq \mathrm{tr}|\rho|P_{\mathrm{anti}}$, and $P_{\mathrm{sym}} + P_{\mathrm{anti}} = \mathbb{I}$,

$$\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1 \leq \frac{2(d-1)}{d^{2\ell}(d+1)}\mathrm{tr}|\rho|\mathbb{L}_Z + \frac{2}{d^\ell}\mathrm{tr}|\rho|(\mathbb{I} - \mathbb{L}_Z), \tag{50}$$

where we dropped the negative term $-\frac{2}{d^{2\ell}(d+1)}|\mathrm{tr}\rho(P_{\mathrm{sym}} - \mathbb{L}_Z)|$. Denoting $\mathrm{tr}|\rho|\mathbb{L}_Z$ and $\mathrm{tr}|\rho|(\mathbb{I} - \mathbb{L}_Z)$ by p_0 and p_1, respectively, we have

$$\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1 \leq \frac{2(d-1)}{d^{2\ell}(d+1)}p_0 + \frac{2}{d^\ell}p_1. \tag{51}$$

From this, we obtain an upper bound of $\sup_{\rho\in\mathcal{B}(\mathcal{H}^{\otimes 2}),\|\rho\|_1=1}\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1$. Since $\|\rho\|_1 = 1$ implies that p_0 and p_1 satisfy $p_0 + p_1 = 1$, and they are positive by definition, Eq. (51) is a convex sum of $\frac{2(d-1)}{d^{2\ell}(d+1)}$ and $\frac{2}{d^\ell}$, where the latter is larger than the former. Hence, the supremum is given by $(p_0, p_1) = (0, 1)$, resulting in

$$\sup_{\rho\in\mathcal{B}(\mathcal{H}^{\otimes 2}),\|\rho\|_1=1}\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1 \leq \frac{2}{d^\ell}. \tag{52}$$

A lower bound of $\sup_{\rho\in\mathcal{B}(\mathcal{H}^{\otimes 2}),\|\rho\|_1=1}\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1$ is obtained by substituting a specific instance of ρ given by $\Phi_{i_0j_0} := |\phi_{i_0j_0}\rangle\langle\phi_{i_0j_0}|$ $(i_0 > j_0)$, which gives

$$\|\mathcal{G}^{(2)}_{D[\ell]}(\Phi_{i_0j_0}) - \mathcal{G}^{(2)}_{U_H}(\Phi_{i_0j_0})\|_1 = \frac{2}{d^{2\ell}(d+1)} + \sum_{k>l}\left|\frac{2}{d(d+1)}\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d-1)} - \frac{1}{d^\ell}f^{i_0j_0}_{kl}\right|, \tag{53}$$

from Eq. (47). Since $f^{i_0j_0}_{kl}$ satisfies $f^{i_0j_0}_{kl} = 0, 2/d$ for any $k > l$ and $\sum_{k>l}f^{i_0j_0}_{kl} = 1$ from Lemma 7, the number of (k,l) $(k > l)$ for which $f^{i_0j_0}_{kl}$ is nonzero is $d/2$. Due to this fact, we can exactly calculate Eq. (53) as follows:

$$\begin{aligned}\|\mathcal{G}^{(2)}_{D[\ell]}(\Phi_{i_0j_0}) - \mathcal{G}^{(2)}_{U_H}(\Phi_{i_0j_0})\|_1 &= \frac{2}{d^{2\ell}(d+1)} + \frac{d}{2}\left|\frac{2}{d(d+1)}\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d-1)} - \frac{2}{d^{\ell+1}}\right| \\ &\quad + \left(\frac{d(d-1)}{2} - \frac{d}{2}\right)\frac{2}{d(d+1)}\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d-1)},\end{aligned} \tag{54}$$

which is simplified to be

$$\|\mathcal{G}^{(2)}_{D[\ell]}(\Phi_{i_0j_0}) - \mathcal{G}^{(2)}_{U_H}(\Phi_{i_0j_0})\|_1 = \frac{2}{d^\ell} - 2\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d^2-1)}. \tag{55}$$

Hence, we obtain

$$\sup_{\rho\in\mathcal{B}(\mathcal{H}^{\otimes 2}),\|\rho\|_1=1}\|\mathcal{G}^{(2)}_{D[\ell]}(\rho) - \mathcal{G}^{(2)}_{U_H}(\rho)\|_1 \geq \frac{2}{d^\ell} - 2\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d^2-1)} \geq \frac{2}{d^\ell}\left[1 - \frac{2d}{d^2-1}\right]. \tag{56}$$

From these bounds, we obtain, using Lemma 9, upper and lower bounds of $\mathcal{G}^{(2)}_{D[\ell]} - \mathcal{G}^{(2)}_{U_H}$ in terms of the diamond norm,

$$\frac{2}{d^\ell} - 2\frac{d^{\ell+1}+d^\ell-2}{d^{2\ell}(d^2-1)} \leq \|\mathcal{G}^{(2)}_{D[\ell]} - \mathcal{G}^{(2)}_{U_H}\|_\diamond \leq \frac{2}{d^{\ell-2}}. \tag{57}$$

This implies that $D[\ell]$ is not an ϵ-approximate unitary 2-design if $\ell \leq \frac{\log\epsilon^{-1}}{N}$, as the lower bound in Eq. (57) is strictly greater than $1/d^\ell$ if $d > 3$, and is an ϵ-approximate unitary 2-design if $\ell \geq 2 + \frac{1+\log\epsilon^{-1}}{N}$, and concludes the proof. ◀

5 Conclusion

We have proven that an approximate unitary 2-design can be achieved by alternately applying independent random Z- and X-diagonal unitary matrices. We have shown that one iteration of random Z- and X-diagonal unitary matrices is not sufficient, but it rapidly converges to an ϵ-approximate unitary 2-design after a number of iterations. We have also provided an implementation of our construction by a quantum circuit composed of $O\big(N(N+\log 1/\epsilon)\big)$ one- or two-qubit gates, most of which are diagonal in the Pauli-Z basis. This implementation is, in terms of the number of gates, as efficient as many of other constructions using the Clifford circuits and random quantum circuits. An advantage unique to our implementation is its simple form. As the diagonal part can be applied simultaneously and the non-commuting part is depth $O(1)$, the practical time for the implementation will be vastly reduced compared to other implementations. Further applications of random diagonal-unitary matrices for decoupling can be found in Ref. [23].

Acknowledgements. The authors are grateful to Reinhard F. Werner and Omar Fawzi for interesting and fruitful discussions. YN is a JSPS Research Fellow and is partially supported by JSPS Postdoctoral Fellowships for Research Abroad. CM acknowledge support from the EU grants SIQS and QFTCMPS and by the cluster of excellence EXC 201 Quantum Engineering and Space-Time Research. CH and AW are supported by the Spanish MINECO, project FIS2013-40627-P, as well as by the Generalitat de Catalunya, CIRIT project no. 2014 SGR 966. AW is further supported by the European Commission (STREP “RAQUEL”), the European Research Council (Advanced Grant “IRQUAT”) and the Spanish MINECO, project FIS2008-01236, with the support of FEDER funds.

References

1 P. Hayden, M. Horodecki, A. Winter, and J. Yard. A decoupling approach to the quantum capacity. *Open Syst. Inf. Dyn.*, 15:7, 2008.

2 A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols : Restructuring quantum information’s family tree. *Proc. R. Soc. A*, 465:2537, 2009.

3 N. Datta and M.-H. Hsieh. The apex of the family tree of protocols : optimal rates and resource inequalities. *New J. Phys.*, 13:093042, 2011.

4 C. Hirche and C. Morgan. Efficient achievability for quantum protocols using decoupling theorems. In *Proc. 2014 IEEE Int. Symp. Info. Theory*, page 536, 2014.

5 F. Dupuis. *The decoupling approach to quantum information theory.* PhD thesis, Université de Montréal, 2010. arXiv:1004.1641.

6 F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. One-shot decoupling. *Commun. Math. Phys.*, 328:251, 2014.

7 O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary approximate two-designs. *New J. Phys.*, 15:053022, 2013.

8 D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48:580, 2002.

9 C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, 2009.

10 G. Tóth and J. J. García-Ripoll. Efficient algorithm for multiqudit twirling for ensemble quantum computation. *Phys. Rev. A*, 75(4):042311, 2007.

11 D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *J. of Math. Phys.*, 48(5):052104, 2007.

12 W. G. Brown, Y. S. Weinstein, and L. Viola. Quantum pseudorandomness from cluster-state quantum computation. *Phys. Rev. A*, 77(4):040303(R), 2008.

13 Y. S. Weinstein, W. G. Brown, and L. Viola. Parameters of pseudorandom quantum circuits. *Phys. Rev. A*, 78(5):052332, 2008.

14 A. W. Harrow and R. A. Low. Random quantum circuits are approximate 2-designs. *Commun. Math. Phys.*, 291:257, 2009.

15 I. T. Diniz and D. Jonathan. Comment on “Random quantum circuits are approximate 2-designs". *Commun. Math. Phys.*, 304:281, 2011.

16 R. A. Low. *Pseudo-randomness and learning in quantum computation.* PhD thesis, University of Bristol, 2010. arXiv:1006.5227.

17 F. G. S. L. Brandao, A. W. Harrow, and M. Horodecki. Local random quantum circuits are approximate polynomial-designs, 2012. arXiv: 1208.0692.

18 R. Cleve, D. Leung, L. Liu, and C. Wang. Near-linear constructions of exact unitary 2-designs, 2015. arXiv:1501.04592.

19 Y. Nakata and M. Murao. Diagonal-unitary 2-designs and their implementations by quantum circuits. *Int. J. Quant. Inf.*, 11:1350062, 2013.

20 Y. Nakata and M. Murao. Diagonal quantum circuits: their computational power and applications. *Eur. Phys. J. Plus*, 129:152, 2014.

21 D. J. Shepherd and M. J. Bremner. Temporally unstructured quantum computation. *Proc. R. Soc. A*, 465:1413, 2009.

22 M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proc. R. Soc. A*, 467(2126):459, 2011.

23 Y. Nakata, C. Hirche, C. Morgan, and A. Winter, 2015. In preparation.

24 A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation.* American Mathematical Society Boston, MA, USA, 2002.

25 M. L. Metha. *Random Matrices.* Academic Press, Amsterdam San Diego Oxford London, 1990.

26 S. Popescu, A. J. Short, and A. Winter. Entanglement and the foundations of statistical mechanics. *Nature Physics*, 2:754, 2006.

27 P. Hayden and J. Preskill. Black holes as mirrors : quantum information in random subsystems. *J. High Energy Phys.*, 9:120, 2007.

28 Y. Nakata, P. S. Turner, and M. Murao. Phase-random states: Ensembles of states with fixed amplitudes and uniformly distributed phases in a fixed basis. *Phys. Rev. A*, 86(1):012301, 2012.

29 L. del Rio, A. Hutter, R. Renner, and S. Wehner. Relative thermalization, 2014. arXiv:1401.7997.

30 Y. Nakata, M. Koashi, and M. Murao. Generating a state t-design by diagonal quantum circuits. *New J. Phys.*, 16:053043, 2014.

31 N. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000.

32 R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.

33 R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A*, 68:022312, 2003.

34 J. Watrous. Notes on super-operator norms induced by Schatten norms, 2004. arXiv:quant-ph/0411077.

35 R. Goodman and N. R. Wallach. *Representations and Invariants of the Classical Groups.* Cambridge University Press, Cambridge, UK, 1999.

A Proof of Lemma 7

Proof. The statement $f^{ij}_{kl} = f^{kl}_{ij}$ follows from the definition of f^{ij}_{kl}. We first show that f^{ij}_{kl} is either 0 or $2/d$. As f^{ij}_{kl} is defined by $f^{ij}_{kl} = \frac{2}{d^3}\left(\sum_{\alpha=0}^{d-1} \alpha_i\alpha_j\alpha_k\alpha_l\right)^2$, we investigate $\sum_{\alpha=0}^{d-1}\alpha_i\alpha_j\alpha_k\alpha_l$. This is invariant even if Pauli X is applied on the m-th qubit for any $m \in [1, \cdots, N]$, which we denote by X_m, since

$$\sum_{\alpha=0}^{d-1}\alpha_i\alpha_j\alpha_k\alpha_l = d^2\sum_{\alpha=0}^{d-1}\langle\alpha|i\rangle\langle\alpha|j\rangle\langle\alpha|k\rangle\langle\alpha|l\rangle \tag{58}$$

$$= d^2\sum_{\alpha=0}^{d-1}\langle\alpha|\, X_m\, |i\rangle\,\langle\alpha|\, X_m\, |j\rangle\,\langle\alpha|\, X_m\, |k\rangle\,\langle\alpha|\, X_m\, |l\rangle\,. \tag{59}$$

This is due to $\langle\alpha|\, X_m = \pm\langle\alpha|$. Hence, we assume $|i\rangle = |0\rangle^{\otimes N}$ without loss of generality, resulting in $\alpha_i = 1$ for all α. The $\sum_{\alpha=0}^{d-1}\alpha_j\alpha_k\alpha_l$ still has another invariance, that is,

$$\sum_{\alpha=0}^{d-1}\alpha_j\alpha_k\alpha_l = d\sqrt{d}\sum_{\alpha=0}^{d-1}\langle\alpha|j\rangle\langle\alpha|k\rangle\langle\alpha|l\rangle \tag{60}$$

$$= d\sqrt{d}\sum_{\alpha=0}^{d-1}\langle\alpha|\, Z_m\, |j\rangle\,\langle\alpha|\, Z_m\, |k\rangle\,\langle\alpha|\, Z_m\, |l\rangle\,, \tag{61}$$

due to the summation over all α, where Z_m is the Pauli-Z operator acting on the m-th qubit. We then assume $\alpha_j = 1$ for $j = 0, \cdots, d/2-1$ and $\alpha_j = -1$ for $j = d/2, \cdots, d-1$ without loss of generality. This leads to

$$\sum_{\alpha=0}^{d-1}\alpha_i\alpha_j\alpha_k\alpha_l = \left(\sum_{\alpha=0}^{d/2-1} - \sum_{\alpha=d/2}^{d-1}\right)\alpha_k\alpha_l. \tag{62}$$

Denoting $|\alpha\rangle$ by $\left|\alpha^1\alpha^2\cdots\alpha^N\right\rangle$ $(\alpha^m = \pm)$, where $|\pm\rangle$ are the eigenbasis of the Pauli-X with eigenvalues ±1, respectively, and similarly denoting $|k\rangle$ and $|l\rangle$ in binary such as $|k_1\cdots k_N\rangle$ $(k_m = 0, 1)$, $(\sum_{\alpha=0}^{d/2-1} - \sum_{\alpha=d/2}^{d-1})\alpha_k\alpha_l$ is rewritten as

$$\sum_{\alpha_2,\cdots,\alpha_N=\pm}\Big(\langle +|k_1\rangle\langle +|l_1\rangle\langle\alpha_2\cdots\alpha_N|k_1\cdots k_N\rangle\langle\alpha_2\cdots\alpha_N|l_1\cdots l_N\rangle$$
$$- \langle -|k_1\rangle\langle -|l_1\rangle\langle\alpha_2\cdots\alpha_N|k_1\cdots k_N\rangle\langle\alpha_2\cdots\alpha_N|l_1\cdots l_N\rangle\Big). \tag{63}$$

When $k_1 = l_1$, this is simply zero. When $k_1 \neq l_1$, this is equal to $2^N = d$. Thus, $f^{kl}_{ij} \in \{0, 2/d\}$.

We next show $\sum_{k>l} f^{ij}_{kl} = 1$ for any $i > j$.

$$\sum_{k>l} f^{ij}_{kl} = \frac{2}{d^3}\sum_{k>l}\left(\sum_{\alpha}\alpha_i\alpha_j\alpha_k\alpha_l\right)^2 \tag{64}$$

$$= \frac{1}{d^3}\sum_{\alpha,\beta}\alpha_i\alpha_j\beta_i\beta_j\left(\sum_{k,l}\alpha_k\alpha_l\beta_k\beta_l - \sum_k \alpha_k^2\beta_k^2\right). \tag{65}$$

As $\sum_k \alpha_k^2 \beta_k^2 = d$ due to $\alpha_k = \pm 1$, we obtain

$$\frac{1}{d^3} \sum_{\alpha,\beta} \alpha_i \alpha_j \beta_i \beta_j \sum_k \alpha_k^2 \beta_k^2 = \frac{1}{d^2} \sum_{\alpha,\beta} \alpha_i \alpha_j \beta_i \beta_j \tag{66}$$

$$= \left(\sum_\alpha \langle i|\alpha\rangle\langle\alpha|j\rangle \right)^2 \tag{67}$$

$$= 0, \tag{68}$$

where we used that $i \neq j$ for the last line. Hence,

$$\sum_{k>l} f_{kl}^{ij} = \frac{1}{d^3} \sum_{\alpha,\beta} \alpha_i \alpha_j \beta_i \beta_j \left(\sum_k \alpha_k \beta_k \right)^2. \tag{69}$$

As $\sum_k \alpha_k \beta_k$ is given by $\frac{1}{d^2} \sum_k |\alpha\rangle\langle k| \, |k\rangle\langle\beta| = \frac{1}{d^2} \delta_{\alpha\beta}$, we obtain

$$\sum_{k>l} f_{kl}^{ij} = \frac{1}{d} \sum_{\alpha,\beta} \alpha_i \alpha_j \beta_i \beta_j \delta_{\alpha,\beta} = 1. \tag{70}$$

We finally show $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{kl}^{ij}$. To this end, we define a set Ξ_{ij} for $i > j$ by $\Xi_{ij} := \big\{(s,t) | s,t \in \{1, \cdots, N\}, s > t, f_{st}^{ij} = \frac{2}{d}\big\}$. Since $f_{kl}^{ij} \in \{0, 2/d\}$ and $\sum_{k>l} f_{kl}^{ij} = 1$ for any $i > j$, the number of elements in Ξ_{ij},denoted by $|\Xi_{ij}|$, is $d/2$. Due to the definition of f_{st}^{ij}, Ξ_{ij} is also given in terms of α_i's by $\Xi_{ij} = \big\{(s,t) | s,t \in \{1, \cdots, N\}, s > t, \forall \alpha \in [0, \cdots, d-1], \alpha_s \alpha_t = \alpha_i \alpha_j \big\}$. From this, it is observed that $\forall i > j$ and $\forall k > l$, Ξ_{ij} is either equal to Ξ_{kl} or has no intersection with Ξ_{kl}, i.e. $\Xi_{ij} \cap \Xi_{kl} = \emptyset$.

In terms of Ξ_{ij}, $f_{ij}^{kl} = \frac{2}{d} \delta_{kl \in \Xi_{ij}}$, where $\delta_{kl \in \Xi_{ij}} = 1$ if $(k,l) \in \Xi_{ij}$ and 0 otherwise. Note that, as $f_{ij}^{kl} = f_{kl}^{ij}$, $\delta_{kl \in \Xi_{ij}} = \delta_{ij \in \Xi_{kl}}$. Using this notation, we have

$$\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = \left(\frac{2}{d}\right)^2 \sum_{s>t} \delta_{st \in \Xi_{kl}} \delta_{st \in \Xi_{ij}} \tag{71}$$

$$= \left(\frac{2}{d}\right)^2 \sum_{s>t} \delta_{st \in \Xi_{kl} \cap \Xi_{ij}}. \tag{72}$$

When $\Xi_{kl} = \Xi_{ij}$, this is equal to $\frac{2}{d}$ as $|\Xi_{kl}| = d/2$. In this case, $f_{ij}^{kl} = \frac{2}{d} \delta_{kl \in \Xi_{ij}} = \frac{2}{d}$ since $(k,l) \in \Xi_{kl} = \Xi_{ij}$, implying $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{ij}^{kl}$. When $\Xi_{kl} \cap \Xi_{ij} = \emptyset$, Eq. (72) is equal to zero, and f_{ij}^{kl} is also zero by definition. Hence, $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{ij}^{kl}$ holds even in this case. Since Ξ_{ij} is either Ξ_{kl} or satisfies $\Xi_{ij} \cap \Xi_{kl} = \emptyset$, this concludes the proof. ◀

Round Elimination in Exact Communication Complexity

Jop Briët[1], Harry Buhrman[2], Debbie Leung[3], Teresa Piovesan[2], and Florian Speelman[2]

1 **Courant Institute**
New York University, 251 Mercer Street, New York NY 10012, USA
`jop.briet@cims.nyu.edu`

2 **Centrum Wiskunde & Informatica (CWI)**
Science Park 123, 1098 XG Amsterdam, The Netherlands
`{buhrman,piovesan,speelman}@cwi.nl`

3 **University of Waterloo**
200 University Ave W, Waterloo, Ontario N2L3G1, Canada
`wcleung@math.uwaterloo.ca`

Abstract

We study two basic graph parameters, the chromatic number and the orthogonal rank, in the context of classical and quantum exact communication complexity. In particular, we consider two types of communication problems that we call *promise equality* and *list* problems. For both of these, it was already known that the one-round classical and one-round quantum complexities are characterized by the chromatic number and orthogonal rank of a certain graph, respectively.

In a promise equality problem, Alice and Bob must decide if their inputs are equal or not. We prove that classical protocols for such problems can always be reduced to one-round protocols with no extra communication. In contrast, we give an explicit instance of a promise problem that exhibits an exponential gap between the one- and two-round exact quantum communication complexities. Whereas the chromatic number thus captures the complete complexity of promise equality problems, the hierarchy of "quantum chromatic numbers" (starting with the orthogonal rank) giving the quantum communication complexity for every fixed number of communication rounds thus turns out to enjoy a much richer structure.

In a list problem, Bob gets a subset of some finite universe, Alice gets an element from Bob's subset, and their goal is for Bob to learn which element Alice was given. The best general lower bound (due to Orlitsky) and upper bound (due to Naor, Orlitsky, and Shor) on the classical communication complexity of such problems differ only by a constant factor. We exhibit an example showing that, somewhat surprisingly, the four-round protocol used in the bound of Naor et al. can in fact be optimal. Finally, we pose a conjecture on the orthogonality rank of a certain graph whose truth would imply an intriguing impossibility of *round elimination* in quantum protocols for list problems, something that works trivially in the classical case.

1998 ACM Subject Classification F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Communication complexity, round elimination, quantum communication, protocols, chromatic numbers

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.206

1 Introduction

The chromatic number $\chi(G)$ of a graph G is the minimum number of colors needed to color the vertices in such a way that adjacent vertices get different colors. This important graph

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 206–225
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

parameter appears frequently in computer science and mathematics; it is well-known to be NP-hard to compute and has recently found a number of meaningful generalizations in the context of non-local games and entanglement-assisted zero-error information theory. One of those generalizations is the *orthogonal rank* of a graph, denoted $\xi(G)$ and defined as follows. An orthogonal representation of a graph is an assignment of complex unit vectors to the vertices such that adjacent vertices receive orthogonal vectors. The orthogonal rank is the minimum dimension of such a representation. Similar to the chromatic number, the orthogonal rank is NP-hard to compute, which follows from a result of Peeters [29, Theorem 3.1]. In this paper, we study both of these graph parameters in the context of communication complexity.

Classical communication complexity. Since its introduction by Yao [34] communication complexity has become a standard model in computational complexity that enjoys a wide variety of connections to other areas in theoretical computer science [22]. Here two parties, Alice and Bob, receive inputs x, y from sets $\mathcal{X}, \mathcal{Y}$ (resp.) and need to compute the value $f(x, y)$ of a two-variable function f known to them in advance. Usually each party has insufficient information to solve the problem alone, meaning they have to exchange information about each others' inputs. The idea that communication is expensive motivates the study of the *communication complexity* of f, which counts the minimal number of bits that the parties must exchange on worst-case inputs. Throughout this paper, we consider only exact (deterministic) communication protocols, and we will omit the word *exact* from now on. Of particular importance to this paper is the distinction between *one-round* protocols, where all communication flows from Alice to Bob, and *multi-round* protocols, where they take turns in sending messages from one party to the other.

Quantum communication complexity. In yet another celebrated paper, Yao [35] introduced *quantum communication complexity*, where to compute the value $f(x, y)$ the parties are allowed to transmit *qubits* back and forth. The study of this model has also become a well-established discipline in theoretical computer science and quantum information theory. The most basic question that arises when considering the classical and quantum models is whether they are actually substantially different. An upper bound on the possible difference between these models was proved by Kremer [21, Theorem 4].[1]

▶ **Theorem 1.1** (Kremer). *Any quantum protocol that uses ℓ qubits of communication can be turned into a $2^{O(\ell)}$-bit one-round classical protocol for the same problem.*

The first large gap between exact classical and quantum communication complexity was demonstrated by Buhrman, Cleve, and Wigderson [7], who gave a problem admitting a one-round quantum protocol that is exponentially more efficient than any (one- or multi-round) classical protocol.

The chromatic number and orthogonal rank naturally show up in two types of communication problems that we call *promise equality* and *list* problems, discussed next.

1.1 Promise equality

In a *promise equality problem*, Alice and Bob are either given equal inputs or a pair of distinct inputs from a subset $\mathcal{D}$ of $\binom{\mathcal{X}}{2}$ ($\mathcal{D}$ is known to them in advance). Their goal is to decide whether they have equal or different inputs.

[1] The result stated here is actually a slight generalization of Kremer's result (which focuses on boolean functions) that can be proved in the same way; for completeness we give a proof in Appendix A.

Classical complexity of promise problems. It was shown by de Wolf [11, Theorem 8.5.1] that if $G = (\mathcal{X}, \mathcal{D})$ is the graph with vertex set $\mathcal{X}$ and edge set $\mathcal{D}$, then the one-round classical communication of the problem equals $\lceil \log \chi(G) \rceil$. Analogously, for each positive integer r one can define a "level-r" chromatic number of the graph corresponding to the communication complexity of protocols that proceed in r rounds or less. For general communication problems, using more rounds can decrease the total communication, as is the case for the general Pointer Jumping Problem for example, where for every positive integer m there is an instance for which any m-round protocol requires exponentially more communication than the best $(m+1)$-round protocol [22]. However, we show that this is not true for promise equality problems (Lemma 2.1 below), meaning that for such problems the chromatic number not only gives rise to the one-round complexity, but their overall communication complexity.

Quantum complexity of promise problems. The one-round quantum communication complexity of promise equality problems is characterized by the orthogonal rank. It is not difficult to see that a one-round quantum protocol of a promise equality problem is equivalent to an orthogonal representation of the associated graph $G = (\mathcal{X}, \mathcal{D})$; the vectors correspond to the states that Alice would send to Bob and orthogonality is required for Bob's measurement to tell whether they got equal inputs or not. Viewing the orthogonal rank as the "one-round quantum chromatic number" of the graph G naturally leads one to define a hierarchy of such numbers where the level-r quantum chromatic number corresponds to the communication complexity of r-round quantum protocols. One might expect that, as in the classical case, this hierarchy is redundant in that the levels all carry the same number. However, one of our main results shows that in the quantum setting, this is *not* the case.

▶ **Theorem 1.2.** *There exist absolute constants $c, C \in (0, \infty)$ and an infinite family of promise equality problems $(\mathcal{X}_n, \mathcal{D}_n)_{n\in\mathbb{N}}$ such that:*

- *The one-round quantum communication complexity of $(\mathcal{X}_n, \mathcal{D}_n)$ is at least cn.*
- *There is a two-round quantum protocol for $(\mathcal{X}_n, \mathcal{D}_n)$ using at most $C \log n$ qubits.*

During our analysis of the particular promise problem used for Theorem 1.2 we answer an open question of Gruska, Qiu, and Zheng [18]. To explain this, we briefly elaborate on what goes into our result. The problem we consider is simple: Let n be a positive integer multiple of 8. Alice and Bob are given n-bit strings x and y, respectively, that are either equal or differ in exactly $n/4$ coordinates and they must distinguish between the two cases. We denote this problem by EQ-$\binom{n}{n/4}$. Similar promise equality problems were studied before. Buhrman, Cleve, and Wigderson [7] showed the first exponential gap between classical and quantum communication with the problem EQ-$\binom{n}{n/2}$, where Alice and Bob get n-bit strings that are either equal or differ in exactly half of the entries (for n a multiple of 4). They used a distributed version of the Deutsch–Jozsa algorithm to give a one-round $O(\log n)$-qubit quantum protocol for this problem, while a celebrated graph-theoretic result of Frankl and Rödl [14] implies that the classical communication complexity is at least $\Omega(n)$. Similar results were shown (based on similar techniques) in the above-mentioned paper [18] for the analogous problem EQ-$\binom{n}{\alpha n}$ when $\alpha > 1/2$, and the authors pose as an open problem to determine the quantum communication complexity of EQ-$\binom{n}{\alpha n}$ when $\alpha < 1/2$.

We show that the one-round quantum communication complexity of EQ-$\binom{n}{n/4}$ is at least $\Omega(n)$ and we give a two-round protocol for it that uses at most $O(\log n)$ qubits. For the proof of the first bound we use the famous Lovász theta number, which lower bounds the orthogonal rank and therefore the one-round quantum communication complexity. We prove a lower bound on the theta number using the theory of association schemes and known properties of the roots of the Krawtchouk polynomials. Our two-round protocol is based on a distributed version of Grover's algorithm. With a little extra technical work our results can be extended to any of the problems EQ-$\binom{n}{\alpha n}$ with constant $\alpha < 1/2$. In light of Kremer's Theorem and the obvious fact that the one-round classical communication complexity is at least its quantum counterpart, we thus settle the question of [18].

1.2 The list problem

In the *list problem*, inputs are picked from a subset $\mathcal{D} \subseteq \mathcal{X} \times \mathcal{Y}$ and the parties' goal is for Bob to learn Alice's input. The reason for the name "list problem" is that Bob's input y may just as well be given to him as the list (subset) of all of Alice's possible inputs x satisfying $(x, y) \in \mathcal{D}$. A list problem can thus equivalently be given by a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ of lists, where Bob gets a list $L \in \mathcal{L}$, Alice gets an element $x \in L$, and Bob must learn x. We refer to this communication problem as $\mathcal{L}$-LIST.

Classical complexity of list problems. Witsenhausen [33] observed that the one-round classical communication complexity of the list problem is characterized by the chromatic number of the graph with vertex set $\mathcal{X}$ and whose edge set consists of the pairs of distinct elements appearing together in some list $L \in \mathcal{L}$. Denoting this graph by $G_{\mathcal{L}}$, the one-round communication complexity equals $\lceil \log \chi(G_{\mathcal{L}}) \rceil$. The multi-round communication complexity of the list problem was also studied before. Orlitsky [28, Corollary 3 and Lemma 3] proved the following lower bound in terms of the chromatic number of $G_{\mathcal{L}}$, and the cardinality of the largest list, denoted $\omega(\mathcal{L}) = \max\{|L| : L \in \mathcal{L}\}$ (not to be confused with the cardinality of the largest clique $\omega(G_{\mathcal{L}})$ in the graph $G_{\mathcal{L}}$, which can be larger).

▶ **Theorem 1.3** (Orlitsky). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the classical communication complexity of $\mathcal{L}$-LIST is at least* $\max\{\log \log \chi(G_{\mathcal{L}}), \log \omega(\mathcal{L})\}$.

The basic idea behind the above result is that Alice must send sufficient information for Bob to be able to distinguish among $\omega(\mathcal{L})$ elements, and that any multi-round protocol can be simulated by a one-round protocol with at most an exponential difference in communication. In the same work, Orlitsky [28, Theorem 4] gave a two-round classical protocol based on perfect hashing functions that nearly achieves the above lower bound.

▶ **Theorem 1.4** (Orlitsky). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the two-round classical communication complexity of $\mathcal{L}$-LIST is at most* $\log \log \chi(G_{\mathcal{L}}) + 3 \log \omega(\mathcal{L}) + 4$.

It thus follows from Witsenhausen's observation and Theorem 1.4 that list problems have exponentially more efficient two-round protocols than one-round protocols. But Theorem 1.3 shows that—in stark contrast with the Pointer Jumping Problem—using more than two rounds cannot decrease the total amount of communication by more than a factor of 4, since obviously $\log \log \chi(G_{\mathcal{L}}) + 3 \log \omega(\mathcal{L}) \leq 4 \max\{\log \log \chi(G_{\mathcal{L}}), \log \omega(\mathcal{L})\}$. The natural question that thus arises is if the lower bound of Theorem 1.3 can be attained by using more than two rounds of communication. Towards answering this question, Naor, Orlitsky, and Shor [27, Corollary 1] slightly improved on Theorem 1.4 and showed that the four-round communication complexity gets to within a factor of about 3 of the lower bound.

▶ **Theorem 1.5** (Naor–Orlitsky–Shor). *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the four-round classical communication complexity of $\mathcal{L}$-LIST is at most* $\log \log \chi(G_{\mathcal{L}}) + 2 \log \omega(\mathcal{L}) + 3 \log \log \omega(\mathcal{L}) + 7$.

As our contribution to this line of work we show that, surprisingly, for some list problems the four-round protocol of Naor, Orlitsky, and Shor is in fact asymptotically optimal, thus answering the above question in the negative.

▶ **Theorem 1.6.** *For any $\varepsilon > 0$ there exists a set $\mathcal{X}$ and a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ such that the classical communication complexity of $\mathcal{L}$-*LIST *is at least* $\log\log\chi(G_{\mathcal{L}}) + (2-\varepsilon)\log\omega(\mathcal{L})$. *Moreover, there exists such an $(\mathcal{X}, \mathcal{L})$ pair for which $\omega(\mathcal{L}) = \log\chi(G_{\mathcal{L}})$.*

In particular, our result gives a family of list problems with communication complexity at least $(3-\varepsilon)\max\{\log\log\chi(G_{\mathcal{L}}), \log\omega(\mathcal{L})\}$ for any $\varepsilon > 0$.

Quantum complexity of list problems and quantum round elimination. The one-round quantum communication complexity of list problems is given by $\lceil\log\xi(G_{\mathcal{L}})\rceil$, which follows from the same considerations as for the promise equality problems (see Lemma 3.4). Based on a conjecture we make about the orthogonal rank of a certain family of graphs, we believe that in the context of quantum communication complexity, list problems may have the interesting property of resisting a quantum analogue of *round elimination*.

In classical communication complexity, round elimination reduces the number of rounds of a given protocol by having the parties send some extra information instead. Consider the following basic example, where we start with a two-round $(\log n + 1)$-bit protocol in which Bob starts by sending Alice a single bit and Alice replies with an $\log n$-bit string. This protocol can easily be turned into a *one-round* $2\log n$-bit protocol by having Alice directly send Bob two $\log n$-bit strings, one corresponding to the case where Bob sends a 0 in the two-round protocol and another for if he sends a 1. Then Bob can just pick the string corresponding to the bit he would have sent based on his input and solve the problem.

A quantum analogue of the above example would turn a two-round $(\log n + 1)$-qubit protocol into a one-round $2\log n$-qubit protocol. We conjecture that the following family of list problems is a counterexample to the existence of such an analogue. For an even positive integer n and $d \in [n]$, let $\mathcal{L}_d \subseteq 2^{\{0,1\}^n}$ be the family of all lists $L \subseteq \{0,1\}^n$ of maximal cardinality such that all strings in L have Hamming distance exactly d. The example we consider is given by the family $\mathcal{K} = \mathcal{L}_{n/2} \cup \cdots \cup \mathcal{L}_n$. Similar to the classical example above, we give a simple two-round protocol for $\mathcal{K}$-LIST.

▶ **Theorem 1.7.** *For $\mathcal{K} \subseteq 2^{\{0,1\}^n}$ as above, there exists a two-round protocol for $\mathcal{K}$-*LIST *where Bob sends Alice a single qubit and Alice replies with a $(1 + \log n)$-qubit message.*

It is easy to see that the graph $G_{\mathcal{K}} = (\{0,1\}^n, E)$ associated with $\mathcal{K}$ has edge set E given by all pairs of strings with Hamming distance in $\{n/2, \ldots, n\}$.

▶ **Conjecture 1.8.** *The graph $G_{\mathcal{K}}$ as above satisfies $\xi(G_{\mathcal{K}}) \geq n^{\omega(1)}$.*

By the relation between the one-round quantum communication complexity of list problems and the orthogonal rank of their associated graphs, it follows that the validity of the above conjecture would imply that the exact one-round quantum communication complexity of the above problem is super-logarithmic in n, in marked contrast with the classical example of round elimination.

1.3 Connections to other work

Our work strengthens a link between communication complexity and graph theory established by de Wolf [11]. Orthogonal representations appear in the context of zero-error information theory. Indeed they were introduced by Lovász [26] to settle a famous problem of Shannon concerning the (classical) capacity of the 5-cycle and they serve as proxies for entanglement-assisted schemes [8, 9, 24, 5, 6, 10]. They also appear in the context of non-local games [8, 16, 31]. Nevertheless the orthogonal rank is poorly understood. To the best of our knowledge, our result is the first time a *lower bound* on the dimension was used. The use of the Lovász theta number in the context of communication complexity problems also appears to be new and we hope that it may find further applications there in the future. Finally, quantum variants of the chromatic number that appeared in for example non-local games [8, 31] and zero-error information theory [6, 10] can be interpreted as quantum communication complexities of promise equality problems in various different communication models, which puts those parameters in a more unified framework.

Outline of the paper. In Section 2 we study the promise equality problem and in particular we prove Theorem 1.2. In Section 3 we discuss the list problem and prove Theorem 1.6 and Theorem 1.7.

2 Promise Equality

Recall that in a promise equality problem, Alice and Bob each receive an input from a set $\mathcal{X}$ with the promise that their inputs either are equal or come from a subset $\mathcal{D}$ of $\binom{\mathcal{X}}{2}$ (known to the players beforehand). The goal is to distinguish between the two cases. To any promise equality problem, we associate the graph $G = (\mathcal{X}, \mathcal{D})$.

2.1 General properties of promise equality

Recall that the one-round classical communication complexity of the problem equals $\lceil \log \chi(G) \rceil$. We begin by proving that the chromatic number of the associated graph actually gives the overall communication complexity.

▶ **Lemma 2.1.** *For any promise equality problem, the classical communication complexity is attained with a single round of communication.*

Proof. We show how to transform a k-round communication protocol into a one-round protocol that uses the same amount of bits. To summarize, the idea is that Alice mimics all the rounds of communication assuming that her input is equal to Bob's one, and sends them in one-round. He then checks whether the message received is consistent with his input. If this is not the case, then he knows that the two strings are different, otherwise he completes the protocol.

More formally, fix an optimal protocol P that requires k rounds, where $k \geq 2$. Suppose that Alice has input x and Bob has y. We assume that the first round of communication is from Alice to Bob, but the same reasoning applies in the other case. For i odd, let a_i be the message that Alice would send to Bob on the i-th round of communication if she followed protocol P and used the knowledge of the messages exchanged in the previous rounds and of her input x. Similarly, for i even, let $\hat{b}_i$ be the message that Bob would send to Alice on the i-th round of communication if he had $y = x$ as input, followed the protocol P and used the knowledge derived by the previous rounds. Using the protocol P, Alice can mimic Bob's rounds of communication under the assumption that Bob's input is equal to x. Alice uses her input x to produce the string $a_1\hat{b}_2a_3 \ldots a_i\hat{b}_{i+1} \ldots a_k$ and sends it to Bob in one round. From his input y, Bob constructs the messages b_i that he would have produced during the protocol P, with the knowledge of Alice's messages a_ℓ and his messages b_ℓ for all $\ell < i$. If there exists an index i such that $b_i \neq \hat{b}_i$, then x must be different from y. Otherwise, Bob uses the transcript $a_1\hat{b}_2a_3 \ldots a_i\hat{b}_{i+1} \ldots a_k$ to finish the protocol and either outputs $x = y$ or $x \neq y$. We have constructed a one-round communication protocol $\hat{P}$ whose worst-case transcript length is at most as long as the one of the original protocol P. Since P is an optimal protocol so must be $\hat{P}$. ◀

As already mentioned, de Wolf [11, Theorem 8.5.2] showed that one-round quantum protocols are related to orthogonal representations. We include a proof here for completeness.

▶ **Theorem 2.2** (de Wolf). *Consider a promise equality problem defined by the sets $\mathcal{X}$ and $\mathcal{D}$, then its one-round quantum communication complexity is equal to $\lceil \log \xi(G) \rceil$, where $G = (\mathcal{X}, \mathcal{D})$.*

The proof of the above result uses the following standard lemma (see for example [6]).

▶ **Lemma 2.3** (Orthogonality Lemma). *Let $\rho_1, \ldots, \rho_\ell \in \mathbb{C}^{d\times d}$ be a collection of Hermitian positive semidefinite matrices. Then the following are equivalent:*

1. *We have $\rho_i \rho_j = 0$ for every $i \neq j \in [\ell]$.*
2. *There exists a measurement consisting of positive semidefinite matrices $P^1, \ldots, P^\ell$, $P^\perp \in \mathbb{C}^{d\times d}$ such that $\mathsf{Tr}(P^i \rho_j) = \delta_{ij}\, \mathsf{Tr}(\rho_j)$ and $\mathsf{Tr}(P^\perp \rho_j) = 0$ for every $i, j \in [\ell]$.*

In particular, a collection of pure states $|\phi_1\rangle, \ldots, |\phi_\ell\rangle \in \mathbb{C}^d$ can be perfectly distinguished with a quantum measurement if and only if they are pairwise orthogonal.

Proof of Theorem 2.2. Let P be an optimal one-round protocol for the considered promise equality problem. Without loss of generality, Alice sends pure state $|\phi_x\rangle \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. For any pair $(x, y) \in \mathcal{D}$, $|\phi_x\rangle$ and $|\phi_y\rangle$ have to be perfectly distinguishable and therefore, in view of Lemma 2.3, they must be orthogonal. Hence, the map $\phi : \mathcal{X} \to \mathbb{C}^d$ where $\phi(x) = |\phi_x\rangle$ is a d-dimensional orthonormal representation of $G = (\mathcal{X}, \mathcal{D})$ and $\xi(G) \leq d$.

On the other hand, let ϕ be a d-dimensional orthonormal representation of the graph $G = (\mathcal{X}, \mathcal{D})$ and consider the one-round quantum protocol that transmits $\phi(x) \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. This uses $\log d$-qubits of communication. From Lemma 2.3 we know that Bob can use his input y to perform a quantum measurement that allows him to learn whether his input is equal or not to Alice's one. Thus, the one-round quantum communication complexity of this equality problem is at most $\lceil \log \xi(G) \rceil$. ◀

2.2 Proof of Theorem 1.2

The rest of this section will be devoted to the proof of Theorem 1.2, which shows that there is a family of promise equality problems where allowing two rounds of quantum communication is exponentially more efficient than a single round. The problem that exhibits this separation is EQ-$\binom{n}{n/4}$, where Alice and Bob each receive a n-bit string that are either equal or differ in exactly $n/4$ positions (with n multiple of 8). We denote by $H(n, n/4)$ the graph associated with this problem. For any $n, d \in \mathbb{N}$, let $H(n, d)$ be the graph which has all the n-bit strings as vertex set, such that two vertices are adjacent if their Hamming distance is d. We split the proof in two parts: in Section 2.2.1 we bound the one-round quantum communication complexity and in Section 2.2.2 we give the two-round protocol.

2.2.1 One-round quantum communication complexity of EQ-$\binom{n}{n/4}$

The main result of this section is the following theorem.

▶ **Theorem 2.4.** *The one-round quantum communication complexity of* EQ-$\binom{n}{n/4}$ *is at least $\Omega(n)$.*

To prove Theorem 2.4, we use Theorem 2.2 and thus set out to bound the orthogonal rank of the graph $H(n, n/4)$. We prove the desired bound in three steps: first, we show that the Lovász theta number is a lower bound for the orthogonal rank; second, we use structural properties of $H(n, n/4)$ together with known properties of the theta number to reformulate this bound in terms of the eigenvalues of the adjacency matrix of this graph; third, we bound the eigenvalues to get the desired result.

We remark that in the following proofs we consider a more general situation than just the graph $H(n, n/4)$. Indeed, the statement of Theorem 2.4 holds for any problem EQ-$\binom{n}{\alpha n}$ where $\alpha \in (0, 1/2)$ and where both n and $\alpha \cdot n$ are even.

Step 1: The Lovász theta number. This parameter was introduced by Lovász [26] to upper bound the Shannon capacity of a graph. Among its many equivalent definitions, we will use the following primal and dual formulations:

$$\begin{aligned} \vartheta(G) &= \max \sum_{i,j \in V(G)} X_{ij} \quad \text{s.t.} \quad X \succeq 0, \quad \mathsf{Tr}(X) = 1, \quad X_{ij} = 0 \quad \forall ij \in E(G), \\ \vartheta(G) &= \min t \quad \text{s.t.} \quad X \succeq 0, \quad X_{ii} = t - 1 \quad \forall i \in V(G), \quad X_{ij} = -1 \quad \forall ij \in E(\overline{G}), \end{aligned} \tag{1}$$

where $X \succeq 0$ means that X is a symmetric positive semidefinite matrix. The graph $\overline{G}$, called the complement of a graph G, has the same vertex set as the original graph and a pair of vertices is adjacent if and only if it is non adjacent in G.

Lovász [26] proved that ϑ lower bounds the minimum dimension of an orthonormal representation where the vectors are real valued. Note that this is slightly different from our setting where we allow the vectors to have complex entries. However, we show that the Lovász theta number is also a lower bound for $\xi(G)$. The proof is an adaptation to the complex case of a known proof [23].

▶ **Lemma 2.5.** *For any graph G, we have $\xi(G) \geq \vartheta(\overline{G})$.*

Proof. Let $n = |V(G)|$ and label the vertices of the graph G by $\{1, 2, \ldots, n\}$. Suppose that the orthogonal rank of G is equal to d and that $u_1, \ldots, u_n \in \mathbb{C}^d$ are the unit vectors forming an orthogonal representation of G. For every vertex of the graph $i \in [n]$, define a matrix $U_i := u_i u_i^\dagger$ and $U_0 := I_d$. Let Z be a $(n+1) \times (n+1)$ matrix where the i,j-th entry $Z_{ij} := \langle U_i, U_j \rangle = \mathsf{Tr}(U_j^\dagger U_i)$ for every $i, j \in \{0\} \cup [n]$. Notice that Z is positive semidefinite since it is the Gram matrix of a set of complex vectors. Moreover, Z is real valued and we get that $Z_{00} = d$, $Z_{0i} = \langle I, u_i u_i^\dagger \rangle = 1$ and $Z_{ii} = \langle u_i u_i^\dagger, u_i u_i^\dagger \rangle = (u_i^\dagger u_i)^2 = 1$ for all $i \in V(G)$ and that $Z_{ij} = (u_i^\dagger u_j)(u_j^\dagger u_i) \geq 0$ for all $i, j \in V(G)$ with equality if $ij \in E(G)$. By taking the Schur complement[2] in Z with respect to the entry Z_{00}, we obtain a new symmetric positive semidefinite matrix X with $X_{ii} = 1 - 1/d$ for all $i \in V(G)$ and $X_{ij} = -1/d$ for all $ij \in E(G)$. Rescaling X by d, we get a feasible solution for the minimization program in (1) of $\vartheta(\overline{G})$ with value d. We conclude that $d = \xi(G) \geq \vartheta(\overline{G})$. ◀

Step 2: Eigenvalue bound on the theta number. In the second step we show the following useful bound on the theta number of the graph $H(n, d)$ in terms of the eigenvalues of its

[2] Let X be a symmetric matrix of the form $X = \begin{pmatrix} \alpha & b^T \\ b & A \end{pmatrix}$, where $b \in \mathbb{R}^{n-1}$ and $\alpha > 0$. X is positive semidefinite if and only if $A - bb^T/\alpha$ is positive semidefinite. The matrix $A - bb^T/\alpha$ is called the Schur complement in X with respect to the entry α.

adjacency matrix. For the remainder of this step, by the eigenvalues of a graph we mean the eigenvalues of its adjacency matrix.

▶ **Lemma 2.6.** *For every positive integer n and $d \in [n]$, we have $\vartheta(\overline{H(n,d)}) \geq 1 - \binom{n}{d}/\lambda_{\text{MIN}}$, where λ_{MIN} is the smallest eigenvalue of $H(n,d)$.*

The proof of the above lemma uses the fact that for graphs with certain structural properties, the Lovász theta number is characterized by their eigenvalues. Let us recall the following standard definitions. Let $G = (V, E)$ be a graph. A permutation $\pi : V \to V$ is *edge preserving* if for every edge $\{u, v\} \in E$, we have $\{\pi(u), \pi(v)\} \in E$. The graph G is *vertex-transitive* if for every pair of vertices $u, v \in V$ there is an edge-preserving permutation $\pi : V \to V$ such that $\pi(u) = v$. Moreover, G is *edge-transitive* if for every pair of edges $\{u_1, v_1\}, \{u_2, v_2\} \in E$, there is an edge-preserving permutation $\pi : V \to V$ such that $\pi(u_1) = u_2$ and $\pi(v_1) = v_2$. Lovász [26] showed that if a graph is both vertex- and edge-transitive, then the theta number is given by a simple formula involving its eigenvalues.

▶ **Lemma 2.7** (Lovász). *For a positive integer n let G be an n-vertex graph with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. If G is both vertex- and edge-transitive, then $\vartheta(\overline{G}) = 1 - \lambda_1/\lambda_n$.*

Proof of Lemma 2.6. We start by showing that $H(n,d)$ is vertex-transitive. Given any pair of vertices $u, v \in \{0,1\}^n$ of $H(n,d)$, consider the automorphism of the graph $H(n,d)$ that maps $x \mapsto x \oplus u \oplus v$ where $\oplus$ is the bit-wise addition. This map preserves the Hamming distance, and therefore the adjacencies, between the vertices and sends $u \mapsto v$. Hence $H(n,d)$ is vertex-transitive.

To show that $H(n,d)$ is edge-transitive, fix any two edges uv and st and let $p = u \oplus v$, $q = s \oplus t$. Noting that the n-bit strings p and q have the same Hamming weight d, let π be a permutation of the indices such that $\pi(p) = q$. We define ν to be an automorphism that sends a vertex x to $\pi(x \oplus u) \oplus s$. The map ν preserves the edges of $H(n,d)$ and, since the permutation π maps the all-zero string to itself and p to q, we have that $\nu(u) = s$ and $\nu(v) = t$. Hence, $H(n,d)$ is edge-transitive.

Finally, since the largest eigenvalue of a vertex-transitive graph is equal to its degree, we clearly have $\lambda_1(H(n,d)) = \binom{n}{d}$. The result now follows from Lemma 2.7. ◀

Step 3: Bound on the smallest eigenvalue of $H(n,d)$. Finally, we prove an upper bound on the magnitude of the smallest eigenvalue of $H(n,d)$.

▶ **Lemma 2.8.** *Let d and n be even positive integers such that $d < n/2$. Then, the smallest eigenvalue λ_{MIN} of the graph $H(n,d)$ is a negative number such that*

$$|\lambda_{\text{MIN}}| \leq \sqrt{\frac{2^n \binom{n}{d}}{\binom{n}{n/2 - \sqrt{d(n-d)}}}}.$$

The proof of the lemma uses the following facts from coding theory that can be found in the survey [12]. The eigenvalues of $H(n,d)$ play a fundamental role in the theory of Hamming association schemes, where they are expressed in terms of a set of orthogonal polynomials known as the (binary) *Krawtchouk polynomials*. For a positive integer n and $d = 0, 1, \ldots, n$, the Krawtchouk polynomial $K_d^n \in \mathbb{R}[x]$ is a degree-d polynomial that is uniquely defined by

$$K_d^n(x) = \sum_{j=0}^{d} (-1)^j \binom{x}{j} \binom{n-x}{d-j}, \qquad x = 0, 1, \ldots, n.$$

When n and d are even, then K_d^n is symmetric about the point $x = n/2$. Moreover, these polynomials satisfy the important orthogonality relation

$$\sum_{x=0}^{n} \binom{n}{x} K_d^n(x) K_{d'}^n(x) = \delta_{d,d'} \binom{n}{d} 2^n. \tag{2}$$

The set of distinct eigenvalues of $H(n,d)$ turns out to be $\{K_d^n(0), K_d^n(1), \dots, K_d^n(n)\}$. Crucial to our proof of Lemma 2.8 then, is the following result of Levenshtein [25, Theorem 6.1] characterizing the smallest roots of the Krawtchouk polynomials.

▶ **Theorem 2.9** (Levenshtein). *Let n be a positive integer and $d \in [n]$. Then, K_d^n has exactly d distinct roots and its smallest root is given by*

$$n/2 - \max_z \Big(\sum_{i=0}^{d-2} z_i z_{i+1} \sqrt{(i+1)(n-i)} \Big), \tag{3}$$

where the maximum is over all vectors $z = (z_0, \dots, z_{d-1})$ on the real Euclidean unit sphere.

This implies the following general bound on the location of the smallest root of K_d^n. The bound is stated for instance in [20], but since we were unable to find a published proof we include one here for completeness.

▶ **Corollary 2.10.** *Let n and d be positive integers such that $d < n/2$. Then, the smallest root of K_d^n lies in the interval $\big[n/2 - \sqrt{(n-d)d}, n/2\big]$.*

Proof. It is clear that (3) is trivially upper bounded by $n/2$. We focus on the lower bound. To this end, let $z = (z_0, \dots, z_{d-1})$ be a real unit vector achieving the maximum in (3). For $i \in \{0, 1, \dots, d-1\}$ define the numbers $a_i = z_i\sqrt{n-i}$ and $b_i = z_{i+1}\sqrt{i+1}$. By the Cauchy-Schwarz inequality,

$$\begin{aligned}
\Big(\sum_{i=0}^{d-2} z_i z_{i+1} \sqrt{(i+1)(n-i)} \Big)^2 &= \Big(\sum_{i=0}^{d-2} a_i b_i \Big)^2 \\
&\leq \Big(\sum_{i=0}^{d-2} a_i^2 \Big) \Big(\sum_{j=0}^{d-2} b_j^2 \Big) \\
&= \Big(\sum_{i=0}^{d-2} a_i^2 \Big) \Big(\sum_{j=1}^{d-1} b_{j-1}^2 \Big) \\
&\leq \Big(\sum_{i=0}^{d-1} a_i^2 \Big) \Big(\sum_{j=0}^{d-1} b_{j-1}^2 \Big) \\
&= \Big(\sum_{i=0}^{d-1} z_i^2 (n-i) \Big) \Big(\sum_{j=0}^{d-1} z_j^2 j \Big) \\
&= \Big(n - \sum_{i=0}^{d-1} z_i^2 i \Big) \Big(\sum_{j=0}^{d-1} z_j^2 j \Big),
\end{aligned} \tag{4}$$

where in the last equality we used the fact that z is a unit vector. Observe that the sum $\sum_{i=0}^{d-1} z_i^2 i$ lies in the interval $[0, d-1]$. Hence, since $d < n/2$, (4) is at most $\max\{(n-t)t : t \in [0, d-1]\} = (n-(d-1))(d-1) \leq (n-d)d$. ◀

Proof of Lemma 2.8. Since the trace of a matrix equals the sum of its eigenvalues and the trace of an adjacency matrix is zero, it follows that $\lambda_{\text{MIN}} < 0$.

Recall that the eigenvalues of $H(n,d)$ belong to the set $\{K_d^n(x) : x = 0, 1, \ldots, n\}$. Moreover, since by our assumption n and d are even, the polynomial K_d^n is symmetric about the point $n/2$. Also observe that $K_d^n(0) > 0$ and hence the first time this polynomial assumes a negative value is somewhere beyond its smallest root, i.e. the smallest x for which $K_d^n(x) < 0$ lies in between the smallest root and $n/2$. It therefore follows from Corollary 2.10 and from the fact that K_d^n is symmetric about the point $n/2$ that $\lambda_{\text{MIN}} = K_d^n(x^\star)$ for some integer $x^\star \in [n/2 - \sqrt{(n-d)d}, n/2]$.

Clearly (2) implies that

$$\sum_{x=0}^{n} \binom{n}{x} K_d^n(x)^2 = \binom{n}{d} 2^n.$$

Hence,

$$\binom{n}{x^\star} K_d^n(x^\star)^2 \leq \binom{n}{d} 2^n$$

and we can conclude that

$$|\lambda_{\text{MIN}}|^2 = |K_d^n(x^\star)|^2 \leq \frac{2^n \binom{n}{d}}{\binom{n}{x^\star}} \leq \frac{2^n \binom{n}{d}}{\binom{n}{n/2-\sqrt{(n-d)d}}}. \qquad ◀$$

Putting everything together. To conclude this section, we combine the main lemmas of the above three steps to prove Theorem 2.4.

Proof of Theorem 2.4. Combining Lemmas 2.5, 2.6, and 2.8 gives

$$\xi(H(n,d)) \geq \vartheta\big(\overline{H(n,d)}\big) \geq 1 - \binom{n}{d}/\lambda_{\text{MIN}} \geq 1 + \sqrt{\frac{\binom{n}{d}\binom{n}{n/2-\sqrt{(n-d)d}}}{2^n}}. \tag{5}$$

We take the logarithm and use Stirling's approximation: $\log \binom{n}{k} = \big(H(k/n) + o(1)\big)n$, where $H(\epsilon) = -\epsilon \log(\epsilon) - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function and the $o(1)$ term goes to zero as $n \to \infty$ (see for example [32, p. 64]). Then, for $\alpha = d/n$, logarithm of (5) is at least

$$\frac{1}{2} \log \left(\frac{\binom{n}{d}\binom{n}{n/2-\sqrt{(n-d)d}}}{2^n} \right) = \frac{n}{2} \left(H(\alpha) + H\left(1/2 - \sqrt{(1-\alpha)\alpha}\right) - 1 + o(1) \right).$$

A simple check gives that $H(\alpha) + H(1/2 - \sqrt{(1-\alpha)\alpha}) - 1 > 0$ for any $\alpha \in (0, 1/2)$. In particular, $\log \xi(H(n, n/4)) \geq \Omega(n)$. ◀

2.2.2 Two-round quantum communication

Using a distributed version of Grover's search algorithm, we find a quantum communication protocol that solves EQ-$\binom{n}{n/4}$ with a logarithmic number of qubits.

▶ **Theorem 2.11.** *The two-round quantum communication complexity of* EQ-$\binom{n}{n/4}$ *is at most* $2\lceil \log n \rceil + 1$ *qubits.*

Proof. Let x and y be the inputs of Alice and Bob, respectively, and $z = x \oplus y$ be their bit-wise addition. The promise ensures that either $|z| = 0$ if $x = y$ or $|z| = n/4$ in the case where $x \neq y$.

If a bit string $z \in \{0,1\}^n$ is known to contain exactly $n/4$ entries that are 1, Grover's algorithm [17] is able to find one of these entries without error [2], needing only a single query to the string z. For any string we define the query unitary $U_z = \sum_{i=1}^{n}(-1)^{z_i}|i\rangle\langle i|$ and we define $|s\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle$ to be the uniform superposition of all basis states. Then $G = 2|s\rangle\langle s| - I$ is a unitary operation known as the Grover diffusion operator.

The quantum communication protocol can be viewed as combining Grover's algorithm with a special case of the simulation theorem given by Buhrman, Cleve and Wigderson [7, Theorem 2.1]. We want to perform the algorithm on the effective string $z = x \oplus y$, using the fact that performing a single query U_z is the same as performing the operations U_x and U_y in sequence, i.e., $U_z = U_x U_y = U_y U_x$.

At the start of the protocol, Bob first creates the state $U_y|s\rangle$ and sends this state over to Alice using $\lceil \log n \rceil$ qubits. Alice first applies U_x to the incoming state and then applies the Grover operator G. The final state of Grover's algorithm is $\frac{1}{\sqrt{n/4}}\sum_{i \text{ s.t. } z_i=1}|i\rangle$ if $|z| = n/4$. That is, in the case that $x \neq y$ Grover's algorithm has produced a superposition over all indices i such that $x_i \neq y_i$. Alice measures the state, obtaining some index i^* such that $x_{i^*} \neq y_{i^*}$ if $x \neq y$. Then she sends i^* and the value x_{i^*} over to Bob using $\lceil \log n \rceil + 1$ qubits. He outputs 'equal' if and only if $x_{i^*} = y_{i^*}$. The total communication cost of the protocol is then $2\lceil \log n \rceil + 1$ qubits. ◀

This protocol can be extended to efficiently solve the equivalent problem for other distances than $n/4$ in constant rounds, by using a more general exact version of the Grover search algorithm. The construction is described in Appendix B.

3 The list problem

In this section, we consider the $\mathcal{L}$-LIST problem: Bob gets a list $L \in \mathcal{L}$ from a family $\mathcal{L} \subseteq 2^{\mathcal{X}}$ of lists, Alice gets an element $x \in L$, and Bob must learn x.

3.1 Classical communication complexity of the list problem

Here we prove Theorem 1.6. The list problem that gives the result is simple: For positive integers k, N such that $2 \leq k \leq N$, we consider the list problem $\mathcal{L} = \binom{[N]}{k}$, where the family of lists consists of all k-element subsets of $[N]$. Note that for this problem, Theorem 1.5 gives a four-round protocol using at most $\log\log N + 2\log k + O(\log\log k)$ bits of communication.

▶ **Theorem 3.1.** *The classical communication complexity of* $\binom{[N]}{k}$-LIST *is at least*

$$\log\log N + 2\log(k-1) - \log\log(k-1) - O(1).$$

To see that this implies Theorem 1.6 note that for $\mathcal{L}$ as above, we clearly have $\omega(\mathcal{L}) = k$ and that $G_{\mathcal{L}}$ is the complete graph on N vertices, giving $\chi(G_{\mathcal{L}}) = N$. Hence, the bound in the above theorem can be written as $\log\log\chi(G_{\mathcal{L}}) + (2 - o(1))\log\omega(\mathcal{L})$, where the term $o(1)$ goes to zero as $k \to \infty$. Choosing $k = \log N$ then gives the second part of the theorem.

To prove Theorem 3.1, we use a bound on the size of cover-free families due to Dýachkov and Rykov [13]; see [30, 15] for simplified proofs (in English).

▶ **Definition 3.2.** Let r be a positive integer and $\mathcal{S}$ be a finite set. A family $\mathcal{F} \subseteq 2^{\mathcal{S}}$ of at least $r+1$ subsets is *r-cover-free* if every subfamily of $r+1$ distinct sets $F_0, F_1, \dots, F_r \in \mathcal{F}$ satisfies $F_0 \nsubseteq F_1 \cup \cdots \cup F_r$.

▶ **Theorem 3.3** (Dýachkov–Rykov). *There exists an absolute constant $c > 0$ such that the following holds. Let N and r be positive integers such that $N \geq r+1$ and $r \geq 2$. Let $\mathcal{S}$ be a finite set. Let $\mathcal{F} \subseteq 2^{\mathcal{S}}$ be an r-cover free family consisting of N sets. Then,*

$$|\mathcal{S}| \geq \frac{cr^2 \log N}{\log r}.$$

Proof of Theorem 3.1. For a positive integer C, suppose that the communication complexity of $\binom{[N]}{k}$-LIST is C. Fix such a protocol and for every input pair (x, L) in the $\binom{[N]}{k}$-LIST problem, define the *transcript* $T_{x,L} \in \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^C$ as the concatenation of the parties' messages in the order they are sent during their conversation on input (x, L). Let $\mathcal{T}$ be the set of said transcripts.

For each transcript $T \in \mathcal{T}$, denote by T^A the sequence of Alice's messages in T, to be understood as a sequence of strings indexed by her rounds in the conversation. Let $\mathcal{F} = \{F_x\}_{x \in \mathcal{X}} \subseteq 2^{\mathcal{T}}$ be the family where each F_x is the collection of transcripts $T \in \mathcal{T}$ that is consistent with x being Alice's input and that agrees on T^A. We claim that $\mathcal{F}$ is a $(k-1)$-cover free family. To see this, take any k sets of $\mathcal{F}$, say $F_{x_0}, \dots, F_{x_{k-1}}$, and let L be the corresponding k-element list $\{x_0, \dots, x_{k-1}\}$. Consider the transcript $T_{x_0,L}$ of the input pair (x_0, L). Clearly, $T_{x_0,L} \in F_{x_0}$. We show that $T_{x_0,L} \notin F_{x_i}$ for each $i \in \{1, \dots, k-1\}$, which gives the claim as this implies that $F_{x_0} \nsubseteq F_{x_1} \cup \cdots \cup F_{x_{k-1}}$. Suppose that $T_{x_0,L} \in F_{x_i}$ holds for some $i \in \{1, \dots, k-1\}$. This means that Alice sends identical message sequences on inputs x_0 and x_i and therefore that Bob is not able to distinguish between these two cases for the input pair (x_0, L), contradicting our assumption that we started with a functional protocol.

We also claim that $\mathcal{F}$ consists of at least N sets. Indeed, for every pair $x, y \in [N]$, there is a list $L \in \binom{[N]}{k}$ containing both x and y. Since we must have $T^A_{x,L} \neq T^A_{y,L}$ for Bob to be able to distinguish x and y on input L, the inputs x and y induce distinct transcript sets.

It thus follows from Theorem 3.3 that the total number of distinct transcripts is at least

$$|\mathcal{T}| \geq \frac{c(k-1)^2 \log N}{\log(k-1)}.$$

Hence, since $\mathcal{T} \subseteq \{0,1\} \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^C$, we have

$$\frac{2^{C+1}-1}{2-1} = \sum_{l=0}^{C} 2^l \geq \frac{c(k-1)^2 \log N}{\log(k-1)},$$

for some absolute constant $c > 0$. Taking logarithms now gives the claim. ◀

3.2 Quantum communication complexity of the list problem

Analogous to Witsenhausen's result, the one-round quantum communication complexity of a list problem is characterized in terms of the orthogonality dimension of its associated graph.

▶ **Lemma 3.4.** *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the one-round quantum communication complexity of $\mathcal{L}$-LIST equals $\lceil \log \xi(G_{\mathcal{L}}) \rceil$.*

Proof. Consider an optimal one-round protocol. Without loss of generality, we can assume that Alice sends to Bob a pure state $|\phi_x\rangle \in \mathbb{C}^d$ on input $x \in \mathcal{X}$. Then, given a list $L \in \mathcal{L}$, Bob has a measurement that allows him to distinguish the states $\{|\phi_x\rangle : x \in L\}$. It thus follows from Lemma 2.3 that these states must be orthogonal. In particular, since for every list $L \in \mathcal{L}$, each pair of distinct elements $x, y \in L$ forms an edge in $G_{\mathcal{L}}$, the vectors $|\phi_x\rangle$, $x \in \mathcal{X}$, form a d-dimensional orthogonal representation. Hence, $\xi(G_{\mathcal{L}}) \leq d$.

Conversely, let $f : V(G_{\mathcal{L}}) \to \mathbb{C}^d$ be an orthogonal representation of $G_{\mathcal{L}}$. Then, for every list $L \in \mathcal{L}$, the vectors $\{f(x) : x \in L\}$ are pairwise orthogonal. If Bob gets a list $L \in \mathcal{L}$ and Alice gets an element $x \in L$, it follows from Lemma 2.3 that there is a quantum measurement allowing Bob to uniquely identify x when Alice sends $f(x)$ using $\log d$-qubits. Hence, the one-round quantum communication complexity is at most $\lceil \log \xi(G_{\mathcal{L}}) \rceil$. ◀

For multi-round protocols, a quantum analogue of Theorem 1.3 also holds.

▶ **Lemma 3.5.** *For every family $\mathcal{L} \subseteq 2^{\mathcal{X}}$, the quantum communication complexity of $\mathcal{L}$-*LIST *is at least* $\max\{\Omega(\log\log \chi(G_{\mathcal{L}})), \log \omega(\mathcal{L})\}$.

Proof. Kremer's Theorem (Theorem 1.1) shows that there is at most an exponential difference between the (multi-round) quantum and one-round classical communication complexity. Hence, by Witsenhausen's result, the former is at least $\Omega(\log\log \chi(G_{\mathcal{L}}))$. Moreover, on the worst input Bob has to be able to distinguish among $\omega(\mathcal{L})$ different elements. Hence, $\log \omega(\mathcal{L})$ bits of information must be communicated and Holevo's Theorem [19] says that to retrieve $\log \omega(\mathcal{L})$ bits of information $\log \omega(\mathcal{L})$ qubits are necessary. ◀

3.3 Proof of Theorem 1.7

Recall that we are considering the following family of lists. For an even positive integer n and $d \in [n]$, let $\mathcal{L}_d \subseteq 2^{\{0,1\}^n}$ be the family of all lists $L \subseteq \{0,1\}^n$ of maximal cardinality such that all strings in L have Hamming distance exactly d. We denote by $\mathcal{K}$ the union $\mathcal{L}_{n/2} \cup \cdots \cup \mathcal{L}_n$.

Proof of Theorem 1.7. Let $\ell = \lceil \log n \rceil$ and U be an $(\ell+1)$-qubit unitary matrix satisfying

$$U\,|0\rangle\,|0\rangle^{\otimes \ell} = |0\rangle\,|0\rangle^{\otimes \ell}$$

$$U\,|1\rangle\,|0\rangle^{\otimes \ell} = \frac{1}{\sqrt{n}}|1\rangle \sum_{i=1}^{n} |i\rangle.$$

Moreover, for any 2^ℓ-bit string z, we define the conditional query unitary U_z which acts on the computational basis states as $U_z|0\rangle|i\rangle = |0\rangle|i\rangle$ and $U_z|1\rangle|i\rangle = (-1)^{z_i}|1\rangle|i\rangle$. For a small technicality, if n is not a power of 2, i.e. $\ell > \log n$, we will map any n-bit string to a 2^ℓ-bit string obtained by padding zeros to the original string. We can now explain the protocol.

Suppose that Bob receives a list $L \in \mathcal{L}_d$ and Alice a string $x \in L$. From L, Bob computes the distance d and he sends to Alice a single qubit $\gamma|0\rangle + \sqrt{1-\gamma^2}|1\rangle$ where $\gamma^2 = 1 - \frac{n}{2d} > 0$. Alice pads ℓ zero qubits to the one she received and then applies in sequence the unitaries U

and U_x, obtaining the state

$$\begin{aligned}|\phi_x\rangle &:= U_x U\left(\gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{1-\gamma^2}|1\rangle|0\rangle^{\otimes\ell}\right)\\ &= U_x\left(\gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{\frac{1-\gamma^2}{n}}\sum_{i=1}^{n}|1\rangle|i\rangle\right)\\ &= \gamma|0\rangle|0\rangle^{\otimes\ell} + \sqrt{\frac{1-\gamma^2}{n}}\sum_{i=1}^{n}(-1)^{x_i}|1\rangle|i\rangle\end{aligned}$$

which she sends to Bob, using $\lceil\log n\rceil + 1$ qubits. Notice that if $x, y \in \{0,1\}^n$ differ in exactly d positions, then the states $|\phi_x\rangle$ and $|\phi_y\rangle$ are orthogonal to each other. Hence, by Lemma 2.3, using the list L Bob can perform a measurement that allows him to learn Alice's input x. This protocol requires a total communication of $\lceil\log n\rceil + 2$ qubits. ◀

Acknowledgements. Part of this work was conducted while H. B., D. L., T. P. and F. S. were at the Newton Institute of Mathematical Sciences in Cambridge, UK. J. B. was supported by a Rubicon grant from the Netherlands Organization for Scientific Research (NWO). H. B., T. P. and F. S. were funded in part by the EU project SIQS. D. L. is supported by NSERC, CRC, and CIFAR.

References

1 Andris Ambainis. Quantum search algorithms. *SIGACT News*, 35(2):22–35, June 2004.

2 M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998.

3 G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum computation and information (Washington, DC, 2000)*, volume 305 of *Contemp. Math.*, pages 53–74. Amer. Math. Soc., Providence, RI, 2002.

4 G. Brassard, P. Høyer, and A. Tapp. Quantum counting. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, ICALP'98, pages 820–831, London, UK, 1998. Springer-Verlag.

5 J. Briët, H. Buhrman, and D. Gijswijt. Violating the Shannon capacity of metric graphs with entanglement. *Proceedings of the National Academy of Sciences*, 2012.

6 J. Briët, H. Buhrman, M. Laurent, T. Piovesan, and G. Scarpa. Entanglement-assisted zero-error source-channel coding. *Information Theory, IEEE Transactions on*, 61(2):1124–1138, 2015. A previous version appeared in EuroComb 2014.

7 H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 1998)*, pages 63–68, 1998.

8 P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter. On the quantum chromatic number of a graph. *The electronic journal of combinatorics*, 14(R81):1, 2007.

9 T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104(23):230503, 2010.

10 T. S. Cubitt, L. Mančinska, D. E. Roberson, S. Severini, D. Stahlke, and A. Winter. Bounds on entanglement assisted source-channel coding via the lovasz theta number and its variants. *IEEE Transactions of Information Theory*, 60(11):7330–7344, 2014.

11 R. de Wolf. *Quantum Computing and Communication Complexity.* PhD thesis, Universiteit van Amsterdam, 2001.

12 P. Delsarte and V. I. Levenshtein. Association schemes and coding theory. *IEEE Transactions on Information Theory*, 44(6):2477–2504, 1998.

13 A. G. Dýachkov and V. V. Rykov. Bounds on the length of disjunctive codes. *Problemy Peredachi Informatsii*, 18(3):7–13, 1982. In Russian.

14 P. Frankl and V. Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

15 Z. Füredi. On r-cover-free families. *Journal of Combinatorial Theory, Series A*, 73(1):172–173, 1996.

16 C. D. Godsil and M. W. Newman. Coloring an orthogonality graph. *SIAM Journal on Discrete Mathematics*, 22(2):683–692, March 2008.

17 L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of STOC'96*, pages 212–219, 1996.

18 J. Gruska, D. Qiu, and S. Zheng. Generalizations of the distributed deutsch-jozsa promise problem. *Preprint available at arXiv:1402.7254*, 2014.

19 A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9:177–183, 1973.

20 I. Krasikov and S. Litsyn. *Survey of binary Krawtchouk polynomials.*, pages 199–211. Providence, RI: AMS, American Mathematical Society, 2001.

21 I. Kremer. Quantum communication. Master's thesis, Hebrew University, Computer Science Department, 1995.

22 E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, 1997.

23 M. Laurent. Private communications, 2014.

24 D. Leung, L. Mančinska, W. Matthews, M. Ozols, and A. Roy. Entanglement can increase asymptotic rates of zero-error classical communication over classical channels. *Communications in Mathematical Physics*, 311:97–111, 2012.

25 V. I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in hamming spaces. *IEEE Trans. Inf. Theor.*, 41(5):1303–1321, 1995.

26 L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

27 M. Naor, A. Orlitsky, and P. Shor. Three results on interactive communication. *IEEE Transactions on Information Theory*, 39:1608–1615, 1993.

28 A. Orlitsky. Worst-case interactive communication i: Two messages are almost optimal. *IEEE Transactions on Information Theory*, 36:1111–1126, 1990.

29 M. J. P. Peeters. Orthogonal representations over finite fields and the chromatic number of graphs. *Combinatorica*, 16(3):417–431, 1996.

30 M. Ruszinkó. On the upper bound of the size of the r-cover-free families. *Journal of Combinatorial Theory, Series A*, 66(2):302–310, 1994.

31 G. Scarpa and S. Severini. Kochen-Specker Sets and the Rank-1 Quantum Chromatic Number. *IEEE Transactions on Information Theory*, 58(4):2524–2529, 2012.

32 Joel Spencer. *Asymptopia*, volume 71 of *Student Mathematical Library.* American Mathematical Society, Providence, RI, 2014. With Laura Florescu.

33 H. S. Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Transactions on Information Theory*, 22(5):592–593, 1976.

34 A. C.-C. Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11th annual ACM symposium on Theory of computing (STOC 1979)*, pages 209–213, 1979.

35 A. C.-C. Yao. Quantum circuit complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science (FOCS 1993)*, pages 352–361, 1993.

A Kremer's Theorem

Here we prove Kremer's Theorem (Theorem 1.1), which we restate for convenience. The original proof by Kremer [21] applied to boolean functions; we give a slight generalization of the statement so that it applies to functions with arbitrary range. It is important to notice that the statements in this section hold for general communication protocols, not only exact ones.

▶ **Theorem A.1.** *Let ℓ be a positive integer, $X, Y, \mathcal{R}$ be finite sets and $\mathcal{D} \subseteq X \times Y$. Let $f : \mathcal{D} \to \mathcal{R}$ be a function and suppose that f admits an ℓ-qubit quantum protocol. Then, there exists a one-round $2^{O(\ell)}$-bit classical protocol for f.*

The proof uses the following lemma of Yao [35] and Kremer [21]. To reduce the amount of notation needed in the proof we assume that the parties use the following general protocol. At any point during the protocol, both Alice and Bob have a private quantum register. If it is Alice's turn to communicate, say ℓ-qubits, she appends a fresh ℓ-qubit register to her existing register, applies a unitary to both registers and sends the ℓ-qubit register over to Bob, who then absorbs the ℓ-qubit register into his private register. If it's his turn to communicate, Bob operates similarly. This assumption will allow us to deal more easily with protocols in which different numbers of qubits are sent in each round.

▶ **Lemma A.2** (Yao–Kremer). *Let ℓ be a positive integer, $X, Y, \mathcal{R}$ be finite sets and $\mathcal{D} \subseteq X \times Y$. Suppose that there exists an r-round quantum protocol for a function $f : \mathcal{D} \to \mathcal{R}$, where ℓ_i qubits are communicated in round $i \in [r]$. Then, the final state of the protocol on input $(x, y) \in \mathcal{D}$ can be written as*

$$\sum \alpha_{\mathbf{u}}(x)\beta_{\mathbf{u}}(y)|A_{\mathbf{u}}(x)\rangle|B_{\mathbf{u}}(y)\rangle,$$

where the sum is over all $\mathbf{u} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_r}$, the $\alpha_{\mathbf{u}}(x), \beta_{\mathbf{u}}(y)$ are complex numbers and the $|A_{\mathbf{u}}(x)\rangle, |B_{\mathbf{u}}(y)\rangle$ are complex unit vectors.

Proof. By induction on r. The base case $r = 1$ is trivial, since then Alice sends Bob an ℓ-qubit state. For some $i \in \{2, 3, \ldots, r\}$, suppose that after $i - 1$ rounds the state is given by

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y)|A_{\mathbf{v}}(x)\rangle|B_{\mathbf{v}}(y)\rangle,$$

where the sum is over all $\mathbf{v} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_{i-1}}$. Assume that the i-th round is Alice's turn (the case of Bob's turn is handled similarly). She appends a fresh ℓ_i-qubit register to her current register, causing the state to become

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y)|A_{\mathbf{v}}(x)\rangle|0_1 \cdots 0_{\ell_i}\rangle|B_{\mathbf{v}}(y)\rangle.$$

Next, she applies a unitary over both of her registers, turning the state into

$$\sum \alpha_{\mathbf{v}}(x)\beta_{\mathbf{v}}(y)\left(\sum_{\mathbf{w}\in\{0,1\}^{\ell_i}} \gamma_{\mathbf{w}}|A_{\mathbf{v},\mathbf{w}}(x)\rangle|\mathbf{w}\rangle\right)|B_{\mathbf{v}}(y)\rangle,$$

where $\gamma_{\mathbf{w}}$ is a complex number (which might depend on x) and for some unit vectors $|A_{\mathbf{v},\mathbf{w}}(x)\rangle$. Now define

$$\alpha_{\mathbf{v},\mathbf{w}}(x) := \alpha_{\mathbf{v}}(x)\gamma_{\mathbf{w}}, \qquad \beta_{\mathbf{v},\mathbf{w}}(y) := \beta_{\mathbf{v}}(y) \qquad \text{and} \qquad |B_{\mathbf{v},\mathbf{w}}(y)\rangle := |\mathbf{w}\rangle|B_{\mathbf{v}}(y)\rangle,$$

so that after the ith round, after Alice has sent the ℓ_i-qubit register to Bob, the state equals

$$\sum_{\mathbf{v},\mathbf{w}} \alpha_{\mathbf{v},\mathbf{w}}(x)\beta_{\mathbf{v},\mathbf{w}}(y)|A_{\mathbf{v},\mathbf{w}}(x)\rangle|B_{\mathbf{v},\mathbf{w}}(y)\rangle.$$

After r rounds the state thus looks like as claimed in the lemma. ◀

Proof of Theorem 1.1. Assume that the protocol proceeds in r rounds and that ℓ_i qubits are communicated during round $i \in [r]$. By Lemma A.2 the final state of the protocol can be written as

$$\sum \alpha_{\mathbf{u}}(x)\beta_{\mathbf{u}}(y)|A_{\mathbf{u}}(x)\rangle|B_{\mathbf{u}}(y)\rangle,$$

To produce his output, Bob performs a measurement $\{M_1,\dots,M_k\}$ on his register. For each pair $\mathbf{u},\mathbf{v} \in \{0,1\}^{\ell_1} \times \cdots \times \{0,1\}^{\ell_r}$ and $j \in [k]$ we define the complex numbers

$$\begin{aligned} a_{\mathbf{u},\mathbf{v}}(x) &:= \overline{\alpha_{\mathbf{u}}(x)}\alpha_{\mathbf{v}}(x)\langle A_{\mathbf{u}}(x)|A_{\mathbf{v}}(x)\rangle \\ b^j_{\mathbf{u},\mathbf{v}}(x) &:= \overline{\beta_{\mathbf{u}}(y)}\beta_{\mathbf{v}}(y)\langle B_{\mathbf{u}}(y)|M_j|B_{\mathbf{v}}(y)\rangle. \end{aligned}$$

Then, the probability that Bob gets measurement outcome j equals

$$p_j(x,y) = \sum_{\mathbf{u},\mathbf{v}} a_{\mathbf{u},\mathbf{v}}(x) b^j_{\mathbf{u},\mathbf{v}}(y).$$

The classical one-round protocol works in the following way. Let ℓ be the total communication of the protocol and define $\tilde{a}_{\mathbf{u},\mathbf{v}}(x)$ as an approximation of $a_{\mathbf{u},\mathbf{v}}(x)$ using $2\ell+4$ bits for the real part and $2\ell+4$ bits for the imaginary part, so that $|\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)| \leq 2^{-2\ell-3}$. Alice's message consists of all $2^{2\ell}$ numbers $\tilde{a}_{\mathbf{u},\mathbf{v}}(x)$, making the total communication cost $O(\ell 2^{2\ell})$ bits. Bob calculates his approximation of the probability of getting outcome j as

$$\tilde{p}_j(x,y) = \sum_{\mathbf{u},\mathbf{v}} \tilde{a}_{\mathbf{u},\mathbf{v}}(x) b^j_{\mathbf{u},\mathbf{v}}(y).$$

We can bound the difference between this approximation and the acceptance probability of the original quantum protocol by

$$\begin{aligned} |\tilde{p}_j(x,y) - p_j(x,y)| &= \left|\sum_{\mathbf{u},\mathbf{v}} (\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)) b^j_{\mathbf{u},\mathbf{v}}(y)\right| \\ &\leq \sum_{\mathbf{u},\mathbf{v}} \left|\tilde{a}_{\mathbf{u},\mathbf{v}}(x) - a_{\mathbf{u},\mathbf{v}}(x)\right| \left|b^j_{\mathbf{u},\mathbf{v}}(y)\right| \\ &\leq 2^{-2\ell-3} 2^{2\ell} \leq \frac{1}{8}. \end{aligned}$$

Therefore, given a quantum protocol with sufficiently high success probability, in this paper in particular probability 1, Bob can (deterministically) choose the unique outcome j for which $\tilde{p}_j(x,y)$ is strictly greater than $\frac{1}{2}$, and this outcome j is equal to the function value $f(x,y)$, by correctness of the original quantum protocol. ◀

B Multi-round quantum protocols for EQ-$\binom{n}{\alpha n}$ with $\alpha < 1/2$

Using distributed versions of Grover's search algorithm, we find multi-round quantum communication protocols that solve the EQ-$\binom{n}{\alpha n}$ problem for $\alpha < 1/2$ with a logarithmic number of qubits. For $\alpha = 1/4$, this statement is proven in Theorem 2.11.

When $d = \alpha \cdot n$ where $\alpha \in (1/4, 1/2)$, we can pad zeros to the inputs such that the new strings are either equal or differ in exactly 1/4-th of the positions and run the above two-rounds protocol on the new strings. This is the simple key idea behind the following theorem.

▶ **Theorem B.1.** *For $d = \alpha \cdot n$ with $\alpha \in (1/4, 1/2)$, the two-round quantum communication complexity of* $\mathrm{EQ}\text{-}\binom{n}{\alpha n}$ *is at most* $2\lceil \log n \rceil + 2\lceil \log(4\alpha) \rceil + 1$ *qubits.*

Proof. Let x and y be Alice's and Bob's inputs. They know that x and y are either equal or they differ in exactly $d = \alpha \cdot n$ positions where $d > n/4$. Suppose that Alice and Bob pad their respective inputs with k consecutive zeros with $k = 4d - n$. The new bit strings $\hat{x}$ and $\hat{y}$ have length $n' = n + k = 4d$ and they are either equal or differ in exactly $\alpha' \cdot n' = n'/4$ positions.

Alice and Bob can now run the distributed Grover's search protocol described in the proof of Theorem 2.11 on the new inputs $\hat{x}, \hat{y} \in \{0,1\}^{n'}$. The total communication cost is $2\lceil \log n' \rceil + 1 = 2\lceil \log(4\alpha \cdot n) \rceil + 1 \leq 2\lceil \log n \rceil + 2\lceil \log(4\alpha) \rceil + 1$ qubits. ◀

For $d = \alpha \cdot n$ where $\alpha \in (0, 1/4)$, we need to introduce some technicalities to ensure an exact version of Grover's search algorithm.

▶ **Theorem B.2.** *For $d = \alpha \cdot n$ with $\alpha \in (0, 1/4)$, the quantum communication complexity of* $\mathrm{EQ}\text{-}\binom{n}{\alpha n}$ *is at most $O(\log n)$ qubits. The quantum communication protocol uses $O(\frac{1}{\sqrt{\alpha}})$ rounds.*

Proof. If a n-bit string z is known to contain exactly d entries that are 1, Grover's algorithm can be modified such that it finds an index for one of them with certainty [3, Theorem 16] [4, 1]. The number of queries ℓ that the exact version of Grover's algorithm needs in this case is given by

$$\ell = \left\lceil \frac{\pi}{4 \arcsin \sqrt{\frac{d}{n}}} - \frac{1}{2} \right\rceil < \frac{\pi}{4}\sqrt{\frac{n}{d}} + 1 \,.$$

The exact version of Grover's algorithm is the same as the original algorithm, except for an adapted final step, which uses a parametrized diffusion operator $G(\phi)$ and partial query $V_z(\varphi)$, where ϕ and φ are angles that depend on the Hamming distance d. As these angles do not have a nice closed formula, we refer the reader to [3, Equation (12)] for the relation that ϕ and φ must satisfy. Here

$$V_z(\varphi)|j\rangle = \begin{cases} |j\rangle & \text{if } z_j = 0 \\ e^{i\varphi}|j\rangle & \text{if } z_j = 1 \end{cases}$$

and

$$G(\phi) = F_n V_0(\phi) F_n^\dagger \,,$$

where F_n is the $n \times n$ discrete quantum Fourier transform.[3]

Take $x, y \in \{0,1\}^n$ to be the input strings of Alice and Bob and let $z = x \oplus y$. As in the proof of the $n/4$ case of Theorem 2.11, we turn this search algorithm into a quantum communication protocol by writing a single query $U_z = U_x U_y = U_y U_x$. We can use the

[3] Note that if n is a power of 2, it is also possible to use the $n \times n$ Hadamard transform.

commutativity of U_x and U_y to save rounds: The exact Grover's algorithm is performed by executing the operations

$$G(\phi)V_z(\varphi)\underbrace{GU_z\dots GU_z}_{\ell-1\text{ times}}$$

on starting state $|s\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle$. Since we can write two alternations as $GU_zGU_z = GU_xU_yGU_yU_x$, alternating whether Alice or Bob executes the query first that round, only $\ell-1$ rounds are needed for the $\ell-1$ ordinary Grover iterations. Alice starts the protocol if ℓ is even, and Bob sends the first message if ℓ is odd.

For the final step, the players need to simulate a query $V_z(\varphi)$ by local operations that depend only on x or y. At this point in the protocol it is Alice's turn to communicate. She currently holds the state

$$|\psi\rangle = \underbrace{GU_z\dots GU_z}_{\ell-1\text{ times}}|s\rangle\,.$$

Now Alice adds an auxiliary qubit that starts in $|0\rangle$ state. Define the unitary operation Q_x by its action on the computational basis states as

$$Q_x|j\rangle|b\rangle = |j\rangle|b\oplus x_j\rangle$$

and the (diagonal) unitary matrix $R_y(\varphi)$ as

$$R_y(\varphi)|j\rangle|b\rangle = e^{i\varphi(b\oplus y_j)}|j\rangle|b\rangle\,.$$

Now Alice first applies Q_x on the state $|\psi\rangle|0\rangle$, sends this state to Bob who performs $R_y(\varphi)$, sending the state back to Alice who again performs Q_x. It is easy to check that $Q_xR_y(\varphi)Q_x|\psi\rangle|0\rangle = (V_z(\varphi)\otimes I)|\psi\rangle|0\rangle$, therefore Alice now discards the auxiliary qubit and applies $G(\phi)$ to finish the simulation of the exact version of Grover's algorithm.

The final state of the exact Grover's algorithm is $\frac{1}{\sqrt{d}}\sum_{i\text{ s.t. }z_i=1}|i\rangle$ if $|z| = d$. If Alice has this state in her possession, she performs a measurement in the computational basis, obtaining an index i^* such that $x_{i^*} \neq y_{i^*}$ if $x \neq y$. Then she sends i^* and the value x_{i^*} over to Bob, who outputs 'equal' if and only if $x_{i^*} = y_{i^*}$. This final message consists of $\lceil\log n\rceil + 1$ qubits. By the correctness of the exact Grover's algorithm, this protocol correctly outputs 'not equal' if the Hamming distance between x and y is the fixed value d. Therefore we turned a ℓ-query execution of the exact version of Grover's algorithm into a protocol that uses $(\ell+2)\lceil\log n\rceil + 2$ qubits of communication in $\ell+2$ rounds. ◀

On the Robustness of Bucket Brigade Quantum RAM

Srinivasan Arunachalam[1,2], Vlad Gheorghiu[2,3], Tomas Jochym-O'Connor[2,4], Michele Mosca[2,3,5,6], and Priyaa Varshinee Srinivasan[7,8]

1 **Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands**
2 **Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada**
3 **Department of Combinatorics & Optimization, University of Waterloo, Waterloo, ON, N2L 3G1, Canada**
4 **Department of Physics & Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1, Canada**
5 **Perimeter Institute for Theoretical Physics, Waterloo, ON, N2L 6B9, Canada**
6 **Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8, Canada**
7 **David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, N2L 3G1, Canada**
8 **Institute for Quantum Science and Technology, University of Calgary, Calgary, AB, T2N 1N4, Canada**

Abstract

We study the robustness of the bucket brigade quantum random access memory model introduced by Giovannetti, Lloyd, and Maccone [Phys. Rev. Lett. **100**, 160501 (2008)]. Due to a result of Regev and Schiff [ICALP'08 pp. 773], we show that for a class of error models the error rate per gate in the bucket brigade quantum memory has to be of order $o(2^{-n/2})$ (where $N = 2^n$ is the size of the memory) whenever the memory is used as an oracle for the quantum searching problem. We conjecture that this is the case for any realistic error model that will be encountered in practice, and that for algorithms with super-polynomially many oracle queries the error rate must be super-polynomially small, which further motivates the need for quantum error correction. We introduce a circuit model for the quantum bucket brigade architecture and argue that quantum error correction for the circuit causes the quantum bucket brigade architecture to lose its primary advantage of a small number of "active" gates, since all components have to be actively error corrected.

1998 ACM Subject Classification J.2 Physical Sciences and Engineering

Keywords and phrases Quantum Mechanics, Quantum Memories, Quantum Error Correction

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.226

1 Introduction

A random access memory (RAM) is a device that stores information in an array of memory cells in the form of bits. In contrast to other types of information storage devices, the access latency to any memory cell is constant and does not depend on the location of the information in the RAM. Information stored in the RAM is retrieved by inputting the address of the desired memory cell in a routing circuit. Any address in a RAM with $N = 2^n$ memory cells can by addressed via a unique n bit input query string. The corresponding output register contains the contents of the addressed memory location.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Eds.: Salman Beigi and Robert König; pp. 226–244
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The typical physical implementation of the addressing mechanism uses the fanout architecture [17, 26], in which the routing scheme corresponds to a binary tree. Each node consists of a pair of transistors which routes the electronic signal down one of the two paths to the subsequent level. In the fanout architecture, a given level has all nodes sharing the same routing direction (left or right), set by the corresponding address bit. An n bit query string determines a unique path in the binary tree, corresponding to the desired memory location. In the process, $\mathcal{O}(2^n)$ transistors are activated.

Alternative routing schemes with $\mathcal{O}(\mathrm{poly}(n))$ activated transistors have been proposed, corresponding to exponentially lower energy consumption. One such example is the "bucket brigade" scheme [13, 12]. However, most of the classical implementations follow the simpler fanout architecture, as the power consumption of RAM is negligible in comparison with the power consumption of other components in the architecture.

The classical RAM addressing scheme can be generalized to a quantum RAM (which we simply call qRAM from here on) scheme, where the input is a quantum state, the routing components are inherently quantum, and the information stored can be either classical, i.e. $|0\rangle$ or $|1\rangle$ but not a superposition of both, or quantum, i.e. any arbitrary superposition of $|0\rangle$ and $|1\rangle$. In the present paper we consider qRAM that stores only classical information. Such memory allows querying superposition of addresses

$$\sum_j \alpha_j |j\rangle|0\rangle \overset{qRAM}{\longrightarrow} \sum_j \alpha_j |j\rangle|m_j\rangle, \tag{1}$$

where $\sum_j \alpha_j |j\rangle$ is a superposition of queried addresses and $|m_j\rangle$ represents the content of the j-th memory location. A memory that stores classical information but allows queries in superposition is required for quantum algorithms such as Grover's search on a classical database [23], collision finding [6], element distinctness [1], dihedral hidden subgroup problem [20] and various practical applications mentioned in [3]. In fact, such a quantum memory plays the role of the oracle and is ideal in implementing any oracle-based quantum algorithm, in which the oracle is used to query classical data in superposition.

A conceptually simple physical implementation of a qRAM corresponds to a direct generalization of the fanout architecture used in classical RAMs. However, the number of faulty components that can be tolerated by the quantum architecture is of prime importance due to the difficulty in maintaining quantum coherence. This motivates searching for schemes with fewer faulty components. A fundamental assumption of the qRAM architecture is that "active" gates[1] are the only ones with significant errors.

In this paper we investigate the bucket brigade qRAM proposal introduced in [13, 12]. Assuming one requires a constant error probability for the oracle query, then with the bucket brigade error model it suffices to have an error rate that is on the order of $\mathcal{O}(1/n^2)$. In the bucket brigade model, one assumes that each computational path only contains $\mathcal{O}(n)$

[1] The concept of "active" gates introduced in [13, 12] is somewhat unnatural when extended to quantum gates. At the physical level, a gate is considered active if it physically acts on its input. Since the qRAM may be in a superposition of querying many (or all) possible bit values in the memory, every gate may be in a superposition of being active or not. Implicitly, there is a physical process that is checking whether each gate is active, and then acting in that case, and such a process will not be perfect in practice. Translated into the circuit model, such gates may be modelled as controlled-gates, i.e. gates that act on its input provided that the control qubit is set to $|1\rangle$. Therefore, such a gate is considered "active" if its control is set to $|1\rangle$ and "non-active" otherwise.
In practice, even non-active gates will be prone to errors. The implicit assumption is that these errors are much smaller than the errors in active gates, and the focus of the bucket brigade models is to reduce the impact of the higher order errors found in the active part of a gate.

components that are faulty, and that a total of $\mathcal{O}(n^2)$ faulty operations are performed. One can argue that it is optimistic to assume that the so-called "non-active" components will be completely error-free. And, one could counter-argue that the error rates will be much lower, and thus ignored for problem instances of appropriate size. For the purposes of this article, we set aside these concerns and accept the premise of there only being $\mathcal{O}(n)$ faulty components.

In contrast to such a qRAM, if one just used a regular fanout circuit for the lookup, with no error correction, one would need to maintain quantum coherence over an exponential number of components [12]. In order to achieve a constant error rate for the query in this case, one would need to implement a fault-tolerant version of the look-up circuit, which would normally incur an overhead that is polynomial in n. One advantage of bucket brigade qRAM is thus to bypass the poly-log overhead of fault tolerant quantum error correction needed to achieve a constant error rate for a look-up. Such an error rate would be sufficient if the qRAM is used in an algorithm making a constant number of queries, for example, for certain state generation algorithms [22, 14]. In general, for an algorithm with inverse polynomially many queries, it would suffice to reduce the query error rate to be inverse polynomial in n, e.g. [21, 11].

In this article, we firstly shed doubt on the usefulness of a qRAM that provides queries with constant probability of error, when used with algorithms that make super-polynomially many oracle queries. As an aside, we note that if the imperfect query operation is assumed to be unitary, and if one can apply the inverse of this imperfect query, then one can apply simple amplification methods to achieve queries with arbitrarily small error δ using a number of repetitions that is proportional to $\log(1/\delta)$. It was shown that this logarithmic overhead is not necessary for quantum searching [16] and other problems [9]. However, there is no reason to expect the errors in a realistic qRAM to behave this way, and in this article we consider incoherent errors.

We first show that a very simple model of incoherent physical errors induces an overall query error similar to the one described by Regev and Schiff [25]. Consequently, a qRAM that produces queries with constant error will not permit the quadratic speed-up in Grover's search algorithm or any other quantum search algorithm one might design. We show that one cannot escape achieving an error rate that is super-polynomially small. We conjecture that this error model nullifies the asymptotic speed-ups of other quantum query algorithms as well, and leave as open questions the extension of this result to other important query problems.

This negative result implies the need for some means of error reduction for the qRAM, with a look-up error rate exponential in n. For consistency we assume a physical error rate that is inverse polynomial in n, the logarithm of the size of the database. We thus explore a natural approach, using quantum error correcting codes, to provide this error reduction, and argue that the apparent advantage of qRAM disappears in this case; in principle, one can make the error rate arbitrarily small, however the advantage of a small number of activated gates in the bucket brigade architecture appears to be lost when active error correction has to be performed on each gate. The main motivation for the quantum bucket brigade approach over a straightforward binary-tree approach is that the equivalent of the active gates are the only gates prone to error, and thus an inverse polynomial in n error rate suffices in order to achieve an overall constant error per qRAM look-up.

The remainder of this paper is organized as follows. In Sec. 2 we describe the bucket brigade qRAM architecture and prove that for the Regev and Schiff model [25] the error rate per gate must scale as inverse polynomial in the size of the database. In Sec. 3 we

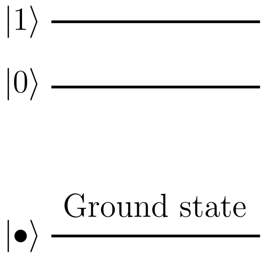


Figure 1 Representation of the energy levels of a qutrit used at the nodes of the routing binary tree. The states $|0\rangle$ and $|1\rangle$ form a metastable subspace since the energy difference between the states is required to be much smaller than the difference between the ground state $|\bullet\rangle$ and $|0\rangle$.

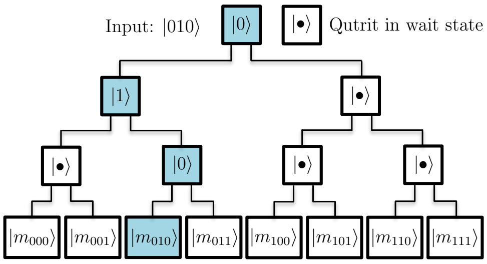


Figure 2 (Color online) Bucket brigade scheme for a qRAM with 8 memory locations. The address register is $|010\rangle$, corresponding to the memory location m_{010}. The path $0 \to 1 \to 0$ is established by sequentially introducing the address qubits $|010\rangle$ into the root of the tree.

develop and analyze a simple error model that provides intuition for the overall behaviour of the memory with realistic noisy environments. In Sec. 4, in order to discuss approaches for introducing quantum error correction inside the qRAM architecture, we introduce a circuit model for the bucket brigade architecture. We then argue in Sec. 5 that a fault-tolerant bucket brigade qRAM loses the advantage of small number of active components. Finally, in Sec. 6 we conclude and present some open problems and directions for future research.

2 Quantum RAM Architectures

In [13, 12], Giovanetti *et al.* proposed a quantum bucket brigade addressing scheme requiring only $\mathcal{O}(n)$ activations per memory call. The nodes of the routing binary tree are three level quantum systems (qutrits), with an energy spectrum schematically depicted in Fig. 1.

The 2^n qutrits at the nodes of the binary tree are initially prepared in the ground state $|\bullet\rangle$, named the "wait" state, and the memory address is specified by the n-qubit state $|a_0 a_1 \ldots a_{n-1}\rangle$. At time t_0, the address qubit $|a_0\rangle$ is input at the root of the tree and it interacts with the qutrit at node 0 changing its state from $|\bullet\rangle$ to $|a_0\rangle$. The states $\{|0\rangle, |1\rangle\}$ of the node qutrit are coupled to two spatial directions (paths), right and left respectively. The role of the coupling is to route the following incoming address photon along the correct path of the binary routing tree. At time t_1, the subsequent address qubit $|a_1\rangle$ is input at the root of the tree. The address qubit $|a_1\rangle$ interacts with the qutrit at node 0 and is physically routed down the left or right path of the tree depending upon the state $|a_0\rangle$ of node 0. Consequently it changes the state of the corresponding node at level 1 to $|a_1\rangle$. The process continues until all the remaining address qubits are sent through the tree, with the k-th address qubit changing the state of the node at the k-th level from $|\bullet\rangle$ to $|a_k\rangle$. After $\mathcal{O}(n^2)$ time steps[2], a routing path is assigned from the root of the tree to the desired memory location, with only n nodes in the path (one node per level) having a state different from $|\bullet\rangle$. A bucket brigade routing scheme for an 2^3-address qRAM is schematically depicted in Fig. 2. The proposed physical implementation of bucket brigade in [12] uses atoms in a cavity as routing nodes and polarization photon states as addressing qubits.

[2] The k-th address qubit interacts with the first $k-1$ routing nodes, followed by a single interaction with the corresponding node at the k-th level. Considering each interaction takes a single time step, the k-th address qubit changes the state of the corresponding node at the k-th level after k time steps. Considering there are a total of n address qubits, the overall time required is $\mathcal{O}(n^2)$.

In [12], the authors claim that the bucket brigade scheme is coherent as long as the error per gate, ε scales as $\mathcal{O}(1/n^2)$. For this error scaling, as n increases, the *overall* error rate of the qRAM oracle asymptotically approaches a constant. Yet constant overall error rates are not favourable for some important quantum algorithms. For example, Regev and Schiff [25] showed that the quadratic speed-up in Grover's searching algorithm vanishes when using oracles with a constant error rate. Namely, in order to regain the quadratic speed-up, the error rate per oracle call should scale no worse than $\mathcal{O}(2^{-n/2})$ (therefore the error rate not only needs to be non-constant it must vanish at a fast enough rate with increasing n).

In the next few sections, we construct a simple model of bucket brigade qRAM with errors and show in Appendix A that Regev and Schiff error model [25] resembles the model we construct. Based on this resemblance and assuming $\mathcal{O}(n^2)$ faulty operations per memory call, we conjecture that in order to implement the qRAM for quantum searching, the overall error rate per memory call has to be in $\mathcal{O}(2^{-n/2})$. In fact, for this to hold, the error rate per gate ε should decrease faster than $1/f(n)$, where $f(n) \in \omega(2^{n/2})$. Thus ε has to be in $o(2^{-n/2})$ and hence much smaller than $\mathcal{O}(1/n^2)$, since the overall error rate per memory call must scale as

$$1 - \left(1 - \frac{1}{f(n)}\right)^{\mathcal{O}(n^2)} \in \Omega\left(\frac{n^2}{f(n)}\right), \tag{2}$$

and in order to satisfy

$$1 - \left(1 - \frac{1}{f(n)}\right)^{\mathcal{O}(n^2)} \in \mathcal{O}(2^{-n/2}), \tag{3}$$

it is required that

$$f(n) \in \Omega\left(n^2 2^{n/2}\right) \implies \frac{1}{f(n)} \in \mathcal{O}\left(\frac{1}{n^2 2^{n/2}}\right) \implies \varepsilon \in o(2^{-n/2}). \tag{4}$$

Recently Hong et al. [15] proposed a bucket brigade qRAM scheme in which the number of time steps required per memory call is reduced from $\mathcal{O}(n^2)$ to $\mathcal{O}(n)$. While this reduction decreases the overall error rate, the error rate per gate ε must still be in $o(2^{-n/2})$.

The need for super-polynomially small (in n) error rate per gate for real world applications motivates a more thorough analysis of the bucket brigade qRAM scheme and the need for quantum error correction, these topics being the subject of the following sections.

3 Errors Analysis

In this section we introduce a simple toy error model for the physical implementation proposed in [12], in which the qutrits are implemented by trapped atoms in cavities. The address qubits are implemented by photons that propagate along the network of cavities, and excite the corresponding qutrit to either of the states $|0\rangle$ or $|1\rangle$, depending on their polarization. In this way, the incoming address photons create a "path" through the binary tree of cavities, leading to the desired memory location. The readout is performed by injecting a "bus" qubit (photon) at the root of the tree that interacts with the desired memory location, copies its value (the states stored by the memory are $|0\rangle$ or $|1\rangle$, and not any superposition), and finally is sent back along the routing tree exiting through the root with the corresponding memory location content. For more details about the physical model an interested reader is referred to [12].

3.1 Toy Error Model

In the following we assume that the only source of errors in the above model is due to random flips between the states $|0\rangle$ and $|1\rangle$ of the qutrit. We assume a typical symmetric bit-flip error, in which at each time step the state $|j\rangle$ can either flip to $|j \oplus 1\rangle$ with probability ε or remain unchanged with probability $1 - \varepsilon$. The motivation for considering this error model is that, since the states $\{|0\rangle, |1\rangle\}$ are close together in the energy spectrum, significantly less energy is required to cause a flip between them, hence such flips are more likely to occur. In reality, there may be other sources of errors such as coupling errors, decaying of excited qutrit states to the ground state, loss of photons during the routing process and so on. However, our toy model illustrates the effects of an error that would naturally occur in a realistic physical realization of a qRAM. There is no reason to expect these other sources of errors would help matters (otherwise, one could seek to deliberately introduce or simulate such errors).

It is not hard to observe that any error in the routing process can propagate through the tree resulting in various possibilities. Considering all possible errors in such a model, the possible paths that the bus photon could take in the final step termed as *right path*, *wrong path* and *no-path*, respectively. For convenience, we further assume the operations used to un-compute the path information encoded in the qRAM are error-free.

1) Right path. This scenario occurs when no flips (errors) arise during the routing process. In this ideal scenario, the bus reaches the correct location in the qRAM as specified by the input address. Fig. 2 depicts an example of a *right path* given an input address $|010\rangle$.

To compute the probability p_{rp} of such an event, we require that no bit flip occurs at each of the j levels. Taking the intersection of such events for all $n - 1$ levels of the binary tree gives the probability of the *right path*

$$p_{rp} = \prod_{j=0}^{n-1} (1-\varepsilon)^{n-j} = (1-\varepsilon)^{\sum\limits_{j=0}^{n-1}(n-j)} = (1-\varepsilon)^{n(n+1)/2}. \tag{5}$$

2) Wrong path. This error refers to the cases wherein the the bus reaches *any other* location in the qRAM other than the location corresponding to the input address. A *wrong path* error occurs at level i if the state $|j\rangle$ of the active routing qutrit at level i flips to $|j \oplus 1\rangle$ and no other errors occur subsequently (at later time steps). The scenario where another error occurs at a later time step in the levels preceding to the j-th level leads to a *no-path* error which we discuss later. The following two figures illustrate two possible *wrong path*s for the input address $|010\rangle$. In Fig. 3, the error is assumed to occur in the third time step, due to which the bus accesses the wrong location corresponding to $|011\rangle$. In Fig. 4, the error is assumed to occur in the second time step, with the bus wrongly accessing the location corresponding to $|000\rangle$.

In order to calculate the probability of a *wrong path* occurring, we consider the probability of any path occurring, regardless of whether it is the *right* or *wrong* path, we denote this probability by p_{path}. Suppose the state $|\psi_j\rangle$ is being routed down the qRAM circuit to the j-th level. If any of the $(j-2)$ first routing nodes have flipped then the state will be routed down an unexpected branch and will not excite the j-th level of the tree, resulting in a *no-path*. The probability of success at this given time step is therefore $(1-\varepsilon)^{j-1}$, where ε is the probability of a node flipping, recall we must include the level-0 root node here. This can only for levels 2 and above. The overall probability of success is therefore the product of each of the individual probabilities of success at each time step (including the time step

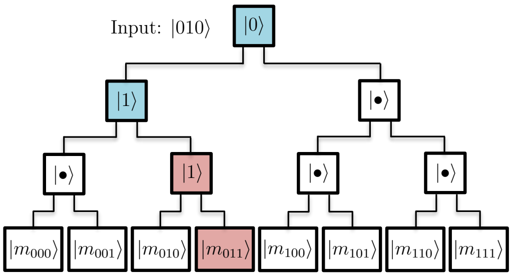


Figure 3 (Color online) Example of a *wrong path* produced by an error at the third time step, given the address |010⟩.

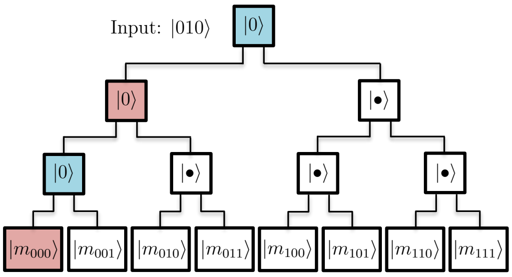


Figure 4 (Color online) Example of a *wrong path* produced by an error at the second time step, given the address |010⟩.

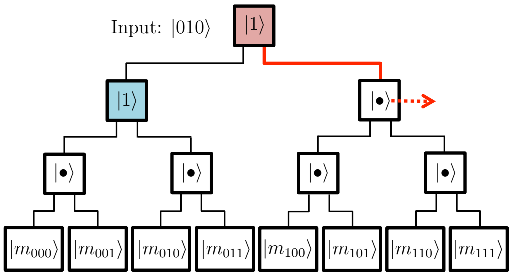


Figure 5 (Color online) Example of a *no-path* given the address |010⟩.

to send the bus qubit down the tree to recover the information stored in the RAM). This probability is given by:

$$p_{path} = p_{wp} + p_{rp} = \prod_{j=2}^{n} (1-\varepsilon)^{j-1} = (1-\varepsilon)^{\sum_{j=2}^{n}(j-1)} = (1-\varepsilon)^{n(n-1)/2}. \tag{6}$$

As we computed before the probability of a *right path* p_{rp} in Eq. (5), the probability of a *wrong path* is then

$$p_{wp} = p_{path} - p_{rp} = (1-\varepsilon)^{n(n-1)/2} - (1-\varepsilon)^{n(n+1)/2}. \tag{7}$$

3) No-path. This error refers to the scenario where the bus never reaches *any* location of the qRAM. Such an error arises when a bit flip error occurs in levels 0 to $n-3$. The smallest such tree where this error can occur is therefore a three-level tree (corresponding to a qRAM with 2^3 memory cells), as shown in Fig. 5. The difference between a *wrong path* and a *no-path* is that, in the latter, the bus photon does not reach the memory address, hence does not read any information, whereas in the former scenario the bus reaches the wrong address in the qRAM and after the un-computing stage, the bus contains the information of *some* particular address in the qRAM.

We present an example of a *no-path* error in Fig. 5, for an input address 010. At the first time instant, the first address photon (i.e. |0⟩) activates the switch (qutrit) in the first layer of the tree. At the second time instant, the address photon |1⟩ interacts with the switch in the first layer, now in state |0⟩, to decide the direction in which it has to be routed. Assuming no error during the second time step, the second address photon is correctly routed to the left path. Assume now that at the third time instant, a flip error occurs on the root qutrit, which flips its state from $|0\rangle$ to $|1\rangle$. The third address photon would then be incorrectly routed to the path on the right. As it can be seen from Fig. 5, at the third time instant there are two activated switches in the second level. The readout bus photon can no longer reach any of the memory locations, and will be lost in the second level of routing tree.

The probability of a *no-path* event is simply

$$p_{np} = 1 - p_{wp} - p_{rp} = 1 - (1 - \varepsilon)^{n(n-1)/2}. \tag{8}$$

If the qRAM is used to implement a quantum oracle O, then O will be faulty, with an error model described by

$$\rho \overset{O}{\to} p_{rp}\hat{O}\rho\hat{O}^{\dagger} + p_{wp}\mathcal{E}_{wp}(\rho) + p_{np}\mathcal{E}_{np}(\rho), \tag{9}$$

with $\hat{O}$ denoting a perfect oracle. Here $\mathcal{E}_{wp}(\cdot)$ and $\mathcal{E}_{np}(\cdot)$ are error channels that corresponds to the *wrong path* and *no-path* errors, respectively.

Our error model Eq. (9) is less optimistic than the one of Regev and Schiff [25] of the form $\rho \overset{O}{\to} (1-p)\hat{O}\rho\hat{O}^{\dagger} + p\rho$. The main difference is that the latter does not mix the amplitudes of the initial starting superposition state in Grover's search algorithm, whereas our model decoheres the system much faster due to the non-trivial errors $\mathcal{E}_{wp}$ and $\mathcal{E}_{np}$. Although we do not have a proof that the quantum query complexity of our model cannot be less than the one considered in [25] (i.e. linear in N), we argue (based on a formal proof for a similar decoherence model, see Appendix A) that this is indeed the case.

3.2 Asymptotic Behaviour

In Figs. 6, 7 and 8 we analyze the probabilities of the three types of errors discussed in the previous subsection. The parameters of interest are the error probability per gate, denoted by ε, the overall fidelity of the addressing circuit (i.e. the probability of a *right-path*), denoted by p_{rp}, and the number of levels in the qRAM addressing binary tree denoted by n (corresponding to 2^n memory locations).

For a fixed ε, we see that the *no-path* behaviour becomes the dominating term in the error model, asymptotically with n, as depicted in Fig. 6.

For a fixed n, again the *no-path* term dominates when the error per gate ε becomes large, see Fig. 7.

Finally, for a fixed desired overall fidelity p_{rp}, the maximum allowed error probability per gate ε to achieve the overall fidelity p_{rp} decays exponentially as a function of n, as plotted in Fig. 8.

From Fig. 8 it can be seen that, the error rate per gate of $\mathcal{O}(1/n^2)$ (blue line in Fig. 8) as considered in Giovannetti et al. [12] is more optimistic than our error rate $\varepsilon(n)$ (red line in Fig. 8)

For larger output fidelity p_{rp}, $\varepsilon(n)$ will always be bounded above by $1/n^2$, with the gap between the two increasing as p_{rp} approaches towards 1. Asymptotically in n, the two graphs converge towards zero.

Simply, the difference between our error $\varepsilon(n)$ and the one in [12] can best be understood by investigating the series expansion

$$p_{rp} = (1-\varepsilon)^{n^2} = 1 + 2\log(1-\varepsilon)\frac{1}{n(n+1)} + \mathcal{O}(\frac{1}{n^4}). \tag{10}$$

In [12] the authors considered only the first order $1/n^2$ as a desirable error rate per gate. However, when the output fidelity p_{rp} approaches 1, this approximation is no longer accurate,

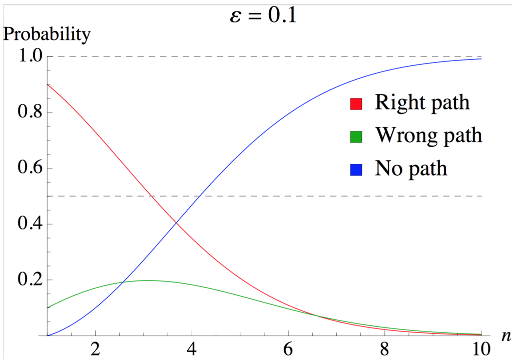


Figure 6 (Color online) Comparison of errors for fixed ε as a function of n.

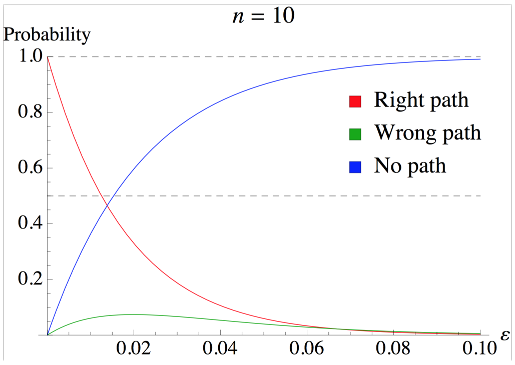


Figure 7 (Color online) Comparison of errors for fixed n as a function of ε.

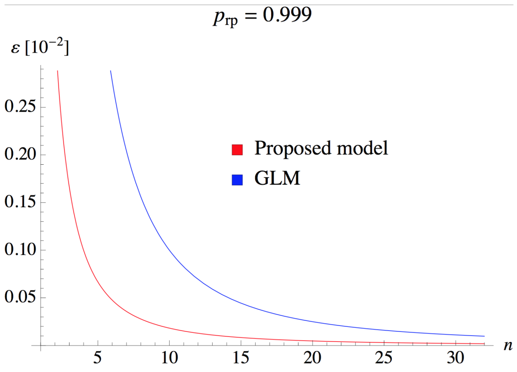


Figure 8 (Color online) Required ε (in dimensionless units of 10^{-2}) as a function of n, for a fixed circuit fidelity. GLM denotes the model proposed in [12].

and higher order terms are important. As mentioned at the end of Sec. 2, inverse polynomial error rates are not good enough in implementing Grover's search with a qRAM-based oracle. In fact, overall error rates of at most $\mathcal{O}(2^{-n/2})$ are essential.

The dominant *no-path* error term poses a fundamental implementation problem, due to lack of oracle information, similar (see Appendix A) to the noise model investigated by Regev and Schiff [25]. If in the future, qRAM designs could be constructed without the presence of such a *no-path* term (i.e. with only *wrong-path* noise), one can attempt error correction to efficiently reduce the error rate. We demonstrate in Appendix B a possible error correction scheme for a simplified *wrong-path* term governed by bit-flip channels, then show however that the scheme is not applicable to our errormodel or to the Regev and Schiff error model [25].

4 Circuit Model

In Fig. 9 we present a circuit description for an $N = 2^3$ qubit bucket brigade qRAM, in which the memory contains only states in the computational basis $\{|0\rangle, |1\rangle\}$. Our circuit is immediately extendable to $N = 2^n$ and closely simulates the physical model proposed in [12].

The circuit description of the bucket brigade addressing scheme accounts for the temporal aspects of the bucket brigade scheme. Namely, since the address qubits are introduced into

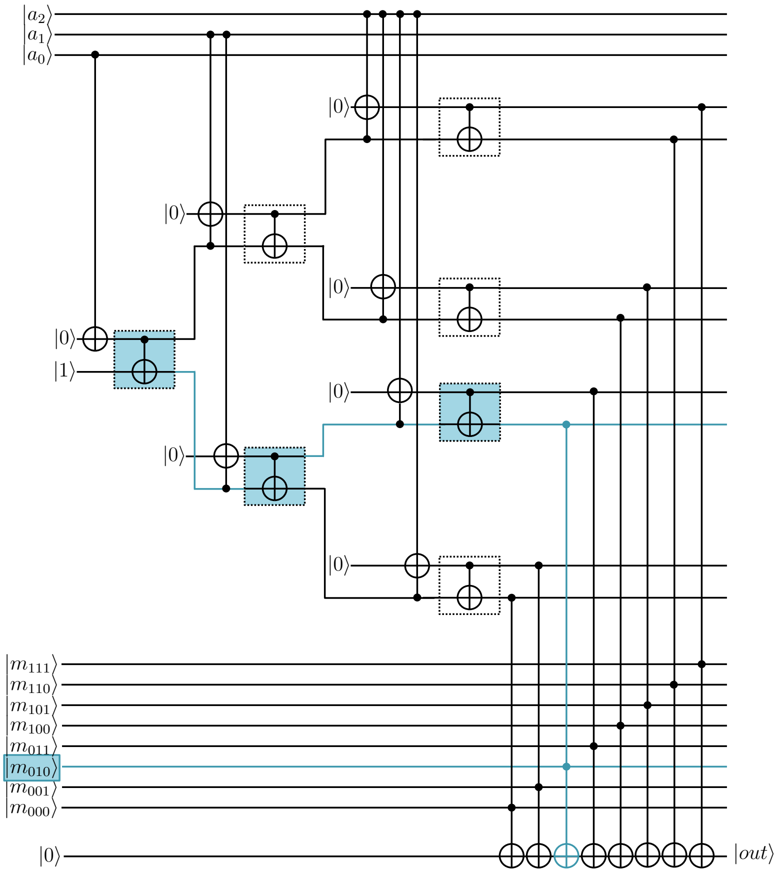


Figure 9 (Color online) Circuit for bucket brigade qRAM. Nodes to the left of the memory cell are *routing nodes*. The dashed squares represents the memory locations. The first layer of nodes immediately to the right of the memory are the *coupling nodes*. Finally, the nodes on the right are the *read out nodes*. A possible input is e.g. $|a_0 a_1 a_2\rangle = |010\rangle$, for which the circuit reads the memory location m_{010}. The path leading to the location m_{010} is represented in blue colour, and the active routing and readout nodes are highlighted. One could more closely mimic the physical flow of information in the bucket brigade qRAM by adding an additional qubit at each node in the binary tree we see in the diagram. Then, for each $k = 0, \ldots, n-1$, we add an initial controlled-NOT gate to copy a_k to the root node, followed by a series of $\mathcal{O}(2^k)$ controlled-SWAPs that will bring the value of a_k to the unique node in level k defined by the bits $a_0, a_1, \ldots, a_{k-1}$. While this adds exponentially many gates, it does not change the overall gate complexity, and these additional gates only add $\mathcal{O}(k)$ to the depth of the circuit. This also illustrates that the exponential depth implicit in the circuit we describe in the diagram can easily be reduced to polynomial depth by mimicking the ideas presented in the qRAM proposal. We leave the circuit diagram in this simpler form, since it does not affect our arguments in Sections 3 and 5.

the binary tree architecture sequentially, the circuit description should respect this ordering. The input to the circuit are the address qubits $|a_0 a_1 \ldots a_n\rangle$. The circuit resembles a binary tree composed of $2^n - 1$ routing nodes, 2^n memory cells and 2^n readout nodes that perform the inverse operations of the routing circuit, used to decouple the qRAM from the address qubits. Additionally, a bus qubit is introduced that interacts with the memory nodes to extract the information stored in the appropriate memory location. It is worth noting that this bus qubit as described may not be physically realistic since it may interact with all the bits in the qRAM. We leave it as such, for simplicity. In practice, if such a non-local qubit is not feasible, one may either work with a phase shift oracle (as described in Ch. 8 of [19]), or one may use a binary-tree circuit to bring the result of the qRAM look-up to a specific qubit that will be accessed by the quantum algorithm that performs the look-up.

The address qubit $|a_0\rangle$ is used to activate the appropriate branch at the first level of the routing. The address qubit is coupled via a CNOT to an ancillary state prepared in the state $|0\rangle$. This qubit then serves as one of the input qubits along with an additional qubit prepared in the $|1\rangle$ state for the routing node (a CNOT gate with the first qubit as control). Depending on the state of the address qubit, the resulting two-qubit output of the routing node will have a single excited qubit in the $|1\rangle$ state, which we shall call the activated qubit. The activated branch of the tree governs the routing of the subsequent interactions with the address qubits, playing the role of the routing atom in the case of the bucket brigade outlined in [12].

The two qubits at the exit of the level-0 routing node serve as inputs to the second register of the two level-1 routing nodes. These qubits control which of the routing nodes are activated at the next level of the qRAM binary tree architecture. Namely, the qubit that is excited in the $|1\rangle$ state allows for the coupling between the address qubit and an introduced $|0\rangle$ state ancilla via a Toffoli gate. Therefore the input to the active routing node is either $|01\rangle$ or $|11\rangle$ depending on the state of the address qubit $|a_1\rangle$. Effectively, the routing operation given by a CNOT gate activates a branch of the tree. For the node that is non-active, the state at the output of the previous level is $|0\rangle$, meaning the Toffoli is not activated and the resulting input and output state to the routing node remains $|00\rangle$. Therefore, after two routing node levels, the output of the routing qubits is composed of 2^2 qubits, with only a single branch being excited depending on the state of the first two address qubits $|a_0a_1\rangle$. Therefore, this corresponds to an isometry:

$$|00\rangle_{a_0a_1} \to |0001\rangle, \quad |01\rangle_{a_0a_1} \to |0010\rangle, \quad |10\rangle_{a_0a_1} \to |0100\rangle, \quad |11\rangle_{a_0a_1} \to |1000\rangle, \tag{11}$$

where the excited output qubits in the $|1\rangle$ state represent an active physical path for the subsequent qRAM operations. This procedure is repeated for n levels, where at the k-th level there are 2^k Toffoli gates and routing nodes. The 2^k Toffoli gates are required to route of the address qubit $|a_k\rangle$ through the previous k levels and the routing node establish the output states in order to route the subsequent address qubits. Since such a circuit performs the appropriate unitary mapping of the address qubits for all computational basis state inputs, by linearity it will extend to all superpositions of input address qubits. An example of the routing procedure for a three-qubit input address state $|010\rangle$ is presented in Fig. 9, where the blue highlighted nodes correspond to the activated nodes.

After the completion of the n routing node levels, memory readout is performed. The reading is performed by introducing a bus qubit prepared in the $|0\rangle$ state which is the target of 2^n Toffoli gates. Each of the 2^n qubits at the output of the qRAM routing nodes pair with one of the memory cells to serve as control qubits for the Toffoli gates. Since only a single output qubit from the routing scheme is activated, only a single Toffoli gate couples with a memory location to the bus qubit. The bus qubit is represented by the bottom qubit in Fig. 9 while the 2^3 memory qubits are represented between the qRAM routing architecture and the bus qubit.

Having completed the coupling of the address qubit, the state of the qRAM routing qubits must be decoupled from the address and bus qubits. Each of the gates from the routing circuit are performed in reverse order, which corresponds to performing the inverse unitary coupling transformation between the address qubits and the routing qubits. The resulting state couples the address qubits with the corresponding memory qubit and has decouples the routing qubits to their input ancillary states.

5 Error Correction

The results from Sec. 3 motivate the need for quantum error correction to be implemented at each node in order to protect against errors that may cause detrimental faults in path information.

5.1 Imposing a quantum error correcting code

In choosing a quantum error correcting code (QECC) to protect the path information that is stored in each node, it is essential to choose an encoding that can be implemented fault-tolerantly, to allow for the generalization to large computational systems. Moreover, the QECC should be chosen such that it can naturally be incorporated from the quantum computer that is accessing the qRAM. In order to analyze the desired error correction properties of a bucket brigade qRAM architecture we consider the circuit presented in Fig. 9. The key gate components at each site are the CNOT and Toffoli gates.

The most natural construction of a QECC that can implement such operations with minimal overhead would be the 15-qubit Reed-Muller code. The reason for choosing such a code would be that decomposing the gate operations in the routing circuit as a sequence of CNOT and Toffoli gates has the advantage that each of these gates can be implemented in a transversal manner. Transversality is defined as the ability to implement a logical gate by applying physical gates that have support at at most a single location per encoded codeblock: it is the most natural way to guarantee fault-tolerance. However, if the quantum computing device leads more naturally to another form of quantum error correction encoding, methods such as state distillation or other schemes for universal fault-tolerance can be used [8, 24, 4, 18, 2].

The focus of many fault-tolerant implementations are through the CSS code construction [28, 10, 29]. A CSS quantum code is constructed using two classical error correcting codes, each individually used to address X and Z type errors. Given that any quantum error can be decomposed in terms of a linear combination of Pauli operators, developing an error correcting code that can address both types of errors will be sufficient for the construction of a QECC.

Let $\mathcal{C}_X$ be a classical error correcting code of length n that has the associated parity check matrix H_X, where each 0 in the parity check matrix of the classical code is replaced by the two-dimensional identity matrix I and each 1 in the classical parity check matrix is replaced by the Pauli X operator. Similarly, let $\mathcal{C}_Z$ be a second classical error correcting code of length n with an associated parity check matrix H_Z, where each 1 in the classical parity check matrix has been now replaced by the Pauli Z operator. If $\mathcal{C}_X^\perp \subseteq \mathcal{C}_Z$ then by combining the stabilizers generated from the parity check matrices of both codes, H_X and H_Z, the resulting stabilizer code forms a QECC. The number of physical qubits in the code is n, the number of logical qubits is given by $k_X + k_Z - n$, where k_i is the number of logical states in the given classical code i and the distance of the code is at least the minimum of the distance of the two classical codes. One of the many appealing features of the CSS code construction is the transversality of the CNOT gate, a feature of the X and Z stabilizers being independent. A particular example of a CSS code is the 15-qubit Reed-Muller code mentioned above.

5.2 Number of activations in a CSS code

In the implementation of Giovanetti *et al.* [12], one of the primary advantages is the number of gate activations that are needed per level of the bucket brigade scheme. More simply, a

CNOT (Toffoli) gate in their scheme is "activated" only when the control qubit(s) is (are) in the state $|1\rangle$. Since only one register is in such a state at a given level, the total number of activations can thus be kept low. In a physical implementation, this is relevant as an activated path may represent the presence of a physical excitation without which no physical process occurs, therefore one can think of these non-activated gates as in fact being the identity operation. However, such an advantage vanishes when imposing a CSS code in order to protect from errors due to the symmetry in the number of $|0\rangle$ and $|1\rangle$ states the logical states encoding the path information.

In the CSS code construction, two classical codes were taken to form a QECC. Therefore, given some codeword of the classical code $c \in \mathcal{C}_Z$, the equivalent quantum state written out in computation basis $|c\rangle$ must be stabilized by the Z generators of the code, by definition of being a codeword of the classical code $\mathcal{C}_Z$. However, in order to be a logical state of the CSS code, it must also be stabilized by the elements of the group generated by the X stabilizers. Therefore, the codestate will be the superposition of the application of all X stabilizers upon $|c\rangle$,

$$|c + \mathcal{C}_Z^{\perp}\rangle = \sum_{x \in \mathcal{C}_Z^{\perp}} |c + x\rangle = \frac{1}{2^{n-k_X}} \prod_i (I^{\otimes n} + S_{X,i})|c\rangle, \tag{12}$$

where $\{S_{X,i}\}$ are the generators of the X stabilizer group, equivalently given by the rows of the parity check matrix H_X.

Consider the form of Eq. (12), given the state $|c\rangle$ written in the computational basis, the action of the operator $(I^{\otimes n} + S_{X,1})$ will be the equally weighted superposition of the state $|c\rangle$ and $S_{X,1}|c\rangle$, which will differ at the location where $S_{X,1}$ has a Pauli X in its description. Therefore, at these locations half of the states in the superposition will have a physical $|0\rangle$ state and half will have a physical $|1\rangle$ state. Then acting upon the state with the operator $(I^{\otimes n} + S_{X,2})$ will have the same effect on all the states in the superposition, with now an even number of physical $|0\rangle$ and $|1\rangle$ states occurring at location with Pauli X in $S_{X,2}$. Repeating this for all X generators, any location with a X operator in one of the stabilizers will necessarily have half of the states in the superposition in each of the physical basis states. In order for the code to protect against any arbitrary single qubit error, each physical qubit must be protected by at least one X stabilizer operator with support the given location, otherwise it would be vulnerable to a single Z error at this location. As such, all relevant CSS codesstate will have an equal number of each of the physical basis states when writing out the expansion of the state in the computational basis.

In a physical implementation, such as that of Giovanetti *et al.* [12], a qubit in the state $|1\rangle$ represents an activated physical process, and as such the advantage of the bucket brigade scheme is that the number of such processes are kept low. However, due to the symmetry in the number of activations that must exist in both the logical ground and excited states, this advantage no longer exists when considering CSS codes. More generally, non-symmetric codes, that is codes where the logical $|0\rangle$ state and logical $|1\rangle$ have a differing number of physical states in the excited state $|1\rangle$, are not desirable for the purposes of error correction as they will be more susceptible to Z errors. The three-qubit repetition code is an extreme example of such a property.

In principle, for the physical error model discussed in Section 3, one can envision using the detection of a photon lost in the routing structure as a means to correct for *no-path* errors (see Fig. 5). However, detecting the exact node at which a photon was lost reveals path information about the state being read by the qRAM (since the previous node in the routing structure would have necessarily been activated by the address qubits) which leads to a loss of coherence in the system. Therefore, any photon detection has to identify the level at which the photon was lost, while not revealing exactly where. It is hard to envisage a practical means for experimentally realizing a photon detection with this property (for example, by somehow symmetrizing the loss of the photon across the exponentially many nodes at a given level). Furthermore, even if this is achieved, one still faces the problem that the lost photon contained path information. Thus, destroying the photon with this path information is equivalent to a dephasing error leading to a further loss of coherence.

In conclusion, if one encodes each node of the bucket brigade qRAM in an error correcting code, then all nodes of the circuit are activated at a physical level, and essentially the qRAM architecture becomes equivalent to a fanout architecture. Even it the latter case, designing a good quantum error correcting code is highly non-trivial. An important issue is that the syndrome measurement should not reveal any information whatsoever about the physical location of the nodes affected by errors. Otherwise, path information is being revealed, which decoheres the system.

6 Conclusions and open questions

We analyzed the robustness of the bucket brigade qRAM scheme introduced in [13, 12] under an optimistic error model. The primary advantage of the bucket brigade scheme is the need for a polynomial in n (rather than exponential) number of gate activations per memory reading. Yet, we give evidence for the hypothesis that for realistic error models, whenever the qRAM is used as a oracle for quantum searching, its error rate per gate has to scale as $o(2^{-n/2})$. Such an error rate is exponentially smaller than the error $\mathcal{O}(1/n^2)$ proposed in [12] (which is sufficient for algorithms with low query complexity), motivating the need for quantum error correction.

We argued that using traditional error correcting techniques offsets the main advantage of the bucket brigade scheme when used with algorithms that make super-polynomially many oracle queries. Since each component of the routing architecture has to be actively error corrected in order to protect against detrimental faults, the overall scheme requires an exponential number of physical gate activations, even if the number of logical gate activations remains polynomial.

An interesting open question is the existence of a realistic architecture-specific error correction technique that could recover the polynomial number of physical gate activations of the routing scheme while still guaranteeing fault-tolerance. For example, if one tries to use an error correction mechanism whereby one only uses multi-qubit code states along the active path, then one has the problem of extracting syndromes and applying corrections in a way that does not identify which path has the non-trivial syndromes (since such information would lead to decoherence). If in this case, for example, one attempts to extract the syndrome without leaving a trace of which node in a given level it came from, then the problem seems at least as challenging as implementing a reliable qRAM.

Moreover, it would be interesting to investigate whether the requirement for a super-polynomial suppression of the error rate is a characteristic of quantum searching algorithms or a more general feature of query complexity with faulty oracles.

Acknowledgements. We thank Daniel Gottesman, Stacey Jeffery, Seth Lloyd, Lorenzo Maccone and Matteo Mariantoni for numerous insightful discussions and suggestions. We thank Seth Lloyd for pointing out to us nice examples of important algorithms that only use polynomially many queries. The authors were supported in part by NSERC, CIFAR, FQRNT, OGS, CryptoWorks21 and Industry Canada. IQC and PI are supported in part by the Government of Canada and the Province of Ontario. S.A. is grateful to Ronald de Wolf's ERC Consolidator Grant QPROGRESS and Michele Mosca for support from NSERC.

References

1 Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, April 2007.

2 Jonas T. Anderson, Guillaume Duclos-Cianci, and David Poulin. Fault-tolerant conversion between the steane and reed-muller quantum codes. *Phys. Rev. Lett.*, 113:080501, Aug 2014.

3 Srinivasan Arunachalam. Quantum speed-ups for boolean satisfiability and derivative-free optimization. Master's Thesis, University of Waterloo, 2014.

4 H. Bombin. Optimal transversal gates under geometric constraints. e-print arXiv:1311.0879 [quant-ph].

5 H. Bombin and M. A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97:180501, Oct 2006.

6 Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *SIGACT News*, 28(2):14–19, June 1997.

7 Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

8 Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, Feb 2005.

9 Harry Buhrman, Ilan Newman, Hein Roehrig, and Ronald de Wolf. Robust polynomials and quantum algorithms. e-print arXiv:quant-ph/0309220.

10 A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

11 Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC'03, pages 59–68, New York, NY, USA, 2003. ACM.

12 Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Architectures for a quantum random access memory. *Phys. Rev. A*, 78:052310, Nov 2008.

13 Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Phys. Rev. Lett.*, 100:160501, Apr 2008.

14 Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. e-print arXiv:quant-ph/0208112.

15 Fang-Yu Hong, Yang Xiang, Zhi-Yan Zhu, Li-zhen Jiang, and Liang-neng Wu. Robust quantum random access memory. *Phys. Rev. A*, 86:010306, Jul 2012.

16 Peter Høyer, Michele Mosca, and Ronald de Wolf. Quantum search on bounded-error inputs. In JosC.M. Baeten, JanKarel Lenstra, Joachim Parrow, and GerhardJ. Woeginger, editors, *Automata, Languages and Programming*, volume 2719 of *Lecture Notes in Computer Science*, pages 291–299. Springer Berlin Heidelberg, 2003.

17 R. C. Jaeger and T. N. Blalock. *Microelectronic Circuit Design.* McGraw-Hill, Dubuque, 2003.

18 Tomas Jochym-O'Connor and Raymond Laflamme. Using concatenated quantum codes for universal fault-tolerant quantum gates. *Phys. Rev. Lett.*, 112:010505, Jan 2014.

19 Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing.* Oxford University Press, 2007.

20 Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, July 2005.

21 Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum algorithms for supervised and unsupervised machine learning. e-print arXiv:1307.0411 [quant-ph].

22 Michele Mosca and Phillip Kaye. Quantum networks for generating arbitrary quantum states. In *Optical Fiber Communication Conference and International Conference on Quantum Information*, page PB28. Optical Society of America, 2001.

23 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 1 edition, January 2004.

24 Adam Paetznick and Ben W. Reichardt. Universal fault-tolerant quantum computation with only transversal gates and error correction. *Phys. Rev. Lett.*, 111:090505, Aug 2013.

25 Oded Regev and Liron Schiff. Impossibility of a quantum speed-up with a faulty oracle. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Part I*, ICALP'08, pages 773–781, Berlin, Heidelberg, 2008. Springer-Verlag.

26 A. S. Sedra and K. C. Smith. *Microelectronic Circuits*. Oxford Press, New York, 1998.

27 Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

28 A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, Jul 1996.

29 Andrew M. Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

A A simple decoherence model

Let us consider the error model considered in [25],

$$\mathcal{R}_p(\rho) := (1-p)\hat{O}\rho\hat{O}^\dagger + p\rho, \tag{13}$$

with $\hat{O}$ denoting the perfect oracle for quantum searching and let us define

$$\mathcal{D}_q(\rho) := (1-q)\rho + q\vec{X}\rho\vec{X}^\dagger \tag{14}$$

as the multi-qubit bit-flip channel where $\vec{X}$ is a shorthand notation for a tensor product of σ_X bit-flip operators acting on some fixed subset of the oracle qubits. The proof technique presented below for $\mathcal{D}_q$ also applies to the case of multi-qubit dephasing channels).

The error model proposed in this paper (see Eq. (9)) is

$$O(\rho) := p_{rp}\hat{O}\rho\hat{O}^\dagger + p_{wp}\mathcal{E}_{wp}(\rho) + p_{np}\mathcal{E}_{np}(\rho). \tag{15}$$

We show that the composition $\mathcal{R}_p \circ \mathcal{D}_q$ resembles (although it is not exactly the same) our error model Eq. (9), for suitable chosen p and q. It follows immediately that $\Omega(N)$ lower bound for the searching algorithm considered in [25] is also a lower bound for the composition $\mathcal{R}_p \circ \mathcal{D}_q$, since channel composition cannot decrease the query complexity (one can simply incorporate $\mathcal{D}_q$ into an appropriate unitary for the $\mathcal{R}_p$ algorithm).

A simple calculation yields:

$$\begin{aligned}\mathcal{R}_p \circ \mathcal{D}_q(\rho) &= (1-p)\hat{O}\mathcal{D}_q(\rho)\hat{O}^\dagger + p\mathcal{D}_q(\rho)\\ &= (1-p)(1-q)\hat{O}\rho\hat{O}^\dagger + (1-p)q\hat{O}(\vec{X}\rho\vec{X}^\dagger)\hat{O}^\dagger + p(1-q)\rho + pq\vec{X}\rho\vec{X}^\dagger\\ &= (1-p)(1-q)\hat{O}\rho\hat{O}^\dagger + (1-p)q\hat{O}(\vec{X}\rho\vec{X}^\dagger)\hat{O}^\dagger + p\mathcal{D}_q(\rho).\end{aligned} \tag{16}$$

We now identify the coefficients in Eq. (15) and Eq. (16)

$$\begin{cases} p_{rp} = (1-p)(1-q) \\ p_{wp} = (1-p)q \\ p_{np} = p, \end{cases} \tag{17}$$

and note that for any given probabilities p_{rp}, p_{wp}, p_{np} satisfying $p_{rp} + p_{wp} + p_{np} = 1$, the system of equations Eq. (17) has the solution

$$\begin{cases} p = p_{np} \\ q = \dfrac{p_{wp}}{p_{wp} + p_{rp}}. \end{cases} \tag{18}$$

We can therefore write

$$\mathcal{R}_p \circ \mathcal{D}_q(\rho) = p_{rp}\hat{O}\rho\hat{O}^\dagger + p_{wp}\hat{O}(\vec{X}\rho\vec{X}^\dagger)\hat{O}^\dagger + p_{np}\mathcal{D}_q(\rho). \tag{19}$$

Comparing Eq. (15) and Eq. (19), we observe that the term $\hat{O}(\vec{X}\rho\vec{X}^\dagger)\hat{O}^\dagger$ is very similar to our wrong path term $\mathcal{E}_{wp}(\rho)$ (the error that corresponds to reading out an incorrect memory location). The last term term $\mathcal{D}_q(\rho)$ in Eq. (19) is not of the form of our no-path error term $\mathcal{E}_{np}(\rho)$, as the latter consists of depolarizing channels of different strengths depending on the position of the address qubit (i.e., the qubits are affected in decreasing order of significance, that is, the first qubit is affected the most, whilst the last one the least). However, $\mathcal{D}_q(\rho)$ is a decohering term, which seems to be a "weaker" form of noise than $\mathcal{E}_{np}(\rho)$. We showed above that even with this weaker decoherence term the quadratic speedup of any searching algorithm is lost. Therefore we have strong reasons to believe that adding a stronger decoherence term will not lower the quantum query complexity for the quantum searching problem. A rigorous proof of this conjecture remains an open problem.

B Error correction schemes

B.1 Correcting simple bit-flip errors

We show below that for a qRAM governed by a toy error model of the form

$$O(\rho) = (1-p)\hat{O}\rho\hat{O}^\dagger + p\hat{O}(\vec{X}\rho\vec{X}^\dagger)\hat{O}^\dagger, \tag{20}$$

the query error rate can be made arbitrarily small by using quantum error correction. Here $\hat{O}$ denotes the perfect oracle and $\vec{X}$ represents a multi-qubit bit-flip channel (a tensor product of individual bit-flip operators acting on an arbitrary subset of qubits). While such error models are not realistic for the architecture presented in this work, it may be that future designs allow for simpler error propagation. Such schemes could benefit from quantum error correction to sufficiently reduce their error rate to enable Grover search.

As Grover's algorithm requires $\mathcal{O}(\sqrt{N})$ steps, one desires a target logical error rate of $\delta = \mathcal{O}(1/\sqrt{N})$. Since the faulty oracle has an error model that consists of a bit flip channel followed by the perfect oracle call, one can use a quantum error correcting code and apply the oracle in parallel along the qubits composing the code. The parallelism of the oracle calls mimics majority counting and allows for error correction to be performed between logical oracle call steps. For simplicity, we provide an example that corrects against bit flip errors only using the repetition code, however such an analysis could be extended to correct for phase flips using code families such as the color codes [5], higher dimensional Shor codes [27], or triorthogonal codes [7].

For example, consider an oracle of the form $|a\rangle|b\rangle \to |a\rangle|b \oplus f(a)\rangle$, where $a,\ b \in \{0,1\}$. A logical oracle call that uses an n-qubit repetition code behaves as follows for states in the computational basis:

$$|a\rangle|b\rangle \xrightarrow{V} |a\rangle^{\otimes n}|b\rangle^{\otimes n} \xrightarrow{\hat{O}^{\otimes n}} |a\rangle^{\otimes n}|b \oplus f(a)\rangle^{\otimes n}, \tag{21}$$

where V denotes the isometric encoding. Therefore, given a repetition code of length d, the code corrects for all errors up to $d/2-1$ physical bit flips by majority counting, using non-destructive Z-type stabilizer measurements. Therefore, the logical error rate becomes $p_L = p^{d/2}$. Choosing d large enough allows the logical error rate to satisfy $p_L = p^{d/2} < \delta$, where δ is the desired target fidelity. Therefore

$$d > \frac{2\log\delta}{\log p} = \frac{2\log\left(1/\sqrt{N}\right)}{\log p} = \frac{n}{\log\left(1/p\right)}. \tag{22}$$

Each of the n address qubits that serve as input to the oracle call must be encoded into a repetition code of length d. Hence, the total number of oracle calls for the complete Grover search algorithm is $\mathcal{O}(nd\sqrt{N}) = \mathcal{O}(n^2\sqrt{N}) = \mathcal{O}(\sqrt{N}(\log N)^2)$. As such, there is a logarithmic penalty for error correction, yet the scaling is not linear as in the error model of Regev and Schiff [25].

B.2 The failure of repetition codes for Regev and Schiff error model

The above error correction scheme is not applicable to the error model presented in [25], described by $\mathcal{R}_p(\rho) = (1-p)\hat{O}\rho\hat{O}^\dagger + p\rho$, since the failure of an oracle call can lead to an uncorrectable error, as demonstrated below. Consider the following example of the 3-qubit repetition code, where rather than all three oracles calls succeeding, the oracle call on the first set of qubits fails. The computational states evolve as:

$$|000\rangle|000\rangle \xrightarrow{\hat{O}_2\hat{O}_3} |000\rangle|0f(0)f(0)\rangle \tag{23}$$

$$|111\rangle|000\rangle \xrightarrow{\hat{O}_2\hat{O}_3} |111\rangle|0f(1)f(1)\rangle. \tag{24}$$

Consider the action of such a faulty oracle on the encoded state $(|000\rangle + |111\rangle)/\sqrt{2}$, for $f(0) = 0$ and $f(1) = 1$. The resulting mapping is

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes |000\rangle \xrightarrow{\hat{O}_2\hat{O}_3} \frac{1}{\sqrt{2}}(|000\rangle|000\rangle + |111\rangle|011\rangle). \tag{25}$$

The syndrome check operators for the repetition code are the parity check operators $\{Z_1Z_2, Z_2Z_3\}$. They are used to determine if an oracle call has failed by measuring the ancilla qubits. However, the measurement collapses the state to either $|000\rangle|000\rangle$ or $|111\rangle|011\rangle$. Upon applying the appropriate correction based on the measured syndromes, the resulting state becomes either $|000\rangle|000\rangle$ or $|111\rangle|111\rangle$. Therefore, the logical oracle call has failed, since the correct result must yield the superposition $(|000\rangle|000\rangle + |111\rangle|111\rangle)/\sqrt{2}$.

As expected, the error correction properties of the repetition code are not in violation of the results of Ref. [25], which state that a linear number of noisy black-box oracle calls are required, even with the addition of error correction.

B.3 The failure of repetition codes for our error model

Consider the oracle error model:

$$O(\rho) := p_{rp}\hat{O}\rho\hat{O}^{\dagger} + p_{wp}\mathcal{E}_{wp}(\rho) + p_{np}\mathcal{E}_{np}(\rho), \tag{26}$$

where $\hat{O}$ is the perfect oracle call while $\mathcal{E}_{wp}(\rho)$ and $\mathcal{E}_{np}(\rho)$ are the *wrong path* and *no-path* terms, respectively. We model the *wrong path* term as a convex combinations of bit-flip channels followed by perfect oracle calls. An example of one of those terms is the second term in Equation 20. We model the *no-path* term as taking any input state and mapping it to a fixed state $|g\rangle$, which represents the loss of a qubit to be replaced by any fixed ancillary state. It should be noted that in the *no-path* case, the readout ancilla state does not change. Consider the action of the noisy channel on the five-qubit repetition code. Each instance of the channel has a certain probability of failure given by the associated weights. Focusing on one particular instance where the first address photon is lost and the second is affected by a bit flip, the resulting mapping on the computational basis states is given by:

$$|00000\rangle|00000\rangle \longrightarrow |g1000\rangle|0f(1)f(0)f(0)f(0)\rangle \tag{27}$$
$$|11111\rangle|00000\rangle \longrightarrow |g0111\rangle|0f(0)f(1)f(1)f(1)\rangle. \tag{28}$$

Again choosing $f(0) = 0$ and $f(1) = 1$, a superposition of input states in the computational basis evolves as

$$\frac{1}{2}\mathrm{P}\left[(|00000\rangle + |11111\rangle) \otimes |00000\rangle\right] \longrightarrow \frac{1}{2}\left(\mathrm{P}\left[|g1000\rangle \otimes |01000\rangle\right] + \mathrm{P}\left[|g0111\rangle \otimes |00111\rangle\right]\right), \tag{29}$$

where $\mathrm{P}[\bullet]$ denotes the projector onto its argument. The measurement of the stabilizers of the 5-qubit code on the ancillary states results in the collapse of the state into one of two terms depending on the syndrome measured. Note that the *no-path* term is the term that destroys coherence, similarly to the error term in the Regev and Schiff model [25].

Interferometric Versus Projective Measurement of Anyons

Claire Levaillant[1] and Michael Freedman[2]

1 Department of Mathematics, South Hall Room 6607, University of California, Santa Barbara, CA 93106, USA
2 Station Q, Microsoft Research, Santa Barbara, CA 93106-6105, USA

Abstract

Two distinct methods for measuring topological charge in a nonabelian anyonic system have been discussed in the literature: projective measurement of a single point-like quasiparticle and interferometric measurement of the total topological charge of a group of quasiparticles. Projective measurement by definition is only applied near a point and will project to a topological charge sector near that point. Thus, if it is to be applied to a *group* of anyons to project to a *total* charge, then the anyons must first be fused one by one to obtain a single anyon carrying the collective charge. We show that interferometric measurement is strictly stronger: Any protocol involving projective measurement can be simulated at low overhead by another protocol involving only interferometric measurement.

1998 ACM Subject Classification J.2 Physical Sciences and Engineering

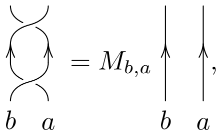
Keywords and phrases anyons, measurement, interferometry, physics

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.245

1 Introduction

We clarify a foundational issue regarding the relative power of two computational schemes which have been long proposed for nonabelian anyons. The two are projective measurement [8] and interferometric measurement; abstractly [11, 10, 5, 4, 1] and in a physical system, [7].

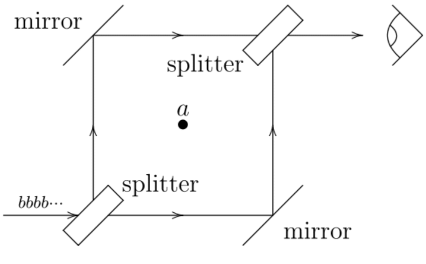
The discussion is restricted to the basic case: unitary modular tensor categories (UMTC) [13]. This is a mathematical idealization of a $(2+1)$-dimension topological quantum field theory (TQFT). The unitary requirement is necessary for the system to be a legitimate model of the non-dissipative physics of the low energy states of a gapped quantum mechanical system. The modularity assumption is a nonsingularity requirement. Abstractly this condition assures us that the quantum system can be consistently defined on a physical torus (and this implies all surfaces [12]) – the system is *not* tied to the plane. Concretely it tells us that every topologically nontrivial excitation (or equivalently "quasiparticle" or "anyon") of the theory a is detected by its braiding with some other anyon b (see page 29 of [1]). For example, when anyons a and b are mutually abelian, i.e., have a unique fusion channel c, braiding assumes the form:



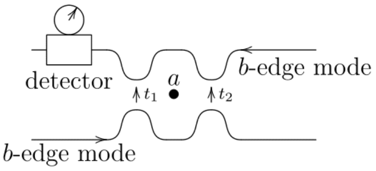
, $M_{b,a}$ a nontrivial phase.

Modularity implies that for each nontrivial particle a, there is a (possibly composite) b so that not only is $M_{b,a} \neq 1$ but $M_{b,a} \neq M_{b,a'}$, $a' = a$, a' an anyon of the theory. Even for *non-abelian* theories, modularity implies that particles are distinguished via braiding.

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).
Editors: Salman Beigi and Robert König; pp. 245–249
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



(A) Mach-Zehnder



(B) Fabry-Perot

Figure 1

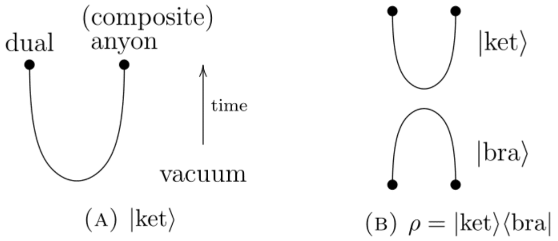
This distinguishability was exploited in [1, 4] to give a full analysis of anyonic interferometers of Mach-Zehnder and Fabry-Perot designs. We note that much of the applied and even experimental literature on measuring topological charge, e.g. [14], has focused on Fabry-Perot geometries. In the low tunnelling (single pass) limit, the Fabry-Perot interferometer determines the same evolution of the system density matrix ρ as the simpler Mach-Zehnder interferometer. Even so, the evolution of ρ under operation of the interferometer is quite complicated. Fortunately, and this is the main conclusion of [1, 4], there is an easy *topological* interpretation of the asymptotic action of an interferometer, Int_a, which has converged to a measurement "a", meaning the total topological charge within the interferometric loop has been measured to be that of an anyon of type a. See Figure 1. Furthermore, convergence to this limit is efficient – exponentially fast.

In contrast, a projective measurement Proj_a to particle type a is the Hermitian orthogonal projection to that particle sector. It is visualized as occurring by bringing some external prob, such as an STM tip, up to an isolated point-like anyon and directly detecting some, perhaps non-universal, signature of that particular particle type in that particular system. For example, even for an electrically neutral ψ, in $\nu = \frac{5}{2}$ fractional quantum Hall effect (FQHE), higher moments of the electric field might provide a signature. In any case, it is this hope which has led to the projective measurement model.

We now show that within the UMTC formalism, any protocol using projective measurement can be efficiently simulated by a protocol which instead uses interferometric measurement.

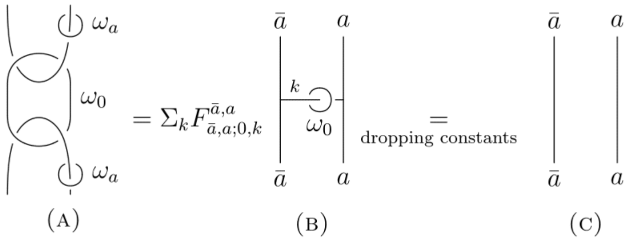
To do this we first need to define, through a density matrix diagram, the asymptotic topological action of Int_a. The diagrams, Figure 2b and on, have a $|\text{ket}\rangle\langle\text{bra}|$ aspect when read from top to bottom. The diagrams in $|\text{ket}\rangle\langle\text{bra}|$ format, of course, represent operators (density matrices), and Figure 2a represents a state vector ($|\text{ket}\rangle$). It should be noted that such representations of operators and states obey topological rules [13] and may or may not correspond bit by bit to a physical process.

We start with a vacuum and create a, perhaps complex, system of anyons which we divide into two halves "inside" and "outside" the interferometer. In Figure 2 these two halves at any given time are depicted simply as points, but they may represent composite anyons, in dual groups, drawn out of the vacuum.



(A) |ket⟩ (B) $\rho = |\text{ket}\rangle\langle\text{bra}|$

Figure 2

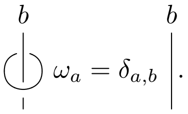

ω_a
ω_0
ω_a
$= \Sigma_k F^{\bar{a},a}_{\bar{a},a;0,k}$
$\bar{a}$
a
k
ω_0
$\underset{\text{dropping constants}}{=}$
$\bar{a}$
a

(A) (B) (C)

Figure 3

From [1, 4], Int_a asymptotically transforms from Figure 2b to Figure 3, assuming that the measurement outcome a, indeed, has nonzero probability. In Figure 3 and below, we drop overall nonzero scalars from the diagrams.

Notation: ω_a is the a^{th} row of the normalized S-matrix which operates as a projector onto the a particle:



The presence of ω_a is expected – it projects onto the a-particle type sector. The ω_0 loop has long been regarded as an unfortunate but unavoidable consequence of running the interferometer. ω_0 encodes a kind of decoherence between inside and outside caused by the intervening stream of prob particles b. In [4], this severing of charge lines k running from the inside to the outside of the interferometer was called *anyonic charge line decoherence*. Topologically, ω_0 surgers the a-lines (Figure 3c) so that a and $\bar{a}$ have forgotten that they came out of the vacuum together – they are no longer correlated.

The presence of this ω_0-loop leads to a general supposition in the community that Int_a and Proj_a were incomparable: Int_a permits non-demolition measurement, as the internal correlations within the two groups of quasiparticles, inside and outside, are *not* disturbed, whereas in order to obtain a localized particle on which to apply Proj_a, the internal structure of the quasiparticle group to be measured would first need to be destroyed by a series of fusions (which produces decoherence even if the fusion outcomes are presumed not to be observed). In contrast, Proj_a does *not* cause anyonic charge line decoherence between the measured subsystem from its complement. Each seemed to have its own peculiar advantages and disadvantages with respect to the preservation of quantum information.

However, we will now show that the anyonic charge line decoherence of a and $\bar{a}$ can be reversed (oddly, this oximoron *is* possible in a topological system) by additional interferometric measurements. The key observation is that if after Int_a we interferometrically measure the collective state of $\bar{a} \cup a$, there is still a nonzero probability of observing the outcome 0, the trivial particle. This is because if the two lines in Figure 3c are recoupled, the F-symbol,

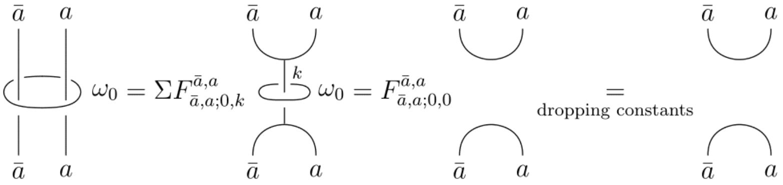

$\bar{a}$
a
$\omega_0 = \Sigma F^{\bar{a},a}_{\bar{a},a;0,k}$
k
$\omega_0 = F^{\bar{a},a}_{\bar{a},a;0,0}$
=
dropping constants

Figure 4

$F^{\bar{a},a}_{\bar{a},a;0,0} \neq 0$, reflecting the fact that a particle and its uncorrelated antiparticle may fuse into the vacuum. (This, in fact, is the definition of an antiparticle.) Suppose we measure $\bar{a} \cup a$ and observe 0, so that Int_0 is applied to the system. The result is given in Figure 4.

We see that Int_0 has restored us to the situation we would have been in if the ω_0 loop associated to the initial Int_a had *not* been present. The decoherence has been reversed.

Of course it is not certain that the second measurement will result in Int_0; other outcomes Int_k are also possible. But now there is an easy "ping-pong" strategy (referred to as "forced measurement" in [3]): Bounce back and forth between measuring the initial inside – which will always return outcome a, Int_a will be applied on the odd steps of this cycle, and measuring the entire system $\bar{a} \cup a$. Each of the odd steps decoheres the inside and outside of the initial interferometer and returns the density matrix to that shown in Figure 3c. Actually, since on the odd steps $3, 5, 7, \ldots$, there is no doubt that topological charge a will be measured, it is *not* necessary to *read* the output of the interferometer, but merely to run the probe particles around the initial loop, thus producing anyonic charge line decoherence. Each of these even step measurements on the entire system constitute an *independent* chance to apply Int_0. Because of independence, the tail event that after $2t$ measurements Int_0 has not been applied decays exponentially in t. The exact exponential rate is easily calculated from the data of any particular UMTC. Since $F^{\bar{a},a}_{\bar{a},a;0,0} = \frac{1}{d_a}$, charge 0 is observed at each step $2t$ with probability $p = \left(\frac{1}{d_a}\right)^2$, so the exponential rate of decay in t is $2 \log_e \left(1 - \frac{1}{d_a^2}\right)$.

2 Conclusion and outlook

We have shown how to "projectively"[1] measure the total topological charge with repeated interferometric measurements of groups of anyons without decohering the group from its complement. In contrast, projective measurement of anyonic charge is in the usual model [8] limited to projecting to the topological charge of a single anyon. A priori, this looks like a strictly *weaker* operation.

It should be remarked, though, that as with all issues of complexity, at this point in history there are no "lower bounds."

Any proof that it is impossible to simulate interferometric measurement by projective measurement would necessarily rely on complexity assumptions. We regard this as an area for future work.

However, evidence of the enhanced strength of interferometric measurement is presented in a series of papers [2, 9] on universal gate systems for qubit and qutrit systems within $SU(2)_4$ and its Jones-Kauffman partner. Previously a universal protocol for a certain qutrit

[1] We place "projectively" in quotes because unlike the usual usage in the arena of anyonic systems, this measurement is both nonlocal and nondemolitional. It is projective in the usual quantum mechanical sense of Hermitian orthogonal projection onto an eigenbasis, in this case the eigenbasis of total topological charge.

within $SU(2)_4$ was found [6] using projective measurement but the argument appears quite special and not applicable to qubits.

We call attention to a shortcut for graphically exploring interferometry protocols. Because of the iterative process we have just described for eliminating the decohering ω_0-loops associated to interferometric measurement, one may proceed – in the manner of a person writing computer code in a higher order language – only to manipulate the $|\text{ket}\rangle$ which describes the current state of the system of anyons. The $|\text{ket}\rangle$ is used at any given time to describe the state that has been pulled out of the vacuum. It is not necessary to double the diagram by adding the dual bra (and the linking $|\text{ket}\rangle\langle\text{bra}|$ by ω_0-loops). Any ω_0-loop will eventually be removed by some even numbered step of our protocol. Thus it is not really necessary to draw the ω_0-loops, or even the $\langle\text{bra}|$, but merely to keep track of the $|\text{ket}\rangle$. In the end, if a density matrix ρ is desired, one may obtain ρ as the outer product of the final $|\text{ket}\rangle_{\text{final}}$ with its dual $\langle\text{bra}|_{\text{final}}$, $\rho = |\text{ket}\rangle_{\text{final}}\langle\text{bra}|_{\text{final}}$.

References

1 Bonderson, P. *Non-abelian anyons and interferometry.* PhD thesis, Caltech, 2007. Physics.

2 Bonderson, P., Freedman, M., Lutchyn, R., Nayak, C., and Wang, Z. Unpublished.

3 Bonderson, P., Freedman, M., and Nayak, C. Measurement-only topological quantum computation via anyonic interferometry. *Annals of Physics 324* (2009), 787.

4 Bonderson, P., Shtengel, K., and Slingerland, J. K. Decoherence of anyonic charge in interferometry measurements. *Phys. Rev. Lett. 98* (2007), 070401.

5 Bonderson, P., Shtengel, K., and Slingerland, J. K. Interferometry of non-Abelian Anyons. *Annals of Physics 323* (2008), 2709.

6 Cui, S. X., and Wang, Z. Universal quantum computation with metaplectic anyons. arXiv:1405.7778, April 2014.

7 Das Sarma, S., Freedman, M., and Nayak, C. Topologically-protected qubits from a possible non-abelian fractional quantum hall state. *Phys. Rev. Lett. 94* (2005), 166802.

8 Kitaev, A. Fault-tolerant computation by anyons. *Ann. Phys. 303* (2003), 2–111.

9 Levaillant, C. 2014, to appear.

10 Overbosch, B., and Bais, F. Inequivalent classes of interference experiements with non-abelian anyons. *Phys. Rev. A 64* (2001), 062107.

11 Preskill, J. Fault-tolerant quantum computation. In *Introduction to Quantum Computation*, H.-K. Lo, S. Popescu, and T. P. Spiller, Eds. World Scientific, 1998.

12 Turaev, V. G. *Quantum invariants of knots and 3-manifolds*, vol. 18 of *Studies in Mathematics.* Walter de Gruyter, 1994.

13 Wang, Z. *Topological quantum computation*, vol. 112 of *Regional Conference Series in Mathematics.* Conference Board of the Mathematical Sciences, 2010.

14 Willet, R., Pfeiffer, L., West, K., and Manfra, M. Aharonov-bohm effect and coherence length of charge $\frac{e}{4}$ quasiparticles at $\frac{5}{2}$ filling factor measured in multiple small fabry-perot interferometers. arXiv:1301.2594, January 2013.