12th Conference on the Theory of Quantum Computation, Communication, and Cryptography

TQC 2017, June 14–16, 2017, Paris, France

Edited by

Mark M. Wilde

LIPICS

Editor

Mark M. Wilde
Hearne Institute for Theoretical Physics
Department of Physics and Astronomy
Center for Computation and Technology
Louisiana State University
Baton Rouge, Louisiana 70803, USA mwilde@lsu.edu

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

ISBN 978-3-95977-034-7

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/978-3-95977-034-7.

Publication date
February, 2018

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.2017.0

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

Preface
Mark M. Wilde vii

Conference Organization
..... ix

Papers

A Single Entangled System Is an Unbounded Source of Nonlocal Correlations and of Certified Random Numbers
Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín 1:1–1:23

The Complexity of Simulating Local Measurements on Quantum Systems
Sevag Gharibian and Justin Yirka 2:1–2:17

Provably Secure Key Establishment Against Quantum Adversaries
Aleksandrs Belovs, Gilles Brassard, Peter Høyer, Marc Kaplan, Sophie Laplante, and Louis Salvail 3:1–3:17

Quantum Coin Hedging, and a Counter Measure
Maor Ganz and Or Sattath 4:1–4:15

Quantum Hedging in Two-Round Prover-Verifier Interactions
Srinivasan Arunachalam, Abel Molina, and Vincent Russo 5:1–5:30

Multiparty Quantum Communication Complexity of Triangle Finding
François Le Gall and Shogo Nakajima 6:1–6:11

Improved Reversible and Quantum Circuits for Karatsuba-Based Integer Multiplication
Alex Parent, Martin Roetteler, and Michele Mosca 7:1–7:15

Fidelity of Quantum Strategies with Applications to Cryptography
Gus Gutoski, Ansis Rosmanis, and Jamie Sikora 8:1–8:13

Minimum Quantum Resources for Strong Non-Locality
Samson Abramsky, Rui Soares Barbosa, Giovanni Carù, Nadish de Silva, Kohei Kishida, and Shane Mansfield 9:1–9:20

Approximate Reversal of Quantum Gaussian Dynamics
Ludovico Lami, Siddhartha Das, and Mark M. Wilde 10:1–10:18

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Preface

The 12th Conference on the Theory of Quantum Computation, Communication, and Cryptography was organized by the Université Pierre et Marie Curie and the Paris Centre for Quantum Computing from the 14th to the 16th of June 2017. 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 2016, Freie Universität Berlin, Germany
- TQC 2015, Université libre de Bruxelles, Belgium
- 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. Contributed talks were solicited for two tracks: Conference Track and Workshop Track. The accepted submissions to the Conference Track appear in these Proceedings, as well as a selection of some that were accepted to the Workshop Track. The papers in these proceedings are listed in their order of submission.

The invited talks were given by David Gosset (IBM), Stephen Jordan (National Institute of Standards and Technology / University of Maryland), Stephen Piddock (University of Bristol), and Barbara Terhal (Delft University of Technology).

The conference was possible thanks to generous donations from Microsoft, CryptoWorks21, Paris Centre for Quantum Computing, Laboratoire d'Informatique de Paris 6, as well as the Institute of Physics. I am indebted to the members of the Program Committee and all subreviewers for their precious contribution in reviewing the submissions. I also wish to thank the members of the Local Organizing Committee, especially Damian Markham, for their considerable efforts in organizing the conference. I would like to thank Marc Herbstritt and Michael Wagner (Dagstuhl Publishing) for their technical help. Finally, I would like to thank the members of the Steering Committee for offering me this opportunity and for their support, and I also thank all contributors and participants.

Mark M. Wilde
October 2017

Conference Organization

Local organizing committee

Damian Markham – chair
Eleni Diamanti – co-chair
Elham Kashefi – co-chair
André Chailloux
Tom Douce
Frédéric Grosshans
Marc Kaplan
Iordanis Kerenidis
Anthony Leverrier
and the entire Quantum Information group at the UPMC

Programme committee

Dominic Berry (Macquarie University)
Mario Berta (Caltech)
Sergey Bravyi (IBM)
Michael Bremner (University Technology Sydney)
Roger Colbeck (University of York)
Nilanjana Datta (University of Cambridge)
David Elkouss (Delft University of Technology)
Omar Fawzi (ENS de Lyon)
Markus Grassl (Max Planck Erlangen)
David Gross (University Freiburg)
Rahul Jain (National University of Singapore)
Zhengfeng Ji (University Technology Sydney)
Stephen Jordan (NIST / University of Maryland)
Shelby Kimmel (University of Maryland / NIST)
Vadym Kliuchnikov (Microsoft)
Francois Le Gall (Kyoto University)
Troy Lee (Nanyang Technological University)
Yeong-Cherng Liang (National Cheng Kung University)
Yi-Kai Liu (NIST / University of Maryland)
Hoi-Kwong Lo (University of Toronto)
Laura Mancinska (University of Bristol)
Prabha Mandayam (IIT Madras)
Tomoyuki Morimae (Gunma University)
Tobias Osborne (University of Hannover)
Lidia del Rio (ETH Zuerich)
Neil J. Ross (University of Maryland / NIST)
Pradeep Sarvepalli (IIT Madras)
Valerio Scarani (National University of Singapore)
Ujjwal Sen (Harish-Chandra Research Institute)
Yaoyun Shi (University Michigan)

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Barbara Terhal (RWTH Aachen University)
Dave Touchette (University of Waterloo / Perimeter Institute)
John Watrous (University of Waterloo)
James Whitfield (Dartmouth College)
Mark M. Wilde (Louisiana State University) (PC Chair)
Man-Hong Yung (South University Science & Technology China)

Steering committee

Anne Broadbent (University of Ottawa)
Wim van Dam (University of California Santa Barbara)
Aram Harrow (Massachusetts Institute of Technology)
Yasuhito Kawano (NTT, Tokyo)
Michele Mosca (Institute for Quantum Computing, Waterloo and Perimeter Institute)
Martin Roetteler (Microsoft Research)
Simone Severini (University College London)
Vlatko Vedral (Oxford University and Centre for Quantum Technologies, Singapore)

A Single Entangled System Is an Unbounded Source of Nonlocal Correlations and of Certified Random Numbers*

Florian J. Curchod[1], Markus Johansson[†2], Remigiusz Augusiak[‡3], Matty J. Hoban[§4], Peter Wittek[¶5], and Antonio Acín[6]

1 **ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Barcelona, Spain**
2 **ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Barcelona, Spain**
3 **Center for Theoretical Physics, Polish Academy of Sciences, Warsaw, Poland**
4 **School of Informatics, University of Edinburgh, Edinburgh, UK**
5 **ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Barcelona, Spain**
6 **ICREA–Institució Catalana de Recerca i Estudis Avançats, Barcelona, Spain and ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Barcelona, Spain**

Abstract

The outcomes of local measurements made on entangled systems can be *certified* to be random provided that the generated statistics violate a Bell inequality. This way of producing randomness relies only on a minimal set of assumptions because it is independent of the internal functioning of the devices generating the random outcomes. In this context it is crucial to understand both qualitatively and quantitatively how the three fundamental quantities – entanglement, nonlocality and randomness – relate to each other. To explore these relationships, we consider the case where repeated (non projective) measurements are made on the physical systems, each measurement being made on the post-measurement state of the previous measurement. In this work, we focus on the following questions: *Given a single entangled system, how many nonlocal correlations in a sequence can we obtain? And from this single entangled system, how many certified random numbers is it possible to generate?* In the standard scenario with a single measurement in the sequence, it is possible to generate non-local correlations between two distant observers only and the amount of random numbers is very limited. Here we show that we can overcome these limitations and obtain *any* amount of certified random numbers from a single entangled pair of qubit in a pure state by making sequences of measurements on it. Moreover, the state can be arbitrarily weakly entangled. In addition, this certification is achieved by near-maximal violation of a particular Bell inequality for each measurement in the sequence. We also present numerical results giving insight on the resistance to imperfections and on the importance of the strength of the measurements in our scheme.

1998 ACM Subject Classification G.3 Probability and Statistics

* This work is supported by the ERC CoG QITBOX and AdG OSYRIS, the AXA Chair in Quantum Information Science, Spanish MINECO (QIBEQI and SEV-2015-0522), Fundación Cellex, Generalitat de Catalunya (SGR 875 and Cerca Program).
† M.J. acknowledges support from the Marie Curie COFUND action through the ICFOnest program.
‡ R. A. acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 705109.
§ M.J.H. acknowledges support from the EPSRC (through the NQIT Quantum Hub), the FQXi Large Grant Thermodynamic vs information theoretic entropies in probabilistic theories, and the hospitality of the Department of Computer Science at the University of Oxford.
¶ P.W. acknowledges computational resources granted by the High Performance Computing Center North (SNIC 2015/1-162 and SNIC 2016/1-320).

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 1; pp. 1:1–1:23
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Keywords and phrases Randomness certification, Nonlocality, Entanglement, Sequences of measurements

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.1

1 Introduction

Bell's theorem [4] has shown that the predictions of quantum mechanics demonstrate non-locality. That is, they cannot be described by a theory in which there are objective properties of a system prior to measurement that satisfy the no-signalling principle (sometimes referred to as "local realism"). Thus, if one requires the no-signaling principle to be satisfied at the operational level then the outcomes of measurements demonstrating non-locality must be unpredictable [4, 19, 15]. This unpredictability, or randomness, is not the result of ignorance about the system preparation but is *intrinsic* to the theory.

Although the connection between quantum non-locality (via Bell's theorem) and the existence of intrinsic randomness is well known [4, 19, 5, 15] it was analyzed in a quantitative way only recently [17, 7]. It was shown how to use non-locality (probability distributions that violate a Bell inequality) to *certify* the unpredictability of the outcomes of certain physical processes. This was termed *device-independent randomness certification*, because the certification only relies on the statistical properties of the outcomes and not on how they were produced. The development of information protocols exploiting this certified form of randomness, such as device-independent randomness expansion [17, 7, 23] and amplification protocols [8, 12], followed.

Entanglement is a necessary resource for quantum non-locality, which in turn is required for randomness certification. It is thus crucial to understand qualitatively and quantitatively how these three fundamental quantities relate to one another. In our work, we focus on asking how many observers in a sequence can be nonlocally correlated and how much certifiable randomness can be obtained from a single entangled state as a resource that is measured repeatedly. An important step to answer this question was recently made in [22], in which it was shown that nonlocality generated by a maximally entangled state can be shared between any number of distant observers, however, at the cost of exponentially diminishing the amount of nonlocality, as measured by the violation of the CHSH Bell inequality, between all the observers. Here we answer a significantly more demanding question that such correlations can be made arbitrarily close to extremal for each observer, a crucial property for randomness certification. In this particular sense we show that the nonlocality does not need to be diminished, as for each observer the generated correlations violate a particular Bell inequality (almost) maximally.

For randomness certification, progress has been made for entangled states shared between two parties, Alice (A) and Bob (B), in the standard scenario where each party makes a single measurement on his share of the system and then discards it. An argument adapted from Ref. [10] shows that either of the two parties, A or B can certify at most $2\log_2 d$ bits of randomness [2], where d is the dimension of the local Hilbert space the state lives in, which in turn implies a bound of $4\log_2 d$ bits when the two outputs are combined. This demonstrates a fundamental limitation for device-independent randomness certification in the standard scenario. The main goal of our work is to show that this limitation on the amount of certifiable random bits from one quantum state can be lifted. To do this we will consider the sequential scenario, where sequences of measurements can be applied to each local system. Our main result is to prove that an unbounded amount of random bits can be certified in this scenario.

Imagine the following situation where, contrary to the device-independent approach that we follow in this article, one has perfect control over the functioning of the device generating randomness. An entangled state initially prepared in the Pauli-Z basis, i.e., a σ_z eigenstate $|0\rangle$ or $|1\rangle$, is measured in the Pauli-X, or σ_x basis $|\pm\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. The outcome of this measurement is perfectly random and the post-measurement state is now one of the two eigenstates of the Pauli-X basis $|\pm\rangle$. If the device now measures this new state in the original Pauli-Z basis, the outcome of this new measurement is again random and one of the σ_z eigenstates is obtained. A device alternating between measurements in those two orthogonal basis thus allows one to obtain any amount of random bits from a single state as input.

Of course, this way of generating randomness can never be trusted, as one can always design a classical device (with deterministic outcomes – a local model) that has the same behavior as the device we described, i.e., their outputs are indistinguishable. To *certify* randomness one needs the generation of non-local correlations, that can not be simulated with classical resources. But is it nevertheless possible to use this idea of measuring a state repeatedly, in a scheme exploiting non-locality, to obtain more random numbers and beat the bounds on randomness certification? Clearly, certifying more randomness by making sequences of measurements on the same state depends on whether one is able to produce sequences of non-local correlations between distant observers, as otherwise no additional randomness can be certified. One of the obstacles to this is that if local (projective) measurements are used to generate the non-local correlations, the entanglement in the state is destroyed. Then the post-measurement state is separable and thus cannot be further used to generate nonlocality or to certify randomness. A challenge is therefore to come up with measurements that do not destroy all the entanglement in the state but nevertheless generate non-local correlations. With such measurements the post-measurement state will still be a potential resource for the generation of more non-local correlations and certified randomness.

Bell tests with sequences of measurements have received less attention in the literature than the standard ones with a single measurement round despite the novel features in this scenario [13], as for example the phenomenon known as hidden nonlocality [18]. In our work we show that they prove useful in the task of randomness certification, which also provides another example [2] where general measurements can overcome limitations of projective ones. More precisely, we describe a scheme where any number m of random bits are certified using a sequence of $n > m$ consecutive measurements on the same system. This work thus shows that the bound of $4\log_2 d$ random bits in the standard scenario can be overcome in the sequential scenario, where it is impossible to establish any bound. The unbounded randomness is certified by a near-maximal violation of a particular Bell inequality for each measurement in the sequence. Moreover, for any finite amount of certified randomness, our scheme has a finite (yet very small) noise robustness. Our results show that

This paper is an extended version of [9], where the main results are already included. The rest of the paper is organized as follows. In section 2, we describe the sequential scenario that allows for multiple measurements on the same state. In section 3, we generalize the concept of guessing probabilities – that allow to certify upper bounds on the predictive power of an adversary trying to guess the random numbers – to the sequential scenario and obtain new results on their continuity properties. In section 4 we introduce the main ingredients we will use in our scheme, in particular we introduce a family of measurements on two qubit states that allow us to retain some entanglement in the post-measurement states. In section 5 we describe our scheme that allows for the generation of nonlocal correlations between any number of distant observers and any amount of certified random numbers. In section 6 we present numerical results on the relation between the amount of violation of the family of inequalities introduced in [1] and the amount of randomness that can be certified from it. In section 7 we obtain numerical results to understand the relation between the strength of the

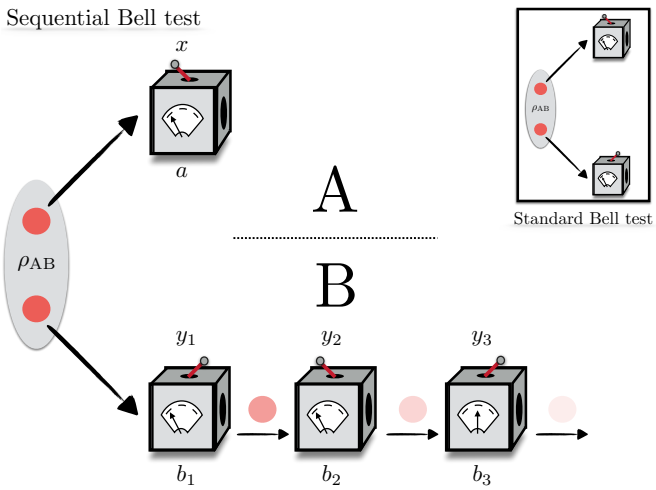

Figure 1 The standard scenario, where parties A and B make a single quantum measurement on their share of the state and discard it versus the sequential scenario where the second party B makes multiple measurements on his share.

measurement and the amount of randomness that can be certified from it. We conclude in section 8 with additional remarks and potential future work.

2 The sequential measurements scenario

Before presenting our results, let us introduce the scenario we work in. We carry over many of the features from the standard scenario except now we allow party B to make multiple measurements in a sequence on his share of the state. One can visualize this as in Fig. 1 where B is split up into several Bs, each one corresponding to a measurement made on the state and labeled by B_i, $i \in \{1, 2, .., n\}$, where n is the total number of measurements made in the sequence. Each B_i makes one measurement and the post-measurement state is sent to B_{i+1}. We organize the Bobs such that B_i is doing his measurement *before* B_j for $i < j$. Thus in principle B_j can receive the information about the inputs and outputs of previous measurements B_i for all $i < j$.

3 Randomness certification: from the standard to the sequential scenario

To quantify the randomness produced in the setup, we put the above scenario in the setting of *non-local guessing games* (e.g. Refs. [1, 16, 11, 2]). Let us consider an additional adversary Eve (E) who is in possession of a quantum system potentially correlated to the one of A and B. The global state is denoted ρ_{ABE}. We assume that at each round of the experiment, E is the one preparing the state ρ_{ABE} and distributes $\rho_{AB} = \mathrm{Tr}_E \rho_{ABE}$ to A and B. This state will be used to make the measurements in the sequence and the aim of E is to try to guess B's outcomes by using measurements on her share of the state ρ_{ABE}. The parties A and B_is, having no knowledge about the state or the real measurements made on it, see their respective devices as black boxes that receive some classical input $x \in \{0, 1\}$ and $y_i \in \{0, 1\}$, $y_1, y_2, .., y_n \equiv \vec{y}$, respectively, and that generate a classical output $a \in \{\pm 1\}$ and $b_i \in \{\pm 1\}$, $(b_1, b_2, .., b_n) \equiv \vec{b}$, respectively (see Fig. 1). They generate statistics from multiple runs of the experiment to obtain the observed probability distribution P_{obs} with elements $p_{\text{obs}}(a, \vec{b}|x, \vec{y})$. This distribution P_{obs} lives inside the set of quantum correlations

$\mathcal{Q}_n$ obtained from measurements on quantum states in a sequence as we described. This set is convex and thus can be described in terms of its extreme points, denoted P_{ext}, and any P_{obs} can be written as $P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}$, where $\sum_{\text{ext}} q_{\text{ext}} = 1$ and every $q_{\text{ext}} \geq 0$.

From studying the outcome statistics *only* we can bound E's predictive power by allowing her to have complete knowledge of how P_{obs} is decomposed into extreme points, i.e., she knows the probability distribution q_{ext} over extreme points P_{ext}. This predictive power is quantified via the *device-independent guessing probability* (DIGP) [1] where we fix the particular input string $y_1^0, y_2^0, .., y_n^0 \equiv \vec{y}^0$ for which E has to guess the outputs $\vec{b}$. The DIGP, denoted by $G(\vec{y}^0, P_{\text{obs}})$, is then calculated as the optimal solution to the following optimization problem [11, 16]:

$$G(\vec{y}^0, P_{\text{obs}}) = \max_{\{q_{\text{ext}}, P_{\text{ext}}\}} \sum_{\text{ext}} q_{\text{ext}} \max_{\vec{b}} p_{\text{ext}}(\vec{b}|\vec{y}^0)$$

subject to:

$$p_{\text{ext}}(\vec{b}|\vec{y}^0) = \sum_a p_{\text{ext}}(a, \vec{b}|x, \vec{y}^0), \qquad \forall x \tag{1}$$

$$P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}, \qquad P_{\text{ext}} \in \mathcal{Q}_n. \tag{2}$$

The operational meaning of this quantity is clear: Eve has a complete description of the observed correlations in terms of extreme points. She then guesses the most probable outcome for each extreme point. The standard scenario with a single measurement round can also be represented in this formalism by simply considering that $\vec{b} = b$ and $\vec{y}^{(0)} = y^{(0)}$. To quantify the amount of bits of randomness that is certified, we use the *min entropy* $H(\vec{y}^0, P_{\text{obs}}) = -\log_2 G(\vec{y}^0, P_{\text{obs}})$ which returns m bits of randomness if $G(\vec{y}^0, P_{\text{obs}}) = 2^{-m}$. The amount of bits of randomness quantified in this way is the figure of merit in this work and our goal is to obtain as many bits as possible from a single system.

We will now derive some general properties of the guessing probability (2) in the form of theorems 3 and 4. Let us stress here that these results are not limited to the guessing probability used in this work but are general properties of guessing probabilities. A more detailed discussion and an introduction to the topic of guessing probabilities and their use in randomness certification can be found in the appendices, as well as the proofs of the theorems that we discuss here.

For a single measurement on each system (i.e. a sequence of $n = 1$ measurement), which corresponds to the standard Bell scenario and $\mathcal{Q} \equiv \mathcal{Q}_1$ the set of quantum correlations for a single measurement on each subsystem we have that:

▶ **Proposition 1.** *The function $G(y^0, P_{obs})$ on the set of quantum distributions $\mathcal{Q}$ is continuous in the interior of $\mathcal{Q}$.*

▶ **Proposition 2.** *The function $G(y^0, P_{obs})$ is continuous in any extremal point of $\mathcal{Q}$.*

The proofs of these two propositions are based mostly on general properties of concave functions [20] and of concave roof extensions in particular [6], and can be found in section B of the appendices. In other words the guessing probability for a single measurement is continuous everywhere except possibly on some points that lie on the surface of the quantum set but that are not extremal. An example of this can be obtained from the measurements described in [17] for a state with arbitrarily little entanglement. The joint conditional probability distribution (introduced below, see (6)) corresponding to those measurements made on such a state has $G(y^0, P_{obs}) = 1/2$ and is at the same time arbitrarily close to a joint conditional probability distribution corresponding to measurements on a product state with $G(y^0, P_{obs}) = 1$, i.e., a local point. The key is that this local point is not extremal, it

lies somewhere on the surface of the local (and quantum) set but can be decomposed into other extremal (local) points, i.e. is not a vertex of the local polytope. Discontinuities of $G(y^0, P_{\text{obs}})$ can thus appear only at the boundary between extremal points and non-extremal points lying on the surface of the set, and in the rest of the set it is continuous.

In general – and in particular in our work – the optimization problem (2) can be relaxed to an optimization where instead of insisting on $P_{\text{obs}} = \sum_{\text{ext}} q_{\text{ext}} P_{\text{ext}}$ (2), one only imposes that the observed statistics P_{obs} give a particular Bell inequality violation [17]. The optimal solution to this new problem is an upper bound to the optimal solution of (2). Crucially, this relaxation often gives non trivial bounds as shown in our case for example. From now on, every time we refer to a guessing probability we refer to this relaxation of the problem to a particular Bell inequality violation.

Now we consider a Bell expression I with its maximal value $t_{\max}$ on the quantum set $\mathcal{Q}$. We define the hyperplane H_t to contain the elements of $\mathcal{Q}$ for which the value of I is $t \leq t_{\max}$ and further we define the restriction $G(y^0, P_{\text{obs}})_t$ of $G(y^0, P_{\text{obs}})$ to the intersection of H_t with $\mathcal{Q}$ and let $\max G(y^0, P_{\text{obs}})_t$ be the maximum of the guessing probability on this intersection. From Propositions (1) and (2) we can show that:

▶ **Theorem 3.** *If the intersection of $H_{t_{max}}$ with $\mathcal{Q}$ is a single (thus extremal) point, there exists a $t_c < t_{max}$ such that $G(y^0, P_{obs})_t$ is a continuous function of t for $t_c \leq t \leq t_{max}$*

The proof of this theorem can be found in section C of the appendices. In the other case, if the intersection of $H_{t_{\max}}$ with $\mathcal{Q}$ has more than one point, it also contains a set of non-extremal points of $\mathcal{Q}$ and therefore a discontinuity of $G(y^0, P_{\text{obs}})_t$ at $t_{\max}$ can not be ruled out by theorem (3). In other words, if the violation of a particular Bell inequality I is achieved by a unique quantum point (as for example the following (5)), the guessing probability close to that point is continuous.

Until now, we have considered the continuity properties of the guessing probability in the standard scenario with a single measurement in the sequence. Now we would like to extend those results to the guessing probability in the sequential measurement scenario with $n \geq 2$ measurements being made on the subsystems. Remember that we split party B into many B_i, so that party B_i makes the ith measurement on the system. The measurement setting of B_i is y_i and its outcome b_i (see Fig. 1). In our work, we will always take $y_i \in \{0, 1\}$ and $b_i \in \{0, 1\}$, but the following results can be generalized to any number of inputs and outcomes (they may even be different for each measurement in the sequence).

Now consider the joint conditional probability distributions $P^i_{\text{obs}}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})$ between A and each B_i, that is the joint conditional probability distribution between A and B_i conditioned on what happened before the ith measurement, namely the input choices $y_1, ..., y_{i-1}$ and the outcomes $b_1, ..., b_{i-1}$ that were obtained *before* measurement i. There are n of those joint conditional probability distributions living in $\mathcal{Q}$ that can be obtained directly from the whole probability distribution for the sequence $P_{\text{obs}}(a\vec{b}|x\vec{y})$ living in $\mathcal{Q}_n$. Now suppose that we play, for each distribution $P^i_{\text{obs}}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})$, a Bell game I_i such that $I_i(P_i(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})) = t_i \leq t_i^{\max}$, where $t_i^{\max}$ is the maximum of I_i over the set $\mathcal{Q}$.

▶ **Theorem 4.** *Suppose that each joint conditional probability distribution $P^i_{obs}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})$ between A and B_i in the sequence is such that $I_i(P_i(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})) = t_i$ and consider the limit where each $t_i \to t_i^{max}$. Suppose also that for each i, $G_i(y_i^0, P^i_{obs}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1}))$ attains its smallest possible value at $t_i = t_i^{max}$. Then if the maximal value t_i^{max} of each I_i is achieved in a unique quantum point in $\mathcal{Q}$:*

$$G(\vec{y}^0, P_{obs}(a\vec{b}|x\vec{y})) \to \prod_{i=1}^{n} G_i(y_i^0, P^i_{obs}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1})) \tag{3}$$

where $G_i(y_i^0, P^i_{\text{obs}}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1}))$ is the (non sequential) relaxed guessing probability (2) of an adversary E trying to guess outcome b_i for input y_i^0 from the observed joint probability distribution $P^i_{\text{obs}}(a, b_i|x, y_1, ..., y_i, b_1, ..., b_{i-1}))$. The proof of this theorem can be found in appendices D and E. In other words, if each measurement in the sequence taken separately – thus not seen as in a sequence – leads to correlations close enough to the unique maximal violation of inequality I_i between A and B_i only, and if this maximal violation corresponds to the minimal possible guessing probability for b_i, then the guessing probability for the whole sequence tends to the product of the individual guessing probabilities of the outcomes b_i.

Before presenting our results, it is worth explaining why the causal constraints imposed by the sequential scenario make it stronger than standard Bell tests with one measurement in the sequence. At first sight, one could be tempted to group all the measurements in the sequence into a single box receiving an input string $\vec{y}_n$ to output another string $\vec{b}_n$, as in a standard Bell test. However, in general a sequence of measurements can not be represented as a single measurement. To understand this, note that in the sequential scenario the outcome b_i can depend only on variables produced in its past, namely the input choices $y_1, y_2, ..., y_i$ and the outcomes $b_1, b_2, ..., b_{i-1}$ that were *previously* obtained. However, in the single measurement scenario, the measurement box receives all inputs and produces all outputs at once. In particular, outcome b_i can now be a function of input choices $y_{j>i}$ and outcomes $b_{j>i}$ that are produced in the *future*. That is, such a big box may violate the physical constraints coming from the sequential arrangement and the assumption that signaling from the future to the past is impossible. These additional causality constraints further limit Eve's predictability with respect to a standard Bell test and are responsible of the unbounded amount of certified randomness.

4 Making non-destructive measurements on qubit states

Alice and Bob share the pure two-qubit state

$$|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{4}$$

that for all $\theta \in]0, \pi/2[$ is entangled. In Ref. [1], a family of Bell inequalities was introduced:

$$I_\theta = \beta\langle\mathbb{B}_0\rangle + \langle\mathbb{A}_0\mathbb{B}_0\rangle + \langle\mathbb{A}_1\mathbb{B}_0\rangle \qquad + \langle\mathbb{A}_0\mathbb{B}_1\rangle - \langle\mathbb{A}_1\mathbb{B}_1\rangle \tag{5}$$

where $\beta = 2\cos(2\theta)/[1 + \sin^2(2\theta)]^{1/2}$, $\langle\mathbb{B}_y\rangle = p(b = +1|y) - p(b = -1|y)$ and $\langle\mathbb{A}_x\mathbb{B}_y\rangle = p(a = b|xy) - p(a \neq b|xy)$ for x, $y \in \{0, 1\}$. This family of inequalities has the following two useful properties: first, its maximal quantum violation, $I_\theta^{\max} = 2\sqrt{2}\sqrt{1 + \beta^2/4}$, is obtained by measuring the state (4) with measurements:

$$\begin{aligned} \mathbb{A}_0 &= \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, \qquad & \mathbb{B}_0 &= \sigma_z, \\ \mathbb{A}_1 &= \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, \qquad & \mathbb{B}_1 &= \sigma_x, \end{aligned} \tag{6}$$

where $\tan\mu = \sin(2\theta)$. Second, when maximally violated, the inequality certifies one bit of local randomness on Bob's side for his second measurement choice $y^0 = 1$: $G(y^0 = 1, P^{\max}_{\text{obs}}) = 1/2$ [1]. These observations are possible because the maximal violation is *uniquely* achieved by the probability distribution $P^{\max}_{\text{obs}}$ that arises from the previously-described state and measurements (4) and (6). Therefore, for the maximal violation, $P^{\max}_{\text{obs}} = P_{\text{ext}}$ in (2) and the guessing probability for input choice $y^0 = 1$ is equal to $1/2$.

However, in general we may not get correlations that maximally violate our Bell inequality but give a violation that is only close to maximal. In section 3 we have shown how to make conclusions about the guessing probability for non-maximal violations. In particular, we

showed that for *any* Bell inequality with a unique point of maximal violation, the guessing probability is a continuous function of the value of the inequality close to the maximal violation. This implies in the particular case we are studying that:

$$I_\theta \to I_\theta^{max} \quad \Rightarrow \quad G(y^0 = 1, P_{\text{obs}}) \to \frac{1}{2}. \tag{7}$$

In section 6, we also provide a numerical upper bound on the guessing probability $G(y^0 = 1, P_{obs})$ by a concave function of the value of I_θ.

Bell inequalities (5) are the first main ingredient in our sequential construction below. The second one is the use of general, non-projective measurements. Indeed, if B_1 performs a projective measurement on the shared entangled state, the resulting post-measurement state, now shared between Alice and B_2, is separable and thus useless for randomness production. Consequently, one needs to consider non-projective measurements to retain some entanglement in the system for the subsequent measurements. For this purpose, let us introduce the following two-outcome quantum measurement (written in the formalism of Kraus operators):

$$M_{\pm 1}(\xi) = \cos\xi|\pm\rangle\langle\pm| + \sin\xi|\mp\rangle\langle\mp| \tag{8}$$

corresponding to the two outcomes $\{\pm 1\}$. This measurement $\hat{\sigma}_x(\xi) \equiv \{M_{+1}^\dagger M_{+1}, M_{-1}^\dagger M_{-1}\}$ can be understood as a generalization of the projective measurement σ_x. It varies from being projective (for $\xi = 0$) to being non-interacting (for $\xi = \pi/4$). One can verify that measuring an entangled state (4) for $\xi \in]0, \pi/4]$ (non-projective measurement) the post-measurement state still retains some entanglement, irrespectively of the outcome. Therefore, by tuning the parameter ξ we are able to vary the destruction of the entanglement of the state at the gain of extracting information from it (cf. Ref. [22]): the closer to being a projective measurement, the lower the entanglement in the post-measurement state, but the bigger the violation of the initial Bell inequality.

5 A scheme for an unbounded amount of nonlocal correlations and certified random numbers

We now combine the previous observations to demonstrate our main result. First, let us recall that, as shown in [1], one can obtain one bit of randomness from any pure entangled two qubit state, irrespective of the amount of entanglement in it. Moreover, one can verify that approximately one random bit can be certified if the measurements are close to the ones in Eq. (6) (in the sense that $\hat{\sigma}_x(\xi)$ is close to a measurement of σ_x for $\mathbb{B}_1$ in Eq. (6)) since I_θ is then close to $I_\theta^{\max}$ in Eq. (7). Second, the measurement in Eq. (8) is only close to projective for ξ close to zero and leaves entanglement in the post-measurement state between Alice and Bob which is thus still useful for randomness certification. By repeated use of these two properties we can certify the production of an unbounded amount of random bits from a single pair of entangled qubits. We now formally describe this process in which Alice makes a single measurement on her share of the state, whereas Bob makes a sequence of n measurements on his.

Each B_i chooses between measurements of σ_z and $\hat{\sigma}_x(\xi_i)$ (8) for inputs $y_i = 0$ and $y_i = 1$, respectively, with outcomes $b_i \in \{\pm 1\}$. The parameter ξ_i is fixed before the beginning of the experiment. The initial entangled state shared between Alice and Bob, before B_1's measurement, is $|\psi^{(1)}(\theta_1)\rangle$ (see Eq. (4) with $\theta = \theta_1$). If the first non-projective measurement of the operator $\hat{\sigma}_x(\xi_1)$ is made by B_1 on the initial state $|\psi^{(1)}(\theta_1)\rangle$, the post-measurement state is of the form

$$|\psi_{b_1}^{(2)}(\theta_1, \xi_1)\rangle = U_A^{b_1}(\theta_1, \xi_1) \otimes V_B^{b_1}(\theta_1, \xi_1)(c|00\rangle + s|11\rangle)\,, \tag{9}$$

where $c = \cos(\theta_{b_1}(\theta_1, \xi_1))$ and $s = \sin(\theta_{b_1}(\theta_1, \xi_1))$ and the two unitaries, $U_A^{b_1}(\theta_1, \xi_1)$ and $V_B^{b_1}(\theta_1, \xi_1)$, and angle $\theta_{b_1}(\theta_1, \xi_i) \in]0, \pi/4]$ depend on the first outcome b_1 and the angles θ_1 and ξ_1.

After his measurement, B_1 applies the unitary $(V_B^{b_1})^\dagger$, conditioned on his outcome b_1, on the post-measurement state going to B_2. This allows B_2 to use the same two measurements $\hat{\sigma}(\xi_2)$ and σ_z independently of the outcome b_1 since the unitary $(V_B^{b_1})$ is canceled in (9). This last procedure will be applied by each B_i after his measurement, before sending the post-measurement state to the next B_{i+1}. If the system passed through *only* the non-projective measurements, the state received by B_i can be one of 2^{i-1} potential states, depending on all of the previous B_j's ($j < i$) outcomes (one for each combination $\vec{b}_{i-1} \equiv (b_1, b_2, .., b_{i-1})$ of outcomes obtained by the previous B_j, these can be computed *before* the beginning of the experiment). Any of these states can be written as:

$$|\psi^{(i)}_{\vec{b}_{i-1}}\rangle = U_A^{\vec{b}_{i-1}} \otimes \mathbb{1}_B \left[\cos(\theta_{\vec{b}_{i-1}})|00\rangle + \sin(\theta_{\vec{b}_{i-1}})|11\rangle\right], \tag{10}$$

where the angles $\theta_{\vec{b}_{i-1}}$ and the matrix $U_A^{\vec{b}_{i-1}}$ both depend on the outcomes $\vec{b}_{i-1}$, on the initial angle θ_1 and the angles ξ_j of the previous B_j's with $j < i$. In the notation, we will always omit the dependence on the angles θ_1 and $\xi_1, \xi_2, .., \xi_j$ since these are fixed *before* the beginning of the experiment. For each of these different potential states with angle $\theta_{\vec{b}_{i-1}}$, Alice adds two measurements to her input choices, where for $k \in \{0, 1\}$, these are measurements of the observables $\mathbb{A}_k^{\vec{b}_{i-1}}$ which are defined as

$$U_A^{\vec{b}_{i-1}} \left[\cos(\mu_{\vec{b}_{i-1}})\sigma_z + (-1)^k \sin(\mu_{\vec{b}_{i-1}})\sigma_x\right] (U_A^{\vec{b}_{i-1}})^\dagger, \tag{11}$$

where $\tan(\mu_{\vec{b}_{i-1}}) = \sin(2\theta_{\vec{b}_{i-1}})$, depending on the specific state $|\psi^{(i)}_{\vec{b}_{i-1}}\rangle$ (10).

We are now ready to describe how the scheme certifies randomness. The measurement operator $\hat{\sigma}_x(\xi_i)$ can be made arbitrarily close to σ_x by choosing ξ_i sufficiently small. This brings the outcome statistics for measurements $\hat{\sigma}_x(\xi_i), \sigma_z$ on Bob's side and $\mathbb{A}_0^{\vec{b}_{i-1}}, \mathbb{A}_1^{\vec{b}_{i-1}}$ on Alice's side on the state in Eq. (10), arbitrarily close to the statistics for the measurements in Eq. (6) and a state of the form in Eq. (4), for $\theta = \theta_{\vec{b}_{i-1}}$. Therefore, the inequality $I_{\theta_{\vec{b}_{i-1}}}$ for Alice and B_i as defined in (5) can be made arbitrarily close to its maximal violation. This in turn guarantees that the guessing probability, $G(y_i^0 = 1, P_{obs})$ can be made arbitrarily close to 1/2. Note that this guessing probability does not only describe the instances when Alice chooses the measurements $\mathbb{A}_j^{\vec{b}_{i-1}}$. Since Eve does not know Alice's measurement choices in advance she cannot use a strategy that gives higher predictive power for the instances when Alice chooses other measurements. Finally, by making $G(y_i^0 = 1, P_{obs})$ sufficiently close to 1/2 for each i (by choosing each ξ_i sufficiently close to 0) the DIGP $G(y_1^0, y_2^0, .., y_n^0, P_{obs})$ can, by continuity, be made arbitrarily close to 2^{-n} (see theorem 4 of section 3.)

At the end, Bob can produce m random bits by a suitably chosen sequence $\hat{\sigma}_x(\xi_i)$, $i \in \{1, 2, .., n\}$, of $n > m$ measurements. The certification only requires that each B_i occasionally chooses the projective measurement σ_z so that the whole statistics can be obtained. Note that Bob can choose σ_z with probability γ_i and $\hat{\sigma}_x(\xi_i)$ with probability $1 - \gamma_i$ for γ_i as close to zero as he wants. Finally, note that the value of *each* inequality $I_{\theta_{\vec{b}_{i-1}}}$ between each B_i and A can be made as close as wanted to the maximal value $I^{\max}_{\theta_{\vec{b}_{i-1}}}$. Therefore, we can certify randomness for each measurement B_i in the sequence at the expense of increasing the number of measurements that Alice chooses from.

This protocol can also be used to certify any finite amount of randomness with some small but strictly non-zero noise robustness. Indeed, assume the goal is to certify m random bits. One can then run the protocol for $m' > m$ bits. By continuity, when adding a small but

finite amount of noise the protocol will certify m random bits. Of course, the noise robustness tends to zero with the number of certified random bits. However, we expect this to be the case for any protocol. This conjecture is based on the following argument: each measurement of a particle of finite dimension can produce only a finite amount of randomness. Thus, to get unbounded randomness, an infinite number of measurements are needed. Moreover, a measurement that is very close to non-interacting is unlikely to produce nonlocal correlations and is thus useless to certify randomness. It therefore appears quite likely that, in the infinite limit, any sequence of local measurements that are useful for randomness certification will destroy all the entanglement in the state, so that the resulting noise resistance tends to zero. We therefore expect that, while quantitative improvements over our protocol in terms of noise robustness can be expected, from a qualitative point of view it goes as far as possible.

6 Numerical bounds on the amount of violation of the family of Bell inequalities of [1] and the certified randomness

Let us now explain some numerical results that should provide some quantitative intuition on the relation between the amount of violation of the family of inequalities (5) and the amount of random bits certified by this violation. This allows one to evaluate how close the value I_θ of the inequalities (5) should be to the maximal one I_θ^{max} in order to certify close to one perfect random bit from the statistics for one measurement $n = 1$.

Let us consider the following two-parameter class of Bell inequalities:

$$I_{\alpha,\beta} := \beta\langle\mathbb{B}_0\rangle + \alpha(\langle\mathbb{A}_0\mathbb{B}_0\rangle + \langle\mathbb{A}_1\mathbb{B}_0\rangle) + \langle\mathbb{A}_0\mathbb{B}_1\rangle - \langle\mathbb{A}_1\mathbb{B}_1\rangle \leq \beta + 2\alpha \tag{12}$$

where $\alpha \geq 1$ and $\beta \geq 0$ such that $\alpha\beta < 2$. For $\alpha = 1$ the above class reproduces the family of Bell inequalities (5) with $\beta = 2\cos(2\theta)/[1 + \sin^2(2\theta)]^{1/2}$. In [1] it was proved that the maximal quantum value $I_{\alpha,\beta}^{\max}$ for these inequalities is given by:

$$I_{\alpha,\beta}^{\max} = \sqrt{(1+\alpha^2)(4+\beta^2)}. \tag{13}$$

Now, we conjecture that the following inequality is satisfied by $I_{\alpha\beta}$:

$$I_{\alpha,\beta}^2 + (2-\alpha\beta)^2\langle\mathbb{B}_1\rangle^2 \leq (1+\alpha^2)(4+\beta^2). \tag{14}$$

We have numerically evaluated this inequality for various values of α and β by maximizing its left-hand side over general one-qubit measurements $\mathbb{A}_i = \vec{m}_i \cdot \vec{\sigma}$ and $\mathbb{B}_i = \vec{n}_i \cdot \vec{\sigma}$ with $\vec{m}_i, \vec{n}_i \in \mathbb{R}^3$ such that $|\vec{m}_i| = |\vec{n}_i| = 1$ for $i = 0, 1$, and two-qubit pure entangled states that can always be written as

$$|\psi\rangle = \cos t|00\rangle + \sin t|11\rangle \tag{15}$$

with $t \in [0, \pi/2]$ now being independent of β. The obtained values were always smaller than or equal to the right-hand side of (14). Notice that in the case of Bell scenarios with two dichotomic measurements one can always optimize expression like the above one over qubit measurements and states (see e.g. Ref. [1]).

From (14), it is easy to obtain an upper bound on the expectation value:

$$|\langle\mathbb{B}_1\rangle| \leq \frac{\sqrt{(1+\alpha^2)(4+\beta^2) - I_{\alpha,\beta}^2}}{2-\alpha\beta} = \frac{\sqrt{(I_{\alpha,\beta}^{\max})^2 - I_{\alpha,\beta}^2}}{2-\alpha\beta}, \tag{16}$$

which, due to the fact that the right-hand side of the above is a concave function in $I_{\alpha,\beta}$, implies an upper bound on the guessing probability:

$$G(y^0 = 1, P_{obs}) \leq \frac{1}{2} + \frac{\sqrt{(I_{\alpha,\beta}^{\max})^2 - I_{\alpha,\beta}^2}}{2(2-\alpha\beta)} \equiv f(I_{\alpha\beta}). \tag{17}$$

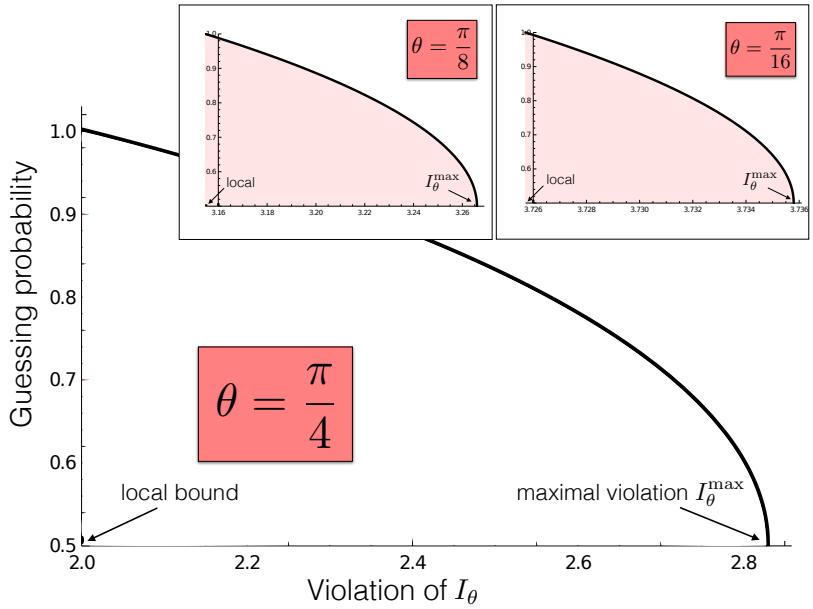

Figure 2 Our numerical upper bounds on the guessing probability in function of the violation of I_θ for $\theta = \frac{\pi}{4}, \frac{\pi}{8}, \frac{\pi}{16}$, where $I_{\theta=\frac{\pi}{4}} =$ CHSH. One can see that these are tight both at the maximal violation of the inequality and at its local bound.

In the particular case of maximal violation of the inequality $I_{\alpha\beta}$ (12) – which saturates inequality (14), this bound implies that the outcome of the first Bob's measurement is completely unpredictable, $G(y^0 = 1, P_{obs}) = 1/2$. Our numerical bound is thus tight at the maximal quantum violation of the inequality, but also when $I_{\alpha\beta}$ attains its classical value $2\alpha + \beta$, for which $G(y^0 = 1, P_{\text{obs}}) = 1$. In general, however, the bound (17) is not tight. Still, it provides a good bound on the guessing probability in terms of the amount of violation of $I_{\alpha\beta}$ (12) and thus also of the family of inequalities I_θ (5) we were using in our scheme.

For example, one can insert the maximal quantum value $I_\theta^{\max}$ (13) in (16) or in (17) and get that $\langle \mathbb{B}_1 \rangle = 0$ or $G(y^0 = 1, P_{obs}) = \frac{1}{2}$, which coincides with the certification of one perfect local random bit for input $y_0 = 1$ on Bob's side for the maximal violation of I_θ. Since the probability distribution of maximal violation is unique, the point is necessarily an extreme point [1], so we can directly use the observed probability distribution P_{obs} to bound the eavesdropper's predictive power (as an extreme point allows only for one decomposition: itself).

Let us finally consider the case of $\alpha = 1$ and $\beta = 2\cos(2\theta)/[1 + \sin^2(2\theta)]^{1/2}$, which results in the Bell inequality (5) considered in the main text. Figure 3 presents the bound (17) for three values of θ, in particular for $\theta = \pi/4$ which corresponds to the CHSH Bell inequality. This should provide one with an intuition of how close quantitatively to the maximal violation I_θ^{max} the observed value I_θ should be in order to get close to one perfect local bit of randomness ($G(y = 1, P_{obs}) \to 1/2$) for a state with a given angle θ.

7 The amount of certified randomness as a function of the strength of the measurement

We know already that the violation of a Bell inequality certifies the existence of randomness in the outcomes of the measurements. The other way is also true, namely that if the solution of the optimization problem (2) gives a solution $G(y^0, P_{obs}) < 1$ then the observed behavior P_{obs}

is necessarily nonlocal. On a purely qualitative level, certified randomness in the outcomes is equivalent to nonlocal correlations.

In this section we analyze with the help of numerical tools the dependency of the certified randomness from the violation of the family of Bell inequalities (5) on the strength parameter ξ of the measurements $\hat{\sigma}_x(\xi) = cos(2\xi)\sigma_x$ (8). For example, what is the maximal value of the parameter ξ – i.e. the minimal strength of the measurement –such that we can generate nonlocal correlations (and thus randomness) from this measurement on an entangled state of the form $|\psi(\theta)\rangle$ (4)? Do less entangled states need stronger measurement to unveil their nonlocal behavior?

To answer these questions, we have been using semi-definite programing (SDP) techniques as explained in [3, 16] to obtain numerical upper bounds on the guessing probabilities (2). One can find the computational details – presented in a pedagogical way – online at `https://github.com/peterwittek/ipython-notebooks/blob/master/Unbounded_randomness.ipynb`. Here we work in the standard scenario with only one measurement $n = 1$ in the sequence. We used states of the form (4):

$$|\psi(\theta)\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle \tag{18}$$

and measurements (6):

$$\begin{aligned} \mathbb{A}_0 &= \cos\mu\,\sigma_z + \sin\mu\,\sigma_x, & \mathbb{B}_0 &= \sigma_z, \\ \mathbb{A}_1 &= \cos\mu\,\sigma_z - \sin\mu\,\sigma_x, & \mathbb{B}_1 &= \hat{\sigma}_x(\xi) = cos(2\xi)\sigma_x, \end{aligned} \tag{19}$$

where $tan(\mu) = sin(2\theta)$. These measurements correspond to the ones in our scheme for an unbounded amount of randomness and where the second measurement $y = 1$ of B is the tunable version $\hat{\sigma}_x(\xi) \equiv \{M_{+1}^{\dagger}M_{+1}, M_{-1}^{\dagger}M_{-1}\}$ of Eq. (8):

$$M_{\pm 1}(\xi) = \cos\xi|\pm\rangle\langle\pm| + \sin\xi|\mp\rangle\langle\mp|, \tag{20}$$

with $\xi \in [0, \frac{\pi}{4}]$. For example, if the parameter $\xi = 0$, the four (projective) measurements in Eq. (19) on any quantum state $|\psi(\theta)\rangle$ with angle θ (18) generates a behavior P_{obs}^{θ} leading to the maximal violation of the inequality I_θ (5) for the same value of θ. This implies that extremal nonlocal correlations are generated and from the results of [1] we know that one perfect random bit – equivalently $G(y^0 = 1, P_{obs}^{\theta}) = \frac{1}{2}$ – is produced. This corresponds to the strongest (projective) version of the measurements. Now, as we increase the parameter $\xi > 0$ of B's $y = 1$ measurement, $\hat{\sigma}_x(\xi)$ gets weaker, the generated correlations cease to be extremal and less than one random bit is produced. At some point, at a particular value $\xi_{\max}^{\theta}$ the measurement of B is so weak that we expect the generated correlations to become local. This exact value might depend on the amount of entanglement θ in the state. The bounds obtained by SDP indicate that this dependency on the angle θ of the maximal value $\xi_{\max}^{\theta}$ is relatively small. As we vary the angle θ, the minimal required strength of the measurement to generate a nonlocal behavior P_{obs}^{θ} stays within a narrow interval: $\xi_{\max}^{\theta} \in [0.519, 0.576]$ for $\theta \in [\frac{\pi}{32}, \frac{\pi}{4}]$.

We now present the results in the form of a graph (see Fig.3). A complete tables with our results for the different states and bounds on the guessing probabilities can be found in the appendices F.

As expected the amount of certified randomness for each state $|\psi(\theta)\rangle$ is one bit when the measurement is projective (for $\xi = 0$) as the correlations are the extremal ones described in [1] regardless of the entanglement θ in the state. As ξ increases the lower bounds on the certified randomness rapidly decreases, with a more rapid decrease for smaller θ. Interestingly, and up to (high) numerical precision, for all values of θ the bounds reach zero certified randomness around the same value $\xi_{\max} \in [0.519, 0.576]$. This indicates, again up to numerical precision,

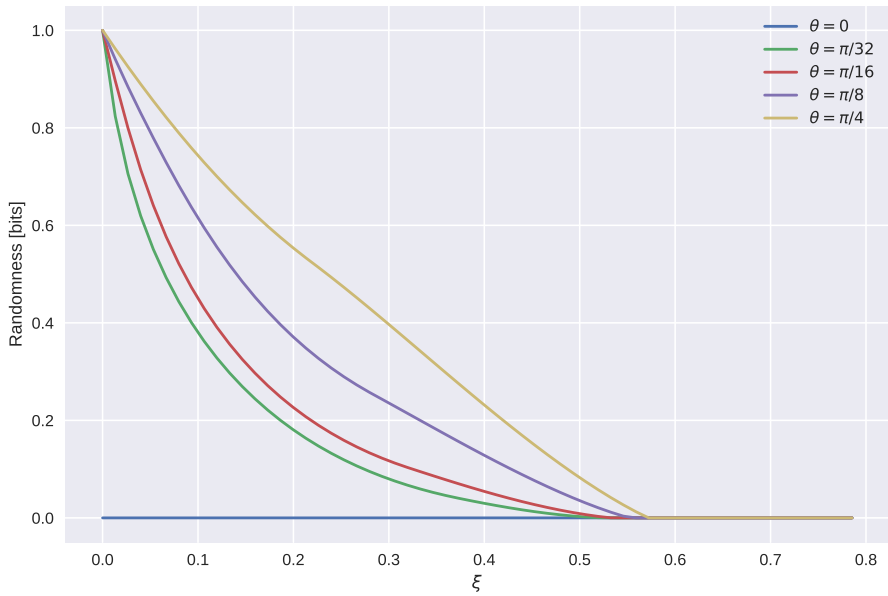

Figure 3 Lower bounds on the amount of randomness certified from the quantum state (4) with angles $\theta = 0, \frac{\pi}{32}, \frac{\pi}{16}, \frac{\pi}{8}, \frac{\pi}{4}$ as function of the strength of the measurement ξ. The measurement is projective for $\xi = 0$ – which certifies the maximal amount of randomness – and is non interacting with the system when $\xi = \frac{\pi}{4}$. It is intriguing to see that for the cases of $\frac{\pi}{32} \leq \theta \leq \frac{\pi}{4}$ considered the generated behavior become local in a small interval $\xi_{\max} \in [0.519, 0.576]$.

that all the generated P^{θ}_{obs} become local – or stop generating randomness – around this critical value.

In the end, we are interested primarily in the amount of certified randomness from P^{θ}_{obs} *close to* the maximal violation of I_θ, corresponding to $\xi \to 0$. There, the SDP solutions indicate that the correlations resisting the best to the weakening of the measurement $\xi > 0$ are the ones coming from the measurements made on the maximally entangled state. Indeed, if the bounds are close to the actual values of certified randomness it is quite clear from the numerical results that the more the state is entangled ($\theta \to \frac{\pi}{4}$) the better it resists. The less entangled states ($\theta \to 0$) appear to generate exponentially less randomness when the parameter ξ increases, or equivalently when the correlations cease to be extremal. This tells us that even though our scheme certifies an unbounded amount of randomness from states $|\psi(\theta)\rangle$ with any nonzero amount of entanglement, i.e. any $\theta > 0$, it is preferential from a practical point of view to use the maximally entangled state as the initial state.

8 Conclusion

We have presented a scheme for certifying an unbounded amount of random bits from a single pair of entangled qubits in the scenario where one of the qubits is subjected to a sequence of measurements. The measurements do not completely destroy the entanglement but map the state to another pure entangled two-qubit state (with reduced entanglement). Our main result made use of the fact that every measurement in Bob's sequence generated an almost-maximally non-local output distribution (in the sense of violating some Bell inequality almost maximally). In Ref. [22], a sequence of non-local correlations is obtained from a single pair of qubits, showing that the nonlocality of a state can be shared between many parties. While it also considers sequences of measurements, one can show that the

correlations obtained in their work do not generate more certified randomness than the simple standard single measurement scenario. Indeed, the maximum of randomness is achieved when all but one measurements do not interact with the particle and their scheme is thus optimal when coinciding with a single measurement one. In our work, we overcome this limitation by producing (almost) extremal correlations for each measurement in the sequence, which is a fundamental property of potential further use for many other device-independent quantum information tasks (in particular for randomness certification). Our work is in many respects a proof-of-principle result: First, it requires an exponentially increasing number of measurements on Alice's side, namely $\sum_{i=1}^{n} 2^i = 2(2^n - 1)$ measurement choices for n measurements in the sequence. Second, the result is based on a continuity argument and there is no control on the noise robustness. All these issues deserve further investigation. Finally, it is worth exploring how to design device-independent randomness generation protocols involving sequences of measurements. However, the sequential scenario is much more demanding from an implementation point of view, because it requires quantum non-demolition measurements. It is then unclear whether with present or near future technology sequential protocols will provide a significant practical advantage over simpler protocols based on standard Bell tests. However, the first experimental works observing non-local correlations in the sequential scenario have recently been reported [21, 14]. In any case, the main implications of our work are fundamental: It shows that a single pair of pure entangled qubits is a potentially unbounded source of certifiable random bits when performing sequences of measurements on it.

We have also provided numerical results that gives us an insight on the resistance to imperfections of a potential protocol that implements our scheme. For a single measurement in the sequence, we have given numerical bounds on how the certified randomness diminishes as the generated correlations cease to be extremal. Second, we have also explored how the certified randomness diminishes when the strength of the measurement is lowering. This allows us to expect that any potential protocol trying to implement our scheme for a finite amount of randomness starting from a single entangled system has an advantage using a maximally entangled one. It is clear from our numerical results that this state offers the best resistance to imperfections. So, while it is true that even arbitrarily little entangled states are a source of unbounded certified randomness, more entanglement offers an advantage in terms of resistance to imperfections.

It would also be interesting to explore whether an unbounded amount of randomness can be obtained versus a post-quantum adversary E, only constrained by the no-signaling condition, trying to guess the outcomes of the measurements. Or, on the contrary, is the amount of certified randomness against no-signaling adversaries bounded also in the sequential scenario? Our conjecture is that the amount of randomness that can be certified is limited in this case. Indeed, the fact that the no-signaling set – consisting of all correlations constrained only by the no-signaling conditions – does not have a continuous set of extremal points (it is a polytope) makes it impossible to obtain a sequence of extremal probability distributions in a sequence as the one that we could obtain in the quantum case. A different approach thus needs to be taken. It is really the fact that the quantum set has curved boundaries made of extremal quantum behaviors that allowed us to derive the results of this paper.

References

1 Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108:100402, Mar 2012. doi:10.1103/PhysRevLett.108.100402.

2 Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93(4):040102, April 2016. doi:10.1103/PhysRevA.93.040102.

3 Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. More randomness from the same data. *New J. Phys.*, 16(3):033011, 2014. doi:10.1088/1367-2630/16/3/033011.

4 John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

5 Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. doi:10.1103/RevModPhys.86.419.

6 Orest Bucicovschi and Jiří Lebl. On the continuity and regularity of convex extensions. *J. Convex Anal.*, 20(4):1113–1126, 2013.

7 Roger Colbeck. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006.

8 Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nat. Phys.*, 8(6):450–454, May 2012. doi:10.1038/nphys2300.

9 Florian J. Curchod, Markus Johansson, Remigiusz Augusiak, Matty J. Hoban, Peter Wittek, and Antonio Acín. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A*, 95(2), feb 2017. doi:10.1103/physreva.95.020102.

10 Giacomo Mauro D'Ariano, Paoloplacido Lo Presti, and Paolo Perinotti. Classical randomness in quantum measurements. *J. Phys. A: Math. Gen.*, 38(26):5979, 2005. doi:10.1088/0305-4470/38/26/010.

11 Gonzalo de la Torre, Matty J. Hoban, Chirag Dhara, Giuseppe Prettico, and Antonio Acín. Maximally nonlocal theories cannot be maximally random. *Phys. Rev. Lett.*, 114(16):160502, 2015. doi:10.1103/physrevlett.114.160502.

12 Rodrigo Gallego, Lluis Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. Full randomness from arbitrarily deterministic events. *Nat. Commun.*, 4:2654, 2013. doi:10.1038/ncomms3654.

13 Rodrigo Gallego, Lars Erik Würflinger, Rafael Chaves, Antonio Acín, and Miguel Navascués. Nonlocality in sequential correlation scenarios. *New J. Phys.*, 16(3):033037, 2014. doi:10.1088/1367-2630/16/3/033037.

14 Meng-Jun Hu, Zhi-Yuan Zhou, Xiao-Min Hu, Chuan-Feng Li, Guang-Can Guo, and Yong-Sheng Zhang. Experimental sharing of nonlocality among multiple observers with one entangled pair via optimal weak measurements. *arXiv:1609.01863*, Sep 2016. arXiv:1609.01863.

15 Lluis Masanes, Antonio Acín, and Nicolas Gisin. General properties of nonsignaling theories. *Phys. Rev. A*, 73(1):012112, Jan 2006. doi:10.1103/physreva.73.012112.

16 Olmo Nieto-Silleras, Stefano Pironio, and Jonathan Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.*, 16(1):013035, 2014. doi:10.1088/1367-2630/16/1/013035.

17 Stefano Pironio, Antonio Acín, Serge Massar, Antoine Boyer de la Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Matthew Olmschenk, David Hayes, Le Luo, T. Andrew Manning, and Christopher R. Monroe. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010. doi:10.1038/nature09008.

18 Sandu Popescu. Bell's inequalities and density matrices: Revealing "hidden" nonlocality. *Phys. Rev. Lett.*, 74(14):2619–2622, Apr 1995. doi:10.1103/physrevlett.74.2619.

19 Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–385, 1994. doi:10.1007/BF02058098.

20 Tyrrell Rockafellar. *Convex Analysis*. Princeton Press, 1970.

21 Matteo Schiavon, Luca Calderaro, Mirko Pittaluga, Giuseppe Vallone, and Paolo Villoresi. Three-observer bell inequality violation on a two-qubit entangled state. *Quantum Science and Technology*, 2(1):015010, mar 2017. doi:10.1088/2058-9565/aa62be.

22 Ralph Silva, Nicolas Gisin, Yelena Guryanova, and Sandu Popescu. Multiple observers can share the nonlocality of half of an entangled pair by using optimal weak measurements. *Phys. Rev. Lett.*, 114(25):250401, 2015. doi:10.1103/physrevlett.114.250401.

23 Umesh Vazirani and Thomas Vidick. Certifiable quantum dice. *Phil. Trans. R. Soc. A.*, 370(1971):3432–3448, Jun 2012. doi:10.1098/rsta.2011.0336.

24 Peter Wittek. Algorithm 950: Ncpol2sdpa - sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables. *ACM Trans. Math. Softw.*, 41(3):21:1–21:12, 2015. doi:10.1145/2699464.

25 Makoto Yamashita, Katsuki Fujisawa, and Masakazu Kojima. Implementation and evaluation of SDPA 6.0 (semidefinite programming algorithm 6.0). *Optimization Methods and Software*, 18(4):491–505, 2003. doi:10.1080/1055678031000118482.

A The guessing probability

We start our appendices with the following discussion, which is a summary of the work done in deriving the device-independent guessing probability (DIGP) [17, 1, 16, 11]. A conditional probability distribution that is the outcome distribution for some measurement on a quantum state is called a quantum distribution. For example, a distribution P with elements $p(ab|xy)$ is quantum if there exist at least one quantum state, i.e., a positive semi-definite hermitian unit trace matrix ρ and at least one set of measurements, i.e., a set of positive semi-definite hermitian matrices $M_{a|x}$, $M_{b|y}$ satisfying $\sum_a M_{a|x} = \sum_b M_{b|y} = 1$ such that $p(ab|xy) = Tr(M_{a|x} \otimes M_{b|y} \cdot \rho)$. We will often abuse notation and refer to a distribution by its elements $p(ab|xy)$ when there is no confusion in doing so.

The set $\mathcal{Q}$ of quantum distributions is convex and a distribution in $\mathcal{Q}$ that cannot be decomposed as a convex combination of other distributions is called *extremal* in $\mathcal{Q}$. For a non-extremal distribution $P(ab|xy)$ there is in general more than one possible convex decomposition.

A non-extremal distribution $p(ab|xy)$ with a convex decomposition $p(ab|xy) = \sum_\lambda q_\lambda p_\lambda(ab|xy)$ can be constructed by sampling the different distributions $p_\lambda(ab|xy)$ with probability q_λ. In this case knowledge about the convex decomposition chosen changes the ability of an eavesdropper to correctly guess the outcomes a and/or b.

Without knowledge of the decomposition, or for extremal distributions, the probability of correctly guessing the outcome of measurement y^0 is $\max_b p(b|y^0)$, the probability of the most likely outcome. With knowledge of the decomposition $p(ab|xy) = \sum_\lambda q_\lambda p_\lambda(ab|xy)$, the probability is larger or equal to $\max_b p(b|y^0)$

$$\sum_\lambda q_\lambda \max_b p_\lambda(b|y^0) \geq \max_b \sum_\lambda q_\lambda p_\lambda(b|y^0) = \max_b p(b|y^0). \tag{21}$$

For a given observed non-extremal distribution P_{obs}, it is possible that it was produced by an agent Eve that has larger predictive power than an agent which only observes the outcomes.

We now want to consider the optimal probability for the agent Eve to correctly guess an outcome b of measurement y^0 given a distribution $p_{obs}(ab|xy)$ and control over its decomposition in extremal points. If the set of quantum distributions is closed there exist one or several optimal ways to decompose the given distribution that maximizes this probability. If the set is not closed but open or semi-open, there may not exist a maximum and the relevant quantity is instead the supremum value of Eves probability to correctly guess the outcome. Since $\max_b p(b|y^0)$ is a continuous function on the set of probability distributions it follows that the supremum value of $\sum_\lambda q_\lambda \max_b p_\lambda(b|y^0)$ as a function of all possible decompositions, indexed by λ, on an open or semi-open set of distributions is the same as the maximum value on the closure of the set. Therefore, in this case we can consider the

closure of the set and express the probability as an optimization over the extremal points of this closed set.

With this disclaimer, the maximal probability for the agent Eve to correctly guess an outcome b of measurement y^0 given a distribution $p_{obs}(ab|xy)$ and control over the decomposition is the DIGP $G(y^0, P_{\text{obs}})$

$$G(y^0, P_{\text{obs}}) = \max_{q_\lambda, p_\lambda(ab|xy)} \sum_\lambda q_\lambda \max_b p_\lambda(b|y^0). \tag{22}$$

where λ is labelling the convex decompositions of $p_{\text{obs}}(ab|xy)$ in terms of extremal distributions $p_\lambda(ab|xy)$. Note that if $\mathcal{Q}$ is not closed a given extremal point may not belong to the set but only to its closure. For any open interval of $\mathcal{Q}$ the function $G(y^0, P_{\text{obs}})$ is a concave function [17]. Therefore this kind of maximization is called a *concave roof* construction.

The guessing probability can be approximated by a hierarchy of semidefinite programming (SDP) relaxations [16, 3]. We used Ncpol2sdpa [24] to generate the relaxations for verifying some of the analytical results. We relied on the arbitrary-precision variant of the SDPA family of solvers [25] for obtaining important numerical values, and the solver Mosek[1] in all other cases.

B Continuity of the guessing probability in interior and extremal points of $\mathcal{Q}$

The guessing probability as a function on the space of probability distributions is not everywhere continuous. An example of this is that the family of Bell-inequalities of Ref. [1] that certifies one bit of randomness for measurements on a state with arbitrarily little entanglement. The probability distribution corresponding to such a state and the measurements in Eq. 6 has $G(y^0, P_{obs}) = 1/2$ and is at the same time arbitrarily close to a distribution corresponding to measurements on a product state with $G(y^0, P_{obs}) = 1$, i.e., a distribution which can be prepared by a local deterministic procedure. There is thus a discontinuity where the guessing probability jumps from 1/2 to 1. The key to understanding this discontinuity is that the local deterministic distribution is not extremal while the quantum distribution in the neighbouring point is extremal. As seen in Eq. 21, the guessing probability is given by different functions depend ing on whether a distribution can be decomposed into other distributions or not, i.e., if it is extremal or not. This means discontinuities can appear at the boundary between extremal points and non-extremal points.

We will now show that discontinuities can *only* appear at such boundaries between extremal and non-extremal points in the boundary $\partial\mathcal{Q}$ of the quantum set $\mathcal{Q}$. To do this we use the property of the guessing probability described in Eq. 21, together with some general properties of concave functions and in particular concave roof constructions.

We want to show that the following propositions are true:

▶ **Proposition 5.** *The function $G(y^0, P_{obs})$ on the set of quantum distributions $\mathcal{Q}$ is continuous in the interior of $\mathcal{Q}$.*

▶ **Proposition 6.** *The function $G(y^0, P_{obs})$ is continuous in any extremal point of $\mathcal{Q}$.*

Proposition 1 is trivial. The guessing probability $G(y^0, P_{\text{obs}})$ is concave by definition and any concave function is continuous on an open subset of its domain [20]. In particular this means that $G(y^0, P_{\text{obs}})$ is continuous in the interior of $\mathcal{Q}$. Note that if $\mathcal{Q}$ is open, i.e. has no boundary, there can thus not exist any discontinuity.

[1] http://mosek.com/

To address proposition 2 we consider the restriction $G(y^0, P_{\text{obs}})^{\partial\mathcal{Q}}$ of $G(y^0, P_{\text{obs}})$ to the boundary $\partial\mathcal{Q}$ of the quantum set. First we note that the function $G(y^0, P_{\text{obs}})^{\partial\mathcal{Q}}$ by definition is continuous on any open set of extremal points since $\max_b p(b|y)$ is a continuous function. Next we observe that the boundary $\partial\mathcal{Q}$ can be decomposed into a collection of open sets of extremal points and a collection $\{S_i\}$ of closed connected possibly overlapping sets where each set is the closure of a maximal open connected subset. A maximal open connected subset M of the non-extremal points is an open set such that any other open connected set of non-extremal points which contains M is M itself. Therefore, each set S_i is the convex hull of the set of extremal points in its closure.

Any closed set S_i has a boundary ∂S_i with the rest of $\partial\mathcal{Q}$ which can be decomposed in the same way into open sets of extremal points and closed connected sets S_{ij} that are closures of maximal open connected sets of non-extremal points. The boundary ∂S_{ij} of S_{ij} with the rest of ∂S_i is in turn decomposable in the same way.

Continuing this successive decomposition of the boundary $\partial\mathcal{Q}$ we will eventually reach sets $S_{ijk\ldots}$ that are one dimensional simplexes, or alternatively sets with only extremal points in the boundary. On sets of these two types $G(y^0, P_{\text{obs}})$ is a continuous function. To see this we introduce the following terminology, and use a theorem from Ref. [6].

A function for which all discontinuities are such that the function takes the higher value at a closed set and the lower value at an open set is called *upper semi-continuous.*

The function $G(y^0, P_{\text{obs}})^S$ defined on a closed convex set S can be viewed as an extension of $G(y^0, P_{\text{obs}})^{\partial S}$ to the interior of S. This extension is called the *concave roof extension.*

▶ **Theorem 7.** *Let C be a compact set and $K = co(C)$ be the convex hull of C. If $F : C \to \mathbb{R}$ is bounded, upper semi-continuous, and concave on C, then the concave roof extension $\hat{F} : K \to \mathbb{R}$ of F to K is upper semi-continuous [6].*

The guessing probability is bounded and concave by definition. If the boundary of S has only extremal points it follows that $G(y^0, P_{\text{obs}})^{\partial S}$ is continuous in ∂S and by theorem 7 $G(y^0, P_{\text{obs}})^S$ is upper semi-continuous on S. Moreover, since $G(y^0, P_{\text{obs}})^S$ is concave it cannot have an upper semi-continuous discontinuity between the boundary and the interior. If S is a one-dimensional simplex we can, if necessary, restrict the domain of the guessing probability to a one dimensional subspace and make the same argument.

Next we consider discontinuities between S and an open set of extremal points.

▶ **Lemma 8.** *Any discontinuity of $G(y^0, P_{obs})$ between a closed set and an open set of extremal points is upper semi-continuous.*

Proof. If the boundary point of the closed set is extremal the $G(y^0, P_{\text{obs}})$ is continuous since $\max_b p(b|y^0)$ is continuous. Next consider a non-extremal boundary point of the closed set. $G(y^0, P_{\text{obs}})$ in the non-extremal point is always greater or equal to $\max_b P(b|y^0)$ by Eq. 21. Thus any discontinuity is upper semi-continuous. ◀

If there is a discontinuity of $G(y^0, P_{\text{obs}})$ on the boundary of S it is, by lemma 8 , upper semi-continuous and at a set of non-extremal points.

By repeated application of Theorem 7 and lemma 8 we can conclude that $G(y^0, P_{\text{obs}})^{\partial\mathcal{Q}}$ is upper semi-continuous on $\partial\mathcal{Q}$ and that $G(y^0, P_{\text{obs}})$ is upper semi-continuous on $\mathcal{Q}$. Since $G(y^0, P_{\text{obs}})$ is concave there cannot be an upper semi-continuous discontinuity between the boundary $\partial\mathcal{Q}$ and the interior of $\mathcal{Q}$. Thus the only discontinuities are between non-extremal points in closed subsets of $\partial\mathcal{Q}$ and extremal points in open subsets of $\partial\mathcal{Q}$.

C Bounds on the guessing probability as a function of a Bell inequality: Continuity at a unique point of maximal violation

We have described the guessing probability as a function on set of quantum distributions, but it is sometimes useful to consider it as a function of the violation of some given Bell inequality I. A Bell expression is a linear function on the space of distributions and the set of distributions for which it takes a given value t is a hyper-plane H_t. The different values of the Bell expression thus defines a family of parallel hyperplanes.

On each hyperplane H_t we can consider the restriction $G(y^0, P_{\text{obs}})_t$ of $G(y^0, P_{\text{obs}})$ to the intersection of H_t with $\mathcal{Q}$ and take its maximum $\max G(y^0, P_{\text{obs}})_t$ on this intersection. This maximum is the highest probability for Eve to guess the outcome of y^0 for any distribution $P \in \mathcal{Q}$ such that $I(P) = t$. The function $\max G(y^0, P_{\text{obs}})_t$ can have a discontinuity at $t = t_c$ only if H_{t_c} intersects with a point in $\mathcal{Q}$ at which $G(y^0, P_{\text{obs}})$ is discontinuous.

Let us consider a Bell expression I and its maximal value t_{max} on $\mathcal{Q}$. If the intersection of $H_{t_{max}}$ and $\mathcal{Q}$ is a single extremal point it follows from Propositions 1 and 2 that there is a $t_c \neq t_{max}$ such that for the range $t_c \leq t \leq t_{max}$ for which $\max G(y^0, P_{\text{obs}})_t$ is a continuous function of t.

If the intersection of $H_{t_{max}}$ and $\mathcal{Q}$ contains more than one extremal point it also contains a set of non-extremal points of $\partial\mathcal{Q}$ and $G(y^0, P_{\text{obs}})$ could have a discontinuity between this set and an open set of extremal points. This discontinuity could lead to a discontinuity of the function $\max G(y^0, P_{\text{obs}})_t$ at t_{max}.

D Guessing probability for a sequence

So far, we have discussed the continuity properties of the guessing probability in the standard scenario, where one single measurement $M_{a|x}$ is made on Alice's side and $M_{b|y}$ on Bob's. The goal of this section is to extend these properties to the case where sequential measurements $M_{a_i|x_i}$ and $M_{b_i|y_i}$ are performed by each party, where i labels the position of a particular measurement in the sequence.

Let us consider a sequence of measurements $\hat{\sigma}(\xi_i)$ chosen by Bob and denote $(\xi_1, \xi_2, \ldots, \xi_n) \equiv \vec{\xi}$. The convex decomposition of the observed outcome distribution that gives Eve optimal probability to correctly guess the sequence of outcomes $\vec{b}_n$ of the measurements $(y_1^0, y_2^0, \ldots, y_n^0) \equiv \vec{y}_n^0$ is a function of $\vec{\xi}$. The guessing probability $G(\vec{y}_n^0, P_{\text{obs}})$ is thus given by

$$G(\vec{y}_n^0, P_{\text{obs}}) = \sum_{\lambda_{\vec{\xi}}} q_{\lambda_{\vec{\xi}}} \max_{\vec{b}_n} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \cdot p_{\lambda_{\vec{\xi}}}(b_2|y_2^0, y_1^0, b_1) \ldots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0 \vec{b}_{n-1}). \tag{23}$$

where the extremal distributions $p_{\lambda_{\vec{\xi}}}(b_n|y_n \ldots)$ and weights $q_{\lambda_{\vec{\xi}}}$ of the optimal convex decomposition are functions of $\vec{\xi}$ as indicated by the index $\lambda_{\vec{\xi}}$. Let us assume that a term which appears in the convex combination is

$$q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0) \ldots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0 \vec{b}_{n-1}). \tag{24}$$

Thus we assume that it corresponds to the most probable sequence of outcomes $\vec{b}_n$ for a specific distribution indexed by $\lambda_{\vec{\xi}}$.

Given that Eve has chosen the optimal convex decomposition for guessing the outcomes of $\vec{y}_n^0$ we consider her probability of correctly guessing the outcome of y_m^0 for $1 \leq m \leq n$ given a particular sequence of previous outcomes $\vec{b}_{m-1}$. It is given by

$$\sum_{\lambda_{\vec{\xi}}} k_{\lambda_{\vec{\xi}}} \max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0 \vec{b}_{m-1}), \tag{25}$$

where $k_{\lambda_{\vec{\xi}}}$ is the probability that the distribution indexed by $\lambda_{\vec{\xi}}$ will be sampled given the sequence of previous outcomes $\vec{b}_{m-1}$

$$k_{\lambda_{\vec{\xi}}} = \frac{q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0\vec{b}_{m-2})}{\sum_{\lambda_{\vec{\xi}}} q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0\vec{b}_{m-2})}. \tag{26}$$

The probability in Eq. 25 is larger or equal to $1/d_m$, where d_m is the number of possible outputs b_m, but is lower or equal to $G(y_m^0, P_{\text{obs}})$, the maximal probability that Eve could guess the outcome of y_m^0 correctly given that she had chosen an optimal strategy for this and not the optimal strategy for guessing the outcomes of the sequence $\vec{y}_n^0$. Thus if $G(y_m^0, P_{\text{obs}})$ is close to $1/d_m$ so is the expression in Eq. 25.

E Arbitrarily close to n random bits for n measurements

We want to prove that $G(\vec{y}_n^0, P_{\text{obs}})$ can be made arbitrarily close to 2^{-n} by making $G(y_m^0, P_{\text{obs}})$ sufficiently close to $1/2$ for each $1 \leq m \leq n$.

The proof relies on the fact that if a convex combination of a collection of numbers x_i equals a, i.e., $\sum_i k_i x_i = a$ where $\sum k_i = 1$, and if $x_i \geq a$ for each i, it follows that for every i either $k_i = 0$ or $x_i = a$.

From this follows that when $G(y_m^0, P_{\text{obs}})$ is very close to $1/2$ either $\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1})$ in Eq. 25 is very close to $1/2$ or $k_{\lambda_{\vec{\xi}}}$ is very close to zero for each $\lambda_{\vec{\xi}}$. To see this more clearly we construct the following bound

$$\begin{aligned} k_{\lambda_{\vec{\xi}}} \max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1}) &\leq G(y_m^0, P_{\text{obs}}) - \sum_{\lambda' \neq \lambda} k_{\lambda'_{\vec{\xi}}} \max_{b_m} p_{\lambda'_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1}) \\ &\leq G(y_m^0, P_{\text{obs}}) - 1/2(1 - k_{\lambda_{\vec{\xi}}}) \end{aligned}$$

where we used $\max_{b_m} p_{\lambda'_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1}) \geq 1/2$ for each $\lambda'_{\vec{\xi}}$ and $\sum_{\lambda' \neq \lambda} k_{\lambda'_{\vec{\xi}}} = 1 - k_{\lambda_{\vec{\xi}}}$. It follows that

$$G(y_m^0, P_{\text{obs}}) - 1/2 \geq k_{\lambda_{\vec{\xi}}}[\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1}) - 1/2],$$

and given Eq. (26) this implies

$$G(y_m^0, P_{\text{obs}}) - 1/2 \geq q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0\vec{b}_{m-2})[\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_n^0\vec{b}_{m-1}) - 1/2].$$

Thus for sufficiently small $G(y_m^0, P_{\text{obs}}) - 1/2$ either $\max_{b_m} p_{\lambda_{\vec{\xi}}}(b_m|\vec{y}_m^0\vec{b}_{m-1}) - 1/2$ can be made arbitrarily small, or the probability $q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_{m-1}|\vec{y}_{m-1}^0\vec{b}_{m-2})$ that the distribution labelled by $\lambda_{\vec{\xi}}$ is sampled when y_m^0 is measured is made arbitrarily small.

The argument can be made for any B_m. For B_1, it follows that either $p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)$ is made arbitrarily close to $1/2$ or $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily close to 0. For B_2, it follows that either $p_{\lambda_{\vec{\xi}}}(b_2|y_2^0 y_1^0 b_1)$ is made arbitrarily close to $1/2$ or $q_{\lambda_{\vec{\xi}}} p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)$ is made arbitrarily close to zero. Given the second option and that $p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)$ is made arbitrarily close to $1/2$ it is implied that that $q_{\lambda(\vec{\xi})}$ is made arbitrarily close to 0. If on the other hand $p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)$ is not very close to $1/2$ it follows that $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily close to zero by the preceding argument.

By induction it is clear that either the term in Eq. 24 satisfies that $p_{\lambda_{\vec{\xi}}}(b_1|y_1^0)\dots p_{\lambda_{\vec{\xi}}}(b_n|\vec{y}_n^0\vec{b}_{n-1})$ can be made arbitrarily close to 2^{-n} or alternatively $q_{\lambda_{\vec{\xi}}}$ is made arbitrarily small. Since the same is true for every $\lambda_{\vec{\xi}}$ in Eq. 23 it follows that $G(\vec{y}_n^0, P_{\text{obs}})$ can be made arbitrarily close to 2^{-n}.

Note that the above argument can be straightforwardly extended to the case where the number of outputs d_i for each B_i can be different from 2. Thus, in this case $G(\bar{y}_n^0, P_{\text{obs}})$ can be made arbitrarily close to $\prod_{i=1}^n d_i^{-1}$ by making $G(y_m^0, P_{\text{obs}})$ sufficiently close to $1/d_m$ for each $1 \leq m \leq n$.

F Our programs to obtain lower bounds on the certified randomness

In this section of the appendices we give the tables of results for section 7. We remind the reader that the computational details – exposed in a pedagogical way – of our results can be found online at: `https://github.com/peterwittek/ipython-notebooks/blob/master/Unbounded_randomness.ipynb`.

Table 1 $\theta = \frac{\pi}{4}$, the maximally entangled state.

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.962
0.027	0.925
0.040	0.890
0.053	0.855
0.067	0.822
0.080	0.790
0.093	0.759
0.106	0.729
0.120	0.700
0.133	0.673
0.146	0.647
0.160	0.622
0.173	0.598
0.186	0.575
0.200	0.554
0.213	0.533
0.226	0.514
0.240	0.494
0.253	0.473
0.266	0.452
0.280	0.430
0.293	0.409
0.306	0.387
0.319	0.365
0.333	0.342
0.346	0.320
0.359	0.298
0.373	0.276
0.386	0.254
0.399	0.233
0.413	0.211
0.426	0.190
0.439	0.170
0.453	0.150
0.466	0.130
0.479	0.111
0.493	0.093
0.506	0.075
0.519	0.058
0.532	0.042
0.546	0.027
0.559	0.012
0.572	0.000

Table 2 $\theta = \frac{\pi}{8}$.

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.941
0.027	0.884
0.040	0.830
0.053	0.779
0.067	0.729
0.080	0.682
0.093	0.637
0.106	0.595
0.120	0.555
0.133	0.519
0.146	0.485
0.160	0.453
0.173	0.424
0.186	0.396
0.200	0.371
0.213	0.348
0.226	0.327
0.240	0.307
0.253	0.289
0.266	0.273
0.280	0.258
0.293	0.243
0.306	0.229
0.319	0.214
0.333	0.200
0.346	0.186
0.359	0.171
0.373	0.157
0.386	0.143
0.399	0.129
0.413	0.115
0.426	0.102
0.439	0.089
0.453	0.077
0.466	0.064
0.479	0.053
0.493	0.041
0.506	0.031
0.519	0.021
0.532	0.012
0.546	0.004
0.559	0.000
0.572	0.000

Table 3 $\theta = \frac{\pi}{16}$.

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.896
0.027	0.800
0.040	0.714
0.053	0.641
0.067	0.577
0.080	0.521
0.093	0.473
0.106	0.429
0.120	0.391
0.133	0.356
0.146	0.325
0.160	0.297
0.173	0.271
0.186	0.248
0.200	0.227
0.213	0.207
0.226	0.190
0.240	0.174
0.253	0.159
0.266	0.146
0.280	0.134
0.293	0.122
0.306	0.112
0.319	0.103
0.333	0.095
0.346	0.087
0.359	0.078
0.373	0.070
0.386	0.062
0.399	0.055
0.413	0.047
0.426	0.040
0.439	0.034
0.453	0.027
0.466	0.021
0.479	0.016
0.493	0.011
0.506	0.007
0.519	0.003
0.532	0.000
0.546	0.000
0.559	0.000
0.572	0.000

Table 4 $\theta = \frac{\pi}{32}$.

ξ	$\sharp$ random bits
0.000	1.000
0.013	0.823
0.027	0.706
0.040	0.619
0.053	0.551
0.067	0.493
0.080	0.444
0.093	0.400
0.106	0.362
0.120	0.328
0.133	0.297
0.146	0.269
0.160	0.244
0.173	0.221
0.186	0.200
0.200	0.181
0.213	0.163
0.226	0.147
0.240	0.133
0.253	0.119
0.266	0.107
0.280	0.095
0.293	0.085
0.306	0.076
0.319	0.067
0.333	0.059
0.346	0.052
0.359	0.046
0.373	0.040
0.386	0.035
0.399	0.030
0.413	0.025
0.426	0.021
0.439	0.017
0.453	0.013
0.466	0.009
0.479	0.006
0.493	0.004
0.506	0.002
0.519	0.000
0.532	0.000
0.546	0.000
0.559	0.000
0.572	0.000

The Complexity of Simulating Local Measurements on Quantum Systems*†

Sevag Gharibian‡[1] and Justin Yirka[2]

1 **Virginia Commonwealth University, Richmond, USA**
sgharibian@vcu.edu
2 **Virginia Commonwealth University, Richmond, USA**
yirkajk@vcu.edu

Abstract

An important task in quantum physics is the estimation of local quantities for ground states of local Hamiltonians. Recently, [Ambainis, CCC 2014] defined the complexity class $\mathrm{P}^{\mathrm{QMA}[\log]}$, and motivated its study by showing that the physical task of estimating the expectation value of a local observable against the ground state of a local Hamiltonian is $\mathrm{P}^{\mathrm{QMA}[\log]}$-complete. In this paper, we continue the study of $\mathrm{P}^{\mathrm{QMA}[\log]}$, obtaining the following results.

- The $\mathrm{P}^{\mathrm{QMA}[\log]}$-completeness result of [Ambainis, CCC 2014] requires $O(\log n)$-local observables and Hamiltonians. We show that simulating even a *single qubit* measurement on ground states of 5-local Hamiltonians is $\mathrm{P}^{\mathrm{QMA}[\log]}$-complete, resolving an open question of Ambainis.
- We formalize the complexity theoretic study of estimating two-point correlation functions against ground states, and show that this task is similarly $\mathrm{P}^{\mathrm{QMA}[\log]}$-complete.
- $\mathrm{P}^{\mathrm{QMA}[\log]}$ is thought of as "slightly harder" than QMA. We justify this formally by exploiting the hierarchical voting technique of [Beigel, Hemachandra, Wechsung, SCT 1989] to show $\mathrm{P}^{\mathrm{QMA}[\log]} \subseteq \mathrm{PP}$. This improves the containment $\mathrm{QMA} \subseteq \mathrm{PP}$ [Kitaev, Watrous, STOC 2000].
- A central theme of this work is the subtlety involved in the study of oracle classes in which the oracle solves a *promise* problem. In this vein, we identify a flaw in [Ambainis, CCC 2014] regarding a $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hardness proof for estimating spectral gaps of local Hamiltonians. By introducing a "query validation" technique, we build on [Ambainis, CCC 2014] to obtain $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hardness for estimating spectral gaps under polynomial-time Turing reductions.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes

Keywords and phrases Complexity theory, Quantum Merlin Arthur (QMA), local Hamiltonian, local measurement, spectral gap

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.2

1 Introduction

The use of computational complexity theory to study the inherent difficulty of computational problems has proven remarkably fruitful over the last decades. For example, the theory of NP-completeness [8, 21, 17] has helped classify the worst-case complexity of hundreds of computational problems which elude efficient classical algorithms. In the quantum setting,

* A full version of the paper is available at https://arxiv.org/abs/1606.05626.

† Part of this work was completed while SG was supported by a Government of Canada NSERC Banting Postdoctoral Fellowship and the Simons Institute for the Theory of Computing at UC Berkeley. SG acknowledges support from NSF grants CCF-1526189 and CCF-1617710.

‡ SG acknowledges support from NSF grants CCF-1526189 and CCF-1617710, an NSERC Banting Postdoctoral Fellowship and a Simons Postdoctoral Fellow at the University of California, Berkeley.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 2; pp. 2:1–2:17
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the study of a quantum analogue of NP, known as Quantum Merlin Arthur[1] (QMA), was started in 1999 by the seminal "quantum Cook-Levin theorem" of Kitaev [19], which showed that estimating the ground state energy of a given k-local Hamiltonian is QMA-complete for $k \geq 5$. Here, a k-local Hamiltonian[2] H can be thought of as a quantum constraint satisfaction system in which each quantum clause acts non-trivially on k qubits. The "largest total weight of satisfiable clauses" is given by the *ground state energy* of H, i.e. the smallest eigenvalue of H. Physically, the ground state energy and its corresponding eigenvector, the *ground state*, are motivated in that they represent the energy level and state of a given quantum system at low temperature, respectively. For this reason, since Kitaev's work [19], a number of physically motivated problems have been shown complete for QMA (see, e.g., [5] and [14] for surveys), a number of which focus on estimating ground state energies of local Hamiltonians.

In recent years, however, new directions in quantum complexity theory involving other physical properties of local Hamiltonians have appeared. For example, Brown, Flammia and Schuch [6] (also Shi and Zhang [25]) introduced a quantum analogue of #P, denoted #BQP, and showed that computing the ground state degeneracy or density of states of local Hamiltonians is #BQP-complete. Gharibian and Kempe [12] introduced cq-Σ_2, a quantum generalization of Σ_2^p, and showed that determining the smallest subset of interaction terms of a given local Hamiltonian which yields a frustrated ground space is cq-Σ_2-complete (and additionally, cq-Σ_2-hard to approximate). Gharibian and Sikora [13] showed that determining whether the ground space of a local Hamiltonian has an "energy barrier" is QCMA-complete, where QCMA [2] is Merlin-Arthur (MA) with a classical proof and quantum prover. Finally, and most relevant to this work, Ambainis [3] introduced $\mathrm{P}^{\mathrm{QMA[log]}}$, which is the class of decision problems decidable by a polynomial time Turing machine with logarithmically many queries to a QMA oracle (i.e. a quantum analogue of $\mathrm{P}^{\mathrm{NP[log]}}$). He showed that $\mathrm{P}^{\mathrm{QMA[log]}}$ captures the complexity of a very natural physical problem: "Simulating" a local measurement against the ground state of a local Hamiltonian (more formally, computing the expectation value of a given local observable against the ground state).

It is worth noting here that, given a local Hamiltonian, often one is not necessarily interested in a description of the *entire* ground state [14]. Rather, one may be interested in local quantities such as the evaluation of a local observable or of a correlation function. This makes $\mathrm{P}^{\mathrm{QMA[log]}}$ a well-motivated complexity class, whose study we continue here.

Our results (summarized under three headings)

1. $\mathrm{P}^{\mathrm{QMA[log]}}$-completeness of estimating local quantities. We begin with the study of two physically motivated problems. The first, APX-SIM, was formalized by Ambainis [3] (formal definitions in Section 2): *Given a k-local Hamiltonian H and an l-local observable A, estimate the expectation value of the measurement A against the ground state of H, i.e. estimate $\langle A \rangle := \langle \psi | A | \psi \rangle$ for $|\psi\rangle$ a ground state of H.* The second problem, which we introduce here and denote APX-2-CORR, is defined similarly to APX-SIM, except one is given observables A and B, and asked to estimate the *two-point correlation function* $\langle A \otimes B \rangle - \langle A \rangle \langle B \rangle$.

Previously, Ambainis [3] showed that APX-SIM is $\mathrm{P}^{\mathrm{QMA[log]}}$-complete for $O(\log n)$-local Hamiltonians and $O(\log n)$-local observables. From a physical standpoint, however, it is

[1] More accurately, QMA is Merlin-Arthur (MA) with a quantum proof and quantum verifier.

[2] $H \in \mathbb{C}^{2^n \times 2^n}$ is a Hermitian matrix with a succinct description $H = \sum_i H_i$, where each local clause $H_i \in \mathbb{C}^{2^k \times 2^k}$ acts non-trivially on k qubits. Implicitly, if H_i acts on a subset $S_i \subseteq [n]$ of qubits non-trivially, then more accurately one writes $H_i \otimes I_{[n] \setminus S_i}$. We write $H = \sum_i H_i$ for simplicity.

typically desirable to have $O(1)$-local Hamiltonians and observables, and whether $\mathrm{P}^{\mathrm{QMA}[\log]}$-hardness holds in this regime was left as an open question. We thus first ask: *Is* APX-SIM *still hard for an* $O(1)$*-local Hamiltonian and* 1*-local observables?*

A priori, one might guess that simulating 1-local measurements might not be difficult — for example, the ground state energy of a 1-local Hamiltonian can be estimated efficiently. Yet, this intuition is incorrect: By embedding a 3-SAT instance ϕ into a 3-local Hamiltonian, and using the ability to repeatedly locally measure observable Z against single qubits of the ground state, we can extract a solution to ϕ! Thus, the 1-local observable case is at least NP-hard. Indeed, we show it is much harder, resolving Ambainis's open question.

▶ **Theorem 1.1.** *Given a* 5*-local Hamiltonian* H *on* n *qubits and a* 1*-local observable* A*, estimating* $\langle A\rangle$ *(i.e.* APX-SIM*) is* $\mathrm{P}^{\mathrm{QMA}[\log]}$*-complete.*

Thus, measuring just a *single* qubit of a local Hamiltonian H's ground state with a fixed single-qubit observable A (in our construction, A is independent of H) is harder than QMA (assuming $\mathrm{QMA} \neq \mathrm{P}^{\mathrm{QMA}[\log]}$, which is likely as otherwise co-QMA $\subseteq$ QMA).

Using similar techniques, we also show APX-2-CORR is $\mathrm{P}^{\mathrm{QMA}[\log]}$-complete.

▶ **Theorem 1.2.** *Given a* 5*-local Hamiltonian* H *on* n *qubits and a pair of* 1*-local observables* A *and* B*, estimating* $\langle A\otimes B\rangle - \langle A\rangle\langle B\rangle$ *(i.e.* APX-2-CORR*) is* $\mathrm{P}^{\mathrm{QMA}[\log]}$*-complete.*

2. An upper bound on the power of $\mathrm{P}^{\mathrm{QMA}[\log]}$. Since $\mathrm{P}^{\mathrm{QMA}[\log]}$ is thought of as "slightly harder" than QMA (note $\mathrm{QMA} \subseteq \mathrm{P}^{\mathrm{QMA}[\log]}$), we next ask: *How much harder than QMA is* $\mathrm{P}^{\mathrm{QMA}[\log]}$*?* Recall that QMA $\subseteq$ PP [20, 26, 23] (note [26] actually shows the stronger containment $\mathrm{QMA} \subseteq \mathrm{A_0PP}$). Here, PP is the set of promise problems solvable in probabilistic polynomial time with *unbounded* error. Our next result shows that $\mathrm{P}^{\mathrm{QMA}[\log]}$ is "not too much harder" than QMA in the following rigorous sense.

▶ **Theorem 1.3.** $\mathrm{P}^{\mathrm{QMA}[\log]} \subseteq \mathrm{PP}$.

3. Estimating spectral gaps and oracles for promise problems. A central theme in this work is the subtlety involved in the study of oracle classes in which the oracle solves a *promise* problem (such as $\mathrm{P}^{\mathrm{QMA}[\log]}$), as opposed to a decision problem (such as $\mathrm{P}^{\mathrm{NP}[\log]}$, where $\mathrm{P}^{\mathrm{NP}[\log]}$ is $\mathrm{P}^{\mathrm{QMA}[\log]}$ except with an NP oracle). As discussed in "Proof techniques and discussions" below, the issue is that a P machine cannot in general determine if the query it makes to a QMA oracle satisfies the promise gap of the oracle. For queries which violate this promise, the oracle is allowed to give an arbitrary answer. We observe that this point appears to have been missed in [3], rendering a claimed proof that determining the spectral gap of a given $O(\log n)$-local Hamiltonian H is $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hard incorrect. ($\mathrm{P}^{\mathrm{UQMA}[\log]}$ is $\mathrm{P}^{\mathrm{QMA}[\log]}$ except with a Unique QMA oracle. Unique QMA is roughly QMA with a unique accepting quantum witness in the YES case.) Our last result both shows how to overcome this difficulty (at the expense of obtaining a "slightly weaker" hardness claim involving a Turing reduction, whereas [3] claimed hardness under a mapping reduction), and improves the locality of H to $O(1)$.

▶ **Theorem 1.4.** *Given a* 4*-local Hamiltonian* H*, estimating its spectral gap (i.e. the problem* SPECTRAL-GAP*) is* $\mathrm{P}^{\mathrm{UQMA}[\log]}$*-hard under polynomial time Turing reductions.*

Proof techniques and discussion

1. $\mathrm{P}^{\mathrm{QMA}[\log]}$-completeness for estimating local quantities. The proofs of our first two $\mathrm{P}^{\mathrm{QMA}[\log]}$-hardness results (Theorem 1.1 and Theorem 1.2) are similar, so we focus on APX-SIM here. Intuitively, our aim is simple: To design our local Hamiltonian H so that its

ground state encodes a so-called history state[3] [19] $|\psi\rangle$ for a given $\mathrm{P}^{\mathrm{QMA[log]}}$ instance, such that measuring observable Z on the designated "output qubit" of $|\psi\rangle$ reveals the answer of the computation. At a high level, this is achieved by combining a variant of Kitaev's circuit-to-Hamiltonian construction [19] (which forces the ground state to follow the P circuit) with Ambainis's "query Hamiltonian" [3] (which forces the ground state to encode correctly answered queries to the QMA oracle). Making this rigorous requires developing a few ideas, including: A careful analysis of Ambainis's query Hamiltonian's ground space when queries violating the promise gap of the oracle are allowed (Lemma 3.1), a simple but useful corollary (Cor. 2.3) of Kempe, Kitaev, and Regev's Projection Lemma [18] (Corollary 2.3, showing that any low energy state of H must be close to a valid history state), and application of Kitaev's unary encoding trick [19] to bring the locality of the Hamiltonian H down to $O(1)$ (Lemma 3.2).

Next, to show containment of APX-2-CORR in $\mathrm{P}^{\mathrm{QMA[log]}}$ (Theorem 1.2), a natural approach would be to run Ambainis's $\mathrm{P}^{\mathrm{QMA[log]}}$ protocol for APX-SIM independently for each term $\langle A \otimes B\rangle$, $\langle A\rangle$, and $\langle B\rangle$. However, if a cheating prover does not send the *same* ground state $|\psi\rangle$ for each of these measurements, soundness of the protocol can be violated. To circumvent this, we exploit a trick of Chailloux and Sattath [7] from the setting of QMA(2): we observe that the correlation function requires only knowledge of the two-body reduced density matrices $\{\,\rho_{ij}\,\}$ of $|\psi\rangle$. Thus, a prover can send classical descriptions of the $\{\,\rho_{ij}\,\}$ along with a "consistency proof" for the QMA-complete Consistency problem [22].

2. An upper bound on the power of $\mathsf{P}^{\mathsf{QMA[log]}}$. We now move to our third result, which is perhaps the most technically involved. To show $\mathrm{P}^{\mathrm{QMA[log]}} \subseteq \mathrm{PP}$ (Theorem 1.3), we exploit the technique of *hierarchical voting* (used by Beigel, Hemachandra, and Wechsung [4] to show $\mathrm{P}^{\mathrm{NP[log]}} \subseteq \mathrm{PP}$), in conjunction with the QMA strong amplification results of Marriott and Watrous [23]. The intuition is best understood in the context of $\mathrm{P}^{\mathrm{NP[log]}}$ [4]. There, the PP machine first attempts to *guess* the answers to each NP query by picking random assignments to the SAT formula ϕ_i representing query i, in the hope of guessing a satisfying assignment for ϕ_i. Since such a guess can succeed only if ϕ_i is satisfiable, it can be seen that the lexicographically *largest* string y^* attainable by this process must be the correct query string (i.e. string of query answers). The scheme then uses several rounds of "hierarchical voting," in which lexicographically smaller query strings reduce their probability of being output to the point where y^* is guaranteed to be the "most likely" query string output. While the quantum variant of this scheme we develop is quite natural, its analysis is markedly more involved than the classical setting due to both the bounded-error nature of QMA and the possibility of "invalid queries" violating the QMA promise gap. (For example, it is no longer necessarily true that the lexicographically largest obtainable y^* is a "correct" query string.)

3. Estimating spectral gaps and oracles for promise problems. Finally, we discuss our fourth result and the theme of "invalid queries". Assume that all calls by the $\mathrm{P}^{\mathrm{QMA[log]}}$ machine to the QMA oracle Q are for an instance (H, a, b) of the Local Hamiltonian Problem (LH): *Is the ground state energy of H at most a (YES case), or at least b (NO case), for* $b - a \geq 1/\mathrm{poly}(n)$? Unfortunately, a P machine cannot in general tell whether the instance (H, a, b) it feeds to Q satisfies the promise conditions of LH (i.e. the ground state energy

[3] A *history state* can be seen as a quantum analogue of the "tableaus" which appear in the proof of the Cook-Levin theorem, i.e. a history state encodes the history of a quantum computation. In contrast to tableaus, however, the history encodes information in quantum superposition.

may lie in the interval (a, b)). If the promise is violated, we call such a query *invalid*, and in this case Q is allowed to either accept or reject. This raises the issue of how to ensure a YES instance (or NO instance) of a $\mathrm{P}^{\mathrm{QMA}[\log]}$ problem is well-defined. To do so, we stipulate (see, e.g., Definition 3 of Goldreich [16]) that the P machine must output the *same* answer regardless of how any invalid queries are answered by the oracle. As mentioned earlier, this point appears to have been missed in [3], where all queries were assumed to satisfy the LH promise. This results in the proofs of two key claims of [3] being incorrect. The first claim was used in the proof of $\mathrm{P}^{\mathrm{QMA}[\log]}$-completeness for APX-SIM (Claim 1 in [3]); we provide a corrected statement and proof in Lemma 3.1 (which suffices for the $\mathrm{P}^{\mathrm{QMA}[\log]}$-hardness results in [3] regarding APX-SIM to hold).

The error in the second claim (Claim 2 of [3]), wherein $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hardness of determining the spectral gap of a local Hamiltonian is shown, appears arguably more serious. The construction of [3] requires a certain "query Hamiltonian" to have a spectral gap, which indeed holds if the $\mathrm{P}^{\mathrm{QMA}[\log]}$ machine makes no invalid queries. However, if the machine makes invalid queries, this gap can close, and it is not clear how one can recover $\mathrm{P}^{\mathrm{QMA}[\log]}$-hardness under mapping reductions. To overcome this, we introduce a technique of "query validation": Given a query to the QMA oracle, we would like to determine if the query is valid or "far" from valid. While it is not clear how a P machine alone can perform such "query validation", we show how to use a SPECTRAL GAP oracle to do so, allowing us to eliminate "sufficiently invalid" queries. Combining this idea with Ambainis's original construction [3], we show Theorem 1.4, i.e. $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hardness for SPECTRAL-GAP for $O(1)$-local Hamiltonians. Since our "query validation" requires a polynomial number of calls to the SPECTRAL-GAP oracle, this result requires a polynomial-time *Turing* reduction. Whether this can be improved to a mapping reduction is left as an open question.

Significance. The problems studied here explore the line of research recently initiated by Ambainis [3] on $\mathrm{P}^{\mathrm{QMA}[\log]}$, and focus on central problems for local Hamiltonian systems. The complexity theoretic study of such problems is appealing in that it addresses the original motivation of celebrated physicist Richard Feynman in proposing quantum computers [10], who was interested in avenues for simulating quantum systems. Indeed, hardness results, such as Kitaev's Cook-Levin theorem, rigorously justify Feynman's intuition that such simulation problems are "hard". Our work (e.g. Theorem 1.1), in particular, strongly supports this view by demonstrating that even some of the "simplest" and most natural simulation tasks, such as measuring a *single qubit (!)* of a ground state, can be harder than QMA.

Our work on the complexity of estimating spectral gaps (Theorem 1.4) further highlights another theme: The subtleties which must be carefully treated when studying oracle classes for promise problems (such as $\mathrm{P}^{\mathrm{QMA}[\log]}$). As quantum complexity theory commonly focuses on such promise problems, we believe this theme would potentially be of interest to a broader computer science audience.

Open questions. Although we resolve one of the open questions from [3], there are others we leave open, along with some new ones. Do our results for APX-SIM and APX-2-CORR hold for more restricted classes of Hamiltonians, such as 2-local Hamiltonians, local Hamiltonians on a 2D lattice, or specific Hamiltonian models of interest (see e.g. [9, 24] for QMA-completeness results for estimating ground state energies of the spin-1/2 Heisenberg anti-ferromagnet)? Is SPECTRAL-GAP $\mathrm{P}^{\mathrm{UQMA}[\log]}$-complete or $\mathrm{P}^{\mathrm{QMA}[\log]}$-complete (recall SPECTRAL-GAP $\in \mathrm{P}^{\mathrm{QMA}[\log]}$, and [3] and our work together show $\mathrm{P}^{\mathrm{UQMA}[\log]}$-hardness)? What is the relationship between $\mathrm{P}^{\mathrm{QMA}[\log]}$ and $\mathrm{P}^{\mathrm{UQMA}[\log]}$? Finally, what is the complexity of other physical tasks "beyond" estimating ground state energies?

Organization. Section 2 gives notation, formal definitions, and a corollary of the Projection Lemma. Section 3 shows various lemmas regarding Ambainis's query Hamiltonian. Section 4 proves Theorem 1.1. As the proof of Theorem 1.2 uses techniques similar to Theorem 1.1, we defer its proof to the full version of this article. Section 5 shows Theorem 1.3. Theorem 1.4 is given in Section 6. Full proofs of selected claims are deferred to the full version.

2 Preliminaries

Notation. For $x \in \{0,1\}^n$, $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$ denotes the computational basis state labeled by x. Let $\mathcal{X}$ be a complex Euclidean space. Then, $\mathrm{L}(\mathcal{X})$ and $\mathrm{D}(\mathcal{X})$ denote the sets of linear and density operators acting on $\mathcal{X}$, respectively. For subspace $\mathcal{S} \subseteq \mathcal{X}$, $\mathcal{S}^\perp$ denotes the orthogonal complement of $\mathcal{S}$. For Hermitian operator H, $\lambda(H)$ and $\lambda(H|_{\mathcal{S}})$ denote the smallest eigenvalue of H and the smallest eigenvalue of H restricted to space $\mathcal{S}$, respectively. The spectral and trace norms are defined $\|A\|_\infty := \max\{\|A|v\rangle\|_2 : \||v\rangle\|_2 = 1\}$ and $\|A\|_{\mathrm{tr}} := \mathrm{Tr}\sqrt{A^\dagger A}$, respectively, where $:=$ denotes a definition. We set $[m] := \{1, \ldots, m\}$.

Definitions and lemmas. PP [15] is the set of decision problems for which there exists a polynomial-time probabilistic Turing machine which accepts any YES instance with probability $> 1/2$, and accepts any NO instance with probability $\leq 1/2$.

$\mathrm{P}^{\mathrm{QMA}[\log]}$, defined by Ambainis [3], is the set of decision problems decidable by a polynomial-time deterministic Turing machine with the ability to query an oracle for a QMA-complete problem (e.g. the 2-local Hamiltonian problem (2-LH) [18]) $O(\log n)$ times, where n is the size of the input. 2-LH is defined as: Given a 2-local Hamiltonian H and inverse polynomially separated thresholds $a, b \in \mathbb{R}$, decide whether $\lambda(H) \leq a$ (YES-instance) or $\lambda(H) \geq b$ (NO-instance). Note that the P machine is allowed to make queries which violate the promise gap of 2-LH, i.e. with $\lambda(H) \in (a, b)$; in this case, the oracle can output either YES or NO. The P machine is nevertheless required to output the same final answer (i.e. accept or reject) regardless of how such "invalid" queries are answered [16].

For any P machine M making m queries to a QMA oracle, we use the following terminology throughout this article. A *valid* (*invalid*) query satisfies (violates) the promise gap of the QMA oracle. A *correct* query string $y \in \{0,1\}^m$ encodes a sequence of correct answers to all of the m queries. Note that for any invalid query of M, any answer is considered "correct", yielding the possible existence of multiple correct query strings. An *incorrect* query string is one which contains at least one incorrect query answer.

We now recall the definition of APX-SIM.

▶ **Definition 2.1** (APX-SIM$(H, A, k, l, a, b, \delta)$ (Ambainis [3])). Given a k-local Hamiltonian H, an l-local observable A, and real numbers a, b, and δ such that $a - b \geq n^{-c}$ and $\delta \geq n^{-c'}$, for n the number of qubits H acts on and $c, c' > 0$ some constants, decide:

- If H has a ground state $|\psi\rangle$ satisfying $\langle\psi| A |\psi\rangle \leq a$, output YES.
- If for any $|\psi\rangle$ satisfying $\langle\psi| H |\psi\rangle \leq \lambda(H) + \delta$, it holds that $\langle\psi| A |\psi\rangle \geq b$, output NO.

Next, we briefly review Kitaev's circuit-to-Hamiltonian construction from the "quantum Cook-Levin theorem" [19]. Given a quantum circuit $U = U_L \cdots U_1$ consisting of 1- and 2-qubit gates U_i and acting on registers Q (proof register) and W (workspace register), this construction maps U to a 5-local Hamiltonian $H = H_{\mathrm{in}} + H_{\mathrm{out}} + H_{\mathrm{prop}} + H_{\mathrm{stab}}$. Here, we use two key properties of $H_{\mathrm{in}} + H_{\mathrm{prop}} + H_{\mathrm{stab}}$. First, the null space of $H_{\mathrm{in}} + H_{\mathrm{prop}} + H_{\mathrm{stab}}$

is spanned by *history states*, which for any $|\psi\rangle$ have form

$$|\psi_{\text{hist}}\rangle = \sum_{t=0}^{L} U_t \cdots U_1 |\psi\rangle_Q |0\cdots 0\rangle_W |t\rangle_C , \tag{1}$$

where C is a clock register keeping track of time [19]. Second, we use the following lower bound[4] on the smallest non-zero eigenvalue of $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}}$:

▶ **Lemma 2.2** (Lemma 3 (Gharibian, Kempe [12])). *The smallest non-zero eigenvalue of $\Delta(H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}})$ is at least $\pi^2\Delta/(64L^3) \in \Omega(\Delta/L^3)$, for $\Delta \in \mathbb{R}^+$ and $L \geq 1$. construction.*

A useful fact for complex unit vectors $|v\rangle$ and $|w\rangle$ is (see, e.g., Equation 1.33 of [11]):

$$\| |v\rangle\langle v| - |w\rangle\langle w| \|_{\text{tr}} = 2\sqrt{1 - |\langle v|w\rangle|^2} \leq 2 \| |v\rangle - |w\rangle \|_2 . \tag{2}$$

Next, let V denote a QMA verification circuit acting on M proof qubits with completeness c and soundness s. If one runs V on "proof" $\rho = I/2^M$, then for a YES instance, V accepts with probability $\geq c/2^M$ (since $I/2^M$ can be viewed as "guessing" a correct proof with probability $\geq 1/2^M$), and in a NO instance, V accepts with probability $\leq s$ (see, e.g., [23, 27]). The class PQP is defined analogously to BQP, except in the YES case, the verifier accepts with probability $> 1/2$, and in the NO case, the verifier accepts with probability $\leq 1/2$.

A corollary of the Projection Lemma. Finally, we give a simple but useful corollary of the Projection Lemma of Kempe, Kitaev, Regev [18]. The Projection Lemma, along with the proof of Corollary 2.3, are given in the full version.

▶ **Corollary 2.3.** *Let $H = H_1 + H_2$ be the sum of two Hamiltonians operating on some Hilbert space $\mathcal{H} = \mathcal{S} + \mathcal{S}^\perp$. The Hamiltonian H_1 is such that $\mathcal{S}$ is a zero eigenspace and the eigenvectors in $\mathcal{S}^\perp$ have eigenvalue at least $J > 2\|H_2\|_\infty$. Let $K := \|H_2\|_\infty$. Then, for any $\delta \geq 0$ and vector $|\psi\rangle$ satisfying $\langle\psi| H |\psi\rangle \leq \lambda(H) + \delta$, there exists a $|\psi'\rangle \in \mathcal{S}$ such that $|\langle\psi|\psi'\rangle|^2 \geq 1 - \left(\frac{K+\sqrt{K^2+\delta(J-2K)}}{J-2K}\right)^2$.*

3 Ambainis's Query Hamiltonian

We now show various results regarding Ambainis's "query Hamiltonian" [3], which intuitively aims to have its ground space contain correct answers to a sequence of QMA queries. Let U be a $\mathrm{P}^{\mathrm{QMA[log]}}$ computation, and let $H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}$ be the 2-local Hamiltonian corresponding to the ith query made by U given that the answers to the previous $i-1$ queries are given by $y_1 \cdots y_{i-1}$. (Without loss of generality, we may assume $H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}} \succeq 0$ by adding multiples of the identity and rescaling.) The oracle query made at step i corresponds to an input $(H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}, \epsilon, 3\epsilon)$ to 2-LH, for $\epsilon > 0$ a fixed inverse polynomial. Then, Ambainis's [3] $O(\log(n))$-local query Hamiltonian H acts on $\mathcal{X} \otimes \mathcal{Y}$, where $\mathcal{X} = (\mathcal{X}_i)^{\otimes m} = (\mathbb{C}^2)^{\otimes m}$ and $\mathcal{Y} = \otimes_{i=1}^m \mathcal{Y}_i$, such that $\mathcal{X}_i$ is intended to encode the answer to query i with $\mathcal{Y}_i$ encoding the

[4] This bound is stated as $\Omega(\Delta/L^3)$ in [12]; the constant $\pi^2/64$ can be derived from the analysis therein.

ground state of the corresponding query Hamiltonian $H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}$. Specifically,

$$\begin{aligned} H &= \sum_{i=1}^{m} \frac{1}{4^{i-1}} \sum_{y_1,\ldots,y_{i-1}} \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes \left(2\epsilon\,|0\rangle\langle 0|_{\mathcal{X}_i} \otimes I_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}\right) \\ &=: \sum_{i=1}^{m} \frac{1}{4^{i-1}} \sum_{y_1,\ldots,y_{i-1}} M_{y_1\cdots y_{i-1}}. \end{aligned} \tag{3}$$

Recall from Section 2 that a sequence of query answers $y = y_1 \cdots y_m \in \{0,1\}^m$ is *correct* if it corresponds to a possible execution of U. Since U can make queries to its QMA oracle which violate the QMA promise gap, the set of correct y is generally not a singleton. However, we henceforth assume without loss of generality that U makes at least one valid query (i.e. which satisfies the QMA promise gap). For if not, then a P machine can solve such an instance by simulating the $\mathrm{P}^{\mathrm{QMA[log]}}$ machine on all possible (polynomially many) query strings $y \in \{0,1\}^m$. If U corresponds to a YES (NO) instance, then *all* query strings lead to accept (reject), which the P machine can verify. We now prove the following about H.

▶ **Lemma 3.1.** *Define for any $x \in \{0,1\}^m$ the space $\mathcal{H}_{x_1\cdots x_m} := \bigotimes_{i=1}^m |x_i\rangle\langle x_i| \otimes \mathcal{Y}_i$. Then, there exists a correct query string $x \in \{0,1\}^m$ such that the ground state of H lies in $\mathcal{H}_{x_1\cdots x_m}$. Moreover, suppose this space has minimum eigenvalue λ. Then, for any incorrect query string $y_1 \cdots y_m$, any state in $\mathcal{H}_{y_1\cdots y_m}$ has energy at least $\lambda + \frac{\epsilon}{4^m}$.*

As discussed in Section 1, Claim 1 of [3] proved a similar statement under the assumption that the correct query string x is unique. In that setting, [3] showed the ground state of H is in $\mathcal{H}_x$, and that for *all* query strings $y \neq x$, the space $\mathcal{H}_y$ has energy at least $\lambda + \frac{\epsilon}{4^{m-1}}$. However, in general invalid queries must be allowed, and in this setting this claim no longer holds — two distinct correct query strings can have eigenvalues which are arbitrarily close if they contain queries violating the promise gap. The key observation we make here is that even in the setting of non-unique x, a spectral gap between the ground space and all *incorrect* query strings can be shown. The proof is deferred to the full version of this article.

The next lemma converts H from an $O(\log n)$-local Hamiltonian to an $O(1)$-local one. Its proof uses Kitaev's unary encoding trick [19], and is given in the full version.

▶ **Lemma 3.2.** *For any $x \in \{0,1\}^m$, let $\hat{x}$ denote its unary encoding. Then, for any $\mathrm{P}^{\mathrm{QMA[log]}}$ circuit U acting on n bits and making $m \geq 1$ queries to a QMA oracle, there exists a mapping to a 4-local Hamiltonian H' acting on space $(\mathbb{C}^2)^{\otimes 2^m - 1} \otimes \mathcal{Y}$ such that there exists a correct query string $x = x_1 \cdots x_m$ satisfying:*

1. *The ground state of H' lies in subspace $|\hat{x}\rangle\langle\hat{x}| \otimes \mathcal{Y}$.*
2. *For any state $|\psi\rangle$ in subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$ where either $\hat{x}'$ is not a unary encoding of a binary string x' or x' is an incorrect query string, one has $\langle\psi| H' |\psi\rangle \geq \lambda(H') + \epsilon/4^m$, for inverse polynomial ϵ.*
3. *For all strings $x' \in \{0,1\}^m$, H' acts invariantly on subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$.*
4. *The mapping can be computed in time polynomial in n (recall $m \in O(\log n)$).*

4 Measuring 1-local observables

Proof of Theorem 1.1. Containment in $\mathrm{P}^{\mathrm{QMA[log]}}$ was shown for $k, l \in O(\log n)$ in [3]; we show $\mathrm{P}^{\mathrm{QMA[log]}}$-hardness. Let U' be an arbitrary $\mathrm{P}^{\mathrm{QMA[log]}}$ circuit for instance Π, such that U' acts on workspace register W and query result register Q. Suppose U' consists of L' gates and makes $m = c\log(n)$ queries, for $c \in O(1)$ and n the input size. Without loss of generality,

U' can be simulated with a similar unitary U which treats Q as a *proof* register which it does not alter at any point: Namely, U does not have access to a QMA oracle, but rather reads bit Q_i whenever it desires the answer to the ith query. Thus, if a correct query string $y_1 \cdots y_m$ corresponding to an execution of U' on input x is provided in Q as a "proof", then the output statistics of U' and U are identical. We can also assume that Q is encoded not in binary, but in unary. Thus, Q consists of $2^m - 1 \in \text{poly}(n)$ bits. For simplicity, however, in our discussion we will speak of m-bit query strings $y = y_1 \cdots y_m$ in register Q.

Next, we map U to a 5-local Hamiltonian H_1 via a modification of the circuit-to-Hamiltonian construction of Kitaev [19], such that H_1 acts on registers W (workspace register), Q (proof register), and C (clock register). Recall (Section 2) that Kitaev's construction outputs Hamiltonian terms $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}} + H_{\text{out}}$. Set $H_1 = \Delta(H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}})$ for Δ to be set as needed. It is crucial that H_{out} be omitted from H_1, as we require our final Hamiltonian H to enforce a certain structure on the ground space *regardless* of whether the computation should accept or reject. The job of "checking the output" is instead delegated to the observable A. Formally, H_1 has a non-trivial null space, which is its ground space, consisting of history states $|\psi_{\text{hist}}\rangle$ (Equation (1)) which simulate U on registers W and Q. These history states correctly simulate U' *assuming that* Q is initialized to a correct proof.

To thus enforce that Q is initialized to a correct proof, let H_2 be our variant of Ambainis's query Hamiltonian from Lemma 3.2, such that H_2 acts on registers Q and Q' (where for clarity $Q = (\mathbb{C}^2)^{\otimes 2^m - 1}$ (recall $m \in O(\log n)$) and $Q' = \mathcal{Y}$ from Lemma 3.2). Hence, our final Hamiltonian is $H = H_1 + H_2$, which is 5-local since H_1 is 5-local. Suppose without loss of generality that U's output qubit is W_1, which is set to $|0\rangle$ until the final time step, in which the correct output is copied to it. Then, set observable $A = (I + Z)/2$ such that A acts on qubit W_1. Set $a = 1 - 1/(L+1)$, and $b = 1 - 1/2L$ for L the number of gates in U. Fix $\eta \geq \max(\|H_2\|_\infty, 1)$ (such an η can be efficiently computed by applying the triangle inequality and summing the spectral norms of each term of H_2 individually). Set $\Delta = L^3 \eta\gamma$ for γ a monotonically increasing polynomial function of L to be set as needed. Finally, set $\delta = 1/\Delta$. This completes the construction.

Correctness. Suppose Π is a YES instance. Then, by Lemma 3.2, the ground space of H_2 is the span of states of the form $|\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$ where $\hat{x}$ is a correct query string encoded in unary. Fix an arbitrary such ground state $|\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$. Note that setting Q to $\hat{x}$ in this manner causes U to accept with certainty. Consider the history state $|\psi_{\text{hist}}\rangle$ on registers W, C, Q, and Q' (Q and Q' together are the "proof register", and the contents of Q' are not accessed by U), which lies in the ground space of H_1. Since U can read but does not alter the contents of Q, the history state has the tensor product form $|\psi'_{\text{hist}}(x)\rangle_{W,C} \otimes |\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$ for some $|\psi'_{\text{hist}}(x)\rangle_{W,C}$, i.e. the action of H_2 on the history state is unaffected. We conclude that $|\psi'_{\text{hist}}(x)\rangle_{W,C} \otimes |\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$ is in the ground space of H. Moreover, since U accepts $\hat{x}$, the expectation of this state against A is $1 - 1/(L+1)$.

Conversely, suppose we have a NO instance Π, and consider any $|\psi\rangle$ satisfying $\langle\psi| H |\psi\rangle \leq \lambda(H) + \delta$. By Lemma 2.2, the smallest non-zero eigenvalue of ΔH_1 is at least $J = \pi^2\Delta/(64L^3) = \pi^2\eta\gamma/64$. Recalling that $\delta = 1/\Delta$, apply Corollary 2.3 to obtain that there exists a valid history state $|\psi'\rangle$ on W, C, Q, and Q' such that $|\langle\psi|\psi'\rangle|^2 \geq 1 - O(\gamma^{-2}L^{-6})$, which by Equation (2) implies

$$\| |\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'| \|_{\text{tr}} \leq \frac{c}{\gamma L^3} \tag{4}$$

for some constant $c > 0$. By definition, such a history state $|\psi'\rangle$ simulates U given "quantum proof" $|\phi\rangle_{Q,Q'}$ in registers Q and Q', i.e. $|\psi'\rangle = \sum_t U_t \cdots U_1 |0\cdots 0\rangle_W |t\rangle_C |\phi\rangle_{Q,Q'}$. By

Equation (4) and the Hölder inequality, $|\mathrm{Tr}(H|\psi\rangle\langle\psi|) - \mathrm{Tr}(H|\psi'\rangle\langle\psi'|)| \leq \frac{c}{\gamma L^3}\|H\|_\infty =: \gamma'$. Thus, $\langle\psi'|H|\psi'\rangle \leq \lambda(H) + (\delta+\gamma')$.

We now analyze the structure of $|\phi\rangle_{Q,Q'}$. By Lemma 3.2, the ground space $\mathcal{G}$ of H_2 is contained in the span of states of the form $|\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'}$ where $\hat{x}$ is a correct query string encoded in unary. Since the ground spaces of H_1 and H_2 have non-empty intersection, i.e. history states acting on "quantum proofs" from $\mathcal{G}$ (which lie in the null space of H_1 and obtain energy $\lambda(H_2)$ against H_2), we know $\lambda(H) = \lambda(H_2)$. Thus, since $H_1 \succeq 0$,

$$\langle\psi'|H_2|\psi'\rangle \leq \langle\psi'|H|\psi'\rangle \leq \lambda(H_2) + (\delta+\gamma'). \tag{5}$$

Write $|\phi\rangle = \alpha|\phi_1\rangle + \beta|\phi_2\rangle$ for $|\phi_1\rangle \in \mathrm{Span}\{\ |\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'} \mid \text{correct query string } x\}$ and $|\phi_2\rangle \in \mathrm{Span}\{\ |\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'} \mid \text{incorrect query string } x\}$ ($|\phi_1\rangle$, $|\phi_2\rangle$ normalized), $\alpha,\beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$. Since any history state $|\psi'\rangle$, for any amplitudes α_x and unit vectors $|\phi'_x\rangle$, has form $\sum_{t,x}\alpha_x U_t\cdots U_1|0\cdots0\rangle_W|t\rangle_C|\hat{x}\rangle_Q|\phi'_x\rangle_{Q'} = \sum_x \alpha_x|\psi'_{\mathrm{hist}}(x)\rangle_{W,C}|\hat{x}\rangle_Q|\phi'_x\rangle_{Q'}$ (i.e. for any fixed x, $|\hat{x}\rangle_Q$ is not altered), and since H_2 is block-diagonal with respect to strings in Q, by Equation (5) and Lemma 3.2 we have

$$\begin{aligned}\lambda(H_2) + (\delta+\gamma') &\geq \langle\psi'|H_2|\psi'\rangle = |\alpha|^2\langle\phi_1|H_2|\phi_1\rangle + |\beta|^2\langle\phi_2|H_2|\phi_2\rangle \\ &\geq |\alpha|^2\lambda(H_2) + |\beta|^2\left(\lambda(H_2) + \frac{\epsilon}{4^m}\right),\end{aligned}$$

which implies $|\beta|^2 \leq 4^m(\delta+\gamma')/\epsilon$. Thus, defining $|\psi''\rangle$ as the history state for "proof" $|\phi_1\rangle_{Q,Q'}$, we have that $\||\psi\rangle\langle\psi| - |\psi''\rangle\langle\psi''|\|_{\mathrm{tr}}$ is at most

$$\||\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'|\|_{\mathrm{tr}} + \||\phi\rangle\langle\phi| - |\phi_1\rangle\langle\phi_1|\|_{\mathrm{tr}} \leq \frac{c}{\gamma L^3} + 2\sqrt{\frac{4^m(\delta+\gamma')}{\epsilon}}, \tag{6}$$

which follows from the triangle inequality and the structure of the history state. Observe now that increasing γ by a polynomial factor decreases $\delta+\gamma'$ by a polynomial factor. Thus, set γ as a large enough polynomial in L such that

$$\frac{c}{\gamma L^3} + 2\sqrt{\frac{4^m(\delta+\gamma')}{\epsilon}} \leq \frac{1}{2L}. \tag{7}$$

Since U rejects any correct query string (with certainty) in the NO case, and since $|\psi''\rangle$ is a valid history state whose Q register is a superposition over correct query strings (all of which must lead to reject), we conclude that $\langle\psi''|A|\psi''\rangle = 1$. Moreover, we have that $|\mathrm{Tr}(A|\psi\rangle\langle\psi|) - \mathrm{Tr}(A|\psi''\rangle\langle\psi''|)| \leq \|A\|_\infty\||\psi\rangle\langle\psi| - |\psi''\rangle\langle\psi''|\|_{\mathrm{tr}} \leq \frac{1}{2L}$, where the first inequality follows from Hölder's inequality, and the second by Equations (6) and (7). We conclude that $\langle\psi|A|\psi\rangle \geq 1 - 1/(2L)$, completing the proof. ◀

5 $\mathsf{P}^{\mathsf{QMA[log]}}$ is in PP

We now prove Theorem 1.3. Our approach is to develop a variant of the hierarchical voting scheme used in the proof of $\mathrm{P}^{\mathrm{NP[log]}} \subseteq \mathrm{PP}$ [4] which uses the strong error reduction technique of Marriott and Watrous [23]. We also require a more involved analysis than present in [4], since QMA is a class of promise problems, not decision problems.

Proof of Theorem 1.3. Let Π be a P machine which makes $m = c\log n$ queries to an oracle for 2-LH, for $c \in O(1)$ and n the input size. . Without loss of generality, we assume all queries involve Hamiltonians on M qubits (M some fixed polynomial in n). Define $q := (M+2)m$. We give a PQP computation simulating Π; since PQP = PP [27], this yields the claim. Let V denote the verification circuit for 2-LH. The PQP computation is (intuition to follow):

1. For i from 1 to m:
   a. Prepare $\rho = I/2^M \in \mathrm{D}\left((\mathbb{C}^2)^{\otimes M}\right)$.
   b. Run V on the ith query Hamiltonian $H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}$ (see Equation (3)) and proof ρ, and measure the output qubit in the standard basis. Set bit y_i to the result.
2. Let $y = y_1 \cdots y_m$ be the concatenation of bits set in Step 1(b).
3. For i from 1 to $n^c - 1$:
   a. If $|y| < i$, then with probability $1 - 2^{-q}$, set $y = \#$, and with probability 2^{-q}, leave y unchanged.
4. If $y = \#$, output a bit in $\{0,1\}$ uniformly at random. Else, run Π on query string y and output Π's answer.

Intuition. In Step 1, one tries to determine the correct answer to query i by guessing a satisfying quantum proof for verifier V. Suppose for the moment that V has zero error, i.e. has completeness 1 and soundness 0, and that Π only makes valid queries. Then, if Step 1(b) returns $y_i = 1$, one knows with certainty that the query answer should be 1. And, if the correct answer to query i is 0, then Step 1(b) returns $y_i = 0$ with certainty. Thus, analogous to the classical case of an NP oracle (as done in [4]), it follows that the lexicographically *largest* query string y^* obtainable by this procedure must be the (unique) correct query string (note that $y^* \neq 1^m$ necessarily[5]). Thus, ideally one wishes to obtain y^*, simulate Π on y^*, and output the result. To this end, Step 3 ensures that among all values of $y \neq \#$, y^* is more likely to occur than all other $y \neq y^*$ combined. We now make this intuition rigorous (including in particular the general case where V is not zero-error and Π makes invalid queries).

Correctness. To analyze correctness of our PQP computation, it will be helpful to refine our partition of the set of query strings $\{0,1\}^m$ into three sets:

- **(Correct query strings)** Let $A \subseteq \{0,1\}^m$ denote the set of query strings which correspond to correctly answering each of the m queries. Note we may have $|A| > 1$ if invalid queries are made.
- **(Incorrect query strings)** Let $B \subseteq \{0,1\}^m \setminus A$ denote the set of query strings such that for any $y \in B$, all bits of y which encode an incorrect query answer are set to 0 (whereas the correct query answer would have been 1, i.e. we failed to "guess" a good proof for this query in Step 1).
- **(Strongly incorrect query strings)** Let $C = \{0,1\}^m \setminus (A \cup B)$ denote the set of query strings such that for any $y \in C$, at least one bit corresponding to an incorrect query answer is set to 1 (whereas the correct query answer would have been 0). Such an error can only arise due to the bounded-error of our QMA verifier in Step 1(b).

Let Y be a random variable corresponding to the query string y obtained at the end of Step 3. To show correctness, we claim that it suffices to show that $\Delta := \Pr[Y \in A] - \Pr[Y \in B \cup C] > 0$. To see this, let p_1, p_2, and p_3 denote the probability that after Step 3, $y = \#$, $y \in A$, and $y \in B \cup C$, respectively. Then, $p_1 + p_2 + p_3 = 1$, and let $p_2 - p_3 = \Delta > 0$. Suppose now that the input to Π is a YES instance. Then, our protocol outputs 1 with probability at least $\frac{p_1}{2} + p_2 = \frac{1-p_2-p_3}{2} + p_2 = \frac{1+\Delta}{2} > \frac{1}{2}$. If the input is a NO instance, the protocol outputs

[5] Under the assumptions that V has zero error and Π makes only valid queries, $y^* = 1^m$ can only be obtained by this procedure if all queries are for YES instances of 2-LH. If, on the other hand, query i is a NO query, then a correct proof cannot be guessed (since it does not exist), and so $y_i^* = 0$ necessarily.

1 with probability $\leq \frac{p_1}{2} + p_3 = \frac{1-\Delta}{2} < \frac{1}{2}$. We hence have a PQP computation, as desired. We thus now show that $\Delta > 0$.

To ease the presentation, we begin by making two assumptions (to be removed later): (i) V is zero-error and (ii) Π makes only valid queries. In this case, assumption (i) implies $C = \emptyset$ (i.e. all incorrect query strings belong to B), and (ii) implies A is a singleton (i.e. there is a unique correct query string y^*). Thus, here $\Delta = \Pr[Y \in A] - \Pr[Y \in B]$.

To begin, note that for any $y \in \{0,1\}^m$, we have

$$\Pr[Y = y] = \Pr[y \text{ chosen in Step 2 }] \cdot \left(\frac{1}{2^q}\right)^{(n^c-1)-|y|}, \tag{8}$$

where $|y|$ denotes the non-negative integer represented by string y. Let $\mathrm{HW}(x)$ denote the Hamming weight of $x \in \{0,1\}^m$. Since each query corresponds to a verifier on M proof qubits, we have for (the unique) $y^* \in A$ that

$$\Pr[y^* \text{ chosen in Step 2 }] \geq 2^{-M \cdot \mathrm{HW}(y^*)} \geq 2^{-Mm} \tag{9}$$

(recall from Section 2 that setting $\rho = I/2^M$ simulates "guessing" a correct proof with probability at least $1/2^M$). It follows by Equations (8) and (9) that

$$\begin{aligned} \Delta &\geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y^*|} \left[\frac{1}{2^{Mm}} - \sum_{y \in B} \left(\frac{1}{2^q}\right)^{|y^*|-|y|}\right] \\ &\geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y^*|} \left[\frac{1}{2^{Mm}} - (2^m)\left(\frac{1}{2^q}\right)\right] \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m}\right], \end{aligned} \tag{10}$$

where the first inequality follows since $\Pr[y \text{ chosen in Step 2 }] \leq 1$, the second since $y \in B$ if and only if $|y| < |y^*|$, and the third since $q = (M+2)m$. Thus, $\Delta > 0$ as desired.

Removing assumption (i). We now remove the assumption that V is zero error. In this case, A is still a singleton; let $y^* \in A$. We can now also have strongly incorrect query strings, i.e. $C \neq \emptyset$ necessarily. Assume without loss of generality that V acts on M proof qubits, and by strong error reduction [23] has completeness $c := 1 - 2^{-p(n)}$ and soundness $s := 2^{-p(n)}$, for p a polynomial to be chosen as needed. Then, since V can err, Equation (9) becomes

$$\begin{aligned} \Pr[y^* \text{ chosen in Step 2 }] &\geq \left(\frac{c}{2^M}\right)^{\mathrm{HW}(y^*)} (1-s)^{m-\mathrm{HW}(y^*)} = \frac{1}{2^M}^{\mathrm{HW}(y^*)} e^{m \ln(1-\frac{1}{2^p})} \\ &\geq \frac{1}{2^{Mm}} \left(1 - \frac{m}{2^p - 1}\right), \end{aligned} \tag{11}$$

where the equality follows by the definitions of c and s, and the second inequality by applying the Maclaurin series expansion of $\ln(1+x)$ for $|x| < 1$ and the fact that $e^t \geq 1 + t$ for all $t \in \mathbb{R}$. Thus, the analysis of Equation (10) yields that

$$\Pr[Y \in A] - \Pr[Y \in B] \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p - 1}\right], \tag{12}$$

i.e. the additive error introduced when assumption (i) is dropped scales as $\approx 2^{-p}$. Crucially, Equation (12) holds for all $y \in B$ even with assumption (i) dropped since the analysis of Equation (10) used only the trivial bound $\Pr[y \text{ chosen in Step 2 }] \leq 1$ for any $y \in B$.

Next, we upper bound the probability of obtaining $y \in C$ in Step 2. For any fixed $y \in C$, suppose the first bit on which y and y^* disagree is bit j. Then, bits j of y and y^* must be

1 and 0, respectively. This means 0 is the correct answer for query j. By the soundness property of V, the probability of obtaining 1 on query j (and hence that of obtaining y in Step 2) is at most 2^{-p}. Thus,

$$\Delta \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p - 1}\right] - \frac{2^m}{2^p}. \tag{13}$$

We conclude that setting p to a sufficiently large fixed polynomial ensures $\Delta > 0$, as desired.

Removing assumption (ii). We now remove the assumption that Π only makes valid queries, which is the most involved step. Here, A is no longer necessarily a singleton. The naive approach would be to let y^* denote the *lexicographically largest* string in A, and attempt to run a similar analysis as before. Unfortunately, this no longer necessarily works for the following reason. For any invalid query i, we do not have strong bounds on the probability that V accepts in Step 1(b); in principle, this value can lie in the range $(2^{-p}, 1 - 2^{-p})$. Thus, running the previous analysis with the lexicographically largest $y^* \in A$ may cause Equation (13) to yield a negative quantity. We hence require a more delicate analysis.

We begin by showing the following lower bound.

▶ **Lemma 5.1.** *Define* $\Delta' := \Pr[Y \in A] - \Pr[Y \in B]$. *Then,*

$$\Delta' \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p - 1}\right].$$

Proof of Lemma 5.1. For any string $y \in \{0,1\}^m$, let $I_y \subseteq \{1, \ldots, m\}$ denote the indices of all bits of y set by invalid queries. We call each such $i \in I_y$ a *divergence point*. Let $p_{y,i}$ denote the probability that (invalid) query i (defined given answers to queries 1 through $i-1$) outputs bit y_i, i.e. $p_{y,i}$ denotes the probability that at divergence point i, we go in the direction of bit y_i. We define the *divergence probability* of $y \in \{0,1\}^m$ as $p_y = \Pi_{i \in I_y} p_{y,i}$, i.e. p_y is the probability of answering all invalid queries as y did.

The proof now proceeds by giving an iterative process, $\Gamma(i)$, where $1 \leq i \leq |A|$ denotes the iteration number. Each iteration defines a 3-tuple $(y^*_{i-1}, y^*_i, B_{y^*_i}) \in \{0,1\}^m \times \{0,1\}^m \times \mathcal{P}(B)$, where $\mathcal{P}(X)$ denotes the power set of set X. Set $\Delta'_i := \Pr[Y \in \{y^*_1, \ldots, y^*_i\}] - \Pr[Y \in B_{y^*_1} \cup \cdots \cup B_{y^*_i}]$, where it will be the case that $\{B_{y^*_i}\}_{i=1}^{|A|}$ is a partition of B. Thus, we have $\Delta' \geq \Delta'_{|A|}$, implying that a lower bound on $\Delta'_{|A|}$ suffices to prove our claim. We hence prove via induction that for all $1 \leq i \leq |A|$, $\Delta'_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right]$. The definition of process $\Gamma(i)$ is integrated into the induction proof below.

Base case (i=1). In this case y^*_0 is undefined. Set y^*_1 to any string in A with divergence probability at least

$$p^*_1 = \prod_{i \in I_{y^*_1}} p_{y^*_1,i} \geq 2^{-\left|I_{y^*_1}\right|}. \tag{14}$$

Such a string must exist, since at each divergence point i, at least one of the outcomes in $\{0,1\}$ occurs with probability at least $1/2$. (Note: Queries are not being made to a QMA oracle here, but to a QMA verifier V with a maximally mixed proof as in Step 1(a). Whereas in the former case the output of the oracle on an invalid query does not have to consistently output a value with any particular probability, in the latter case, there is some fixed probability p with which V outputs 1 each time it is run on a fixed proof.) Finally, define $B_{y^*_1} := \{y \in B \mid |y| < |y^*_1|\}$ (recall $|y|$ is the non-negative integer with binary encoding y).

Let k_* denote the number of divergence points of y_1^* (i.e. $k_* = \left|I_{y_1^*}\right|$), and k_0 (k_1) the number of zeroes (ones) of y_1^* arising from valid queries. Thus, $k_* + k_0 + k_1 = m$. Then, Equation (11) becomes

$$\begin{aligned}\Pr[y_1^* \text{ in Step 2 }] &\geq \left(\frac{c}{2^M}\right)^{k_1} (1-s)^{k_0}\, p_1^* \geq \left(\frac{1}{2^M}\right)^{k_1} \left(\frac{1}{2}\right)^{k_*} \left(1 - \frac{m-k_*}{2^p-1}\right) \\ &\geq \frac{1}{2^{Mm}} \left(1 - \frac{m}{2^p-1}\right), \end{aligned} \tag{15}$$

where the second inequality follows from Equation (14), and the third since $k_* \geq 0$ and $k_1 + k_* \leq m$. Thus, Δ_1' is lower bounded by the expression in Equation (12) via an analogous analysis for y_1^* and $B_{y_1^*}$.

Inductive step. Assume the claim holds for $1 \leq i-1 < |A|$. We show it holds for i. Let y_{i-1}^* be the choice of y^* in the previous iteration $i-1$ of our process. Define $A_{y_i^*} := \{\, y \in A \mid |y| > \left|y_{i-1}^*\right| \,\}$. Partition $A_{y_i^*}$ into sets S_k for $k \in [m]$, such that S_k is the subset of strings in $A_{y_i^*}$ which agrees with y_{i-1}^* on the first $k-1$ bits, but disagrees on bit k. Note that if $S_k \neq \emptyset$, then bit k of y_{i-1}^* is 0 and bit k of any string in S_k is 1. For each $S_k \neq \emptyset$, choose arbitrary representative $z_k \in S_k$, and define *bounded* divergence probability $q_i(k) := \prod_{t \in I_{z_k}^{\leq k}} p_{z_k,t}$ where $I_{z_k}^{\leq k} := \{\, t \in I_{z_k} \mid t \leq k \,\}$. Note that $q_i(k) > 0$ (since $S_k \neq \emptyset$). Else if $S_k = \emptyset$, set $q_i(k) = 0$. Let q_i^* be the max such bounded divergence probability:

$$q_i^* = \max_{k \in [m]} q_i(k) \qquad \text{and} \qquad k_i^* = \arg\max_{k \in [m]} q_i(k). \tag{16}$$

Let y_i^* be the lexicographically largest query string in $S_{k_i^*}$ with divergence probability p_i^* s.t.:

$$p_i^* \geq q_i^* \cdot 2^{-\left|I_{y_i^*}\right| + \left|I_{y_i^*}^{\leq k_i^*}\right|}. \tag{17}$$

That such a $y_i^* \in S_{k_i^*}$ exists follows from an argument similar to Equation (14): By definition, q_i^* denotes the bounded divergence probability for all invalid queries up to and including query k_i^*, and the term exponential in $\left(-\left|I_{y_i^*}\right| + \left|I_{y_i^*}^{\leq k_i^*}\right|\right)$ is obtained by greedily choosing, for all invalid queries of y_i^* *after* query k_i^*, the outcome which occurs with probability at least 1/2. Set $B_{y_i^*} := \{\, y \in B \mid \left|y_{i-1}^*\right| < |y| < |y_i^*| \,\}$. The following is proved in the full version.

▶ **Lemma 5.2.** *For any $y \in B_{y_i^*}$, $\Pr[y$ chosen in Step 2$] \leq q_i^*$.*

To continue with the inductive step, again consider k_*, k_0, and k_1, now corresponding to y_i^*. Then, an argument similar to Equation (15) says $\Pr[y_i^*$ chosen in Step 2] is at least

$$\begin{aligned}\left(\frac{c}{2^M}\right)^{k_1} (1-s)^{k_0}\, p_i^* &\geq \left(\frac{1}{2^M}\right)^{k_1} \left(1 - \frac{m-k_*}{2^p-1}\right) q_i^* \left(\frac{1}{2}\right)^{\left|I_{y_i^*}\right| - \left|I_{y_i^*}^{\leq k_i^*}\right|} \\ &\geq \frac{q_i^*}{2^{Mm}} \left(1 - \frac{m}{2^p-1}\right), \end{aligned} \tag{18}$$

where the first inequality follows from Equation (17), and the second since $\left|I_{y_i^*}\right| - \left|I_{y_i^*}^{\leq k_i^*}\right| \leq k_*$. Now, define $\zeta_i := \Pr[Y = y_i^*] - \Pr[Y \in B_{y_i^*}]$. Applying the argument of Equation (10) yields $\zeta_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y_i^*|} \left[\frac{q_i^*}{2^{Mm}}\left(1 - \frac{m}{2^p-1}\right) - q_i^* \sum_{y \in B_{y_i^*}} \left(\frac{1}{2^q}\right)^{|y_i^*|-|y|}\right]$, where the first q_i^* is due

to Equation (18), and the second q_i^* to Lemma 5.2. Thus, similar to Equation (12), $\zeta_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{q_i^*}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right] > 0$. Observing the recurrence that for all i, $\Delta'_i \geq \Delta'_{i-1} + \zeta_i$, unrolling this recurrence yields $\Delta'_i \geq \Delta_1$, which by the base case yields the claim. ◀

We require one last lemma (proof in the full version).

▶ **Lemma 5.3.** $\Pr(Y \in C) \leq \frac{2^m}{2^p}$.

Finally, combining Lemmas 5.1 and 5.3 yields that $\Pr[Y \in A] - \Pr[Y \in B \cup C]$ is lower bounded by $\Pr[Y \in A] - \Pr[Y \in B] - \Pr[Y \in C] \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p}\right] - \frac{2^m}{2^p}$. For sufficiently large fixed p, this quantity is strictly positive, yielding Theorem 1.3. ◀

6 Estimating spectral gaps

We now prove Theorem 1.4 on SPECTRAL-GAP. UQMA is defined in Appendix A.

▶ **Definition 6.1** (SPECTRAL-GAP(H, ϵ) (Ambainis [3])). Given a Hamiltonian H and a real number $\alpha \geq n^{-c}$ for n the number of qubits H acts on and $c > 0$ some constant, decide:

- If $\lambda_2 - \lambda_1 \leq \alpha$, output YES.
- If $\lambda_2 - \lambda_1 \geq 2\alpha$, output NO.

where λ_2 and λ_1 denote the second and first smallest eigenvalues of H, respectively.

For clarity, if the ground space of H is degenerate, then we define its spectral gap as 0.

We now discuss Theorem 1.4. Previously, Ambainis [3] showed that SPECTRAL-GAP $\in \mathrm{P}^{\mathrm{QMA[log]}}$, and gave a claimed proof that SPECTRAL-GAP is $\mathrm{P}^{\mathrm{UQMA[log]}}$-hard for $O(\log)$-local Hamiltonians under mapping reductions. ($\mathrm{P}^{\mathrm{UQMA[log]}}$ is defined as $\mathrm{P}^{\mathrm{QMA[log]}}$, except with a UQMA oracle in place of a QMA oracle.) As discussed in Section 1, however, Ambainis' proof of the latter result does not hold if the $\mathrm{P}^{\mathrm{UQMA[log]}}$ machine makes invalid queries (which in general is the case). Here, we build on Ambainis' approach [3] to show $\mathrm{P}^{\mathrm{UQMA[log]}}$-hardness of SPECTRAL-GAP under Turing reductions even when invalid queries are allowed, and we also improve the hardness to apply to $O(1)$-local Hamiltonians.

We begin by showing the following modified version of Lemma 3.2 tailored to UQMA. In contrast to Lemma 3.2, the lemma below only proves the *existence* of a Hamiltonian H; it does not give an *efficient* procedure for computing it. The proof is in the full version; roughly, it replaces invalid queries with "dummy" NO queries to obtain the desired spectral gap. The reason why the mapping is not efficient is that generally a polynomial-time machine alone cannot identify such invalid queries.

▶ **Lemma 6.2.** *For any $x \in \{0,1\}^m$, let $\hat{x}$ denote its unary encoding. Then, for any $\mathrm{P}^{\mathrm{UQMA[log]}}$ circuit U acting on n bits and making m queries to a* UQMA *oracle, there exists a 4-local Hamiltonian H acting on space $(\mathbb{C}^2)^{\otimes 2^m - 1} \otimes \mathcal{Y}$ such that there exists a correct query string $x = x_1 \cdots x_m$ such that:*

1. *The unique ground state of H lies in subspace $|\hat{x}\rangle\langle\hat{x}| \otimes \mathcal{Y}$.*
2. *The spectral gap of H is at least $(\epsilon - \delta)/4^m$ for inverse polynomial ϵ, δ with $\epsilon - \delta \geq 1/\mathrm{poly}(n)$.*
3. *For all strings $x' \in \{0,1\}^m$, H acts invariantly on subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$.*

Proof sketch of Theorem 1.4. The key idea is to show how to use an *oracle* for SPECTRAL-GAP polynomially many times to efficiently identify invalid queries, and hence efficiently compute H in Lemma 6.2 given U. (It is these *multiple* uses of the oracle which yield a Turing reduction, rather than a many-one reduction.) Roughly, this is done by using

the SPECTRAL-GAP oracle in conjunction with binary search to estimate the spectral gap of specific Hamiltonian terms in Ambainis's original construction of [3]. Some care is required here: The naive approach, which does not work, would be to apply this spectral gap estimation technique to each 2-local Hamiltonian $H_{\mathcal{Y}_i}^{i,y_1\cdots y_{i-1}}$ corresponding to each query made by U. Rather, the terms we apply this technique to exploit the structure of Ambainis's construction. Finally, with H in hand, we apply Ambainis's [3] original construction to obtain the desired result. The full proof is given in the full version of this article. ◀

Acknowledgements. We thank Xiaodi Wu for stimulating discussions which helped motivate this project, including suggesting to think about two-point correlation functions (which arose via discussions with Aram Harrow, whom we also thank). We also thank Andris Ambainis and Norbert Schuch for helpful discussions, and remark they independently conceived of some of the ideas behind Lemma 3.2 and Theorem 1.1, respectively (private communication).

References

1 D. Aharonov, M. Ben-Or, F. Brandão, and O. Sattath. The pursuit for uniqueness: Extending Valiant-Vazirani theorem to the probabilistic and quantum settings. Available at arXiv.org e-Print quant-ph/0810.4840v1, 2008.

2 D. Aharonov and T. Naveh. Quantum NP - A survey. Available at arXiv.org e-Print quant-ph/0210077v1, 2002.

3 A. Ambainis. On physical problems that are slightly more difficult than QMA. In *Proceedings of 29th IEEE Conference on Computational Complexity (CCC 2014)*, pages 32–43, 2014.

4 R. Beigel, L. A. Hemachandra, and G. Wechsung. On the power of probabilistic polynomial time: $\mathrm{P}^{\mathrm{NP}[\log]} \subseteq \mathrm{PP}$. In *Proceedings of the 4th IEEE Conference on Structure in Complexity Theory*, pages 225–227, 1989.

5 A. D. Bookatz. QMA-complete problems. *Quantum Information & Computation*, 14(5–6), 2014.

6 B. Brown, S. Flammia, and N. Schuch. Computational difficulty of computing the density of states. *Physical Review Letters*, 104:040501, 2011.

7 A. Chailloux and O. Sattath. The complexity of the separable Hamiltonian problem. In *Proceedings of 27th IEEE Conference on Computational Complexity (CCC 2012)*, pages 32–41, 2012.

8 S. Cook. The complexity of theorem proving procedures. In *Proceedings of the 3rd ACM Symposium on Theory of Computing (STOC 1972)*, pages 151–158, 1972.

9 T. Cubitt and A. Montanaro. Complexity classification of local hamiltonian problems. Available at arXiv.org e-Print quant-ph/1311.3161, 2013.

10 R. Feynman. Quantum mechanical computers. *Optics News*, 11:11, 1985.

11 S. Gharibian. *Approximation, proof systems, and correlations in a quantum world.* PhD thesis, University of Waterloo, 2013. Available at arXiv.org e-Print quant-ph/1301.2632.

12 S. Gharibian and J. Kempe. Hardness of approximation for quantum problems. In *Proceedings of 39th International Colloquium on Automata, Languages and Programming (ICALP 2012)*, pages 387–398, 2012.

13 S. Gharibian and J. Sikora. Ground state connectivity of local Hamiltonians. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015)*, pages 617–628, 2015.

14 Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum hamiltonian complexity. *Foundations and Trends in Theoretical Computer Science*, 10(3):159–282, 2015. doi:10.1561/0400000066.

15 J. Gill. Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing*, 6(4):675–695, 1977.
16 O. Goldreich. On promise problems: A survey. *Theoretical Computer Science*, 3895:254–290, 2006.
17 R. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103. New York: Plenum, 1972.
18 J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.
19 A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.
20 A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd ACM Symposium on Theory of Computing (STOC 2000)*, pages 608–617, 2000.
21 L. Levin. Universal search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.
22 Y.-K. Liu. Consistency of local density matrices is QMA-complete. In *Lecture Notes in Computer Science*, volume 4110, pages 438–449, 2006.
23 C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.
24 S. Piddock and A. Montanaro. The complexity of antiferromagnetic interactions and 2d lattices. Available at arXiv.org e-Print quantph/1506.04014, 2015.
25 Y. Shi and S. Zhang. Note on quantum counting classes. URL: `http://www.cse.cuhk.edu.hk/~syzhang/papers/SharpBQP.pdf`.
26 M. Vyalyi. QMA=PP implies that PP contains PH. *Electronic Colloquium on Computational Complexity*, 2003.
27 J. Watrous. *Encyclopedia of Complexity and System Science*, chapter Quantum Computational Complexity. Springer, 2009.

A Additional definitions

▶ **Definition 1.1** (Unique QMA (UQMA) (Aharonov *et al.* [1])). We say a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in Unique QMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{ Q_n \}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a quantum proof $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (Completeness) If $x \in A_{\text{yes}}$, then there exists a proof $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ such that Q_n accepts $(x, |y\rangle)$ with probability at least $2/3$, and for all $|\hat{y}\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ orthogonal to $|y\rangle$, Q_n accepts $(x, |\hat{y}\rangle)$ with probability at most $1/3$.
- (Soundness) If $x \in A_{\text{no}}$, then for all proofs $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$, Q_n accepts $(x, |y\rangle)$ with probability at most $1/3$.

Provably Secure Key Establishment Against Quantum Adversaries*

Aleksandrs Belovs[†1], Gilles Brassard[‡2], Peter Høyer[§3], Marc Kaplan[¶4], Sophie Laplante[‖5], and Louis Salvail[6]**

1 **University of Latvia, Riga, Latvia**
stiboh@gmail.com

2 **DIRO, Université de Montréal, Montréal, Canada and Canadian Institute for Advanced Research, Toronto, Canada**
salvail@iro.umontreal.ca

4 **Department of Computer Science, University of Calgary, Calgary, Canada**
hoyer@ucalgary.ca

5 **School of Informatics, University of Edinburgh, Edinburgh, Great Britain**
kapmarc@gmail.com

6 **IRIF, Université Paris Diderot, Paris, France**
laplante@irif.fr

6 **DIRO, Université de Montréal, Montréal, Canada**
salvail@iro.umontreal.ca

Abstract

At Crypto 2011, some of us had proposed a family of cryptographic protocols for key establishment capable of protecting quantum *and classical* legitimate parties unconditionally against a *quantum* eavesdropper in the query complexity model. Unfortunately, our security proofs were unsatisfactory from a cryptographically meaningful perspective because they were sound only in a worst-case scenario. Here, we extend our results and prove that for any $\varepsilon > 0$, there is a classical protocol that allows the legitimate parties to establish a common key after $O(N)$ expected queries to a random oracle, yet any quantum eavesdropper will have a vanishing probability of learning their key after $O(N^{1.5-\varepsilon})$ queries to the same oracle. The vanishing probability applies to a typical run of the protocol. If we allow the legitimate parties to use a quantum computer as well, their advantage over the quantum eavesdropper becomes arbitrarily close to the quadratic advantage that classical legitimate parties enjoyed over classical eavesdroppers in the seminal 1974 work of Ralph Merkle. Along the way, we develop new tools to give lower bounds on the number of quantum queries required to distinguish two probability distributions. This method in itself could have multiple applications in cryptography. We use it here to study average-case quantum query complexity, for which we develop a new composition theorem of independent interest.

---

* A full version of the paper is available at [6], https://arxiv.org/abs/1704.08182.

† The work of AB is supported in part by the ERC Advanced Grant MQC.

‡ The work of GB is supported in part by the Canadian Institute for Advanced Research (CIFAR), the Canada Research Chair program, Canada's Natural Sciences and Engineering Research Council (NSERC) and Québec's Institut transdisciplinaire d'information quantique.

§ The work of PH is supported in part by CIFAR and NSERC.

¶ The work of MK is supported in part by EPSRC grant number EP1N003829/1 Verification of Quantum Technology.

‖ The work of SL is supported in part by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 600700 (QALGO) and the French ANR Blanc grant RDAM ANR-12-BS02-005.

** The work of LS is supported in part by NSERC discovery grant and discovery accelerator supplements programs.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 3; pp. 3:1–3:17
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1998 ACM Subject Classification A. General Literature

Keywords and phrases Merkle puzzles, Key establishment schemes, Quantum cryptography, Adversary method, Average-case analysis

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.3

1 Introduction

Not taking classified work within secret services into consideration [28], Ralph Merkle is the first person to have asked – and solved – the question of secure communications over insecure channels [24]. In his seminal (rejected!) 1974 project for a Computer Security course at the University of California, Berkeley, he discovered that it is possible for two people who want to communicate securely to establish a secret key by communicating over an authenticated channel that provides no protection against eavesdropping. Merkle's solution to this conundrum offers *quadratic security* in the sense that if the legitimate parties – codenamed Alice and Bob – are willing to expend an effort in the order of N, for some security parameter N, they can establish a key that no eavesdropper – codenamed Eve – can discover with better than vanishing probability without expending an effort in the order of N^2.

This quadratic security may seem unattractive compared to the potential exponential security entailed by the subsequently discovered key establishment protocols of Diffie and Hellman [16] and Rivest, Shamir and Adleman [26], to name a few. However, the security of those currently ubiquitous cryptographic solutions will be compromised with the advent of full-scale quantum computers, as discovered by Peter Shor more than two decades ago [27]. And even if a quantum computer is never built, no one has been able to prove their security against classical attacks, nor that of quantum-resistant candidates based, for instance, on short vectors in lattices. Furthermore, Merkle had already understood in 1974 that quadratic security *could* be practical if the underlying one-way function (see below) can be computed very quickly: if it takes one nanosecond to compute the function and legitimate users are willing to spend one second each, a classical adversary who could only invert the function by exhaustive search would require fifteen expected *years* to break Merkle's original scheme.

The main interest of Merkle's solution is that it offers *provable* security, at least in the *query model* of computational complexity, a model closely related to the random oracle model. In this model, we assume the existence of a *black-box* function $f : D \to R$ from some domain D to some range R, so that the only way to learn something about this function is to query the value of $f(x)$ on inputs $x \in D$ that can be chosen arbitrarily. The *query complexity* of some problem given f is defined as the expected number of calls to f required to solve the problem, using the best possible algorithm. In our case of interest, we shall consider *random* black-box functions, meaning that for each $x \in D$, the value of $f(x)$ is chosen uniformly at random within R, independently of the value of $f(x')$ for any other $x' \in D$. Provided the size r of R is sufficiently large compared to the size d of D, such a random function is automatically one-to-one, except with vanishing probability. The main characteristic of these black-box random functions that is relevant to the proof of security of Merkle's scheme is that, given a randomly chosen point y in the image of f, the only (classical) approach to finding an x so that $f(x) = y$ is exhaustive search: we have to try x's one after another until a solution is found. Indeed, whenever we try some x' and find that $f(x') \neq y$, the *only* thing we have learned is that this particular x' is not a solution. Provided the function is indeed

one-to-one, we expect to have to query the function $d/2$ times on average in order to find the unique solution.

One may argue that black-box random functions do not exist in real life, but we can replace them in practice with one-way functions – provided *they* exist! – which is what Merkle meant by "one-way encryption" in his 1974 class assignment [24]. Thus, we can base the security of Merkle's scheme on the *generic* assumption that one-way functions exist, which is unlikely to be broken by a quantum computer, rather than the assumption that *specific* computational problems such as factorization or finding short vectors in lattices are difficult, at least the first one of which is known not to hold on a quantum computer. Can we do better than provable *quadratic* security in the query model? This question remained open for 35 years, and was finally settled in the negative by Boaz Barak and Mohammad Mahmoody-Ghidary [4], building on earlier work of Russell Impagliazzo and Steven Rudich [19]: any protocol by which the legitimate parties can obtain a shared key after $O(N)$ expected queries to a black-box random function can be broken with $O(N^2)$ expected queries to the same black box.

It was apparently noticed for the first time by one of us in 2005, and published a few years later [15], that Merkle's original 1974 scheme [24], as well as his better known subsequently published *puzzles* [25], are broken by Grover's algorithm [17] on a quantum computer. This attack assumes that the eavesdropper can query the function in quantum superposition, which is perhaps not reasonable if the function is provided as a *physical* classical black box, but is completely reasonable if it is given by the publicly-available *code* of a one-way function (as originally envisioned by Merkle). If the legitimate parties are also endowed with a quantum computer, the same paper [15] gave an obvious fix, by which the legitimate parties can establish a key after $O(N)$ quantum queries to the black-box function, but no quantum eavesdropper can discover it with better than vanishing probability without querying the function $O(N^{3/2})$ times. That paper made the explicit conjecture that this was best possible when quantum codemakers are facing quantum codebreakers in the game of provable security in the random black-box model. The issue of protecting classical codemakers against quantum codebreakers was not addressed in Ref. [15].

At the Crypto 2011 conference [13], several of us disproved the conjecture of Ref. [15] with the introduction of a new quantum protocol that no quantum eavesdropper could break without querying the black-box functions $\Omega(N^{5/3})$ times.[1] We also offered the first protocol provably capable of protecting *classical* codemakers against *quantum* codebreakers, although $O(N^{13/12})$ queries in superposition sufficed for the quantum eavesdropper to obtain the not-so-secret key. Unfortunately, our security proofs were worked out in the traditional computational complexity *worst-case* scenario. In other words, it was only proved that any quantum eavesdropper limited to $o(N^{5/3})$ or $o(N^{13/12})$ queries, depending on whether the legitimate parties are quantum or classical, would be likely to fail *on at least one possible instance* of the protocol. This did not preclude that most instances of the protocol could result in insecure keys against an eavesdropper who would work no harder than the legitimate parties. Said otherwise, our Crypto 2011 result was of limited cryptographic significance.

In subsequent work [14], we claimed to have provided a proper average-case analysis of our protocols, rendering them cryptographically meaningful, so that any quantum eavesdropper has a vanishing probability of learning the key after only $o(N^{5/3})$ or $o(N^{7/6})$ queries[2], where the probabilities are taken not only over the execution of the eavesdropping algorithm but

[1] The word "functions" is plural because the 2011 protocol required *two* black-box random functions.
[2] For classical legitimate parties, the $o(N^{13/12})$ of Ref. [13] had been improved to $o(N^{7/6})$ in Ref. [14].

also over the instance of the protocol run by the legitimate parties. We also extended our results to two sequences of protocols based on the k-SUM problem (Definition 1 in Section 3), where $k \geq 2$ is an integer parameter, in which the legitimate parties query the black-box random functions $O(kN)$ times. It was claimed that any quantum eavesdropper had a vanishing probability of learning the key after $o(N^{\frac{1}{2}+\frac{k}{k+1}})$ or $o(N^{1+\frac{k}{k+1}})$ queries, against the classical or the quantum protocol parametrized by k, respectively. Again, this was claimed to hold not only in the cryptographically-challenged worst-case scenario, but also when the probabilities are taken over the protocols being run by the legitimate parties.

Unfortunately, all our average-case analyses in Ref. [14] were incorrect! The case $k = 2$ can be fixed rather easily, hence the insufficiency of $o(N^{5/3})$ queries for a quantum-against-quantum protocol and of $o(N^{7/6})$ queries for a classical-against-quantum protocol in a cryptographically significant setting can be derived from the incorrect arguments provided in Ref. [14]. However, we also claimed in Ref. [14] that the case $k > 2$ could be proved in ways "similar to" when $k = 2$. This was a mistake due to a fundamental difference in the k-SUM problem whether $k = 2$ or $k > 2$. Whereas the 2-SUM problem is easily seen to be random self-reducible, so that its hardness in worst case implies its hardness on average, this does not seem to be the case for the k-SUM problem when $k > 2$. In particular, the worst-case lower bound proved by Aleksandrs Belovs and Robert Špalek [8] on the difficulty of solving the k-SUM problem on a quantum computer does not extend in any obvious way to a lower bound on average. And without such an average lower bound, our results claimed in Ref. [14] go up in smoke for $k > 2$. Furthermore, for a technical reason explained later, even such an average lower bound would not suffice.

In this paper, we overcome all these problems and give a correct and cryptographically meaningful [3] security proof for all our protocols from Ref. [14]. Consequently, we prove that for any $\varepsilon > 0$ there is a classical protocol that allows the legitimate parties to establish a common key after $O(N)$ expected queries to black-box random functions, yet any quantum eavesdropper will have a vanishing probability of learning their key after $O(N^{1.5-\varepsilon})$ queries to the same oracle. The vanishing probability is over the randomness in the actual run of the protocol followed by that of the eavesdropper's algorithm. If we allow the legitimate parties to use quantum computers as well, their advantage over the quantum eavesdropper becomes arbitrarily close to the quadratic advantage that classical legitimate parties enjoyed over classical eavesdroppers in the seminal 1974 work of Ralph Merkle [24].

Our results require new tools in quantum query complexity, which are of independent interest. In particular, we introduce techniques to lower-bound the quantum query complexity of distinguishing between two probability distributions, which we use to extend the adversary lower bound method in order to handle average-case complexity, but they could have other uses in cryptography. This approach is necessary for the distributions of inputs considered here because the associated decision problems become trivial on average, which prevents us from applying the average-case method developed in Ref. [7]. Furthermore, we prove a composition theorem for this new lower bound method, extending that of Ref. [13], which was valid only to prove cryptographically irrelevant worst-case lower bounds [4]. Using these

[3] To be honest, it is not entirely cryptographically meaningful to restrict the analysis to the number of calls to the black-box functions, taking no account of the computing time that may be required outside those calls. However, if we also restrict the legitimate expected *time* to be in $O(N)$, then our quantum protocol with $k = 3$ remains valid and provably resists any $o(N^{7/4})$-time quantum eavesdropping attack, which was claimed in Ref [14], but with a fundamentally incorrect proof.

[4] Some parts of the proofs are omitted in the present version. They can be found in the extended version of this work [6].

two tools, we prove that any quantum eavesdropper who does not make a prohibitive number of calls to the black-box functions will fail to break a typical instance of the protocol, except with vanishing probability.

This work fits in the general framework of "Cryptography in a quantum world" [12], which addresses the question: "Is the fact that we live in a quantum world a blessing or a curse for codemakers?". It is a blessing if we allow quantum communication, thanks to Quantum Key Establishment (aka Quantum Key Distribution – QKD) [10], at least if the protocols can be implemented faithfully according to theory [29, 22]. On the other hand, it is a curse if we continue to use the current cryptographic infrastructure, which pretends to secure the Internet at the risk of falling prey to upcoming quantum computers. However, it is mostly a draw in the realm of provable query complexity in the black-box model considered in this paper since codemakers enjoy a quadratic (or arbitrarily close to being quadratic) advantage over codebreakers in both an all-classical or an all-quantum world, at least in terms of query complexity (but see footnote 4 again). Furthermore, the known proof that quadratic security is best possible in an all-classical world [4] does not extend to the all-quantum world, and hence the (unlikely) possibility remains that a more secure protocol could exist in our quantum world.

The rest of the paper is organized as follows. Section 2 lists all the techniques and related notations that are used throughout the paper. Section 3 recalls the classical and quantum protocols from Refs [13, 14]. In Section 4, we introduce a new method to prove lower bounds on the difficulty of distinguishing between two probability distributions, which we use to study average-case quantum query complexity. This method extends the extensively studied adversary method. We then apply this method to the k-SUM problem in Section 5, which is at the heart of our hardness result. Finally, in Section 6, we prove a composition theorem for the new adversary method introduced in Section 4. This allows us to conclude that typical runs of the protocols from Refs [13, 14] are indeed secure against quantum adversaries.

2 Preliminaries and Notation

At the heart of this work is a lower bound on the quantum query complexity of a generalisation of the k-SUM problem. Many techniques have been given to prove such lower bounds in the worst-case scenario, including the adversary method [2, 18, 21]. This method is based on the spectral norm of a matrix, Γ, indexed in the rows and columns by inputs to the problem. Roughly, each entry of the matrix $\Gamma[x, y] \in \mathbb{R}$ can be thought of as representing the hardness of distinguishing inputs x and y. It is known that for Boolean functions, the (negative) adversary bound is multiplicative under function composition [18]. For non-Boolean functions, a general composition theorem fails to hold, as counterexamples can be found. Nevertheless, it was shown in Ref. [13] that the adversary method *is* multiplicative under composition with (non-Boolean) unstructured search problems.

In this paper, we extend the quantum adversary method to average-case complexity, which is crucial for cryptographic applications, and we show that a similar composition property holds for this measure. As for the adversary bound, this method is based on the spectral norm of matrices, and involves probability distributions. Below, we summarize the notation related to functions, algebra and probabilities, used throughout the paper.

We consider *decision* or *search* problems denoted F, G or H. These problems are on abelian groups, which are denoted $\mathbb{G}$, or $\mathbb{G}_m$ when we want the order m of the group to appear explicitly. The group operation is denoted "$+$" and its inverse "$-$". For a decision problem F, the inputs in the language F are called *positive* and the inputs not in the language

are *negative*. We compose our problems with an unstructured search problem to make them harder. To do so, we need to add to the alphabet an element that does not belong to $\mathbb{G}$. We denote this element "$\star$".

Fix two problems $\mathsf{F} : A^n \to B$ and $\mathsf{G} : C \to A$ for some $n \in \mathbb{N}$. Then, the composed problem $\mathsf{F} \circ \mathsf{G}^n : C^n \to B$ is defined by $\mathsf{F} \circ \mathsf{G}^n(x_1, \dots x_n) = \mathsf{F}(\mathsf{G}(x_1), \dots, \mathsf{G}(x_n))$ for $(x_1, \dots x_n) \in C^n$.

For any positive integer n we use $[n]$ to denote the set of n elements $\{0, 1, 2, \dots, n-1\}$. We only make use of basic concepts of quantum computing: states, unitary operations and measurements. These notions are used in Section 4, but even there, the calculations boil down to basic linear algebra. The entries of an $n \times m$ matrix Γ are denoted $\Gamma[x, y]$, where $x \in [n]$ and $y \in [m]$. For $X \subseteq [n]$ and $Y \subseteq [m]$, $\Gamma^{X,Y}$ is the restriction of Γ to the rows and columns in X and Y, respectively.

The direct sum of spaces, operators, matrices or vectors is denoted "$\bigoplus$". The inner product of two states (or vectors in an Hilbert space) ψ and ϕ is $\langle \psi, \phi \rangle$. For a matrix A, we use $\|A\|$ for its spectral norm, that is, its largest singular value, and $\|A\|_{\mathrm{F}}$ for the Frobenius norm, that is, the square root of the sum of the squares of the moduli of its elements. For two matrices A and B, we denote $A \circ B$ their entrywise (or Hadamard) product. We make use of the two following matrices: the $n \times n$ identity matrix I_n and the $n \times n$ all-one matrix J_n.

We use $\mathcal{P}$ and $\mathcal{Q}$ for probability distributions over inputs to the problems. The *support* of a distribution is the set of elements with non-zero probability. We sometimes identify distributions with vectors. More precisely, if p_x is the probability of x in $\mathcal{P}$, we can consider the vector $\mathcal{P}$ given by the entries $\mathcal{P}[x] = p_x$. We use "$X \sim \mathcal{P}$" to denote that the random variable X is sampled from $\mathcal{P}$. In this case, it is the variable whose probability is given by $\Pr[X = x] = p_x$. In the specific case of sampling an element x uniformly at random from a set D, we use $x \in_R D$. We also use the indicator function $1_{x \neq y}$ whose value is 1 if $x \neq y$ and 0 otherwise.

We sometimes consider sequences of probabilities, such as the accepting probability ν_n of an algorithm (for a decision problem) as a function of the input size n. For simplicity, we often omit the subscript n, in which case "ν" should be understood as a function of n. We call such a sequence ν *vanishing* if $\nu = o(1)$. If ν decreases faster than the inverse of any polynomial, we say that the event is *negligible*.

3 Provably Secure Key Establishment Protocols

With the exception of Merkle's more famous "puzzles" [25], all key establishment protocols based on black-box random functions (which Merkle called "one-way encryption") begin in a way that is essentially identical to Merkle's original 1974 idea [24], with possible inessential differences [5]. Given a black-box random function $f : D \to R$ from some domain D to some range R, Alice chooses random elements $x_i \in_R D$ and she obtains $y_i = f(x_i)$, which she sends to Bob over an authenticated channel on which Eve can freely eavesdrop. This defines the sets X of x_i's and Y of y_i's, of which X is private information kept by Alice whereas Y becomes known to all parties, including Eve. Upon receiving this information, Bob's first task is to find one or several preimage(s) under f of *any* of the points sent by Alice.

The various schemes that were considered in Refs [24, 15, 13, 14] differ in how Bob

[5] In Merkle's original scheme, there is no asymmetry between Alice and Bob, as they both "guess at keywords" and share and compare their one-way encryptions until they discover that they have guessed at the same keyword. In all the protocols considered here, Alice goes first and Bob works from there.

proceeds to find the preimage(s), how many such preimages he needs to find, and how he informs Alice of which preimage(s) he has found. In Merkle's original scheme [24], he needs to find a single preimage. This is done by querying f on random points in its domain until some x is found such that $f(x) = y \in Y$. Afterwards, Bob sends y back to Alice, who can find efficiently the corresponding x because it is among her set X, which she had kept. This shared x becomes their secret key. The intuition behind the security of this scheme stems from the freedom in Bob's task to invert f on any element of Y, compared to how stringent Eve's is since she must invert it on the specific element that Bob had inverted by chance.

To be more precise, let N be a safety parameter, let the domain of f contain N^2 points and its range be of size N^5, which is large enough to ensure that f is one-to-one except with vanishing probability. If Alice chooses N random points in the domain of f and Bob tries random such points as well until he hits upon an x such that $f(x) \in Y$, it is easy to see that both Alice and Bob need query function f an expected number of N times. However, a classical Eve requires an expected $N^2/2$ queries, which gives a quadratic advantage to the legitimate parties.

Unfortunately, inverting one specific point in the image of f with the help of a quantum computer requires only $\frac{\pi}{4}\sqrt{N^2} = \frac{\pi}{4}N$ queries to f by way of Grover's algorithm [17], which is slightly *fewer* than the effort required by the legitimate parties. This is why Merkle's original scheme is totally broken against a quantum adversary, as first pointed out in Ref. [15]. In order to restore security, two main modifications to Merkle's original scheme have been considered, as we now proceed to describe.

3.1 Variations on Merkle's Idea

If we require Bob to find k distinct preimages among the N points sent by Alice, for some $k > 1$, rather than a single one, he will only have to work roughly k times as hard, provided $k \ll N$. The key shared by Alice and Bob could then be the concatenation of those preimages in the order in which the corresponding images were sent by Alice in the first step. But how can Bob tell Alice which preimages he was able to find in a way that will force Eve to make much more queries than her? A first solution was proposed in Ref. [13] for the case $k = 2$, but a much simpler one was given subsequently in Ref. [14] for arbitrary k. The idea is to introduce a second black-box random function t from the same domain to some sufficiently large group $\mathbb{G}$. If Bob finds preimages $x_{i_1}, x_{i_2}, \ldots, x_{i_k} \in X$, with $1 \leq i_1 < i_2 < \cdots < i_k \leq N$, and sends $w = t(x_{i_1}) + t(x_{i_2}) + \cdots t(x_{i_k})$ to Alice, she needs only call black-box function t on the N points she had kept in X in order to determine Bob's k preimages, provided the order of $\mathbb{G}$ was chosen sufficiently large to ensure the uniqueness of the solution, except with vanishing probability. Taking the order to be N^{4k+1} is sufficient to ensure this. Furthermore, she can do this efficiently, in terms of computing time, when $k = 2$. Hence, Alice needs to query each of functions f and t exactly N times, whereas Bob needs to query function f an expected $O(kN)$ times and function t exactly k times.

How difficult is the cryptanalytic task for quantum Eve, who has seen the y's sent from Alice to Bob and the single w sent from Bob to Alice? We gave an explicit algorithm based on quantum walks [23] in Hamming graphs in Ref. [14], which allows her to discover the secret key after $O(N^{1/2+k/(k+1)})$ calls to the black-box functions. In the same paper, we claimed that a matching $\Omega(N^{1/2+k/(k+1)})$ lower bound holds for a typical instance of the protocol, which is formally stated in Theorem 8 below, but the proof proposed in Ref. [14] fails for $k > 2$ in a way that cannot be repaired. The main purpose of the present paper is to offer a correct proof of this theorem. It follows that for any fixed $\varepsilon > 0$, there is a *classical* key establishment protocol (taking $k = \lfloor 1/\varepsilon \rfloor$) that allows the legitimate parties to establish

a shared key after $O(N)$ expected queries to black-box random functions f and t, yet any *quantum* eavesdropper will have a vanishing probability of learning their key after $O(N^{1.5-\varepsilon})$ queries to the same oracle. If we take account of computational complexity in addition to query complexity, we must be content with $k = 2$, in which case the claim is much more modest, but still the quantum codebreaker must work more than linearly harder than the classical codemakers. Along the way, we need to develop in Section 4 new tools for the study of *average-case* quantum query complexity, which had essentially remained virgin territory despite its obvious importance, in particular but not only for cryptography.

The second modifications to Merkle's original scheme that has been considered [15, 13, 14] is to play a fair game in allowing the codemakers to use quantum computers as well. The first benefit is that we can enlarge the domain of f to contain N^3 points. If Alice proceeds exactly as before, Bob can use an extension of Grover's algorithm known as BBHT [11] in order to find random preimages of the N image points initially sent by Alice at the cost of $O(\sqrt{N^3/N}\,) = O(N)$ queries per preimage, provided $k \ll N$. This increase in the domain size of f, and correspondingly of t, makes it significantly harder for a quantum eavesdropper to solve the conundrum and discover the key shared by Alice and Bob. Indeed, we also prove Theorem 9, stated below, to the effect that no cryptanalytic attack can succeed on a typical instance of the protocol, except with vanishing probability, short of making $\Omega(N^{1+k/(k+1)})$ queries to the black-box functions. Again, this theorem was claimed in Ref. [14] but its proof was fundamentally flawed for $k > 2$. Taking k sufficiently large, this offers a quantum-against-quantum security that is arbitrarily close to the quadratic security that the original scheme of Merkle [24] offered in the classical-against-classical scenario. The second benefit to allowing the codemakers to use quantum computers is that now a quantum Alice can be efficient in terms of computation time, in addition to query complexity, even when $k = 3$. According to Theorem 9, we get an $\Omega(N^{7/4})$ security guarantee for a protocol that could become practical once sufficiently powerful quantum computers start to seriously threaten the security of the current Internet cryptographic infrastructure. This is the most secure *proven* solution ever discovered to the conundrum of post-quantum cryptography [12] when all parties have equal quantum computing capabilities, at least in the random oracle model, and its security is reasonably close to that of Merkle's provably optimal scheme in an all-classical world but otherwise in the same model.

3.2 The k-SUM Problem

The security of the protocols that we study is based on the k-SUM problem, which consists in searching for k elements among N in some abelian group $\mathbb{G}$ whose sum is a given value $w \in \mathbb{G}$.

▶ **Definition 1** (k-SUM problem)**.** Given an abelian group $\mathbb{G}$, a function $t : D \to \mathbb{G}$ for some domain D, a *target* $w \in \mathbb{G}$ and N distinct elements $x_1, x_2, \ldots, x_N \in D$, the problem is to find k indices $1 \le i_1 < i_2 < \cdots < i_k \le N$ such that $w = \sum_{j\in 1}^{k} t(x_{i_j})$, provided a solution exists. The *decision* version of k-SUM is to decide whether or not a solution exists.

It is crucial to understand that we are not interested in how much computation *time* would be required to find a solution, if one exists. Rather, we want to minimize the *number of calls* to function t that will be required. Naturally, a quantum algorithm is allowed to query t on superpositions of elements of D.

When $k = 1$, this is simply the *unstructured search problem*, which consists in finding i such that $t(x_i) = w$, provided it exists. When $k = 2$ and $\mathbb{G}$ is the group of bit strings of a given length under bitwise exclusive-or, k-SUM takes the name of 2-XOR. In turn, when

$w = 0$, 2-XOR becomes the search version of the Element Distinctness (ED) problem, which consists in finding a collision in a given function if it is not one-to-one.

▶ **Definition 2** (Element Distinctness (ED) problem)**.** Given a function $t : D \to R$, the *decision* element distinctness (ED) problem is to decide whether or not this function is one-to-one.

▶ **Definition 3** (Search version of ED)**.** Given a function $t : D \to R$, the *search* version of the element distinctness problem (SED) is to find a pair of distinct $x, x' \in D$ such that $t(x) = t(x')$, provided such a pair exists.

Quantum lower bounds have been proved on all these problems [1, 8, etc.], but only in the worst-case scenario, which is most frequently studied in the field of computational and query complexity. For some of these problems, such as ED, SED, 2-XOR and 2-SUM, a simple *classical* randomized reduction suffices for proving their difficulty on average from their difficulty in the worst case even in the quantum setting, at least if we add the promise that if there is a solution, then it is unique. However, this does not appear to be the case for k-SUM when $k > 2$. Our main mistake in Ref. [14] was to take such a reduction for granted for arbitrary k after having nearly proved it in the case $k = 2$. "Nearly" because the proof for $k = 2$ was flawed, albeit easy to repair. Not so for $k > 2$, however. In order to prove the security of the key establishment protocols described above in a cryptographically meaningful context, we need to prove the difficulty of k-SUM on average for arbitrary k, which requires new quantum lower bound techniques. In fact, we need to prove the difficulty on average of a *composed* version of k-SUM, defined below in Section 3.3, which does not follow by a classical reasoning from the average difficulty of plain k-SUM. Therefore, we also have to develop a new composition theorem that works on average as well.

The first quantum lower bound discovered among these problems was for the decision element distinctness problem. Aaronson and Shi [1] proved that this problem requires $\Omega(d^{2/3})$ queries to t in the worst case, where d is the cardinality of domain D. There was a technical condition in their original proof that required $r \geq d^2$, where r is the cardinality of range R, but that condition was subsequently lifted [3, 20]. Later, Belovs and Špalek [8] proved that solving k-SUM requires $\Omega(N^{k/(k+1)})$ queries to t in the worst case, provided $m \geq N^k$, where m is the order of group $\mathbb{G}$ and N is as in Definition 1.

Even though the technique used by Aaronson and Shi was adequate only to prove worst-case lower bounds, it is elementary to conclude by a classical reasoning that the hardness in worst-case of ED implies the same hardness on average for ED, SED and 2-XOR. But, as we said already, a completely new technique, which we develop in Section 4, is required to prove a matching hardness result for k-SUM on average, which is stated as Theorem 15 in Section 5.

However, even this is not sufficient to derive the security of the key establishment protocols described above in a cryptographically meaningful manner. Indeed, the eavesdropper is not faced with an instance of k-SUM, as specified in Definition 1. He learns the value of w when Bob transmits it to Alice, and he has access to black-box function t, but he does not know the x's, which are kept secret by Alice. Instead, he learns the image of those x's by function f, which we called the y's, when Alice sent them to Bob in the first step of the protocol. In fact, he has to solve the more difficult *Hidden* k-SUM problem, which we now proceed to describe.

3.3 Hidden and Composed k-SUM Problems

The hidden k-SUM problem, defined below, corresponds precisely to the task facing the eavesdropper.

▶ **Definition 4** (Hidden k-SUM problem)**.** Given two sets D and R, an abelian group $\mathbb{G}$, two functions $f : D \to R$ and $t : D \to \mathbb{G}$, N distinct elements $y_1, y_2, \ldots, y_N \in \mathsf{Im}(f)$, and a *target* $w \in \mathbb{G}$, the problem is to find k indices $1 \leq i_1 < i_2 < \cdots < i_k \leq N$ and a preimage x_{i_j} under f for each y_{i_j}, $1 \leq j \leq k$, meaning that $f(x_{i_j}) = y_{i_j}$, such that $w = \sum_{j=1}^{k} t(x_{i_j})$, provided a solution exists. The *decision* version of hidden k-SUM is to decide if a solution exists.

In order to prove lower bounds on the quantum cryptanalytic task of breaking typical instances of the protocols described in Section 3.1, we proceed in two steps. First we have to prove the hardness of the hidden k-SUM problem on average. Then, we have to exhibit a reduction that shows how to solve an average instance of the hidden k-SUM problem using an adversary who thinks he is breaking a typical instance of the key establishment protocol. To prove the hardness of the hidden k-SUM problem on average, it helps to consider a more structured version of it, which is given by the composition of k-SUM with a search problem called pSEARCH, defined below.

▶ **Definition 5** (pSEARCH problem)**.** Let A be some set and $\star$ a symbol not in A. Consider the set P of strings $(a_1, \ldots, a_\ell)$ in $(A \cup \{\star\})^\ell$ with the promise that exactly one value is not $\star$. The problem $\mathsf{pSEARCH}_\ell : P \to A$ consists in finding this non-$\star$ value by making queries that take i as input and return a_i, $1 \leq i \leq \ell$.

An equivalent formulation of the k-SUM problem would consist in a target w in abelian group $\mathbb{G}$ and a list $(t_1, t_2, \ldots, t_N)$ of elements of $\mathbb{G}$. The problem is to find k indices $1 \leq i_1 < i_2 < \cdots < i_k \leq N$ such that $w = t_{i_1} + t_{i_2} + \cdots + t_{i_k}$. We are charged for accessing each t_i given i. This is equivalent to Definition 1 simply by taking $t_i = t(x_i)$, but it is more convenient since it allows us to consider the composition of k-SUM with N instances of pSEARCH. Thus we define the *Composed* version of k-SUM as follows.

▶ **Definition 6** (Composed k-SUM problem)**.** Given a target w in abelian group $\mathbb{G}$ and N instances of the $\mathsf{pSEARCH}_\ell$ problem using $\mathbb{G}$ as set A, we want to solve the k-SUM problem with t_i being the only non-$\star$ element in the ith instance of $\mathsf{pSEARCH}_\ell$. Said otherwise, this is the composition of k-SUM and $\mathsf{pSEARCH}_\ell$ denoted $k\text{-}\mathsf{SUM} \circ \mathsf{pSEARCH}_\ell^N$.

The composed k-SUM problem (Definition 6) is similar to its hidden variant (Definition 4), except that it is more structured, hence easier. Specifically, the x_i's that serve to define $t_i = t(x_i)$ in the hidden version, $1 \leq i \leq N$, can be *a priori* any element of D, whereas they are put in N "buckets" of size ℓ in the composed version. If we choose the size of D to be the product of N and ℓ, any algorithm capable of solving the hidden version can serve directly to solve the composed version simply by taking no account of the additional information provided by the buckets. Moreover, a random instance of the composed version can be transformed into a random instance of the hidden version, essentially by mixing the buckets. It follows that any lower bound on the composed problem translates directly into the same lower bound on the hidden problem, *mutatis mutandis*.

In Sections 4 to 6, which are more technical, we give a lower bound on the composed problem in a series of steps. First, we give a new general method to prove lower bounds for the average-case quantum query complexity (Section 4). This method is closely related to the technique given in Ref. [9], albeit with essential differences. Second, building on techniques from Refs [8, 7], we show a lower bound on the average-case quantum query complexity of k-SUM (Section 5). Third, we show a composition theorem for average-case quantum query complexity, which allows us to conclude with Theorem 18 (Section 6).

When we apply this theorem with the parameters that correspond to the protocols described in Section 3.1, we should take $n = N$, which is the number of images sent by

Alice in the first step of any of these protocols and therefore also the number of buckets. Furthermore, we should take the product of ℓ, the size of the buckets, with n, the number of buckets, to correspond to the size of the domain D used in the protocols.

Putting it all together, Theorem 18 gives us the following lower bound on the difficulty to solve the hidden k-SUM problem if the domain D of functions f and t contains d elements.

▶ **Theorem 7.** *Any quantum algorithm that uses at most T queries to find a solution to the hidden k-SUM problem with success probability at least $\nu_N > 0$ on average over the uniform distribution on positive instances requires*

$$\frac{T}{\nu_N} = \Omega\Big(\sqrt{d/N - 1}\; N^{k/(k+1)}\Big)$$

provided $m = \omega\Big(N^{k+\frac{2}{k+1}}\Big)$, where m is the order of the underlying abelian group.

3.4 The Security of Key Establishment

We proved (correctly!) in Ref. [14] that any eavesdropper who succeeds in obtaining the key with non-vanishing success probability ν in any of the protocols described in Section 3.1, after making no more than T queries, on average over the runs of the protocol, can be used to solve the hidden k-SUM problem with the same parameters. Therefore, using the fact that $d = N^2$ for the classical protocols and $d = N^3$ for the quantum protocol, we can apply Theorem 7 to conclude that the protocols are secure according to the following theorems.

▶ **Theorem 8.** *Any quantum eavesdropping strategy that makes $o\big(N^{\frac{1}{2}+\frac{k}{k+1}}\big)$ queries to the black-box functions against a typical run of the classical protocol using parameter k will fail to recover the key, except with vanishing probability.*

▶ **Theorem 9.** *Any quantum eavesdropping strategy that makes $o\big(N^{1+\frac{k}{k+1}}\big)$ queries to the black-box functions against a typical run of the quantum protocol using parameter k will fail to recover the key, except with vanishing probability.*

Furthermore, we showed in Ref. [14] that these bounds are tight.

4 Average-Case Quantum Adversary Lower Bound Method

We generalize the adversary lower bound method to handle average-case complexity. A similar bound from Ref. [9] already gives a lower bound technique on average-case query complexity, but it cannot be applied directly here, as we explain below.

We use the following complexity measure, closely related to the adversary bound [2, 18]. We give a formulation tailored to the following problem. Given two distributions $\mathcal{P}$ and $\mathcal{Q}$, and an algorithm that attempts to distinguish between them, we consider the number of queries this algorithm must make in order to succeed. The algorithm is given one input, and accepts if it thinks the sample it is given comes from $\mathcal{P}$ and rejects otherwise. The measure of success is given by the probabilities $s_{\mathcal{P}}$ and $s_{\mathcal{Q}}$, which are the probability of accepting when the algorithm is given samples from $\mathcal{P}$ and $\mathcal{Q}$, respectively.

▶ **Definition 10.** Let $\mathcal{P}$ and $\mathcal{Q}$ be two probability distributions on $\mathcal{D}$, and p_x and q_y denote probabilities of x and y in $\mathcal{P}$ and $\mathcal{Q}$, respectively. Let $s_{\mathcal{P}}, s_{\mathcal{Q}}$ be real numbers in $[0,1]$ (representing the acceptance probability on distributions $\mathcal{P}$ and $\mathcal{Q}$, respectively). For a given matrix Γ, define the adversary bound with respect to $\Gamma, \mathcal{P}, s_{\mathcal{P}}, \mathcal{Q}, s_{\mathcal{Q}}$ as

$$\overline{\mathsf{Adv}}(\Gamma; \mathcal{P}, s_{\mathcal{P}}; \mathcal{Q}, s_{\mathcal{Q}}) = \Omega\left(\min_{j\in[n]} \frac{\delta_{\mathcal{P}}^* \Gamma \delta_{\mathcal{Q}} - \tau(s_{\mathcal{P}}, s_{\mathcal{Q}})\|\Gamma\|}{\|\Gamma \circ \Delta_j\|}\right). \tag{1}$$

Here, $\circ$ denotes entrywise (or Hadamard) product, and $\|A\|$ denotes the spectral norm of A (which is equal to its largest singular value). The vectors $\delta_{\mathcal{P}}[x] = \sqrt{p_x}$ and $\delta_{\mathcal{Q}}[y] = \sqrt{q_y}$ are unit vectors in $\mathbb{R}^{\mathcal{D}}$; for $j \in [n]$, the $|\mathcal{D}| \times |\mathcal{D}|$ matrix Δ_j is defined by $\Delta_j[x, y] = 1_{x_j \neq y_j}$; and

$$\tau(s_{\mathcal{P}}, s_{\mathcal{Q}}) = \sqrt{s_{\mathcal{P}} s_{\mathcal{Q}}} + \sqrt{(1 - s_{\mathcal{P}})(1 - s_{\mathcal{Q}})}. \tag{2}$$

▶ **Theorem 11.** *Assume $\mathcal{A}$ is a quantum algorithm that makes T queries to the input string $x = (x_1, \ldots, x_n) \in \mathcal{D}$, and then either accepts or rejects. Let $\mathcal{P}$ and $\mathcal{Q}$ be two probability distributions on $\mathcal{D}$. Let $s_{\mathcal{P}}$ and $s_{\mathcal{Q}}$ be acceptance probability of $\mathcal{A}$ when x is sampled from $\mathcal{P}$ and $\mathcal{Q}$, respectively. Then,*

$$T \geq \overline{\mathsf{Adv}}(\Gamma; \mathcal{P}, s_{\mathcal{P}}; \mathcal{Q}, s_{\mathcal{Q}}),$$

for any $|\mathcal{D}| \times |\mathcal{D}|$ matrix Γ.

If $\mathcal{P}$ and $\mathcal{Q}$ have partial supports, then we may use a matrix Γ whose rows are indexed by elements in the support of $\mathcal{P}$ and columns by elements of the support of $\mathcal{Q}$. In that case we can extend the matrix Γ by adding all-0 rows and columns. Notice that this does not alter the value of $\overline{\mathsf{Adv}}$.

First let us consider why we need two distributions $\mathcal{P}, \mathcal{Q}$ on the inputs (and why we cannot use existing techniques such as Theorem 33 from Ref. [9] for decision problems, where $\mathcal{P} = \mathcal{Q}$). The distribution we care about is the uniform distribution over the positive instances. Under this distribution, the decision problem is of course trivial. Using this distribution as both $\mathcal{P}$ and $\mathcal{Q}$ as in Ref. [9] would give a trivial bound.

Instead, Theorem 11 gives a lower bound on the query complexity of an algorithm that attempts to distinguish between two distributions $\mathcal{P}$ and $\mathcal{Q}$. Taking $\mathcal{P}$ as the uniform distribution over positive instances, and $\mathcal{Q}$ as the uniform distribution over all instances implies a lower bound for the *search* problem of finding k elements that sum to w with the promise that the instance is positive, by the following argument. Assume an algorithm solves the search problem with T queries with non-vanishing probability. Then we can transform this algorithm into a distinguishing algorithm with one-sided error: if the algorithm outputs a candidate solution $a_1, \ldots, a_k$, make k additional queries and check that they sum to w. If they do, accept, else reject. Then the acceptance probability on negative instances is 0. Since most instances are negative, the acceptance probability on the uniform distribution is close to 0. We are interested in the acceptance probability on the positive instances, as a function of the number of queries T.

We now proceed to the proof of Theorem 11. Our proof is closely related the proof of the worst-case negative-weighted adversary bound from Ref. [18]. We follow a slightly simplified version of the proof from Ref. [5]. As usual, we introduce a progress function, show that initially, the progress function is large (Claim 12), at the end, it is small (Claim 13), and that at each step, the decrease is bounded (Claim 14).

Proof of Theorem 11. Recall that a quantum query algorithm is given by the following sequence of operations

$$U_0 \to O_x \to U_1 \to O_x \to U_2 \to \cdots \to U_{T-1} \to O_x \to U_T,$$

where O_x denotes the input oracle, and the U_is are arbitrary unitary transformations. The operator O_x is defined by $O_x|a\rangle|i\rangle = |a + x_i\rangle|i\rangle$ which can be decomposed as

$$O_x = \bigoplus_{j=0}^{n} O_{x_j}, \tag{3}$$

where for $b \in \mathbb{G}_m$, $O_b \colon |a\rangle|i\rangle \mapsto |a+b\rangle|i\rangle$. The addition in the first register is the group operation of $\mathbb{G}_m$.

For an integer t between 0 and T, and $x \in \mathcal{D}$, let

$$\psi_x^{(t)} = U_t O_x U_{t-1} O_x \cdots U_1 O_x U_0 |0\rangle. \tag{4}$$

be the state of the algorithm on the input x after t queries. We define the quantity called the *progress function* as follows

$$W^{(t)} = \sum_{x,y \in \mathcal{D}} \sqrt{p_x q_y}\, \Gamma[x,y] \langle \psi_x^{(t)}, \psi_y^{(t)} \rangle. \tag{5}$$

The proof is split into three parts: proving that $W^{(0)}$ is large, and that both $W^{(T)}$ and $W^{(t)} - W^{(t+1)}$ are small. The proofs of the claims appear in the extended version of the paper [6].

▶ **Claim 12.** $W^{(0)} = \delta_{\mathcal{P}}^* \Gamma \delta_{\mathcal{Q}}$.

▶ **Claim 13.** $W^{(T)} \le \left(\sqrt{s_{\mathcal{P}} s_{\mathcal{Q}}} + \sqrt{(1-s_{\mathcal{P}})(1-s_{\mathcal{Q}})} \right) \|\Gamma\|$.

▶ **Claim 14.** $|W^{(t)} - W^{(t+1)}| \le 2 \max_{j \in [n]} \|\Gamma \circ \Delta_j\|$. ◀

5 Average-Case Complexity of k-SUM

Recall the k-SUM problem on n elements in an abelian group $\mathbb{G}_m$ where m is the order of the group. Let w be a fixed element of $\mathbb{G}_m$. An input $x = (x_1, \ldots, x_n)$ is called *positive* if there exists a k-subset $V = \{t_1, \ldots, t_k\} \subseteq [n]$ such that $x_{t_1} + \cdots + x_{t_k} = w$ in $\mathbb{G}_m$. Otherwise, the input is called *negative*.

Consider the following probability distribution $\mathcal{P}$ on positive inputs:

- Select a k-subset U of $[n]$ uniformly at random;
- assign to U a uniformly random string in $\mathbb{G}_m^{|U|}$ whose sum is w;
- choose the remaining elements uniformly at random.

▶ **Theorem 15.** *Assume $\mathcal{S}$ is a quantum algorithm for the search problem k-SUM that makes T queries and succeeds with probability $\nu > 0$ over inputs sampled from the distribution $\mathcal{P}$.*

Then,

$$\frac{T}{\nu} = \Omega\left(n^{k/(k+1)}\right),$$

provided that $\nu = \omega\left(n^{-1/(k+1)}\right)$ and $m = \Omega\left(n^{k+\frac{2}{k+1}}\right)$ is again the order of the underlying abelian group.

This theorem uses the following claim, whose proof appears in the extended version of the paper [6].

▶ **Claim 16.** *Let the distribution $\mathcal{P}$ be as above, and $\mathcal{Q}$ be the uniform distribution on all the inputs. There exists a matrix Γ satisfying the following constraints:*

$$\delta_{\mathcal{P}}^* \Gamma \delta_{\mathcal{Q}} = n^{k/(k+1)}, \qquad \|\Gamma\| \le \left(1 + O\left(n^{-1/(k+1)}\right)\right) n^{k/(k+1)}, \quad \text{and} \qquad \|\Gamma \circ \Delta_j\| = O(1)$$

in the notation of Theorem 11.

Proof of Theorem 15. Let $\mathcal{S}$ be the algorithm of Theorem 15. We apply Theorem 11 to the algorithm $\mathcal{A}$ defined as follows, using the constraints from Claim 16 to evaluate $\overline{\mathsf{Adv}}$. First, $\mathcal{A}$ executes $\mathcal{S}$ on its input. Let $\{t_1, \ldots, t_k\}$ be the output of $\mathcal{S}$. The algorithm $\mathcal{A}$ then queries the elements $x_{t_1}, \ldots, x_{t_k}$. It accepts if $x_{t_1} + \cdots + x_{t_k} = w$, and rejects otherwise.

The query complexity of $\mathcal{A}$ is $T+k = T+O(1)$. The acceptance probability on distribution $\mathcal{P}$ is $s_{\mathcal{P}} = \nu$. Also, since $\mathcal{A}$ always rejects a negative input,

$$s_{\mathcal{Q}} \leq \Pr_{x\sim\mathcal{Q}}\big[\text{the input } x \text{ is positive}\big] \leq \frac{1}{m}\binom{n}{k},$$

the last inequality following from the union bound. Thus, we have the following estimate on $\tau(s_{\mathcal{P}}, s_{\mathcal{Q}})$:

$$\tau(s_{\mathcal{P}}, s_{\mathcal{Q}}) = \sqrt{s_{\mathcal{P}} s_{\mathcal{Q}}} + \sqrt{(1-s_{\mathcal{P}})(1-s_{\mathcal{Q}})} \leq \sqrt{\frac{1}{m}\binom{n}{k}} + 1 - \frac{\nu}{2},$$

and using the conditions on m and ν, we obtain:

$$\begin{aligned}\frac{\delta_{\mathcal{P}}^{*}\Gamma\delta_{\mathcal{Q}} - \tau(s_{\mathcal{P}}, s_{\mathcal{Q}})\|\Gamma\|}{\|\Gamma\circ\Delta_j\|} &= \frac{n^{k/(k+1)} - \big(1-\Omega(\nu)\big)\Big(1+O\big(n^{-1/(k+1)}\big)\Big)n^{k/(k+1)}}{O(1)} \\ &= \Omega\Big(\nu n^{k/(k+1)}\Big).\end{aligned}$$

◀

6 Composition Theorem for the Average-Case Adversary Bound

We now prove the last remaining theorem needed to obtain the lower bound on the average case complexity of k-$\mathsf{SUM}\circ\mathsf{pSEARCH}_\ell^n$ (see Section 3.3). Recall that in this version, each input variable $x_i \in \mathbb{G}_m$ is embedded into a "bucket", that is, a sequence $(x_{i1}, \ldots, x_{i\ell}) \in (\mathbb{G}_m \cup \{\star\})^\ell$ in which exactly one element is non-$\star$. To apply our average-case adversary lower bound method, we need to define the probability distributions and the matrix that appears in Eq. 1 for the composed problem. Intuitively, this is done by tensoring the matrix of the two problems that are composed, as well as the vectors that represent the probability distributions. However, defining the matrix correctly to get a lower bound for the composed problem requires a careful analysis.

We use the distributions $\mathcal{P}_{\mathsf{F}}$ and $\mathcal{Q}_{\mathsf{F}}$ to pick inputs to the outer function F, and the uniform distribution to place each element of the input independently in its bucket. Formally, we write $\mathcal{P} = \mathcal{P}_{\mathsf{F}} \otimes U_\ell^{\otimes n}$, where U_ℓ is the uniform distribution over $[\ell]$ and the distributions are viewed as real-valued vectors indexed by elements of their supports. The definition of $\mathcal{Q}$ is similar, starting from $\mathcal{Q}_{\mathsf{F}}$.

▶ **Lemma 17.** *Let $\mathsf{F} : A^n \to B$, $\mathsf{pSEARCH}_\ell : P \to A$ where $P \subseteq (A \cup \{\star\})^\ell$ is the set of all possible buckets, $\mathsf{H} = \mathsf{F}\circ\mathsf{pSEARCH}_\ell^n$, and $\mathcal{P}_{\mathsf{F}}$, $\mathcal{Q}_{\mathsf{F}}$, $\mathcal{P}$ and $\mathcal{Q}$ defined as above. Then for any real numbers $s_{\mathcal{P}}$, $s_{\mathcal{Q}} \in [0,1]$ and matrix Γ_{F}, there exists a matrix Γ_{H} such that*

$$\overline{\mathsf{Adv}}(\Gamma_{\mathsf{H}}; \mathcal{P}, s_{\mathcal{P}}; \mathcal{Q}, s_{\mathcal{Q}}) \geq \overline{\mathsf{Adv}}(\Gamma_{\mathsf{F}}; \mathcal{P}_{\mathsf{F}}, s_{\mathcal{P}}; \mathcal{Q}_{\mathsf{F}}, s_{\mathcal{Q}})\sqrt{\ell-1}\,.$$

▶ **Theorem 18.** *Any algorithm that finds a solution to the search version of k-$\mathsf{SUM}\circ\mathsf{pSEARCH}_\ell^n$ within T queries with probability $\nu > 0$ on average over the uniform distribution on positive instances requires*

$$\frac{T}{\nu} = \Omega\Big(\sqrt{\ell-1}\; n^{k/(k+1)}\Big)$$

provided $m = \omega\Big(n^{k+\frac{2}{k+1}}\Big)$.

The rest of this section is devoted to the proof of Theorem 18. It follows closely the proof of the composition theorem in Ref. [13], and in particular the adversary matrix for H we use here has the same structure as the matrices considered in that paper. This allows us to re-use some of the calculations from that paper (see Claims 20 and 21).

We use the following notation. Let $\mathsf{X}, \mathsf{Y} \in A^n$ denote inputs to F. Its components are $\mathsf{X}_i \in A$. The value $\Gamma_{\mathsf{F}}[\mathsf{X}, \mathsf{Y}]$ is a scalar. Notice that for the k-SUM problem, the rows of the matrix defined in the previous section are only defined for positive inputs. In order to reuse the norm calculations from the composition theorem in Ref. [13], we need to extend it to all possible inputs. We do so by extending the matrix for k-SUM with rows of zeros. This transformation does not change the norm of the matrix. Similarly, the vector $s_{\mathcal{P}_{\mathsf{F}}}$ can be extended with zeros to be defined for any input.

Proof of Lemma 17. The adversary matrix for the composed problem H is denoted Γ_{H}. We consider blocks of Γ_{H} indexed by values X, Y, which we denote $\Gamma_{\mathsf{H}}^{\mathsf{X},\mathsf{Y}}$. (These $\ell^n \times \ell^n$ blocks are a submatrix corresponding to all the inputs for which the input to F is X, in the rows, and Y, in the columns.) As in Ref. [13], we define Γ_{H} by blocks as follows:

$$\Gamma_{\mathsf{H}}^{\mathsf{X},Y} = \Gamma_F[\mathsf{X}, \mathsf{Y}] \cdot \bigotimes_{i \in [n]} \overline{\Gamma}^{\mathsf{X}_i, \mathsf{Y}_i},$$

where for $a, b \in A$,

$$\overline{\Gamma}^{a,b} = \begin{cases} \|\mathsf{J}_\ell - \mathrm{I}_\ell\| \cdot \mathrm{I}_\ell & \text{if } a = b \\ \mathsf{J}_\ell - \mathrm{I}_\ell & \text{otherwise.} \end{cases}$$

An optimal adversary matrix for $\mathsf{pSEARCH}$ can be obtained by taking $\mathsf{J}_\ell - \mathrm{I}_\ell$ for all blocks except the diagonal ones that are all zeroes. But if we were using it, a block $\Gamma_{\mathsf{H}}^{X,Y}$ would be zero whenever there is an i such that $X_i = Y_i$. Using the matrix $\overline{\Gamma}$, with modified diagonal blocks, overcomes this issue.

From the distributions $\mathcal{P}_F$ and $\mathcal{Q}_F$, we define the vector $\delta_{\mathcal{P}_F} = \sqrt{\mathcal{P}_F}$, that is, $\delta_{\mathcal{P}_{\mathsf{F}}}[\mathsf{X}] = \sqrt{\Pr_{\mathsf{X} \sim \mathcal{P}_F}[\mathsf{X}]}$ (similarly for $\delta_{\mathcal{Q}_{\mathsf{F}}}$). Again, we can split $\delta_{\mathcal{P}_{\mathsf{F}}}$ into blocks $\delta_{\mathcal{P}_{\mathsf{F}}}^{\mathsf{X}}$.

With these definitions in hand, we can compute the terms that appear in Eq. 1 of Definition 10. This is done in Claims 19, 20, and 21. When referring to Ref. [13], we use $S_i = \mathsf{J}_\ell - \mathrm{I}\ell$ for all i $(1 \le i \le n)$.

▶ **Claim 19.** $\delta_{\mathcal{P}}^\dagger \Gamma_{\mathsf{H}} \delta_{\mathcal{Q}} = \delta_{\mathcal{P}_{\mathsf{F}}}^\dagger \Gamma_F \delta_{\mathcal{Q}_F} \cdot \|\mathsf{J}_\ell - \mathrm{I}_\ell\|^n$.

▶ **Claim 20.** *[13, claim on last line of page 409]* $\|\Gamma_{\mathsf{H}}\| = \|\Gamma_{\mathsf{F}}\| \cdot \|\mathsf{J}_\ell - \mathrm{I}_\ell\|^n$.

▶ **Claim 21.** *[13, claim near the end of page 410] For a query i that corresponds to index q in the bucket p,* $\|\Gamma_{\mathsf{H}} \circ \Delta_i\| = \|\Gamma_{\mathsf{F}} \circ \Delta_p\| \cdot \|\mathsf{J}_\ell - \mathrm{I}_\ell\|^{n-1} \cdot \|(\mathsf{J}_\ell - \mathrm{I}_\ell) \circ \Delta_q\|$.

Claims 20 and 21 were proven in the arXiv extended version of Ref. [13]. Although the claims in the original Crypto version of Ref. [13] consider specifically the Element Distinctness problem, the paper mentions that an explicit description of the adversary matrix is not needed (such a description was indeed unknown when this proof was given). For this reason, these two claims apply to any outer function F, and in particular to k-SUM. Note that the arXiv extended version of Ref. [13] contains the proofs for arbitrary outer functions. The proof of Claim 19 appears in the extended version of the paper [6].

Using the fact that $\|\mathsf{J}_\ell - \mathrm{I}_\ell\| = \ell - 1$ and $\|(\mathsf{J}_\ell - \mathrm{I}_\ell) \circ \Delta_q\| = \sqrt{\ell - 1}$ for any q, we immediately get Lemma 17 by substituting the values obtained in Claims 19, 20 and 21 into Definition 10. ◀

Proof of Theorem 18. Using the values computed in Section 5 we get

$$\begin{aligned} T &= \Omega\left(\frac{\delta^{\dagger}_{\mathcal{P}_{\mathsf{F}}}\Gamma_{\mathsf{F}}\delta_{\mathcal{P}_{\mathsf{F}}} - \tau(s_{\mathcal{P}}, s_{\mathcal{Q}})\|\Gamma_{\mathsf{F}}\|}{\|\Gamma_{\mathsf{F}} \circ \Delta_i\|}\sqrt{\ell-1}\right) \\ &= \Omega\left(n^{k/(k+1)}\sqrt{\ell-1}\left(\frac{\nu}{2} - \sqrt{\frac{1}{m}\binom{n}{k}}\right)\right) \end{aligned}$$

Suppose that ν is non-vanishing. Since m is chosen large enough to make $\frac{1}{m}\binom{n}{k}$ arbitrarily small, we get

$$\frac{T}{\nu} = \Omega\Big(\sqrt{l-1}n^{k/(k+1)}\Big).$$ ◀

Acknowledgements. We are grateful to Kassem Kalach, with whom this work has initiated many years ago. Part of this work was performed when GB visited AB, then at *QuSoft* in Amsterdam.

References

1. S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM* **51**(4):595–605, 2004.
2. A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences* **64**:750–767, 2002.
3. A. Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing* **1**(1):37–46, 2005.
4. B. Barak and M. Mahmoody-Ghidary. Merkle puzzles are optimal – An $O(n^2)$–query attack on any key exchange from a random oracle. In *Advances in Cryptology – Proceedings of Crypto 2009*, pages 374–390, 2009.
5. A. Belovs. *Applications of the Adversary Method in Quantum Query Algorithms*. PhD thesis, University of Latvia, 2014.
6. A. Belovs, G. Brassard, P. Høyer, M. Kaplan, S. Laplante and L. Salvail. Provably secure key establishment against quantum adversaries. Extended version available at `http://arxiv.org/abs/1704.08182`.
7. A. Belovs and A. Rosmanis. On the power of non-adaptive learning graphs. *Computational Complexity* **23**(2):323–354, 2014.
8. A. Belovs and R. Špalek. Adversary lower bound for the k-sum problem. In *Proceedings of 4th ACM Innovations in Theoretical Computer Science*, pages 323–328, 2013.
9. A. Belovs. Variations on quantum adversary. `http://arxiv.org/abs/1504.06943`, April 2015.
10. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems & Signal Processing, Bangalore*, pages 175–179, 1984. Republished in 30th Anniversary Commemorative Issue of *Theoretical Computer Science* **560**(Part 1):7–11, 2014.
11. M. Boyer, G. Brassard, P. Høyer and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik* **46**:493–505, 1998.
12. G. Brassard. Cryptography in a quantum world. In *Proceedings of SOFSEM 2016: Theory and Practice of Computer Science*, pages 3–16, 2016.
13. G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail. Merkle puzzles in a quantum world. In *Advances in Cryptology – Proceedings of Crypto 2011*, pages 391–410, 2011. Extended version available at `http://arxiv.org/abs/1108.2316v1`.

14 G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail. Key establishment à la Merkle in a quantum world. http://arxiv.org/abs/1108.2316v2, February 2015.

15 G. Brassard and L. Salvail. Quantum Merkle puzzles. *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies*, pages 76–79, 2008.

16 W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory* **22**(6):644–654, 1976.

17 L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters* **79**(2):325–328, 1997.

18 P. Høyer, T. Lee and R. Špalek. Negative weights make adversaries stronger. In *Proceedings of 39th Annual ACM Symposium on Theory of Computing*, pages 526–535, 2007. doi:10.1145/1250790.1250867.

19 R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of 21st Annual ACM Symposium on Theory of Computing*, pages 44–61, 1989.

20 S. Kutin. Quantum lower bound for the collision problem with small range. *Theory of Computing* **1**(1):29–36, 2005.

21 T. Lee, R. Mittal, B. W. Reichardt, R. Špalek and M. Szegedy. Quantum query complexity of state conversion. In *Proceedings of 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 344–353, 2011.

22 L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4**(10):686–689, 2010.

23 F. Magniez, A. Nayak, J. Roland and M. Santha. Search via quantum walk. *SIAM Journal on Computing* **41**(1):142–164, 2011.

24 R. Merkle. Publishing a new idea. http://www.merkle.com/1974/.

25 R. Merkle. Secure communications over insecure channels. *Communications of the ACM* **21**(4):294–299, 1978.

26 R. L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**(2):120–126, 1978.

27 P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* **26**:1484–1509, 1997.

28 P. Wayner. British document outlines early encryption discovery. http://www.nytimes.com/library/cyber/week/122497encrypt.html, New York Times Technology Cybertimes column, 24 December 1997.

29 Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A* **78**(4):042333, 2008.

Quantum Coin Hedging, and a Counter Measure*

Maor Ganz[1] and Or Sattath[2]

1 **The Hebrew University, Jerusalem, Israel**
maor.ganz@mail.huji.ac.il

2 **The Hebrew University, Jerusalem, Israel and MIT, Cambridge, USA**
sattath@cs.huji.ac.il

Abstract

A quantum board game is a multi-round protocol between a single quantum player against the quantum board. Molina and Watrous discovered quantum hedging. They gave an example for perfect quantum hedging: a board game with winning probability < 1, such that the player can win with certainty at least 1-out-of-2 quantum board games played in parallel. Here we show that perfect quantum hedging occurs in a cryptographic protocol – quantum coin flipping. For this reason, when cryptographic protocols are composed in parallel, hedging may introduce serious challenges into their analysis.

We also show that hedging cannot occur when playing two-outcome board games in sequence. This is done by showing a formula for the value of sequential two-outcome board games, which depends only on the optimal value of a single board game; this formula applies in a more general setting of possible target functions, in which hedging is only a special case.

1998 ACM Subject Classification F.1.1 Models of Computation, D.4.6. Security and Protection

Keywords and phrases Quantum hedging, Quantum coin-flipping, Quantum cryptography

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.4

1 Introduction

Quantum board games

A quantum board game is a special type of an interactive quantum protocol. The protocol involves two parties: the player and the board. The board implements the rules of the game: in each round i of the protocol, the board applies some quantum operation O_i and sends a quantum message to the player; then the player applies any quantum operation it wants, and sends a quantum message back to the board. At the final round of the board game, the board applies a two outcome measurement, which determines whether the player won or lost. We assume that the player knows the rules of the board game (the length of the messages, the operations O_i and the two outcome measurement). The player has the freedom to decide on his strategy – the protocol does not specify what the player should do in each round; the only constraint posed on the player is that it must send a message of an appropriate length, as expected by the board.[1]

* This work was supported by ERC Grant 030-8301.

[1] Previous works which studied this setting did not introduce a specific term for it [22]. Other, related notions are interactive proof system, that differ from quantum board games since the verifier and prover receive an input, and from quantum games since usually we think of the players, Alice and Bob, as having symmetric roles, whereas here, the player knows that the board only implements the rules of the game, and uses its specified strategy.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 4; pp. 4:1–4:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Perfect hedging

Molina and Watrous showed that hedging is possible in quantum board games [22]. Perfect hedging is best explained by an example: there exists a quantum board game for which no strategy can win with certainty, but it is possible for a player to guarantee winning 1-out-of-2 independent quantum board games, which are played in parallel. A formal definition of hedging is given in Definition (3), but for now, one can think of that example. In a follow up work, Arunachalam, Molina and Russo [6] analyzed a family of quantum board games, and showed a necessary and sufficient condition so that the player can win with certainty in at least 1-out-of-n board games. As discussed later, quantum hedging is known to be a purely quantum phenomenon.

One example where Hedging becomes relevant is when reducing the error (soundness) probability of quantum interactive proof protocols such as QIP(2): since the optimal strategy for winning t-out-of-n parallel repetitions is not necessarily an independent strategy, only Markov bound (and not the Chernoff bound) can be used to show soundness [14]. These aspects resembles the behavior that occurs in the setting of Raz's (classical) parallel repetition theorem [25]; the differences are that in the classical setting there are two players who want to win all board games, whereas in our setting, there is a single player, who wants to win at least t-out-of-n board games.

Coin flipping

Quantum coin flipping is a two player cryptographic protocol which simulates a balanced coin flip. When Alice and Bob are honest, they both agree on the outcome, which is uniform on $\{0, 1\}$. Coin flipping comes in two flavors: Strong and weak. Perhaps the most intuitive one is *weak coin flipping*, in which each side has an opposite desirable outcome: 0 implies that Alice wins, and 1 implies that Bob wins. An important parameter is the optimal winning probability for a cheating player against an honest player. In weak coin flipping we denote them by P_A and P_B. We define $P^* = \max\{P_A, P_B\}$ – the maximum cheating probability of both players. In a *strong coin flipping*, a cheating player might try to bias the result to any outcome. We define P_A^0 to be the maximal winning probability of a cheating Alice who tries to bias the result to 0, and P_A^1, P_B^0, P_B^1 are defined similarly. In strong coin flipping $P^* = \max\left\{P_A^0, P_A^1, P_B^0, P_B^1\right\}$ that is P^* bounds the possible bias to any of the outcomes, by either a cheating Alice or a cheating Bob. In the classical settings, it is known that without computational assumptions, in any coin flipping protocol (either weak or strong) at least one of the players can guarantee winning with probability 1 ($P^* = 1$) [12]. Under mild computational assumption, coin flipping can be achieved classically [7]. All of the results in the rest of this paper hold information theoretically, that is, without any computational assumptions. Unconditionally secure (i.e. without computational assumptions) quantum strong coin flipping protocols with large but still non-trivial $P^* < 0.9143$ were first discovered by [3]. Kitaev then proved that in strong coin flipping, every protocol must satisfy $P_0^* \cdot P_1^* \geq \frac{1}{2}$, hence $P^* \geq \frac{\sqrt{2}}{2}$ ([16], see also [5]). Therefore, the hope to find protocols with arbitrarily small cheating probability moved to weak coin flipping. Protocols were found with decreasing P^*([26, 4] showed strong coin flipping with $P^* = \frac{3}{4}$, [19] showed weak coin flipping with $P^* = 0.692$), until it was finally proved that there are families of weak coin flipping protocols for which P^* converges to $\frac{1}{2}$ [20] (see also [2]). Following this, [9] showed how such protocol can be adopted, in order to create (arbitrarily close to) optimal strong coin flipping (so that P^* can be made arbitrarily close to $\frac{\sqrt{2}}{2}$). Although this would not be relevant for our work, analysis of coin flipping protocols was adapted, and later implemented, for experimental setups [23, 24]. There is also a strong connection between coin-flipping and bit-commitment protocols [26, 10], and to a lesser extent to oblivious transfer [8].

Is it possible to hedge in quantum coin flips? In Section 2 we give an example for perfect quantum hedging in the context of coin flipping. The result can be best explained in the context of weak coin flipping (although, a similar statement can be proved for strong coin flipping): there exists a weak coin flipping protocol where $P^* = \cos^2(\frac{\pi}{8})$ introduced by Aharonov [1] yet a cheating Bob can guarantee winning in at least 1-out-of-2 board games played in parallel.

Avoiding hedging through sequential repetition

Consider a cryptographic quantum protocol, which involves several uses of quantum two-outcome board games. For example, the protocol may use several occurrences of quantum coin flips played in parallel. As we have seen, the possibility of hedging makes it hard to analyze the resulting protocol, by simply analyzing each of the board games in it. In Section 3 we show that quantum hedging cannot happen when the two-outcome board games are played in sequence, even if the players are computationally unbounded.

We give a more generalized formulation for sequential board games. Suppose the player's utility for the outcome vector $a = (a_1, \ldots, a_n)$ is given by some target function $t(a)$, and the players goal is to maximize $\mathbb{E}[t(a)]$ over all possible strategies. In Theorem 10 we show that this maximal value is fully determined by the properties of each board game, and does *not* require an analysis of the entire system, which is the case when playing in parallel.

The authors are not aware of previous precise mathematical formulation proofs of that sort. It was recently brought to our attention the following intuitive discussion in [13, p. 8], and [17, p. 9] made for related models. The intuition for our proof is fairly simple and arguably not very surprising: if it is possible to hedge n games, then by simulating the board in the first game, and conditioning on some good event, allows the player to hedge $n-1$ games. But since hedging cannot occur in one game, we get a contradiction.

In Appendix B we give examples, in the classical setting, for board games and target functions, such that the sequential value of the board games is larger than the parallel value of the board games, and vice-versa.

Arunachalam, Molina and Russo [6] showed a different approach to avoid hedging: they showed that hedging is impossible in a quantum single round board game played in parallel, where the player has the possibility to force a restart of the board game.

2 Quantum coin flip hedging

In this section we will give an example for a coin flipping protocol, for which a cheater cannot guarantee a win in one flip, but one of the players can force a win in 1-out-of-2 flips:

▶ **Theorem 1.** *There exists a weak coin flipping protocol with $P^* < 1$ s.t. by playing 2 coin flips in parallel, Bob can guarantee winning in at least one of the flips.*

We will first describe the weak coin flipping protocol and its properties, and then analyze the hedging strategy of Bob. We conclude by explaining why Alice cannot hedge.

2.1 The coin flipping protocol

In this work, Aharonov's coin flipping protocol [1] will play an important role.

A quantum coin flipping protocol

Alice		**Bob**
Prepares $\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$		
	$\xrightarrow{\text{second qubit}}$	
		Samples $b \in_R \{0,1\}$.
	$\xleftarrow{\text{sends } b}$	
If $b = 1$, then apply H.		If $b = 1$, then apply H.
Measure in the standard basis		Measure in the standard basis
Alice wins if the outcome is 0		Alice wins if the outcome is 0
Bob wins if the outcome is 1		Bob wins if the outcome is 1

▶ **Theorem 2.** *The protocol above is a weak coin-flipping protocol with* $P^* = P_A = P_B = \cos^2 \frac{\pi}{8}$.

The proof is given in Appendix A. This protocol is not only a weak coin flipping with $P^* = \cos^2 \frac{\pi}{8}$, but also a strong coin flipping protocol with the same value of P^*. The proof is essentially the same. We state the result this way because it provides a natural interpretation for statements such as "Bob wins in 1 out of 2 flips". Of course, similar statements can be made for strong coin flipping, but are omitted for the sake of readability.

2.2 Coin hedging is possible

Assume a cheating Bob plays two coin flips in parallel with an honest Alice (it does not matter if he plays against the same person twice, or against two different players, since they behave the same – because they are honest). We want to know the maximum probability for a cheating Bob to win at least one coin flip. Surprisingly, this is equal to 1 in the protocol we previously described. This is impossible if Bob were to play the two coin flips sequentially (see Theorem 5).

We saw that for one coin flipping, $P_A = P_B = \cos^2 \frac{\pi}{8} \approx 0.853$. By cheating each coin flip independently, the best Bob can get is

$$\Pr(\text{Bob wins at-least one game}) = 1 - (1 - P_B)^2 = 1 - \left(1 - \cos^2 \frac{\pi}{8}\right)^2 \approx 0.978.$$

We will now show Bob's perfect hedging strategy (which is not independent), in which he wins exactly one out of the two coin flips w.p. 1, which completes the proof of Theorem 2. Alice's initial state is

$$\frac{1}{2} \sum_{i_1, i_2 \in \{0,1\}} |i_1, i_2\rangle |i_1, i_2\rangle = \frac{1}{2} \sum_{i=0}^{3} |\alpha_i\rangle |\alpha_i\rangle, \tag{1}$$

where[2]

$$
\begin{aligned}
|\alpha_0\rangle &= |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle - |-+\rangle\right) \\
|\alpha_1\rangle &= |\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\
|\alpha_2\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle - |\Psi^-\rangle\right) = \frac{1}{\sqrt{2}}\left(|0-\rangle + |1+\rangle\right) \\
|\alpha_3\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle + |\Psi^-\rangle\right) = \frac{1}{\sqrt{2}}\left(|-0\rangle + |+1\rangle\right). \qquad (2)
\end{aligned}
$$

Eq. (1) can be justified by a direct calculation, or by using the Choi–Jamiołkowski isomorphism [11, 15], see also [27], and noting that the associated matrix for the l.h.s. and the r.h.s. are equal (both are proportional to the identity matrix). Bob is given the right register of the state above. Bob applies the unitary transformation $U = \sum_i |\gamma_i\rangle\langle\alpha_i|$, where $|\gamma_0\rangle = |11\rangle, |\gamma_1\rangle = |00\rangle, |\gamma_2\rangle = |01\rangle, |\gamma_3\rangle = |10\rangle$, so that the overall state becomes $\frac{1}{2}\sum_{i=0}^{3}|\alpha_i\rangle|\gamma_i\rangle$, and sends the right register back to Alice. Alice measures the right register in the standard basis (of course, Bob could have done this just before sending the right register, if he is restricted to sending classical information). The results of those measurements determines the basis in which she measures the left register. This strategy guarantees that Bob wins in exactly one coin flip: for example, if Alice measures the qubits $|\gamma_0\rangle = |11\rangle$ then the left register collapses to $|\alpha_0\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|+-\rangle + |-+\rangle\right)$, and since in this case Alice measures both of the left register qubits in the Hadamard basis, Bob will win in exactly one out of the two coin flips. The right-most expressions in Eq. (2) are presented in this form so that it is easy to see the similar behavior in the 3 other cases.

One may wonder how strong the effect of hedging is. In particular, can Bob guarantee fn out of n winnings, as long as $f \leq P^*$? The answer is no: by playing three coin flipping of this protocol, he cannot guarantee winning $2 = \frac{2}{3}\cdot 3$ with probability 1, even though $\frac{2}{3} \leq P^*$: we numerically calculated that Bob can only win with probability ≈ 0.986 at least 2 out of 3 coin flips. This is still higher than the optimal independent cheating that achieves a success probability of ≈ 0.94.

Fortunately for Bob, Alice can not guarantee winning in 1-out-of-2 played in parallel using this weak coin flipping protocol. In fact, she cannot do any hedging. This is true, essentially for the same reasons error reduction for QMA works in a simple manner (vis-à-vis QIP(2)). The following argument uses the definitions from Section 3.1. Recall that from Bob's perspective, he is provided with a quantum state given from Alice, and he measures it to determine whether he wins or loses. Therefore $m(a_i) = \min_{|\psi_i\rangle}\langle\psi_i|M^i_{a_i}|\psi_i\rangle$ (where $M^i_{a_i}$ is Bob's measurement operator which determines whether he gets the outcome a_i in the ith game), which is equal to the smallest eigenvalue of $M^i_{a_i}$; and $m^{par}(a_1,\ldots,a_n) = \min_{|\psi\rangle}\langle\psi|M^i_{a_1}\otimes\cdots\otimes M^i_{a_n}|\psi\rangle$ which is equal to the smallest eigenvalue of $M^i_{a_1}\otimes\cdots\otimes M^i_{a_n}$. But since $M^i_{a_i}$ is a measurement operator, its eigenvalues are non-negative, and we conclude that $m^{par}(a_1,\ldots,a_n) = m(a_1)\cdot\ldots\cdot m(a_n)$.

[2] One may wonder whether the states $|\alpha_i\rangle$ are the Bell states ($|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$), written in a non-standard local basis. This is not the case: for every Bell state $|\Omega\rangle$, $SWAP|\Omega\rangle = \pm|\Omega\rangle$. This is also true if a local basis change is applied to both qubits: for $|\Omega'\rangle = U\otimes U|\Omega\rangle$, $SWAP|\Omega'\rangle = \pm|\Omega'\rangle$. Since $|\alpha_2\rangle = SWAP|\alpha_3\rangle \neq \pm|\alpha_2\rangle$, these vectors are not the Bell states written in a non-standard local basis.

3 How to circumvent hedging

Our solution to circumvent hedging is to play the board games in sequence, instead of in parallel. We will prove in Section 3.1 that in the simple scenario, in which the goal is to win at least 1-out-of-n sequential board games, hedging is not possible (i.e. the best cheating strategy is to use the optimal cheating strategy in each board game independently). We will generalize this in Section 3.2, where we will prove that the same result holds for every target function. Throughout this section, we will consider only two-outcome board games (such as coin flipping), but a generalization to any number of outcomes seems not too difficult to achieve as well.

3.1 Playing sequentially circumvents 1-out-of-n hedging

Molina and Watrous [22] defined *hedging* as the following phenomenon.[3] Suppose G_1, G_2 are two board games with multiple outcomes A_1, A_2. For $a_1 \in A_1$ let $m(a_1)$ be the minimal probability that can be achieved for the outcome a_1 in G_1, and similarly for $m(a_2)$. If the board game G is not clear from the context, we may use $m^{G_2}(a_2)$. Now suppose that two board games are played in parallel, and the goal is to minimize the probability for getting the outcome a_1 in the first board game and a_2 in the second board game, which is defined as $m^{par}(a_1, a_2)$. Since the two strategies can be played independently, clearly, $m^{par}(a_1, a_2) \leq m(a_1)\, m(a_2)$. *Parallel Hedging* for two board games is the case where this inequality is strict, that is $m^{par}(a_1, a_2) < m(a_1)\, m(a_2)$. Molina and Watrous gave an example for perfect parallel hedging in which $m^{par}(a_1, a_2) = 0$ whereas $m(a_1) = m(a_2) > 0$. This definition can be naturally generalized to more than two board games.

▶ **Definition 3** (Parallel Hedging)**.** Let $G_1, \ldots, G_n$ be n quantum board games with possible outcomes $A_1, \ldots, A_n$. For $a_i \in A_i$, let $m(a_i)$ be the minimal probability that can be achieved for the outcome a_i in G_i. Similarly, let $m^{par}(a_1, \ldots, a_n)$ be the minimal probability that can be achieved for outcomes $(a_1, \ldots, a_n)$ when playing these n board games in parallel. We say that hedging is possible in 1-out-of-n board games if there exist $a_1, \ldots, a_n$ s.t.

$$m^{par}(a_1, a_2, \ldots, a_n) < \prod_{i=1}^{n} m(a_i). \tag{3}$$

If $m^{par}(a_1, a_2, \ldots, a_n) = 0$ and $\prod_{i=1}^{n} m(a_i) > 0$, then it is called *prefect hedging*.

It is known that inequality (3) is actually an equality in the classical case for single round board games [22, 18]. We do not know whether the equality holds for multi-round classical board games. What happens when the board games are played in sequence?

▶ **Definition 4.** Given board games $\{G_i\}_{i=1}^{n}$, the protocol for playing the board games $\{G_i\}$ in order is called *sequential*, assuming the player knows the result of G_i before the start of G_{i+1} (this can be achieved by adding a last round for each board game in which the board returns the outcome).

Our next result shows that there is no sequential hedging for board games (with any number of outcomes), and the cheater cannot do better than to cheat each board game independently;

[3] Molina and Watrous restricted their definition to quantum board games with a single round of communication (the board sends an initial quantum state to the player, the player sends back another quantum state back to the board, and then the board applies a measurement to determine whether the player wins).

that is if $\{G_i\}_{i=1}^n$ are board games, then $m^{seq}(a_1,\ldots,a_n) = m(a_1)\cdot\ldots\cdot m(a_n)$, where $m^{seq}(a_1,\ldots,a_n)$ is defined similarly to $m^{par}(a_1,\ldots,a_n)$ for sequential board games. For simplicity and clarity, we will consider only the case where all the board games are identical and $a_i = a_j = a$ for all i,j, but the same proof will work for the general scenario as well (one will just have to add indices indicating the board game for everything).

▶ **Theorem 5.** *Let G be a board game, played sequentially n times, then $m^{seq}(a,\ldots,a) = m(a)\cdot\ldots\cdot m(a) = m(a)^n$ for every outcome a.*

Proof. If the outcome of a single board game is a, then we say that the player *lost* that board game. We denote by "*failure*" the event in which the player gets the outcome a in all n games (i.e. loses all n rounds).

We define ℓ^* to be the probability to get the outcome a in the optimal strategy for one board game. Let ℓ_n be probability to get the outcome a over all the n-board games, in the best independent strategy. It is easy to see that

$$\ell_n = \min_{S\in\text{independent strategies}} \Pr(\text{failure} \mid S) = (\ell^*)^n \tag{4}$$

Define similarly ℓ'_n to be the minimum losing probability over all (not necessarily independent) strategies, i.e. $\ell'_n \equiv \min_{S\in\text{sequential strategies}} \Pr(\text{failure} \mid S)$. Clearly $\forall n\in\mathbb{N},\ \ell'_n \le \ell_n$ and $\ell'_1 = \ell_1$. Our goal is to show that $\forall n\in\mathbb{N},\ \ell'_n = \ell_n$. Assume towards a contradiction that this is not the case. Then there exists a minimal $n>1$ for which $\ell'_n < \ell_n$.

$$(\ell^*)^n \overset{\text{by (4)}}{=} \ell_n > \ell'_n = \ell'_{n,L}\Pr(\text{lost first round}) \ge \ell'_{n,L}\ell^*$$

where $\ell'_{n,L} := \Pr(\text{failure} \mid \text{lost first round})$. The last inequality naturally holds because $\Pr(\text{lost first round}) \ge \ell^*$, otherwise there exists a better strategy. Therefore,

$$(\ell^*)^{n-1} = \ell_{n-1} > \ell'_{n,L}$$

The strategy in which the cheater Alice (the first player) plays with Rob (Alice's imaginary friend) the first board game, and conditioned on losing, plays with Bob (the second player) the next rounds, has a losing probability $\ell'_{n,L}$.

Therefore

$$\ell_{n-1} > \ell'_{n,L} \ge \ell'_{n-1}$$

which contradicts the minimality of n. ◀

▶ **Corollary 6.** *Suppose the goal of a player is to win at least 1-out-of-n board games played sequentially. The optimal strategy is to play independently, by using the optimal cheating strategy in each of the board games.*

3.2 Playing sequentially circumvents any form of hedging

Let us consider a more general setting, in which the player's goal is to maximize the expectation of some target function; i.e., for a vector $t = (t_a \in \mathbb{R})_{a\in\{0,1\}^n}$, let

$$\mathrm{SVal}(t) \equiv \max_{S\in\text{sequential strategies}} \sum_{a\in\{0,1\}^n} t_a \cdot \Pr(a \mid S)$$

and similarly

$$\mathrm{PVal}(t) \equiv \max_{S\in\text{parallel strategies}} \sum_{a\in\{0,1\}^n} t_a \cdot \Pr(a \mid S).$$

In general there are no relations between the parallel and sequential values: in Appendix B we give a classical one round board game in which $\mathrm{SVal}(t) > \mathrm{PVal}(t)$ and another in which $\mathrm{SVal}(t) < \mathrm{PVal}(t)$.

▶ **Definition 7.** Given a two-outcome board game, let q_i be the maximal probability of the player to achieve the outcome $i \in \{0, 1\}$.

Note that always $q_0 \geq 1 - q_1$ and vice-versa. As we have seen before, the parallel value of a two-outcome board game heavily depends on the details of the game. In contrast, the sequential value is fully determined by q_0 and q_1.

In the following we will analyze the sequential value of the board game. For that we will define the tree value function TVal, which as the following theorem shows, is equal to the sequential value of the board game. For simplicity we will assume that for all i, $G_i = G$, but this can be easily extended for general $\{G_i\}_{i=1}^n$.

▶ **Definition 8.** For a vector $t = (t_a)_{a\in\{0,1\}^n}$ let $t_b^{\leftarrow} = t_{0b}$ and $t_b^{\rightarrow} = t_{1b}$. The tree value with parameters q_0, q_1 is defined as:

$$\mathrm{TVal}(t) \equiv \max\left\{q_0\,\mathrm{TVal}(t^{\leftarrow}) + (1-q_0)\,\mathrm{TVal}(t^{\rightarrow})\ ,\ q_1\,\mathrm{TVal}(t^{\rightarrow}) + (1-q_1)\,\mathrm{TVal}(t^{\leftarrow})\right\},$$

and for $c \in \mathbb{R}$, $\mathrm{TVal}(c) = c$.

▶ **Definition 9.** Consider a quantum board game G played n times in sequence. A strategy is said to be *pure black box* strategy if the strategy used in the i-th board game is fully determined by the outcomes of the previous board games. For a set $\mathcal{S}$ of strategies for a single board game G, an $\mathcal{S}$-black-box strategy is a pure black-box strategy in which the strategy at the i-th board game (conditioning on previous outcomes) is in $\mathcal{S}$.

▶ **Theorem 10.** *For every two-outcome board game (with parameters q_0, q_1), every n and every $t \in \mathbb{R}^{2^n}$, $\mathrm{SVal}(t) = \mathrm{TVal}(t)$.*

Furthermore, its value can be obtained by an $\{S_0, S_1\}$-black-box strategy, where S_0 (S_1) are any strategies that achieve outcomes 0 (1) with probability q_0 (q_1).

S_0 and S_1 are greedy strategies that simply try to maximize the chance of achieving the outcomes 0 and 1 respectively in the board game at hand. This theorem is in fact a generalization of Theorem 5 for 2-outcome board games: By choosing $t_a = 1 - \delta_{a,a'}$ we get that

$$\begin{aligned}\mathrm{SVal}(t) &\equiv \max_{S\in\text{sequential strategies}} \sum_{a\in\{0,1\}^n} t_a \cdot \Pr(a \mid S) = \max_{S\in\text{sequential strategies}} \sum_{a\neq a'} \Pr(a \mid S)\\ &= \max_{S\in\text{sequential strategies}} 1 - \Pr(a' \mid S)\\ &= 1 - \min_{S\in\text{sequential strategies}} \Pr(a' \mid S) = 1 - m^{seq}(a')\,. \end{aligned} \tag{5}$$

By expanding the recursion, a simple inductive argument shows that for our choice of t,

$$\mathrm{TVal}(t) = 1 - m(a_1)\cdot\ldots\cdot m(a_n). \tag{6}$$

By combining Theorem 10 and Eqs. (5) and (6), we reprove Theorem 5.

Proof of Theorem 10. First we show that $\mathrm{SVal}(t) \geq \mathrm{TVal}(t)$, by explicitly constructing an $\{S_0, S_1\}$-black-box strategy with the value $\mathrm{TVal}(t)$. The strategy can be best explained by defining a binary full tree with depth n. We fill the value of each node in the tree, from

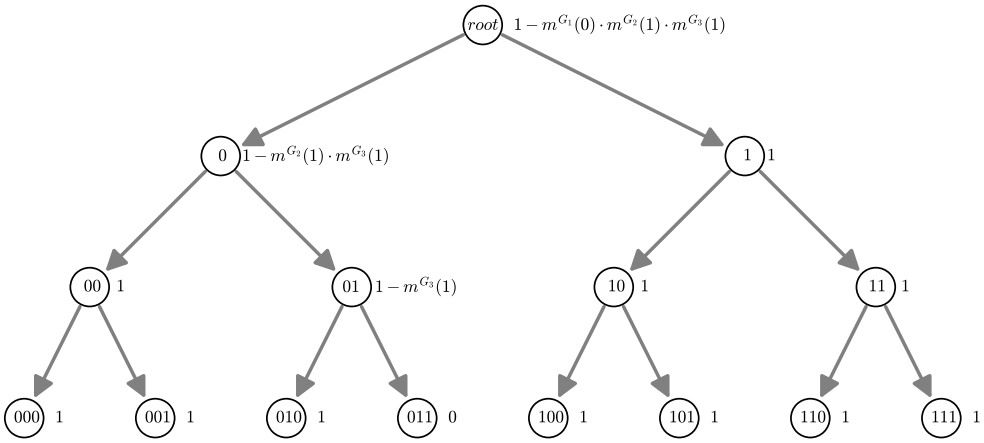

Figure 1 TVal for $t_a = 1 - \delta_{a,011}$. The labels of the leaves represent all the possible outcomes a of the values in the $n = 3$ board games, and the values on the right of each node are the TVal of that node. Indeed $t_a = 1$ for all $a \neq 011$. Note that $m(0) = 1 - q_1$ and $m(1) = 1 - q_0$, and for example $\mathrm{TVal}(01) = q_0 = 1 - m^{G_3}(1)$, and $\mathrm{TVal}(0) = q_0 + (1 - q_0) q_0 = 1 - m^{G_2}(1) + m^{G_2}(1)\left(1 - m^{G_3}(1)\right) = 1 - m^{G_2}(1) \cdot m^{G_3}(1)$.

bottom to top. The leaves of the tree will have values t_a. The values of a parent of two children with values $v^{\leftarrow}, v^{\rightarrow}$ will have the value:

$$\max\{q_0 v^{\leftarrow} + (1 - q_0) v^{\rightarrow}, q_1 v^{\rightarrow} + (1 - q_1) v^{\leftarrow}\}$$

It can be easily verified that the value of the root is $\mathrm{TVal}(t)$.

Consider the following strategy which applies S_0 if $q_0 v^{\leftarrow} + (1 - q_0) v^{\rightarrow} \geq q_1 v^{\rightarrow} + (1 - q_1) v^{\leftarrow}$ and S_1 otherwise, and continues in the same fashion with respect to the left child if the outcome is 0, and the right child if the outcome is 1. It can be proved by a simple inductive argument that the expected value of this strategy is the value of the root which is indeed $\mathrm{TVal}(t)$. Clearly, this strategy is an $\{S_0, S_1\}$ black-box strategy.

Next we show that $\mathrm{SVal}(t) \leq \mathrm{TVal}(t)$. This will be proven by induction on n – the number of board games played. Clearly, for $n = 1$, the optimal strategy has the value $\mathrm{TVal}(t)$. Let n be the minimal number, such that there exists some target t, for which there is a strategy with value greater than $\mathrm{TVal}(t)$ and denote the contradicting strategy by S. We now introduce some notation. Let $p^j = \Pr(j \text{ in first game} \mid \text{using strategy } S)$, $p^j_{\mathbf{i}} = \Pr(\mathbf{i} \text{ in the last n-1 games} \mid j \text{ in the first game, using strategy } S)$. Let $\mathcal{S}^n$ be the set of all strategies over n sequential board games.

$$\mathrm{opt} = \max_{S' \in \mathcal{S}^n} \sum_{\mathbf{i} \in 2^n} t_{\mathbf{i}} \Pr(\mathbf{i} \mid \text{ using strategy } S')$$

For $j \in \{0, 1\}$, let $\mathrm{opt}^j \equiv \max_{S' \in \mathcal{S}^{n-1}} \sum_{\mathbf{i} \in 2^{n-1}} t_{j,\mathbf{i}} \Pr(\mathbf{i} \mid \text{using strategy } S')$. Since the optimization is over board games of length $n - 1$, by the induction hypothesis, $\mathrm{opt}^0 = \mathrm{TVal}(t^{\leftarrow})$, and similarly $\mathrm{opt}^1 = \mathrm{TVal}(t^{\rightarrow})$. We know that

$$\mathrm{opt} > q_0 \cdot \mathrm{opt}^0 + (1 - q_0) \cdot \mathrm{opt}^1 \tag{7}$$

and similarly

$$\mathrm{opt} > q_1 \cdot \mathrm{opt}^1 + (1 - q_1) \cdot \mathrm{opt}^0 \tag{8}$$

otherwise, $\text{opt} = \text{TVal}(t)$. Assume WLOG that

$$q_0 \cdot \text{opt}^0 + (1 - q_0) \cdot \text{opt}^1 \geq q_1 \cdot \text{opt}^1 + (1 - q_1) \cdot \text{opt}^0$$

then we get that $\text{opt}^0 (q_0 - 1 + q_1) \geq \text{opt}^1 (q_1 - 1 + q_0)$ hence $\text{opt}^0 \geq \text{opt}^1$ or $(q_1 - 1 + q_0) \leq 0$, because $q_0 \geq 1 - q_1$. Since $p^j \leq q_j$ we get that $q_0 + q_1 \leq 1$ implies $p^0 = q_0$ and $p^1 = q_1$. We know that (for both the above cases)

$$\text{opt} = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\leftarrow} p^0 p_{\mathbf{i}}^0 + t_{\mathbf{i}}^{\rightarrow} p^1 p_{\mathbf{i}}^1.$$

Let us denote

$$v^0 = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\leftarrow} p_{\mathbf{i}}^0 \ , \ v^1 = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\rightarrow} p_{\mathbf{i}}^1$$

hence $\text{opt} = p^0 v^0 + p^1 v^1$ where $p^j \leq q_j$.

▶ **Claim 11.** $v^j \leq opt^j$

Proof. The cheater can play himself (his honest self), according to his strategy, until he gets j in the first board game and then continue to play the rest $(n-1)$ of the board games against the real honest player. This is a valid strategy for $n-1$ board games with value v^j, but since opt^j is an optimal such strategy, we get that $v^j \leq \text{opt}^j$. ◀

Using the above claim,

$$\text{opt} = p^0 v^0 + p^1 v^1 \leq p^0 \text{opt}^0 + p^1 \text{opt}^1 = p^0 \text{opt}^0 + \left(1 - p^0\right) \text{opt}^1. \tag{9}$$

By subtracting Eq. 9 from Eq. 7 we get that

$$0 > \text{opt}^0 \left(q_0 - p^0\right) + \text{opt}^1 \left(1 - q_0 - 1 + p^0\right) = \left(\text{opt}^0 - \text{opt}^1\right) \left(q_0 - p^0\right)$$

but either $\text{opt}^0 \geq \text{opt}^1$, $q_0 \geq p^0$ and we get $0 > 0$ and contradiction, or $p^0 = q_0$ hence again we get $0 > 0$ and contradiction. Altogether we now know that Eq. (7) is wrong, hence

$$\text{opt} = q_0 \cdot \text{opt}^0 + (1 - q_0) \cdot \text{opt}^1 \tag{10}$$

and by the hypothesis assumption we get that $\text{opt} = \text{TVal}\,(t)$. ◀

4 Open questions

- Is there a formal connection between the setting discussed in the parallel repetition Theorem (as was discussed in the introduction) and the setting that occurs in quantum hedging?
- How general is coin hedging? Does hedging (as in Definition 3) happen in every non-trivial ($\epsilon < \frac{1}{2}$) coin flipping protocol? The same questions can be asked for perfect hedging. We conjecture that the answer for these questions is positive.
- In our example for coin hedging, we saw that the hedging player reduces the expected number of wins: The cheater could guarantee that he will win one flip out of two, thus getting an expectation 0.5 for winning, while the expectation of winning in independent cheating is ≈ 0.85. Does the expected ratio of wins in the perfect hedging of this protocol scenario increase with n? In this protocol (or, perhaps, another coin flipping protocol),

when flipping n coins in parallel and $n \to \infty$, can Bob guarantee winning $\sim nP^*$ coin flipping out of n (Of course the expected number of parallel wins cannot be higher than the expected number of independent wins (which is $\frac{1}{2}$), as was proved formally in [21])?

This property cannot hold for every protocol. The reason is essentially that P^* can be artificially increased in a way which does not help the cheating player to achieve perfect hedging. Consider some coin flipping protocol with $P^* = \frac{1}{2}$ (even though this is impossible, for $P^* > \frac{1}{2}$ a simple adaptation of the following argument applies), then a cheating Bob clearly cannot guarantee winning more than $\frac{1}{2}n$. If we now alter the protocol, such that in the last round of the protocol, with probability δ, Alice asks Bob what his outcome of the protocol was, and declares that as her outcome. This changes P^* to $P^{*\prime} = \frac{1}{2} + \frac{\delta}{2}$, but with probability δ^n these protocols coincide, and Bob cannot guarantee more than $\frac{1}{2}n$ wins, which is less than $P^{*\prime}n$ as required by the statement above.

- Can one define and show hedging for bit-commitment?

Acknowledgments. We thank Dorit Aharonov for the weak coin flipping protocol which we used and other valuable discussions, and to the anonymous referees for their comments.

References

1. Dorit Aharonov. Personal communication, 2007.
2. Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. *SIAM J. Comput.*, 45(3):633–679, 2016. doi:10.1137/14096387X.
3. Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew Chi-Chih Yao. Quantum bit escrow. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 705–714. ACM, 2000. doi:10.1145/335305.335404.
4. Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004. doi:10.1016/j.jcss.2003.07.010.
5. Andris Ambainis, Harry Buhrman, Yevgenity Dodis, and Hein Rörig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. doi:10.1109/CCC.2004.19.
6. Srinivasan Arunachalam, Abel Molina, and Vincent Russo. Quantum hedging in two-round prover-verifier interactions. *arxiv preprint arxiv:1310.7954*, 2013. arXiv:1310.7954.
7. Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983. doi:10.1145/1008908.1008911.
8. André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago J. Theor. Comput. Sci.*, 2016, 2016. arXiv:1310.3262.
9. André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 527–533. IEEE Computer Society, 2009. doi:10.1109/FOCS.2009.71.
10. André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 354–362. IEEE Computer Society, 2011. doi:10.1109/FOCS.2011.42.
11. Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. doi:10.1016/0024-3795(75)90075-0.

12 Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 364–369. ACM, 1986. doi:10.1145/12130.12168.

13 Gus Gutoski and John Watrous. Quantum interactive proofs with competing provers. In Volker Diekert and Bruno Durand, editors, *STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24-26, 2005, Proceedings*, volume 3404 of *Lecture Notes in Computer Science*, pages 605–616. Springer, 2005. doi:10.1007/978-3-540-31856-9_50.

14 Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 534–543. IEEE Computer Society, 2009. doi:10.1109/FOCS.2009.30.

15 Andrzej Jamiolkowski. Linear transformations which preserve trace and positive semi-definiteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972. doi:10.1016/0034-4877(72)90011-0.

16 Alexei Kitaev. Quantum coin flipping. Talk at the 6th workshop on Quantum Information Processing, 2003.

17 Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. In Ran Canetti, editor, *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.*, volume 4948 of *Lecture Notes in Computer Science*, pages 107–124. Springer, 2008. doi:10.1007/978-3-540-78524-8_7.

18 Rajat Mittal and Mario Szegedy. Product rules in semidefinite programming. In Erzsébet Csuhaj-Varjú and Zoltán Ésik, editors, *Fundamentals of Computation Theory, 16th International Symposium, FCT 2007, Budapest, Hungary, August 27-30, 2007, Proceedings*, volume 4639 of *Lecture Notes in Computer Science*, pages 435–445. Springer, 2007. doi:10.1007/978-3-540-74240-1_38.

19 Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 2–11. IEEE Computer Society, 2004. doi:10.1109/FOCS.2004.55.

20 Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arxiv preprint arxiv:0711.4114*, 2007. arXiv:0711.4114.

21 Abel Molina. Parallel repetition of prover-verifier quantum interactions. *Arxiv preprint arXiv:1203.4885*, 2012.

22 Abel Molina and John Watrous. Hedging bets with correlated quantum strategies. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, pages 2614–2629, 2012. doi:10.1098/rspa.2011.0621.

23 Anna Pappa, André Chailloux, Eleni Diamanti, and Iordanis Kerenidis. Practical quantum coin flipping. *Phys. Rev. A*, 84:052305, 2011. doi:10.1103/PhysRevA.84.052305.

24 Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nature Communications*, 5, 2014. Article. doi:10.1038/ncomms4717.

25 Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, 1998. doi:10.1137/S0097539795280895.

26 Robert W. Spekkens and Terry Rudolph. Degrees of concealments and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(01):012310, 2001. doi:10.1103/PhysRevA.65.012310.

27 John Watrous. *Theory of quantum information.* Available online, 2011. URL: https://cs.uwaterloo.ca/~watrous/TQI/.

A Proof of Theorem 2

We will use the same method we use in other sections, which is based on semi-definite programming (SDP). See, for example, [5]. We will follow the notations used in [2, 20]. We will prove that the maximal cheating probability for both players is $P^* = P_A = P_B = \cos^2 \frac{\pi}{8}$.

If Alice is the cheater, a cheating strategy is described entirely by the one qubit state ρ which she sends to Bob. Her winning probability is given by

$$\Pr\left(\text{Alice wins}\right) = \frac{1}{2}\operatorname{Tr}\left(\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\rho\right).$$

Since

$$\begin{aligned}\max_{\rho\succeq 0, \operatorname{Tr}\rho=1} \frac{1}{2}\operatorname{Tr}\left(\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\rho\right) &= \max_{|\psi\rangle} \frac{\langle\psi|\frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)|\psi\rangle}{\langle\psi\mid\psi\rangle} \\ &= \lambda_{max}\left(\frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\right) \\ &= \cos^2\frac{\pi}{8},\end{aligned}$$

the maximal cheating probability is $P_A = \cos^2 \frac{\pi}{8}$.

Let us look at a cheating Bob (and an honest Alice). The initial density matrix is $\rho_0^{\mathcal{AM}} = |\phi^+\rangle\langle\phi^+|$ on Alice and the message registers $\mathcal{A}\otimes\mathcal{M}$. Then, Bob applies an operation to the $\mathcal{M}$ qubit. Alice's reduced density matrix cannot be changed due to Bob's operation. Hence our condition is $\operatorname{Tr}_{\mathcal{M}}\rho_1^{\mathcal{AM}} = \rho_1^{\mathcal{A}} = \rho_0^{\mathcal{A}} = \frac{1}{2}I$. Bob's maximal cheating probability is given by:

$$\begin{aligned}\text{maximize} \quad & \operatorname{Tr}\left[\left(|1\rangle\langle 1|\otimes|0\rangle\langle 0| + |-\rangle\langle -|\otimes|1\rangle\langle 1|\right)\cdot\rho_1^{\mathcal{AM}}\right] \\ \text{subject to} \quad & \rho_1^{\mathcal{AM}} \succeq 0 \\ & \rho_0^{\mathcal{AM}} = \left|\Phi^+\rangle\langle\Phi^+\right| \\ & \operatorname{Tr}_{\mathcal{M}}\rho_1^{\mathcal{AM}} = \rho_0^{\mathcal{A}}\end{aligned} \tag{11}$$

The maximization is justified because if the message qubit is 0, Alice measures her qubit in the computational basis, and Bob wins if her outcome is 1; if the message qubit is 1, Alice measures her qubit in the Hadamard basis, and Bob wins if her outcome is $|-\rangle$.

Solving this SDP gives

$$\rho_1^{\mathcal{AM}} = \begin{pmatrix} 0.0732 & 0 & 0.1768 & 0 \\ 0 & 0.4268 & 0 & -0.1768 \\ 0.1768 & 0 & 0.4268 & 0 \\ 0 & -0.1768 & 0 & 0.0732 \end{pmatrix}$$

with a maximum value of ≈ 0.8536.

It is possible to verify that indeed the value of the SDP is not only close, but is exactly equal to $\cos^2\frac{\pi}{8} \approx 0.8536$: One can see that $P_B \leq \cos^2\frac{\pi}{8}$, via Kitaev's formalism to find the Z matrix that bounds ρ (see [20, 2] for details). Alternatively, we can use the SDP formulation of games as described in [22], which applies to the coin-flipping protocol (with Bob as the player): the matrix $Y = \frac{1}{8}\begin{pmatrix} 3+\sqrt{2} & 1 \\ 1 & 1+\sqrt{2}\end{pmatrix}$ is dual-feasible, hence its trace $\operatorname{Tr}[Y] = \frac{1}{4}\left(2+\sqrt{2}\right) = \cos^2\frac{\pi}{8}$ gives the correct bound.

We now show an explicit strategy with winning probability $\cos^2\frac{\pi}{8}$, which shows that $P_B \geq \cos^2\frac{\pi}{8}$, which completes the proof. Bob applies a $-\frac{3\pi}{8}$ rotation

$$U = \begin{pmatrix} \cos -\frac{3\pi}{8} & -\sin -\frac{3\pi}{8} \\ \sin -\frac{3\pi}{8} & \cos -\frac{3\pi}{8} \end{pmatrix} = \begin{pmatrix} \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \\ -\cos\frac{\pi}{8} & \sin\frac{\pi}{8} \end{pmatrix}$$

on the $\mathcal{M}$ qubit, which transforms the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to:

$$\begin{aligned} |\zeta\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left(\sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\right) + |1\rangle \otimes \left(\sin\frac{\pi}{8}|1\rangle + \cos\frac{\pi}{8}|0\rangle\right)\right) \\ &= \frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right) \otimes |0\rangle\right) + \\ &\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8} - \cos\frac{\pi}{8}\right)|+\rangle - \left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)|-\rangle\right) \otimes |1\rangle\right) \end{aligned}$$

We simplify

$$\frac{1}{\sqrt{2}}\left(\sin\frac{\pi}{8} + \cos\frac{\pi}{8}\right) = \frac{1}{\sqrt{2}}\sqrt{\frac{1}{2}\left(2+\sqrt{2}\right)} = \frac{\sqrt{2+\sqrt{2}}}{2} = \cos\frac{\pi}{8}$$

and similarly, $\frac{1}{\sqrt{2}}\left(\cos\frac{\pi}{8} - \sin\frac{\pi}{8}\right) = \frac{\sqrt{2-\sqrt{2}}}{2} = \sin\frac{\pi}{8}$. Hence,

$$|\zeta\rangle = \frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right)|0\rangle - \left(\sin\frac{\pi}{8}|+\rangle + \cos\frac{\pi}{8}|-\rangle\right)|1\rangle\right).$$

Bob measures the r.h.s. qubit in the computational basis, and sends the classical result to Alice. His winning probability is thus $\cos^2\frac{\pi}{8}$. This completes the proof that $P_A = P_B = P^* = \cos^2\frac{\pi}{8}$.

B Relations between parallel and sequential board games

Here we show that the value of the sequential board games can be larger than the parallel board games and vice-versa, depending on the target function, even in the classical setting. Out standard example for a sequential superiority uses the target function: "must win *exactly* 1-out-of-2 board games". This of course, gives the sequential run an advantage over the parallel run, of knowing the outcomes of the previous board games. For that we define a very simple one-round board game: the player chooses a bit b, which is sent to the board.

- If $b = 0$, the player loses (with probability 1).
- If $b = 1$, the player wins with probability $\frac{1}{2}$.

▶ **Lemma 12.** *In the above board game,* $\mathrm{SVal}(t) \geq \frac{3}{4} > \frac{1}{2} = \mathrm{PVal}(t)$.

Proof. The optimal winning probability in a single board game for an honest player is $\frac{1}{2}$ by always sending $b = 1$. Also note, that the player can force a loss with probability 1, by sending $b = 0$. Assume that we are now playing two board games. If the board games are played in sequence, then the optimal strategy will be to try and win the first board game by sending $b_1 = 1$. With probability $\frac{1}{2}$ he will win, then he can lose the second board game by sending $b_2 = 0$. If the player lost the first board game, he will try to win the second board game by sending $b_2 = 1$. Altogether, this strategy wins exactly once with probability $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, proving the first inequality.

Let us look at the four deterministic possibilities for the player when the two board games are played in parallel. If he sends $b_0 = b_1 = 0$, he then loses with probability 1. If he

sends $b_0 \neq b_1$, i.e. loses one of the board games and tries to win the other, then his winning probability of exactly one board game is $\frac{1}{2}$. If he sends $b_0 = b_1 = 1$, i.e. trying to win both, then his winning probability of exactly one board game is again $\frac{1}{2}$ (because no matter what the outcome of the first board game is, the second outcome must be different, and this happens with probability $\frac{1}{2}$). Since every random strategy is a convex combination of these deterministic strategies, every classical strategy will also have a winning probability of at most $\frac{1}{2}$, which is inferior to the winning probability in the sequential setting. Naturally, giving the player quantum powers, does not help him in this classical simple board game, to achieve anything better. ◀

In the other direction, we give an example for a classical board game in which the parallel setting, achieves better value than the classical one. Define a board game, in which the board sends a bit a equally distributed, and then the player returns a bit b. If $a = 0$, then the player loses if $b = 0$, and if $b = 1$ then the player wins with probability p. If $a = 1$, then the player wins if $b = 0$, and if $b = 1$ then the player loses with probability p. We think of p to be of a parameter $p < \frac{3}{4}$. Our target function is the same as before – win *exactly* 1-out-of-2 board games.

▶ **Lemma 13.** *In the above board game,* $\mathrm{PVal}(t) \geq \frac{1}{2} + 2p\,(1-p) > \frac{1}{2} + \frac{1}{2}p = \mathrm{SVal}(t)$.

Proof. In the parallel settings, the player gets the a_1, a_2 and only then sends b_1, b_2, which gives him the edge. If $a_1 \neq a_2$, his strategy is to send $b_1 = 0, b_2 = 0$ and he will win exactly one board game out of the two. If $a_1 = a_2$ then he will send $b_1 = b_2 = 1$ and he will win exactly one of the board games with probability $p\,(1-p)$. Overall we see that $\mathrm{PVal}(t) \geq \frac{1}{2} + 2p\,(1-p)$. In the sequential setting, it does not matter what happened in the first board game, as the second board game will determine the result (the outcome of the second board game must be different than the first). With probability $\frac{1}{2}$ the board will send a good a_2, resulting in the player winning with certainty exactly 1 out of the 2 board games if they send $b_2 = 0$. With probability $\frac{1}{2}$ the board will send a bad a_2, resulting in the player winning with probability p exactly 1 out of the 2 board games if they send $b_2 = 1$, and doing so with probability 0 otherwise. In total we get that $\mathrm{SVal}(t) = \frac{1}{2} + \frac{1}{2}p$. By taking $p < \frac{3}{4}$, we will get that $P^*_{seq} < P^*_{par}$ (because then $\frac{1}{2} + 2p\,(1-p) > \frac{1}{2} + \frac{1}{2}p$). ◀

In the quantum setting, we already saw that parallel can achieve better value, in our coin flipping example in section 2. We conclude that there is no general connection between the value of the parallel setting and the sequential setting. In parallel, you know the rest of the questions before giving an answer to question 1, while in sequence you know the outcomes of all previous games before you have to give an answer. Either one might be beneficial, depending on the situation.

Quantum Hedging in Two-Round Prover-Verifier Interactions*

Srinivasan Arunachalam[1], Abel Molina[2], and Vincent Russo[3]

1 **QuSoft, CWI, Amsterdam, The Netherlands**
srinivasan1390@gmail.com
2 **Institute for Quantum Computing and David R. Cheriton School of Computer Science, University of Waterloo, Ontario, Canada**
abelmolinauw@gmail.com
3 **Institute for Quantum Computing and David R. Cheriton School of Computer Science, University of Waterloo, Ontario, Canada**
vincentrusso1@gmail.com

Abstract

We consider the problem of a particular kind of quantum correlation that arises in some two-party games. In these games, one player is presented with a question they must answer, yielding an outcome of either "win" or "lose". Molina and Watrous [30] studied such a game that exhibited a perfect form of *hedging*, where the risk of losing a first game can completely offset the corresponding risk for a second game. This is a non-classical quantum phenomenon, and establishes the impossibility of performing strong error-reduction for quantum interactive proof systems by parallel repetition, unlike for classical interactive proof systems. We take a step in this article towards a better understanding of the hedging phenomenon by giving a complete characterization of when perfect hedging is possible for a natural generalization of the game in [30]. Exploring in a different direction the subject of quantum hedging, and motivated by implementation concerns regarding loss-tolerance, we also consider a variation of the protocol where the player who receives the question can choose to restart the game rather than return an answer. We show that in this setting there is no possible hedging for any game played with state spaces corresponding to finite-dimensional complex Euclidean spaces.

1998 ACM Subject Classification F.1.0 Computation by Abstract Devices

Keywords and phrases prover-verifier interactions, parallel repetition, quantum information

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.5

1 Overview and motivation

The interactions we study consist of parallel repetitions of a game played between players Alice and Bob, also referred to as the *verifier* and *prover* respectively. The setting of the game is:

1. Alice prepares a question, and sends this question to Bob.
2. Bob generates an answer, and sends it back to Alice.
3. Alice evaluates this answer and decides if Bob wins or loses.

* This work was partially supported by Canada's NSERC, the US ARO, the ERC Consolidator Grant QPROGRESS, the Mike and Ophelia Lazaridis Fellowship program, and the David R. Chariton Graduate Scholarship program.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 5; pp. 5:1–5:30
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

It is assumed that Bob has complete knowledge of Alice's specification, including both the method used to determine Alice's question and the criteria that she uses to determine whether Bob has won or lost the game.

Molina and Watrous [30] consider a specific instance of this setting where Alice sends half of a 2-qubit Bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ to Bob. Bob replies with a qubit and Alice evaluates Bob's answer by measuring his qubit and the second half of the Bell state against the state $\cos(\pi/8)|00\rangle + \sin(\pi/8)|11\rangle$. A victory for Bob corresponds to the outcome of Alice measurement corresponding to $\cos(\pi/8)|00\rangle + \sin(\pi/8)|11\rangle$. When Alice and Bob play two repetitions of this game in parallel, the results in [30] show that there exists a strategy for Bob that guarantees he wins *at least one* of the two repetitions with probability 1. However, when the game is played once, the probability that Bob wins is at most $\cos(\pi/8)^2 \approx 0.8536$. Playing two repetitions in parallel leads then to a *hedging* phenomenon, where if Bob wants to decrease his chance of losing both repetitions, he can do so by not playing each game independently and optimally. This hedging is also *perfect*, in the sense that Bob can completely offset the risk of losing both games.

This is a completely quantum phenomenon, with no classical counterpart. Indeed, when classical information is considered, and for any game that fits the setting we study, it is immediate to show that when Bob wants to win at least k out of n parallel repetitions, it is optimal for him to play independently (however, this is not the case when considering multiple provers [18, 16, 34, 24, 8]). This establishes the non-triviality of the set of outcome distributions that are possible to obtain from parallel repetition of the games that we study, when compared to the classical case. In particular, it immediately illustrates that the technique of parallel repetition cannot be used to trivially achieve strong error reduction for the complexity class QIP(2), a class studied for example in [35, 42, 25, 23]. The quantum hedging phenomenon is also an example where the quantum version of a game produces outcomes unachievable by its classical counterpart. Most famously considered by Bell [6], this type of violation has been observed in a number of game-like frameworks [13, 29, 32, 14, 9, 36, 15].

It is natural then to ask how general is the hedging phenomenon, both qualitatively and quantitatively. A complete understanding of this question would allow us to characterize the outcome distributions that can arise from Alice and Bob playing n parallel repetitions of a prover-verifier game in our setting. Consequently, it could lead to a protocol for achieving error reduction via parallel repetition for QIP(2) simpler than the one currently known [25]. The techniques used to achieve such an understanding could conceivably also extend to the analysis of prover-verifier games involving further rounds of communication, and more generally to other kinds of multi-party quantum interactions. This would lead to results for the corresponding complexity classes (and likely also for their classical parallels) about error reduction by parallel repetition. Taking a step towards such a complete understanding, we consider in Section 3 a 2-parameter generalization of the game in [30], and characterize when Bob can guarantee that he wins at least 1 out of n parallel repetitions, for every n. We also give optimal strategies for Bob to win at least 1 out of n parallel repetitions, both when perfect hedging is possible and not possible. We believe these findings are a valuable stepping stone towards a more complete understanding of hedging behaviors for fully arbitrary initial states, fully arbitrary quantum measurements, and k-out-of-n settings, as well as highly non-trivial from a mathematical point of view. The formulas that we obtain also open the door for connections between the hedging phenomenon and recent work [5] involving generalizations of the PBR game [33], as we will discuss further in Section 5.

Exploring in a different direction the subject of quantum hedging, it also seems natural to consider the possibility of implementing a game that exhibits quantum hedging using existing quantum information processing devices. One possible choice would be to use

optical quantum devices, but the immediate concern arises [38] of how to account for the fact that photon losses will often occur, leading to a communication error between Alice and Bob. Even if one chose another implementation method where communication is more reliable, one would still need to consider the general fact that communication errors can occur. More generally, the consideration of implementation inaccuracies is a standard direction in which to extend results concerning quantum information protocols – see for example recent work regarding loss-tolerant protocols for quantum coin-flipping [2] and QKD, [39] and noise-tolerant protocols for quantum money [31], quantum coin-flipping [44] and quantum randomness amplification [7].

Along this direction, we consider a loss-tolerant formalism in Section 4, and prove that under our formalism quantum hedging is not possible. To model communication errors, we assume that Alice cannot distinguish a communication error from Bob choosing not to return an answer. Therefore, our formalism simply allows for the possibility that Bob chooses not to return an answer, in which case the game is repeated. Bob choosing in our formalism a random whether to return an answer or not would correspond to a genuine disruption of communication, while Bob strategizing about when to return an answer would correspond to Bob using communication errors as an excuse to avoid a losing outcome. Our particular choice of framework can also be seen as adding postselection to two-round quantum prover-verifier interactions. This addition of post-selection has been previously considered in the case of single-party quantum computation [1, 37, 43, 28], but not to our knowledge in the context of quantum prover-verifier interactions.

The techniques used to obtain our results in Section 4 are inspired by the techniques in [17], which studies a particular case of quantum cloning. The connection between quantum cloning and semidefinite programming was observed in [4], and has been used to obtain results regarding quantum cloning (see the review in [10]). However, this is the first time to our knowledge that this connection with semidefinite programming acts as a bridge to apply ideas about optimal quantum cloning to the context of fully general two-round quantum prover-verifier interactions.

Both of our results leave room for further progress. In particular, one can consider hedging in a wider context than the setting in Section 3, and consider formalisms that model communication errors in a different way than in Section 4. We give some suggestions in Section 5 concerning corresponding choices for further exploration.

2 Notation

We will denote the set of binary strings with length n as $\{0,1\}^n$. These strings will be indexed from 0 to $n-1$. Therefore, we will denote the n successive binary symbols or bits in $a \in \{0,1\}^n$ as $a_0, \ldots a_{n-1}$. $\wedge r, \vee r$, and $\bigoplus r$ refer to the logical AND, OR, and XOR of the bits of $r \in \{0,1\}^n$, respectively, while $|r|$ refers to its Hamming weight.

Vector spaces associated with a quantum system are defined as complex Euclidean spaces. We denote these spaces by the capital script letters $\mathcal{X}, \mathcal{Y}$, and $\mathcal{Z}$. The dual x^* of a vector x in a complex Euclidean vector space $\mathcal{X}$ will be the linear functional (i.e. the map $\mathcal{X} \to \mathbb{C}$) that maps y to $\langle x, y\rangle$. For a d-dimensional complex Euclidean space, we will often fix a standard *computational* basis and, using bra-ket notation, address its elements and their duals as $\{|0\rangle, \ldots, |d-1\rangle\}$ and $\{\langle 0|, \ldots, \langle d-1|\}$, respectively. The encoding of the label inside a bra or a ket will often be done in binary for ease of explanation.

The complex vector space of linear operators of the form $A : \mathcal{X} \to \mathcal{Y}$ is denoted by $\mathrm{L}(\mathcal{X}, \mathcal{Y})$. We write $A \in \mathrm{L}(\mathcal{X})$ as a shorthand for $A : \mathcal{X} \to \mathcal{X}$. The adjoint X^* of an operator

$X \in \mathrm{L}(\mathcal{X})$ is the operator such that for all $u, v \in \mathcal{X}$, $\langle u, Xv\rangle = \langle X^* u, v\rangle$. An operator $H \in \mathrm{L}(\mathcal{X})$ is *Hermitian* if $H = H^*$. We write $\mathrm{Herm}(\mathcal{X})$ to denote the set of all Hermitian operators. The inner product $\langle A, B\rangle = \mathrm{Tr}(AB)$ between two operators $A, B \in \mathrm{Herm}(\mathcal{X})$ is real and satisfies $\langle A, B\rangle = \langle B, A\rangle$. If an operator $P \in \mathrm{Herm}(\mathcal{X})$, and all eigenvalues of P are non-negative, then we call P *positive semidefinite*, and refer to all such operators as $P \in \mathrm{Pos}(\mathcal{X})$. For a Hermitian operator H, $\|H\|$ denotes the operator norm of H, that is, the largest absolute value of an eigenvalue. If for an operator $\rho \in \mathrm{Pos}(\mathcal{X})$ it is the case that $\mathrm{Tr}(\rho) = 1$, then ρ is said to be a *density operator*, and is referred to as $\rho \in \mathrm{D}(\mathcal{X})$. We adopt the convention of writing $\mathcal{I}_{\mathcal{X}}$ as opposed to $\mathcal{I}$ to indicate that the identity is acting on the space $\mathcal{X}$ when convenient to do so. We will define the $\mathrm{vec} : \mathrm{L}(\mathcal{X}, \mathcal{Y}) \to \mathcal{X} \otimes \mathcal{Y}$ mapping to be the one that takes yx^* to $x \otimes y$, for x and y elements of the standard/computational basis of $\mathcal{X}$ and $\mathcal{Y}$. This can be seen as flattening a matrix into a vector. For any two operators $A, B \in \mathrm{L}(\mathcal{X}, \mathcal{Y})$, it will hold that $\langle A, B\rangle = \langle \mathrm{vec}\,(A), \mathrm{vec}\,(B)\rangle$.

We also consider linear mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$. The space of all such mappings is denoted as $\mathrm{T}(\mathcal{X}, \mathcal{Y})$. For each $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, a unique adjoint mapping $\Phi^* \in \mathrm{T}(\mathcal{Y}, \mathcal{X})$ is defined by the property that $\langle Y, \Phi(X)\rangle = \langle \Phi^*(Y), X\rangle$ for all $X \in \mathrm{L}(\mathcal{X})$ $Y \in \mathrm{L}(\mathcal{Y})$. Throughout this work, we define quantum states by the set of density operators $\rho \in \mathrm{D}(\mathcal{X})$, with $\mathcal{X}$ a complex Euclidean space. Associated with the space $\mathcal{X}$ one may consider a *register* denoted X in which the state ρ is contained. We consider measurements of a register X as being described by a set of positive semidefinite operators $\{P_a : a \in \Sigma\}$ indexed by a finite non-empty set Σ of measurement outcomes which satisfies the constraint $\sum_{a\in\Sigma} P_a = \mathcal{I}_{\mathcal{X}}$. By performing a measurement on X in state ρ, the outcome $a \in \Sigma$ results with probability $\langle P_a, \rho\rangle$. These measurements are known as POVMs. We can also consider quantum states stored across n registers $(\mathsf{X}_1, \mathsf{X}_2, \cdots, \mathsf{X}_\mathsf{n})$. We can describe the joint state of those registers by a density operator $\sigma \in \mathrm{D}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n)$.

A linear mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ is said to be *completely positive* if $\Phi \otimes \mathcal{I}_{\mathcal{Z}}$ is a map that preserves positive semidefiniteness for every complex Euclidean space $\mathcal{Z}$ and Φ is said to be *trace-preserving* if $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ for all $X \in L(\mathcal{X})$. We define a *quantum channel* as a linear mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ that is completely positive and trace preserving. A channel transforms some state ρ stored in register X into the state $\Phi(\rho)$ of another register Y. The set of all channels between such two registers is denoted by $\mathrm{C}(\mathcal{X}, \mathcal{Y})$, and is a compact and convex set. Note that the channel corresponding to an unitary operator U is the one that maps a quantum state σ to $U\sigma U^*$.

For spaces $\mathcal{X}$ and $\mathcal{Y}$, one may define the Choi representation of an operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as $J(\Phi) = \sum_{i,j} \Phi\left(|i\rangle\langle j|\right) \otimes |i\rangle\langle j|$, where $J : \mathrm{T}(\mathcal{X}, \mathcal{Y}) \to \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$, and i and j iterate over the computational basis for $\mathcal{X}$. Note that the mapping J is linear, bijective, and multiplicative with respect to the tensor product. The Choi representation has a number of more complex properties, three of which will be useful to us:

▶ **Lemma 1.**
1. *The mapping Φ is completely positive if and only if $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$.*
2. *The mapping Φ is trace preserving if and only if $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathcal{I}_{\mathcal{X}}$*
3. $\Phi(Z) = \mathrm{Tr}_{\mathcal{X}}\left[J(\Phi)\left(\mathcal{I}_{\mathcal{Y}} \otimes Z^T\right)\right]$

We refer the reader to [41] for the proof of Lemma 1 and further details on the notation.

3 Hedging to win 1 out of n parallel repetitions of a game

Let G denote the following game:

1. Alice prepares the 2-qubit state $\rho_\alpha = u_\alpha u_\alpha^* \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$ in registers (X, Z) where

$$u_\alpha = \alpha \left|00\right\rangle + \sqrt{1-\alpha^2}\left|11\right\rangle \in \mathcal{X} \otimes \mathcal{Z}, \tag{1}$$

   for $\alpha \in (0, 1]$. Alice sends register X to Bob.
2. Bob applies a channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ to the contents of X. This results in a state $\sigma \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{Z})$, contained in registers (Y, Z). Register Y is sent back to Alice.
3. Alice performs a measurement on the state σ. This measurement is $\{P_{0,\theta}, P_{1,\theta}\}$ for $\theta \in [0, 2\pi)$, with

$$\begin{aligned} P_{1,\theta} = v_\theta v_\theta^*,\ P_{0,\theta} = \mathcal{I} - P_{1,\theta}, \\ v_\theta = \cos(\theta)\left|00\right\rangle + \sin(\theta)\left|11\right\rangle \in \mathcal{Y} \otimes \mathcal{Z}. \end{aligned} \tag{2}$$

   An outcome of "0" or "1" denotes a losing or winning outcome for Bob, respectively.

One can imagine repeating the game G n times in parallel. This is denoted as G^n, and illustrated in Figure 1. In this setting, Alice prepares n states $\rho_{1,\alpha}, \ldots, \rho_{n,\alpha}$ in registers $((\mathsf{X}_1, \mathsf{Z}_1), \cdots, (\mathsf{X}_n, \mathsf{Z}_n))$ where

$$\rho_{1,\alpha} \in \mathrm{D}(\mathcal{X}_1 \otimes \mathcal{Z}_1), \ldots, \rho_{n,\alpha} \in \mathrm{D}(\mathcal{X}_n \otimes \mathcal{Z}_n). \tag{3}$$

Alice sends the registers $(\mathsf{X}_1, \ldots, \mathsf{X}_n)$ to Bob and he applies his quantum channel,

$$\Phi_n \in \mathrm{C}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n). \tag{4}$$

The resulting states are sent back to Alice and she performs a series of n projective measurements with respect to the operators $P_{0,\theta}, P_{1,\theta}$. These give n outcomes of either 0 or 1, loss or win. Since Bob's actions are not required to respect the independence of the measurements, they may cause correlations between the n measurement outcomes.

Indeed, in [30], Molina and Watrous analyzed G^n for $n = 2$ where $\alpha = 1/\sqrt{2}$ and $\theta = \pi/8$, and found that Bob wins one out of the two games with certainty if he applies a specific correlated strategy. If on the other hand, Bob treated each repetition independently, it would *not* be guaranteed that Bob would win at least one of the games.

We consider G^n for any $n \geq 1$ and ask for what values of α and θ is it true that Bob can make sure to win with certainty *at least* one out of the n games in G^n. Let $p_{n,\alpha,\theta}(\Phi_n) \in [0, 1]$ be the probability that Bob loses all n outcomes of G^n using the strategy defined by Φ_n. This is given by:

$$p_{n,\alpha,\theta}(\Phi_n) = \left\langle P_{0,\theta}^{\otimes n}, (\Phi_n \otimes \mathcal{I}_{\mathcal{Z}_1 \otimes \cdots \otimes \mathcal{Z}_n}) \left(\bigotimes_{i=1}^{n} \rho_{i,\alpha} \right) \right\rangle. \tag{5}$$

Let $m_{n,\alpha,\theta} \in [0, 1]$ be $\min_{\Phi_n} p_{n,\alpha,\theta}(\Phi_n)$. We refer to a quantum channel Φ_n that minimizes $m_{n,\alpha,\theta}$ as an *optimal strategy*. That is, equal to the *minimum probability* with which Bob loses each game over all choices of quantum channels Φ_n of the form in (4). If $m_{n,\alpha,\theta}$ evaluates to 0, then there exists a Φ_n that ensures Bob wins at least one game.

The quantity $m_{n,\alpha,\theta}$ is expressible as the optimal value of a semidefinite program. Let $Q_{0,\alpha,\theta} \in \mathrm{Pos}(\mathcal{Y}_i \otimes \mathcal{X}_i)$ be defined as

$$Q_{0,\alpha,\theta} = (\mathcal{I}_{\mathcal{Y}_i} \otimes \Psi_{\rho_\alpha})(P_{0,\theta}), \tag{6}$$

where the mapping $\Psi_{\rho_\alpha} : \mathrm{L}(\mathcal{Z}) \to \mathrm{L}(\mathcal{X})$ is defined by $J(\Psi_{\rho_\alpha}) = \overline{\rho_\alpha}$ (the entry-wise complex conjugate of ρ_α). This makes $Q_{0,\alpha,\theta}$ a function of both $P_{0,\theta}$ and ρ_α.

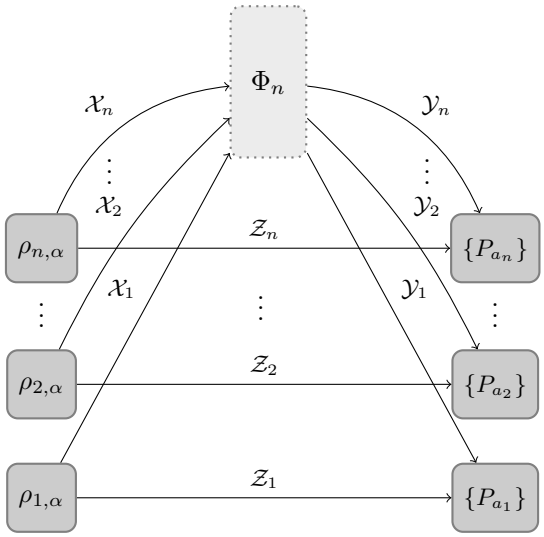

Figure 1 The parallel repetition G^n of n copies of a game G of the type we study.

It follows from Lemma 1 of [30] that Q_0 is positive semidefinite, and that for any channel $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$, we have $\langle P_{0,\theta}, (\Phi \otimes \mathcal{I})(\rho_{i,\alpha})\rangle = \langle Q_{0,\theta}, J(\Phi)\rangle$. This can be proved by considering the case where $\rho_{i,\alpha}$ corresponds to a rank-1 operator that transforms a state of the computational basis into another one, and then using the linearity properties of the inner product (see Appendix A.1 for more details of this derivation). Putting this together with facts 1 and 2 about the Choi representation in Lemma 1, and the bijective property of the $J(\cdot)$ map, we obtain that the following primal and dual pair gives a semidefinite program to compute $m_{n,\alpha,\theta}$:

$$\underline{m_{n,\alpha,\theta}\text{: Primal problem}}$$

$$\begin{aligned} \text{minimize:} \quad & \left\langle Q_{0,\alpha,\theta}^{\otimes n}, X \right\rangle \\ \text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}_1\otimes\cdots\otimes\mathcal{Y}_n}(X) = \mathcal{I}_{\mathcal{X}_1\otimes\cdots\otimes\mathcal{X}_n}, \\ & X \in \mathrm{Pos}(\mathcal{Y}_1 \otimes \mathcal{X}_1 \otimes \cdots \otimes \mathcal{Y}_n \otimes \mathcal{X}_n). \end{aligned} \tag{7}$$

$$\underline{m_{n,\alpha,\theta}\text{: Dual problem}}$$

$$\begin{aligned} \text{maximize:} \quad & \mathrm{Tr}(Y) \\ \text{subject to:} \quad & \pi\left(\mathcal{I}_{\mathcal{Y}_1\otimes\cdots\otimes\mathcal{Y}_n} \otimes Y\right)\pi^* \leq Q_{0,\alpha,\theta}^{\otimes n}, \\ & Y \in \mathrm{Herm}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n). \end{aligned} \tag{8}$$

where π is a unitary permutation operator defined by the action

$$\pi(y_1 \otimes \cdots \otimes y_n \otimes x_1 \otimes \cdots \otimes x_n) = y_1 \otimes x_1 \otimes \cdots \otimes y_n \otimes x_n$$

for all $y_1 \in \mathcal{Y}_1, \cdots, y_n \in \mathcal{Y}_n$ and $x_1 \in \mathcal{X}_1, \cdots, x_n \in \mathcal{X}_n$. Note that strong duality holds for the above semidefinite program, by choosing the primal and dual feasible solutions (X, Y) for the application of Slater's theorem as a scalar multiple of the identity. The derivation to obtain this semidefinite program is similar to that in [30], and previously in [22] and [21]. We point the reader to [3] for MATLAB code that solves SDPs (7) and (8), using the CVX convex optimization package [20].

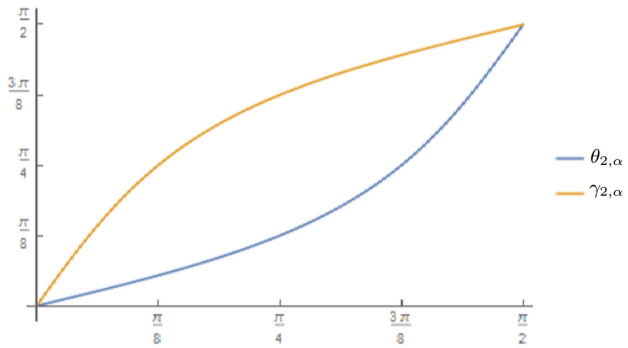

Figure 2 $\gamma_{2,\alpha}$ and $\theta_{2,\alpha}$ as a function of $\tan^{-1}\left(\frac{\sqrt{1-\alpha^2}}{\alpha}\right)$.

We present now for fixed n and α the range of θ which characterizes the measurements for which Bob can make sure he wins at least 1 parallel repetition in G^n. That is, it characterizes when is Bob able to perform perfect hedging. Furthermore, we present strategies that give Bob an optimal probability to win at least 1 out of n games, both when Bob is able to perform perfect hedging and when he is not.

▶ **Theorem 2.** *Let*

$$\begin{aligned}\theta_{n,\alpha} &= \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(2^{1/n}-1\right)\right),\\ \gamma_{n,\alpha} &= \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(\frac{1}{2^{1/n}-1}\right)\right),\end{aligned} \tag{9}$$

where the trigonometric domain is restricted to $[0,\pi/2]$*. If and only if Alice's rank-1 projective measurement* $\{P_0,P_1\}$ *is parametrized by* $\theta\in[\theta_{n,\alpha},\gamma_{n,\alpha}]$*, then there exists a strategy for Bob to perform perfect hedging.*

We see then that the angle $\pi/8$ used for θ in [30] corresponds to the lower bound $\theta_{2,1/\sqrt{2}}=\pi/8$ from Theorem 2, but also that perfect hedging can be attained for this setting up to $\gamma_{2,\frac{1}{\sqrt{2}}}=3\pi/8$. Note that as the number of games n increases, the size of this range increases. Moreover, for any choice of θ in $(0,\pi/2)$, there is an n large enough for perfect hedging to be possible. As one can see in our plot of $\theta_{n,\alpha}$ and $\gamma_{n,\alpha}$, the cases where perfect hedging are posssible are symmetric with respect to the case where the initial state and the desired final state are the same (i.e., $\theta=\tan^{-1}(\sqrt{1-\alpha^2}/\alpha)$). Note also that the size of the range where perfect hedging is possible is minimized for $\theta=0$ and $\theta=\pi/2$, which correspond to a standard basis measurement done by Alice.

The proof of Theorem 2 follows immediately from Lemma 5 and Lemma 6, stated below. Theorem 2 results in the following corollary:

▶ **Corollary 3.** *For a fixed* n*, perfect hedging occurs for the largest range of* θ *angles when Alice initially prepares a maximally entangled state (that is, when* $\alpha=\frac{1}{\sqrt{2}}$*).*

The proof for the corollary follows from directly maximizing $\gamma_{n,\alpha}-\theta_{n,\alpha}$ over all α, by taking derivatives with respect to α. The corollary tells us then that the maximally entangled represents an extremal case in our quantum hedging context. One might be able to use this when trying to generalize our results, as we will further discuss in Section 5.

In the following lemmas, we define an optimal choice for Bob of the channel Φ that he applies to the input he receives from Alice:

▶ **Lemma 4.** *Let $n \geq 2$ be a positive integer, let $\alpha \in (0,1]$, let $\theta_{n,\alpha}$ and $\gamma_{n,\alpha}$ be angles defined as in Theorem 2, and let*

$$\begin{aligned} \Lambda_n &= \sum_{r\in\{0,1\}^n} (-1)^{\wedge r+\oplus r} \left|r\right\rangle \left\langle r\right|, \\ \Xi_n &= \sum_{r\in\{0,1\}^n} (-1)^{\vee r+\oplus r} \left|r\right\rangle \left\langle r\right|, \end{aligned} \tag{10}$$

be unitary operators that Bob applies as his strategy in G^n. Then it holds that

$$p_{n,\alpha,\theta_{n,\alpha}}\left(\Lambda_n\right) = 0 = p_{n,\alpha,\gamma_{n,\alpha}}\left(\Xi_n\right). \tag{11}$$

This shows the existence of strategies $\{\Lambda_n, \Xi_n\}$ for Bob at $\{\theta_{n,\alpha}, \gamma_{n,\alpha}\}$ that achieve a value of 0 for the SDP (7). The next lemma proves that for all points within these two bounds there exists such a strategy as well. Note that Λ_n and Ξ_n do not depend on α. Also, note that when $n = 2$, Bob's unitary Λ_2 on the two qubits that he receives is

$$\Lambda_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \tag{12}$$

which gives us the same strategy as in [30]. The proof of the lemma follows from observing that the final state after Bob applies $\Lambda_n/\ \Xi_n$ has zero overlap with the state corresponding to Bob losing all the repetitions. The details of the derivation are included in Appendix A.2.

▶ **Lemma 5.** *In the scenario where the projective measurements are parametrized by $\theta \in [\theta_{n,\alpha}, \gamma_{n,\alpha}]$ for $\theta_{n,\alpha}$ and $\gamma_{n,\alpha}$ defined as in Theorem 2, Bob can apply the strategy corresponding to the following unitary operator to achieve perfect hedging for 1 out of n games:*

$$(-1)^n |0^n\rangle\langle 0^n| - |1^n\rangle\langle 1^n| + \sum_{i=1}^{n-1} \sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} (-1)^{n+i} k_r \left|r\right\rangle \left\langle r\right|, \tag{13}$$

where for a fixed choice of $|r| = i$, the corresponding k_r are $\binom{n}{i}$ complex numbers with the following properties

$$k_r = \begin{cases} s_{\theta,\alpha,n} + i\sqrt{1 - s_{\theta,\alpha,n}^2} \text{ for } \left\lfloor \binom{n}{i}/2 \right\rfloor \text{ values of } r, \\ s_{\theta,\alpha,n} - i\sqrt{1 - s_{\theta,\alpha,n}^2} \text{ for } \left\lfloor \binom{n}{i}/2 \right\rfloor \text{ values of } r, \\ -1 \text{ for the remaining values of } r \text{ when } \binom{n}{i} \text{ is} \\ \text{ odd and } \tan(\theta) \geq \sqrt{\frac{1}{\alpha^2} - 1}, \\ 1 \text{ for the remaining values of } r \text{ when } \binom{n}{i} \text{ is odd} \\ \text{ and } \tan(\theta) < \sqrt{\frac{1}{\alpha^2} - 1}, \end{cases}$$

where $s_{\theta,\alpha,n}$ is a real number $\in [-1, 1]$ whose existence we guarantee in the proof of this lemma.

Since Bob has complete knowledge of the game, for any $\theta \in [\theta_{n,\alpha}, \gamma_{n,\alpha}]$ Bob can apply the strategy corresponding to the angle θ selected by Alice. It is clear that the optimal strategy for Bob is not unique, since our definition does not uniquely specify which coefficients k_r correspond to which values of r. This lemma is derived by performing a computation (similar to the one for Lemma 4) that computes the overlap between the resulting state after Bob applies the strategy we describe and the state corresponding to Bob losing all n repetitions. Then, we consider the cases $s_{\theta,\alpha,n} = -1$ and $s_{\theta,\alpha,n} = 1$ and obtain through continuity arguments that there must be a value of $s_{\theta,\alpha,n}$ in the $[-1, 1]$ range that results in perfect hedging. The details of the corresponding derivation are included in Appendix A.3.

We have thus far considered the case when perfect hedging is possible. The following result deals with characterizing the scenario when perfect hedging is not possible, and provides a corresponding strategy for Bob to play optimally.

▶ **Lemma 6.** *For $n \geq 2$ and for $\theta \in [0, \theta_{n,\alpha}) \cup (\gamma_{n,\alpha}, \pi/2]$ perfect hedging cannot occur, and the strategies Λ_n and Ξ_n mentioned in Lemma 4 are respective optimal strategies for Bob.*

The proof of this lemma is obtained by using SDP complementary slackness [40] to obtain a candidate solution for the dual SDP (8) with the same objective value as the chance of achieving 1-out-of-n hedging for Λ_n/Ξ_n. Then, one can use a direct sum decomposition of the matrices involved in the SDP constraint to prove the feasibility of this candidate solution. The details of the corresponding calculations are available in Appendix A.4. Note that the strategy Bob adopts is independent of the parameter θ, implying that when perfect hedging is not possible the strategy is optimal regardless of the projective measurements chosen by Alice.

It can also be observed from Lemma 5 and Lemma 6 that a unitary (and in fact, a diagonal in the computational basis) strategy is always sufficient for Bob to win at least once with optimal probability. Note that it intuitively makes sense that Bob's strategy is a diagonal unitary, since switching a $|0\rangle$ to a $|1\rangle$ or vice-versa on his side will produce a state with no overlap with the target state $\cos(\theta)|00\rangle + \sin(\theta)|11\rangle$.

4 (Lack of) Hedging in a Loss-Tolerant Prover-Verifier Model

We consider a variation of the prover-verifier setting where Bob has the choice to not respond to Alice, in order to model communication errors, as described in Section 1. If Bob chooses not to respond, and therefore Alice does not receive an answer, the game is repeated again, and this goes on until an answer is returned by Bob. Bob might want to do this whenever using his complete knowledge of the game, he can predict that an answer will result in Alice obtaining a negative outcome in her measurement. Indeed, to see how this variation can change the result of an interaction, consider the following game where Bob is always forced to return an answer:

1. Alice prepares the maximally entangled state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and sends the second qubit to Bob.
2. Bob responds by sending a qubit to Alice.
3. Alice ignores Bob's answer, and measures the qubit she kept with respect to the projective measurement $\{P_0, P_1\}$, where $P_0 = |1\rangle\langle 1|$ and $P_1 = |0\rangle\langle 0|$.

It is clear that the maximum probability for Bob to win the game is 50%. This follows from the fact that the actions of Bob cannot alter the reduced state that Alice holds, and the outcome of the interaction depends only on this state. However, the situation changes drastically when Bob is allowed to return no answer in the second step. In that case, Bob

can choose to perform a measurement using the computational basis on the qubit he receives. If the measurement results in the outcome $|0\rangle$, corresponding to P_1, he will return an answer, and otherwise he will not, and force a restart. The entanglement between the qubit that Alice keeps and the one that Bob receives guarantees then that the outcome will always be the successful one.

It seems clear then that giving Bob the choice to abort the protocol can have significant changes on what optimal behaviors for Bob are like. This motivates the consideration of whether any form of quantum hedging (perfect or not) is still possible in the "repetition after communication error" setting for an arbitrary two-message quantum-verifier interaction (described by an arbitrary finite-dimensional inital quantum state ρ prepared by Alice and an arbitrary finite-dimensional POVM $\{P_i\}$ used to determine the interaction's outcome.) We ask in this context then whether it will be optimal for Bob to play each interaction independently when trying to optimize his chance of winning at least k out of n parallel interactions.

To answer this question, we will assume in our analysis that Bob always has a nonzero chance of winning a single interaction. If this were not the case, the question of whether or not hedging occurs would be uninteresting. This is because in this case, the optimal probability for Bob to win k out of n parallel repetitions would always be zero. To see why, assume to the contrary that Bob can manage to win $k > 0$ out of $n > 1$ repetitions with non-zero probability. Then, whenever Bob plays a single game with Alice, he could simulate the input for $n-1$ additional interactions, and since the possibility that he wins $k > 0$ of the n games is greater than zero, and the situation is symmetrical, the possibility that he wins the single "real" game is greater than zero as well, which contradicts our starting premise.

Furthermore, we need to specify how does the "repetition after communication error" aspect of the framework interacts with the "repeating n interactions in parallel" aspect of the framework. For simplicity, we will make in our model the assumption that whenever Alice does not receive an answer to one out of n parallel interactions, she will restart all of the n parallel interactions.

To start our analysis, we consider an intermediate setting where we allow Bob to not give an answer, and Alice does not repeat the interaction when she doesn't obtain an answer, and instead counts that as a loss for Bob. This means that Bob can return a state with trace less than one. Using the properties of the Choi representation, and following the same analysis as in [30] and Section 3, the optimal probability for Bob of achieving outcome a is the value of

Primal problem

$$\begin{aligned} \text{maximize:} \quad & \langle Q_a, X \rangle \\ \text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathcal{I}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}\left(\mathcal{Y} \otimes \mathcal{X}\right), \end{aligned} \tag{14}$$

where Q_a is defined as in (6), starting from an arbitrary POVM $\{P_i\}$ and a state ρ. Without loss of generality, we assume that Bob wants to achieve quantum hedging with respect to outcome a, and group all other outcomes into a single outcome corresponding to Q_{1-a}.

Now we take into account the fact that the interaction is repeated whenever an answer is not received. To do this, it is enough to divide the objective function, which corresponds to the probability of obtaining outcome a, by the probability that an answer is returned. This is because we can ignore previous rounds of the interaction, since the repeated rounds occur in series, and Alice acts independently between them. Indeed, the way in which previous rounds would be taken into account would be with an additional input for Bob, corresponding to his

memory after the previous rounds of the protocol. But the fact that there is no computational restriction on Bob and no hidden information means that for any possible value of that input, Bob could just simulate the previous rounds to generate it, so the additional memory input is not needed, and we can ignore previous rounds.

Note that the division by the probability that Bob returns an answer would not be possible if Bob just chose not to return an answer. However, that strategy can just be ignored as a non-optimal one, since we are assuming Bob can win with non-zero probability.

The probability that an answer is returned is the trace of the state after Bob returns an answer, which is a linear function of the variable X in SDP (14). In particular, the probability is given by $\langle E, X\rangle$, where

$$\begin{aligned} E &= \sum_i Q_i = \sum_i \left(\mathcal{I}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi_\rho\right)(P_i) \\ &= \left(\mathcal{I}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi_\rho\right) \mathcal{I}_{\mathcal{Y}\otimes\mathcal{Z}} = \mathcal{I}_{\mathcal{Y}} \otimes \mathrm{Tr}_{\mathcal{Z}}(\overline{\rho}), \end{aligned} \tag{15}$$

and the last step uses the third fact in Lemma 1. Note that since $\sum_i Q_i = E$, $Q_a \leq E$.

This tells us then how to modify the SDP (14) that describes Bob's optimal probability of obtaining outcome a in a way that takes into account our loss-tolerant framework. In particular, we have that the equivalent of SDP (14) is now given by

$$\begin{array}{ll} & \underline{\text{Primal problem}} \\ \text{maximize:} & \dfrac{\langle Q_a, X\rangle}{\langle E, X\rangle} \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathcal{I}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}\left(\mathcal{Y}\otimes\mathcal{X}\right), \langle E, X\rangle \neq 0. \end{array} \tag{16}$$

We use now an analysis inspired by the one in [10] to obtain a more explicit form for the value of this SDP. First, notice that scaling a solution X by a nonzero constant will not change the value of the objective function. Since the partial trace operation preserves positive semidefiniteness, we can then get rid of the $\mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathcal{I}_{\mathcal{X}}$ constraint:

$$\begin{array}{ll} & \underline{\text{Primal problem}} \\ \text{maximize:} & \dfrac{\langle Q_a, X\rangle}{\langle E, X\rangle} \\ \text{subject to:} & X \in \mathrm{Pos}\left(\mathcal{Y}\otimes\mathcal{X}\right), \langle E, X\rangle \neq 0. \end{array} \tag{17}$$

At this point, we can assume that X corresponds to a rank-one operator. To see why, consider an X that corresponds to a sum of two solutions, X_1 and X_2. Then, the value of the objective function will be

$$\frac{\langle Q_a, X_1\rangle + \langle Q_a, X_2\rangle}{\langle E, X_1\rangle + \langle E, X_2\rangle} \leq \max\left(\frac{\langle Q_a, X_1\rangle}{\langle E, X_1\rangle}, \frac{\langle Q_a, X_2\rangle}{\langle E, X_2\rangle}\right), \tag{18}$$

where the inequality follows from the fact that all values on the left-hand side are positive. We obtain the problem

$$\begin{array}{ll} & \underline{\text{Primal problem}} \\ \text{maximize:} & \dfrac{x^* Q_a x}{x^* E x} \\ \text{subject to:} & x \in \mathcal{Y}\otimes\mathcal{X}, x^* E x \neq 0. \end{array} \tag{19}$$

Note now that we can assume without loss of generality that an optimal solution x is contained within the support of E. In this domain the Moore-Penrose pseudo-inverse of E, E^+, acts as a bijection. Therefore, we replace x by $(E^+)^{1/2}x$ in the objective function, and obtain

$$\begin{array}{ll} & \underline{\text{Primal problem}} \\ \text{maximize:} & \dfrac{x^*(E^+)^{1/2}Q_a(E^+)^{1/2}x}{x^*x} \\ \text{subject to:} & x \in \mathcal{Y} \otimes \mathcal{X}, x \perp \ker(E), \end{array} \tag{20}$$

which has the value $\|(E^+)^{1/2}Q_a(E^+)^{1/2}\|$. We denote this as $\|\Lambda\|$.

When Bob wants to be successful in at least k out of n parallel interactions, with Alice acting independently, one just needs to replace Q_a by the sum of tensor products of Q_i's corresponding to at least k outcomes equal to a. Remembering that the sum of all the Q_i is equal to E, the same analysis that we performed for a single repetition gives us an optimal probability of $\|\Lambda_{k,n}\|$, with $\Lambda_{k,n}$ given by :

$$\left\|(\sqrt{E^+})^{\otimes n}\left(E^{\otimes n} - \sum_{t=0}^{k-1}\pi_t\left(Q_{1-a}^{\otimes n-t}\otimes Q_a^{\otimes t}\right)\right)(\sqrt{E^+})^{\otimes n}\right\| \tag{21}$$

where $\pi_t(x)$ is the sum of all $\binom{n}{t}$ unique permutations of x.

As an aside, note that one can assume that ρ corresponds to a pure state ψ. This is because given a protocol where Alice initially prepares a mixed state, we can easily modify it so that Alice prepares a purification of that state instead, and just ignores the extra qubits when performing the final measurement. Using this, we observe an interesting fact about this model, which is that at least when one restricts Bob to perform a rank-one measurement, the optimal success probability for Bob does not depend on the Schmidt coefficients of ψ. This is proved by letting the initial state that Alice holds be given by $\sum_i \sqrt{p_i}a_i \otimes b_i$, and the state corresponding to Bob's projection by $\sum_i \sqrt{q_i}c_i \otimes d_i$. Using algebraic manipulations we obtain that the optimal probability of winning for Bob in a single parallel repetition is

$$\left\|\sum_{i,j,k,l}\sqrt{q_j q_l}b_i^* d_l d_j^* b_k \overline{a_i a_k}^* \otimes c_j c_l^*\right\|, \tag{22}$$

with no dependence on the p_i.

This suggests that the example we gave at the beginning of this section might capture all the additional power Bob has in this model. In particular, it suggests that an optimal strategy for Bob might always consist of performing an orthogonal measurement on the qubits he is given, and then refusing to give an answer except when he obtains the "best" outcome.

As for our main subject of concern (quantum hedging), it turns out that in the model we just described quantum hedging is not possible. One can interpret this as saying that Bob is already so powerful in one single repetition (since he can choose not to return an answer) than the power to entangle several answers does not add anything in comparison. More precisely, we have the following theorem:

▶ **Theorem 7.** *Consider a two-message prover-verifier interaction characterized by an arbitrary initial state ρ and an arbitrary POVM $\{P_i\}$, both on a finite number of qubits.*

Then, under the loss-tolerant setting described in this section, it is optimal for Bob to play independently in order to maximize his chance of winning at least k out of n parallel interactions.

The statement of the theorem results from a straightforward spectral analysis of the $\Lambda_{k,n}$ operator by induction on n and then k. The details of the corresponding computation are included in Appendix A.5.

5 Discussion

We have analyzed generalizations of a specific prover-verifier interaction where the verifier can use a quantum hedging strategy to win at least one of n parallel repetitions with a higher probability than what would have been possible playing each game independently. This interesting phenomenon was originally described in [30], where the authors illustrated an explicit example of perfect hedging when two repetitions of the game were carried out. It was previously unknown how the perfect hedging phenomenon generalizes to the case when n repetitions of the game are performed. We resolved this question for a generalization of the game in [30], and provided strategies for Bob that allow him to achieve perfect hedging whenever it is possible.

We also analyzed a variant of this setting where Bob is not obligated to return an answer to Alice. In a practical sense, Bob's refusal to respond to Alice can be viewed in terms of an experimental setup where the lack of a response could correspond to a communication error [38]. This consideration led to a different semidefinite program that characterized the interaction between Alice and Bob. We then used this SDP (16) to ask whether or not Bob still had the ability to take advantage of hedging behavior, with a negative answer.

While we have considered this hedging behavior in a number of settings, there are still many questions remaining. As mentioned, we have characterized the conditions that allow Bob to win 1 out of n repetitions in a framework that generalizes the game in [30]. However, it still remains open to determine the conditions under which Bob can always win at least k out of n repetitions for some $k > 1$. It would be interesting to determine the threshold of k for which perfect hedging occurs, and to also provide a characterization in regards to the strategy that Bob uses to achieve this result. Running numerical instances for higher values of k and n using a simple formulation in CVX [20] quickly becomes computationally infeasible, as can be observed from the software we have provided in [3]. It is possible that this code could be optimized to consider further cases, leading to conjectures regarding the behavior for arbitrary k and n that could be then proved analytically. Based on our current numerical evidence, it is possible that Bob cannot perfectly hedge more than $k = n/2$ games. Note also that when $k \leq n/2$ one can design a strategy for the goal of winning k out of n repetitions by dividing the n parallel repetitions into several smaller groups, and then using the strategies described in this paper in order to always win at least one repetition in each group. It is left as an open question (whose solution we believe to be a significant task) whether the range of parameters in which the resulting strategy always wins k out of n repetitions is the optimal one. Motivated by our results in Corollary 3, one could also look into the subject of reducibility between different games in our framework, asking for example whether there is a procedure with an intuitive operational description that transforms a game with an arbitrary shared initial state between Alice and Bob to one where the initial shared state is now maximally entangled, while the possibilities of achieving k-out-of-n hedging remains the same.

It is also worth noting that the problem of conclusive state exclusion, which was recently considered in [5], seems to be connected to the interaction we have analyzed in this work. In this problem, Alice prepares a mixed state from a given distribution and sends it to Bob, and for Bob to win, he has to accurately discard at least one of the possible options. In [5] the PBR game, originally formulated in [33], was analyzed in terms of an semidefinite program using the conclusive state exclusion framework. Some of the formulas we obtain in Section 3 are similar to the ones [5] derive in their analysis of the PBR game, specifically equations (9) and (10). Looking at the SDPs involved in their work and in ours, it seems clear that the similarity arises from the fact that diagonal unitaries happen to be optimal for hedging. The fact that they are optimal means that the optimization problem we examine in SDP (7) is equivalent to that of optimizing along complex vectors where each entry of the vector is a unit. Then, to establish the connection with the PBR setting, one would establish an equivalence between these types of vectors and highly symmetrical projective measurements like those obtained as optimal solutions in the corresponding PBR state exclusion setting. However, in a setting with initial states outside the $\alpha |00\rangle + \sqrt{1-\alpha^2} |11\rangle$ family we consider in Section 3, there is no reason why the optimal channel for winning 1 out of n parallel interactions should correspond to a diagonal unitary. It remains then to see whether any similar connections can be established between such a setting and a state exclusion setting. It seems plausible that further work clarifying these connections could be used to apply existing results concerning the conclusive state exclusion framework to the hedging framework, and vice versa.

One could also further consider the setting in which protocol errors are considered. Here, we have assumed that Bob can delay returning an answer for as many iterations of the protocol as he desires. An obvious follow-up question then is to determine whether an advantage from hedging behavior is possible when this is not the case. One might restrain Bob to behaviors where on average he will return an answer within a fixed number of iterations, or introduce constraints be of the form “After X iterations, Bob’s probability of having return an answer must be at least equal to Y”. A special case of those constraints that might be particularly interesting is when Bob is required to return an answer within a fixed number of iterations. We could also modify the way in which the “repeating after failure" and “repeating in parallel" frameworks interact. In particular, we could have Alice repeat only a subset of interactions if answers corresponding to the other interactions have been obtained from Bob.

Note that when trying to analyze more general models (in both the ideal and loss-tolerant cases) along the lines described in this section, it might be fruitful to look into whether it is possible to again use ideas from the quantum cloning literature, as we did here in Section 4. It is possible as well that progress can be made using representation theory tools to simplify or avoid the analysis of semidefinite programs, as done for example in [19, 11, 12, 27].

Acknowledgements. We would like to thank Devin Smith for the question that led to Section 4 in this paper. A significant amount of thanks is also due to John Watrous for numerous insightful discussions and suggestions. We thank Ronald de Wolf for helpful comments. We wish to thank Nathaniel Johnston for helpful suggestions, as well as for the use of his QETLAB quantum entanglement MATLAB package [26]. Thanks are also due to Alessandro Cosentino, Gus Gutoski, and Christopher Perry for insightful discussions. The suggestions of several anonymous referees have also been taken into account during the elaboration of this manuscript.

References

1 Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 461, pages 3473–3482. The Royal Society, 2005.

2 Nati Aharon, Serge Massar, and Jonathan Silman. Family of loss-tolerant quantum coin-flipping protocols. *Physical Review A*, 82(5):052307, 2010.

3 Srinivasan Arunachalam, Abel Molina, and Vincent Russo. Software for implementing some of the semidefinite programs in this paper. Available at `https://bitbucket.org/vprusso/quantum-hedging`, 2013.

4 Koenraad Audenaert and Bart De Moor. Optimizing completely positive maps using semidefinite programming. *Physical Review A*, 65(3):030302, 2002.

5 Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim, and Christopher Perry. Conclusive exclusion of quantum states. *Physical Review A*, 89(2):022336, 2014.

6 John Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

7 Fernando GSL Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek, and Hanna Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices. *Nature communications*, 7, 2016.

8 Mark Braverman and Ankit Garg. Small value parallel repetition for general games. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 335–340. ACM, 2015.

9 Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald de Wolf. Near-optimal and explicit bell inequality violations. *Theory of Computing*, 8(1):623–645, 2012.

10 Nicolas Cerf and Jaromir Fiurasek. Optical quantum cloning. *Progress in Optics*, 49:455, 2006.

11 Andrew M Childs, Andrew J Landahl, and Pablo A Parrilo. Quantum algorithms for the ordered search problem via semidefinite programming. *Physical Review A*, 75(3):032335, 2007.

12 Matthias Christandl, Norbert Schuch, and Andreas Winter. Highly entangled states with almost no secrecy. *Physical Review Letters*, 2010.

13 John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 1969.

14 Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.

15 Tom Cooney, Marius Junge, Carlos Palazuelos, and David Pérez-García. Rank-one quantum games. *Computational Complexity*, 24(1):133–196, 2015.

16 Uriel Feige. On the success probability of the two provers in one-round proof systems. In *Structure in Complexity Theory Conference, 1991., Proceedings of the Sixth Annual*, pages 116–123. IEEE, 1991.

17 Jaromír Fiurášek. Optimal probabilistic cloning and purification of quantum states. *Physical Review A*, 70(3):032308, 2004.

18 Lance Jeremy Fortnow. *Complexity-theoretic aspects of interactive proof systems*. PhD thesis, Massachusetts Institute of Technology, 1989.

19 Karin Gatermann and Pablo A Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra*, 192(1):95–128, 2004.

20 Michael Grant, Stephen Boyd, and Yinyu Ye. CVX: Matlab software for disciplined convex programming. `http://cvxr.com/cvx/`, 2008.

21 Gus Gutoski. Quantum strategies and local operations. *arXiv preprint arXiv:1003.0038*, 2010.

22 Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574. ACM, 2007.

23 Patrick Hayden, Kevin Milner, and Mark Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Information & Computation*, 14(5&6):384–416, 2014.

24 Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419. ACM, 2007.

25 Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543. IEEE, 2009.

26 Nathaniel Johnston. QETLAB: MATLAB Software for quantum entanglement. Available at `http://www.qetlab.com/`, 2015.

27 Hari Krovi, Saikat Guha, Zachary Dutton, and Marcus P da Silva. Optimal measurements for symmetric quantum states with applications to optical communication. *Physical Review A*, 92(6):062333, 2015.

28 Urmila Mahadev and Ronald de Wolf. Rational approximations and quantum algorithms with postselection. *Quantum Information & Computation*, 15(3&4):295–307, 2015.

29 N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373, 1990.

30 Abel Molina and John Watrous. Hedging bets with correlated quantum strategies. In *Proc. R. Soc. A*. The Royal Society, 2012.

31 Fernando Pastawski, Norman Y Yao, Liang Jiang, Mikhail D Lukin, and J Ignacio Cirac. Unforgeable noise-tolerant quantum tokens. *Proceedings of the National Academy of Sciences*, 109(40):16079–16082, 2012.

32 Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.

33 Matthew Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nature Physics*, 2012.

34 Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

35 Ran Raz. Quantum information and the PCP theorem. In *46th Annual IEEE Symposium on Foundations of Computer Science.*, pages 459–468. IEEE, 2005.

36 Oded Regev. Bell violations through independent bases games. *Quantum Information & Computation*, 12(1-2):9–20, 2012.

37 Oksana Scegulnaja-Dubrovska, Lelde Lāce, and Rūsiņš Freivalds. Postselection finite quantum automata. In *International Conference on Unconventional Computation*, pages 115–126. Springer, 2010.

38 Devin Smith. Personal communication, 2011.

39 Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, 90(5):052314, 2014.

40 John Watrous. `https://cs.uwaterloo.ca/~watrous/CS766/ProblemSets/solutions.2.pdf`.

41 John Watrous. Theory of quantum information lecture notes. `https://cs.uwaterloo.ca/~watrous/LectureNotes.html`, 2011.

42 Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *STACS 2006*, pages 162–171. Springer, 2006.

43 Abuzer Yakaryilmaz and AC Say. Probabilistic and quantum finite automata with postselection. *arXiv preprint arXiv:1102.0666*, 2011.

44 Sheng Zhang and Yuexin Zhang. Quantum coin flipping secure against channel noises. *Physical Review A*, 92(2):022313, 2015.

A Mathematical derivations

A.1 Verification of procedure to group the starting state and the final measurement into a single variable

Consider first the case where we have a matrix $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Z})$ that corresponds to a rank-1 operator that transforms a state of the computational basis into another one. Let it be equal to $|a\rangle\langle c| \otimes |b\rangle\langle d|$, with $|a\rangle\langle c| \in \mathrm{L}(\mathcal{X})$, $|b\rangle\langle d| \in \mathrm{L}(\mathcal{Z})$. The channel $\Psi_A : \mathrm{L}(\mathcal{Z}) \to \mathrm{L}(\mathcal{X})$ such that $J(\Psi_A) = \overline{A}$ is then the one that maps $|b\rangle\langle d| \in \mathrm{L}(\mathcal{Z})$ to $|a\rangle\langle c| \in \mathrm{L}(\mathcal{X})$, and everything else in the computational basis for $\mathrm{L}(\mathcal{Z})$ to 0.
Consider now an operator $M \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{Z})$, and a channel $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$. We want to verify that

$$\langle M, (\Phi \otimes \mathcal{I})(A)\rangle = \langle (\mathcal{I} \otimes \Psi_A)(M), J(\Phi)\rangle . \tag{23}$$

To do so, consider a computational basis decomposition $M = \sum_{i,j,k,l} m_{i,j,k,l} |i\rangle\langle j| \otimes |k\rangle\langle l|$, with $|i\rangle\langle j| \in \mathrm{L}(\mathcal{Y})$, $|k\rangle\langle l| \in \mathrm{L}(\mathcal{Z})$. Then, the left hand side of (23) is equal to

$$\left\langle \sum_{i,j,k,l} m_{i,j,k,l} |i\rangle\langle j| \otimes |k\rangle\langle l|, \Phi(|a\rangle\langle c|) \otimes |b\rangle\langle d| \right\rangle = \left\langle \sum_{i,j} m_{i,j,b,d} |i\rangle\langle j|, \Phi(|a\rangle\langle c|) \right\rangle ,$$

and the right hand side of (23) is equal to

$$\begin{aligned}\left\langle (\mathcal{I} \otimes \Psi_A) \left(\sum_{i,j,k,l} m_{i,j,k,l} |i\rangle\langle j| \otimes |k\rangle\langle l| \right), J(\Phi) \right\rangle &= \left\langle \sum_{i,j} m_{i,j,b,d} |i\rangle\langle j| \otimes |a\rangle\langle c|, J(\Phi) \right\rangle \\ &= \left\langle \sum_{i,j} m_{i,j,b,d} |i\rangle\langle j|, \Phi(|a\rangle\langle c|) \right\rangle ,\end{aligned}$$

so (23) holds.

(23) does extend by linearity to any choice of $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Z})$. Indeed, assume that it holds for $A, B \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Z})$, and consider a linear combination $\lambda_A A + \lambda_B B$, with $\lambda_A, \lambda_B \in \mathbb{C}$. Then, the left hand side of (23) will be given by

$$\begin{aligned}\langle M, (\Phi \otimes \mathcal{I})(\lambda_A A + \lambda_B B)\rangle &= \lambda_A \langle M, (\Phi \otimes \mathcal{I})(A)\rangle + \lambda_B \langle M, (\Phi \otimes \mathcal{I})(B)\rangle \\ &= \lambda_A \langle (\mathcal{I} \otimes \Psi_A)(M), J(\Phi)\rangle + \lambda_B \langle (\mathcal{I} \otimes \Psi_B)(M), J(\Phi)\rangle \\ &= \left\langle \overline{\lambda_A} (\mathcal{I} \otimes \Psi_A)(M) + \overline{\lambda_B} (\mathcal{I} \otimes \Psi_B)(M), J(\Phi) \right\rangle .\end{aligned}$$

We want to prove then that

$$\overline{\lambda_A} (\mathcal{I} \otimes \Psi_A)(M) + \overline{\lambda_B} (\mathcal{I} \otimes \Psi_B)(M) = (\mathcal{I} \otimes \Psi_{\lambda_A A + \lambda_B B})(M).$$

To do so, we use the third property of the Choi representation introduced in Lemma 1,

and express $\overline{\lambda_A}\,(\mathcal{I}\otimes\Psi_A)\,(M)+\overline{\lambda_B}\,(\mathcal{I}\otimes\Psi_B)\,(M)$ as

$$\begin{aligned}
&\overline{\lambda_A}\,\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(J(\mathcal{I}_{\mathrm{L}(Y)}\otimes\Psi_A)(\mathcal{I}_{\mathcal{X}\otimes\mathcal{Z}}\otimes M^T)\right)+\\
&\overline{\lambda_B}\,\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(J(\mathcal{I}_{\mathrm{L}(Y)}\otimes\Psi_B)(\mathcal{I}_{\mathcal{X}\otimes\mathcal{Z}}\otimes M^T)\right)\\
=&\,\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(\left(\overline{\lambda_A}J(\mathcal{I}_{\mathrm{L}(Y)}\otimes\Psi_A)+\overline{\lambda_B}J(\mathcal{I}_{\mathrm{L}(Y)}\otimes\Psi_B)\right)(\mathcal{I}_{\mathcal{X}\otimes\mathcal{Z}}\otimes M^T)\right)\\
=&\,\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(\left(J(\mathcal{I}_{\mathrm{L}(Y)})\otimes\overline{\lambda_A A}+J(\mathcal{I}_{\mathrm{L}(Y)})\otimes\overline{\lambda_B B}\right)(\mathcal{I}_{\mathcal{X}\otimes\mathcal{Z}}\otimes M^T)\right)\\
=&\,\mathrm{Tr}_{\mathcal{Y}\otimes\mathcal{Z}}\left(\left(J(\mathcal{I}_{\mathrm{L}(Y)})\otimes\left(\overline{\lambda_A A}+\overline{\lambda_B B}\right)\right)(\mathcal{I}_{\mathcal{X}\otimes\mathcal{Z}}\otimes M^T)\right)\\
=&\,(\mathcal{I}\otimes\Psi_{\lambda_A A+\lambda_B B})\,(M).
\end{aligned}$$

A.2 Derivation for Lemma 4

Proof. Given that n parallel repetitions of the game are considered, our claim states that Bob will win *at least* one out of the n repetitions if he adopts Λ_n as his strategy when the projective measurement made by Alice corresponds to the parameter $\theta_{n,\alpha}$. A similar argument also holds for Ξ_n at the corresponding angle $\gamma_{n,\alpha}$. We prove this explicitly for the strategy Λ_n , and the other case follows using the same argument. The proof of this lemma uses a technique of conditioning where we consider the resulting state conditioned on Bob obtaining a losing outcome in the first projective measurement of Alice, and the corresponding probability for such an outcome. Then, we generalize this procedure to the rest of the parallel repetitions. To conclude the proof, we set the probability of the "all-losing state" at the end to zero, which allows us to solve for θ in the final equation.

First, let us define the pure states:

$$\begin{aligned}
v_\theta &= \cos(\theta)\,|00\rangle+\sin(\theta)\,|11\rangle\,, \quad s_\theta=|01\rangle\,,\\
w_\theta &= \sin(\theta)\,|00\rangle-\cos(\theta)\,|11\rangle\,, \quad t_\theta=|10\rangle\,,
\end{aligned}\tag{24}$$

where we recall from Section 3 that $v_\theta\in\mathcal{Y}\otimes\mathcal{Z}$ is the state which corresponds to the winning projective measurement outcome, and w_θ, s_θ, and $t_\theta\in\mathcal{Y}\otimes\mathcal{Z}$ are the states that correspond to the losing projective measurement. Essentially, Bob is trying then to transform the state prepared by Alice to something as close as possible to v_θ, while restricted to operating on one half on the state.

Let Λ_n be the operator defined as

$$\Lambda_n=\sum_{r\in\{0,1\}^n}(-1)^{\wedge r+\oplus r}\,|r\rangle\langle r|,\tag{25}$$

Λ'_n be the similar operator

$$\Lambda'_n=\sum_{r\in\{0,1\}^n}(-1)^{\oplus r}\,|r\rangle\langle r|.\tag{26}$$

and define the vector κ_n as

$$\kappa_n=\sum_{a\in\{0,1\}^n}\bigotimes_{i=0}^{n-1}\alpha^{(1-a_i)}\left(1-\alpha^2\right)^{a_i/2}|a_ia_i\rangle\,.\tag{27}$$

We run now through the parallel repetition of n copies of the game. Since the initial shared state is $u_\alpha^{\otimes n}=\left(\alpha\,|00\rangle+\sqrt{1-\alpha^2}\,|11\rangle\right)^{\otimes n}$, the state after Bob applies his channel (acting on his qubits for all of the n parallel repetitions) is

$$f_\alpha^0=(\Lambda_n\otimes\mathcal{I}_{\mathcal{Z}_1\otimes\cdots\otimes\mathcal{Z}_n})\,\kappa_n\tag{28}$$

We shall condition now on Bob losing the first out of n parallel repetitions. It should be noted that since Alice starts with the entangled state $u_\alpha^{\otimes n}$ and Bob performs a unitary diagonal operation, the states s_θ and t_θ in (24) do not contribute to the losing projective measurement outcome. Once we condition on Bob losing the first game, the resulting state is then a normalization of

$$\begin{aligned} f^1_{\alpha,\theta} &= (w_\theta w_\theta^* \otimes \mathcal{I})\, f^0_\alpha \\ &= w_\theta \otimes \alpha \sin(\theta) \left(\Lambda'_{n-1} \otimes \mathcal{I}_{\mathcal{Z}_2 \otimes \cdots \otimes \mathcal{Z}_n}\right) \kappa_{n-1} \\ &\quad + w_\theta \otimes \sqrt{1-\alpha^2} \cos(\theta) \left(\Lambda_{n-1} \otimes \mathcal{I}_{\mathcal{Z}_2 \otimes \cdots \otimes \mathcal{Z}_n}\right) \kappa_{n-1}, \end{aligned} \tag{29}$$

with the associated probability being $(f^1_{\alpha,\theta})^* f^1_{\alpha,\theta}$.

Generalizing this to Bob losing all n games, one can observe that the -1's for the $\cos(\theta)$ term in w_θ cancel the negative terms from the $(-1)^{\bigoplus r}$ term in Λ_n, as happens to make the last line of (29) have a positive coefficient. Taking into account the negative term from $(-1)^{\wedge r}$ in Λ_n, (29) generalizes then to:

$$\begin{aligned} f^n_{\alpha,\theta} &= (w_\theta)^{\otimes n} \Big(\alpha^n \sin(\theta)^n + n(\alpha^{n-1}\sqrt{1-\alpha^2}) \sin(\theta)^{n-1} \cos(\theta) + \dots \\ &\quad + n(\alpha(1-\alpha^2)^{(n-1)/2}) \cos(\theta)^{n-1} \sin(\theta) - (1-\alpha^2)^{n/2} \cos(\theta)^n \Big) \qquad (30) \\ &= (w_\theta)^{\otimes n} \left((\alpha \sin(\theta) + \sqrt{1-\alpha^2} \cos(\theta))^n - 2(1-\alpha^2)^{n/2} \cos(\theta)^n \right). \qquad (31) \end{aligned}$$

In order for Bob to ensure he wins *at least* 1 out of the n games with certainty, we require that $\left\| f^n_{\alpha,\theta} \right\| = 0$, which implies:

$$(\alpha \sin(\theta) + \sqrt{1-\alpha^2} \cos(\theta))^n - 2(1-\alpha^2)^{n/2} \cos(\theta)^n = 0. \tag{32}$$

This implies that for the angle $\theta_{n,\alpha} = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2} - 1}\left(2^{1/n} - 1\right)\right)$, the strategy corresponding to Λ_n gives us a perfect hedging strategy. Following the same procedure, using the strategy corresponding to Ξ_n yields the similar condition that:

$$(\alpha \sin(\theta) + \sqrt{1-\alpha^2} \cos(\theta))^n - 2\alpha^n \sin(\theta)^n = 0, \tag{33}$$

giving us as a solution $\gamma_{n,\alpha} = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2} - 1}\left(\frac{1}{2^{1/n}-1}\right)\right)$. ◀

A.3 Derivation for Lemma 5

Proof. As in the previous proof, to win at least 1 out of n games, Bob needs to avoid the outcome corresponding to the state $(\sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle)^{\otimes n}$ (other states for the losing outcome can be ignored since Bob's strategy corresponds to a diagonal matrix). Let us now define a matrix

$$D = \sum_{r \in \{0,1\}^n} (-1)^{|r|} \sin(\theta)^{n-|r|} \cos(\theta)^{|r|} |r\rangle\langle r|, \tag{34}$$

such that $(\sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle)^{\otimes n} = \mathrm{vec}\,(D)$. For convenience, we denote $\lambda = \tan(\theta)$, and rewrite D as

$$D = \cos(\theta)^n \sum_{r \in \{0,1\}^n} (-1)^{|r|} \lambda^{n-|r|} |r\rangle\langle r|. \tag{35}$$

We also introduce an operator

$$F = \sum_{r\in\{0,1\}^n} (1-\alpha^2)^{|r|/2}\alpha^{n-|r|}|r\rangle\langle r|, \tag{36}$$

such that $u_\alpha^{\otimes n} = \mathrm{vec}\,(F)$, where u_α is again the pure state $\alpha\,|00\rangle + \sqrt{1-\alpha^2}\,|11\rangle$ shared by Alice and Bob at the beginning of a single repetition of the protocol.

From our construction the unitary U that Bob applies in Lemma 5 to his portion of the entangled state $u_\alpha^{\otimes n}$ is

$$U = (-1)^n|0\rangle\langle 0| - |1\rangle\langle 1| + \sum_{i=1}^{n-1}\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} (-1)^{n+i}k_r\,|r\rangle\,\langle r|\,. \tag{37}$$

The state that Alice holds before measurement is then $(U\otimes\mathcal{I}_{\mathcal{Z}_{1\ldots n}})u_\alpha^{\otimes n}$. We analyze how successful the application of this channel would be to avoid $(\sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle)^{\otimes n}$. Upon explicit computation of the formula $\langle \mathrm{vec}\,(D)\,, (U\otimes\mathcal{I}_{\mathcal{Z}_{1\ldots n}})\mathrm{vec}\,(F)\rangle$, and using repeatedly the fact that $\mathrm{vec}\,(V) = (V\otimes\mathcal{I})\mathrm{vec}\,(\mathcal{I})$, we obtain $\langle \mathrm{vec}\,(D)\,, \mathrm{vec}\,(UF)\rangle$, which is equal to $\langle D, UF\rangle$ by the properties of the vec operator, resulting in the following expression:

$$\begin{aligned}
\langle D, UF\rangle &= \mathrm{Tr}\Big((-1)^n\alpha^n\lambda^n|0^n\rangle\langle 0^n| + (1-\alpha^2)^{n/2}(-1)^{n+1}|1^n\rangle\langle 1^n| \\
&\quad + \sum_{i=1}^{n-1}\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} (-1)^n k_r(1-\alpha^2)^{i/2}\alpha^{n-i}\lambda^{n-i}\,|r\rangle\,\langle r|\Big) \\
&= (-1)^n\alpha^n\,\mathrm{Tr}\Big(\lambda^n|0^n\rangle\langle 0^n| - \left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n|1^n\rangle\langle 1^n| \\
&\quad + \sum_{i=1}^{n-1}\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} k_r\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^i\lambda^{n-i}\,|r\rangle\,\langle r|\Big) \\
&= (-1)^n\alpha^n\left(\lambda^n - \left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n + \sum_{i=1}^{n-1}\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} k_r\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^i\lambda^{n-i}\right) \\
&= (-1)^n\alpha^n\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n\left(\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1}\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} k_r\lambda_\alpha^{n-i}\right),
\end{aligned} \tag{38}$$

where $\lambda_\alpha = \lambda\cdot\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^{-1}$.

Note that for the range of θ we are considering, it holds that $2^{1/n}-1 \le \lambda_\alpha \le \frac{1}{2^{1/n}-1}$. Note as well that from our choice of k_r, for all i we have that $\mathrm{Im}\left(\sum_{\substack{r\in\{0,1\}^n\\ |r|=i}} k_r\lambda_\alpha^{n-i}\right) = 0$, and therefore the imaginary part of (38) is equal to 0. It then suffices to prove that for any choice of λ_a and n, there exists an $s_{\theta,\alpha,n}\in[-1,1]$ such that, when plugged into the

definition of k_r in the statement of Lemma 5 we have

$$\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}\,(k_r)\,\lambda_\alpha^{n-i} = 0. \tag{39}$$

Now, as the left hand side of (39) is an affine function of $s_{\theta,\alpha,n}$ with a positive linear coefficient, to prove the existence of such an $s_{\theta,\alpha,n}$, it suffices to prove that the left hand side of (39)) ≤ 0 when $s_{\theta,\alpha,n} = -1$, and that the left hand side of (39) ≥ 0 when $s_{\theta,\alpha,n} = 1$.

We look first into the case when $s = -1$. Then, when $1 \leq \lambda_\alpha \leq \dfrac{1}{2^{1/n}-1}$ it holds that:

$$\begin{aligned}\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}\,(k_r)\,\lambda_\alpha^{n-i} &= \lambda_\alpha^n - 1 - \sum_{i=1}^{n-1} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= 2\lambda_\alpha^n - \lambda_\alpha^n - 1 - \sum_{i=1}^{n-1} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= 2\lambda_\alpha^n - (1+\lambda_\alpha)^n, \end{aligned} \tag{40}$$

which is ≤ 0 whenever $\lambda_\alpha \leq \dfrac{1}{2^{1/n}-1}$. When $2^{1/n} - 1 \leq \lambda_\alpha < 1$, that the left hans side of (39) ≤ 0 follows from two simple facts. First, the fact that $\lambda_\alpha^n < 1$, so $\lambda_\alpha^n - 1 < 0$. Second, the fact that for each $\sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}\,(k_r)\,\lambda_\alpha^{n-i}$ term, $\sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}\,(k_r) \leq -\binom{n}{i} + 1 \leq 0$.

We look now into the case when $s = 1$. Then, when $2^{1/n} - 1 \leq \lambda_\alpha < 1$ it holds that:

$$\begin{aligned}\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}\,(k_r)\,\lambda_\alpha^{n-i} &= \lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= -2 + \lambda_\alpha^n + 1 + \sum_{i=1}^{n-1} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= -2 + (1+\lambda_\alpha)^n, \end{aligned} \tag{41}$$

which is ≥ 0 whenever $\lambda_\alpha \geq 2^{1/n} - 1$. When $1 \leq \lambda_\alpha \leq \dfrac{1}{2^{1/n}-1}$, that the left hand side of (39) ≥ 0 follows from two simple facts. First, the fact that $\lambda_\alpha^n \geq 1$. Second, the fact that for each $\sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}(k_r)\lambda_\alpha^{n-i}$ term, it is the case that $\sum_{\substack{r\in\{0,1\}^n \\ |r|=i}} \mathrm{Re}(k_r) \geq \binom{n}{i} - 1$. ◀

A.4 Derivation for Lemma 6

Proof. We will consider here the case where $\theta < \theta_{n,\alpha}$. The other case proceeds similarly.

Remember first that we characterized the chance of achieve 1-out-of-n hedging by the following SDP program in Section 3:

$m_{n,\alpha,\theta}$: Primal problem

$$\begin{aligned} \text{minimize:} \quad & \left\langle Q_{0,\alpha,\theta}^{\otimes n}, X \right\rangle \\ \text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}_1\otimes\cdots\otimes\mathcal{Y}_n}(X) = \mathcal{I}_{\mathcal{X}_1\otimes\cdots\otimes\mathcal{X}_n}, \\ & X \in \mathrm{Pos}(\mathcal{Y}_1 \otimes \mathcal{X}_1 \otimes \cdots \otimes \mathcal{Y}_n \otimes \mathcal{X}_n). \end{aligned} \tag{42}$$

$m_{n,\alpha,\theta}$: Dual problem

$$\begin{aligned} \text{maximize:} \quad & \mathrm{Tr}(Y) \\ \text{subject to:} \quad & \pi\left(\mathcal{I}_{\mathcal{Y}_1\otimes\cdots\otimes\mathcal{Y}_n} \otimes Y\right)\pi^* \leq Q_{0,\alpha,\theta}^{\otimes n}, \\ & Y \in \mathrm{Herm}(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_n). \end{aligned} \tag{43}$$

Then, to prove that perfect hedging is not possible when $\theta < \theta_{n,\alpha}$, we prove the feasibility in the dual SDP (43) of an operator Y with positive objective value. This operator is obtained from applying complementary slackness conditions to the primal solution corresponding to Λ_n. Therefore, it has value for the dual equal to the value in the primal SDP (42) for the solution corresponding to Λ_n. By weak duality, its feasibility proves then the optimality of Λ_n when $\theta < \theta_{n,\alpha}$.

To prove the feasibility of Y, we will express $Q_{0,\alpha,\theta}^{\otimes n} - \pi\left(\mathcal{I}_{\mathcal{Y}_1\otimes\cdots\otimes\mathcal{Y}_n} \otimes Y\right)\pi^*$ as a direct sum of smaller matrices. This reduces the question about feasibility of Y to a question about the positive-semidefiniteness of these smaller matrices. Each of these smaller matrices will have all proper leading principal minors be positive semi-definite, so by Sylvester's criterion it will suffice to check that their determinant is non-negative. We will then obtain a closed formula for these determinants, and prove that they are indeed non-negative.

We will first consider the case with $\alpha = 1/\sqrt{2}$, and then give an overview of the small changes involved in adapting the proof to other values of α. To simplify our argument, we will incur in a bit of notation abuse in this section, and omit the permutation operators in the definition of the dual SDP (43) that remind us that matrices at the sides of a $\leq$ inequality must have their entries reordered to make the spaces on which they are defined be in the same order at both sides of the inequality.

A.4.1 Study of $Q_{0,1/\sqrt{2},\theta}^{\otimes n}$

$Q_{0,\alpha,\theta} \in \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ is given by $\left|\psi_0^1\right\rangle\left\langle\psi_0^1\right| + \left|\psi_0^2\right\rangle\left\langle\psi_0^2\right| + \left|\psi_0^3\right\rangle\left\langle\psi_0^3\right|$, where the $\left|\psi_0^i\right\rangle$ are defined as

$$\begin{aligned} \left|\psi_0^1\right\rangle &= \alpha\sin(\theta)\left|00\right\rangle - \sqrt{1-\alpha^2}\cos(\theta)\left|11\right\rangle, \\ \left|\psi_0^2\right\rangle &= \alpha\left|01\right\rangle, \\ \left|\psi_0^3\right\rangle &= \sqrt{1-\alpha^2}\left|10\right\rangle. \end{aligned} \tag{44}$$

This follows from considering the definition of $P_{0,\theta}$ given in Section 3, and observing that the operator Ψ_{ρ_α} satisfying $J(\Psi_{\rho_\alpha}) = \overline{u_\alpha u_\alpha^*}$ (with $u_\alpha = \alpha\left|00\right\rangle + \sqrt{1-\alpha^2}\left|11\right\rangle$ the initial state shared between Alice and Bob) maps a state $\sigma \in \mathrm{D}(\mathcal{Z})$ to $(\alpha|0\rangle\langle 0| + \sqrt{1-\alpha^2}|1\rangle\langle 1|)\sigma(\alpha|0\rangle\langle 0| +$

$\sqrt{1-\alpha^2}|1\rangle\langle 1|)$. We can then write $Q^{\otimes n}_{0,1/\sqrt{2},\theta}$ as

$$\begin{aligned} Q^{\otimes n}_{0,1/\sqrt{2},\theta} = & \left(\frac{1}{2}\right)^n \Big((\sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle)(\sin(\theta)\,\langle 00| - \cos(\theta)\,\langle 11|) \\ & + |01\rangle\langle 01| + |10\rangle\langle 10|\Big)^{\otimes n} \qquad (45) \\ = & \left(\frac{1}{2}\right)^n \sum_{a,b,c,d\in\{0,1\}^n} |a\rangle\,|b\rangle\,\langle c|\,\langle d| \prod_{i=0}^{n-1} \Big(\delta_{c_i,1-d_i}\delta_{a_i,c_i}\delta_{b_i,d_i} \\ & + \delta_{a_i,b_i}\delta_{c_i,d_i}\Big(\delta_{a_i,1-c_i}(-\sin(\theta)\cos(\theta)) + \delta_{a_i,c_i}\delta_{a_i,1}\cos(\theta)^2 \\ & + \delta_{a_i,c_i}\delta_{a_i,0}\sin(\theta)^2\Big)\Big) \\ = & \left(\frac{1}{2}\right)^n \sum_{a,c\in\{0,1\}^n} |a\rangle\langle c| \otimes \sum_{b,d\in\{0,1\}^n} |b\rangle\langle d| \prod_{i=0}^{n-1} \Big(\delta_{a_i,1-b_i}\delta_{c_i,1-d_i}\delta_{a_i,c_i} + \\ & \delta_{a_i,b_i}\delta_{c_i,d_i}\Big(\delta_{a_i,1-c_i}(-\sin(\theta)\cos(\theta)) + \delta_{a_i,c_i}\delta_{a_i,1}\cos(\theta)^2 \\ & + \delta_{a_i,c_i}\delta_{a_i,0}\sin(\theta)^2\Big)\Big). \qquad (46) \end{aligned}$$

The key insight to go ahead with the proof is to notice that this matrix can be written as a direct sum of 3^n smaller matrices. Indeed, observe that (45) can be equivalently written as

$$\frac{1}{2^n} \sum_{w\in\{0,1,2\}^n} \bigotimes_{i=0}^{n-1} |\psi_{w_i}\rangle\langle\psi_{w_i}|, \text{ where } |\psi_{w_i}\rangle = \begin{cases} \sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle\,, \text{ if } w_i = 0 \\ |01\rangle\,, \text{ if } w_i = 1 \\ |10\rangle\,, \text{ if } w_i = 2 \end{cases}. \qquad (47)$$

Then, the coefficient for each $|a\rangle\langle c| \otimes |b\rangle\langle d|$ term in the summation in (46) will receive contribution from at most one of the elements in (47). This element will be the one with $w_i = \begin{cases} 0 \text{ if } a_i = b_i \\ 1 \text{ if } (a_i, b_i) = (0,1) \\ 2 \text{ if } (a_i, b_i) = (1,0) \end{cases}$.

Since this only depends on $|ab\rangle$, all elements on the same row of $Q^{\otimes n}_{0,1/\sqrt{2},\theta}$ come from the same term in (47). As each row of $Q^{\otimes n}_{0,1/\sqrt{2},\theta}$ has at least one non-zero term, (47) implies then a decomposition $Q^{\otimes n}_{0,1/\sqrt{2},\theta}$ into a direct sum of smaller matrices, each of them with rank 1.

We can then identify each of these matrices by the corresponding choice of w in (47). We will do so by writing them as $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$. We denote the number of 0s, 1s and 2s in w by $n_0(w)$, $n_1(w)$ and $n_2(w)$, respectively. Also, note that there will be 3^n matrices in our decomposition, with the dimension of $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$ being given by $2^{n_0(w)}$. Also, note that the number of matrices of size 2^k is given by $\binom{n}{k}2^{n-k}$. This corresponds to choosing on which k positions $w_i = 0$, and what is the value of w_i for the other ones.

It will be convenient later to have a formula for the restriction to the diagonal of $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$. Using the description in (47), we have that it is given by

$$\left(\frac{1}{2}\right)^n \sum_{w'\in M_w\subseteq\{0,1\}^n} g(w,w')\,|w'\rangle\,|f(w,w')\rangle\,\langle w'|\,\langle f(w,w')| \qquad (48)$$

where M_w is given by the cartesian product $\bigtimes_{i=0}^{n-1} M_{w_i}$, with $\begin{cases} M_0 = \{0,1\} \\ M_1 = \{0\} \\ M_2 = \{1\} \end{cases}$,

$g(w,w') = \prod_{i=0}^{n-1} g(w_i, w'_i)$ with $\begin{cases} g(0,0) = \sin^2(\theta) \\ g(0,1) = \cos^2(\theta) \\ g(1,0) = 1 \\ g(2,1) = 1 \end{cases}$, $f(w,w')_i = \begin{cases} w'_i \text{ if } w_i = 0 \\ 1 - w'_i \text{ if } w_i = 1 \end{cases}$.

Note that by definition of M_w, it is not necessary to define $g(w_i, w'_i)$ for values of (w_i, w'_i) not included in our definition of g.

A.4.2 Study of our candidate for Y in the $\alpha = 1/\sqrt{2}$ case

We define now our candidate solution Y for the dual problem, given by

$$Y = -\epsilon \left(\left(\frac{1}{\sqrt{2}} \sin(\theta) \left|0\right\rangle \left\langle 0\right| + \frac{1}{\sqrt{2}} \cos(\theta) \left|1\right\rangle \left\langle 1\right| \right)^{\otimes n} - 2 \left(\frac{1}{\sqrt{2}} \cos(\theta) \left|1\right\rangle \left\langle 1\right| \right)^{\otimes n} \right), \tag{49}$$

where ϵ is a value > 0 given by $\left(\frac{1}{2}\right)^{n/2} (2\cos(\theta)^n - (\cos(\theta) + \sin(\theta))^n)$. Note that the definition of $\theta_{n,1/\sqrt{2}}$ implies that this value is positive indeed for $\theta < \theta_{n,1/\sqrt{2}}$. We can then write Y as

$$\sum_{a \in \{0,1\}^n} \lambda_a \left|a\right\rangle \left\langle a\right|, \text{where } \lambda_a = \begin{cases} -\epsilon \left(\frac{1}{2}\right)^{n/2} \sin(\theta)^{n-|a|} \cos(\theta)^{|a|} & \text{for } a \neq 1^n \\ \epsilon \left(\frac{1}{2}\right)^{n/2} \cos(\theta)^n & \text{for } a = 1^n \end{cases} \tag{50}$$

Note that its trace (i.e., its value for the dual program) is given by

$$-\left(\frac{1}{2}\right)^{n/2} \epsilon \Big((\sin(\theta) + \cos(\theta))^n - 2\cos(\theta)^n \Big), \tag{51}$$

which will again be positive for $\theta < \theta_{n,1/\sqrt{2}}$ by definition of $\theta_{n,1/\sqrt{2}}$.

This Y has been obtained from the strategy Λ_n in Lemma 4, and its feasibility proves the optimality of Λ_n for $\theta < \theta_{n,1/\sqrt{2}}$. This is an example of complementary slackness behavior, and follows from an observation [40] that given a feasible solution X to the primal SDP (42), $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(Q_{0,\alpha,\theta}^{\otimes n} X)$ is an operator with the same objective value for the dual SDP (43). Furthermore, $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(Q_{0,\alpha,\theta}^{\otimes n} X)$ satisfies the feasibility constraints of the dual if and only if X represents an optimal solution to the primal. Therefore, after we experimentally observed that Λ_n seemed to be optimal for $\theta < \theta_{n,\alpha}$ to obtain our proposed Y we computed the corresponding value of $\mathrm{Tr}_{\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_n}(Q_{0,1/\sqrt{2},\theta}^{\otimes n} X)$. X is given in this computation by the primal solution that represents the channel for the unitary in Λ_n,

$$X = \sum_{i,j \in \{0,1\}^n} \left|ii\right\rangle \left\langle jj\right| (-1)^{\wedge i + \bigoplus i + \wedge j + \bigoplus j}. \tag{52}$$

A.4.3 Feasibility of Y in the $\alpha = 1/\sqrt{2}$ case

We want to prove that Y is feasible - that is to say, $Q_{0,1/\sqrt{2},\theta}^{\otimes n} - Y \otimes \mathcal{I} \geq 0$. Since Y is diagonal, the direct sum decomposition of $Q_{0,1/\sqrt{2},\theta}^{\otimes n}$ corresponds to a direct sum decomposition of Y.

Since positive semidefiniteness is preserved by the direct sum operator, it is then enough to prove that each of the $S_w = Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w) - (Y \otimes \mathcal{I})(w)$ matrices are positive semidefinite, where $(Y \otimes \mathcal{I})(w)$ denotes $Y \otimes \mathcal{I}$ restricted to the rows/columns of $Q^{\otimes n}_{0,1/\sqrt{2},\theta}$ assigned to $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$.

Consider first the largest of these matrices. This will be S_{0^n}, with size 2^n. Using (47), we have that it is given by

$$S_{0^n} = \left(\frac{1}{2}\right)^n \sum_{a,c\in\{0,1\}^n} |aa\rangle\langle cc| \Big(\prod_{i=0}^{n-1}\Big(\delta_{a_i,1-c_i}\cdot -\sin(\theta)\cos(\theta) + \delta_{a_i,c_i}\delta_{a_i,1}\cos(\theta)^2 + \delta_{a_i,c_i}\delta_{a_i,0}\sin(\theta)^2\Big) - 2^n\lambda_a\Big).$$

For example, for $n = 2$, S_{00} is given by

$$\frac{1}{4}\begin{pmatrix} \sin(\theta)^4 - 4\lambda_{00} & -\sin(\theta)^3\cos(\theta) & -\sin(\theta)^3\cos(\theta) & \sin(\theta)^2\cos(\theta)^2 \\ -\sin(\theta)^3\cos(\theta) & \sin(\theta)^2\cos(\theta)^2 - 4\lambda_{01} & \sin(\theta)^2\cos(\theta)^2 & -\sin(\theta)\cos(\theta)^3 \\ -\sin(\theta)^3\cos(\theta) & \sin(\theta)^2\cos(\theta)^2 & \sin(\theta)^2\cos(\theta)^2 - 4\lambda_{10} & -\sin(\theta)\cos(\theta)^3 \\ \sin(\theta)^2\cos(\theta)^2 & -\sin(\theta)\cos(\theta)^3 & -\sin(\theta)\cos(\theta)^3 & \cos(\theta)^4 - 4\lambda_{11} \end{pmatrix}$$

Consider now that since $Q^{\otimes n}_{0,1/\sqrt{2},\theta} \geq 0$, and for $a \neq 1^n$, $\lambda_a < 0$, the first $2^n - 1$ principal minors of S_{0^n} are ≥ 0. By Sylvester's criterion, to prove that $S_{0^n} \geq 0$, it suffices then to prove that $\det(S_{0^n}) \geq 0$. Note that $\det(S_{0^n})$ is a polynomial in ϵ. This polynomial has all the coefficients below the one for ϵ^{2^n-1} equal to 0. This is because $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(0^n)$ has rank 1 - therefore, each minor of it with at least two rows will have determinant equal to zero. Using this, and going through the determinant formula, we see that $\det(S_{0^n})$ is given by

$$\left(\epsilon^{2^n-1}(-1)^{2^n-1}\sum_{a\in\{0,1\}^n}\left(\frac{1}{2}\right)^n\cos(\theta)^{2|a|}\sin(\theta)^{2(n-|a|)}\prod_{\substack{b\in\{0,1\}^n\\ b\neq a}}\frac{\lambda_b}{\epsilon}\right)$$

$$+\left(\epsilon^{2^n}(-1)^{2^n}\prod_{a\in\{0,1\}^n}\frac{\lambda_a}{\epsilon}\right) \tag{53}$$

$$=\epsilon^{2^n-1}\left(\epsilon - \sum_{a\in\{0,1\}^n}\frac{\left(\frac{1}{2}\right)^n\cos(\theta)^{2|a|}\sin(\theta)^{2(n-|a|)}}{\lambda_a/\epsilon}\right)\prod_{a\in\{0,1\}^n}\frac{\lambda_a}{\epsilon} \tag{54}$$

$$=\epsilon^{2^n-1}\left(\epsilon + \sum_{a\in\{0,1\}^n}\left(\frac{1}{2}\right)^{n/2}\cos(\theta)^{|a|}\sin(\theta)^{n-|a|} - 2\left(\frac{1}{2}\right)^{n/2}\cos(\theta)^n\right)\prod_{a\in\{0,1\}^n}\frac{\lambda_a}{\epsilon} \tag{55}$$

Since all of the λ_a/ϵ except the one for 1^n are negative, we have that $\epsilon^{2^n-1}\prod_{a\in\{0,1\}^n}\frac{\lambda_a}{\epsilon}$ is negative whenever $\epsilon > 0$. Therefore,

$$\det(S_{0^n,0^n}) \geq 0 \iff \tag{56}$$

$$\epsilon + \sum_{a\in\{0,1\}^n}\left(\frac{1}{2}\right)^{n/2}\cos(\theta)^{|a|}\sin(\theta)^{n-|a|} - 2\left(\frac{1}{2}\right)^{n/2}\cos(\theta)^n \leq 0 \iff \tag{57}$$

$$\epsilon \leq \left(\frac{1}{2}\right)^{n/2}\left(2(\cos(\theta))^n - (\cos(\theta)+\sin(\theta))^n\right), \tag{58}$$

which is true by definition of ϵ. We have then that our proposed feasible solution Y produces a positive-semidefinite S_{0^n}. To verify the feasibility of Y, it remains to prove the positive-semidefiniteness of the rest of the S_w.

To do so, consider an arbitrary S_w, $w \in \{0,1,2\}^n - \{0^n\}$, with a corresponding M_w, as defined in (48). Note that M_w is the set of indices such that λ_i appears in the diagonal of S_w, and that that each λ_i appears in the diagonal of S_w at most once, as we can see from the expression in (48). If $1^n \notin M_w$, then S_w is trivially positive-semidefinite, since it is obtained by adding a positive-semidefinite diagonal matrix $Y(w)$ to a positive-semidefinite matrix $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$. Otherwise, our appeal to Sylvester's criterion from the 0^n case applies again, and it is enough to prove that $\det(S_w) \geq 0$. Also, since $Q^{\otimes n}_{0,1/\sqrt{2},\theta}(w)$ has rank 1, our argument that $\det(S_w)$ is a polynomial of minimum degree $|M_w| - 1$ applies again.

Then, using (48), we have that $\det(S_w)$ is given by

$$\epsilon^{|M_w|-1}\left(\prod_{c\in M_w}\frac{\lambda_c}{\epsilon}\right)\left(\epsilon - \left(\frac{1}{2}\right)^n \sum_{d\in M_w}\frac{g(w,d)}{\lambda_d/\epsilon}\right) \tag{59}$$

Using the recursive definition of M_w in (48), and realizing that $1^n \in M_w$ implies that $n_1(w) = 0$, we have that

$$\sum_{d\in M_w}\frac{g(w,d)}{|\lambda_d/\epsilon|} = \left(\frac{1}{2}\right)^{n/2}(\sin(\theta)+\cos(\theta))^{n_0(w)}\left(\frac{1}{\cos(\theta)}\right)^{n_2(w)}. \tag{60}$$

Now, we have that

$$\frac{1}{\cos(\theta)} \leq \sin(\theta)+\cos(\theta) \iff \frac{1}{\cos(\theta)^2} \leq \tan(\theta)+1 \tag{61}$$

$$\iff \tan(\theta)^2 \leq \tan(\theta) \iff \theta \leq \pi/4 \tag{62}$$

Since we are looking at the range $\theta < \theta_{n,1/\sqrt{2}} \leq \pi/4$, and $n_0(w) + n_2(w) = n$, we have that

$$(\sin(\theta)+\cos(\theta))^{n_0(w)}\left(\frac{1}{\cos(\theta)}\right)^{n_2(w)} \leq (\sin(\theta)+\cos(\theta))^n. \tag{63}$$

Therefore, since $n_2(w) \leq n$,

$$\left(\frac{1}{2}\right)^n \sum_{d\in M_w}\frac{g(w,d)}{\lambda_d/\epsilon} \geq \left(\frac{1}{2}\right)^{n/2}\left(2(\cos(\theta))^n - (\cos(\theta)+\sin(\theta))^n\right). \tag{64}$$

We see then that any ϵ that makes $\det(S_{0^n})$ non-negative will make the determinant of the other S_w non-negative as well.

A.4.4 Generalization to $\alpha \neq 1/\sqrt{2}$

For $\alpha \neq 1/\sqrt{2}$, the changes necessary to make the proof work are limited to arithmetic adjustments. $Q^{\otimes n}_{0,\alpha,\theta}$ will now be given by

$$\sum_{a,c\in\{0,1\}^n}|a\rangle\langle c| \otimes \sum_{b,d\in\{0,1\}^n}|b\rangle\langle d| \prod_{i=0}^{n-1}\Big(\delta_{a_i,1-b_i}\delta_{c_i,1-d_i}\delta_{a_i,c_i}\Big(\delta_{a_i,1}(1-\alpha^2)+\delta_{a_i,0}\alpha^2\Big)$$
$$+\delta_{a_i,b_i}\delta_{c_i,d_i}\Big(\delta_{a_i,1-c_i}\cdot -\alpha\sin(\theta)\sqrt{1-\alpha^2}\cos(\theta)+\delta_{a_i,c_i}\delta_{a_i,1}(1-\alpha^2)\cos(\theta)^2$$
$$+\delta_{a_i,c_i}\delta_{a_i,0}\alpha^2\sin(\theta)^2\Big)\Big). \tag{65}$$

Note that its direct sum decomposition is not affected, since the choice of which terms of $Q_{0,\alpha,\theta}^{\otimes n}$ appear on each term does not depend on α.

Similarly, Y is given now by

$$\sum_{a\in\{0,1\}^n} \lambda_a |a\rangle\langle a|, \text{ where } \lambda_a = \begin{cases} -\epsilon(\alpha\sin(\theta))^{n-|a|}\left(\sqrt{1-\alpha^2}\cos(\theta)\right)^{|a|} & \text{for } a \neq 1^n \\ \epsilon\left(\sqrt{1-\alpha^2}\right)^n \cos(\theta)^n & \text{for } a = 1^n \end{cases}$$
$$\text{and } \epsilon = 2\left(\sqrt{1-\alpha^2}\cos(\theta)\right)^n - (\sqrt{1-\alpha^2}\cos(\theta) + \alpha\sin(\theta))^n. \tag{66}$$

As for the feasibility of Y, we have then that $\det(S_w)$ is given by

$$\epsilon^{|M_w|-1}\left(\prod_{c\in M_w}\frac{\lambda_c}{\epsilon}\right)\left(\epsilon - \sum_{d\in M_w}\frac{g(w,d)\alpha^{2(n-|d|)}(1-\alpha^2)^{|d|}}{\lambda_d/\epsilon}\right), \tag{67}$$

again non-negative whenever

$$\begin{aligned}\epsilon &\leq \sum_{d\in M_w}\frac{g(w,d)\alpha^{2(n-|d|)}(1-\alpha^2)^{|d|}}{\lambda_d/\epsilon} \\ &= 2\left(\sqrt{1-\alpha^2}\right)^n\cos(\theta)^{2n_0(w)-n} - \sum_{d\in M_w}\frac{g(w,d)\alpha^{2(n-|d|)}(1-\alpha^2)^{|d|}}{|\lambda_d|/\epsilon}.\end{aligned} \tag{68}$$

Note that we have now that using the recursive definition of M_w in (48),

$$\begin{aligned}&\sum_{d\in M_w}\frac{g(w,d)\alpha^{2(n-|d|)}(1-\alpha^2)^{|d|}}{|\lambda_d|/\epsilon} \\ =&(\alpha\sin(\theta)+\sqrt{1-\alpha^2}\cos(\theta))^{n_0(w)}\left(\frac{\sqrt{1-\alpha^2}}{\cos(\theta)}\right)^{n_2(w)}.\end{aligned}$$

To prove that (68) holds we will need an argument slightly more involved than the corresponding one for the $\alpha = \frac{1}{\sqrt{2}}$ case. First, we consider that for $n_0(w) = n$, the right hand side of (68) is equal to ϵ, by definition of ϵ. Then, we prove that the right hand side of (68) increases as we decrement $n_0(w)$, and increase $n_2(w) = n - n_0(w)$ in parallel. This is because the positive term in the right hand side increases with each decrease of $n_0(w)$, and it does so by a larger factor than the one by which the negative term decreases. More rigorously, consider the expression

$$k = \frac{1}{\cos(\theta)^2} - \frac{\sqrt{1-\alpha^2}}{\left(\alpha\sin(\theta)+\sqrt{1-\alpha^2}\cos(\theta)\right)\cos(\theta)}. \tag{69}$$

First, note that

$$k \geq 0 \iff \sqrt{1-\alpha^2}\cos(\theta)^2 \leq \left(\alpha\sin(\theta)+\sqrt{1-\alpha^2}\cos(\theta)\right)\cos(\theta) \tag{70}$$
$$\iff \cos(\theta) \leq \frac{\alpha}{\sqrt{1-\alpha^2}}\sin(\theta)+\cos(\theta) \tag{71}$$
$$\iff 0 \leq \frac{\alpha}{\sqrt{1-\alpha^2}}\sin(\theta), \tag{72}$$

which is always true when $0 \leq \theta \leq \pi/2$, which is always the case within the trigonometric domain that we consider. Then, if we denote the right hand side of (68) by $r_{n_0(w)}$, we have

the recursive relation

$$r_{n_0(w)} = r_{n_0(w)+1}\frac{1}{\cos(\theta)^2} + k(\alpha\sin(\theta) + \sqrt{1-\alpha^2}\cos(\theta))^{n_0(w)}\left(\frac{\sqrt{1-\alpha^2}}{\cos(\theta)}\right)^{n-n_0(w)}$$

We can see indeed that this defines an increasing sequence as we decrease $n_0(w)$, since the second summand is positive, and the first summand multiplies the previous value of r by an amount greater than one. We have then successfully proved that (68) holds in the $\alpha \neq \frac{1}{\sqrt{2}}$ case. ◀

A.5 Derivation for Theorem 7

Proof. For didactic purposes, we show our derivation along the line of thought used by us when obtaining it. Therefore, we first consider simple proofs for two particular cases, and then finish with a general proof.

A.5.1 Absence of hedging for the protocol in [30]

It is easy to establish that in a generalization of the example in [30] , the hedging behavior *disappears* if Bob can avoid returning an answer. This generalization considers the set of protocols where the initial quantum state shared between Alice and Bob is a pure state ψ such that $\mathrm{Tr}_{\mathcal{X}}(\psi\psi^*) = \mathcal{I}_{\mathcal{Z}}/\dim(\mathcal{Z})$. It suffices to prove it for one of such states, as the other ones can be obtained from it by Bob applying a unitary. We prove it then for

$$\psi = \frac{1}{\sqrt{\dim(\mathcal{X})}}\sum_i e_i \otimes e_i, \tag{73}$$

with e_i being the computational basis for $\mathcal{X}$, and corresponding to the case $\dim(\mathcal{X}) = \dim(\mathcal{Z})$.

The reason no hedging behavior is possible is because in this situation, it is always possible for Bob to make sure he obtains the desired outcome. To see this, notice that the operator that we apply to get Q_a from P_a is the identity divided by $\dim(\mathcal{X})$. Similarly, $E = \mathcal{I}_{\mathcal{X}\otimes\mathcal{Y}}/\dim(\mathcal{X})$. Therefore, $(E^+)^{1/2}Q_a(E^+)^{1/2} = P_a$. As this is a projector into a non-empty space (from the assumption that Bob has a nonzero probability of obtaining the desired outcome), the norm of this operator is 1.

A.5.2 Absence of hedging in the classical case

We look now at the behavior when a game is repeated twice in parallel, and the information exchanged between Alice and Bob is classical. This is reflected in the operators ρ and P_a we consider in our model being diagonal matrices. As ρ is a diagonal matrix, then Ψ_ρ maps diagonal matrices to diagonal matrices, so E and the Q_a are diagonal too. Then, if we denote by $\Omega(E)$ the matrix that has a one in a position whenever the corresponding entry of E is nonzero, and a zero otherwise, we have that

$$\|\Lambda_{1,2}\| = \left\|\Omega(E)\otimes\Omega(E) - \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)(Q_{1-a}\otimes Q_{1-a})\left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)\right\|.$$

Now, whenever $\Omega(E)$ has a zero entry, $(E^+)^{1/2}Q_{1-a}(E^+)^{1/2}$ has a zero entry as well in that position, as $Q_{1-a} \leq E$. We define now $\lambda_E(X)$ as the minimum entry of a diagonal matrix X, restricted to the positions where E has a nonzero entry. We have then that the

value of the game when Bob is trying to win one out of two parallel repetitions is given by:

$$\begin{aligned} &1-\lambda_E\Big((Q_{1-a}\otimes Q_{1-a})\left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)\left(Q_{1-a}\otimes Q_{1-a}\right)\Big)\\ &=1-\lambda_E\left((E^+)^{1/2}Q_{1-a}(E^+)^{1/2}\right)^2. \end{aligned} \tag{74}$$

Since we have that

$$\begin{aligned} \Omega(E)&=(E^+)^{1/2}E(E^+)^{1/2}\\ &=(E^+)^{1/2}(Q_a+Q_{1-a})(E^+)^{1/2}\\ &=(E^+)^{1/2}Q_{1-a}(E^+)^{1/2}+(E^+)^{1/2}Q_a(E^+)^{1/2} \end{aligned} \tag{75}$$

we have then that

$$\lambda_E\left((E^+)^{1/2}Q_{1-a}(E^+)^{1/2}\right)^2=1-\|(E^+)^{1/2}Q_a(E^+)^{1/2}\| \tag{76}$$

so

$$1-\lambda_E\left((E^+)^{1/2}Q_{1-a}(E^+)^{1/2}\right)^2=\|(E^+)^{1/2}Q_a(E^+)^{1/2}\|. \tag{77}$$

Therefore, there is no hedging in this case. Our argument applies similarly to the case where Bob is trying to win k out of n repetitions.

A.5.3 Absence of hedging in the general case

We begin by defining the following operators:

$$A=\Lambda=(E^+)^{1/2}Q_a(E^+)^{1/2}, B=(E^+)^{1/2}E(E^+)^{1/2}. \tag{78}$$

Note that $[Q_a,(E^+)E]=0$, as $(E^+)E$ is equal to the identity on the support of E and zero outside it, and $Q_a\le E$, so $E^+EQ_a=Q_aE^+E=Q_a$. We have then that $[A,B]=0$, so A and B are simultaneously diagonalizable. This means that any tensor products of A, B, and $\mathcal{I}$ of the same dimension are simultaneously diagonalizable as well.

We consider first the case where $k=1$ and $n=2$, and then use a proof by induction to take care of larger n and k. Using the operators A and B, we can use the fact that $Q_{1-a}=E-Q_a$ to write $\left\|\Lambda_{1,2}\right\|$ in terms of A and B as

$$\left\|A\otimes B+B\otimes A-A\otimes A\right\|\le\left\|A\otimes\mathcal{I}+\mathcal{I}\otimes A-A\otimes A\right\|=2\|A\|-\|A\|^2, \tag{79}$$

where the inequality follows from the fact that $0\le B\le\mathcal{I}$. The equality follows from considering a basis where A is diagonal, and using the fact that since $Q_a\le E$, $0\le A\le\mathcal{I}$, so all the eigenvalues of A are at most 1.

We have then that $\|\Lambda_{1,2}\|=1-(1-\|A\|)^2$, since the fact that Bob can just choose to play independently implies $\|\Lambda_{1,2}\|\ge 1-(1-\|A\|)^2$. Therefore, we obtain that playing each game independently is an optimal behavior.

In the general case where Bob is trying to win k out of n games, we can again express Q_{1-a} as $E-Q_a$, and thus reduce $\Lambda_{k,n}$ to a sum of tensor products of A and B.

Consider first the case where $k=1$. Then observe that we can write

$$\Lambda_{1,n}=\Lambda_{1,n-1}\otimes(B-A)+B^{\otimes n-1}\otimes A\le\Lambda_{1,n-1}\otimes(\mathcal{I}-A)+\mathcal{I}^{\otimes n-1}\otimes A \tag{80}$$

Using as basis the nth tensor product of a basis where A is diagonal, we obtain by induction on n that $\|\Lambda_{1,n}\| = 1-(1-\|A\|)^n$. This is because for diagonal positive semidefinite matrices $J \leq \mathcal{I}$ and K, we have $\|J(\mathcal{I}-K)+\mathcal{I}\cdot K\| = \|J\|(1-\|K\|)+\|K\|$.

Note as well that if x is a largest eigenvalue eigenvector of Λ, a maximum-eigenvalue eigenvector of $\Lambda_{1,n}$ is given by $x^{\otimes n}$. Using this fact, we obtain a proof for the case with $k > 1$. To do this, observe that

$$\Lambda_{k,n} = \Lambda_{k,n-1} \otimes (B-A) + \Lambda_{k-1,n-1} \otimes A \leq \Lambda_{k,n-1} \otimes (\mathcal{I}-A) + \Lambda_{k-1,n-1} \otimes A \tag{81}$$

Then, using again as basis the nth tensor product of a basis where A is diagonal, we obtain by induction that $\|\Lambda_{k,n}\| = 1-\sum_{t=0}^{k-1}\binom{n}{t}\|A\|^t(1-\|A\|)^{n-t}$, and that for all choices of k and n, a maximum-eigenvalue eigenvector of $\Lambda_{k,n}$ is given by $x^{\otimes n}$, for x a largest eigenvector of Λ. This is because for diagonal positive semidefinite matrices J, K, H, where J and H share a largest eigenvector, and $\|J\| \leq \|H\|$, we have $\|J(\mathcal{I}-K)+H\cdot K\| = \|J\|(1-\|K\|)+\|H\|\|K\|$.

We obtain then that in this setting, no quantum advantage can be obtained by correlating Bob's strategy between parallel repetitions. ◀

Multiparty Quantum Communication Complexity of Triangle Finding*

François Le Gall[1] and Shogo Nakajima[2]

1 **Department of Communications and Computer Engineering, Graduate School of Informatics, Kyoto University, Kyoto, Japan**
legall@i.kyoto-u.ac.jp

2 **Department of Computer Science, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, Japan**
nakajimashogo@is.s.u-tokyo.ac.jp

Abstract

Triangle finding (deciding if a graph contains a triangle or not) is a central problem in quantum query complexity. The quantum communication complexity of this problem, where the edges of the graph are distributed among the players, was considered recently by Ivanyos et al. in the two-party setting. In this paper we consider its k-party quantum communication complexity with $k \geq 3$. Our main result is a $\tilde{O}(m^{7/12})$-qubit protocol, for any constant number of players k, deciding with high probability if a graph with m edges contains a triangle or not. Our approach makes connections between the multiparty quantum communication complexity of triangle finding and the quantum query complexity of graph collision, a well-studied problem in quantum query complexity.

1998 ACM Subject Classification F.2.2 Nonnumerical Algorithms and Problems

Keywords and phrases Quantum communication complexity, triangle finding, graph collision

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.6

1 Introduction

1.1 Triangle finding

A triangle in an undirected graph $G = (V, E)$ is a set of three vertices v_1, v_2, and v_3 such that $\{v_1, v_2\}$, $\{v_1, v_3\}$, and $\{v_2, v_3\}$ are edges. The problem of deciding whether a given graph contains a triangle or not is called triangle finding, and has been the subject of thorough investigations in the past years in both the classical and quantum settings.

In the classical setting, several new applications of this problem have been discovered recently. In particular, Vassilevska Williams and Williams [20] showed in 2010 a surprising reduction from Boolean matrix multiplication to triangle finding. Several works followed (e.g., [17, 21]), which have now placed triangle finding as a central problem in the recent theory of fine-grained complexity.

In the quantum setting, triangle finding has played a prominent role in the development of quantum query algorithms. For query algorithms solving graph-theoretic problems like triangle finding, information about the set of edges E can be obtained only by queries

* This work is supported by the Grant-in-Aid for Young Scientists (A) No. 16H05853, the Grant-in-Aids for Scientific Research (A) No. 15H01677 and 16H01705, and the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Japan Society for the Promotion of Science and the Ministry of Education, Culture, Sports, Science and Technology in Japan.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 6; pp. 6:1–6:11
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

to an oracle representing the adjacency matrix of the input graph: given two vertices u and v of G, the oracle outputs one if $\{u, v\} \in E$ and zero if $\{u, v\} \notin E$ (in the quantum setting the queries can naturally be done in superposition). The trivial upper bound on the quantum query complexity of triangle finding is $O(n^{3/2})$, where n denotes the number of vertices of the graph, by Grover search. A series of works spreading over more than a decade [4, 7, 10, 12, 14, 16] successively improved this bound to $O(n^{5/4})$ by using more advanced techniques like quantum walks, learning graphs, variable costs quantum search and quantum nested walks. On the other hand, the best known lower bound on the quantum query complexity of triangle finding is the trivial $\Omega(n)$. Understanding whether the $O(n^{5/4})$ upper bound is tight or not is now the main open problem concerning the quantum query complexity of triangle finding in dense graphs. Several quantum query algorithms for triangle finding over sparse graphs have been constructed as well [6, 7, 8, 13].

1.2 Communication complexity of triangle finding

In this paper we consider triangle finding not in the quantum query complexity model, but in the quantum communication complexity model. As usual when considering graph-theoretic problems in the communication complexity setting, we assume that the edges of the graphs are distributed among the players (in this paper we consider the most general case where the subsets of edges owned by the players can overlap). In the two-party case, for instance, the first player Alice receives a set of edges $E_A \subseteq E$ and the second player Bob receives a set of edges $E_B \subseteq E$ such that $E_A \cup E_B = E$ (the intersection of these two sets is not necessarily empty). The players must decide if the whole graph contains a triangle or not. We will use $\mathsf{TF}^k_{n,m}$ to denote this distributed version of triangle finding, where k represents the number of players, $n = |V|$ and m is an upper bound on $|E|$.

The problem TF^2_{n,n^2} has been studied by Ivanyos et al. [9] and is well understood: its bounded-error quantum communication complexity is $\Theta(n)$. Indeed, it is easy to see that in the two-party setting triangle finding reduces to the computation of the disjointness[1] function $\mathsf{DISJ}_{n'}$ with $n' = n^2$. The upper bound then follows from the $O(\sqrt{n'})$-qubit protocol by Aaronson and Ambainis for disjointness [1]. The lower bound follows by combining the observation that conversely disjointness can be reduced to triangle finding with the $\Omega(\sqrt{n'})$-qubit lower bound on the quantum communication complexity of disjointness [19]. More generally, for possibly sparse graphs, the bounded-error quantum communication complexity of $\mathsf{TF}^2_{n,m}$ is $\Theta(\sqrt{m})$. Note that the classical bounded-error communication complexity of this problem is $\Theta(m)$: the upper bound follows from the trivial protocol where Alice sends all her input to Bob and the lower bound follows from lower bounds on the classical communication complexity of disjointness [11, 18].

1.3 Our contributions

In this paper, we consider the three-party quantum communication complexity of triangle finding, i.e., the problem $\mathsf{TF}^3_{n,m}$ where the edges of the graph are distributed among three players (Alice, Bob and Charlie). In the classical bounded-error communication complexity setting, the communication complexity of this problem is again $\Theta(m)$, since it is not easier than the two-party case (we can consider that one player has no edge as input). To our knowledge the quantum communication complexity of this problem has never been studied before the present work.

[1] The disjointness function $\mathsf{DISJ}_{n'}$ in the two-party setting is the following problem: Alice has a subset $x \subseteq \{1, \ldots, n'\}$, Bob has a subset $y \subseteq \{1, \ldots, n'\}$, and they want to decide if $x \cap y \neq \emptyset$.

Note that the communication complexity of $\mathsf{TF}^k_{n,m}$ for any constant $k > 3$ is equal (up to possible constant factors) to the communication complexity of $\mathsf{TF}^3_{n,m}$, which further motivates the study of the latter problem. Indeed, the former problem is again obviously not easier than the latter problem and, conversely, since a triangle consists of three edges, in the k-party case we can apply a protocol for the three-party case independently for each triple of players (the number of such triples is constant if k is constant) in order to decide whether the whole graph has a triangle or not.

Our main result is the following upper bound.[2]

▶ **Theorem 1.** *The bounded-error quantum communication complexity of* $\mathsf{TF}^3_{n,m}$ *is* $\tilde{O}(m^{7/12})$.

Let us briefly explain the main ideas that lead to the construction of our quantum protocol showing Theorem 1. The main part of the protocol consists of procedures simulating the quantum query algorithm for graph collision by Magniez, Santha, and Szegedy [16]. Indeed, for the dense case (i.e., $m \approx n^2$), it is fairly easy to see that a simple combination of a procedure implementing Grover search and another procedure simulating (in the communication complexity setting) the $\tilde{O}(n^{2/3})$-query algorithm for graph collision by Magniez, Santha, and Szegedy [16] gives the claimed $\tilde{O}(n^{7/6})$ upper bound. For sparse graphs, a first observation is that a quantum query algorithm for graph collision exploiting the sparsity of the given graph would help us to design an efficient quantum communication protocol for three-party triangle finding. However, whether graph collision can be solved with $O(n^{2/3-c})$ queries for some constant $c > 0$ even for $m = n^{4/3}$ (i.e., even when the graph is significantly sparse) is a long-standing open problem. To overcome this difficulty we consider a variant of graph collision, design a quantum algorithm for it based on quantum walks, and then show how to implement this algorithm efficiently in our setting of communication complexity (exploiting the property that each player has complete knowledge of part of the edges). We also divide the set of vertices of the graph into two sets: the set of vertices with degree smaller than n^s and the set of vertices with degree larger than n^s, where s is a parameter. This classification helps us, via Ambainis' variable costs quantum search technique [3], to reduce the communication cost needed to simulate the quantum algorithm for the variant of graph collision.

Next, we investigate whether the upper bound of Theorem 1 is tight. The trivial lower bound on the bounded-error quantum communication complexity of $\mathsf{TF}^3_{n,m}$ is $\Omega(\sqrt{m})$, since the three-party case is not easier than the two-party case. We first consider the dense case and observe that proving any better lower bound would require a breakthrough:

▶ **Proposition 2.** *If the bounded-error quantum communication complexity of* TF^3_{n,n^2} *is* $\Omega(n^{1+\epsilon})$ *for some constant* $\epsilon > 0$*, then the quantum query complexity of graph collision is* $\Omega(n^{1/2+\epsilon})$.

Proposition 2 indeed shows that proving any nontrivial lower bound on the quantum communication complexity of triangle finding would give a nontrivial lower bound on the quantum query complexity of graph collision (proving such a lower bound is a long-standing open problem in quantum query complexity). We then consider the sparse case. Theorem 1 implies that, for any value of m, any improvement over $\tilde{O}(m^{7/12})$ for the quantum communication complexity of $\mathsf{TF}^3_{n,m}$ would imply an improvement over $\tilde{O}(n^{7/6})$ for TF^3_{n,n^2} (since we can apply Theorem 1 with $n = \sqrt{m}$). We also show the following sparse version of Proposition 2:

[2] In Theorem 1 and through the paper, the notation $\tilde{O}(\cdot)$ removes the polylog(n) factors.

▶ **Proposition 3.** *If the bounded-error quantum communication complexity of* $\mathsf{TF}^3_{n,m}$ *is* $\Omega(m^{4/7+\epsilon})$ *for some* m *(seen as a function of* n*) and some constant* $\epsilon > 0$*, then the quantum query complexity of graph collision is* $\Omega(n^{1/2+\delta})$ *for some* $\delta > 0$*.*

Proposition 3 shows that giving a lower bound of the form $\Omega(m^{4/7+\epsilon})$ for some value $m < n^2$, and in particular showing that the bounds of Theorem 1 are optimal for some value of m, would also lead to a significant breakthrough. Note nevertheless that there is a gap between the best lower bound $\Omega(\sqrt{m})$ on the bounded-error quantum communication complexity of $\mathsf{TF}^3_{n,m}$ and the quantity $\Omega(m^{4/7})$ from Proposition 3. It thus still remains possible that in the sparse regime the trivial lower bound $\Omega(\sqrt{m})$ can be improved without any impact on the quantum query complexity of graph collision.

2 Preliminaries

2.1 Quantum communication complexity

Let $A_1, \ldots, A_k$ be k finite sets. Consider k players and assume that for each $i \in \{1, \ldots, k\}$ the i-th player receives as input an element $a_i \in A_i$. In the model of communication complexity, first introduced in the classical two-party setting by Yao [22], the players want to compute a function $f\colon A_1 \times \cdots A_k \to \{0,1\}$ by running a protocol such that, at the end of the protocol, each player outputs $f(a_1, \ldots, a_k)$, and they want to minimize the communication they need to compute the function f. In the quantum communication model, introduced by Yao [23], the players are allowed to communicate with qubits. More precisely, the quantum communication complexity of a quantum protocol $\mathcal{P}$ is the maximum (over all inputs) number of qubits that $\mathcal{P}$ sends. The bounded-error quantum communication complexity of f is the minimum communication complexity of any quantum protocol that computes f with probability (over the random coins used by the protocol) at least $2/3$.

2.2 Quantum query complexity of graph problems

For any finite set S and any $r \in \{1, \ldots, |S|\}$ we denote $\mathcal{X}(S, r)$ the set of all subsets of r elements of S.

Let $G = (V, E)$ be an undirected and unweighted graph, where V denotes the set of vertices and E denotes the set of edges. In the quantum query complexity setting, we only access the set of edges E through a quantum unitary operation $\mathcal{O}_G$ defined as follows. For any pair $\{u, v\} \in \mathcal{X}(V, 2)$, any bit $b \in \{0,1\}$, and any binary string $z \in \{0,1\}^*$, the operation $\mathcal{O}_G$ maps the basis state $|\{u,v\}\rangle|b\rangle|z\rangle$ to the state

$$\mathcal{O}_G|\{u,v\}\rangle|b\rangle|z\rangle = \begin{cases} |\{u,v\}\rangle|b \oplus 1\rangle|z\rangle & \text{if } \{u,v\} \in E, \\ |\{u,v\}\rangle|b\rangle|z\rangle & \text{if } \{u,v\} \notin E, \end{cases}$$

where $\oplus$ denotes the bit parity. Consider a quantum algorithm that computes some property of G. We say that the algorithm uses k queries if the operation $\mathcal{O}_G$, which is given as an oracle, is called k times by the algorithm.

We describe below two quantum query algorithms that we will use to construct our quantum protocol for $\mathsf{TF}^3_{n,m}$ in the communication complexity setting.

2.2.1 Quantum search with variable costs

Let X be a finite set of size N. Let $f_G\colon X \to \{0,1\}$ be a Boolean function depending on the input graph G. Assume that, for each $x \in X$, there exists a checking procedure $\mathcal{P}^x$ that

computes $f_G(x)$ using t_x queries to $\mathcal{O}_G$ with high probability. The goal is to find an element $x \in X$ such that $f_G(x) = 1$ if such an element exists. When we use Grover search, this task can be solved with $O(\sqrt{N} \times t_{max})$ queries with high probability, where $t_{max} = \max_{x \in X} t_x$. Ambainis [3] proposed a more general quantum algorithm, which solves with high probability this task using

$$\tilde{O}\left(\sqrt{\sum_{x \in X} t_x^2}\right)$$

queries. In this paper, we call this algorithm Ambainis' variable costs search.

2.2.2 Quantum walk over Johnson graphs

Let S be a finite set and r be an integer such that $1 \leq r \leq |S|$. Let $f_G \colon \mathcal{X}(S, r) \to \{0, 1\}$ be a Boolean function depending on a graph G. We say that a set $A \in \mathcal{X}(S, r)$ is marked if $f_G(A) = 1$. Consider the task whose goal is to find a marked set, if such a set exists, or report that there is no marked set. Ambainis [2] developed the quantum walk search approach, which solves this task using a quantum walk over a Johnson graph.

Let us first define Johnson graphs.

▶ **Definition 4.** Let X be a finite set and $k \in \{1, \ldots, |X|\}$. A Johnson graph $J(X, k)$ is an undirected graph with vertex set $\mathcal{X}(X, k)$ where two vertices $R, R^{'} \in \mathcal{X}(X, k)$ are adjacent if and only if $|R \cap R^{'}| = k - 1$.

The state of a quantum walk over a Johnson graph $J(S, r)$ corresponds to a vertex of the Johnson graph (i.e., to a set in $\mathcal{X}(S, r)$). The key idea of the quantum walk search approach is that each state A of the walk has a data structure $D(A)$, which in general depends on G. There are three costs of the walk to consider:

- Set up cost S: The worst case number of queries to $\mathcal{O}_G$ needed to construct $D(A)$ for $A \in \mathcal{X}(S, r)$.
- Update cost U: The worst case number of queries to $\mathcal{O}_G$ needed to update $D(A)$ to $D(A')$ when one step of the quantum walk is performed (i.e., a state A of the walk moves to A' for some $A' \in \mathcal{X}(S, r)$ such that $|A \cap A'| = r - 1$).
- Checking cost C: The worst case number of queries to $\mathcal{O}_G$ needed to check if the current set A is marked by using $D(A)$ (i.e., checking whether $f_G(A) = 1$).

Let $\varepsilon > 0$ be the fraction of marked sets. The quantum walk search approach finds a marked set if such a set exists with quantum query complexity

$$\tilde{O}\left(\mathsf{S} + \frac{1}{\sqrt{\varepsilon}}\left(\sqrt{r} \times \mathsf{U} + \mathsf{C}\right)\right),$$

with high probability (see [2, 15]).

2.3 Graph collision

Graph collision is a variant of collision problems such as element distinctness or two-to-one collision. In the quantum query complexity setting this problem is defined as follows. Given a known graph $G = (V, E)$ with $|V| = n$ and an oracle $f \colon V \to \{0, 1\}$, the graph collision problem asks whether there exists an edge $\{a, b\} \in E$ such that $f(a) = f(b) = 1$. The best known upper bound on the quantum query complexity of graph collision, obtained in [16] using quantum walks, is $\tilde{O}(n^{2/3})$. No lower bound better than the trivial $\Omega(\sqrt{n})$ is known.

In this paper, we consider the following three-party distributed version of graph collision, which is parametrized by two disjoint vertex sets $\mathcal{V}_A$, $\mathcal{V}_B$ such that $|\mathcal{V}_A| = |\mathcal{V}_B| = n$:

Three-Party Graph Collision, $\mathsf{GC}^3_{\mathcal{V}_A,\mathcal{V}_B}$
Alice's input: Boolean function $f_A : \mathcal{V}_A \to \{0,1\}$
Bob's input: Boolean function $f_B : \mathcal{V}_B \to \{0,1\}$
Charlie's input: set of edges $\mathcal{E}$ between $\mathcal{V}_A$ and $\mathcal{V}_B$
Output: $\mathsf{GC}^3_{\mathcal{V}_A,\mathcal{V}_B}(f_A, f_B, \mathcal{E}) = \bigvee_{\{i,j\}\in\mathcal{E}} f_A(i)f_B(j)$

This problem can be solved using $\tilde{O}(n^{2/3})$ qubits of communication by implementing, using standard techniques (see, e.g., [5]) to convert a query algorithm into a quantum protocol, the quantum query algorithm mentioned above since Charlie knows completely the set of edges $\mathcal{E}$ of the corresponding graph.

3 Upper Bound

In this section we show a quantum protocol for $\mathsf{TF}^3_{n,m}$ that has $\tilde{O}(m^{7/12})$-qubit communication complexity, which proves Theorem 1.

Let $G = (V, E)$, with E distributed among Alice, Bob and Charlie, be the input of $\mathsf{TF}^3_{n,m}$. Let E_A be the edges owned by Alice, E_B be the edges owned by Bob and E_C be the edges owned by Charlie. We will write $V = \{v_1, \ldots, v_n\}$. Let s be a parameter, to be chosen later, such that $0 \le s \le 1$.

3.1 Reduction to finding triangles in tripartite graphs

Observe that triangles with three edges in E_A (or three edges in E_B, or three edges in E_C) can be found without communication. Detecting if G contains a triangle with two edges in the same set (e.g., two edges in E_A and one edge in E_B) can be done easily with $O(\sqrt{m})$-qubit of communication, by a straightforward reduction to the two-party case and then using the two-party protocol from [9] described in the introduction. The hard case is detecting the existence of a triangle with one edge in E_A, one edge in E_B and one edge in E_C. We show below how to reduce this problem to triangle finding in some tripartite graph.

Consider the following tripartite graph G'. The set of vertices of G' is the union of the three sets $I = \{v_1^1, \ldots, v_n^1\}$, $J = \{v_1^2, \ldots, v_n^2\}$, and $K = \{v_1^3, \ldots, v_n^3\}$. The set of edges of G' is $\mathcal{E}_A \cup \mathcal{E}_B \cup \mathcal{E}_C$, where $\mathcal{E}_A$, $\mathcal{E}_B$ and $\mathcal{E}_C$ are constructed from E as follows:

- Put edges $\{v_s^1, v_t^2\}$ and $\{v_t^1, v_s^2\}$ to $\mathcal{E}_A$ if and only if $\{v_s, v_t\} \in E_A$.
- Put edges $\{v_s^1, v_t^3\}$ and $\{v_t^1, v_s^3\}$ to $\mathcal{E}_B$ if and only if $\{v_s, v_t\} \in E_B$.
- Put edges $\{v_s^2, v_t^3\}$ and $\{v_t^2, v_s^3\}$ to $\mathcal{E}_C$ if and only if $\{v_s, v_t\} \in E_C$.

Observe that, without communicating with each other, Alice, Bob and Charlie can construct the tripartite graph G' in the following sense: Alice can create $\mathcal{E}_A$, Bob can create $\mathcal{E}_B$, and Charlie can create $\mathcal{E}_C$.

Note that G' contains a triangle if and only if G contains a triangle with one edge in E_A, one edge in E_B and one edge in E_C. For instance, if the graph G contains a triangle consisting of three vertices v_a, v_b, v_c in V such that Alice has the edge $\{v_a, v_b\} \in E_A$, Bob has the edge $\{v_a, v_c\} \in E_B$, and Charlie has the edge $\{v_b, v_c\} \in E_C$, then the tripartite graph G' contains the triangle with three edges $\{v_a^1, v_b^2\} \in \mathcal{E}_A$, $\{v_a^1, v_c^3\} \in \mathcal{E}_B$ and $\{v_b^2, v_c^3\} \in \mathcal{E}_C$.

3.2 Protocol for dense graphs

The dense case is easy to deal with: we can simply combine Grover search (implemented in a distributed setting) with the protocol for graph collision mentioned in Section 2.3. This gives a quantum protocol with communication complexity $\tilde{O}(\sqrt{n} \times n^{2/3}) = \tilde{O}(n^{7/6})$. For later reference we state this upper bound as follows.

▶ **Proposition 5.** *The bounded-error quantum communication complexity of* TF^3_{n,n^2} *is* $\tilde{O}(n^{7/6})$.

3.3 Classifying the vertices of G'

For any vertex v in G', let us denote the degree of v by d_v. For any $v \in I$, let us denote the set of neighbors in J of v by $N^I_J(v)$, and denote the set of neighbors in K of v by $N^I_K(v)$. For any $v \in J$, let us denote the set of neighbors in I of v by $N^J_I(v)$, and denote the set of neighbors in K of v by $N^J_K(v)$. For any $v \in K$, let us denote the set of neighbors in I of v by $N^K_I(v)$, and denote the set of neighbors in J of v by $N^K_J(v)$. Alice, Bob, and Charlie classify all vertices in I into two sets:

$$I^s_h = \{v \in I \mid |N^I_J(v)| \geq n^s \text{ or } |N^I_K(v)| \geq n^s\},$$
$$I^s_l = I \setminus I^s_h,$$

all vertices in J into two sets:

$$J^s_h = \{v \in J \mid |N^J_I(v)| \geq n^s \text{ or } |N^J_K(v)| \geq n^s\},$$
$$J^s_l = J \setminus J^s_h,$$

all vertices in K into two sets:

$$K^s_h = \{v \in K \mid |N^K_I(v)| \geq n^s \text{ or } |N^K_J(v)| \geq n^s\},$$
$$K^s_l = K \setminus K^s_h.$$

We will say that a vertex v of G' is s-high if $v \in I^s_h \cup J^s_h \cup K^s_h$, and say it is s-low if $v \in I^s_l \cup J^s_l \cup K^s_l$.

The classification of I can be done with $\tilde{O}(\frac{m}{n^s})$ bits of communication as follows. Since Alice holds the set of edges $\mathcal{E}_A$ between I and J, Alice knows, with no communication, the set $\{v \in I \mid |N^I_J(v)| \geq n^s\}$. Then Alice sends this set to both Bob and Charlie with $\tilde{O}(\frac{|\mathcal{E}_A|}{n^s}) = \tilde{O}(\frac{m}{n^s})$ bits of communication. Since Bob holds the set of edges $\mathcal{E}_B$ between I and K, Bob knows, with no communication, the set $\{v \in I \mid |N^I_K(v)| \geq n^s\}$, and then sends this set to both Alice and Charlie with $\tilde{O}(\frac{|\mathcal{E}_B|}{n^s}) = \tilde{O}(\frac{m}{n^s})$ bits of communication. Thus they obtain the sets I^s_h and I^s_l with $\tilde{O}(\frac{m}{n^s})$-bit communication. Similarly, they can obtain the classifications of J and K using $\tilde{O}(\frac{m}{n^s})$ bits of communication.

3.4 Finding a triangle with a low vertex

The following proposition is the main technical contribution of this paper.

▶ **Proposition 6.** *The existence of a triangle of* G' *containing at least one* s*-low vertex can be checked in* $\tilde{O}(\sqrt{m}n^{s/6})$ *qubits of communication.*

Proof. Let us consider, without loss of generality, the case where Alice, Bob, and Charlie check if G' has a triangle with an s-low vertex in I^s_l. In this case, Alice simulates Ambainis'

variable costs search over I_l^s. The goal is to find one vertex (in I_l^s) of a triangle of $G^{'}$. For each $i \in I_l^s$ the checking procedure $\mathcal{P}^i$ of the search decides if there exists an edge $\{j,k\} \in \mathcal{E}_C$ such that $\{i,j,k\}$ is a triangle of $G^{'}$. The checking procedure $\mathcal{P}^i$ can be simulated as follows.

Let us fix $i \in I_l^s$. Let q be a parameter to be chosen later such that $0 \leq q \leq 1$. Alice and Bob define two bijective functions: $g_A^i \colon \{1,\ldots,|N_J^I(i)|\} \to N_J^I(i)$, and $g_B^i \colon \{|N_J^I(i)|+1,\ldots,|N_J^I(i)|+|N_K^I(i)|\} \to N_K^I(i)$, respectively. Then Alice and Bob send $|N_J^I(i)|$ and $|N_K^I(i)|$ to Charlie. After receiving the two values $|N_J^I(i)|$ and $|N_K^I(i)|$, Charlie simulates the following quantum walk search $\mathcal{A}_{\mathcal{W}}^i$ in order to check if there exists an edge in $\mathcal{E}_C$ that forms a triangle of $G^{'}$ with i. The walk $\mathcal{A}_{\mathcal{W}}^i$ searches for a set $R \in \mathcal{X}(\{1,\ldots,|N_J^I(i)|+|N_K^I(i)|\}, \lceil(|N_j(i)|+|N_K^I(i)|)^q\rceil) = \mathcal{X}(\{1,\ldots,d_i\},\lceil d_i^q\rceil)$ which contains two indices $x \in \{1,\ldots,|N_J^I(i)|\}$ and $y \in \{|N_J^I(i)+1,\ldots,|N_J^I(i)+|N_K^I(i)|\}$ such that $\{i, g_A^i(x), g_B^i(y)\}$ is a triangle of $G^{'}$. When the set of marked sets is not empty, the fraction of marked sets is

$$\varepsilon = \Omega\left(\left(|N_J^I(i)|+|N_K^I(i)|\right)^{2(q-1)}\right) = \Omega\left(d_i^{2(q-1)}\right).$$

The data structure $D(R)$ stores $\{(x, g_A^i(x)) \mid x \in R \cap \{1,\ldots,|N_J^I(i)|\}\}$ and $\{(y, g_B^i(y)) \mid y \in R \cap \{|N_J^I(i)|+1,\ldots,|N_J^I(i)|+|N_K^I(i)|\}\}$. In order to construct this data structure $D(R)$ of the initial state of the walk, Charlie asks Alice to send the vertex $g_A^i(r)$ to him if $r \leq |N_J^I(i)|$, and asks Bob to send the vertex $g_B^i(r)$ to him if $r > |N_J^I(i)|$, for each $r \in R$. More precisely, for any $r \in R$, Alice and Bob perform the following unitary operators $\mathcal{O}_{g_A^i}$, $\mathcal{O}_{g_B^i}$ to the basis state $|r\rangle|0\rangle$, respectively, where $|0\rangle$ consisting of $\lceil \log n\rceil$ qubits. For any $r \in R$, the unitary operator $\mathcal{O}_{g_A^i}$ maps the basis state $|r\rangle|0\rangle$ to the state

$$\mathcal{O}_{g_A^i}|r\rangle|0\rangle = \begin{cases} |r\rangle|g_A^i(r)\rangle & \text{if } r \leq |N_J^I(i)|, \\ |r\rangle|0\rangle & \text{if } r > |N_J^I(i)|. \end{cases}$$

For any $r \in R$, the unitary operator $\mathcal{O}_{g_B^i}$ maps the basis state $|r\rangle|0\rangle$ to the state

$$\mathcal{O}_{g_B^i}|r\rangle|0\rangle = \begin{cases} |r\rangle|g_B^i(r)\rangle & \text{if } r > |N_J^I(i)|, \\ |r\rangle|0\rangle & \text{if } r \leq |N_J^I(i)|. \end{cases}$$

Thus the setup communication cost of this walk is $\mathsf{S}_{\mathcal{C}} = \tilde{O}(|R|) = \tilde{O}(d_i^q)$ qubits. The update communication cost is $\mathsf{U}_{\mathcal{C}} = \tilde{O}(1)$ qubits, and the checking communication cost is $\mathsf{C}_{\mathcal{C}} = 0$. Thus Charlie can simulate, with high probability, the quantum walk search $\mathcal{A}_{\mathcal{W}}^i$ with

$$\tilde{O}\left(\mathsf{S}_{\mathcal{C}} + \sqrt{1/\varepsilon}\left(|R|^{1/2} \times \mathsf{U}_{\mathcal{C}} + \mathsf{C}_{\mathcal{C}}\right)\right) = \tilde{O}(d_i^q + d_i^{1-q/2}), \tag{1}$$

qubits of communication. Setting $q = \frac{2}{3}$ gives the upper bound $\tilde{O}(d_i^{2/3})$.

For each $i \in I_l^s$, Alice, Bob and Charlie can thus implement $\mathcal{P}^i$ with $\tilde{O}(d_i^{2/3})$ qubits of communication. Alice can therefore simulate Ambainis' variable costs search with

$$\tilde{O}\left(\sqrt{\sum_{i \in I_l^s}\left(d_i^{2/3}\right)^2}\right).$$

qubits of communication. To analyze this upper bound, we divide the set of s-low vertices I_l^s into subsets $I_{l,p}^s = \{i \in I_l^s \mid 2^{p-1} \leq d_i \leq 2^p\}$, for $p = 1,\ldots,\lceil \log n^s\rceil$. Note that $|I_{l,p}^s| = O(\frac{m}{2^{p-1}})$, for each $p = 1,\ldots,\lceil \log n^s\rceil$. The quantum communication complexity of

the quantum protocol is thus

$$\begin{aligned}
\tilde{O}\left(\sqrt{\sum_{i\in I_l^s} d_i^{4/3}}\right) &= \tilde{O}\left(\sqrt{\sum_{p=1}^{\lceil s\log n\rceil} |I_{l,p}^s|(2^p)^{4/3}}\right) \\
&= \tilde{O}\left(\sqrt{\sum_{p=1}^{\lceil s\log n\rceil} \frac{m}{2^{p-1}}(2^p)^{4/3}}\right) \\
&= \tilde{O}\left(\sqrt{\lceil s\log n\rceil \times m(2^{s\log n})^{1/3}}\right) \\
&= \tilde{O}\left(\sqrt{m(n^s)^{1/3}}\right) \\
&= \tilde{O}\left(\sqrt{m}n^{s/6}\right),
\end{aligned}$$

as claimed. ◀

3.5 Putting everything together

Checking if G' contains a triangle can be divided into four problems:

1. Checking if G' contains a triangle with one vertex in I_l^s, another vertex in J, and the other vertex in K.
2. Checking if G' contains a triangle with one vertex in I, another vertex in J_l^s, and the other vertex in K.
3. Checking if G' contains a triangle with one vertex in I, another vertex in J, and the other vertex in K_l^s.
4. Checking if G' contains a triangle with one vertex in I_h^s, another vertex in J_h^s, the other vertex in K_h^s.

Cases 1, 2 and 3 can be solved with $\tilde{O}(\sqrt{m}n^{s/6})$ qubits of communication, from Proposition 6. For case 4 (checking if G' contains a triangle with three s-high vertices), Alice, Bob, and Charlie directly use Proposition 5. Since $I_h^s = O(\frac{m}{n^s})$, $J_h^s = O(\frac{m}{n^s})$, and $K_h^s = O(\frac{m}{n^s})$, Case 4 can be solved with $\tilde{O}\left(\left(\frac{m}{n^s}\right)^{7/6}\right)$ qubits of communication.

Thus the total communication cost of the quantum protocol for $\mathsf{TF}^3_{n,m}$ is

$$\tilde{O}\left(\frac{m}{n^s} + m^{1/2}n^{s/6} + \frac{m^{7/6}}{n^{7s/6}}\right),$$

which is optimized by taking s such that $n^s = m^{1/2}$, giving the final quantum communication complexity of $\tilde{O}(m^{7/12})$.

4 Lower Bounds

In this section we give the proofs of Propositions 2 and 3. Let us denote by $\mathcal{Q}_{\mathsf{GC}}(n)$ the quantum query complexity of graph collision, when parametrized by graphs with n vertices.

Proof of Proposition 2. From the construction of the protocol giving the bound of Proposition 5, it follows that there exists a quantum protocol which computes, with high probability, TF^3_{n,n^2} with $\tilde{O}(\sqrt{n} \times \mathcal{Q}_{\mathsf{GC}}(n))$ qubits of communication. Thus, an $\Omega(n^{1+\epsilon})$ lower bound on the bounded quantum communication complexity of TF^3_{n,n^2} for some constant $\epsilon > 0$ implies an $\Omega(n^{1/2+\epsilon})$ lower bound on the quantum query complexity of graph collision. ◀

Proof of Proposition 3. Let s be a parameter such that $0 \leq s \leq 1$. From Section 3.5 and the construction of the protocol giving the bound of Proposition 5, it follows that there exists a quantum communication protocol which computes $\mathsf{TF}^3_{n,m}$ with bounded-error quantum communication complexity

$$\tilde{O}\left(\frac{m}{n^s} + m^{1/2}n^{s/6} + \sqrt{\frac{m}{n^s}} \times \mathcal{Q}_{\mathsf{GC}}(m/n^s)\right).$$

Suppose an $\Omega(m^{4/7+\epsilon})$ lower bound on the bounded-error quantum communication complexity of $\mathsf{TF}^3_{n,m}$ for some constant $\epsilon > 0$. Setting $n^s = m^{3/7+6\epsilon}$ gives the upper bound

$$\tilde{O}\left(m^{4/7+\epsilon} + m^{2/7-3\epsilon} \times \mathcal{Q}_{\mathsf{GC}}(m^{4/7-6\epsilon})\right).$$

This implies the claimed lower bound $\Omega(n^{\frac{2/7+4\epsilon}{4/7-6\epsilon}})$ on the quantum query complexity of graph collision. ◀

References

1. Scott Aaronson and Andris Ambainis. Quantum search of spatial regions. In *Proceedings of the 51st Symposium on Foundations of Computer Science*, pages 200–209, 2003.
2. Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.
3. Andris Ambainis. Quantum search with variable times. *Theory of Computing Systems*, 47(3):786–807, 2010.
4. Aleksandrs Belovs. Span programs for functions with constant-sized 1-certificates. In *Proceedings of the 44th Symposium on Theory of Computing*, pages 77–84, 2012.
5. Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Symposium on Theory of Computing*, pages 63–68, 1998.
6. Harry Buhrman, Christoph Dürr, Mark Heiligman, and Peter Høyer. Quantum algorithms for element distinctness. *SIAM Journal on Computing*, 34(6):1324–1330, 2005.
7. Titouan Carette, Mathieu Laurière, and Frédéric Magniez. Extended learning graphs for triangle finding. In *Proceedings of the 34th International Symposium on Theoretical Aspects of Computer Science*, pages 20:1–20:14, 2017.
8. Andrew M. Childs and Robin Kothari. Quantum query complexity of minor-closed graph properties. *SIAM Journal on Computing*, 41(6):1426–1450, 2012.
9. Gábor Ivanyos, Hartmut Klauck, Troy Lee, Miklos Santha, and Ronald de Wolf. New bounds on the classical and quantum communication complexity of some graph properties. In *Proceedings of the 32nd International Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 148–159, 2012.
10. Stacey Jeffery, Robin Kothari, and Frédéric Magniez. Nested quantum walks with quantum data structures. In *Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1474–1485, 2013.
11. Bala Kalyanasundaram and Georg Schintger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992.
12. François Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of the 28th Symposium on the Theory of Computing*, pages 216–225, 2014.
13. François Le Gall and Shogo Nakajima. Quantum algorithm for triangle finding in sparse graphs. In *Proceedings of the 26th International Symposium on Algorithms and Computation*, pages 590–600, 2015.

14 Troy Lee, Frédéric Magniez, and Miklos Santha. Improved quantum query algorithms for triangle finding and associativity testing. In *Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1486–1502, 2013.

15 Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. Search via quantum walk. *SIAM Journal on Computing*, 40(1):142–164, 2011.

16 Frédéric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007.

17 Mihai Patrascu. Towards polynomial lower bounds for dynamic problems. In *Proceedings of the 42nd Symposium on Theory of Computing*, pages 603–610, 2010.

18 Alexander A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, 1992.

19 Alexander A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya Mathematics*, 67(1):145–159, 2003.

20 Virginia Vassilevska Williams and Ryan Williams. Subcubic equivalences between path, matrix and triangle problems. In *Proceedings of the 51st Symposium on Foundations of Computer Science*, pages 645–654, 2010.

21 Virginia Vassilevska Williams and Ryan Williams. Finding, minimizing, and counting weighted subgraphs. *SIAM Journal on Computing*, 42(3):831–854, 2013.

22 Andrew C. Yao. Some complexity questions related to distributive computing (preliminary report). In *Proceedings of the 11th Symposium on Theory of Computing*, pages 209–213, 1979.

23 Andrew C. Yao. Quantum circuit complexity. In *Proceedings of the 34st Symposium on Foundations of Computer Science*, pages 352–361, 1993.

Improved Reversible and Quantum Circuits for Karatsuba-Based Integer Multiplication

Alex Parent[1], Martin Roetteler[2], and Michele Mosca[3]

1 **Institute for Quantum Computing, University of Waterloo, Waterloo, Canada**
alexparent@gmail.com
2 **Quantum Architectures and Computation Group, Microsoft Research, Redmond, U.S.A.**
martinro@microsoft.com
3 **Institute for Quantum Computing, University of Waterloo, Waterloo, Canada**
mmosca@iqc.ca

Abstract

Integer arithmetic is the underpinning of many quantum algorithms, with applications ranging from Shor's algorithm over HHL for matrix inversion to Hamiltonian simulation algorithms. A basic objective is to keep the required resources to implement arithmetic as low as possible. This applies in particular to the number of qubits required in the implementation as for the foreseeable future this number is expected to be small. We present a reversible circuit for integer multiplication that is inspired by Karatsuba's recursive method. The main improvement over circuits that have been previously reported in the literature is an asymptotic reduction of the amount of space required from $O(n^{1.585})$ to $O(n^{1.427})$. This improvement is obtained in exchange for a small constant increase in the number of operations by a factor less than 2 and a small asymptotic increase in depth for the parallel version. The asymptotic improvement are obtained from analyzing pebble games on complete ternary trees.

1998 ACM Subject Classification F.1.1 Models of Computation, F.2 Analysis of Algorithms and Problem Complexity

Keywords and phrases Quantum algorithms, reversible circuits, quantum circuits, integer multiplication, pebble games, Karatsuba's method

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.7

1 Introduction

Multiplication of integers is a fundamental operation on a classical computer. In quantum computing, integer multiplication is also an important operation and indeed is at the core of what needs to be performed in order to carry out Shor's algorithm for factoring integers [30]. While much effort has been spent on optimizing the arithmetic needed to implement Shor's algorithm—e.g., via constant optimization [26], see also [27]—the basic underlying method for multiplication considered in most works is the simple school method for multiplying integers that runs in time $O(n^2)$ elementary operations. Elementary operations are here counted e.g. as the total number of Toffoli gates, which form a universal gate set. Significantly less effort has been spent on leveraging methods for fast multiplication which are well known classically, e.g., Karatsuba's method and other recursive methods.

Shor's factoring algorithm is special in that only multiplication by constants are required, which leads to significant simplifications in the circuits to implement Shor's algorithm [30]. For more general period finding problems, e.g., Hallgren's algorithm [15] and generalizations

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 7; pp. 7:1–7:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

to computing the unit group in number fields of arbitrary degree [14] and to computing class numbers and the principal ideal problem [6], more advanced arithmetic is required. This includes polynomial arithmetic which as a primitive building block requires integer multiplication $|x, y, 0\rangle \mapsto |x, y, xy\rangle$ where inputs x and y can *both* be in superposition.

Another example is the quantum algorithm for nonlinear structures [10]: a full circuit level implementation of this algorithm will require the implementation of polynomial arithmetic over a finite field, which typically is reduced to integer arithmetic. Further examples where integer multiplication is a useful primitive is to implement a fast quantum Fourier transform: it was shown in [12] that the computation of the Fourier transform can be reduced to integer multiplication, i.e., any fast algorithm for this problem gives rise to a quantum circuit for computing a Fourier transform on a quantum computer with the same time complexity.

Finally, the implementation of arithmetic functions such as integer multiplication is an important primitive for quantum simulation algorithms [5, 4, 23]. Once a full gate level implementation of the quantum simulation algorithms is performed, arguably arithmetic operations are useful to implement the indexing functions of row- and column-computable matrices that appear in the decomposition of the Hamiltonian that is to be simulated. A similar reasoning applies to HHL type algorithms for matrix inversion [16, 11], where the implementation of the underlying matrix may involve arithmetic operations such as integer multiplication for the computation of the entries.

A simple approach to integer multiplication is to reduce it to addition in a straightforward way by using n adders as in the familiar school method. If we let $Size(n)$ denotes the total size of a circuit—measured as the total number of Toffoli gates—where n is the bit-size of the numbers to be multiplied. $Depth(n)$ denotes the depth of the circuit, allowing gates to be applied in parallel, and $Space(n)$ denotes the total space requirements including input qubits, output qubits, and ancillas (i.e., qubits needed for intermediate scratch space), then the school method requires $Size(n) = Depth(n) = O(n^2)$ and $Space(n) = O(n)$.

Classically, Karatsuba's algorithm allows to reduce the circuit size from $O(n^2)$ to $O(n^{\log_2 3})$ by recursively decomposing the problem for size n into 3 subproblems of size $n/2$. However, there is an issue with applying this algorithm to the quantum case: while it is still possible to obtain a size reduction to $Size(n) = O(n^{\log_2 3})$, in the straightforward way of circuitizing the recursion also the space complexity increases, so that overall $O(n^{\log_2 3})$ qubit are required. This was observed in the earlier work [21], where also an improvement of the total depth to $O(n)$ was obtained, however, the number of qubits still scaled as $O(n^{\log_2 3})$.

As quantum memory is a very scarce commodity and indeed early quantum computers are expected to only support a few hundred or perhaps thousands of logical qubits, it is paramount to save space as much as possible. This leads to the question:

Can recursions be leveraged on a quantum computer in such a way that the space overhead does not grow as the total size of the circuit?

Or in a small variation of the above question: when considering the *volume* of a quantum circuit computing the integer product of two n bit numbers, where volume is defined as the circuit depth $\times$ circuit width, is it possible to compute this product in a volume that is strictly smaller than $O(n^{1+\log_2 3})$ which was the previously best volume?

Our results. The results of [21] and the results derived in this paper can be compared as in the following table. Here "parallel" and "sequential" refer to different ways the recursion was unraveled in [21], namely whether each of the 3 circuits for subroutine calls to problems of half size are arranged in parallel or are executed in sequence.

Sequential [21]	Parallel [21]	This paper
$Size(n) = O(n^{\log_2 3})$	$Size(n) = O(n^{\log_2 3})$	$Size(n) = O(n^{\log_2 3})$
$Depth(n) = O(n^{\log_2 3})$	$Depth(n) = O(n)$	$Depth(n) = O(n^{1.158})$
$Space(n) = O(n^{\log_2 3})$	$Space(n) = O(n^{\log_2 3})$	$Space(n) = O(n^{1.427})$

Our main result is to give an affirmative answer to the question whether it is possible to implement recursions in less space than the circuit size dictates. More precisely, our implementation requires $O(n^{1.427})$ qubits which improves slightly over $O(n^{\log_2 3}) = O(n^{1.585})$, as recorded up to 3 digits to the right of the decimal point in the last column of the table. For the total volume, defined as $Depth(n) \times Space(n)$, there is actually no advantage over [21] as it turns out that this quantity is asyptotically equal to $O(n^{1+\log_2 3})$.

To achieve the bounds shown in the table, we apply a pebble game analysis of the recurrence structure of the Karatsuba algorithm. In this case the underlying graph that needs to be pebbled with as few pebbles as possible is a complete ternary tree. Perhaps surprisingly, even for seemingly simple graphs such as the complete k-ary trees, where $k = 2$ or $k = 3$, the optimal pebble game for a fixed number of pebbles seems not to be known. We provide a heuristic which allows to pebble the ternary tree corresponding to a bitsize of n using $O(n\left(\frac{3}{2}\right)^{(\log_2 3)/(2\log_2 3-1)\log_2(n)}) = O(n^{1.427})$ pebbles. To the best of our knowledge, this is the first work that achieves an asymptotic improvement of the space complexity for integer multiplication while maintaining the $O(n^{\log_2 3})$ bound on the size of the quantum circuit.

Besides the mentioned work [21] which investigated Karatsuba-like circuits for integer multiplication, along similar lines there is also work for the case of binary multiplication, i.e., multiplication over the finite field $\mathbb{F}_{2^n}$. To analyze our algorithm we use the framework of pebble games as introduced by Bennett [3] to study space-time tradeoffs for reversible computations. The pebble games we study are played on directed acylic graphs that have the structure of ternary trees. In related work [20] pebbling of other classes of trees has been considered, in particular that of complete binary trees.

2 Preliminaries

The underlying gate model. As with classical circuits, reversible functions can be constructed from universal gate sets. It is known [24] that the Toffoli gate which maps $(x, y, z) \mapsto (x, y, z \oplus xy)$, together with the controlled-NOT gate (CNOT) which maps $(x, y) \mapsto (x, x \oplus y)$ and the NOT gate which maps $x \mapsto x \oplus 1$, is universal for reversible computation. When moving from reversible to quantum computations, gate sets go beyond the set of classical gates in that they allow to create so-called superposition of inputs. For instance, popular choices of universal quantum gate sets are the so-called Clifford+T gate set and the Toffoli+Hadamard gate set. Universality in this case means that it is possible to approximate any given target unitary operation that we intend to execute on a quantum computer by a finite-length sequence of operations over the given gate set. Herein the length of the sequence typically scales as a polynomial in $\log(1/\varepsilon)$ where ε is the target accuracy of the approximation, a result which has been established for the Clifford+T gate set [18, 29, 25] as well as probabilistic variants thereof [7, 8].

We point out that it is known that the Toffoli gate has an exact realization over Clifford+T [24], so all circuits for integer multiplication presented in this paper can be exactly implemented over this gate set as well. Furthermore, we refer the reader to [1] for more information

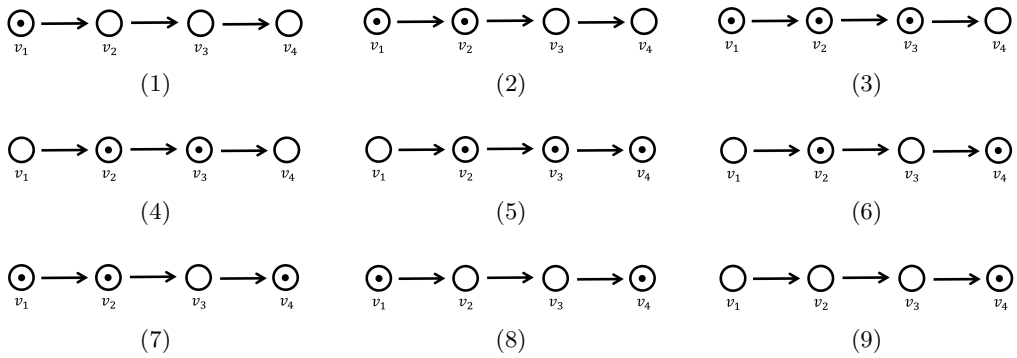

Figure 1 A pebble game played on a directed graph on 4 vertices. If 4 pebbles are available, one can simply proceed from left to right, pebbling one vertex at a time until the rightmost vertex is reached. After these 4 steps, all pebbles except the one on the right are removed, requiring a total of 7 steps. If only 3 pebbles are available, the optimal strategy for this game requires 9 moves which are shown in the subfigures (1) until (9).

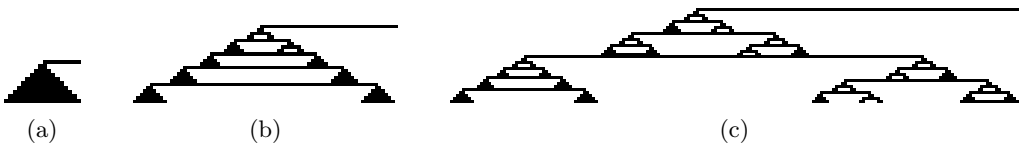

Figure 2 Visualization of three different pebble strategies. (a) Bennett's strategy; (b) middle-ground heuristic strategy; (c) Lange-McKenzie-Tapp method.

about the definition of T-depth and possible time-space tradeoffs for implementing Toffoli gates and other reversible gates over the Clifford+T gate set.

Pebble games. To study space-time tradeoffs in reversible circuit synthesis, Bennett [3] introduced reversible pebble games. This allow to explore ways to save on scratch space at the expense of recomputing intermediate results.

A pebble game is defined on a directed acyclic graph $G = (V, E)$, where $V_{in} \subseteq V$ is a special subset of vertices of in-degree 0, and $V_{out} \subseteq V$ is a subset of vertices of out-degree 0. In each step of the game, a pebble can either be put or be removed on a vertex v, provided that for all $w \in V$ such that $(w, v) \in E$ already a pebble has been placed on w. Typically, a total bound $S \geq 0$ on the number of available pebbles is given. Vertices in V_{in} can be pebbled at any time, provided enough pebbles remain. The task is to put a pebble on all vertices of V_{out} and to do so in the minimal number of moves possible. An example is given in Figure 1. Here $V = \{v_1, v_2, v_3, v_4\}$, $V_{in} = \{v_1\}$, $V_{out} = \{v_4\}$. It turns out that the optimal strategy for $S = 3$ requires 9 steps and the corresponding moves are shown in subfigures (1) until (9).

For a more formal treatment and further background information about pebble games we refer to [9]. If the graph on which the pebble game is played is a line, then the optimal pebbling strategies for a given space bound S can be computed in practice quite well using dynamical programming [19]. For general graphs, finding the optimal strategy is PSPACE complete [9], i.e., it is unlikely to be solvable efficiently.

In Figure 2 we display three different pebbling strategies that all succeed in computing a pebble game for the special case of linear graph, similar to one shown in Figure 1, but for much larger number of vertices. In Figure 2 time is displayed from left to right, vertices are

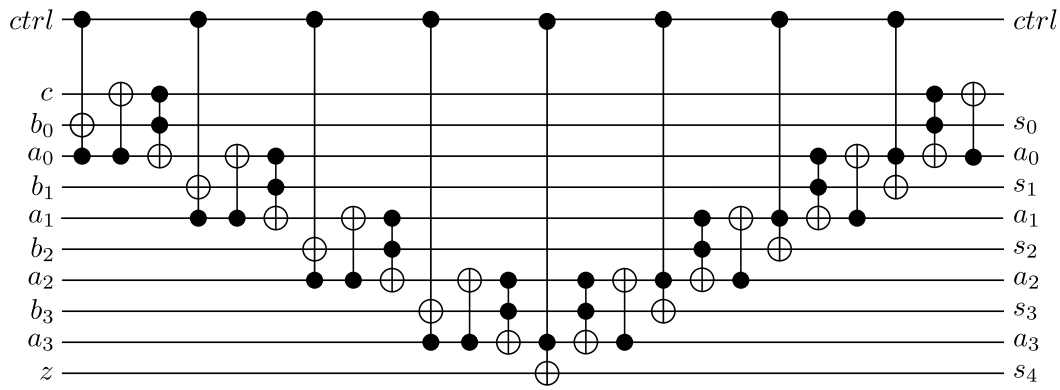

Figure 3 Controlled ripple adder based on Cuccaro et al. [13].

displayed vertically, with the vertex in V_{in} on the bottom and the vertex in V_{out} on top. The strategy shown in (a) corresponds to Bennett's compute-copy-uncompute method [2] where the time cost is linear. The strategy shown in (c) corresponds to the Lange-McKenzie-Tapp method [22] that resembles a fractal. In (b), a possible middle ground is shown, namely an incremental heuristic that first uses up as many pebbles as possible, then aggressively cleans up all bits except for the last bit, and the repeats the process until it ultimately runs out of pebbles.

For a line graph with $|V| = n$, the Lange-McKenzie-Tapp strategy requires only $O(\log(n))$ pebbles and has an overall number of $O(n \log(n))$ steps, i.e., it is known that the line can be optimally pebbled in a number of steps that scales poynomially with the number of vertices.

If the underlying graph G is a complete binary tree on n vertices such a polynomial bound is unfortunately not known. While it is known that the smallest number of pebbles required to pebble a binary tree of height h is given by $S = \log(h) + \Theta(\log^*(h))$, where $\log^*$ denotes the iterated logarithm, to our knowledge the best upper bound on the number of steps is $n^{O(\log\log(n))}$, given in [20]. It is an open problem if a binary tree on n vertices can be pebbled with a polynomial number of steps provided that only S pebbles are available, where S is as above. In this paper, we consider complete ternary trees as they arise naturally from the Karatsuba recursion. However, we do not strive for the optimal strategy and are content with a strategy that is good enough to give an asymptotic improvement.

3 Addition

Circuits for multiplication of integers naturally rely on circuits to add integers as subroutines, hence we first discuss circuits to perform addition. The adder shown in Fig. 3 is a circuit described in Cuccaro et al. [13] and forms the basis of simple multiplication circuits.

Note that not all the optimizations described in [13] are desirable in our context as we wish to minimize T gates when adding controls to the overall circuit. It can be observed that that every Toffoli gate in the basic circuit given in [13] shares its controls with another. We can therefore use "directional" Toffoli gates [28]. Each directional Toffoli uses four T-gates, requires one ancilla and has a T-depth of one. This circuit contains a total of $2n$ Toffoli gates and they are all in series. The adder therefore has $8n$ T-Gates and a total T-depth of $2n$.

To implement a controlled adder we further note that not all gates in this circuit need be controlled: controlling a set of gates which if removed would transform the circuit into the identity is sufficient. In the case of the in-place adder the MAJ and UMA subcircuits that

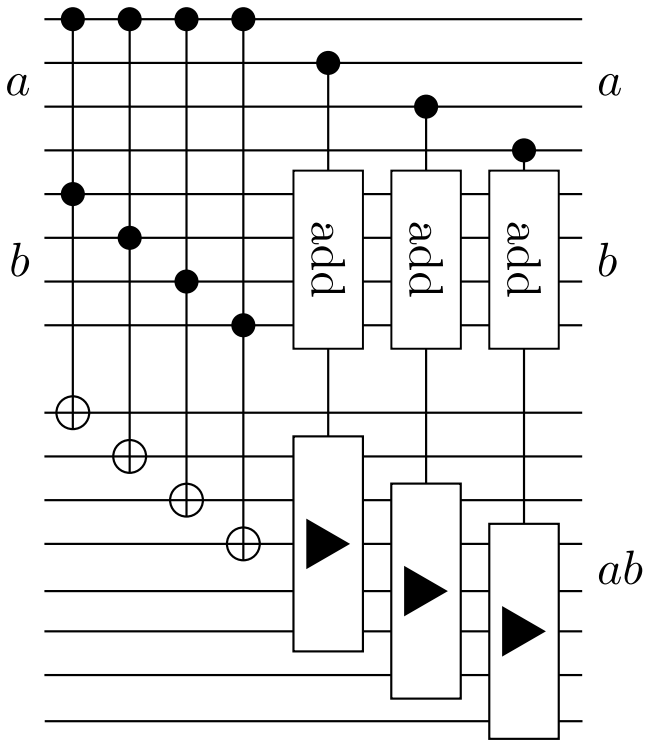

Figure 4 Controlled addition multiplier. In the above circuit notation the triangle designates the modified bits in the adder. The circuit consists of a sequence of controlled additions as in Fig. 3 with the exception of the first block which can be replaced by a cascade of Toffoli gates as the ancilla qubits at the bottom are initialized in the zero state. The total gate count scales asymptotically as $O(n^2)$.

were introduced in [13] can be made to cancel by removing one gate each. Figure 3 shows the resulting circuit. The circuit has a total number of $4n$ Toffoli gates, all of which are in series. Therefore, the total T-count of the controlled adder is $16n$ and the total T-depth is $4n$.

A simple $O(n^2)$ implementation of multiplication as a controlled addition circuit is shown in Fig. 4. Given two numbers as bit strings a and b their product can be found by repeatedly shifting forward by one and adding b to the result controlled on the next bit in a. The overall circuit is an out-of-place multiplier that uses only 1 additional ancilla for the adder circuits.

This circuit takes n Toffoli gates to copy down the initial value. It then uses $n-1$ controlled in place addition circuits to produce the final value. If we define A_n^{ctrl} to be the Toffoli count for a controlled adder of size n we get $M_n = n + (n-1)A_n^{ctrl}$, where M_n is the gate count for a controlled addition based multiplication circuit of size n. We know from the above discussion that the controlled addition circuit uses $4n$ Toffoli gates. This yields a total Toffoli count of the integer multiplication of

$$M_n = 4n^2 - 3n, \tag{1}$$

and a space complexity that scales linear with the number of qubits.

The rest of the paper will consider methods to reduce this total gate count to $O(n^{\log_2 3})$ while improving the amount of ancillas that are required to do so when compared to prior approaches.

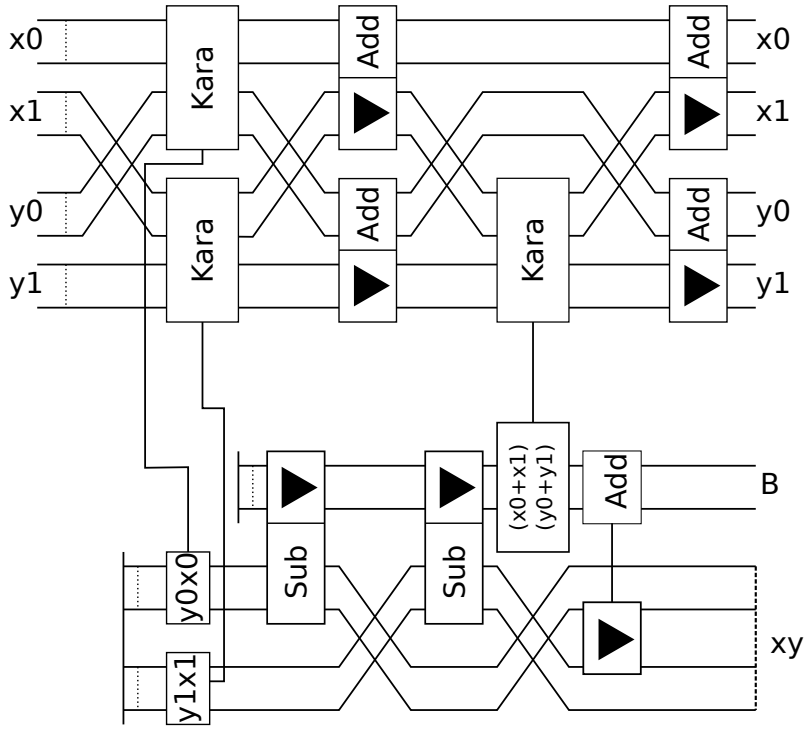

Figure 5 Karatsuba multiplication circuit. Besides the output (denoted "xy") this circuit outputs also the intermediate result "B" as in the Karatsuba recursion $xy = 2^n A + 2^{\lfloor n/2 \rfloor} B + C$ mentioned in the text. In order to remove B, we copy out the result "xy" and run the circuit backward. The main contribution of this paper is an analysis on when to perform this uncomputation as a function of the level of the recursion. Note that the final two adders return the inputs to their original state in order to save space. These adders can be removed at the cost of additional garbage bits.

4 Reversible Karatsuba multiplier

The following reversible algorithm for Karatsuba improves upon previous work [21]. It does this primarily by using in place addition to minimize garbage growth at each level. It also attempts to choose optimal splits instead of dividing the number in half at each step, This is helpful when the integer size is not a power of 2. Further an asymptotic improvement in space use (yielding as well an asymptotic improvement in the space-time product), is shown by using pebble games in the analysis.

Let $n \geq 1$ and let x and y be n-bit integers. The well-known Karatsuba [17] algorithm is based on the observation that by writing $x = x_1 2^{\lceil n/2 \rceil} + x_0$ and $y = y_1 2^{\lceil n/2 \rceil} + y_0$ the product xy can be evaluated as $xy = 2^n A + 2^{\lceil n/2 \rceil} B + C$, where

$$A = x_1 y_1,$$
$$B = (x_0 + x_1)(y_0 + y_1) - x_0 y_0 - x_1 y_1,$$
$$C = x_0 y_0.$$

Note that computation of A, B, and C only requires multiplication of integers that have bits size $n/2$, i.e., half the bit size of x and y. The final addition is carried out as the addition of n bit integers.

4.1 Analysis

Note that the cost for the computation of A, B, and C are 3 multiplications and four additions. Note further that the additions to compose the final result do not have to be carried out as the bit representation of xy is the concatenation of the bit representations of A, B, and C. For $m \geq 1$, let M_m^g denote the Toffoli cost of a circuit that multiplies m-bit inputs x and y using ancillas, i.e., a circuit that maps $(x, y, 0, 0) \mapsto (x, y, g(x, y), xy)$, where xy is a $2m$-bit output, and $g(x, y)$ is an garbage output on $k \geq 1$ bits. Furthermore, denote by A_m the cost for an (in-place) adder of two m-bit numbers. It is known that A_m can be bounded by at most $2m$ Toffoli gates. Let K_n denote the number of Toffoli gates that arise in the quantum Karatsuba algorithm (See Fig. 5). The outputs of one step of the recursion are x_0,x_1, y_0, y_1, x_0y_0, x_1y_1, and xy. It is easy to see that allowing garbage, K_n^g can be implemented using 3 multipliers of half the bit size, 4 in-place adders of size n and 4 in place adders of size $n/2$ (note the subtracters are just reversed adders). The base case is a multiplier for two one-bit numbers which can be done with one Toffoli gate, i.e., $K_1^g = 1$. We obtain the following recursion:

$$K_n^g = 3K_{n/2}^g + 4\left(A_n + A_{n/2}\right); \quad K_1^g = 1. \tag{2}$$

For the overall clean implementation of the Karatsuba algorithm we first run this circuit forward, copy out the final result using n CNOTs, and then run the whole circuit backward. This leads to an overall cost of $K_n = 2K_n^g$ and n CNOTs. For the moment we focus on the Toffoli cost only. By expansion we obtain that:

$$\begin{aligned} K_n^g &= 3^{\log_2(n)} K_1^g + 4\left(A_n + A_{n/2}\right) + 12\left(A_{n/2} + A_{n/4}\right) \\ &\quad + \ldots + 4 \cdot 3^{\log_2(n)-1}\left(A_2 + A_1\right). \end{aligned} \tag{3}$$

Using that the Toffoli cost of $A_{n/2^i}$ is $2(n/2^i)$, we obtain for the overall Toffoli cost the following bound:

$$\begin{aligned} K_n &= 2\left(3^{\log_2 n} + 4\sum_{i=0}^{\log_2 n - 1} 3^i 2(3n/2^i)\right) \\ &= 2n^{\log_2 3} + 48\,n\left(\frac{1-(3/2)^{\log_2 n}}{1-3/2}\right) \\ &= 2n^{\log_2 3} + 96\,n\left((3/2)^{\log_2 n} - 1\right) \leq 98\,n^{\log_2 3}. \end{aligned} \tag{4}$$

This bound can be improved by replacing the recursive call to Karatsuba with naive multiplication once a certain cutoff has been reached. In Fig. 6 we provide a comparison of various cutoff values (the naive method based on eq. (1) is also plotted for reference).

Another way to improve this algorithm is to attempt to choose more intelligent splits rather than always splitting the inputs in half at each level. This is important because the bit length of the numbers we are adding together may not be a power of two so dividing the input in two at each level might not be optimal. In Fig. 6 the line plotted as `aKara11` shows the result of using the optimal splits at each level. These were found by a simple dynamic program which evaluated the total gate size for every possible split at every level and chose the optimal ones. Using these methods we find an optimal cutoff value of 11 (see Fig. 7).

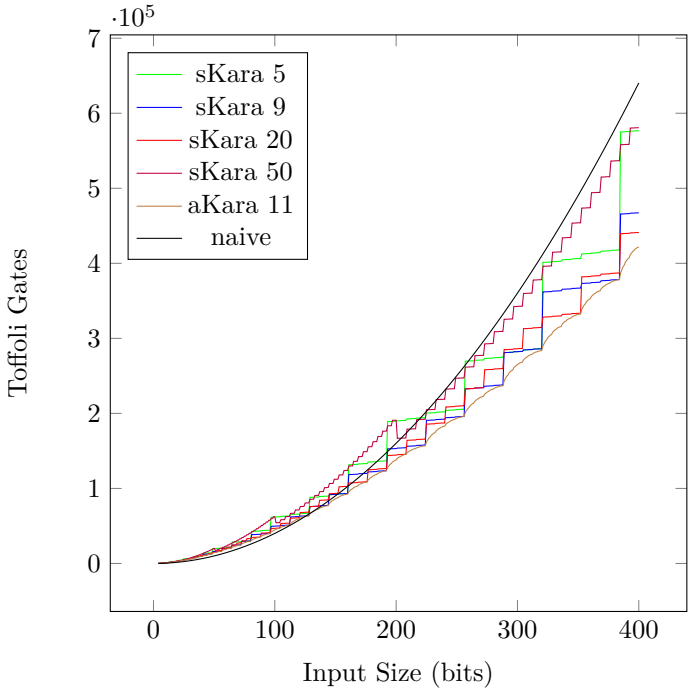

Figure 6 Plot of circuit sizes versus input size for various various Karatsuba cutoffs. The Legend shows the implementation (skara for the simple version and aKara for the adaptive cutoff) as well as a number indicating the cutoff size. For instance for a bit-size of $n = 400$ the naive method requires about $400n^2 = 640,000$ Toffoli gates, whereas the best strategy `aKara11` found by our search requires only about $422,000$ Toffoli gates.

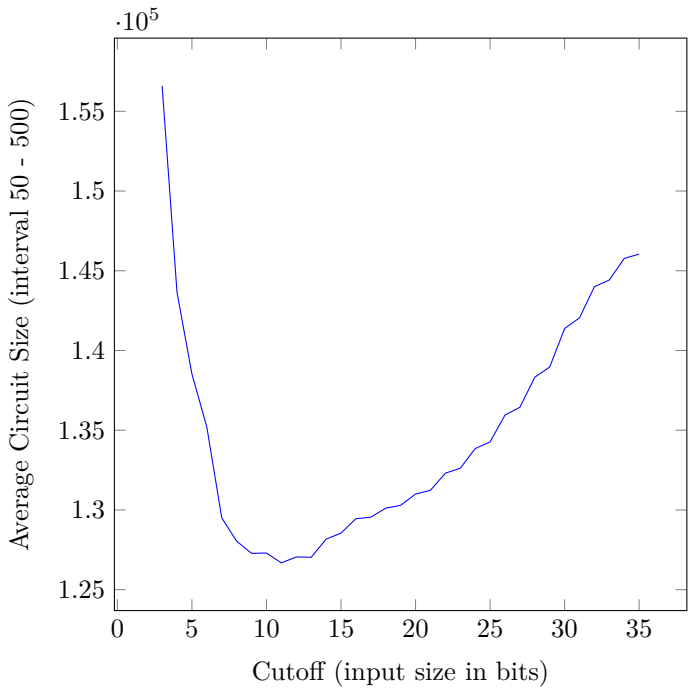

Figure 7 Average circuit size over the interval 50-500 for various cutoff values.

4.2 Time-space tradeoffs

We see in Figs. 6 and 9 that there are trade-offs available between circuits size and gate count available by changing the cutoff value. A higher cutoff value results in a larger naive multiplication circuits which are much more space efficient.

The reversible pebble game may be used to gain an asymptotic improvement in the space required to implement this algorithm. Note the tree structure of the recursive dependencies shown in Fig. 11. We find a level such that the size of each node's subtree is approximately equal to the size of the sum of all nodes at that level and above. Then for each node at that level in sequence compute the node and uncompute all nodes below it.

For the Karatsuba circuit on input of size n at a level x in the tree there are 3^x nodes of size $2^{-x}n$ for a total cost of

$$n\left(\frac{3}{2}\right)^x.$$

So the total cost of the full tree is given by

$$n\sum_{i=0}^{N}\left(\frac{3}{2}\right)^i,$$

where $N = \log_2 n$. To pebble the underlying ternary tree, we would like to break the tree into approximately equal sized subtrees at some level. Each tree at that level will be computed then uncomputed leaving only the top node. To minimize space we will choose the size of these subtrees to be approximately equal to the remaining size of the tree above them. In order to find the height k of such a tree we set:

$$\sum_{i=0}^{N-k-1}\left(\frac{3}{2}\right)^i = \frac{1}{2^{N-k}}\sum_{i=0}^{k-1}\left(\frac{3}{2}\right)^i.$$

Since this is a geometric series we can use the identity $\sum_{k=0}^{n-1} r^k = \frac{1-r^n}{1-r}$ which holds for all r and obtain

$$\frac{1-{}^3\!/_2{}^{N-k}}{1-{}^3\!/_2} = \frac{1}{2^{N-k}}\frac{1-{}^3\!/_2{}^k}{1-{}^3\!/_2}.$$

Rearranging terms, we obtain

$$1-{}^3\!/_2{}^{N-k} = 2^{k-N} - \frac{3^k}{2^N}.$$

Since $k \leq N$ and since we want that ${}^3\!/_2{}^{N-k} \geq \frac{3^k}{2^N}$ a simple calculation shows that this will be the case for $k \leq \frac{N}{2-\frac{\log 2}{\log 3}} = 0.731N$. The total space use without this optimization can be calculated as

$$n\sum_{k=0}^{\log_2 n-1}\left(\frac{3}{2}\right)^k = n\frac{1-({}^3\!/_2)^{\log_2 n}}{1-{}^3\!/_2}.$$

This gives space use of $O(n({}^3\!/_2)^{\log_2 n}))$ which is equivalent to $O(n^{\log_2 3})$ or approximately $O(n^{1.585})$. Using the above optimization we get space usage that can be bounded by

$$O\left(n\left(\frac{3}{2}\right)^{\left(\frac{\log 3}{2\log 3-\log 2}\log_2 n\right)}\right) \approx O(n^{1.427}).$$

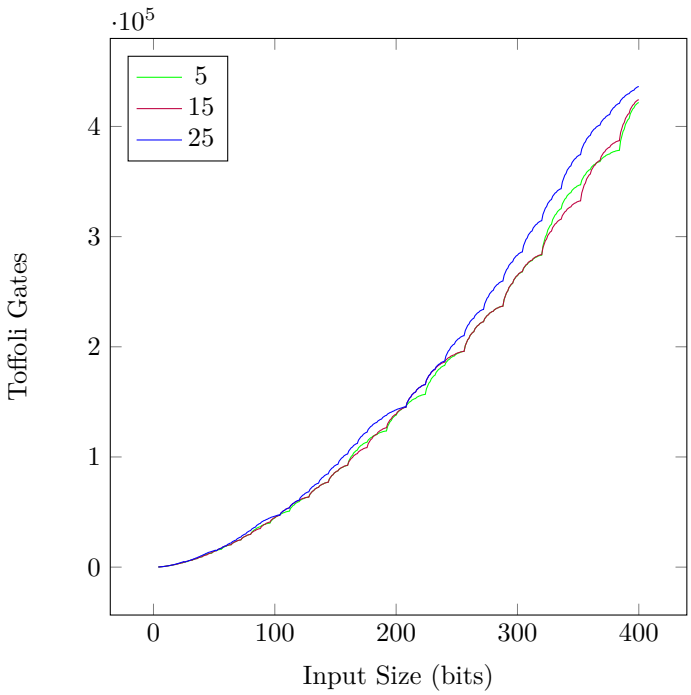

Figure 8 Comparison of various choices for adaptive cutoffs.

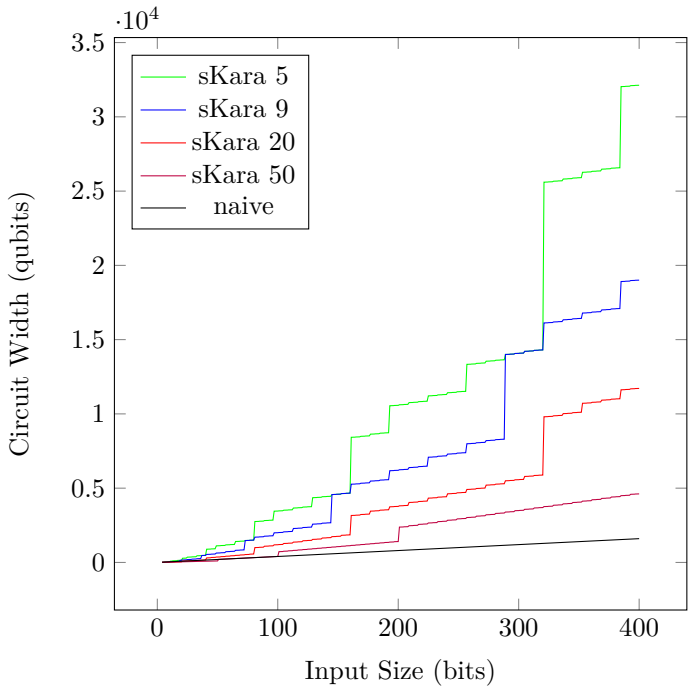

Figure 9 Qubits used versus input size for various Karatsuba cutoffs.

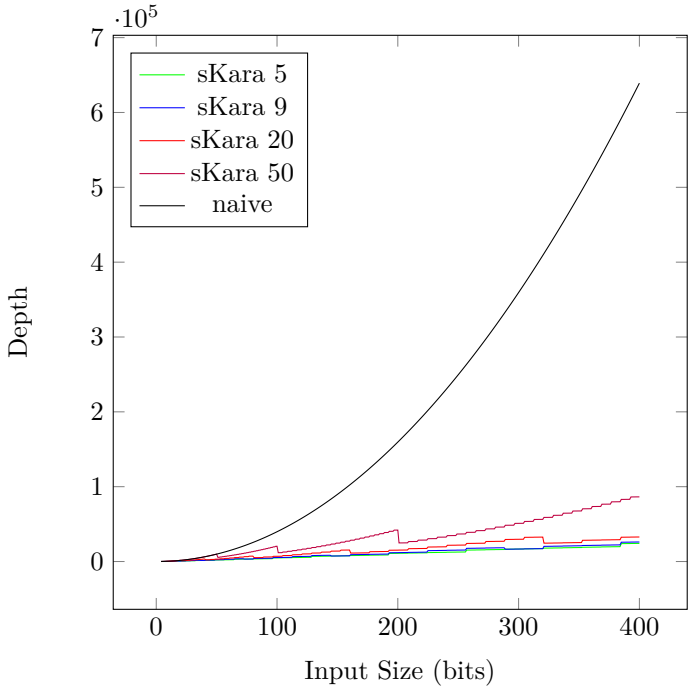

Figure 10 Toffoli depth versus input size for various Karatsuba cutoffs.

To find the depth of the circuit note that each node at level k must be computed sequentially. At level k the number of trees is

$$3^{\left(1-\frac{\log 3}{2\log 3-\log 2}\right)\log_2 n}.$$

Each tree is of depth

$$\frac{n}{2^{1-\frac{\log 3}{2\log 3-\log 2}}}.$$

This gives an overall depth for computing the k level of

$$n\left(\frac{3}{2}\right)^{\left(1-\frac{\log 3}{2\log 3-\log 2}\right)\log_2 n} \approx n^{1.158}.$$

Overall, we get a space-depth volume of our circuit that scales as $n^{1+\log_2 3}$.

4.3 Generalization to other recursions

Assume that we are given a function with input size n which splits a problem into a total of a subproblems of size n/b where the total cost to subdivide and recombine is $O(n)$. Then the overall work to compute the function for a problem of size n is given by:

$$n\sum_{i=0}^{N}\left(\frac{a}{b}\right)^i.$$

Solving as above we have:

$$k \leq \frac{\log_b n}{2-\frac{\log b}{\log a}}.$$

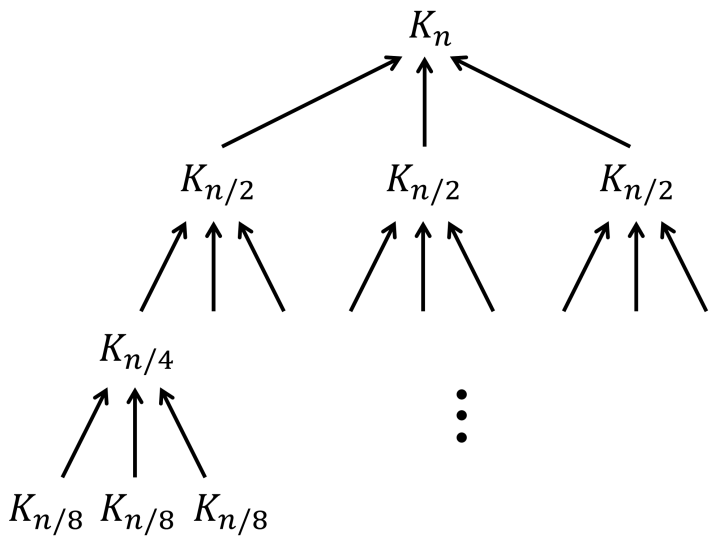

Figure 11 Structure of a pebble game for recursively implementing the Karatsuba circuit. Here K_i for $i = 1, 2, \ldots, n$ stands for the problem at level i, i.e., a problem with input-size i bits.

This means that our method is effective for recursive functions where the number of sub-problems is greater than the problem size reduction factor. This is intuitive since if the problem size reduction factor is equal to or greater than the number of sub-problems then adding up the total size of all nodes in levels above a given node will always result in a sum greater than or equal to the sum for that node's subtree.

By setting b in $\log b / \log a$ equal to 1 we get a square root reduction in space. This should be compared with a pebble game for complete binary graphs that was reported on in [20] in which a similar recursive structure was considered.

5 Conclusions and outlook

We considered the problem of optimizing the implementation of integer arithmetic on a quantum computer. Prior to our work, the state of the art was that in order to get a subquadratic overall gate count for a reversible multiplier a quite significant price had to be paid in that $O(n^{\log_2 3})$ qubits of memory were needed. By using pebble games played on the recursion tree, we find an improved number of ancillas needed for Karatsuba's recursion, which turns out to be upper bounded by $O(n^{1.427})$, while maintaining the asymptotic overall gate count of $O(n^{\log_2 3})$ for the number of gates. An interesting open problem is to apply these ideas to other recursions, which leads to the question of finding good pebbling strategies for trees of higher valency. Another open problem relates to the volume of the circuits for integer multiplication, specifically, whether it is possible to reduce the volume asymptotically below $O(n^{1+\log_2 3})$ and whether non-trivial space-time lower bounds for reversible integer multiplication can be shown that improve over the trivial $\Omega(n^2)$ lower bound for the volume.

Acknowledgments. The authors would like to thank BIRS for hosting Banff Seminar 16w5029: Quantum Computer Science, during which part of this research was carried out, and the anonymous referees for providing valuable feedback.

References

1. Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Trans. on CAD of Integrated Circuits and Systems*, 32(6):818–830, 2013. doi:10.1109/TCAD.2013.2244643.
2. Charles H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17:525–532, 1973.
3. Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM Journal on Computing*, 18:766–776, 1989.
4. Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Exponential improvement in precision for simulating sparse Hamiltonians. In *Symposium on Theory of Computing, STOC 2014*, pages 283–292, 2014.
5. Dominic W. Berry, Andrew M. Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015*, pages 792–809, 2015.
6. Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016*, pages 893–902, 2016.
7. Alex Bocharov, Martin Roetteler, and Krysta M. Svore. Efficient synthesis of probabilistic quantum circuits with fallback. *Physical Review A*, 91:052317, 2015.
8. Alex Bocharov, Martin Roetteler, and Krysta M. Svore. Efficient synthesis of universal Repeat-Until-Success circuits. *Physical Review Letters*, 114:080502, 2015.
9. Siu Man Chan. *Pebble games and complexity.* PhD thesis, Electrical Engineering and Computer Science, UC Berkeley, 2013. Tech report: EECS-2013-145.
10. Andrew M. Childs, Leonard J. Schulman, and Umesh V. Vazirani. Quantum algorithms for hidden nonlinear structures. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007)*, pages 395–404, 2007.
11. Brian D. Clader, Bryan C. Jacobs, and Chad R. Sprouse. Preconditioned quantum linear system algorithm. *Phys. Rev. Lett.*, 110:250504, 2013.
12. Richard Cleve and John Watrous. Fast parallel circuits for the quantum Fourier transform. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pages 526–536, 2000.
13. Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin, and David Petrie Moulton. A new quantum ripple-carry addition circuit. http://arxiv.org/abs/quant-ph/0410184, 2004.
14. Kirsten Eisenträger, Sean Hallgren, Alexei Y. Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Symposium on Theory of Computing, STOC 2014*, pages 293–302, 2014.
15. Sean Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *J. ACM*, 54(1):4:1–4:19, 2007.
16. Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for solving linear systems of equations. *Phys. Rev. Lett.*, 103:150502, 2009.
17. Anatoly Karatsuba and Yuri Ofman. Multiplication of many-digital numbers by automatic computers. *Doklady Akad. Nauk SSSR*, 145:293–294, 1962.
18. Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits. *Physical Review Letters*, 110:190502, 2013.
19. Emanuel Knill. An analysis of Bennett's pebble game. arXiv.org preprint quant-ph/9508218.
20. Balagopal Komarath, Jayalal Sarma, and Saurabh Sawlani. Pebbling meets coloring: reversible pebble game on trees. http://arxiv.org/abs/1604.05510.

21 Luis Antonio Brasil Kowada, Renato Portugal, and Celina Miraglia Herrera de Figueiredo. Reversible Karatsuba's algorithm. *Journal of Universal Computer Science*, 12(5):499–511, 2006.

22 Klaus-Jörn Lange, Pierre McKenzie, and Alain Tapp. Reversible space equals deterministic space. *J. Comput. Syst. Sci.*, 60(2):354–367, 2000.

23 Guang Hao Low and Isaac L. Chuang. Hamiltonian simulation by qubitization, 2016. arXiv:1610.06546.

24 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

25 Neil J. Ross and Peter Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information & Computation*, 16(11&12):901–953, 2016.

26 Mehdi Saeedi and Igor L. Markov. Constant-optimized quantum circuits for modular multiplication and exponentiation. *Quantum Information and Computation*, 12(5&6):361–394, 2012.

27 Mehdi Saeedi and Igor L. Markov. Synthesis and optimization of reversible circuits - a survey. *ACM Comput. Surv.*, 45(2):21, 2013.

28 Peter Selinger. Quantum circuits of T-depth one. *Phys. Rev. A*, 87:042302, 2013.

29 Peter Selinger. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information & Computation*, 15(1-2):159–180, 2015.

30 Peter W. Shor. Algorithms for quantum computation: discrete logarithm and factoring. In *Proc. FOCS'94*, pages 124–134. IEEE Computer Society Press, 1994.

Fidelity of Quantum Strategies with Applications to Cryptography*†

Gus Gutoski‡[1], Ansis Rosmanis[2], and Jamie Sikora§[3]

1 **Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada**
gus.gutoski@isara.com
2 **Centre for Quantum Technologies, National University of Singapore, Singapore and Nanyang Technological University, Singapore**
ansis@ntu.edu.sg
3 **Centre for Quantum Technologies, National University of Singapore, Singapore and MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore**
cqtjwjs@nus.edu.sg

Abstract

We introduce a definition of the fidelity function for multi-round quantum strategies, which we call the *strategy fidelity*, that is a generalization of the fidelity function for quantum states. We provide many interesting properties of the strategy fidelity including a Fuchs-van de Graaf relationship with the strategy norm. We illustrate an operational interpretation of the strategy fidelity in the spirit of Uhlmann's Theorem and discuss its application to the security analysis of quantum protocols for interactive cryptographic tasks such as bit-commitment and oblivious string transfer. Our analysis is very general in the sense that the actions of the protocol need not be fully specified, which is in stark contrast to most other security proofs. Lastly, we provide a semidefinite programming formulation of the strategy fidelity.

1998 ACM Subject Classification G.1.6 Optimization, K.6.5 Security and Protection, J.2 Physical Sciences and Engineering

Keywords and phrases Quantum strategies, cryptography, fidelity, semidefinite programming

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.8

1 Introduction

1.1 Review of quantum strategies

In this paper we consider multiple-round interactions between two parties involving the exchange of quantum information. There is a natural asymmetry between the parties as only one of the parties can send the first message or receive the final message. Since we are not

* Research at the Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. Research at the Centre for Quantum Technologies at the National University of Singapore is partially funded by the Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant "Random numbers from quantum processes," (MOE2012-T3-1-009). This material is based on research supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13.

† A full version of the paper is available at https://arxiv.org/abs/1704.04033.

‡ GG also acknowledges support from CryptoWorks21.

§ JS acknowledges support from NSERC Canada.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 8; pp. 8:1–8:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

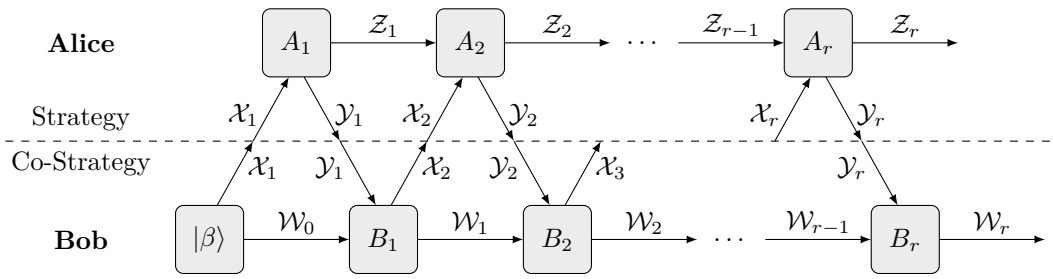

Figure 1 An r-round interaction between a pure strategy of Alice (the linear isometries above the dashed line) and a pure co-strategy of Bob (the linear isometries below the dashed line). Arrows crossing the dashed line represent messages exchanged between the parties, while horizontal arrows represent private memory.

concerned about optimizing the number of messages exchanged, without loss of generality both of these tasks are done by the same party, which, for convenience, we call *Bob*. Let us call the other party *Alice*. The interaction between Alice and Bob decomposes naturally into a finite number r of *rounds* (see Figure 1).

Such interactions are conveniently described by the formalism of quantum strategies introduced in Ref. [13]. We closely follow that formalism here with the exception that we consider two mathematically different objects: *strategies* and *pure strategies*. Pure strategies are implemented using linear isometries and preserve their final memory space, while strategies trace out the final memory space. The object we call a strategy is called a *non-measuring strategy* in Ref. [13]. For additional details on quantum strategies, one may refer to [13, 9, 11].

▶ **Definition 1** (Pure strategy and pure co-strategy)**.** Let $r \geq 1$ and let $\mathcal{X}_1, \ldots, \mathcal{X}_r, \mathcal{Y}_1, \ldots, \mathcal{Y}_r, \mathcal{Z}_r, \mathcal{W}_r$ be complex Euclidean spaces and, for notational convenience, let $\mathcal{X}_{r+1} := \mathbb{C}$ and $\mathcal{Z}_0 := \mathbb{C}$. An *$r$-round pure strategy* $\tilde{A}$ having *input spaces* $\mathcal{X}_1, \ldots, \mathcal{X}_r$, *output spaces* $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$, and *final memory space* $\mathcal{Z}_r$, consists of:

1. complex Euclidean spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_{r-1}$, called *intermediate memory spaces*, and
2. an r-tuple of linear isometries $(A_1, \ldots, A_r)$ of the form $A_i : \mathcal{X}_i \otimes \mathcal{Z}_{i-1} \to \mathcal{Y}_i \otimes \mathcal{Z}_i$.

An *r-round pure co-strategy* having input spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$, output spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r$, and final memory space $\mathcal{W}_r$, consists of:

1. complex Euclidean intermediate memory spaces $\mathcal{W}_0, \ldots, \mathcal{W}_{r-1}$,
2. a pure quantum state $|\beta\rangle \in \mathcal{X}_1 \otimes \mathcal{W}_0$, called the *initial state*, and
3. an r-tuple of linear isometries $(B_1, \ldots, B_r)$ of the form $B_i : \mathcal{Y}_i \otimes \mathcal{W}_{i-1} \to \mathcal{X}_{i+1} \otimes \mathcal{W}_i$.

A pure strategy and a pure co-strategy are said to be *compatible* when the input spaces of one are the output spaces of the other, and vice versa. The *final state* of the interaction between $\tilde{A}$ and $\tilde{B}$ is denoted by

$$|\psi(\tilde{A}, \tilde{B})\rangle := (I_{\mathcal{Z}_r} \otimes B_r)(A_r \otimes I_{\mathcal{W}_{r-1}}) \cdots (I_{\mathcal{Z}_1} \otimes B_1)(A_1 \otimes I_{\mathcal{W}_0})|\beta\rangle \in \mathcal{Z}_r \otimes \mathcal{W}_r.$$

In order to extract classical information from the interaction it suffices to permit Alice and Bob to measure their respective parts of the final state $|\psi(\tilde{A}, \tilde{B})\rangle$.

A pure strategy $\tilde{A}$ specified by linear isometries $(A_1, \ldots, A_r)$ can be represented by a single isometry

$$\tilde{A} := (A_r \otimes I_{\mathcal{Y}_{1\ldots r-1}}) \ldots (I_{\mathcal{X}_{3\ldots r}} \otimes A_2 \otimes I_{\mathcal{Y}_1})(I_{\mathcal{X}_{2\ldots r}} \otimes A_1) : \mathcal{X}_{1\ldots r} \to \mathcal{Y}_{1\ldots r} \otimes \mathcal{Z}_r,$$

where $\mathcal{X}_{i\ldots j}$ is short for $\mathcal{X}_i \otimes \cdots \otimes \mathcal{X}_j$ and $\mathcal{Y}_{i\ldots j}$ is short for $\mathcal{Y}_i \otimes \cdots \otimes \mathcal{Y}_j$. We abuse the notation[1] $\tilde{A}$ here and elsewhere in the paper by using it to denote both a pure strategy and the linear isometry representing it, and we do the same for pure co-strategies $\tilde{B}$, discussed next. A pure co-strategy $\tilde{B}$ specified by the initial state $|\beta\rangle$ and linear isometries $(B_1, \ldots, B_r)$ can be represented by a single isometry

$$\tilde{B} := (B_r \otimes I_{\mathcal{X}_{1\ldots r}}) \cdots (I_{\mathcal{Y}_{2\ldots r}} \otimes B_1 \otimes I_{\mathcal{X}_1})(I_{\mathcal{Y}_{1\ldots r}} \otimes |\beta\rangle) : \mathcal{Y}_{1\ldots r} \to \mathcal{X}_{1\ldots r} \otimes \mathcal{W}_r.$$

Note that two pure strategies that are represented by the same linear isometry are effectively indistinguishable, and the same holds true for pure co-strategies.

Any one party is not affected by what the other party does with their final memory space. Hence, from the point of view of that party, the other party can trace it out. In view of this, a *strategy* A is obtained from a pure strategy $\tilde{A}$ by tracing out the final memory space $\mathcal{Z}_r$ and a *co-strategy* B is obtained from a pure co-strategy $\tilde{B}$ by tracing out the final memory space $\mathcal{W}_r$. Multiple pure strategies (co-strategies) can yield the same strategy (co-strategy), and we call any such pure strategy (co-strategy) a *purification*. We will use tildes to indicate purifications.

Just as a pure strategy and a pure co-strategy can be specified by linear isometries $\tilde{A}$ and $\tilde{B}$, respectively, their corresponding strategy A and co-strategy B can be specified by quantum channels

$$\begin{aligned}\Phi_A &: \mathbf{L}(\mathcal{X}_{1\ldots r}) \to \mathbf{L}(\mathcal{Y}_{1\ldots r}) : X \mapsto \mathrm{Tr}_{\mathcal{Z}_r}(\tilde{A}X\tilde{A}^*),\\ \Psi_B &: \mathbf{L}(\mathcal{Y}_{1\ldots r}) \to \mathbf{L}(\mathcal{X}_{1\ldots r}) : Y \mapsto \mathrm{Tr}_{\mathcal{W}_r}(\tilde{B}Y\tilde{B}^*).\end{aligned}$$

In turn, both of these channels can be specified using their Choi-Jamiołkowski representations, but, due to the asymmetry between strategies and co-strategies, it is convenient to specify the latter one using the Choi-Jamiołkowski representation of its adjoint map. Thus, we can represent a strategy A by $J(\Phi_A)$ and a co-strategy B by $J(\Psi_B^*)$, both of which are positive semidefinite operators acting on $\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}$. In a similar abuse of notation as mentioned before, we refer to $J(\Phi_A)$ as the strategy A and to $J(\Psi_B^*)$ as the co-strategy B.

For compatible pure strategy $\tilde{A}$ and pure co-strategy $\tilde{B}$, let

$$\rho_A(\tilde{B}) := \mathrm{Tr}_{\mathcal{Z}_r}\left(|\psi(\tilde{A}, \tilde{B})\rangle\langle\psi(\tilde{A}, \tilde{B})|\right) \tag{1}$$

denote the reduced state of the final memory space $\mathcal{W}_r$ of $\tilde{B}$ after the interaction between $\tilde{A}$ and $\tilde{B}$. Since this state is the same for all purifications of A, we omit the tilde above A in this notation.

1.2 The definition of strategy fidelity

Recall that the fidelity $\mathrm{F}(P, Q)$ between two positive semidefinite operators P and Q is defined as

$$\mathrm{F}(P, Q) := \left\|\sqrt{P}\sqrt{Q}\right\|_{\mathrm{Tr}}.$$

When applied to density operators ρ, ξ, the fidelity function $\mathrm{F}(\rho, \xi)$ is a useful distance measure for quantum states. We would like to construct a generalization of the fidelity function that can serve as a useful distance measure for quantum strategies.

[1] It will be clear from context to which we are referring.

Just as the trace norm $\|\rho - \xi\|_{\mathrm{Tr}}$ quantifies the distinguishability of quantum states, the strategy norm $\|S - T\|_{\diamond\mathrm{r}}$ studied in [12] quantifies the distinguishability of quantum strategies S and T having the same input and output spaces. In other words, $\|S - T\|_{\diamond\mathrm{r}}$ is proportional to the maximum bias with which an interacting pure co-strategy $\tilde{B}$ can distinguish S from T. Another expression for this maximum bias can be derived as follows. Let $\mathcal{W}_r$ be the final memory space of $\tilde{B}$ and let $\rho_S(\tilde{B}), \rho_T(\tilde{B})$ be the reduced states of this final memory space after an interaction between $\tilde{B}$ and S, T, respectively, as defined in (1). It is clear that the maximum bias with which S can be distinguished from T is proportional to the maximum over all such $\tilde{B}$ with which the final state $\rho_S(\tilde{B})$ can be distinguished from $\rho_T(\tilde{B})$, which is precisely $\|\rho_S(\tilde{B}) - \rho_T(\tilde{B})\|_{\mathrm{Tr}}$.

▶ Remark. All purifications $\tilde{B}$ of B are equivalent up to a unitary acting on $\mathcal{W}_r$. Thus, unitarily invariant distance measures between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$ (including the trace distance and the fidelity) depend only upon B and not upon the specific purification $\tilde{B}$.

The strategy norm is defined so that

$$\|S - T\|_{\diamond\mathrm{r}} = \max_B \|\rho_S(\tilde{B}) - \rho_T(\tilde{B})\|_{\mathrm{Tr}}. \tag{2}$$

In light of this observation, we define the strategy fidelity by replacing the maximization of the trace distance between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$ with the minimization of the fidelity between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$.

▶ **Definition 2** (Strategy fidelity)**.** For any r-round strategies S and T having the same input and output spaces, the *strategy fidelity* is defined as

$$\mathrm{F}_{\mathrm{r}}(S, T) := \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) \tag{3}$$

where the minimization is over all compatible co-strategies B and the states $\rho_S(\tilde{B}), \rho_T(\tilde{B})$ are as defined in (1).

In the following discussion, we argue that this definition is a meaningful one by proving analogues of the Fuchs-van de Graaf inequalities and Uhlmann's Theorem for the strategy fidelity, among many other properties.

▶ Remark. The same definition of fidelity has been considered for the case of channels [2]. In that setting, they establish several properties which we generalize to the strategy setting.

First, let us observe that the fidelity for quantum states is recovered as a special case of the strategy fidelity when S, T are one-round strategies with no input (that is, $\mathcal{X}_1 = \mathbb{C}$) and only one output message. To see this, observe that one-round strategies such as S, T are simply states ρ, ξ acting on $\mathcal{Y}_1$. Bob's most general pure co-strategy is an isometry $\tilde{B} : \mathcal{Y}_1 \to \mathcal{W}_1$. In this case the effect of Bob's purified strategy $\tilde{B}$ is cancelled in the computation of $\mathrm{F}_{\mathrm{r}}(S, T)$ so that

$$\mathrm{F}_1(S, T) = \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) = \mathrm{F}(\tilde{B}\rho\tilde{B}^*, \tilde{B}\xi\tilde{B}^*) = \mathrm{F}(\rho, \xi)$$

as claimed.

1.2.1 Basic properties of the strategy fidelity

We now list several other properties of the strategy fidelity, all of which immediately hold using the corresponding properties of the fidelity of quantum states.

▶ **Proposition 3** (Basic properties).

- *(Fuchs-van de Graaf inequalities for strategies) For any r-round strategies S and T, it holds that*

$$1 - \frac{1}{2}\|S - T\|_{\diamond \mathrm{r}} \leq \mathrm{F_r}(S,T) \leq \sqrt{1 - \frac{1}{4}\|S - T\|_{\diamond \mathrm{r}}^2}. \tag{4}$$

- *(Symmetry) For any r-round strategies S and T, it holds that $\mathrm{F_r}(S,T) = \mathrm{F_r}(T,S)$.*
- *(Joint concavity) For any r-round strategies $S^1, \ldots, S^n$ and $T^1, \ldots, T^n$, and nonnegative scalars $\lambda_1, \ldots, \lambda_n$ satisfying $\sum_{i=1}^n \lambda_i = 1$, we have*

$$\mathrm{F_r}\left(\sum_{i=1}^n \lambda_i S^i, \sum_{i=1}^n \lambda_i T^i\right) \geq \sum_{i=1}^n \lambda_i \, \mathrm{F_r}\left(S^i, T^i\right).$$

- *(Bounds on the strategy fidelity) For any r-round strategies S and T, it holds that $0 \leq \mathrm{F_r}(S,T) \leq 1$. Moreover, $\mathrm{F_r}(S,T) = 1$ if and only if $S = T$ and $\mathrm{F_r}(S,T) = 0$ if and only if S and T are perfectly distinguishable.*

We later discuss that the strategy version of the Fuchs-van de Graaf inequalities is crucial to our cryptographic applications. This was also used implicitly in [10].

1.2.2 Operational interpretation (min-max properties)

Here we propose an operationally motivated generalization of Uhlmann's Theorem [24] to the strategy fidelity. In so doing we elucidate the need for a min-max theorem. Recall that Uhlmann's Theorem for quantum states asserts that the fidelity $\mathrm{F}(\rho, \xi)$ between any two quantum states ρ and ξ, acting on $\mathcal{X}$, is given by

$$\mathrm{F}(\rho, \xi) = \max_U |\langle \phi | (U \otimes I_{\mathcal{X}}) | \psi \rangle|$$

where $|\phi\rangle, |\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$ are any purifications of ρ, ξ and the maximization is over all unitaries U acting on $\mathcal{Y}$ alone.

Intuitively, $\mathrm{F_r}(S,T)$ should quantify the extent to which any purifications $\tilde{S}, \tilde{T}$ of two strategies S, T can be made to look the same by acting only on the final memory space $\mathcal{Z}_r$. It follows immediately from the definition of the strategy fidelity and Uhlmann's Theorem that

$$\mathrm{F_r}(S,T) = \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) = \min_B \max_U \left| \langle \psi(\tilde{S}, \tilde{B}) | \, (U \otimes I_{\mathcal{W}_r}) \, | \psi(\tilde{T}, \tilde{B}) \rangle \right| \tag{5}$$

where, again, the maximization is over all unitaries U acting on $\mathcal{Z}_r$ alone.

Notice the order of minimization and maximization in (5). This could be viewed as a competitive game between Alice (who plays according to S or T) and Bob (who plays according to any arbitrary co-strategy B) in which Bob is trying to distinguish S from T and Alice is trying to make S and T look the same. To these ends, Bob chooses his strategy B so as to minimize the overlap $|\langle \psi(\tilde{S}, \tilde{B}) | \psi(\tilde{T}, \tilde{B}) \rangle|$; given such a choice B for Bob, Alice's responds with a unitary U that maximizes this overlap.

The problem is that Alice's choice of U may depend upon Bob's co-strategy B. The task of distinguishing S from T should depend only upon S and T—Alice should not be granted the ability to tweak S or T after she has acquired knowledge of Bob's specific choice of distinguishing co-strategy B. From an operational perspective, it would be much more desirable if the order of minimization and maximization in (5) were reversed. Alice should

select her unitary U so as to make S look as much as possible like T *before* Bob selects his distinguishing co-strategy B. Thus, we require a type of *min-max theorem*.

The set of all co-strategies B for Bob is compact and convex [13], but it is not at all clear that the objective function in (5) is convex in B; we show later (Lemma 9) that this is indeed the case. However, the set of all unitaries U for Alice is not a convex set. One might think that we could extend the domain of maximization to the convex hull of the unitaries in the hopes that there is a saddle point (U, B) with U unitary. Unfortunately, saddle points do not in general occur at extreme points of the domain, so we are not guaranteed that such a unitary saddle point exists. Thus, a min-max theorem for the strategy fidelity involving unitaries is not so easily forthcoming.

However, if we allow Alice to apply a general *quantum channel*, we are able to obtain a min-max result, as stated below.

▶ **Theorem 4** (Strategy generalization of Uhlmann's Theorem). *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. Let $|\psi(\tilde{S}, \tilde{B})\rangle$, $|\psi(\tilde{T}, \tilde{B})\rangle$ be as defined in Definition 1. We have*

$$\mathrm{F_r}(S,T)^2 = \max_{\Xi} \min_{B} \langle\psi(\tilde{S},\tilde{B})| \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)}\right)\left(|\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})|\right)\right] |\psi(\tilde{S},\tilde{B})\rangle \tag{6}$$

where the minimum is over all r-round pure co-strategies $\tilde{B}$ and the maximum is over all quantum channels Ξ acting on $\mathcal{Z}_r$ alone.

Note that similar min-max results are derived in [2] and [10]. It will be convenient to define the following quantum channel.

▶ **Definition 5.** A *strategy fidelity-achieving* channel Ξ is a channel which attains the maximum in (6), above.

1.2.3 Semidefinite programming formulation of strategy fidelity

It was shown in [12] that the strategy norm has a semidefinite programming formulation. Also, the fidelity of quantum states has semidefinite programming formulations, see [26, 27] for examples. It is natural to ask whether the strategy fidelity has such a formulation. We answer this question in the affirmative, below.

▶ **Theorem 6** (Semidefinite programming formulation of strategy fidelity). *Fix any purifications $\tilde{S}$ and $\tilde{T}$ of r-round strategies S and T, respectively. Then $\mathrm{F_r}(S,T)^2$ is equal to the optimal objective function value of the following semidefinite program:*

$$\begin{array}{rrcl}
\mathrm{F_r}(S,T)^2 = & \max & t & \\
& \text{subject to} & tI_{\mathcal{X}_1} & \preceq \mathrm{Tr}_{\mathcal{Y}_1}(R_1) \\
& & R_j \otimes I_{\mathcal{X}_{j+1}} & \preceq \mathrm{Tr}_{\mathcal{Y}_{j+1}}(R_{j+1}), \text{ for } j \in \{1,\ldots,r-1\}, \\
& & R_r & \preceq \frac{1}{2}\mathrm{Tr}_{\mathcal{Z}_r}\left((K \otimes I_{\mathcal{Y}_{1\ldots r}\otimes\mathcal{X}_{1\ldots r}})\,|\tilde{T}\rangle\!\rangle\langle\!\langle\tilde{S}|\right) + h.c. \\
& & \begin{bmatrix} I_{\mathcal{Z}_r} & K \\ K^* & I_{\mathcal{Z}_r} \end{bmatrix} & \succeq 0
\end{array}$$

where the variables R_j are Hermitian acting on $\mathcal{Y}_{1\ldots j} \otimes \mathcal{X}_{1\ldots j}$ for each $j \in \{1,\ldots,r\}$, and h.c. denotes the Hermitian conjugate.

1.3 Applications to two-party quantum cryptography

Since the seminal work of Wiesner [28] and Bennett and Brassard [3], there has been much interest in knowing the advantages, and limitations, of quantum protocols for cryptographic

tasks. Due to the interactive setting of such protocols, the use of quantum strategy analysis has proven to be useful. In [13], it was shown how to rederive Kitaev's lower bound for coin-flipping [15]. In [10], it was shown how to find a simple proof of the impossibility of interactive bit-commitment. Here, we find a similar proof of this and extend the argument to oblivious string transfer.

In this paper, we present our ideas using the machinery we have developed for the strategy fidelity. In particular, we show that the strategy version of the Fuchs-van de Graaf inequalities (Eqn. (4)) are of central importance in providing security lower bounds. In fact, due to the nature of the strategy norm and strategy fidelity, we are able to bound the security without even specifying the entire protocol! This is in stark contrast to many other security proofs/models studied, for example in [15, 23, 25, 19, 1, 14, 13, 5, 6, 7, 8, 20, 21, 4, 22] where Alice and Bob's actions are assumed to be fully specified (and known to cheating parties). We note that our proposed security model is implicit in the bit-commitment security bounds in [10] and in the channel setting in [2].

In this paper, we show the impossibility of ideal quantum protocols for interactive *bit-commitment* and *oblivious string transfer*.

1.3.1 Interactive bit-commitment

In bit-commitment, we require Alice and Bob to interact over two communication stages:

- Commit Phase: Alice chooses a uniformly random bit a and interacts with Bob using an r-round pure strategy $\tilde{A}^a$.
- Reveal Phase: Alice sends a to Bob and continues her interaction with him (so that Bob can test if she has cheated).
- Cheat Detection: Bob, knowing which pure strategy $\tilde{B}$ he has used, measures to check if the final state is consistent with Alice's pure strategy $\tilde{A}^a$. He aborts the protocol if this measurement detects the final state is not consistent with Alice's pure strategy $\tilde{A}^a$. If Alice is honest, he never aborts.

Protocols are designed with the intention to achieve the following two important properties of interest:

- Binding: Alice cannot change her mind after the Commit Phase and reveal the other value of a (without being detected by Bob).
- Hiding: Bob cannot learn Alice's bit a before she reveals it during the Reveal Phase.

Finding a protocol with perfect binding and hiding properties is known to be impossible [18, 16, 17]. However, these security proofs rely on an assumption that we do not make, that honest Bob's actions are specified beforehand (and thus known to Alice).

We define the cheating probabilities of Alice and Bob as follows:

$\mathrm{B_{BC}}$: The maximum probability with which a dishonest Bob can *learn* an honest Alice's committed bit $a \in \{0, 1\}$ after the Commit Phase.

$\mathrm{A_{BC}}$: The maximum probability with which Alice can change her commitment from 0 to 1 (or from 1 to 0) before the Reveal Phase.

▶ Remark. Note that in the definition of cheating Alice above, we do not assume Alice knows Bob's actions. It could even be the case that Bob's sole purpose is to choose a co-strategy such as to minimize $\mathrm{A_{BC}}$.

Cheating Bob wishes to distinguish between one of two uniformly randomly chosen strategies. We know from [12] that

$$\mathrm{B_{BC}} = \frac{1}{2} + \frac{1}{4}\|A^0 - A^1\|_{\diamond\mathrm{r}}.$$

In Section 4, we show that

$$\mathrm{A_{BC}} \geq \mathrm{F}_r(A^0, A^1)^2.$$

An interesting observation is that this only depends on Alice's honest strategies, not Bob's.

Thus, by the Fuchs-van de Graaf inequalities for strategies (Proposition 3), we have the following trade-off lower bound.

▶ **Theorem 7.** *In any interactive quantum protocol for bit-commitment, we have that*

$$\sqrt{\mathrm{A_{BC}}} + 2\mathrm{B_{BC}} \geq 2.$$

Moreover, we have that Alice or Bob can cheat with probability at least $\frac{9-\sqrt{17}}{8} \approx 61\%$.

Note that this is a similar bound to the one obtained in [10] for the interactive setting and exactly the same as in [2] in the channel setting.

We remark that, when Alice and Bob's actions are completely specified, optimal protocols are known [6].

1.3.2 1-out-of-2 interactive oblivious string transfer

This is an interactive cryptographic task between Alice and Bob where Bob has two bit-strings[2] (x_0, x_1) and Alice wishes to learn one of the two in the following manner:

- Alice chooses a uniformly random bit a which corresponds to her choice of which string she wishes to learn, and interacts with Bob via the r-round pure strategy $\tilde{A}^a$.
- For every (x_0, x_1), Bob uses a pure co-strategy $\tilde{B}^{x_0,x_1}$, such that Alice learns the string x_a with certainty by measuring her private space $\mathcal{Z}_r$ at the end of the protocol.

Note that we do not assume any structure on how Bob behaves other than the consistency condition above. For example, x_0 and x_1 may be the result of another protocol of which Alice is not part, and thus she does not even know the distribution from which they are drawn. Again, Bob's strategy may be such that, conditioned on the above requirements, he just wants to foil Alice's cheating, as defined below.

We define the cheating probabilities of Alice and Bob as follows:

$\mathrm{B_{OT}}$: The maximum probability with which a dishonest Bob can *learn* an honest Alice's choice bit a.

$\mathrm{A_{OT}}$: The maximum probability with which a dishonest Alice can learn x_0 after learning x_1 with certainty, or vice versa.

Cheating Bob behaves the exact same as in a bit-commitment protocol. Thus his cheating probability is again

$$\mathrm{B_{OT}} = \frac{1}{2} + \frac{1}{4}\|A^0 - A^1\|_{\diamond\mathrm{r}}.$$

In Section 4, we show the following bound on cheating Alice:

$$\mathrm{A_{OT}} \geq \mathrm{F}_r(A^0, A^1)^2.$$

This yields the same bound as in bit-commitment, below.

[2] The bit-length of the strings are, surprisingly, not important for the purposes of this paper.

▶ **Theorem 8.** *In any interactive quantum protocol for 1-out-of-2 oblivious string transfer, we have that*

$$\sqrt{\mathrm{A_{OT}}} + 2\mathrm{B_{OT}} \geq 2.$$

Moreover, we have that Alice or Bob can cheat with probability at least $\frac{9-\sqrt{17}}{8} \approx 61\%$.

Note that in the case where Bob has two *bits* (i.e., the strings have bit-length 1), an optimal security trade-off between Alice and Bob is known [4]:

$$\mathrm{A_{OT}} + 2\mathrm{B_{OT}} \geq 2.$$

However, this assumes perfect knowledge of Alice and Bob's honest strategies. Thus, our bound for cheating Alice is a bit weaker, but has the added benefit of only depending on her honest strategies.

2 Technical lemmas and the strategy generalization of Uhlmann's Theorem

In this section we prove two lemmas that allow us to establish nontrivial properties of the strategy fidelity. These lemmas are used to prove the strategy generalization of Uhlmann's Theorem (Theorem 4) and to provide a semidefinite programming formulation of the strategy fidelity (Theorem 6).

Before we proceed, let us introduce some notation. Let $\mathcal{Y}_{i\ldots j}\mathcal{X}_{i'\ldots j'}$ be short for $\mathcal{Y}_{i\ldots j} \otimes \mathcal{X}_{i'\ldots j'}$. Let $\mathbf{L}(\mathcal{X})$, $\mathbf{U}(\mathcal{X})$, $\mathbf{Her}(\mathcal{X})$, $\mathbf{Pos}(\mathcal{X})$, and $\mathbf{Dens}(\mathcal{X})$ be, respectively, the set of all linear, unitary, Hermitian, positive semidefinite, and density operators acting on $\mathcal{X}$. Let $\mathbf{K}(\mathcal{X})$ be the convex hull of $\mathbf{U}(\mathcal{X})$, namely, the set of all operators $K \in \mathbf{L}(\mathcal{X})$ such that $\|K\| \leq 1$. Suppose $\mathcal{X}$ and $\mathcal{Y}$ are two complex Euclidean spaces with fixed standard basis. Given a linear operator $A : \mathcal{X} \to \mathcal{Y}$ written in the standard basis as

$$A = \sum_{i=1}^{\dim(\mathcal{X})} \sum_{j=1}^{\dim(\mathcal{Y})} a_{i,j} |j\rangle\langle i|,$$

the *vectorization* of A is

$$|A\rangle\!\rangle := \sum_{i=1}^{\dim(\mathcal{X})} \sum_{j=1}^{\dim(\mathcal{Y})} a_{i,j} |j\rangle \otimes |i\rangle \in \mathcal{Y} \otimes \mathcal{X}$$

and its adjoint is $\langle\!\langle A| := (|A\rangle\!\rangle)^*$.

▶ **Lemma 9** (Inner product is linear in B)**.** *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. Let B be a compatible r-round co-strategy and let $\tilde{B}$ be any purification of B. Let $|\psi(\tilde{S}, \tilde{B})\rangle, |\psi(\tilde{T}, \tilde{B})\rangle$ be as in Definition 1 and let $K \in \mathbf{L}(\mathcal{Z}_r)$. It holds that*

$$\langle\psi(\tilde{S}, \tilde{B})| \left(K \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{T}, \tilde{B})\rangle = \langle\!\langle \tilde{S}| \left(K \otimes B\right) |\tilde{T}\rangle\!\rangle.$$

Note that the inner product above depends on B but not on its purification $\tilde{B}$. This exemplifies what we stated earlier in the remark above Eqn. (2).

The proof is similar to a proof in Ref. [13, Theorem 5]. Lemma 9 is useful for proving the following lemma. Proofs of both these results will be included in the full version.

▶ **Lemma 10.** *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. It holds that*

$$\mathrm{F_r}(S,T) = \max_K \min_B \Re\left(\langle\!\langle \tilde{S}| \left(K \otimes B\right) |\tilde{T}\rangle\!\rangle\right)$$

where the minimum is over all compatible r-round co-strategies B for Bob and the maximum is over all $K \in \mathbf{K}(\mathcal{Z}_r)$ acting on the final memory space $\mathcal{Z}_r$ for Alice.

Now, with Lemmas 9 and 10 at our disposal, we proceed to prove the strategy generalization of Uhlmann's Theorem.

Proof of Theorem 4. From Lemma 10, it follows that

$$\mathrm{F_r}(S,T) \leq \max_K \min_B \left|\langle\!\langle \tilde{S}| \left(K \otimes B\right) |\tilde{T}\rangle\!\rangle\right|.$$

We square this inequality and apply Lemma 9 to obtain

$$\mathrm{F_r}(S,T)^2 \leq \max_K \min_B \langle\psi(\tilde{S},\tilde{B})| \left(K \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})| \left(K^* \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{S},\tilde{B})\rangle.$$

Let us define $\bar{K} = \sqrt{I_{\mathcal{Z}_r} - K^*K}$ (noting that $K^*K \preceq I_{\mathcal{Z}_r}$) and

$$\Xi_K : \mathbf{L}(\mathcal{Z}_r) \to \mathbf{L}(\mathcal{Z}_r) : X \mapsto KXK^* + \bar{K}X\bar{K}^*,$$

which is a quantum channel as its Kraus representation $\{K, \bar{K}\}$ satisfies $K^*K + \bar{K}^*\bar{K} = I_{\mathcal{Z}_r}$. Since

$$\langle\psi(\tilde{S},\tilde{B})| \left(\bar{K} \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})| \left(\bar{K}^* \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{S},\tilde{B})\rangle \geq 0$$

for all K and all $\tilde{B}$, we have

$$\begin{aligned}\mathrm{F_r}(S,T)^2 &\leq \max_K \min_B \langle\psi(\tilde{S},\tilde{B})| \left[\left(\Xi_K \otimes I_{\mathbf{L}(\mathcal{W}_r)}\right) \left(|\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})|\right)\right] |\psi(\tilde{S},\tilde{B})\rangle \\ &\leq \max_\Xi \min_B \langle\psi(\tilde{S},\tilde{B})| \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)}\right) \left(|\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})|\right)\right] |\psi(\tilde{S},\tilde{B})\rangle. \qquad (7)\end{aligned}$$

However, we clearly have

$$\mathrm{F_r}(S,T)^2 = \min_B \max_\Xi \langle\psi(\tilde{S},\tilde{B})| \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)}\right) \left(|\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})|\right)\right] |\psi(\tilde{S},\tilde{B})\rangle$$

due to Eqn. (5) and the fact that Uhlmann's Theorem also holds replacing unitaries with channels. Hence, the inequality (7) is in fact an equality due to the max–min inequality. ◀

3 Semidefinite programming formulation for strategy fidelity

In this section, we use Lemma 10 to prove Theorem 6. From Lemma 10, we have that

$$\mathrm{F_r}(S,T)^2 = \max\left\{\phi(K) : K \in \mathbf{K}(\mathcal{Z}_r)\right\}$$

where $\phi(K) := \min_B \Re\langle\!\langle \tilde{S}| \left(K \otimes B\right) |\tilde{T}\rangle\!\rangle$, and B is Bob's co-strategy. By defining

$$C := \frac{1}{2}\mathrm{Tr}_{\mathcal{Z}_r}\left(\left(K \otimes I_{\mathcal{Y}_{1\ldots r}\mathcal{X}_{1\ldots r}}\right) |\tilde{T}\rangle\!\rangle\langle\!\langle\tilde{S}|\right) + \frac{1}{2}\left[\mathrm{Tr}_{\mathcal{Z}_r}\left(\left(K \otimes I_{\mathcal{Y}_{1\ldots r}\mathcal{X}_{1\ldots r}}\right) |\tilde{T}\rangle\!\rangle\langle\!\langle\tilde{S}|\right)\right]^*$$

we can write

$$\phi(K) = \min_B \langle C, B\rangle.$$

From [13, Corollary 7], we know that B must satisfy $B = Q_r \otimes I_{\mathcal{Y}_r}$ for some $(Q_1, \ldots, Q_r)$ satisfying

$$\mathrm{Tr}(Q_1) = 1, \quad \mathrm{Tr}_{\mathcal{X}_i}(Q_i) = Q_{i-1} \otimes I_{\mathcal{Y}_{i-1}}, \text{ for } i \in \{2, \ldots, r\}$$

and $Q_1 \in \mathbf{Pos}(\mathcal{X}_1)$, $Q_i \in \mathbf{Pos}(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i})$, for $i \in \{2, \ldots, r\}$. Thus, $\phi(K)$ can be formulated as a semidefinite program. Its dual can be written as

$$\begin{aligned}\alpha(K) := \max \big\{\, t \ : & tI_{\mathcal{X}_1} \preceq \mathrm{Tr}_{\mathcal{Y}_1}(R_1),\ R_r \preceq C, \\ & R_j \otimes I_{\mathcal{X}_{j+1}} \preceq \mathrm{Tr}_{\mathcal{Y}_{j+1}}(R_{j+1}) \text{ for } j \in \{1, \ldots, r-1\} \,\big\},\end{aligned}$$

where $R_j \in \mathbf{Her}(\mathcal{Y}_{1\ldots j} \otimes \mathcal{X}_{1\ldots j})$. Since this has a strictly feasible solution, as does the primal, we know $\alpha(K) = \phi(K)$ by strong duality and $\alpha(K)$ attains an optimal solution. We now let $M = \begin{bmatrix} I_{\mathcal{Z}_r} & K \\ K^* & I_{\mathcal{Z}_r} \end{bmatrix}$ and set $M \succeq 0$ to get $\|K\| \leq 1$. We can check that C is a linear function in M (since M is Hermitian). Thus, we have that the strategy fidelity can be written as in Theorem 6.

4 Alice's cheating in interactive bit-commitment and oblivious string transfer

In this section we show that Alice can cheat with probability $\mathrm{F}_r(A^0, A^1)^2$ in either bit-commitment or oblivious string transfer. The cheating has the same flavour in both cases: Alice will follow the protocol honestly, then try to change her state as to make it look like she chose the other strategy from the beginning. Suppose Alice uses pure strategy $\tilde{A}^a$ and Bob uses pure co-strategy $\tilde{B}$. For brevity, define for each $a \in \{0, 1\}$ the following states

$$|\psi_a\rangle := |\psi(\tilde{A}^a, \tilde{B})\rangle \quad \text{and} \quad \sigma_a := (\Xi^a \otimes I_{\mathcal{W}_r})(|\psi_a\rangle\langle\psi_a|) \tag{8}$$

where Ξ_a is the strategy fidelity-achieving channel (from Definition 5) such that

$$\langle\psi_{\bar{a}}|\sigma_a|\psi_{\bar{a}}\rangle \geq \mathrm{F_r}(A^0, A^1)^2. \tag{9}$$

Note that the aim of Ξ^a is to get σ_a as close as possible to $|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|$.

4.1 Bit-commitment

When we study interactive bit-commitment, we are applying the strategy/co-strategy formalism to *only* the commit phase. From the above discussion, Alice can create the state $\sigma_a \in \mathbf{Dens}(\mathcal{Z}_r \otimes \mathcal{W}_r)$ to try to change her commitment from a to $\bar{a}$. Then Alice continues her actions to "reveal" $\bar{a}$ in the Reveal Phase, as does Bob (even though Bob's actions are not specified to Alice). We just assume that this entire process is done by a unitary $U_{\bar{a}}$ acting on $\mathcal{Z}_r \otimes \mathcal{W}_r$. Then, Bob has a projective measurement $\{\Pi_{accept}, \Pi_{reject}\}$ which accepts $U_{\bar{a}}|\psi_{\bar{a}}\rangle$ with certainty, thus leading to a *non-destructive measurement*. Thus, we have

$$(I_{\mathcal{Z}_r} \otimes \Pi_{accept})U_{\bar{a}}|\psi_{\bar{a}}\rangle = U_{\bar{a}}|\psi_{\bar{a}}\rangle.$$

This implies that

$$(I_{\mathcal{Z}_r} \otimes \Pi_{accept}) \succeq U_{\bar{a}}|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|U_{\bar{a}}^*.$$

However, Alice's actions have led to them sharing $U_{\bar{a}}\sigma_a U_{\bar{a}}^*$ at the end of the protocol. So, we have that Alice successfully reveals $\bar{a}$ with probability

$$\mathrm{A_{BC}} \geq \langle I_{\mathcal{Z}_r} \otimes \Pi_{accept}, U_{\bar{a}}\sigma_a U_{\bar{a}}^*\rangle \geq \langle U_{\bar{a}}|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|U_{\bar{a}}^*, U_{\bar{a}}\sigma_a U_{\bar{a}}^*\rangle = \langle|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|, \sigma_a\rangle \geq \mathrm{F}_r(A^0, A^1)^2$$

using Eqn. (9), as desired.

4.2 Oblivious string transfer

We can assume Alice uses a projective measurement $\{\Pi_z^a\}$ to learn her desired string. Note that since x_a is learned with certainty, this is a *non-destructive measurement*, as in the bit-commitment analysis above. That is, we have

$$\left(\Pi_{x_a}^a \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle = |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle$$

for all a and (x_0, x_1). Again, this implies

$$\Pi_{x_a}^a \otimes I_{\mathcal{W}_r} \succeq |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle\langle\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})|. \tag{10}$$

Thus, after learning x_a, she can create the state σ_a (defined above) to try to learn $x_{\bar{a}}$. (Here, the $\tilde{B}$ in the definition of σ_a is $\tilde{B}^{x_0,x_1}$.) Then she measures as if she had used pure strategy $\tilde{A}^{\bar{a}}$ (that is, using $\{\Pi_z^{\bar{a}}\}$) to try to learn $x_{\bar{a}}$. Then, using (10) and the definitions in (8), we have

$$\mathrm{A_{OT}} \geq \langle \Pi_{x_{\bar{a}}}^{\bar{a}} \otimes I_{\mathcal{W}_r}, \sigma_a\rangle \geq \langle \psi_{\bar{a}}|\sigma_a|\psi_{\bar{a}}\rangle \geq \mathrm{F_r}(A^0, A^1)^2,$$

as desired.

References

1. Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Röhrig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. doi:10.1109/CCC.2004.19.
2. Viacheslav P. Belavkin, Giacomo Mauro D'Ariano, and Maxim Raginsky. Operational distance and fidelity for quantum channels. *Journal of Mathematical Physics*, 46(6):062106, 2005. arXiv:quant-ph/0408159.
3. Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE Computer Society, 1984.
4. André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science*, 2016.
5. André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science*, FOCS 2009, pages 527–533, 2009. arXiv:0904.1511 [quant-ph].
6. André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 354–362. IEEE Computer Society, 2011. doi:10.1109/FOCS.2011.42.
7. André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information and Computation*, 13(1&2):158–177, 2013. arXiv:1007.1875 [quant-ph].
8. André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Strong connections between quantum encodings, nonlocality, and quantum cryptography. *Phys. Rev. A*, 89:022334, 2014. arXiv:1304.0983 [quant-ph].
9. Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009. arXiv:0904.4483 [quant-ph].
10. Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, Dirk Schlingemann, and Reinhard F. Werner. A short impossibility proof of quantum bit commitment. *Physics Letters A*, 377(15):1076–1087, 2013. arXiv:0905.3801v1 [quant-ph].

11 Gus Gutoski. *Quantum strategies and local operations*. PhD thesis, University of Waterloo, 2009. arXiv:1003.0038 [quant-ph].

12 Gus Gutoski. On a measure of distance for quantum strategies. *Journal of Mathematical Physics*, 53(3):032202, 2012. arXiv:1008.4636 [quant-ph].

13 Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC 2007)*, pages 565–574, 2007. arXiv:quant-ph/0611234.

14 Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131–135, 2004. arXiv:quant-ph/0206121. doi:10.1016/j.ipl.2003.07.007.

15 Alexei Kitaev. Quantum coin-flipping. Presentation at the 6th Workshop on *Quantum Information Processing* (QIP 2003), 2002.

16 Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. doi:10.1103/PhysRevLett.78.3410.

17 Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1–2):177–187, 1998. Proceedings of the Fourth Workshop on Physics and Consumption. doi:10.1016/S0167-2789(98)00053-0.

18 Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. doi:10.1103/PhysRevLett.78.3414.

19 Ashwin Nayak and Peter Shor. Bit-commitment based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003. arXiv:quant-ph/0206123. doi:10.1103/PhysRevA.67.012304.

20 Ashwin Nayak, Jamie Sikora, and Levent Tunçel. Quantum and classical coin-flipping protocols based on bit-commitment and their point games. Available as arXiv.org e-Print quant-ph/1504.04217, 2015.

21 Ashwin Nayak, Jamie Sikora, and Levent Tunçel. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming*, 156(1):581–613, 2016.

22 Jamie Sikora. Simple, near-optimal quantum protocols for die-rolling. In *Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, pages 1–14, 2016.

23 Robert W. Spekkens and Terence Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001. doi:10.1103/PhysRevA.65.012310.

24 A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

25 Salil P. Vadhan. An unconditional study of computational zero knowledge. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 176–185. IEEE Computer Society, 2004. doi:10.1109/FOCS.2004.13.

26 John Watrous. Semidefinite programs for completely bounded norms. *Theory of Computing*, 5:217–238, 2009. arXiv:0901.4709v2 [quant-ph].

27 John Watrous. Simpler semidefinite programs for completely bounded norms. *Chicago Journal of Theoretical Computer Science*, 2013.

28 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. doi:10.1145/1008908.1008920.

Minimum Quantum Resources for Strong Non-Locality*

Samson Abramsky[1], Rui Soares Barbosa[2], Giovanni Carù[3], Nadish de Silva[4], Kohei Kishida[5], and Shane Mansfield[6]

1 **Department of Computer Science, University of Oxford, Oxford, UK**
samson.abramsky@cs.ox.ac.uk
2 **Department of Computer Science, University of Oxford, Oxford, UK**
rui.soares.barbosa@cs.ox.ac.uk
3 **Department of Computer Science, University of Oxford, Oxford, UK**
giovanni.caru@cs.ox.ac.uk
4 **Department of Computer Science, University College London, London, UK**
nadish.desilva@utoronto.ca
5 **Department of Computer Science, University of Oxford, Oxford, UK**
kohei.kishida@cs.ox.ac.uk
6 **School of Informatics, University of Edinburgh, Edinburgh, UK**
smansfie@staffmail.ed.ac.uk

Abstract

We analyse the minimum quantum resources needed to realise strong non-locality, as exemplified e.g. by the classical GHZ construction. It was already known that no two-qubit system, with any finite number of local measurements, can realise strong non-locality. For three-qubit systems, we show that strong non-locality can only be realised in the GHZ SLOCC class, and with equatorial measurements. However, we show that in this class there is an infinite family of states which are pairwise non LU-equivalent that realise strong non-locality with finitely many measurements. These states have decreasing entanglement between one qubit and the other two, necessitating an increasing number of local measurements on the latter.

1998 ACM Subject Classification F.0 Theory of Computation – General

Keywords and phrases strong non-locality, maximal non-locality, quantum resources, three-qubit states

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.9

1 Introduction

In this paper, we aim at identifying the minimum quantum resources needed to witness strong contextuality [3], and more specifically, strong (or maximal) non-locality. Non-locality

* This work was carried out in part while some of the authors visited the Simons Institute for the Theory of Computing (supported by the Simons Foundation) at the University of California, Berkeley, as participants of the Logical Structures in Computation programme (AB, RSB, GC, NdS, SM), and while SM was based at the Institut de Recherche en Informatique Fondamentale, Université Paris Diderot – Paris 7. Support from the following is also gratefully acknowledged: EPSRC EP/N018745/1 and EP/N017935/1, Contextuality as a Resource in Quantum Computation (SA, RSB, NdS); EPSRC Doctoral Training Partnership and Oxford–Google Deepmind Graduate Scholarship (GC); U.S. AFOSR FA9550-12-1-0136, Topological & Game-Semantic Methods for Understanding Cyber Security (KK); Fondation Sciences Mathématiques de Paris, post-doctoral research grant otpFIELD15RPOMT-FSMP1, Contextual Semantics for Quantum Theory (SM).

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 9; pp. 9:1–9:20
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

is, of course, a fundamental phenomenon in quantum mechanics – both from a foundational point of view, and with respect to quantum information and computation, in which it plays a central rôle.

The original form of Bell's argument [9], as well as its now more standard formulation due to Clauser, Horne, Shimony, and Holt (CHSH) [13], rests on deriving an inequality that must be satisfied by probabilities arising from any local realistic theory, but which is violated by those predicted by quantum mechanics for a particular choice of a state and a finite set of measurements. Greenberger, Horne, Shimony, and Zeilinger (GHSZ) [19, 18] gave a stronger, inequality-free argument for quantum non-locality. This depended only on the *possibilistic* aspects of quantum predictions, i.e. on which joint outcomes given a choice of measurements have non-zero probability, regardless of the actual value of the probabilities. Their argument was later simplified by Mermin [27, 28]. Whereas the Bell–CHSH argument used local measurements on a two-qubit system prepared in a maximally entangled state, the GHZ–Mermin argument required a three-qubit system in the GHZ state. Subsequently, Hardy showed that one can indeed find a proof of non-locality "without inequalities", i.e. based on possibilistic information alone, using a bipartite, two-qubit system [21]. Hardy's argument works on any two-qubit entangled state bar the maximally entangled ones [22]. In fact, a similar argument works on almost all n-qubit states [4], the exceptions being those states which are products of one-qubit states and two-qubit maximally entangled states, which provably do *not* admit any non-locality argument "without inequalities" [26]. However, there is an important logical distinction between the GHSZ and Hardy possibilistic arguments.

Abramsky and Brandenburger [3] introduced a general mathematical framework for contextuality, in which non-locality arises as a particular case. This approach studies these phenomena at a level of generality that abstracts away from the particularities of quantum theory. The point is that contextuality and non-locality are witnessed by the empirical data itself, without presupposing any physical theory. For this reason, one deals with "empirical models" – tables of data for a given experimental scenario, obtained from empirical observations or predicted by some physical theory, specifying probabilities of joint outcomes for the allowed sets of compatible measurements.

Various kinds of contextuality (or, in particular, non-locality) arguments were studied and classified at this abstract level, leading to the introduction of a qualitative hierarchy of strengths of contextuality in [3], with further refinements in [5, 1]. The classic arguments for quantum non-locality, familiar from the literature, sit at different levels in this hierarchy. There is a strict relationship of strengths of non-locality, rendered as

$$\text{Bell} < \text{Hardy} < \text{GHZ},$$

where these representative examples correspond, respectively, to probabilistic non-locality, possibilistic non-locality, and strong non-locality.

Strong contextuality (or, in particular, non-locality) arises when there is *no assignment of outcomes to all the measurements* consistent with the events that the empirical model deems possible, i.e. to which it attributes non-zero probability. It is exactly this impossibility which is shown by Mermin's classic argument in [27]. Strong contextuality is also the highest level of contextuality in a different, quantitative sense. It turns out to coincide with the notion of maximal contextuality, the property that an empirical model admits no proper decomposition into a convex combination of a non-contextual model and another model. This corresponds to attaining the maximum value of 1 for the *contextual faction*, a natural measure of contextuality introduced in [3] as a generalisation of the notion of non-local

fraction [16, 8, 7]. The contextual fraction is shown in [2] to be equal to the *maximal normalised violation* of a contextuality-witnessing inequality. Hence, a model is strongly contextual if and only if it violates a generalised Bell inequality up to its algebraic bound.

Strong non-locality is particularly relevant to quantum computing. It is exhibited, for example, by all graph states under stabiliser measurements [20], which provide resource states and measurements for universal quantum computing via the one-way or measurement-based model [31]. It is also known to be necessary for increasing computational power in certain models of measurement-based quantum computing with restricted classical co-processing [30]. For instance, in [6] it was shown that GHZ strong non-locality enables a linear classical co-processor to implement the non-linear AND function, and subsequently in [14] that it enables the function to be implemented in a secure delegated way. Moreover, strong non-locality has important consequences for certain information processing tasks: in particular, it is known to be required for perfect strategies [25] in certain cooperative games [2].

Summary of results

In this paper, our aim is to analyse the minimum quantum resources needed to realise strong non-locality. More precisely, we consider n-qubit systems viewed as n-partite systems,[1] where each party can perform one-qubit local projective measurements.[2] We shall consider the case where each party has a finite set of measurements available – this is what corresponds to the standard experimental scenarios for non-locality.

- The first result we present is limitative in character. It shows that strong non-locality *cannot* be realised by a two-qubit system with any finite number of local measurements. This result was already proven, using different terminology, in [12]. However, we include it for completeness and because its proof is useful as a warm-up for proving the other results in this paper.[3]

  There is a subtle counterpoint to this in a result from [8], which shows that using a maximally entangled bipartite state, and an infinite family of local measurements, strong non-locality is achieved "in the limit" in a suitable sense. More precisely, as more and more measurements from the family are used, the local fraction – the part of the behaviour which can be accounted for by a local model – tends to 0, or equivalently the non-local fraction tends to 1. There is an interesting connection to this in our results for the tripartite case.

  However, there is a practical advantage in being able to witness strong non-locality with a fixed finite number of measurements. If one wishes to design an experimental test for maximal non-locality, it is desirable that one can increase precision, i.e. increase the lower bound on the non-local fraction, without needing to expand the experimental setup – in particular, the number of measurement settings required to be performed – but rather by simply performing more runs of the same experiment.

[1] We know by a result of Heywood and Redhead [23] that strong contextuality can be realised using a bipartite system, but with a qutrit at each site. Hence our focus on qubits.

[2] Throughout this paper, we focus on projective measurements. The more general POVMs are justified as physical processes by Naĭmark's dilation, since they are described as projective measurements in a larger physical system. Given that we are interested in characterising the minimum resources needed in order to witness strong non-locality, it seems reasonable to focus on PVMs, which do not need to be seen as measurements on a part of a larger system.

[3] Note that, in the same paper, it is also shown that the result applies to any bipartite state where one of the systems is a qubit, by an application of Schmidt decomposition of any bipartite state. This means that the optimal dimention in which strong non-locality can be realised is $2 \times 2 \times 2 = 8$, i.e. a three-qubit system, since a two-qutrit system has dimension 9.

- Having shown that strong non-locality cannot be realised in the two-qubit case, we turn to the analysis of three-qubit systems. Of course, we know by the classical GHSZ–Mermin construction that strong non-locality *can* be achieved in this case, using the GHZ state and Pauli X and Y measurements on each of the qubits. Our aim is to analyse for which states, and with respect to which measurements, can strong non-locality be achieved. We use the classification into SLOCC classes for tripartite qubit systems from [15]. According to this analysis, there are two maximal SLOCC classes, the GHZ and W classes. Below these, there are the degenerate cases of products of an entangled bipartite state with a one-qubit state, e.g. $AB{-}C$. By the previous result, these degenerate cases cannot realise strong non-locality. We furthermore show that no state in the W class can realise strong non-locality, for any choice of finitely-many local measurements.
- This leaves us with the GHZ SLOCC class. We use the detailed description of this class as a parameterised family of states from [15]. We first show that any state in this class witnessing strong non-locality with finitely many local measurements must satisfy a number of constraints on the parameters. In particular, the state must be balanced in the sense that the coefficients in its unique linear decomposition into a pair of product states have the same complex modulus. We furthermore show that *only equatorial measurements need be considered* (the equators being uniquely determined by the state) – no other measurements can contribute to a strong non-locality argument.
- Having thus narrowed the possibilities for realising strong non-locality considerably, we find a new infinite family of models displaying strong non-locality using states within the GHZ SLOCC class that are not LU-equivalent to the GHZ state. The states in this family start from GHZ and tend in the limit to the state $|\Phi^+\rangle \otimes |+\rangle$ in the AB–C class with maximal entanglement on the first two qubits, and in product with the third. This family is actually closely related to the construction from [8] in which an increasing number of measurements on a bipartite maximally entangled state eventually squeezes the local fraction to zero in the limit. Our family is obtained by adding a third qubit to this setup, with two available local measurements, and some entanglement between the first two qubits and the third one, thus allowing strong non-locality to be witnessed with a finite number of measurements. There is a trade-off between the number of measurement settings available on the first two qubits – and, consequently, the lower bound for the non-local fraction these measurements can witness – and the amount of entanglement necessary between the third qubit and the original two.

Outline. The remainder of this article is organised as follows: Section 2 summarises some background material on non-locality and entanglement classification of three-qubit states, Section 3 shows that strong non-locality cannot be witnessed by two-qubit states and a finite number of local measurements; Section 4 does the same for three-qubit states in the SLOCC class of W; Section 5 deals with states in the SLOCC class of GHZ, deriving conditions on these necessary for strong non-locality; Section 6 presents the family of strong non-locality arguments using states in the GHZ-SLOCC class; and Section 7 concludes with some discussion of open problems and further directions.

2 Background

2.1 Measurement scenarios and empirical models

We summarise some of the main ideas of [3], with particular emphasis on non-locality. This is merely an instance of contextuality in a particular kind of measurement scenarios known

as multipartite Bell-type scenarios. For each notion, we introduce the general definition followed by its specialisation to multipartite Bell-type scenarios.

Measurement scenarios are abstract descriptions of experimental setups. In general, a *measurement scenario* is described by a set of measurement labels X, a set of outcomes O, and a cover $\mathcal{M}$ of X consisting of measurement contexts, i.e. maximal sets of measurements that can be jointly performed. We are typically interested in measurement scenarios with finite X, but for technical reasons it will be useful to consider scenarios with infinitely many measurements in order to prove results about all their finite 'subscenarios' at once. Throughout this paper, we shall also restrict our attention to dichotomic measurements, with outcome set $O = \{-1, +1\}$. This is a reasonable restriction, especially since our main focus shall be projective measurements on single qubits. Multipartite Bell-type scenarios are a particular kind of measurement scenario which can be thought to describe multiple parties at different sites, each independently choosing to perform one of a number of measurements available to them. More formally, an n-partite Bell-type scenario is described by sets $X_1, \ldots, X_n$ labelling the measurements available at each site (so that $X := X_1 \sqcup \cdots \sqcup X_n$), with maximal contexts corresponding to a single choice of measurement for each party, or in other words a tuple $\mathbf{m} = \langle m_1, \ldots, m_n \rangle \in X_1 \times \cdots \times X_n$ (so $\mathcal{M} \cong \prod_{i=1}^n X_i$).

An empirical model is a collection of probabilistic data representing possible results of running the experiment represented by a measurement scenario. Given a measurement scenario $\langle X, \mathcal{M}, O \rangle$, an *empirical model* on that scenario is a family $\{e_C\}_{C \in \mathcal{M}}$ where each $e_C \in \mathcal{D}(O^C)$ is a distribution over the set of joint outcomes to the measurements of C. Given an assignment $s \colon C \longrightarrow O$ of outcomes to each measurement in C, the value $e_C(s)$ is the probability of obtaining the outcomes determined by s when jointly performing the measurements in the context C.

In the particular case of a Bell-type scenario, we have a family $\{e_{\mathbf{m}} \in \mathcal{D}(O^n)\}_{\mathbf{m} \in \prod_i X_i}$ of probability distributions. Given a vector of outcomes $\mathbf{o} = \langle o_1, \ldots, o_n \rangle \in O^n$, the probability $e_{\mathbf{m}}(\mathbf{o})$ of obtaining the joint outcomes $\mathbf{o}$ upon performing the measurements $\mathbf{m}$ at each site is often denoted in the literature on non-locality as follows:

$$e_{\mathbf{m}}(\mathbf{o}) = \mathsf{Prob}(\mathbf{o}|\mathbf{m}) = \mathsf{Prob}(o_1, \ldots, o_n | m_1, \ldots, m_n).$$

Empirical models are usually assumed to satisfy a *compatibility* condition: that marginal distributions agree on overlapping contexts, i.e. for all C and C' in $\mathcal{M}$, $e_C|_{C \cap C'} = e_{C'}|_{C \cap C'}$. In the case of multipartite scenarios, this corresponds to the familiar *no-signalling* condition.

2.2 Contextuality and non-locality

An empirical model is said to be *non-contextual* if there is a distribution on assignments of outcomes to all the measurements, $d \in \mathcal{D}(O^X)$, that marginalises to the empirical probabilities for each context, i.e. $\forall C \in \mathcal{M}.\ d|_C = e_C$. Note that this means there is a deterministic, non-contextual hidden-variable theory with the set of global assignments O^X serving as a canonical hidden variable space. Indeed, the existence of such a global distribution is in fact equivalent to the existence of a probabilistic hidden variable theory that is factorisable, a notion that in multipartite scenarios specialises to the standard formulation of Bell locality: there is a set of hidden variables Λ, a distribution in $h \in \mathcal{D}(\Lambda)$, and ontic probabilities $\mathsf{Prob}(\mathbf{o}|\mathbf{m}, \lambda)$ that are consistent with the empirical ones, i.e. for all $\mathbf{m} \in \mathcal{M}$ and $\mathbf{o} \in O_n$

$$\sum_{\lambda \in \Lambda} \mathsf{Prob}(\mathbf{o}|\mathbf{m}, \lambda) h(\lambda) = \mathsf{Prob}(\mathbf{o}|\mathbf{m}) = e_{\mathbf{m}}(\mathbf{o}),$$

and that factorise when conditioned on each $\lambda \in \Lambda$, i.e.

$$\mathsf{Prob}(\mathbf{o}|\mathbf{m}, \lambda) = \prod_{i=1}^{n} \mathsf{Prob}(o_i|m_i, \lambda).$$

where the probabilities on the right-hand side are obtained as the obvious marginals. The equivalence between the two formulations of non-contextuality or locality – in terms of a probability distribution on global assignments (canonical deterministic hidden variable theory) and in terms of factorisable hidden variable theory – was proven in [3] for general measurement scenarios, vastly extending a result by Fine [17]. This justifies viewing non-locality as the special case of contextuality in multipartite systems.

For some empirical models, it suffices to consider their possibilistic content, i.e. whether events are possible (non-zero probability) or impossible (zero probability), to detect the presence of contextuality. In this case, we say that the model is *logically contextual*. An even stronger form of contextuality, which will be our main concern in this article, arises when no global assignment of outcomes to all measurements is consistent with the events deemed possible by the model: the empirical model e is said to be *strongly contextual* if there is no assignment $g\colon X \longrightarrow O$ such that $\forall C \in \mathcal{M}.\ e_C(g|_C) > 0$. In the particular case of multipartite scenarios, such a global assignment is determined by a family of maps $g_i\colon X_i \longrightarrow O$ for each site i so that $g = \bigsqcup_{i=1}^{n} g_i\colon \bigsqcup_{i=1}^{n} X_i \longrightarrow O$. The consistency condition then reads: for any choice of measurements $\mathbf{m} = \langle m_1, \ldots, m_n\rangle \in \prod X_i$, writing $g(\mathbf{m}) = \langle g_1(m_1), \ldots, g_n(m_n)\rangle$, we have

$$e_{\mathbf{m}}(g(\mathbf{m})) = \mathsf{Prob}(g(\mathbf{m})|\mathbf{m}) = \mathsf{Prob}(g_1(m_1), \ldots, g_n(m_n)|m_1, \ldots, m_n) > 0.$$

As mentioned in Section 1, strong contextuality was shown in [3] to exactly capture the notion of maximal contextuality. The proof of this equivalence depends crucially on the finiteness of the number of measurements. If one would consider an infinite number of measurements, a situation could occur in which there is a global assignment g consistent with the model, in the sense that $\forall C \in \mathcal{M}.\ e_C(g|_C) > 0$, but where $\inf_{C\in\mathcal{M}} e_C(g|_C) = 0$, in which case g does not correspond to any positive fraction of the model. This will indeed be the case for all the consistent global assignments described in this paper. Note, however, that proving the failure of strong contextuality in a scenario with an infinite number of measurements, even if the witnessing global assignment has $\inf_{C\in\mathcal{M}} e_C(g|C) = 0$, is nonetheless sufficient to show that maximal contextuality cannot be realised using only a finite subset of the measurements.

2.3 Quantum realisable models

We are mainly concerned with empirical models that are realisable by quantum systems. This means that one can find a quantum state and associate to each measurement label a quantum measurement in the same Hilbert space such that measurements in the same context commute and the probabilities of the various outcomes are given by the Born rule.

More specifically, we are concerned with models arising from n-qubit systems with local, i.e. single-qubit, measurements. The Bloch sphere representation of one-qubit pure states will be useful: assuming a preferred orthonormal basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$, we shall use the notation

$$|\theta, \varphi\rangle := \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

for any $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi)$.

Any single-qubit projective measurement is fully determined by specifying such a normalised vector in $\mathbb{C}^2$, namely the pure state corresponding to the $+1$ eigenvalue or outcome. Hence, the set of local measurements for a single qubit is labelled by

$$\mathsf{LM} = [0, \pi] \times [0, 2\pi)$$

The quantum measurement determined by $(\theta, \varphi) \in \mathsf{LM}$ has eigenvalues $O = \{+1, -1\}$ with the eigenvector corresponding to outcome $o \in O$ given by:

$$|\theta, \varphi \mapsto o\rangle := \begin{cases} |\theta, \varphi\rangle & \text{if } o = +1 \\ |\pi - \theta, \varphi + \pi\rangle & \text{if } o = -1 \end{cases}$$

Throughout this paper, we shall be considering the n-partite measurement scenario with $X_i = \mathsf{LM}$ for every site. Measurement contexts correspond to a choice of single qubit measurements for each of the n sites, represented by a tuple $(\boldsymbol{\theta}, \boldsymbol{\varphi}) = \langle(\theta_1, \varphi_1), \ldots, (\theta_n, \varphi_n)\rangle$. Performing all the measurements of a context in parallel yields an outcome $\mathbf{o} = \langle o_1, \ldots, o_n\rangle \in O^n$. The vector corresponding to this outcome is denoted

$$|\boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto \mathbf{o}\rangle := |\theta_1, \varphi_1 \mapsto o_1\rangle \otimes \cdots \otimes |\theta_n, \varphi_n \mapsto o_n\rangle.$$

We shall also find it useful to write

$$|\boldsymbol{\theta}, \boldsymbol{\varphi}\rangle := |\theta_1, \varphi_1\rangle \otimes \cdots \otimes |\theta_n, \varphi_n\rangle = |\boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto \langle +1, \ldots, +1\rangle\rangle$$

for the vector corresponding to the joint outcome assigning $+1$ at every site.

An n-qubit state $|\psi\rangle$ determines an empirical model $e^{|\psi\rangle}$ for this measurement scenario:

$$e^{|\psi\rangle}_{(\boldsymbol{\theta}, \boldsymbol{\varphi})}(\mathbf{o}) = \mathsf{Prob}^{|\psi\rangle}(o_1, \ldots, o_n | (\theta_1, \varphi_1), \ldots, (\theta_n, \varphi_n)) := |\langle \boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto \mathbf{o} | \psi\rangle|^2.$$

We are concerned with checking for strongly non-local behaviour on such a model. As explained in the previous section, this amounts to checking for the existence of maps $g_i \colon \mathsf{LM} \longrightarrow O$ for each site such that for any choice of measurements $(\boldsymbol{\theta}, \boldsymbol{\varphi})$, the corresponding outcome has positive probability:

$$\begin{aligned} e_{(\boldsymbol{\theta}, \boldsymbol{\varphi})}(g(\boldsymbol{\theta}, \boldsymbol{\varphi})) &= \mathsf{Prob}^{|\psi\rangle}(g_1(\theta_1, \varphi_1), \ldots, g_n(\theta_n, \varphi_n) | (\theta_1, \varphi_1), \ldots, (\theta_n, \varphi_n)) \\ &= |\langle \boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto g(\boldsymbol{\theta}, \boldsymbol{\varphi}) | \psi\rangle|^2 > 0. \end{aligned}$$

Given that these are quantum probabilities, we can rephrase this condition in terms of non-vanishing amplitudes: $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto g(\boldsymbol{\theta}, \boldsymbol{\varphi}) | \psi\rangle \neq 0$.

The following fact will be used throughout. Suppose we want to check the consistency with the empirical model of a given global assignment $g = \bigsqcup_{i=1}^n g_i$. If this assignment satisfies

$$\forall i \in \{1, \ldots, n\}. \; g_i(\theta, \varphi) = -g_i(\pi - \theta, \varphi + \pi), \tag{1}$$

that is, measurements with $+1$ eigenstates diametrically opposed in the Bloch spehere (i.e. measurements that are the negation of each other) are assigned opposite outcomes, then

$$|\theta, \varphi \mapsto g_i(\theta, \varphi)\rangle = \begin{cases} |\theta, \varphi\rangle & \text{if } g_i(\theta, \varphi) = +1 \\ |\pi - \theta, \varphi + \pi\rangle & \text{if } g_i(\theta, \varphi) = -1 \quad (\Leftrightarrow g_i(\pi - \theta, \varphi + \theta) = +1) \end{cases}$$

meaning that $|\boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto g(\boldsymbol{\theta}, \boldsymbol{\varphi})\rangle = |\boldsymbol{\theta}', \boldsymbol{\varphi}'\rangle$ with $g_i(\theta'_i, \varphi'_i) = +1$ for all i. In other words, should we wish to calculate the amplitude for a joint outcome $\mathbf{o}$ on a given context $(\boldsymbol{\theta}, \boldsymbol{\varphi})$, we may

equivalently calculate the amplitude for the joint outcome $\langle +1, \ldots, +1\rangle$ on a new context $(\boldsymbol{\theta}', \boldsymbol{\varphi}')$ obtained by substituting $\theta_i \mapsto \pi - \theta_i$ and $\varphi_i \mapsto \pi + \varphi_i$ for all i such that $o_i = -1$. Therefore, it suffices to verify the equation $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto g(\boldsymbol{\theta}, \boldsymbol{\varphi})|\psi\rangle \neq 0$ for all contexts whose measurements are all assigned $+1$. Indeed, the same is true if (1) is relaxed to simply say that $g_i(\pi - \theta, \varphi + \pi) = -1 \Rightarrow g_i(\theta, \varphi) = +1$. Incidentally, even though we shall not need this fact, note that if there is any global assignment consistent with the model, there will be one that satisfies (1), for this would only require a subset of the conditions.

We conclude this subsection with two observations regarding these particular quantum empirical models. First, note that local unitaries (LU) on the state don't affect non-locality, or indeed strong non-locality, of the resulting empirical model. This follows from the fact that by moving from the Schrödinger to the Heisenberg picture, we may equivalently leave the state fixed and apply the corresponding unitaries to the sets of available local measurements. Since the available local measurements are all the projective one-qubit measurements, a local unitary, which can be seen as a rotation of the Bloch sphere, merely maps this set to itself. Secondly, if we are dealing with a product state of n-qubits, $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, then the resulting empirical model is necessarily local. This is because the probabilities factorise:

$$\mathsf{Prob}^{|\psi\rangle}(\mathbf{o}|(\boldsymbol{\theta}, \boldsymbol{\varphi})) = |\langle \boldsymbol{\theta}, \boldsymbol{\varphi} \mapsto \mathbf{o}|\psi\rangle|^2 = \left|\prod_{i=1}^{n} \langle \theta_i, \varphi_i \mapsto o_i|\psi_i\rangle\right|^2 = \prod_{i=1}^{n} |\langle \theta_i, \varphi_i \mapsto o_i|\psi_i\rangle|^2 .$$

2.4 SLOCC classes of three-qubit states

A classification of multipartite quantum states by their degree of entanglement is given by the notion of LOCC (local operations and classical communication) equivalence [10, 29, 24]. A protocol is said to be LOCC if it is of the following form: each party may perform local measurements and transformations on their system, and may communicate measurement outcomes to the other parties, so that local operations may be conditioned on measurement outcomes anywhere in the system. A state $|\psi_1\rangle$ is LOCC-convertible to a state $|\psi_2\rangle$ if there exists a LOCC protocol that *deterministically* produces $|\psi_2\rangle$ when starting with $|\psi_1\rangle$. Intuitively, such a protocol cannot increase the degree of entanglement and so we think of $|\psi_1\rangle$ as being at least as entangled as $|\psi_2\rangle$. The notion of LOCC-convertibility defines a preorder[4] on multipartite states that in turn yields a notion of LOCC-equivalence of states: the states $|\psi\rangle$ and $|\phi\rangle$ are LOCC-equivalent when $|\psi\rangle$ is LOCC-convertible to $|\phi\rangle$ and *vice versa*. The LOCC-convertibility preorder then naturally defines a partial order on the collection of LOCC equivalence classes of states.

A coarser classification of multipartite quantum states is given by relaxing the requirement that our conversion protocols succeed deterministically to the requirement that they succeed with non-zero probability [11]. The previous paragraph holds true for SLOCC (stochastic LOCC) *mutatis mutandis*. Note that equivalence of two states under LU transformations implies their SLOCC-equivalence. More generally, two states are SLOCC-equivalent if and only if they are related by an invertible local operator (ILO) [15].

Dür, Vidal, and Cirac [15] classified the SLOCC classes of three-qubit systems and found there to be exactly six classes (see Figure 1). The GHZ and W states are representatives of the two maximal, non-comparable classes. Three intermediate classes are characterised by bipartite entanglement between two of the qubits, which are in a product with the third. Finally, the minimal class is given by product states.

[4] A preorder is a reflexive and transitive relation; i.e. it is like a partial order except that it can deem two distinct elements equivalent.

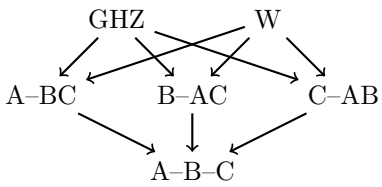

Figure 1 Hasse diagram of the partial order of three-qubit SLOCC classes.

By the last observation in the previous section, it is obvious that a state in the A–B–C class cannot realise non-locality, and that the case of a state in one of the intermediate classes can be reduced to that of the two qubits that are entangled. Hence, we shall first discuss strong non-locality for two-qubit states and then proceed in turn to each of the maximal SLOCC classes of three-qubit states, W and GHZ.

3 Two-qubit states are not strongly non-local

Every two-qubit state can be written, up to LU, uniquely as

$$|\psi\rangle = \cos\delta|00\rangle + \sin\delta|11\rangle, \tag{2}$$

where $\delta \in [0, \frac{\pi}{4}]$. The state (2) is either: the product state $|00\rangle$, which is obviously non-contextual since it is separable, when $\delta = 0$; or an entangled state in the SLOCC class of the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, when $\delta > 0$.

▶ **Theorem 1** (equivalent to [12, Theorem 1]). *Two-qubit states do not admit strongly non-local behaviour.*

Proof. This proof rests on defining an explicit global assignment $g : \mathsf{LM} \sqcup \mathsf{LM} \to O$ consistent with the possible events of the empirical model. More specifically, the map g is obtained by assigning outcome $+1$ to one hemisphere of the Bloch sphere, and -1 to the other, with special conditions on the poles and a slight asymmetry between the two parties.

We start by computing the amplitude $\langle \boldsymbol{\theta}, \boldsymbol{\varphi}|\psi\rangle$ of measuring $(\boldsymbol{\theta}, \boldsymbol{\varphi}) = \langle(\theta_1, \varphi_1), (\theta_2, \varphi_2)\rangle$ on the general state (2) and obtaining joint outcome $\langle +1, +1\rangle$:

$$\langle \boldsymbol{\theta}, \boldsymbol{\varphi}|\psi\rangle = \cos\delta\cos\frac{\theta_1}{2}\cos\frac{\theta_2}{2} + \sin\delta\sin\frac{\theta_1}{2}\sin\frac{\theta_2}{2}e^{-i(\varphi_1+\varphi_2)}$$

Since $\delta = 0$ gives rise to a product state, we will assume $\delta \neq 0$.

We define the following maps:

$$g_1 \colon \mathsf{LM} \longrightarrow O :: (\theta, \varphi) \longmapsto \begin{cases} +1 & \text{if } \theta = \pi \text{ or } \left(\theta \neq 0 \text{ and } \varphi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)\right) \\ -1 & \text{if } \theta = 0 \text{ or } \left(\theta \neq \pi \text{ and } \varphi \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right)\right) \end{cases}$$

$$g_2 \colon \mathsf{LM} \longrightarrow O :: (\theta, \varphi) \longmapsto \begin{cases} +1 & \text{if } \theta = \pi \text{ or } \left(\theta \neq 0 \text{ and } \varphi \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right]\right) \\ -1 & \text{if } \theta = 0 \text{ or } \left(\theta \neq \pi \text{ and } \varphi \in \left(\frac{\pi}{2}, \frac{3\pi}{2}\right]\right) \end{cases}$$

and let $g := g_1 \sqcup g_2 \colon \mathsf{LM} \sqcup \mathsf{LM} \longrightarrow O$ be a global assignment. A graphical representation of the map g can be found in Figure 2.

Let $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ be a context whose individual measurements are mapped to $+1$ by g (see Section 2.3 for why this is sufficient). In particular, it holds that $\theta_1, \theta_2 \neq 0$. Since $\delta \neq 0$, we

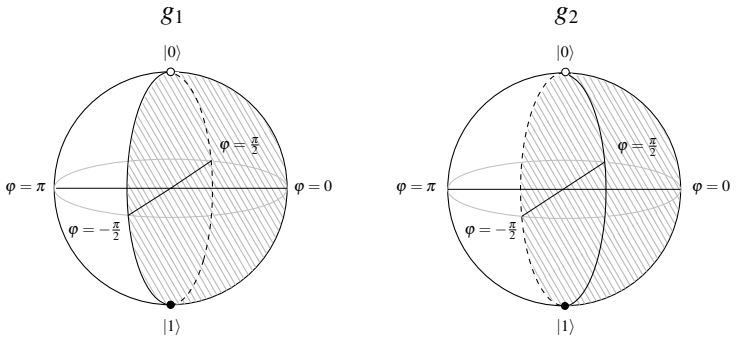

Figure 2 Graphical representation of the global assignment g. The shaded region corresponds to the measurements mapped to $+1$ by g.

have

$$s := \sin\delta \sin\frac{\theta_1}{2}\sin\frac{\theta_2}{2} > 0 \qquad \text{and} \qquad c := \cos\delta\cos\frac{\theta_1}{2}\cos\frac{\theta_2}{2} \geq 0.$$

If $\theta_1 = \pi$ or $\theta_2 = \pi$, then $c = 0$, which implies $\langle \boldsymbol{\theta}, \boldsymbol{\varphi}|\psi\rangle = se^{-i(\varphi_1+\varphi_2)} \neq 0$. Otherwise, $\varphi_1 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)$, $\varphi_2 \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right]$ and $\langle \boldsymbol{\theta}, \boldsymbol{\varphi}|\psi\rangle = c + se^{-i(\varphi_1+\varphi_2)}$ is the sum of a positive real number and a non-zero complex number. For it to be zero, the latter must be real and negative, hence

$$\varphi_1 + \varphi_2 = \pi \mod 2\pi,$$

which cannot be satisfied in the domain of φ_1, φ_2. ◀

4 W-SLOCC states are not strongly non-local

A general state in the SLOCC class of the W state $|\mathsf{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ can be written, up to LU, as

$$|\psi_{\mathsf{W}}\rangle = \sqrt{a}|001\rangle + \sqrt{b}|010\rangle + \sqrt{c}|100\rangle + \sqrt{d}|000\rangle, \tag{3}$$

where $a, b, c \in \mathbb{R}_{>0}$ and $d := 1 - (a + b + c) \in \mathbb{R}_{\geq 0}$. Indeed, we can obtain $|\psi_{\mathsf{W}}\rangle$ from $|\mathsf{W}\rangle$ by applying the following ILO to $|\mathsf{W}\rangle$:

$$\begin{pmatrix} \sqrt{a} & \sqrt{b} \\ 0 & \sqrt{c} \end{pmatrix} \otimes \begin{pmatrix} \sqrt{3} & 0 \\ 0 & \frac{\sqrt{3b}}{\sqrt{a}} \end{pmatrix} \otimes I.$$

In order to prove that W-SLOCC states are not strongly non-local, we will need the following lemma, which generalises the argument used in the proof of Theorem 1 to show that the amplitude could not be zero.

▶ **Lemma 2.** *Let $z_1, \ldots, z_m \in \mathbb{C}$, and $r \in \mathbb{R}_{\geq 0}$. If*

$$\sum_{i=1}^{m} z_i + r = 0, \tag{4}$$

then one of the following holds: (i) $z_1 = \cdots = z_m = r = 0$; (ii) there exists a $z_k \in \mathbb{R}_{<0}$; (iii) there exists $1 \leq k, l \leq m$ such that $\mathrm{Arg}(z_k) \in (0, \pi)$ and $\mathrm{Arg}(z_l) \in (-\pi, 0)$.

Proof. If all the z_i are real, then, since r is non-negative, we must have either (i) or (ii). Now, suppose there is a $1 \leq k \leq m$ such that $\mathrm{Im}(z_k) \neq 0$. By (4), we have $\sum_{i=1}^{n} \mathrm{Im}(z_i) = 0$. Thus,

$$\sum_{i \neq k} \mathrm{Im}(z_i) = -\mathrm{Im}(z_k) \quad \Leftrightarrow \quad \sum_{i \neq k} |z_i| \sin(\mathrm{Arg}(z_i)) = -|z_k| \sin(\mathrm{Arg}(z_k)).$$

Hence, there exists at least one $l \neq k$ for which the sign of $\mathrm{Im}(z_l)$ is opposite to that of $\mathrm{Im}(z_k)$, which implies that z_l and z_k are in different sides of the real axis, implying the condition about $\mathrm{Arg}(z_l)$ and $\mathrm{Arg}(z_k)$. ◀

▶ **Theorem 3.** *States in the SLOCC class of W do not admit strongly non-local behaviour.*

Proof. Similarly to the bipartite case of Theorem 1, the key idea of the proof is the definition of a global assignment $g : \mathsf{LM} \sqcup \mathsf{LM} \sqcup \mathsf{LM} \to O$ whose restriction to each context is contained in the support of the model. Once again, g is obtained by partitioning the Bloch sphere into two hemispheres to which are assigned different outcomes, with asymmetric polar conditions across the parties.

We start by computing the amplitude $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \psi_{\mathsf{W}} \rangle$ of measuring $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ on the general state (3) and obtaining joint outcome $\langle +1, +1, +1 \rangle$:

$$\begin{aligned} \langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \psi_{\mathsf{W}} \rangle = & \underbrace{\sqrt{a} \left(\cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \sin \frac{\theta_3}{2} e^{-i\varphi_3} \right)}_{=: z_3 \in \mathbb{C}} + \underbrace{\sqrt{b} \left(\cos \frac{\theta_1}{2} \cos \frac{\theta_3}{2} \sin \frac{\theta_2}{2} e^{-i\varphi_2} \right)}_{=: z_2 \in \mathbb{C}} \\ & + \underbrace{\sqrt{c} \left(\cos \frac{\theta_2}{2} \cos \frac{\theta_3}{2} \sin \frac{\theta_1}{2} e^{-i\varphi_1} \right)}_{=: z_1 \in \mathbb{C}} + \underbrace{\sqrt{d} \left(\cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \cos \frac{\theta_3}{2} \right)}_{=: r \in \mathbb{R}_{\geq 0}} . \end{aligned} \tag{5}$$

Define the following functions:

$$h = g_1 = g_2 \colon \mathsf{LM} \longrightarrow O :: (\theta, \varphi) \longmapsto \begin{cases} +1 & \text{if } \theta = 0 \text{ or } (\theta \neq \pi \text{ and } \varphi \in (-\pi, 0]) \\ -1 & \text{if } \theta = \pi \text{ or } (\theta \neq 0 \text{ and } \varphi \in (0, \pi]) \end{cases}$$

$$g_3 \colon \mathsf{LM} \longrightarrow O :: (\theta, \varphi) \longmapsto \begin{cases} +1 & \text{if } \theta = \pi \text{ or } (\theta \neq 0 \text{ and } \varphi \in (-\pi, 0]) \\ -1 & \text{if } \theta = 0 \text{ or } (\theta \neq \pi \text{ and } \varphi \in (0, \pi]) \end{cases}$$

and let $g := h \sqcup h \sqcup g_3 \colon \mathsf{LM} \sqcup \mathsf{LM} \sqcup \mathsf{LM} \longrightarrow O$ be a global assignment. The map g is graphically represented in Figure 3.

Let $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ be a context whose individual measurements are mapped to $+1$ by g. In particular, $\theta_1, \theta_2 \neq \pi$ and $\theta_3 \neq 0$. Since $a > 0$, we have

$$|z_3| = \sqrt{a} \cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \sin \frac{\theta_3}{2} > 0,$$

which implies $z_3 \neq 0$. Now, if $\theta_3 = \pi$, then $z_1 = z_2 = r = 0$ and $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \psi_{\mathsf{W}} \rangle = z_3 \neq 0$.

Otherwise, $\theta_3 \neq \pi$ and $\varphi_3 \in (-\pi, 0]$, implying that $\mathrm{Arg}(z_3) = -\varphi_3 \in [0, \pi)$. For $i = 1, 2$, we either have $\theta_i = 0$ or $\varphi_i \in (-\pi, 0]$, implying that $z_i = 0$ or $\mathrm{Arg}(z_i) = -\varphi_i \in [0, \pi)$. Using Lemma 2, we conclude that $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \psi_{\mathsf{W}} \rangle \neq 0$: (i) fails because $z_3 \neq 0$, while (ii) and (iii) fail because $\mathrm{Arg}(z_i) \in [0, \pi)$ whenever $z_i \neq 0$. ◀

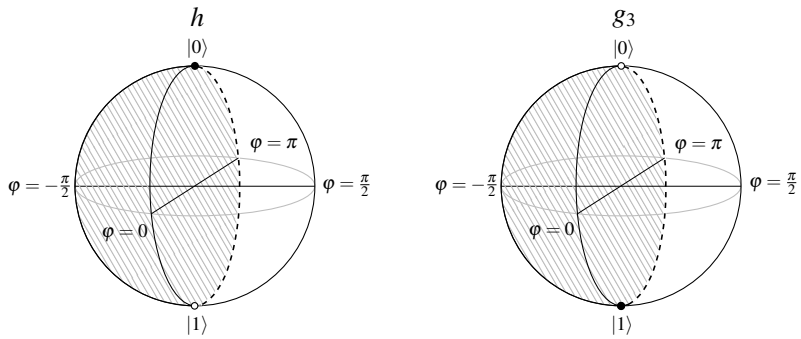

Figure 3 Graphical representation of the global assignment g. The shaded region corresponds to the measurements mapped to $+1$ by g.

5 Strong non-locality in the SLOCC class of GHZ

5.1 The n-partite GHZ state and local equatorial measurements

Before we tackle the general case of GHZ-SLOCC states, we consider the GHZ state itself. We show that equatorial measurements are the only relevant ones in the study of strong non-locality for this state. In fact, this holds for the general n-partite GHZ state,

$$|\mathsf{GHZ}(n)\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right),$$

and consequentely, in light of the remark towards the end of Section 2.3, for any state in its LU class. In the next section, we generalise this result to arbitrary states in the SLOCC class of the tripartite GHZ state, and study conditions for strong non-locality within this class.

▶ **Theorem 4.** *Any strongly non-local behaviour of $|\mathsf{GHZ}(n)\rangle$ can be witnessed using only equatorial measurements. That is, there is a global assignment g consistent with the model $e^{|\mathsf{GHZ}(n)\rangle}$ in all contexts that are not exclusively composed of equatorial measurements.*

Proof. The proof is achieved using a construction of a global assignment similar to the ones previously discussed.

First, we derive the formula for the amplitude $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \mathsf{GHZ}(n)\rangle$ of measuring $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ and obtaining joint outcome $\langle +1, \ldots, +1\rangle$:

$$\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \mathsf{GHZ}(n)\rangle = \frac{1}{\sqrt{2}}\left(\prod_{i=1}^{n} \cos\frac{\theta_i}{2} + e^{-i\sum_{i=1}^{n}\varphi_i} \prod_{i=1}^{n} \sin\frac{\theta_i}{2}\right).$$

Consider the function

$$h\colon \mathsf{LM} \longrightarrow O :: (\theta, \varphi) \longmapsto \begin{cases} +1 & \text{if } \theta \in \left[0, \frac{\pi}{2}\right] \\ -1 & \text{if } \theta \in \left(\frac{\pi}{2}, \pi\right] \end{cases}$$

i.e. h assigns $+1$ to the equator and the northern hemisphere, and -1 to the southern hemisphere. Let $g := \bigsqcup_{i=1}^{n} h\colon \bigsqcup_{i=1}^{n} \mathsf{LM} \longrightarrow O$. We show that this global assignment is consistent with the probabilities at all contexts that include at least a non-equatorial measurement.

Let $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ be a context whose measurements are mapped to $+1$ by g. In particular, $\theta_i \leq \frac{\pi}{2}$ for all i. If $\langle \boldsymbol{\theta}, \boldsymbol{\varphi} | \mathsf{GHZ}(n)\rangle = 0$, then

$$\prod_{i=1}^{n} \cos\frac{\theta_i}{2} = -e^{-i\left(\sum_{i=1}^{n}\varphi_i\right)} \prod_{i=1}^{n} \sin\frac{\theta_i}{2}$$

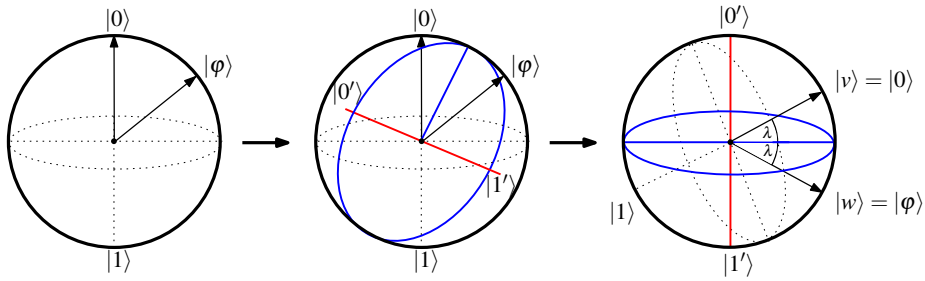

Figure 4 Choice of a new basis $\{|0'\rangle, |1'\rangle\}$ for each qubit that allows the state to be described in the form (7).

Taking the modulus of both sides and dividing the right-hand by the left-hand side yields:

$$\prod_{i=1}^{n} \tan \frac{\theta_i}{2} = 1$$

which is verified if and only if $\theta_i = \frac{\pi}{2}$ for all $1 \leq i \leq n$. ◀

5.2 Balanced GHZ-SLOCC states and local equatorial measurements

A general state in the SLOCC class of the GHZ state can be written, up to LU, as

$$|\psi_{\mathsf{GHZ}}\rangle = \sqrt{K}(\cos\delta|000\rangle + \sin\delta e^{i\Phi}|\varphi_1\rangle|\varphi_2\rangle|\varphi_3\rangle), \tag{6}$$

where $K = (1 + 2\cos\delta\sin\delta\cos\alpha\cos\beta\cos\gamma\cos\Phi)^{-1}$, and

$$|\varphi_1\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle, \quad |\varphi_2\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle, \quad |\varphi_3\rangle = \cos\gamma|0\rangle + \sin\gamma|1\rangle,$$

for some $\delta \in (0, \pi/4]$, $\alpha, \beta, \gamma \in (0, \pi/2]$, and $\Phi \in [0, 2\pi)$. Indeed, $|\psi_{\mathsf{GHZ}}\rangle$ is obtained from $|\mathsf{GHZ}\rangle$ via the ILO

$$\sqrt{2K}\begin{pmatrix} \cos\delta & \sin\delta\cos\alpha e^{i\Phi} \\ 0 & \sin\delta\sin\alpha e^{i\Phi} \end{pmatrix} \otimes \begin{pmatrix} 1 & \cos\beta \\ 0 & \sin\beta \end{pmatrix} \otimes \begin{pmatrix} 1 & \cos\gamma \\ 0 & \sin\gamma \end{pmatrix}.$$

In order to prove the results of this section, it is convenient to describe $|\psi_{\mathsf{GHZ}}\rangle$ in a slightly different form. By applying local unitaries, we can rewrite it as

$$|\psi_{\mathsf{GHZ}}\rangle = \sqrt{K}(\cos\delta|v_{\lambda_1}\rangle|v_{\lambda_2}\rangle|v_{\lambda_3}\rangle + \sin\delta e^{i\Phi}|w_{\lambda_1}\rangle|w_{\lambda_2}\rangle|w_{\lambda_3}\rangle), \tag{7}$$

where

$$|v_\lambda\rangle = |\lambda, 0\rangle = \cos\frac{\lambda}{2}|0\rangle + \sin\frac{\lambda}{2}|1\rangle, \quad |w_\lambda\rangle = |\pi - \lambda, 0\rangle = \sin\frac{\lambda}{2}|0\rangle + \cos\frac{\lambda}{2}|1\rangle \tag{8}$$

for some $\lambda_i \in [0, \frac{\pi}{2})$, $i = 1, 2, 3$. The action of this LU can be thought of as choosing a new orthonormal basis for each qubit: a graphical illustration of this process can be found in Figure 4. A key advantage of this LU-equivalent description of a general state in the GHZ SLOCC class is that the equator of the i-th qubit's Bloch sphere coincides with the great circle that bisects the i-th components of the two unique product states that form a linear decomposition of the state. Note that any state in the GHZ SLOCC class thus uniquely defines an equator in each Bloch sphere. It is to the measurements lying on these that we refer as being *equatorial*.

We say that a state in the GHZ SLOCC class is *balanced* if the coefficients in its unique linear decomposition into a pair of product states have the same complex modulus – when the state is written in the form (7), this corresponds to having $\delta = \frac{\pi}{4}$, hence $\cos\delta = \sin\delta = \frac{1}{\sqrt{2}}$.

▶ **Lemma 5.** *Let $|v_\lambda\rangle$ and $|w_\lambda\rangle$ be given as in (8), with $\lambda \in [0, \pi/2)$, and consider a measurement (θ, φ) with $\theta \in [0, \pi/2)$, i.e. with $+1$ eigenstate in the 'northern hemisphere'. Then $|\langle\theta, \varphi|v_\lambda\rangle| > |\langle\theta, \varphi|w_\lambda\rangle|$.*

Proof. We have

$$|\langle\theta, \varphi|v_\lambda\rangle| > |\langle\theta, \varphi|w_\lambda\rangle| \Leftrightarrow \left|\cos\frac{\theta}{2}\cos\frac{\lambda}{2} + \sin\frac{\theta}{2}\sin\frac{\lambda}{2}e^{-i\varphi}\right| > \left|\cos\frac{\theta}{2}\sin\frac{\lambda}{2} + \sin\frac{\theta}{2}\cos\frac{\lambda}{2}e^{-i\varphi}\right|$$
$$\Leftrightarrow \left|1 + \tan\frac{\lambda}{2}\tan\frac{\theta}{2}e^{-i\varphi}\right| > \left|\tan\frac{\lambda}{2} + \tan\frac{\theta}{2}e^{-i\varphi}\right|,$$

where, for the last step, we divide both sides by $\cos\frac{\lambda}{2}\cos\frac{\theta}{2}$, which is never 0 since $\lambda, \theta \in [0, \pi/2)$. Let $x := \tan\frac{\lambda}{2}$ and $y := \tan\frac{\theta}{2}$, then

$$\begin{aligned}|1 + xye^{-i\varphi}| > |x + ye^{-i\varphi}| &\Leftrightarrow |1 + xy(\cos\varphi - i\sin\varphi)| > |x + y(\cos\varphi - i\sin\varphi)| \\ &\Leftrightarrow 1 + 2xy\cos\varphi + x^2y^2 > x^2 + 2xy\cos\varphi + y^2 \\ &\Leftrightarrow 1 + x^2y^2 - x^2 - y^2 > 0 \Leftrightarrow (1 - x^2)(1 - y^2) > 0\end{aligned}$$

and this is always verified since $x, y \in [0, 1)$ by the definition of the domains of θ and λ. ◀

We use this lemma to generalise Theorem 4 to arbitrary states in the SLOCC class of the tripartite GHZ state.

▶ **Theorem 6.** *A state in the SLOCC class of GHZ that displays strong non-locality must be balanced. Moreover, any such strongly non-local behaviour can be witnessed using only equatorial measurements.*

Proof. The proof of this theorem can be derived by taking advantage of the special properties of balanced states and combining them with the argument used for Theorem 4.

As before, we compute the amplitude $\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|\psi_{\mathsf{GHZ}}\rangle$:

$$\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|\psi_{\mathsf{GHZ}}\rangle = \sqrt{K}\left(\cos\delta\prod_{i=1}^{3}\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|v_{\lambda_i}\rangle + \sin\delta e^{i\Phi}\prod_{i=1}^{3}\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|w_{\lambda_i}\rangle\right)$$

Take $h\colon \mathsf{LM} \longrightarrow O$ as defined in the proof of Theorem 4 and let $g := h \sqcup h \sqcup h$. We claim that g is consistent with the empirical probabilities at all contexts that include at least a non-equatorial measurement.

Let $(\boldsymbol{\theta}, \boldsymbol{\varphi})$ be a context whose measurements are all mapped to $+1$ by g. In particular, $\theta_i \leq \frac{\pi}{2}$ for $i = 1, 2, 3$. If $\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|\psi_{\mathsf{GHZ}}\rangle = 0$, then

$$\cos\delta\prod_{i=1}^{3}\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|v_{\lambda_i}\rangle = -\sin\delta e^{i\Phi}\prod_{i=1}^{3}\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|w_{\lambda_i}\rangle,$$

and taking the complex modulus of both sides,

$$\cos\delta\prod_{i=1}^{3}|\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|v_{\lambda_i}\rangle| = \sin\delta\prod_{i=1}^{3}|\langle\boldsymbol{\theta}, \boldsymbol{\varphi}|w_{\lambda_i}\rangle|$$

Since $\delta \in (0, \pi/4]$ we have $\cos\delta \geq \sin\delta$, with equality iff $\delta = \frac{\pi}{4}$. By Lemma 5, we conclude that this equation can only be satisfied if $\delta = \frac{\pi}{4}$ (i.e. the state is balanced) and $\theta_i = \frac{\pi}{2}$ for $i = 1, 2, 3$ (i.e. all the measurements are equatorial). ◀

5.3 Further restrictions

The theorem above allows us to reduce the scope of our search for strongly non-local behaviour in the SLOCC class of GHZ to: (i) balanced states, i.e. those of the form

$$|\mathsf{B}_{\boldsymbol{\lambda},\Phi}\rangle := \sqrt{\frac{K}{2}}(|v_{\lambda_1}\rangle|v_{\lambda_2}\rangle|v_{\lambda_3}\rangle + e^{i\Phi}|w_{\lambda_1}\rangle|w_{\lambda_2}\rangle|w_{\lambda_3}\rangle),$$

determined by a tuple $\boldsymbol{\lambda} = \langle\lambda_1, \lambda_2, \lambda_3\rangle \in \left[0, \frac{\pi}{2}\right)^3$ and a phase Φ, where $|v_\lambda\rangle$ and $|w_\lambda\rangle$ are given as in (8); (ii) local equatorial measurements in the sense defined above, i.e. those with $+1$ eigenstate

$$|\varphi\rangle := \left|\frac{\pi}{2}, \varphi\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$$

for $\varphi \in [0, 2\pi)$. Given this premise, we are interested in understanding when the amplitude function $\langle\boldsymbol{\varphi}|\mathsf{B}_{\boldsymbol{\lambda},\Phi}\rangle$ is 0. We have:

$$\begin{aligned}
\langle\boldsymbol{\varphi}|\mathsf{B}_{\boldsymbol{\lambda},\Phi}\rangle = 0 &\Leftrightarrow \prod_{i=1}^{3}\langle\varphi_i|v_{\lambda_i}\rangle + e^{i\Phi}\prod_{i=1}^{3}\langle\varphi_i|w_{\lambda_i}\rangle = 0 \\
&\Leftrightarrow \prod_{i=1}^{3}\langle\varphi_i|w_{\lambda_i}\rangle = -e^{-i\Phi}\prod_{i=1}^{3}\langle\varphi_i|v_{\lambda_i}\rangle \\
&\Leftrightarrow \prod_{i=1}^{3}\langle\varphi_i|w_{\lambda_i}\rangle = -e^{-i\Phi}\prod_{i=1}^{3}e^{-i\varphi_i}\overline{\langle\varphi_i|w_{\lambda_i}\rangle} \qquad (9) \\
&\Leftrightarrow \prod_{i=1}^{3}e^{i\varphi_i}\langle\varphi_i|w_{\lambda_i}\rangle\overline{\langle\varphi_i|w_{\lambda_i}\rangle}^{-1} = -e^{-i\Phi} \\
&\Leftrightarrow \prod_{i=1}^{3}e^{i\varphi_i}\left(\frac{\langle\varphi_i|w_{\lambda_i}\rangle}{|\langle\varphi_i|w_{\lambda_i}\rangle|}\right)^2 = -e^{-i\Phi} \\
&\Leftrightarrow \sum_{i=1}^{3}(\varphi_i + 2\mathrm{Arg}\langle\varphi_i|w_{\lambda_i}\rangle) = \pi - \Phi \mod 2\pi
\end{aligned}$$

where to get (9) we use

$$\langle\varphi|v_\lambda\rangle = \frac{1}{\sqrt{2}}\left(\cos\frac{\lambda}{2} + \sin\frac{\lambda}{2}e^{-i\varphi}\right) = \frac{e^{-i\varphi}}{\sqrt{2}}\left(\cos\frac{\lambda}{2}e^{i\varphi} + \sin\frac{\lambda}{2}\right) = e^{-i\varphi}\overline{\langle\varphi|w_\lambda\rangle}.$$

and for the last step we take the argument of two complex numbers of norm 1. Defining

$$\beta(\lambda, \varphi) := \varphi + 2\mathrm{Arg}\langle\varphi|w_\lambda\rangle = \varphi - 2\arctan\left(\frac{\sin\frac{\lambda}{2}\sin\varphi}{\cos\frac{\lambda}{2} + \sin\frac{\lambda}{2}\cos\varphi}\right),$$

we can rewrite the condition above as

$$\langle\boldsymbol{\varphi}|\mathsf{B}_{\boldsymbol{\lambda},\Phi}\rangle = 0 \quad\Leftrightarrow\quad \sum_{i=1}^{3}\beta(\lambda_i, \varphi_i) = \pi - \Phi \mod 2\pi \qquad (10)$$

▶ **Proposition 7.** *If $\lambda_1 + \lambda_2 + \lambda_3 > \frac{\pi}{2}$, the state $|\mathsf{B}_{\boldsymbol{\lambda},0}\rangle$ does not admit strongly non-local behaviour.*

Proof. We start by showing that the map $\beta(\lambda, \varphi)$, seen as a function of φ, is strictly increasing for all $\lambda \in \left[0, \frac{\pi}{2}\right)$. To see this, it is sufficient to compute the derivative:

$$\forall \lambda \in \left[0, \frac{\pi}{2}\right), \varphi \in [0, 2\pi). \quad \frac{\partial}{\partial \varphi}\beta(\lambda, \varphi) = \frac{\cos\lambda}{1 + \cos\varphi \sin\lambda}.$$

This is strictly positive since $\cos\lambda > 0$ and $\cos\varphi\sin\lambda > -1$ since $0 \leq \sin\lambda < 1$.

Now, define a function $h\colon [0, 2\pi) \longrightarrow O$ by

$$h(\varphi) := \begin{cases} +1 & \text{if } \varphi \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ -1 & \text{if } \varphi \in \left(\frac{\pi}{2}, \frac{3\pi}{2}\right] \end{cases}$$

and let $g := h \sqcup h \sqcup h$. Take a context $\boldsymbol{\varphi}$ whose measurements are assigned $+1$ by g, i.e. $\varphi_i \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Using the fact that $\beta(\lambda, -)$ is increasing, we have

$$\left|\sum_{i=1}^{3} \beta(\lambda_i, \varphi_i)\right| \leq \sum_{i=1}^{3} |\beta(\lambda_i, \varphi_i)| \leq \sum_{i=1}^{3} \beta\left(\lambda_i, \frac{\pi}{2}\right) = \sum_{i=1}^{3}\left(\frac{\pi}{2} - \lambda_i\right) = \frac{3\pi}{2} - \sum_{i=1}^{3}\lambda_i < \frac{3\pi}{2} - \frac{\pi}{2} = \pi.$$

Consequently, $\sum_{i=1}^{3} \beta(\lambda_i, \varphi_i) \neq \pi \mod 2\pi$, hence by (10), $\langle \boldsymbol{\varphi} | \mathsf{B}_{\boldsymbol{\lambda},0} \rangle \neq 0$ as required. ◀

6 A family of strongly non-local three-qubit models

▶ **Theorem 8.** *Let $m \in \mathbb{N}_{>0}$ and $N := 2m$ an even number. Consider the tripartite measurement scenario with $X_1 = X_2 = \{0, \ldots, N-1\}$ and $X_3 = \left\{0, \frac{N}{2}\right\}$. The empirical model determined by the state $|\mathsf{B}_{\langle 0,0,\lambda_N\rangle,0}\rangle$, where $\lambda_N := \frac{\pi}{2} - \frac{\pi}{N}$, with the measurement label i at each site interpreted as the local equatorial measurement $\cos\frac{i\pi}{N}\sigma_X + \sin\frac{i\pi}{N}\sigma_Y$ (i.e. the measurement with $+1$ eigenstate $|\frac{\pi}{2}, i\frac{\pi}{N}\rangle$), is strongly non-local.*

Proof. This proof rests on deriving, using the algebraic structure of $\mathbb{Z}_{2N}$, a (conditional) system of linear equations over $\mathbb{Z}_2$ that must be satisfied by any global assignment consistent with the possible events of the empirical model, yet does not admit any solution. This seems to be closely related to the general concept of all-vs-nothing (AvN) arguments introduced in [1], but does not quite fit this setting. The reason is that the system of linear equations that a global assignment g must satisfy depends on the value that g assigns to a particular measurement. In that sense, this could be seen as a conditional version of an AvN argument.

Consider a context $\langle i, j, k\rangle \in X_1 \times X_2 \times X_3$, with $i, j \in \{0, \ldots, N-1\}$, $k \in \{0, m\}$, and a triple of outcomes $\langle a_i, b_j, c_k\rangle \in \mathbb{Z}_2^3$ for the measurements in the context.[5] From equation (10), we know that measuring $\langle i, j, k\rangle$ and obtaining outcomes $\langle a_i, b_j, c_k\rangle$ has probability zero if and only if

$$\beta\left(0, i\frac{\pi}{N} + a_i\pi\right) + \beta\left(0, j\frac{\pi}{N} + b_j\pi\right) + \beta\left(\frac{\pi}{2} - \frac{\pi}{N}, k\frac{\pi}{N} + c_k\pi\right) = \pi \mod 2\pi \tag{11}$$

With simple computations, we can show that $\beta(0, \varphi) = \varphi$ for all $\varphi \in [0, 2\pi)$, and that

$$\beta\left(\frac{\pi}{2} - \frac{\pi}{N}, c_0\pi\right) = c_0\pi \quad \text{and} \quad \beta\left(\frac{\pi}{2} - \frac{\pi}{N}, \frac{\pi}{2} + c_m\pi\right) = (-1)^{c_m}\frac{\pi}{N}. \tag{12}$$

An arbitrary global assignment is defined by choosing outcomes for all the measurements in $X_1 \sqcup X_2 \sqcup X_3$:

$$a_0, \ldots, a_{N-1}, b_0, \ldots, b_{N-1}, c_0, c_m \in \mathbb{Z}_2.$$

[5] For this proof, it is convenient to relabel $+1, -1, \times$ as $0, 1, \oplus$, where $\oplus$ denotes addition modulo 2.

By (11) and (12), such an assignment is consistent with the probabilities of the empirical model at every context if and only if

$$\begin{cases} i\frac{\pi}{N} + a_i\pi + j\frac{\pi}{N} + b_j\pi + c_0\pi \neq \pi & \mod 2\pi \quad \forall i,j \in \{0,\dots,N-1\} \\ i\frac{\pi}{N} + a_i\pi + j\frac{\pi}{N} + b_j\pi + (-1)^{c_m}\frac{\pi}{N} \neq \pi & \mod 2\pi \quad \forall i,j \in \{0,\dots,N-1\} \end{cases}$$

We will proceed to show that this system admits no solution, which implies strong non-locality. By identifying the group $\left\{k\frac{\pi}{N} \mid k \in \mathbb{Z}_{2N}\right\}$ with $\mathbb{Z}_{2N}$, we can equivalently rewrite

$$\begin{cases} i + a_iN + j + b_jN + c_0N \neq N & \mod 2N \quad \forall i,j \\ i + a_iN + j + b_jN + (-1)^{c_m} \neq N & \mod 2N \quad \forall i,j \end{cases}$$

$\Leftrightarrow$

$$\begin{cases} i + j + N(a_i \oplus b_j \oplus c_0) \neq N & \mod 2N \quad \forall i,j \\ i + j + (-1)^{c_m} + N(a_i \oplus b_j) \neq N & \mod 2N \quad \forall i,j \end{cases}$$

$\Leftrightarrow$

$$\begin{cases} a_i \oplus b_j \oplus c_0 = 0 & \forall i,j \text{ s.t. } i+j=0 \\ a_i \oplus b_j \oplus c_0 = 1 & \forall i,j \text{ s.t. } i+j=N \\ \\ a_i \oplus b_j = 0 & \forall i,j \text{ s.t. } i+j+(-1)^{c_m}=0 \\ a_i \oplus b_j = 1 & \forall i,j \text{ s.t. } i+j+(-1)^{c_m}=N. \end{cases}$$

$\Leftrightarrow$

$$\begin{cases} a_0 \oplus b_0 \oplus c_0 = 0 & & \\ a_i \oplus b_{N-i} \oplus c_0 = 1 & \forall i \text{ s.t. } 1 \leq i \leq N-1 & \\ \\ a_i \oplus b_{N-i-1} = 1 & \forall i \text{ s.t. } 0 \leq i \leq N-1 & \text{if } c_m = 0 \\ \\ a_0 \oplus b_1 = 0 & & \\ a_1 \oplus b_0 = 0 & & \text{if } c_m = 1 \\ a_i \oplus b_{N+1-i} = 1 & \forall i \text{ s.t. } 2 \leq i \leq N-1 & \end{cases}$$

Since $N = 2m$ is even, if we sum all the N equations from the first two lines we obtain

$$\bigoplus_{i=0}^{N-1} a_i \oplus \bigoplus_{j=0}^{N-1} b_j = 1.$$

On the other hand, if we sum any of the other two groups of N equations we get

$$\bigoplus_{i=0}^{N-1} a_i \oplus \bigoplus_{j=0}^{N-1} b_j = 0,$$

showing that the system is unsatisfiable regardless of whether $c_m = 0$ or $c_m = 1$. ◀

This new family of strongly non-local three-qubit systems is tightly connected to a construction on two-qubit states due to Barrett, Kent, and Pironio [8]. In particular, our empirical models restricted to the first two parties coincide, up to a rotation of the equatorial

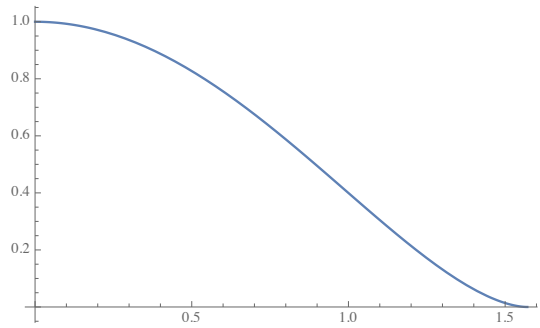

Figure 5 Von Neumann entanglement entropy between the third qubit of $|\mathsf{B}_{\langle 0,0,\lambda\rangle,0}\rangle$ and the other two as a function of λ.

measurements, to those used in [8]. The local fraction of these bipartite empirical models tends to zero as the number of measurements increases, but obviously none of them are strongly non-local. Despite the lack of strong non-locality in the bipartite systems constructed in [8], we show that it is possible to witness strongly non-local behaviour with a finite amount of measurements by adding a third qubit with some entanglement, and only two local measurements – Pauli X and Y – available on it. An interesting aspect is that there is a trade-off between the number of measuring settings available on the first two qubits and the amount of entanglement between the third qubit and the system comprised of the other two.

We illustrate this by computing the bipartite von Neumann entanglement entropy between the first two qubits and the third, i.e. the von Neumann entropy of the reduced state of $|\mathsf{B}_{\langle 0,0,\lambda\rangle,0}\rangle$ corresponding to the third qubit, as a function of λ. Let ρ_{ABC} denote the density matrix of $|\mathsf{B}_{\langle 0,0,\lambda\rangle,0}\rangle$. The reduced density matrix corresponding to the third qubit is

$$\rho_C(\lambda) = \mathrm{Tr}_{AB}[\rho_{ABC}] = \langle 00|_{AB}\rho_{ABC}|00\rangle_{AB} + \langle 11|_{AB}\rho_{ABC}|11\rangle_{AB} = \frac{1}{2}\begin{pmatrix} 1 & 2\cos\frac{\lambda}{2}\sin\frac{\lambda}{2} \\ 2\cos\frac{\lambda}{2}\sin\frac{\lambda}{2} & 1 \end{pmatrix}.$$

The eigenvalues of $\rho_C(\lambda)$ are $\epsilon_\pm(\lambda) := \frac{1}{2}(1 \pm \sin\lambda)$. Hence, by rewriting $\rho_C(\lambda)$ in its eigenbasis, we can easily compute the von Neumann entropy S_C as a function of λ:

$$S_C(\lambda) := -\,\mathrm{Tr}\left[\rho_C(\lambda)\log_2\rho_C(\lambda)\right] = -\epsilon_+(\lambda)\log_2\epsilon_+(\lambda) - \epsilon_-(\lambda)\log_2\epsilon_-(\lambda)$$

The plot of the function $S_C(\lambda)$ is shown in Figure 5. Notice that the entanglement entropy is maximal, i.e. equal to 1, when $N = 2$, in which case $\lambda_2 = 0$ and so $|\mathsf{B}_{\langle 0,0,\lambda_2\rangle,0}\rangle = |\mathsf{GHZ}\rangle$. This corresponds to the usual GHSZ argument with Pauli measurements X,Y for each qubit. On the other hand, $S(\lambda)$ becomes arbitrarily small as $N \to \infty$, when $\lambda_N \to \frac{\pi}{2}$ and $|\mathsf{B}_{\langle 0,0,\lambda_N\rangle,0}\rangle$ approaches the state $|\Phi^+\rangle \otimes |+\rangle$, which has no entanglement between the first two qubits and the third.

7 Outlook

Our analysis of strong non-locality for three-qubit systems has been quite extensive. We shall discuss a number of directions for further research.

1. First, it remains to complete our classification of all instances of three-qubit strong non-locality.
2. The original GHSZ–Mermin model witnesses the yet stronger algebraic notion of all-versus-nothing (AvN) non-locality, formalised in a general setting in [1], and indeed

provides one of the motivating examples for considering this kind of non-locality. The family of strongly non-local models introduced in Section 6 does not fit this framework exactly. Nevertheless, our proof of strong non-locality does make essential use of the algebraic structure of $\mathbb{Z}_{2N}$ (or the circle group), in what amounts to a conditional version of an AvN argument. One may wonder whether a similar property will hold for all instances of three-qubit strong non-locality.

3. This family also highlights an inter-relationship between non-locality, entanglement and the number of measurements available, and raises the question of whether this is an instance of a more general relationship.
4. Finally, while the present results provide necessary conditions for strong non-locality in three-qubit states, the more general question of characterising strong non-locality of n-qubit states, where little is known about SLOCC classes, remains open.

References

1. Samson Abramsky, Rui Soares Barbosa, Kohei Kishida, Raymond Lal, and Shane Mansfield. Contextuality, cohomology and paradox. In Stephan Kreutzer, editor, *24th EACSL Annual Conference on Computer Science Logic, CSL 2015, September 7-10, 2015, Berlin, Germany*, volume 41 of *LIPIcs*, pages 211–228. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015. doi:10.4230/LIPIcs.CSL.2015.211.
2. Samson Abramsky, Rui Soares Barbosa, and Shane Mansfield. The contextual fraction as a measure of contextuality. to appear, 2017.
3. Samson Abramsky and Adam Brandenburger. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics*, 13(11):113036, 2011. doi:10.1088/1367-2630/13/11/113036.
4. Samson Abramsky, Carmen M. Constantin, and Shenggang Ying. Hardy is (almost) everywhere: nonlocality without inequalities for almost all entangled multipartite states. *Information and Computation*, 250:3–14, 2016.
5. Samson Abramsky, Shane Mansfield, and Rui Soares Barbosa. The cohomology of non-locality and contextuality. In Bart Jacobs, Peter Selinger, and Bas Spitters, editors, *Proceedings 8th International Workshop on Quantum Physics and Logic, QPL 2011, Nijmegen, Netherlands, October 27-29, 2011.*, volume 95 of *EPTCS*, pages 1–14, 2011. doi:10.4204/EPTCS.95.1.
6. Janet Anders and Dan E. Browne. Computational power of correlations. *Physical Review Letters*, 102:050502, Feb 2009. doi:10.1103/PhysRevLett.102.050502.
7. Leandro Aolita, Rodrigo Gallego, Antonio Acín, Andrea Chiuri, Giuseppe Vallone, Paolo Mataloni, and Adán Cabello. Fully nonlocal quantum correlations. *Physical Review A*, 85(3):032107, Mar 2012. doi:10.1103/PhysRevA.85.032107.
8. Jonathan Barrett, Adrian Kent, and Stefano Pironio. Maximally nonlocal and monogamous quantum correlations. *Physical Review Letters*, 97(17):170409, Oct 2006. doi:10.1103/PhysRevLett.97.170409.
9. John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.
10. Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53:2046–2052, Apr 1996. doi:10.1103/PhysRevA.53.2046.
11. Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure-state entanglement. *Physical Review A*, 63:012307, Dec 2000. doi:10.1103/PhysRevA.63.012307.

12 Gilles Brassard, André Allan Méthot, and Alain Tapp. Minimum entangled state dimension required for pseudo-telepathy. *Quantum Information & Computation*, 5(4):275–284, Jul 2005.

13 John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, Oct 1969. doi:10.1103/PhysRevLett.23.880.

14 Vedran Dunjko, Theodoros Kapourniotis, and Elham Kashefi. Quantum-enhanced secure delegated classical computing. *Quantum Information & Computation*, 61(1):61–86, Jan 2016.

15 W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, Nov 2000. doi:10.1103/PhysRevA.62.062314.

16 Avshalom C. Elitzur, Sandu Popescu, and Daniel Rohrlich. Quantum nonlocality for each pair in an ensemble. *Phys. Lett. A*, 162(1):25–28, 1992. doi:10.1016/0375-9601(92)90952-I.

17 Arthur Fine. Hidden variables, joint probability, and the Bell inequalities. *Physical Review Letters*, 48(5):291–295, Feb 1982. doi:10.1103/PhysRevLett.48.291.

18 Daniel M. Greenberger, Michael A. Horne, Abner Shimony, and Anton Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990. doi:10.1119/1.16243.

19 Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's theorem, quantum theory, and conceptions of the universe*, pages 69–72. Kluwer, 1989.

20 Otfried Gühne, Géza Tóth, Philipp Hyllus, and Hans J. Briegel. Bell inequalities for graph states. *Physical Review Letters*, 95:120405, Sep 2005. doi:10.1103/PhysRevLett.95.120405.

21 Lucien Hardy. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Physical Review Letters*, 68(20):2981–2984, May 1992. doi:10.1103/PhysRevLett.68.2981.

22 Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71(11):1665–1668, 1993.

23 Peter Heywood and Michael L. G. Redhead. Nonlocality and the Kochen–Specker paradox. *Foundations of physics*, 13(5):481–499, 1983. doi:10.1007/BF00729511.

24 Adrian Kent, Noah Linden, and Serge Massar. Optimal entanglement enhancement for mixed states. *Physical Review Letters*, 83:2656–2659, Sep 1999. doi:10.1103/PhysRevLett.83.2656.

25 Laura Mančinska, David E. Roberson, and Antonios Varvitsiotis. On deciding the existence of perfect entangled strategies for nonlocal games. *Chicago Journal of Theoretical Computer Science*, 2016(5):1–16, Apr 2016.

26 Shane Mansfield. Consequences and applications of the completeness of Hardy's nonlocality. *Physical Review A*, 95:022122, Feb 2017. doi:10.1103/PhysRevA.95.022122.

27 N. David Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58(8):731–734, 1990. doi:10.1119/1.16503.

28 N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373–3376, Dec 1990. doi:10.1103/PhysRevLett.65.3373.

29 M. A. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436–439, Jul 1999. doi:10.1103/PhysRevLett.83.436.

30 Robert Raussendorf. Contextuality in measurement-based quantum computation. *Physical Review A*, 88:022322, Aug 2013. doi:10.1103/PhysRevA.88.022322.

31 Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, May 2001. doi:10.1103/PhysRevLett.86.5188.

Approximate Reversal of Quantum Gaussian Dynamics

Ludovico Lami*[1], Siddhartha Das†[2], and Mark M. Wilde‡[3]

1 **Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, Barcelona, Spain**
ludovico.lami@gmail.com

2 **Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Louisiana State University, Baton Rouge, USA**
sdas21@lsu.edu

3 **Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation & Technology, Louisiana State University, Baton Rouge, USA**
mwilde@lsu.edu

Abstract

Recently, there has been focus on determining the conditions under which the data processing inequality for quantum relative entropy is satisfied with approximate equality. The solution of the exact equality case is due to Petz, who showed that the quantum relative entropy between two quantum states stays the same after the action of a quantum channel if and only if there is a *reversal channel* that recovers the original states after the channel acts. Furthermore, this reversal channel can be constructed explicitly and is now called the *Petz recovery map*. Recent developments have shown that a variation of the Petz recovery map works well for recovery in the case of approximate equality of the data processing inequality. Our main contribution here is a proof that bosonic Gaussian states and channels possess a particular closure property, namely, that the Petz recovery map associated to a bosonic Gaussian state σ and a bosonic Gaussian channel $\mathcal{N}$ is itself a bosonic Gaussian channel. We furthermore give an explicit construction of the Petz recovery map in this case, in terms of the mean vector and covariance matrix of the state σ and the Gaussian specification of the channel $\mathcal{N}$.

1998 ACM Subject Classification H.1.1 Systems and Information Theory

Keywords and phrases Gaussian dynamics, Petz recovery map

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.10

1 Introduction

1.1 Introduction to recoverability in quantum information

Strong subadditivity of quantum entropy is one of the cornerstones of quantum information theory, on which many fundamental results rely. Defining the conditional mutual information of a tripartite state ρ_{ABC} as

$$I(A;B|C)_\rho := S(AC)_\rho + S(BC)_\rho - S(ABC)_\rho - S(C)_\rho, \tag{1}$$

* LL acknowledges financial support from the European Research Council (AdG IRQUAT No. 267386), the Spanish MINECO (Project no. FIS2013-40627-P and no. FIS2016-86681-P), and the Generalitat de Catalunya (CIRIT Project no. 2014 SGR 966).
† SD acknowledges support from the Economic Development Assistantship of Louisiana State University.
‡ MMW acknowledges support from the National Science Foundation under Award No. CCF-1350397.

12th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2017).
Editor: Mark M. Wilde; Article No. 10; pp. 10:1–10:18
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

where $S(G)_\sigma \equiv -\operatorname{Tr}[\sigma_G \log \sigma_G]$ is the quantum entropy of a state σ_G of a system G, strong subadditivity is equivalent to the non-negativity of conditional mutual information: $I(A;B|C)_\rho \geq 0$. Initially conjectured in 1967 [55, 26], it was subsequently proven six years later [35, 36]. Afterward, its equivalence to the data processing inequality for the quantum relative entropy [68] was realized [66, 37, 38, 56]. This latter inequality has the form

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)), \tag{2}$$

being valid for all states ρ, σ and all quantum channels $\mathcal{N}$ (completely positive, trace-preserving maps). Here, the quantum relative entropy is defined for quantum states ρ and σ as

$$D(\rho\|\sigma) \equiv \operatorname{Tr}[\rho(\log \rho - \log \sigma)], \tag{3}$$

whenever the support of ρ is contained in the support of σ, and it is set to $+\infty$ otherwise [68].

The interest in strong subadditivity has not fallen over time, and many different proofs for it have been proposed in the last four decades (see for instance [43]). At the same time, new improvements of the original inequality have recently been found. Extending methods originally proposed in [17], an operator generalization of strong subadditivity was recently proven in [28].

A line of research which is of particular interest to us focuses on investigating the conditions under which strong subadditivity, or more generally the data processing inequality for relative entropy, is satisfied with equality or approximate equality. The solution of the exact equality case dates back to the 1980s: in [50, 51, 52], it was shown that the relative entropy between two states stays the same after the action of a quantum channel if and only if there is a *recovery channel* bringing back both images to the original states. Furthermore, this reversing channel can be constructed explicitly and now takes the name *Petz recovery map*. Afterward, [42, 41] proved a structure theorem giving a form for states and a channel saturating the data-processing inequality for relative entropy, and, related to this development, the form of tripartite states satisfying strong subadditivity with equality was determined in [24].

Characterising the structure of states for which strong subadditivity is nearly saturated requires different techniques, and progress was not made until more recently. In 2011, a lower bound on conditional mutual information in terms of one-way LOCC norms [40] was proven in [9], the motivation for [9] lying in the question of faithfulness of an entanglement measure called squashed entanglement [14] (see also [64, 65] for discussions related to squashed entanglement). Later on, a conjecture put forward in [75] proposed another operationally meaningful remainder term for the relative entropy decrease induced by a quantum channel, given by the relative entropy between the state ρ and a "recovered version" of $\mathcal{N}(\rho)$. The authors of [75] proposed the following conjecture as a refinement of (2):

$$D(\rho\|\sigma) \overset{?}{\geq} D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) + D(\rho\|(\mathcal{R}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho)), \tag{4}$$

where $\mathcal{R}_{\sigma,\mathcal{N}}$ should be a quantum channel depending only on σ and $\mathcal{N}$ and such that $(\mathcal{R}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\sigma) = \sigma$. The authors of [75] proved (4) in the classical case, when the states ρ and σ commute and the channel is classical as well, and they showed how the recovery channel in this case can be taken as the Petz recovery map. This conjecture has now been proven in a number of special, yet physically relevant cases as well [2, 11, 39, 32, 3]. Unfortunately, the authors of [75] showed that in the general quantum case, $\mathcal{R}_{\sigma,\mathcal{N}}$ in (4) cannot be taken as the Petz recovery map. For further details, see also [29, 33], and for related conjectures, see [7, 59].

While the general form of the conjecture in (4) remains unproven, in [18], it was shown that if the conditional mutual information $I(A;B|C)_\rho$ is small, then the state ρ_{ABC} can be very well approximated by one of its "reconstructed" versions $\mathcal{R}_{C\to BC}(\rho_{AC})$. That is, the authors of [18] proved the following inequality:

$$I(A;B|C)_\rho \geq -\log F(\rho_{ABC}, \mathcal{R}_{C\to BC}(\rho_{AC}))\,, \tag{5}$$

where F denotes the quantum fidelity [67], defined as $F(\omega,\tau) := \|\sqrt{\omega}\sqrt{\tau}\|_1^2$ for quantum states ω and τ, and $\mathcal{R}_{C\to BC}$ is a recovery channel taking an input system C to output systems BC. Furthermore, the channel $\mathcal{R}_{C\to BC}$ can be taken as the Petz recovery map up to some unitary rotations preceding and following its action, but note that the unitary rotations given in [18] generally depend on the full state ρ_{ABC}.

After the result of [18] appeared, much activity surrounding entropy inequalities and recovery channels occurred. An alternative and simpler proof of the faithfulness of squashed entanglement following the lines of [75] immediately appeared [33], while an alternative proof of (5) that makes use of quantum state redistribution [15, 76] appeared in [10]. In [62], an important particular case of (5) was proven; that is, it was shown that the recovery map in (5) can be chosen to depend only on ρ_{BC} and to obey $\mathcal{R}_{C\to BC}(\rho_C) = \rho_{BC}$. A different approach was delivered in [71], based on the methods of complex interpolation [6] and generalized Rényi entropies [7, 59]. The main result of [71] states that a lower bound on the decrease in relative entropy induced by a quantum channel is given by the negative logarithm of the fidelity between the first state and its recovered version, which is a step closer to the proof of the conjecture in (4). However, the recovery term in [71] is weaker than the right-hand side of (4), and the map appearing in it lacks one of the two properties that it is required to obey. Another step toward the proof of the conjecture in (4) was performed in [27], where a more general tool from complex analysis [25] and the methods of [7, 59, 71] were exploited in order to prove a statement similar to (4), with the relative entropy on the right-hand side substituted by a negative log-fidelity, but with the recovery map depending only on σ and $\mathcal{N}$ and furthermore satisfying $\mathcal{R}_{\sigma,\mathcal{N}}(\mathcal{N}(\sigma)) = \sigma$. Meanwhile, a different proof approach based on pinching was delivered in [63], and then a systematic method for deriving matrix inequalities by forcing the operators to commute via the application of suitably chosen "pinching maps" was proposed in [61]. This method as well as the complex interpolation techniques in [16] can be also applied to prove multioperator trace inequalities [16, 61, 72], which generalise the celebrated Golden-Thompson inequality $\mathrm{Tr}[e^{X+Y}] \leq \mathrm{Tr}[e^X e^Y]$ (X, Y hermitian) and the stronger statements given in [34]. The results of [61] also marked further progress toward establishing the conjecture in (4).

1.2 Introduction to quantum Gaussian states and channels

A major platform for the application of quantum information theory to physical information processing is constituted by quantum optics [20] with a finite number of electromagnetic modes or quantum harmonic oscillators. From the mathematical perspective, this framework can be thought of as quantum mechanics applied to separable Hilbert spaces endowed with a finite number of operators obeying canonical commutation relations [58].

A typical free Hamiltonian of such a system is quadratic in the canonical operators, and in fact, a special role within this context is played by ground or thermal states of such Hamiltonians, commonly called *Gaussian states*. These states define a useful operational framework for several reasons, stemming from both physics and mathematics [1, 58]. From the physical point of view, they are easily produced and manipulated in the laboratory and

can be used to implement effective quantum protocols [4, 69]. Mathematically convenient properties that qualify them as defining a legitimate framework include

1. the closure under so-called Gaussian unitary evolutions, that is, unitaries induced by piecewise time evolution via quadratic Hamiltonians, as well as more generally
2. the closure under Gaussian channels, which can be understood as the operation of adding an ancillary system in a vacuum state, applying a global Gaussian unitary, and tracing out one of the subsystems [12].

Recently, more advanced "closure" properties have been established, such as the optimality of Gaussian states for optimising the output entropy of one-mode, phase-covariant quantum channels, even when a fixed value of the input entropy is prescribed [23, 48, 46, 47]. These facts have the striking implication that it suffices to select coding strategies according to Gaussian states in order to achieve optimal rates in several quantum communication tasks [22, 73, 21, 54, 74, 47].

1.3 Summary of main result

The main contribution of our paper is a proof that Gaussian states and channels possess another closure property: the Petz recovery map associated to a Gaussian state σ and a Gaussian channel $\mathcal{N}$ is itself a Gaussian channel (see Theorem 1). Additionally, we achieve this result through an explicit construction of the action of such a Gaussian Petz channel, which lends itself to multiple applications. For instance, with the formulas we provide, it is possible to construct a counterexample to the inequality in (4), in which all the states and channels involved are Gaussian and $\mathcal{R}_{\sigma,\mathcal{N}}$ is the Petz recovery map. This is similar to what happens in the finite-dimensional case. Another application of our main result is a more explicit form for an entropy inequality from [27], whenever the states and channel involved are Gaussian.

This paper is structured as follows. In Section 2, we review some background material and establish notation. In particular, we review the Petz recovery map (Section 2.1) and bosonic Gaussian states and channels (Section 2.2). In Section 3, we state our main result, Theorem 1, which establishes that the Petz recovery map for a Gaussian state σ and a Gaussian channel $\mathcal{N}$ is itself a Gaussian channel, and we give an explicit form for it in terms of the parameters that characterize σ and $\mathcal{N}$. Corollary 2 establishes a similar result for the rotated Petz maps from [71]. For our detailed proof of Theorem 1, we refer to [30, Sections 3.1–3.4]. We conclude in Section 4 with a summary and some open questions.

2 Background and notation

2.1 Petz recovery map

As discussed in Section 1.1, the Petz recovery map is a notable object playing a crucial role in the theory of quantum recoverability. It has been interpreted in [31] as a quantum generalization of the Bayes rule from probability theory. Given a state σ and a channel $\mathcal{N}$, the associated Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$ is defined as a linear map satisfying the following [50, 51, 44]:

$$\langle A, \mathcal{N}^\dagger(B)\rangle_\sigma = \langle \mathcal{P}^\dagger_{\sigma,\mathcal{N}}(A), B\rangle_{\mathcal{N}(\sigma)}, \quad \forall A, B, \tag{6}$$

where A and B are bounded operators and the weighted Hilbert–Schmidt inner product is defined for bounded operators τ_1 and τ_2 and a trace-class operator ξ as

$$\langle \tau_1, \tau_2\rangle_\xi \equiv \mathrm{Tr}[\tau_1^\dagger \xi^{1/2} \tau_2 \xi^{1/2}]. \tag{7}$$

The map $\mathcal{P}_{\sigma,\mathcal{N}}$ is unique if $\mathcal{N}(\sigma)$ is a faithful operator [50, 51, 44], and otherwise, it is unique on the support of this operator. If σ acts on a finite-dimensional Hilbert space and $\mathcal{N}$ is a quantum channel with finite-dimensional inputs and outputs, then the Petz map takes the following explicit form [24]:

$$\mathcal{P}_{\sigma,\mathcal{N}}(\omega) \equiv \sigma^{1/2}\mathcal{N}^{\dagger}\left(\mathcal{N}(\sigma)^{-1/2}\omega\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2}, \tag{8}$$

where $\mathcal{N}(\sigma)^{-1/2}$ is understood as a generalized inverse (i.e., inverse on the support of $\mathcal{N}(\sigma)$). Sometimes we the dependence of $\mathcal{P}$ on σ and $\mathcal{N}$ for the sake of simplicity. A rotated Petz map $\mathcal{P}^t_{\sigma,\mathcal{N}}$ for $t \in \mathbb{R}$, a state σ, and a channel $\mathcal{N}$ is defined as [71]

$$\mathcal{P}^t_{\sigma,\mathcal{N}}(\omega) \equiv \sigma^{it}\mathcal{P}_{\sigma,\mathcal{N}}(\mathcal{N}(\sigma)^{-it}\omega\mathcal{N}(\sigma)^{it})\sigma^{-it}, \tag{9}$$

with $\sigma^{it} = \exp(it\log\sigma)$ being understood as a unitary evolution according to the Hamiltonian $\log\sigma$.

2.2 Quantum Gaussian states and channels

Here we provide some background on quantum Gaussian states and channels (see [12, 1, 58] for reviews). An n-mode quantum system is described by a density operator acting on a tensor-product Hilbert space. To the jth Hilbert space in the tensor product, for $j \in \{1,\ldots,n\}$, we let x_j and p_j denote the position- and momentum-quadrature operator, respectively. These operators satisfy the canonical commutation relations: $[x_j, p_k] = i\delta_{j,k}$, where we have set $\hbar = 1$. It is convenient to form a vector $r = (x_1,\ldots,x_n,p_1,\ldots,p_n)^T$ from these operators, and then we can rewrite the canonical commutation relations in matrix form as follows:

$$[r, r^T] = i\Omega, \tag{10}$$

where

$$\Omega \equiv \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes I_n, \tag{11}$$

and I_n denotes the $n \times n$ identity matrix. We often make use of the identities $\Omega^T\Omega = I$ and $\Omega^T = -\Omega$.

The displacement (Weyl) operator D_z plays an important role in Gaussian quantum information, defined for $z \in \mathbb{R}^{2n}$ as

$$D_z \equiv \exp(iz^T\Omega r). \tag{12}$$

For $z_1, z_2 \in \mathbb{R}^{2n}$, the displacement operators satisfy the following composition rule:

$$D_{z_1}D_{z_2} = D_{z_1+z_2}e^{-\frac{i}{2}z_1^T\Omega z_2}. \tag{13}$$

It can be shown that displacement operators form a complete, orthogonal set of operators, and their Hilbert–Schmidt orthogonality relation is as follows:

$$\mathrm{Tr}[D_{z_1}D_{-z_2}] = (2\pi)^n\delta(z_1 - z_2). \tag{14}$$

Moreover, due to their completeness, these operators allow for a Fourier-Weyl expansion of a quantum state, in terms of a characteristic function. In more detail, a quantum state ρ has a characteristic function $\chi_\rho(w)$, defined as

$$\chi_\rho(w) \equiv \mathrm{Tr}[\rho D_{-w}], \tag{15}$$

and the original state ρ can be written in terms of $\chi_\rho(w)$ as

$$\rho = \int \frac{d^{2n}w}{(2\pi)^n}\ \chi_\rho(w)\ D_w. \tag{16}$$

The mean vector $s_\rho \in \mathbb{R}^{2n}$ and $2n \times 2n$ covariance matrix V_ρ of a quantum state ρ are defined as

$$s_\rho \equiv \langle r \rangle_\rho = \mathrm{Tr}[r\rho], \tag{17}$$

$$V_\rho \equiv \langle \{r - s_\rho, r^T - s_\rho^T\} \rangle_\rho = \mathrm{Tr}[\{r - s_\rho, r^T - s_\rho^T\}\rho]. \tag{18}$$

It follows from the above definition that the covariance matrix V_ρ is symmetric.

A quantum Gaussian state is a ground or thermal state of a Hamiltonian that is quadratic in the position- and momentum-quadrature operators. In particular, up to an irrelevant additive constant, any such Hamiltonian has the form $\frac{1}{2}\,(r-s)^T\,H\,(r-s)$, where $s \in \mathbb{R}^{2n}$ and H is a $2n \times 2n$ positive definite matrix that we refer to as the Hamiltonian matrix. Then a quantum Gaussian state ρ takes the form

$$\rho = Z_\rho^{-1} \exp\left(-\frac{1}{2}(r - s_\rho)^T H_\rho (r - s_\rho)\right), \tag{19}$$

where $Z_\rho \equiv \mathrm{Tr}\big[\exp\big(-\frac{1}{2}(r - s_\rho)^T H_\rho (r - s_\rho)\big)\big]$ and one can show that $\langle r \rangle_\rho = s_\rho \in \mathbb{R}^{2n}$ (i.e., s_ρ is the mean vector of ρ). Defining

$$V_\rho \equiv \coth\left(\frac{i\Omega H_\rho}{2}\right) i\Omega, \tag{20}$$

one can also show that V_ρ is the covariance matrix of ρ, whose matrix elements satisfy $V_\rho^{j,k} = \langle \{r_j - s_\rho^j, r_k - s_\rho^k\} \rangle_\rho$ and the Heisenberg uncertainty relation [60]:

$$V_\rho + i\Omega \geq 0. \tag{21}$$

A quantum Gaussian state is faithful (having full support) if $V_\rho + i\Omega > 0$.

A quantum Gaussian state ρ with mean vector s_ρ and covariance matrix V_ρ has the following Gaussian characteristic function:

$$\chi_\rho(w) = \exp\left(-\frac{1}{4}\,(\Omega w)^T\,V_\rho \Omega w + i\,(\Omega w)^T\,s_\rho\right), \tag{22}$$

so that it can be written in the following way:

$$\rho = \int \frac{d^{2n}w}{(2\pi)^n}\ \exp\left(-\frac{1}{4}\,(\Omega w)^T\,V_\rho \Omega w + i\,(\Omega w)^T\,s_\rho\right) D_w. \tag{23}$$

After a change of variables ($w \to \Omega w$), this representation becomes

$$\rho = \int \frac{d^{2n}w}{(2\pi)^n}\ \exp\left(-\frac{1}{4} w^T V_\rho w - i w^T s_\rho\right) D_{\Omega w}. \tag{24}$$

A quantum Gaussian channel is a completely positive, trace-preserving map that takes Gaussian input states to Gaussian output states. A quantum Gaussian channel $\mathcal{N}$ that takes n-mode Gaussian input states to m-mode Gaussian output states is specified by a $2m \times 2n$ transformation matrix X, a $2m \times 2m$ positive semi-definite, additive noise matrix Y, and a displacement vector $\delta \in \mathbb{R}^{2n}$. The action of such a channel on a generic state ρ with

characteristic function $\chi_\rho(w)$ is to output a state $\mathcal{N}(\rho)$ having the following characteristic function:

$$\chi_{\mathcal{N}(\rho)}(w) = \chi_\rho(\Omega^T X^T \Omega w) \exp\left(-\frac{1}{4}\left(\Omega w\right)^T Y \Omega w + i\left(\Omega w\right)^T \delta\right). \tag{25}$$

Then the channel $\mathcal{N}$ leads to the following transformation of the covariance matrix V and mean vector s of an input quantum Gaussian state:

$$\mathcal{N}: \left\{ \begin{array}{lcl} V & \longmapsto & XVX^T + Y \\ s & \longmapsto & Xs + \delta \end{array} \right. . \tag{26}$$

The matrices X and Y should satisfy the following condition in order for the map $\mathcal{N}$ to be completely positive:

$$Y + i\Omega \geq iX\Omega X^T. \tag{27}$$

The adjoint of a quantum channel $\mathcal{N}$ is defined as the unique linear map satisfying the following for all A and B:

$$\langle A, \mathcal{N}(B)\rangle = \langle \mathcal{N}^\dagger(A), B\rangle, \tag{28}$$

where B is an arbitrary trace-class operator, A is an arbitrary bounded operator, and the Hilbert–Schmidt inner product is defined for operators A_1 and A_2 as $\langle A_1, A_2\rangle \equiv \mathrm{Tr}[A_1^\dagger A_2]$. The adjoint map $\mathcal{N}^\dagger$ is completely positive and unital if $\mathcal{N}$ is completely positive and trace-preserving. The action of the adjoint $\mathcal{N}^\dagger$ of a quantum Gaussian channel $\mathcal{N}$ defined by (26) is as follows [12, 19], when acting on a displacement operator $D_{\Omega z}$:

$$\mathcal{N}^\dagger(D_{\Omega z}) = D_{\Omega X^T z} \exp\left(-\frac{1}{4} z^T Y z + i z^T \delta\right). \tag{29}$$

The action of the adjoint $\mathcal{N}^\dagger$ on a quantum Gaussian state with covariance matrix V and mean vector s is then to output a quantum Gaussian operator described by covariance matrix $X^{-1}\left(V+Y\right)X^{-T}$ and mean vector $X^{-1}(s-\delta)$ whenever X is invertible [19, Appendix B]. We summarize these transformation rules as follows:

$$\mathcal{N}^\dagger: \left\{ \begin{array}{lcl} V & \longmapsto & X^{-1}\left(V+Y\right)X^{-T} \\ s & \longmapsto & X^{-1}(s-\delta) \end{array} \right. . \tag{30}$$

Typically one thinks of the channel $\mathcal{N}$ as acting in the Schrödinger picture, taking input states to output states, and one thinks of the adjoint $\mathcal{N}^\dagger$ as acting in the Heisenberg picture, taking input bounded operators to output bounded operators. So this is why we have specified the channel $\mathcal{N}$ in terms of its action on characteristic functions, which describe states, and the adjoint $\mathcal{N}^\dagger$ in terms of its action on displacement operators, a natural choice of bounded operators in our context here.

Often we find it useful to write

$$\sigma = D_{s_\sigma}^\dagger \sigma_0 D_{s_\sigma}, \tag{31}$$

where σ_0 is a Gaussian state with the same covariance matrix as σ but with vanishing mean vector. Analogously, the channel $\mathcal{N}$ in (25) admits the following decomposition:

$$\mathcal{N}(\cdot) = D_\delta^\dagger \mathcal{N}_0(\cdot) D_\delta, \tag{32}$$

where $\mathcal{N}_0$ is a zero-displacement Gaussian channel, acting as in (26) but with $\delta = 0$. Taking the adjoint gives

$$\mathcal{N}^\dagger(\cdot) = \mathcal{N}_0^\dagger\left(D_\delta(\cdot)D_\delta^\dagger\right). \tag{33}$$

Applying $\mathcal{N}$ to σ yields

$$\mathcal{N}(\sigma) = D_{Xs+\delta}^\dagger \mathcal{N}_0(\sigma_0) D_{Xs+\delta}, \tag{34}$$

which follows from (26). We also make use of the following channel covariance relations:

$$\mathcal{N}(D_\gamma^\dagger(\cdot)D_\gamma) = D_{X\gamma+\delta}^\dagger \mathcal{N}_0(\cdot) D_{X\gamma+\delta}, \tag{35}$$

$$\mathcal{N}^\dagger(D_\gamma^\dagger(\cdot)D_\gamma) = D_{X^{-1}(\gamma-\delta)}^\dagger \mathcal{N}_0^\dagger(\cdot) D_{X^{-1}(\gamma-\delta)}, \tag{36}$$

which follow from (25), (26), (29), and (30). Note that (36) holds whenever X is invertible.

Finally, given a Gaussian state σ with mean vector s_σ and covariance matrix V_σ, we can consider a unitary rotation of the form $\sigma^{it} = \exp(it\log\sigma)$ for $t \in \mathbb{R}$. By using the representation in (19) with the Hamiltonian matrix H_σ, we can write the unitary σ^{it} as

$$\sigma^{it} = \exp\left(-\frac{i}{2}\left(r - s_\sigma\right)^T H_\sigma t \left(r - s_\sigma\right)\right) \exp(-it\log Z_\sigma) \tag{37}$$

$$= D_{-s_\sigma}\left[\exp\left(\frac{i}{2} r^T \left(-H_\sigma t\right) r\right) \exp(-it\log Z_\sigma)\right] D_{s_\sigma}, \tag{38}$$

where we have used the fact that $\left(r - s_\sigma\right)^T H_\sigma \left(r - s_\sigma\right) = D_{-s_\sigma} r^T H_\sigma r D_{s_\sigma}$ and the operator identity $B\exp(A)B^{-1} = \exp(BAB^{-1})$. The unitary σ^{it} is a Gaussian unitary because it is generated by a Hamiltonian no more than quadratic in the position- and momentum-quadrature operators. Let us define the symplectic transformation corresponding to the unitary $\exp\left(\frac{i}{2} r^T \left(-H_\sigma t\right) r\right)$ as

$$S_{\sigma,t} \equiv \exp(\Omega H_\sigma t), \tag{39}$$

so that

$$\sigma^{it} r \sigma^{-it} = S_{\sigma,-t}\left(r - s_\sigma\right) + s_\sigma, \tag{40}$$

where we used that $D_{s_\sigma} r D_{-s_\sigma} = r + s_\sigma$. The above formula implies that

$$V_{\sigma^{it}\omega\sigma^{-it}} = S_{\sigma,t} V_\omega S_{\sigma,t}^T, \tag{41}$$

$$s_{\sigma^{it}\omega\sigma^{-it}} = S_{\sigma,t}(s_\rho - s_\sigma) + s_\sigma. \tag{42}$$

3 Main result: Petz map as a quantum Gaussian channel

Our main result is the following theorem:

▶ **Theorem 1.** *Let σ be a quantum Gaussian state with mean vector s_σ and covariance matrix V_σ, and let $\mathcal{N}$ be a quantum Gaussian channel with its action on an input state as described in* (26)*. Suppose furthermore that $\mathcal{N}(\sigma)$ is a faithful quantum state. Then the Petz recovery map $\mathcal{P}_{\sigma,\mathcal{N}}$ is a quantum Gaussian channel with the following action:*

$$\mathcal{P}_{\sigma,\mathcal{N}} : \left\{ \begin{array}{lcl} V & \longmapsto & X_P V X_P^T + Y_P \\ s & \longmapsto & X_P s + \delta_P \end{array} \right. , \tag{43}$$

where

$$X_P \equiv \sqrt{I + (V_\sigma \Omega)^{-2}} V_\sigma X^T \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}}^{-1} V_{\mathcal{N}(\sigma)}^{-1}, \tag{44}$$

$$Y_P \equiv V_\sigma - X_P V_{\mathcal{N}(\sigma)} X_P^T, \tag{45}$$

$$\delta_P \equiv s_\sigma - X_P \left(X s_\sigma + \delta\right), \tag{46}$$

$$V_{\mathcal{N}(\sigma)} = X V_\sigma X^T + Y. \tag{47}$$

That is, $\mathcal{P}_{\sigma,\mathcal{N}}$ in (43) *is the unique linear map satisfying* (6) *for σ and $\mathcal{N}$ as described above.*

The following corollary is a direct consequence of Theorem 1 and the discussion surrounding (37)–(40):

▶ **Corollary 2.** *For σ and $\mathcal{N}$ as given in Theorem 1, the rotated Petz map $\mathcal{P}^t_{\sigma,\mathcal{N}}$ (defined in* (9)*) is also a quantum Gaussian channel with the same action as the Petz recovery channel $\mathcal{P}_{\sigma,\mathcal{N}}$ but with the substitutions*

$$X_P \to X_P^t \equiv S_{\sigma,t} X_P S_{\mathcal{N}(\sigma),-t}, \tag{48}$$

$$Y_P \to Y_P^t \equiv S_{\sigma,t} Y_P S_{\sigma,t}^T, \tag{49}$$

$$\delta_P \to \delta_P^t \equiv s_\sigma - X_P^t \left(X s_\sigma + \delta\right). \tag{50}$$

That is, $\mathcal{P}^t_{\sigma,\mathcal{N}}$ is a quantum Gaussian channel with the following action:

$$\mathcal{P}^t_{\sigma,\mathcal{N}} : \begin{cases} V & \longmapsto & X_P^t V (X_P^t)^T + Y_P^t \\ s & \longmapsto & X_P^t s + \delta_P^t \end{cases}. \tag{51}$$

▶ Remark. The following entropy inequality was proven to hold whenever ρ and σ are density operators and $\mathcal{N}$ is a quantum channel [27]:

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) - \int_{\mathbb{R}} dt\; p(t) \log F(\rho, (\mathcal{P}^{t/2}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho)), \tag{52}$$

where $p(t) := \frac{\pi}{2}(\cosh(\pi t) + 1)^{-1}$ is a probability distribution parametrized by $t \in \mathbb{R}$. In the case that ρ and σ are quantum Gaussian states and $\mathcal{N}$ is a quantum Gaussian channel, Corollary 2 allows us to conclude that $\mathcal{P}^{t/2}_{\sigma,\mathcal{N}}$ is a quantum Gaussian channel for all $t \in \mathbb{R}$. Furthermore, there are explicit, compact formulas for the relative entropy [57, 13, 53] and fidelity [49, 70, 5] of two quantum Gaussian states. In both cases, the formulas are given exclusively in terms of the mean vectors and covariance matrices of the involved states. Thus, when the states and channel involved are all Gaussian, the above inequality can be rewritten in a simpler form involving only finite-dimensional matrices instead of trace-class operators acting on infinite-dimensional Hilbert spaces.

The forthcoming subsections sketch the first steps of our proof of Theorem 1, and a detailed, complete proof can be found in [30]. Before delving into our proof, we highlight our proof strategy, which proceeds according to the following steps:

1. *Even though the explicit form of the Petz map in* (8) *is not generally valid in the infinite-dimensional case because the inverse of a density operator may be unbounded, we work with it anyway, as an ansatz* (call this **Ansatz 1**). Under Ansatz 1, we first show that it suffices to consider the case when the state σ is a zero-mean Gaussian state and the channel $\mathcal{N}$ does not apply any displacement to the mean vector of its input, so that $s_\sigma = 0$ and $\delta = 0$, with δ defined in (25) and (26).

2. Under the same Ansatz 1, we arrive at the hypothesis that (43) gives the explicit form for the action of the Petz map on a Gaussian input state. Recall from (8) that the Petz map is a serial concatenation of three completely positive maps:

$$(\cdot) \to \mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2}, \tag{53}$$
$$(\cdot) \to \mathcal{N}^{\dagger}(\cdot), \tag{54}$$
$$(\cdot) \to \sigma^{1/2}(\cdot)\sigma^{1/2}. \tag{55}$$

To handle the first completely positive map in (53), we proceed with an additional ansatz (**Ansatz 2**) *that taking the inverse of a Gaussian state corresponds to negating its covariance matrix.* This is motivated by the representation in (19), in which inverting the density operator has the effect of negating the Hamiltonian matrix, which in turn has the effect of negating the covariance matrix due to the fact that arcoth is an odd function. Furthermore, results of [5, Appendix B-2] allow us to conclude that sandwiching a Gaussian state by the square root of another Gaussian state is a Gaussian map resulting in another unnormalized, Gaussian state. To handle the second map in (54), we can directly apply a result given in [19, Appendix B], which gives an explicit form for the action of the adjoint of a Gaussian channel on a Gaussian state (see also the review in (30)). We also work with a final **Ansatz 3**, *which is the assumption that the matrix X in* (26) *is invertible.* Later, we show how this assumption is not necessary. To handle the third completely positive map in (55), we again apply the aforementioned result about sandwiching a Gaussian state by the square root of another.

3. After arriving at an explicit form for the Petz map by using Ansatzes 1–3, we verify that this explicit form satisfies the equations in (6) whenever the operators A and B are Hilbert–Schmidt operators.

4. We finally employ a limiting argument to conclude that if (6) is satisfied when A and B are Hilbert–Schmidt operators, then the equations are satisfied when A and B are arbitrary bounded operators. By a result of [50, 51, 44], we can finally conclude that the Gaussian channel given in Theorem 1 is the unique quantum channel satisfying (6). This step then concludes our proof of Theorem 1.

In the subsections that follow, we provide details of the first two steps above, and we refer to [30] for the rest of the steps of our proof of Theorem 1.

3.1 Step 1: Sufficiency of focusing on zero-mean Gaussian states and zero-displacement Gaussian channels

As mentioned above, we employ Ansatz 1 in this first step, in which we work with the explicit form of the Petz map in (8), in spite of the fact that the inverse of a Gaussian density operator is unbounded. Let σ be a quantum Gaussian state with mean vector s_σ and covariance matrix V_σ, and let $\mathcal{N}$ be a quantum Gaussian channel with the action on an input state as described in (26).

In this first step, we show how it suffices to consider the case $s_\sigma = \delta = 0$ in (8). To see this, consider the action of the Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$ on an arbitrary input state ω:

$$\begin{aligned}
\mathcal{P}_{\sigma,\mathcal{N}}(\omega) &= \sigma^{1/2}\mathcal{N}^\dagger\left(\mathcal{N}(\sigma)^{-1/2}\omega\mathcal{N}(\sigma)^{-1/2}\right)\sigma^{1/2} && (56)\\
&= \left(D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma}\right)\mathcal{N}_0^\dagger\left[D_\delta D^\dagger_{Xs_\sigma+\delta}\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma+\delta}\,\omega\,D^\dagger_{Xs_\sigma+\delta}\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma+\delta}D^\dagger_\delta\right]\\
&\quad\times\left(D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma}\right) && (57)\\
&= \left(D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma}\right)\mathcal{N}_0^\dagger\left[D^\dagger_{Xs_\sigma}\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma+\delta}\,\omega\,D^\dagger_{Xs_\sigma+\delta}\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma}\right]\\
&\quad\times\left(D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma}\right) && (58)\\
&= D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma}D^\dagger_{X^{-1}(Xs_\sigma)}\mathcal{N}_0^\dagger\left[\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma+\delta}\,\omega\,D^\dagger_{Xs_\sigma+\delta}\mathcal{N}_0(\sigma_0)^{-1/2}\right]\\
&\quad\times D_{X^{-1}(Xs_\sigma)}D^\dagger_{s_\sigma}\sigma_0^{1/2}D_{s_\sigma} && (59)\\
&= D^\dagger_{s_\sigma}\sigma_0^{1/2}\mathcal{N}_0^\dagger\left[\mathcal{N}_0(\sigma_0)^{-1/2}D_{Xs_\sigma+\delta}\,\omega\,D^\dagger_{Xs_\sigma+\delta}\mathcal{N}_0(\sigma_0)^{-1/2}\right]\sigma_0^{1/2}D_{s_\sigma} && (60)\\
&= D^\dagger_{s_\sigma}\;\mathcal{P}_{\sigma_0,\mathcal{N}_0}\left(D_{Xs_\sigma+\delta}\,\omega\,D^\dagger_{Xs_\sigma+\delta}\right)\;D_{s_\sigma}\,. && (61)
\end{aligned}$$

For the first equality, we use the definition of the Petz map and Ansatz 1. The second equality follows from (31)–(34) and the fact that $f(UAU^\dagger) = Uf(A)U^\dagger$ for a function f, a unitary operator U, and a Hermitian operator A. The third equality follows because $D_\delta D^\dagger_{Xs_\sigma+\delta} = D^\dagger_{Xs_\sigma}e^{i\phi}$ for ϕ a phase. The fourth equality follows from the adjoint channel covariance relation in (36) and Ansatz 3. The fifth equality follows because $D_{s_\sigma}D^\dagger_{X^{-1}(Xs_\sigma)} = e^{i\varphi}I$ for some phase φ. The final equality follows by recognizing the form of the Petz map $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$, corresponding to the zero-mean state σ_0 and the zero-displacement channel $\mathcal{N}_0$.

The above reasoning suggests that we should focus on determining an explicit form for $\mathcal{P}_{\sigma_0,\mathcal{N}_0}(\omega)$. That is, the above reasoning suggests that an arbitrary Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$ can be realized as a serial concatenation of the displacement $D_{Xs_\sigma+\delta}$, the Petz map $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$, and the displacement $D^\dagger_{s_\sigma}$. After we give an explicit form for $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$ as a quantum Gaussian channel with matrices X_P and Y_P, it should become clear why the displacement δ_P in the Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$ has the form in (46).

3.2 Step 2: Deducing a hypothesis for an explicit form for the Petz map, by considering Gaussian input states

In this step, we continue working with Ansatzes 1-3, with our main objective being to arrive at a hypothesis for the action of the Petz recovery map $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$ on the mean vector and covariance matrix of an input Gaussian state. Here we consider the serial concatenation of the three completely positive maps in (53)–(55). We begin by considering the action of the last completely positive map on a zero-mean Gaussian input state ω_0. To this end, recall from [5, Appendix C] that if ω_0 and σ_0 are zero-mean Gaussian states, then $\sqrt{\sigma_0}\omega_0\sqrt{\sigma_0}$ is an (unnormalized) Gaussian operator with zero mean vector and covariance matrix given by

$$V_{\sqrt{\sigma_0}\omega_0\sqrt{\sigma_0}} = V_{\sigma_0} - \left(V_{\sqrt{\sigma_0}} - V_{\sigma_0}\right)\left(V_{\omega_0} + V_{\sigma_0}\right)^{-1}\left(V_{\sqrt{\sigma_0}} - V_{\sigma_0}\right). \tag{62}$$

Applying a formula from [5, Appendix B-2] (while noting our different convention for Gaussian states), we find that

$$V_{\sqrt{\sigma_0}} = \left(\sqrt{I + (V_{\sigma_0}\Omega)^{-2}} + I\right)V_{\sigma_0}\,, \tag{63}$$

which is a symmetric matrix because V_{σ_0} is. Indeed, consider that

$$V_{\sqrt{\sigma_0}}^T = \left[\left(\sqrt{I + (V_{\sigma_0}\Omega)^{-2}} + I\right) V_{\sigma_0}\right]^T = V_{\sigma_0}\left(\sqrt{I + (\Omega V_{\sigma_0})^{-2}} + I\right) \tag{64}$$

$$= \Omega^{-1}\Omega V_{\sigma_0}\left(\sqrt{I + (\Omega V_{\sigma_0})^{-2}} + I\right) = \Omega^{-1}\left(\sqrt{I + (\Omega V_{\sigma_0})^{-2}} + I\right)\Omega V_{\sigma_0} \tag{65}$$

$$= \left(\sqrt{\Omega^{-1}\left[I + (\Omega V_{\sigma_0})^{-2}\right]\Omega} + I\right) V_{\sigma_0} = \left(\sqrt{\left[I + (\Omega^{-1}\Omega V_{\sigma_0}\Omega)^{-2}\right]} + I\right) V_{\sigma_0} \tag{66}$$

$$= \left(\sqrt{I + (V_{\sigma_0}\Omega)^{-2}} + I\right) V_{\sigma_0} = V_{\sqrt{\sigma_0}}. \tag{67}$$

The equality in (63) implies that

$$V_{\sqrt{\sigma_0}} - V_{\sigma_0} = \sqrt{I + (V_{\sigma_0}\Omega)^{-2}} V_{\sigma_0}, \tag{68}$$

and in turn, after substituting into (62), that

$$V_{\sqrt{\sigma_0}\omega_0\sqrt{\sigma_0}} = V_{\sigma_0} - \sqrt{I + (V_{\sigma_0}\Omega)^{-2}} V_{\sigma_0}\left(V_{\omega_0} + V_{\sigma_0}\right)^{-1} V_{\sigma_0}\sqrt{I + (\Omega V_{\sigma_0})^{-2}}. \tag{69}$$

Thus, (69) establishes the action of the completely positive map $(\cdot) \to \sqrt{\sigma_0}(\cdot)\sqrt{\sigma_0}$ on an arbitrary zero-mean Gaussian state ω_0.

From this discussion we already start seeing that the Petz map constructed out of a Gaussian state σ and a Gaussian channel $\mathcal{N}$ should send normalized Gaussian states to normalized Gaussian states, because (i) conjugation by the square root of a Gaussian state (or the inverse square root of a Gaussian state as we will see) preserves the Gaussian form; (ii) the adjoint of a Gaussian channel is still Gaussian; and (iii) the Petz map is a priori known to be trace-preserving whenever $\mathcal{N}(\sigma)$ is a faithful state [50, 51, 44]. Then, [45, Theorem III.1] ensures that $\mathcal{P}$ must act as in (26), for some X_P, Y_P, and δ_P to be determined.

With this preliminary identity in hand, we are ready to determine a hypothesis for the explicit action of $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$. For the sake of simplicity, we consider the input Gaussian state to have vanishing first moments. In any case, since we are working to deduce a hypothesis for an explicit form for the Petz map, this is by no means a loss of generality. By applying (69) and Ansatz 2 (that the following density operator transformation $\omega \to \omega^{-1}$ induces the transformation $V_\omega \to -V_\omega$ on the level of covariance matrices), we can conclude that the completely positive map in (53) has the following effect on covariance matrices:

$$V_{\sqrt{\mathcal{N}_0(\sigma_0)}^{-1}\omega_0\sqrt{\mathcal{N}_0(\sigma_0)}^{-1}}$$
$$= -V_{\mathcal{N}(\sigma)} - \sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)}\left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)}\sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}}. \tag{70}$$

In the above, we have also used the identities $V_{\mathcal{N}_0(\sigma_0)} = V_{\mathcal{N}(\sigma)}$ and $V_{\omega_0} = V_\omega$. So now we consider further concatenating with the completely positive map in (54), by applying (30) and Ansatz 3 (that X is invertible):

$$V_{\mathcal{N}_0^\dagger(\sqrt{\mathcal{N}_0(\sigma_0)}^{-1}\omega_0\sqrt{\mathcal{N}_0(\sigma_0)}^{-1})} =$$
$$X^{-1}\left[-V_{\mathcal{N}(\sigma)} - \sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)}\left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)}\sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}} + Y\right] X^{-T}. \tag{71}$$

But consider that $V_{\mathcal{N}(\sigma)} = XV_\sigma X^T + Y$, so that (71) simplifies as follows:

$$
\begin{aligned}
&V_{\mathcal{N}_0^\dagger(\sqrt{\mathcal{N}_0(\sigma_0)}^{-1}\omega_0\sqrt{\mathcal{N}_0(\sigma_0)}^{-1})} \\
&= X^{-1}\Bigg[-\left(XV_\sigma X^T + Y\right) \\
&\quad - \sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)} \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}} + Y\Bigg] X^{-T} \\
&= X^{-1}\left[-XV_\sigma X^T - \sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)} \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}}\right] X^{-T} \qquad (72) \\
&= -V_\sigma - X^{-1}\sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)} \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}} X^{-T}. \qquad (73)
\end{aligned}
$$

So then we can finally consider the serial concatenation of the three completely positive maps in (53)–(55):

$$
\begin{aligned}
&V_{\sqrt{\sigma_0}\mathcal{N}_0^\dagger(\sqrt{\mathcal{N}_0(\sigma_0)}^{-1}\omega_0\sqrt{\mathcal{N}_0(\sigma_0)}^{-1})\sqrt{\sigma_0}} \\
&= V_\sigma - \sqrt{I + (V_\sigma\Omega)^{-2}} V_\sigma \\
&\quad \times \left(-V_\sigma - X^{-1}\sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)} \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}} X^{-T} + V_\sigma\right)^{-1} \\
&\quad \times V_\sigma \sqrt{I + (\Omega V_\sigma)^{-2}} \qquad (74)
\end{aligned}
$$

$$
\begin{aligned}
&= V_\sigma - \sqrt{I + (V_\sigma\Omega)^{-2}} V_\sigma \\
&\quad \times \left(-X^{-1}\sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}} V_{\mathcal{N}(\sigma)} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right)^{-1} V_{\mathcal{N}(\sigma)} \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}} X^{-T}\right)^{-1} \\
&\quad \times V_\sigma \sqrt{I + (\Omega V_\sigma)^{-2}} \qquad (75) \\
&= V_\sigma + \sqrt{I + (V_\sigma\Omega)^{-2}} V_\sigma X^T \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}}^{-1} V_{\mathcal{N}(\sigma)}^{-1} \left(V_\omega - V_{\mathcal{N}(\sigma)}\right) \\
&\quad \times V_{\mathcal{N}(\sigma)}^{-1} \sqrt{I + \left(V_{\mathcal{N}(\sigma)}\Omega\right)^{-2}}^{-1} X V_\sigma \sqrt{I + (V_\sigma\Omega)^{-2}}. \qquad (76)
\end{aligned}
$$

An inspection of (76) above suggests that the Petz map $\mathcal{P}_{\sigma_0,\mathcal{N}_0}$ is a quantum Gaussian channel with the following action on an input covariance matrix V_ω:

$$
V_{\mathcal{P}_{\sigma_0,\mathcal{N}_0}(\omega_0)} = X_P V_\omega X_P^T + Y_P, \qquad (77)
$$

where

$$
\begin{aligned}
X_P &\equiv \sqrt{I + (V_\sigma\Omega)^{-2}} V_\sigma X^T \sqrt{I + \left(\Omega V_{\mathcal{N}(\sigma)}\right)^{-2}}^{-1} V_{\mathcal{N}(\sigma)}^{-1}, \qquad (78) \\
Y_P &\equiv V_\sigma - X_P V_{\mathcal{N}(\sigma)} X_P^T. \qquad (79)
\end{aligned}
$$

Combining with the development in Section 3.1, the results in (77), (61) and [45, Theorem III.1] imply that in general

$$
\mathcal{P}_{\sigma,\mathcal{N}} : \left\{ \begin{array}{ccc} V & \longmapsto & X_P V X_P^T + Y_P \\ s & \longmapsto & X_P s + \delta_P \end{array} \right. , \qquad (80)
$$

where

$$
\delta_P \equiv s_\sigma - X_P \left(X s_\sigma + \delta\right) , \qquad (81)
$$

and δ is the vector appearing in (26); it follows because

$$\mathcal{P}_{\sigma,\mathcal{N}}(\omega) = D^{\dagger}_{s_\sigma} \mathcal{P}_{\sigma_0,\mathcal{N}_0} \left(D_{X s_\sigma + \delta} \omega D^{\dagger}_{X s_\sigma + \delta} \right) D_{s_\sigma}, \tag{82}$$

which implies that

$$s_{\mathcal{P}_{\sigma,\mathcal{N}}(\omega)} = X_P (s_\omega - X s_\sigma - \delta) + s_\sigma. \tag{83}$$

So by using Ansatzes 1-3, we have arrived at our hypothesis (80) for the Gaussian form of the Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$. In [30], we give the final steps of the proof that the Gaussian channel specified in (80) is indeed equal to the Petz map $\mathcal{P}_{\sigma,\mathcal{N}}$.

4 Conclusion

The main result of this paper is Theorem 1, which establishes an explicit form for the Petz map as a bosonic Gaussian channel whenever the state σ and the channel $\mathcal{N}$ are bosonic Gaussian. Our proof approach is first to consider three ansatzes in order to arrive at a hypothesis for the Gaussian form of the Petz map. These ansatzes included 1) working with the form of the Petz map in (8) in spite of the fact that $[\mathcal{N}(\sigma)]^{-1}$ is an unbounded operator, 2) negating the covariance matrix of the Gaussian state σ if σ is inverted, and 3) assuming that the X matrix in (25), corresponding to a Gaussian channel, is invertible. After deducing a hypothesis for an explicit form, [30] proves that this hypothesis is in fact correct, by demonstrating that the Gaussian Petz channel satisfies the equations in [30, Equation 3.107] for all bounded operators A and B.

In future work, it would be interesting to determine whether the following inequality, considered in [7, 59], could be satisfied whenever all of the objects involved are Gaussian:

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) - \log F(\rho, (\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho)). \tag{84}$$

More generally, one could consider the various inequalities proposed in [8] for the Gaussian case.

Acknowledgements. We thank Gerardo Adesso, Prabha Mandayam, Alessio Serafini, Kaushik Seshadreesan, and Andreas Winter for discussions related to this paper. LL thanks Davide Orsucci for his contribution to the proof contained in [30, Section 3.4].

References

1 Gerardo Adesso, Sammy Ragy, and Antony R. Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Systems and Information Dynamics*, 21(01–02):1440001, June 2014. arXiv:1401.4679.

2 Alvaro M. Alhambra, Stephanie Wehner, Mark M. Wilde, and Mischa P. Woods. Work and reversibility in quantum thermodynamics, June 2015. arXiv:1506.08145.

3 Alvaro M. Alhambra and Mischa P. Woods. Dynamical maps, quantum detailed balance and Petz recovery map, September 2016. arXiv:1609.07496.

4 Hans-A. Bachor and Timothy C. Ralph. *A Guide to Experiments in Quantum Optics*. Wiley, second edition, March 2004.

5 Leonardo Banchi, Samuel L. Braunstein, and Stefano Pirandola. Quantum fidelity for arbitrary Gaussian states. *Physical Review Letters*, 115(26):260501, December 2015. arXiv:1507.01941. doi:10.1103/PhysRevLett.115.260501.

6 J. Bergh and Jorgen Löfström. *Interpolation Spaces*. Springer-Verlag Berlin Heidelberg, 1976.

7 Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. Rényi generalizations of the conditional quantum mutual information. *Journal of Mathematical Physics*, 56(2):022205, February 2015. arXiv:1403.6102.

8 Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde. Rényi generalizations of quantum information measures. *Physical Review A*, 91(2):022333, February 2015. arXiv:1502.07977. doi:10.1103/PhysRevA.91.022333.

9 Fernando G. S. L. Brandao, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750. doi:10.1007/s00220-011-1302-1.

10 Fernando G. S. L. Brandao, Aram W. Harrow, Jonathan Oppenheim, and Sergii Strelchuk. Quantum conditional mutual information, reconstructed states, and state redistribution. *Physical Review Letters*, 115(5):050501, July 2014. arXiv:1411.4921.

11 Francesco Buscemi, Siddhartha Das, and Mark M. Wilde. Approximate reversibility in the context of entropy gain, information gain, and complete positivity. *Physical Review A*, 93(6):062314, June 2016. arXiv:1601.01207. doi:10.1103/PhysRevA.93.062314.

12 Filippo Caruso, Jens Eisert, Vittorio Giovannetti, and Alexander S. Holevo. Multi-mode bosonic Gaussian channels. *New Journal of Physics*, 10:083030, August 2008. arXiv:0804.0511.

13 Xiao-yu Chen. Gaussian relative entropy of entanglement. *Physical Review A*, 71(6):062320, June 2005. arXiv:quant-ph/0402109. doi:10.1103/PhysRevA.71.062320.

14 Matthias Christandl and Andreas Winter. "Squashed entanglement" - an additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, March 2004. arXiv:quant-ph/0308088.

15 Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Physical Review Letters*, 100(23):230501, June 2008. doi:10.1103/PhysRevLett.100.230501.

16 Frederic Dupuis and Mark M. Wilde. Swiveled Rényi entropies. *Quantum Information Processing*, 15(3):1309–1345, March 2016. arXiv:1506.00981.

17 Edward G. Effros. A matrix convexity approach to some celebrated quantum inequalities. *Proceedings of the National Academy of Sciences of the United States of America*, 106(4):1006–1008, January 2009. arXiv:0802.1234.

18 Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. *Communications in Mathematical Physics*, 340(2):575–611, December 2015. arXiv:1410.0664.

19 Marco G. Genoni, Ludovico Lami, and Alessio Serafini. Conditional and unconditional Gaussian quantum dynamics. *Contemporary Physics*, 57(3):331–349, January 2016. arXiv:1607.02619. doi:10.1080/00107514.2015.1125624.

20 Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, November 2004.

21 Vittorio Giovannetti, Raul Garcia-Patron, Nicolas J. Cerf, and Alexander S. Holevo. Ultimate classical communication rates of quantum optical channels. *Nature Photonics*, 8:796–800, September 2014. arXiv:1312.6225.

22 Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Jeffrey H. Shapiro, and Horace P. Yuen. Classical capacity of the lossy bosonic channel: The exact solution. *Physical Review Letters*, 92(2):027902, January 2004. arXiv:quant-ph/0308012. doi:10.1103/PhysRevLett.92.027902.

23 Vittorio Giovannetti, Alexander S. Holevo, and Raul Garcia-Patron. A solution of Gaussian optimizer conjecture for quantum channels. *Communications in Mathematical Physics*, 334(3):1553–1571, March 2015. arXiv:1312.2251.

24 Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in Mathematical Physics*, 246(2):359–374, April 2003. arXiv:quant-ph/0304007.

25 Isidore Isaac Hirschman. A convexity theorem for certain groups of transformations. *Journal d'Analyse Mathématique*, 2(2):209–218, December 1952.

26 Oscar Lanford III and Derek W. Robinson. Mean entropy of states in quantum-statistical mechanics. *Journal of Mathematical Physics*, 9(7):1120–1125, July 1968.

27 Marius Junge, Renato Renner, David Sutter, Mark M. Wilde, and Andreas Winter. Universal recovery from a decrease of quantum relative entropy, September 2015. arXiv:1509.07127.

28 Isaac H. Kim. Operator extension of strong subadditivity of entropy. *Journal of Mathematical Physics*, 53(12):122204, December 2012. arXiv:1210.5190.

29 Isaac H. Kim. Application of conditional independence to gapped quantum many-body systems, 2013. http://www.physics.usyd.edu.au/quantum/Coogee2013.

30 Ludovico Lami, Siddhartha Das, and Mark M. Wilde. Approximate reversal of quantum Gaussian dynamics, 2017. arXiv:1702.04737.

31 Matthew S. Leifer and Robert W. Spekkens. Towards a formulation of quantum theory as a causally neutral theory of Bayesian inference. *Physical Review A*, 88(5):052130, November 2013. arXiv:1107.5849. doi:10.1103/PhysRevA.88.052130.

32 Marius Lemm and Mark M. Wilde. Information-theoretic limitations on approximate quantum cloning and broadcasting, August 2016. arXiv:1608.07569.

33 Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps, October 2014. arXiv:1410.4184.

34 Elliott H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Advances in Mathematics*, 11(3):267–288, December 1973.

35 Elliott H. Lieb and Mary Beth Ruskai. A fundamental property of quantum-mechanical entropy. *Physical Review Letters*, 30(10):434–436, March 1973.

36 Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *Journal of Mathematical Physics*, 14(12):1938–1941, December 1973.

37 Göran Lindblad. Expectations and entropy inequalities for finite quantum systems. *Communications in Mathematical Physics*, 39(2):111–119, June 1974.

38 Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40(2):147–151, June 1975. doi:10.1007/bf01609396.

39 Iman Marvian and Seth Lloyd. From clocks to cloners: Catalytic transformations under covariant operations and recoverability, August 2016. arXiv:1608.07325.

40 William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, November 2009. arXiv:0810.2327.

41 Milán Mosonyi. *Entropy, Information and Structure of Composite Quantum States*. PhD thesis, Katholieke Universiteit Leuven, 2005. Available at https://lirias.kuleuven.be/bitstream/1979/41/2/thesisbook9.pdf.

42 Milán Mosonyi and Dénes Petz. Structure of sufficient quantum coarse-grainings. *Letters in Mathematical Physics*, 68(1):19–30, April 2004. arXiv:quant-ph/0312221. doi:10.1007/s11005-004-4072-2.

43 Michael A. Nielsen and Denés Petz. A simple proof of the strong subadditivity inequality. *Quantum Information and Computation*, 5(6):507–513, September 2005. arXiv:quant-ph/0408130.

44 Masanori Ohya and Denes Petz. *Quantum Entropy and Its Use*. Springer-Verlag, 1993.

45 Giacomo De Palma, Andrea Mari, Vittorio Giovannetti, and Alexander S. Holevo. Normal form decomposition for Gaussian-to-Gaussian superoperators. *Journal of Mathematical Physics*, 56(5):052202, May 2015. arXiv:1502.01870.

46 Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Gaussian states minimize the output entropy of one-mode quantum Gaussian channels, October 2016. arXiv:1610.09970.

47 Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. One-mode quantum-limited Gaussian channels have Gaussian maximizers, October 2016. arXiv:1610.09967.

48 Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Gaussian states minimize the output entropy of the one-mode quantum attenuator. *IEEE Transactions on Information Theory*, 63(1):728–737, January 2017. arXiv:1605.00441.

49 Gh.-S. Paraoanu and Horia Scutaru. Fidelity for multimode thermal squeezed states. *Physical Review A*, 61(2):022306, January 2000. arXiv:quant-ph/9907068. `doi:10.1103/PhysRevA.61.022306`.

50 Denes Petz. Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. *Communications in Mathematical Physics*, 105(1):123–131, 1986.

51 Denes Petz. Sufficiency of channels over von Neumann algebras. *Quarterly Journal of Mathematics*, 39(1):97–108, 1988.

52 Denes Petz. Monotonicity of quantum relative entropy revisited. *Reviews in Mathematical Physics*, 15(01):79–91, March 2003. arXiv:quant-ph/0209053.

53 Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications, September 2016. arXiv:1510.08863v6.

54 Haoyu Qi and Mark M. Wilde. Capacities of quantum amplifier channels. *Physical Review A*, 95(1):012339, January 2017. arXiv:1605.04922.

55 Derek W. Robinson and David Ruelle. Mean entropy of states in classical statistical mechanics. *Communications in Mathematical Physics*, 5(4):288–300, August 1967.

56 Mary Beth Ruskai. Inequalities for quantum entropy: a review with conditions for equality. *Journal of Mathematical Physics*, 43:4358–4375, 2002. erratum **46**, 019901 (2005); arXiv:quant-ph/0205064.

57 Stefan Scheel and Dirk-Gunnar Welsch. Entanglement generation and degradation by passive optical devices. *Physical Review A*, 64(6):063811, November 2001. arXiv:quant-ph/0103167. `doi:10.1103/PhysRevA.64.063811`.

58 Alessio Serafini. *Quantum Continuous Variables*. CRC Press, 2017.

59 Kaushik P. Seshadreesan, Mario Berta, and Mark M. Wilde. Rényi squashed entanglement, discord, and relative entropy differences. *Journal of Physics A: Mathematical and Theoretical*, 48(39):395303, September 2015. arXiv:1410.1443.

60 R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: $U(n)$ invariance, squeezing, and normal forms. *Physical Review A*, 49(3):1567–1583, March 1994. `doi:10.1103/PhysRevA.49.1567`.

61 David Sutter, Mario Berta, and Marco Tomamichel. Multivariate trace inequalities. *Communications in Mathematical Physics*, 352(1):37–58, May 2017. arXiv:1604.03023.

62 David Sutter, Omar Fawzi, and Renato Renner. Universal recovery map for approximate Markov chains. *Proceedings of the Royal Society A*, 472(2186), February 2016. arXiv:1504.07251.

63 David Sutter, Marco Tomamichel, and Aram W. Harrow. Strengthened monotonicity of relative entropy via pinched Petz recovery map. *IEEE Transactions on Information Theory*, 62(5):2907–2913, May 2016. arXiv:1507.00303.

64 Robert R. Tucci. Quantum entanglement and conditional information transmission, September 1999. arXiv:quant-ph/9909041.

65 Robert R. Tucci. Entanglement of distillation and conditional mutual information, February 2002. arXiv:quant-ph/0202144.

66 Armin Uhlmann. Endlich dimensionale dichtmatrizen, ii. *Wiss. Z. Karl-Marx-University Leipzig*, 22(Jg. H. 2.):139, 1973.

67 Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

68 Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

69 Xiang-Bin Wang, Tohya Hiroshima, Akihisa Tomita, and Masahito Hayashi. Quantum information with Gaussian states. *Physics Reports*, 448(1—4):1–111, August 2007. arXiv:0801.4604. doi:10.1016/j.physrep.2007.04.005.

70 Xiang-Bin Wang, L. C. Kwek, and C. H. Oh. Bures fidelity for diagonalizable quadratic Hamiltonians in multi-mode systems. *Journal of Physics A: Mathematical and General*, 33(27):4925, July 2000. URL: http://stacks.iop.org/0305-4470/33/i=27/a=310.

71 Mark M. Wilde. Recoverability in quantum information theory. *Proceedings of the Royal Society A*, 471(2182):20150338, October 2015. arXiv:1505.04661.

72 Mark M. Wilde. Monotonicity of p-norms of multiple operators via unitary swivels, October 2016. arXiv:1610.01262.

73 Mark M. Wilde, Patrick Hayden, and Saikat Guha. Information trade-offs for optical quantum communication. *Physical Review Letters*, 108(14):140501, April 2012. arXiv:1105.0119.

74 Mark M. Wilde and Haoyu Qi. Energy-constrained private and quantum capacities of quantum channels, September 2016. arXiv:1609.01997.

75 Andreas Winter and Ke Li. A stronger subadditivity relation? with applications to squashed entanglement, sharability and separability. notes available online at http://www.maths.bris.ac.uk/∼csajw/stronger_subadditivity.pdf , see also http://www.scribd.com/document/337859204, 2012.

76 Jon Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55(11):5339–5351, November 2009. arXiv:0706.2907.